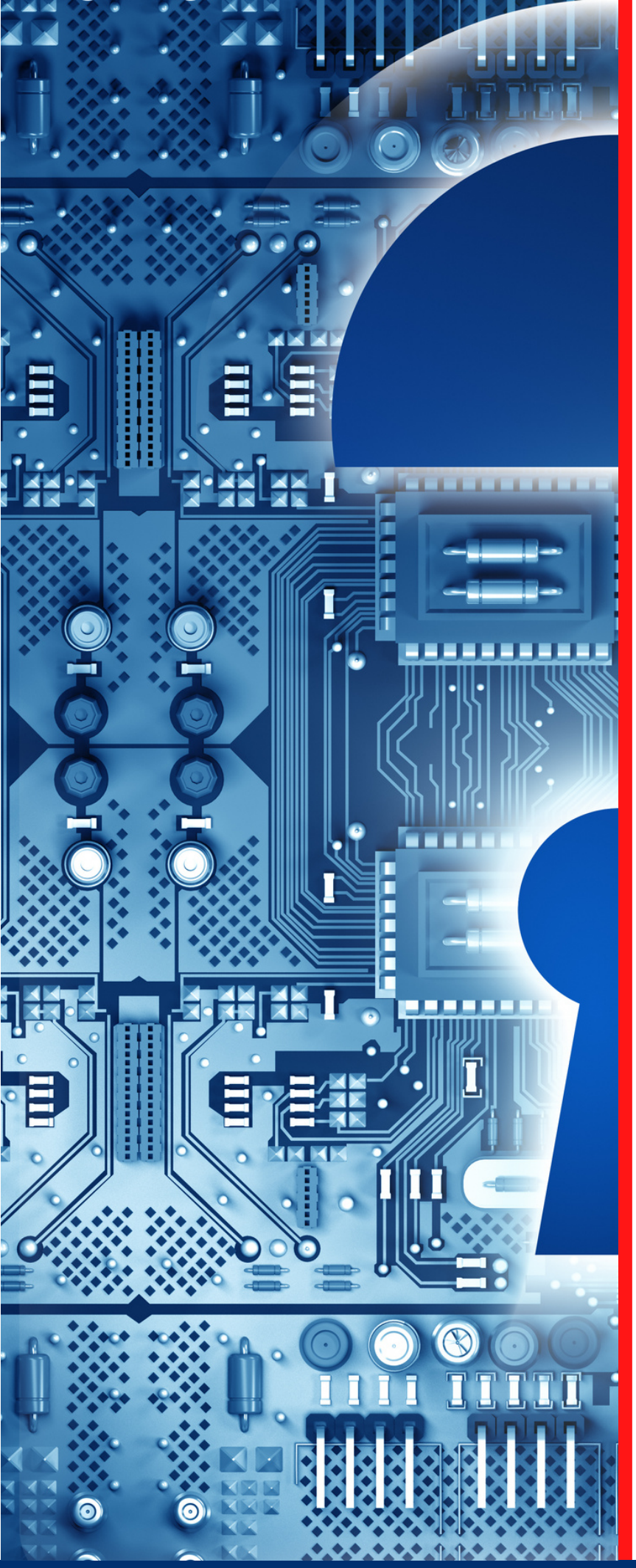


# OSIC

## ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

**14/2023**

## Ransomware

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO

**Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.**

TLP:CLEAR

# Prefácio

A análise de diversos incidentes de *ransomware* causados pelos principais grupos envolvidos nesse tipo de operação revelou que as técnicas básicas permanecem as mesmas em praticamente toda a cadeia de morte cibernética. Os padrões de ataque assim revelados não são acidentais, porque esta classe de ataque exige que os atores de ameça passem por certas etapas, como penetrar na rede corporativa ou no *host* alvo, realizar a entrega do *malware*, realizar o mapeamento do ambiente e expandir suas atividades nesse ambiente e, finalmente, roubando dados e causando o maior impacto possível na vítima.

Este trabalho foi escrito tanto para os usuários comuns, de forma que tenham um entendimento básico sobre o *ransomware* e seu ciclo de vida, como para as equipes de tecnologia da informação, analistas de segurança da informação, especialistas em forense digital e todos aqueles que estejam envolvidos no processo de resposta a incidentes de *ransomware* e que precisam proteger seu ambiente de incidentes de *ransomware*.

Por esse motivo, foram selecionadas as técnicas mais comumente utilizadas pelos 8 (oito) grupos mais populares e ativos (Conti/Ryuk, Pysa, Clop, Hive, Lockbit, RagnarLocker, BlackByte, BlackCat), analisando de forma mais detalhada essas técnicas e apresentando algumas possibilidades de mitigação e detecção dessas técnicas.

Este trabalho se divide em:

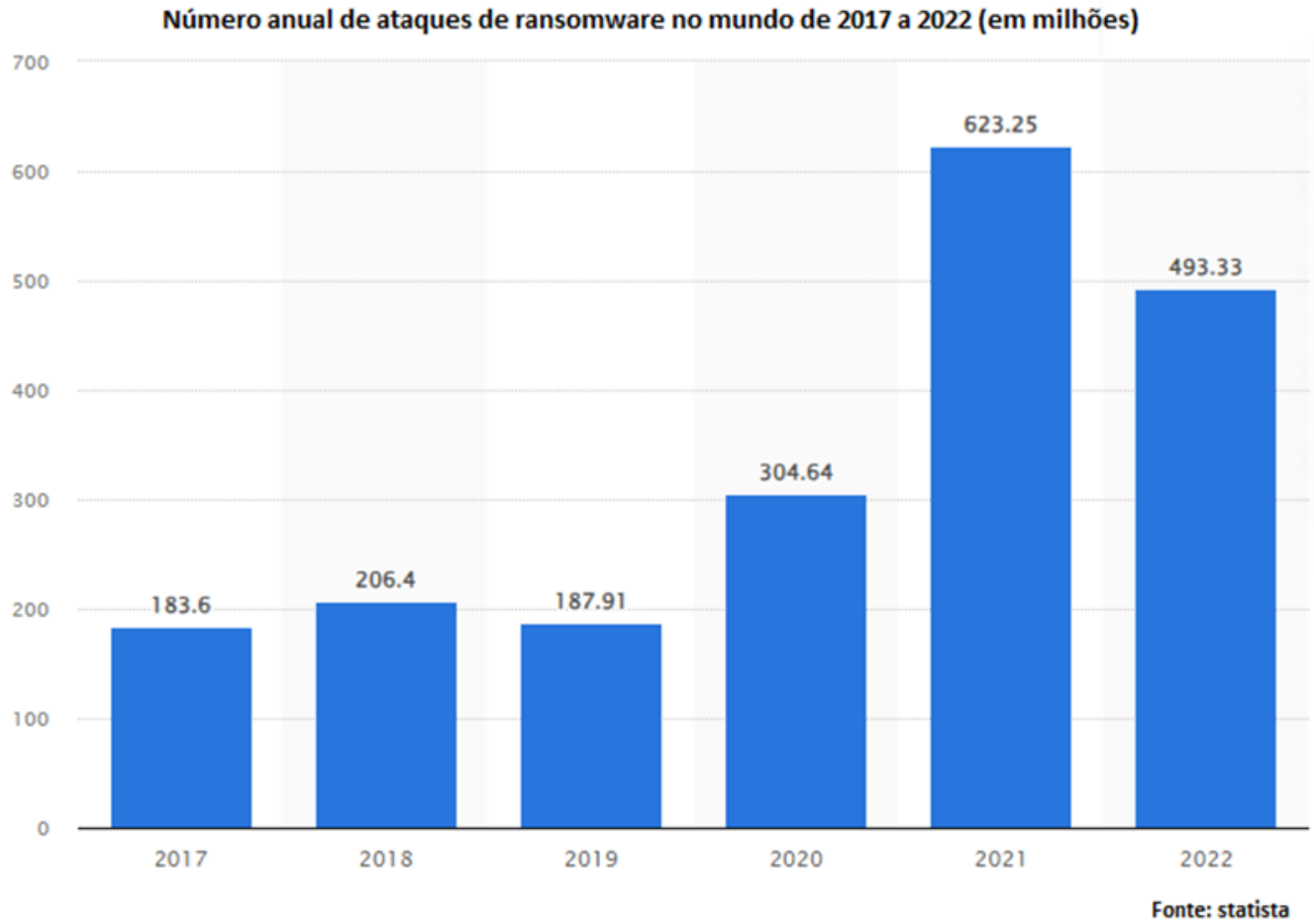
- Uma breve introdução sobre o cenário atual do *ransomware* no mundo;
- Um breve histórico sobre a evolução do *ransomware*;
- O surgimento do *Ransomware as a Service* (RaaS) e do modelo *Big Game Hunting* (BGH);
- A relação entre o *ransonware* e as criptomoedas;
- O ciclo de vida de um incidente de *ransomware* e os atores envolvidos nas fases do incidente;
- As etapas de um ataque de *ransomware*, detalhando as técnicas mais comumente utilizadas relativas:
    - Ao acesso inicial;
    - Ao estabelecimento do ponto de apoio e Comando-e-Controle (C2);
    - As ações de mapeamento e expansão das atividades de ataque;
    - A exfiltração de dados; e
    - A geração de impacto no ambiente vítima;

- A fase de comunicação e extorsão pelo ator de ameaça e algumas considerações sobre o pagamento de resgate;
- A fase de recuperação do ambiente em função de um incidente de *ransomware*; e
- Considerações finais.

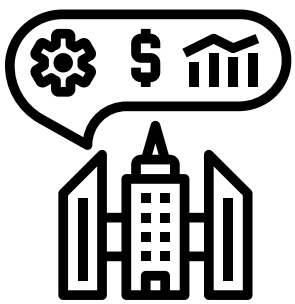
Foram utilizadas como referências para a elaboração deste trabalho as melhores práticas e recomendações do *Escal Institute of Advanced Technologies* (SANS), do *Cybersecurity and Infrastructure Security Agency* (CISA), do *Multi-State Information Sharing and Analysis Center* (MS-ISAC), do *National Institute of Standards and Technology* (NIST) e do MITRE ATT&CK.

# I - Introdução

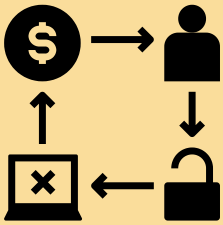
O *ransomware* tem sido uma ameaça proeminente desde meados dos anos 2000. Em 2017, o *Internet Crime Complaint Center* (IC3) do FBI recebeu 1.783 reclamações de *ransomware* que custaram às vítimas mais de US$ 2,3 milhões (https://www.ic3.gov/Home/AnnualReports?redirect=true). Essas denúncias, no entanto, representam apenas os ataques relatados ao IC3. O número real de incidentes e custos de *ransomware* é muito maior. Na verdade, houve cerca de 493 milhões de ataques de *ransomware* somente no ano passado (https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ ).




Os ataques de *ransomware* geralmente visam organizações que coletam grandes quantidades de dados e são extremamente importantes. No caso de um ataque, muitas dessas organizações preferem pagar o resgate para restaurar os dados roubados em vez de relatar o ataque imediatamente. Os incidentes de perda de dados também prejudicam a reputação das empresas, sendo este um dos motivos pelos quais os ataques de *ransomware* não são reportados.



# II - Um breve histórico do *ransomware*



A criação do termo *ransomware* se baseou na ideia da utilização de um *software* de sequestro (*ransom software*).

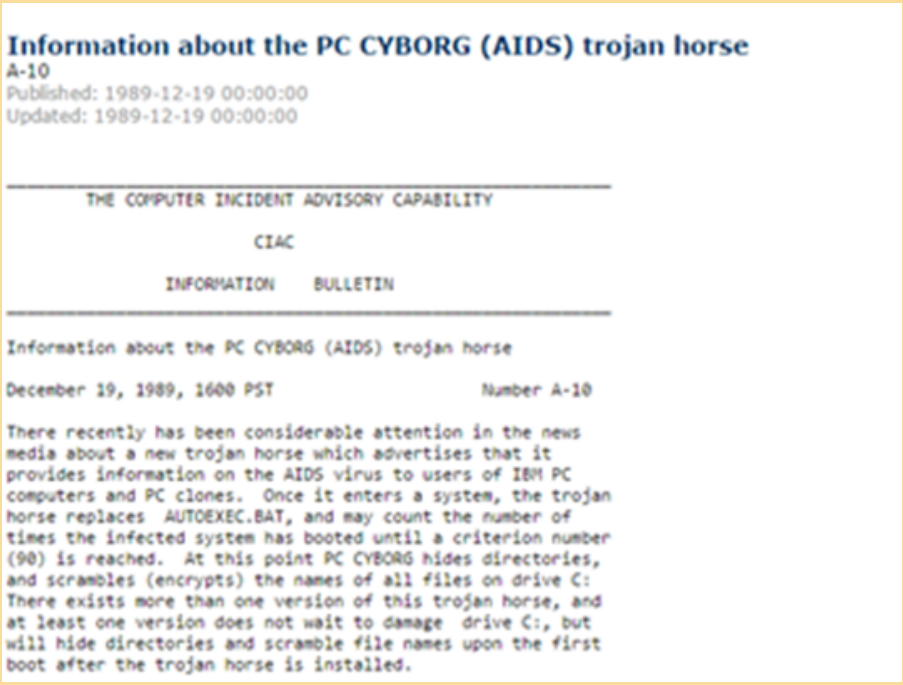
Embora o *ransomware* tenha estado nas manchetes consistentemente nos últimos cinco anos, a ideia de tornar arquivos ou computadores de usuários reféns de um ator de ameaça através da criptografia dos arquivos, dificultando o acesso ao sistema ou outros métodos – e exigindo um resgate para devolvê-los – é bastante antiga.

No final da década de 1980, criminosos já mantinham arquivos criptografados como reféns em troca de dinheiro enviado pelos correios. Um dos primeiros incidentes de *ransomware* já documentados foi o AIDS *Trojan*, lançado em 1989 por Joseph Popp, PhD e pesquisador da AIDS. Ele realizou o ataque distribuindo pelo correio 20.000 disquetes aos participantes da conferência sobre AIDS da Organização Mundial da Saúde em Estocolmo. Os pesquisadores recebiam o disquete com a informação de que eles continham um programa que analisava o risco de um indivíduo adquirir AIDS através do uso de um questionário.


**Foto de um dos 20.000 discos distribuídos com o AIDS Trojan.** Fonte: Eddy Willem

Ao instalar o programa, os computadores das vítimas eram contaminados com o PC Cyborg (um vírus simples que aplica uma criptografia simétrica nos arquivos da vítima) e que inicialmente ficava dormente, sendo ativado apenas após o computador vítima ser reiniciado 90 vezes. Quando esse limite era atingido, o *malware* era ativado e apresentava uma mensagem exigindo o pagamento de US$ 189 para uma caixa postal no Panamá para restaurar o acesso aos seus sistemas e mais US$ 387 pelo licenciamento do *software* de questionário.

O esquema ganhou as manchetes e apareceu no *Virus Bulletin*, uma revista de segurança para profissionais, um mês depois dos primeiros casos.



**Information about the PC CYBORG (AIDS) trojan horse**
A-10
Published: 1989-12-19 00:00:00
Updated: 1989-12-19 00:00:00

THE COMPUTER INCIDENT ADVISORY CAPABILITY

CIAC

INFORMATION BULLETIN

Information about the PC CYBORG (AIDS) trojan horse

December 19, 1989, 1600 PST Number A-10

There recently has been considerable attention in the news media about a new trojan horse which advertises that it provides information on the AIDS virus to users of IBM PC computers and PC clones. Once it enters a system, the trojan horse replaces AUTOEXEC.BAT, and may count the number of times the infected system has booted until a criterion number (90) is reached. At this point PC CYBORG hides directories, and scrambles (encrypts) the names of all files on drive C: There exists more than one version of this trojan horse, and at least one version does not wait to damage drive C:, but will hide directories and scramble file names upon the first boot after the trojan horse is installed.

**Aviso sobre o PC Cyborg no Virus Bulletim, em 1989.** Fonte: Security Focus

Embora fosse um *malware* bastante básico, foi a primeira vez que muitas pessoas ouviram falar do conceito - ou de extorsão digital. Não está claro se alguma pessoa ou organização pagou o resgate, mas é certo que o incidente causou enormes danos à época, com diversos pesquisadores perdendo todo o trabalho armazenado nos computadores afetados.

Inicialmente, os ataques de *ransomware* continuaram explorando o conceito de um ator de ameaça utilizando um programa para criptografar os arquivos de uma vítima e exigindo um resgate em troca da chave de descriptografia associada a esses arquivos.

Um exemplo de ataque de *ransomware* concentrado na criptografia de dados é o Jigsaw. O *ransomware* Jigsaw original foi criado em 2016 em associação com um esquema de *phishing* por *e-mail*. Tornou-se famoso graças a uma imagem do assassino Jigsaw do filme '*Saw*' exibida na nota de resgate (daí seu nome) e sua maneira única de persuadir as vítimas a pagar o resgate - se os pagamentos não fossem feitos no período de 60 minutos, o Jigsaw começaria a excluir arquivos da máquina infectada.

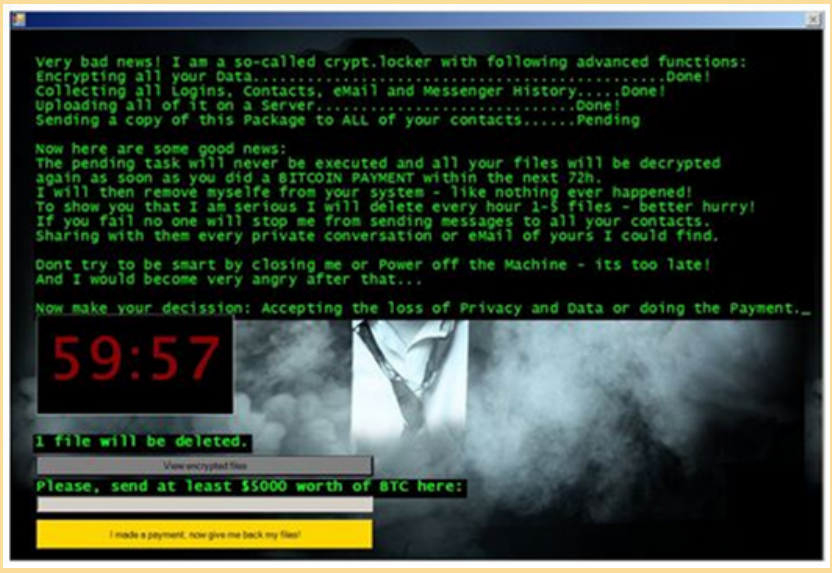
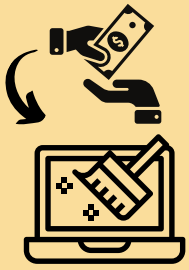



**Imagem da tela de resgate do Jigsaw** Fonte: Check Point Software Technologies

A tela de resgate também incluía um botão que a vítima deveria pressionar (“*I made a payment, now give me back my files!*”) assim que o pagamento fosse feito. O *ransomware* então verificava a conta para o depósito e se o pagamento realmente fosse realizado, ele atualizava o *malware* para descriptografar todos os arquivos e, em seguida, excluir todos os componentes do *ransomware*, colocando o computador de volta em seu estado original.




Ainda em 2016, uma equipe de pesquisadores do *Check Point Software Technologies* realizou vários testes com o Jigsaw, sem efetuar o pagamento solicitado, e verificou que ao clicar no botão “*I made a payment, now give me back my files!*” o programa realizava uma chamada HTTP GET para:

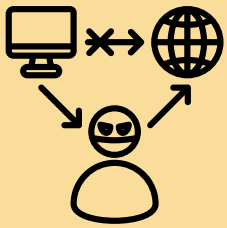
btc.blockr[.]io/api/v1/address/balance/<bitcoin-account>

e recebia como resposta um json

{“status”:”success”,”data”:{“address”:”<bitcoin- account>”,”balance”:0,”balance_multisig”:0},”code”: 200,”message”:””}

o que ainda mantinha o *malware* ativo.

Os pesquisadores então utilizaram uma solução *man-in-the-middle* para alterar a resposta recebida de forma a burlar o *malware*, alterando a variável “balance” na resposta de 0 para 10 (que seria o valor em *bitcoins* para pagar o resgate no teste). A solução funcionou e o *malware*, acreditando que o pagamento havia sido realizado, iniciou o processo de descriptografação dos arquivos e de sua auto remoção do computador infectado.

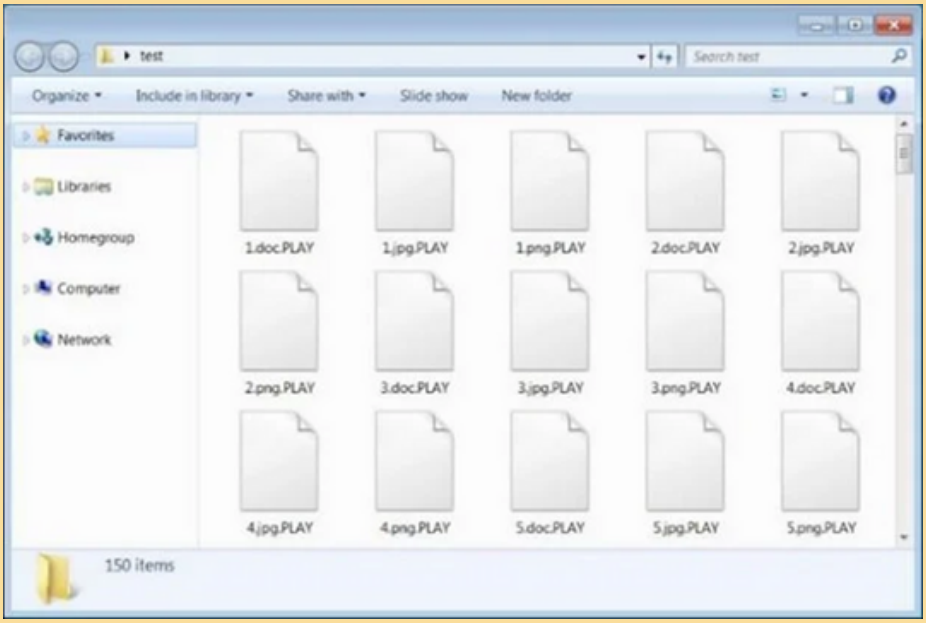


Essa solução simples ainda funciona contra várias das variantes do Jigsaw, e a *Check Point* disponibiliza uma ferramenta de decriptação (*CheckPoint Jigsaw Puzzle Solver*) baseada nessa solução:
(http://blog.checkpoint.com/wp-content/uploads/2016/07/JPS_release.zip ).

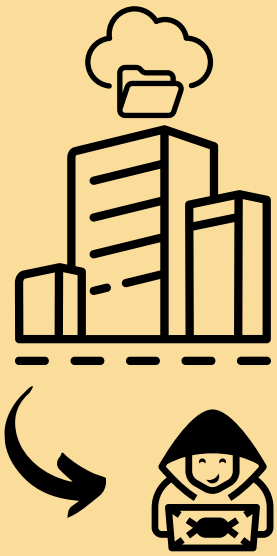
Uma das novas variantes do Jigsaw atua de maneira mais destrutiva. Uma vez instalada, ela procura por arquivos da vítima no armazenamento do OneDrive. Depois de criptografar esses arquivos, ela se vale da sincronização automática do OneDrive com as unidades locais e de rede, o que acaba por possibilitar a infecção de organizações inteiras de uma só vez.

Como uma forma de combater organizações que tinham *backups* seguros ou os recursos necessários para quebrar os métodos de criptografia utilizados, os atores de ameaça passaram a utilizar um método que é conhecido como campanha de extorsão dupla na qual o ator de ameaça não apenas criptografa os dados, mas também os extrai antes da criptografia. Isso fornece aos atores de ameaça uma vantagem extra nas negociações de resgate, pois mesmo que a vítima consiga recuperar os arquivos, o ator de ameaça ainda pode ameaçar a vítima de liberar dados privados para o público caso o pagamento não ocorra.

O *ransomware* PLAY (também conhecido como PlayCrypt) é um exemplo de campanha que utiliza a extorsão dupla. Lançado em junho de 2022, concentrou seus esforços iniciais em organizações na América Latina – sendo o Brasil seu principal alvo – e atualmente tem ampliado seu escopo de ataque, sendo utilizado em organizações na Índia, Hungria, Espanha e Holanda.



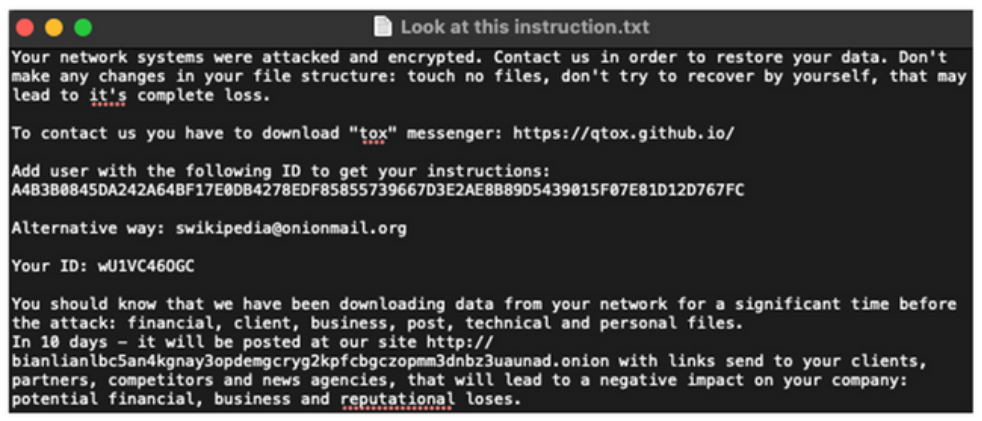

O Play criptografa os arquivos da vítima – incluindo a extensão .play nos arquivos criptografados (daí o seu nome) – e também exfiltra dados do sistema infectado, incluindo no diretório raiz das máquinas infectadas uma nota de *ransomware* com um endereço de *e-mail* para as vítimas entrarem em contato. A vítima, além de perder acesso aos seus arquivos também sofre a ameaça do vazamento público dos dados exfiltrados caso o pagamento não seja realizado.



Além do impacto imediato do vazamento de dados ou de sua criptografia, o *ransomware* pode gerar inúmeros efeitos em cascata para seus usuários. O ataque de *ransomware* ao Kronos Private Cloud, uma suíte de software de recursos humanos do Ultimate Kronos Group – UKG, ocorrido em 2022, interrompeu as operações na nuvem de diversas empresas por todo o mundo, em especial os relativos ao sistema de folha de pagamento. Nos Estados Unidos da América, o incidente obrigou cidades e estados inteiros a elaborarem planos de emergência para pagar os salários de seus trabalhadores, além de afetar as operações de recursos humanos de grandes empresas como o Metrô de Nova Iorque, Honda Motors, GameStop, Tesla e outras (https://www.theverge.com/2021/12/15/22838737/kronos-ukg-ransomware-attack-payroll-tesla-whole-foods-cybercrime).

Curiosamente, agora em 2023, foi observada uma nova evolução nas técnicas de ataque de *ransomware*, com o grupo de *ransomware* BianLian abandonando seus esforços de criptografia e se concentrando apenas na extorsão em função da exfiltração de dados.

Originalmente, as campanhas do BianLian usavam a extorsão dupla, como pode ser visto na nota de resgate da figura na próxima página.



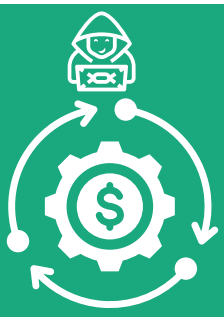

Fonte: https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye

Uma das razões para essa mudança tem sido o surgimento de ferramentas de decriptação específicas contra campanhas de *ransomware*. No caso específico do grupo BianLian, a mudança na maneira de conduzir suas operações ocorreu após o lançamento pela Avast de uma ferramenta de decriptação que permitiria que uma vítima do BianLian recuperasse seus arquivos (https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/ ).

Em vez de continuar seguindo o típico modelo de extorsão dupla, com a criptografia de arquivos e ameaça de vazamento dos dados exfiltrados, o grupo BianLian tem optado por renunciar à criptografia dos dados das vítimas e se concentrar em convencê-las a pagar apenas usando uma demanda de extorsão em troca do silêncio, prometendo não vazar os dados roubados ou divulgar o fato de que a organização vítima sofreu uma violação após o pagamento. O grupo BianLian oferece essas garantias com base no fato de que seu "negócio" depende de sua reputação, utilizando o texto a seguir (https://www.cybersecurityconnect.com.au/strategy/8838-ransomware-group-bianlian-refines-tactics-in-the-face-of-free-decrypter ).

*"Our business depends on the reputation even more than many others. If we will take money and spread your information – we will have issues with payments in future. So, we will stick to our promises and reputation. That works in both ways: if we said that we will email all your staff and publicly spread all your data – we will."*

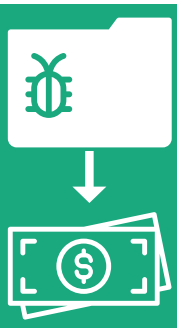
## III - *Ransomware* como Serviço (*Ransomware as a Service*) – RaaS e o *Big Game Hunting* - BGH



O modelo de negócios de *Ransomware* como Serviço– RaaS existe há mais de uma década e é um modelo que envolve grupos de *ransomware* e grupos afiliados. Os grupos de *ransomware* desenvolvem modelos de ataque e os distribuem num formato de RaaS para seus grupos afiliados. Os grupos afiliados utilizam esses modelos de forma independente para atacarem os seus alvos de interesse. De acordo com esse modelo de negócios, o grupo de *ransomware* que criou o RaaS recebe uma taxa de serviço por resgate coletado.

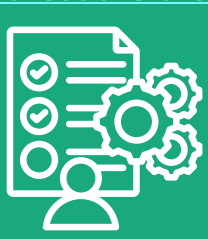
Os grupos de *ransonware* Petya e Cerber foram pioneiros em esquemas de RaaS. Os autores do Cerber foram especialmente oportunistas, oferecendo suas operações de *ransomware* como um serviço em troca de um retorno de 40% nos lucros obtidos com resgates pagos.

De acordo com os pesquisadores da Check Point, o Cerber infectou 150.000 vítimas apenas em julho de 2016, recebendo cerca de US$ 195.000 – dos quais US$ 78.000 foram para os autores do *ransomware*. (https://www.zdnet.com/article/ransomware-as-a-service-for-allows-wannabe-hackers-to-cash-in-on-cyber-extortion/ ). Atualmente, os afiliados do grupo de *ransomware* Qilin – também conhecido como Agenda – podem ficar com até 80% do resgate pago – se o resgate for de até US$ 3 milhões. Acima dos 3 milhões de dólares, os afiliados podem ficar com até 85% do resgate (https://www.theregister.com/2023/05/17/ransomware_affiliates_money/#:~:text=Ransomware-flinging%20affiliates%20are%20often%20large%20organizations%20with%20upwards,LockBit%2C%20BlackCat%2C%20Hive%2C%20and%20BlackBasta%2C%20according%20to%20Malwarebytes ).



Os altos lucros obtidos têm alavancado o modelo RaaS. No primeiro trimestre de 2022, foram identificados 31 grupos de extorsão de RaaS em todo o mundo, em comparação com os 19 grupos existentes no mesmo trimestre de 2021 (https://www.statista.com/statistics/1374743/number-of-raas-and-extortion-groups-worldwide/ ).

As operações dos desenvolvedores de RaaS se assemelham a modelos legítimos de SaaS. As organizações vendem ou alugam seus kits RaaS para afiliados que os utilizam para realizar seus próprios ataques. Os grupos RaaS também oferecem outros serviços, como suporte, ofertas agrupadas, análises e fóruns. Já os grupos afiliados que realizam o ataque de *ransomware* geralmente são grandes organizações com mais de 100 funcionários, entre eles desenvolvedores, gerentes, negociadores e outros funcionários. Alguns afiliados estão entre os grupos de ameaças mais notórios do mundo, como LockBit, BlackCat, Hive e BlackBasta (https://www.theregister.com/2023/05/17/ransomware_affiliates_money/#:~:text=Ransomware-flinging%20affiliates%20are%20often%20large%20organizations%20with%20upwards,LockBit%2C%20BlackCat%2C%20Hive%2C%20and%20BlackBasta%2C%20according%20to%20Malwarebytes ).



Para otimizar seus esforços, os agentes de ataque, em especial os que utilizam o RaaS, decidiram abandonar o estilo de ataques "pulverizar e rezar" que dominava o espaço do *ransomware* e se concentrar no modelo *Big Game Hunting* – BGH, que utiliza o *ransomware* com táticas, técnicas e procedimentos (TTPs) comuns em ataques direcionados a organizações de alto valor.

De um modo geral, as vítimas são escolhidas com base em sua capacidade de pagar um resgate, bem como na probabilidade de fazê-lo para retomar as operações comerciais ou evitar o escrutínio público. Alvos comuns podem incluir:


- Grandes corporações;
- Bancos e outras instituições financeiras;
- Serviços de utilidade pública;
- Hospitais e outras instituições de saúde;
- Agências governamentais;
- Indivíduos com alto patrimônio líquido, como celebridades e líderes empresariais proeminentes;
- Qualquer organização que possua dados confidenciais, incluindo propriedade intelectual, segredos comerciais, dados pessoais ou registros médicos.

Os grupos que atuam em BGH são extremamente sofisticados, muitas vezes trabalhando como parte de um grupo organizado para derrubar alvos importantes. Em muitos casos, esses grupos operam como redes altamente estruturadas e organizadas, não muito diferentes das empresas corporativas, e utilizando o RaaS. Alguns desses grupos, inclusive, são patrocinados por um Estado, com vínculos diretos com agências governamentais ou com figuras públicas proeminentes.

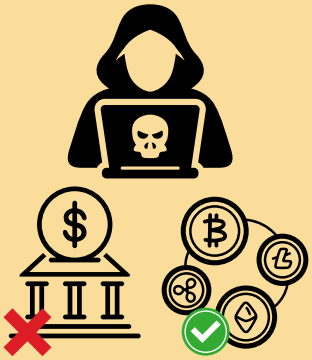
A tabela abaixo apresenta alguns RaaS e operadores BGH afiliados.

| RaaS | Técnica | Operador BGH afiliado |
|---|---|---|
| DarkSide | Os operadores DarkSide tradicionalmente se concentram em máquinas Windows e recentemente expandiram para o Linux, visando ambientes corporativos executando hipervisores VMware ESXi sem patch ou roubando credenciais do vCenter. | CARBON SPIDER |
| REvil | REvil é um RaaS que se baseia mais em extorsão, com as vítimas recebendo um aviso de vazamento de dados iminente se o resgate não for pago. | PINCHY SPIDER |
| Dharma | Os ataques de ransomware Dharma estão associados principalmente a ataques de protocolo de área de trabalho remota (RDP). As variantes do Dharma vêm de muitas fontes e são de natureza quase idêntica, tornando difícil determinar quem está por trás de um ataque. | Ligado a um grupo de ameaças iranianas com motivação financeira. Não controlado centralmente. |
| LockBit | Em desenvolvimento desde 2019, os ataques LockBit exigem um resgate para evitar a publicação de um conjunto de dados roubados. Está confirmado que o RaaS esteve envolvido em pelo menos nove ataques | Afiliado a usuários russos, ou usuários que falem russo, ou usuários de língua inglesa com um garantidor que fale russo. |

Fonte: Crowdstrike (https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/ )

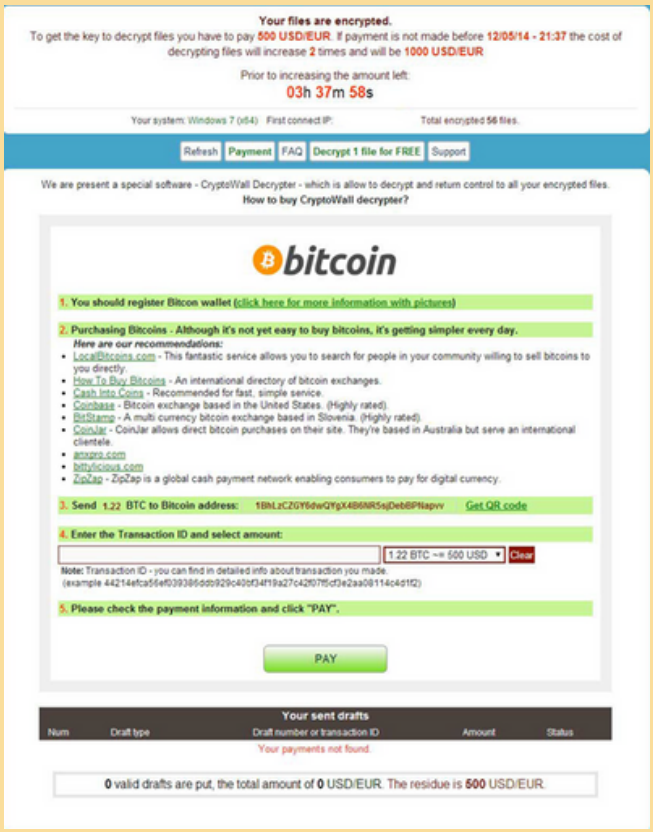
# IV – A relação entre o *Ransomware* e as Criptomoedas

É importante observar que apesar de sua longa história, os incidentes de *ransomware* ainda não eram tão difundidos nos anos 2000 – provavelmente devido a dificuldades com a cobrança de pagamentos. O surgimento e popularização das criptomoedas, como o Bitcoin em 2010, mudou tudo isso. À medida que as criptomoedas começaram a ganhar mais popularidade, os desenvolvedores de *ransomware* perceberam que esse era o método de transação monetária que procuravam.



As trocas em criptomoedas forneciam aos atores de ameaça os meios de receber pagamentos instantâneos de suas vítimas de forma anônima e não rastreável, sendo todas as transações realizadas fora das restrições das instituições financeiras tradicionais. Apesar dessa facilidade, esse modelo de negócios de *ransomware* ainda é imperfeito porque embora os pagamentos em criptomoedas sejam transações úteis para os criminosos cibernéticos, eles nem sempre são fáceis de utilizar por vítimas que não são experientes nesse tipo de tecnologia.

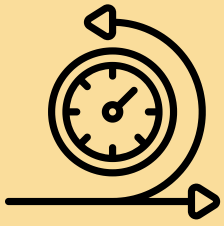
Em 2015, alguns grupos, como o Cryptowall 4 criaram páginas personalizadas para suas vítimas com orientações de como realizar a aquisição de criptomoedas para o pagamento de resgates.




Página do grupo CryptoWall 4 fornece instruções a uma vítima dos procedimentos para a aquisição de bitcoins para o pagamento de resgates e do tempo restante para a realização do pagamento (fonte da imagem https://www.bleepingcomputer.com/news/security/cryptowall-4-0-released-with-new-features-such-as-encrypted-file-names/ )

A evolução da gravidade dos ataques de *ransomware* e dos valores solicitados pelos atores de ameaça, implicando na aquisição de volumes significativos de criptomoedas, tornou o pagamento dos resgates mais problemático. Isso levou os principais grupos de *ransomware* a implementar ou contratar *call centers* tanto para pressionar as vítimas como fornecer o suporte técnico relativo ao processo de inscrição e operação com os corretores de criptomoedas a fim de realizar o pagamento dos resgates (https://www.bankinfosecurity.com/interviews/ransomware-gangs-practice-customer-relationship-management-i-4441 e https://www.bankinfosecurity.com/ransomware-call-centers-cold-call-victims-to-demand-ransom-a-15535 ).

Esse tipo de dificuldade também levou ao aparecimento de empresas que funcionam como corretores de criptomoedas que auxiliam as vítimas de *ransomware* no processo de pagamento do resgate (https://www.cnbc.com/2021/06/10/digitalmint-helps-ransomware-victims-make-bitcoin-payments.html ). A Digitalmint, por exemplo, é uma empresa especialista que é contratada depois que os consultores forenses, a empresa e as partes interessadas, determinaram que esgotaram todas as opções técnicas e que pagar o resgate do ponto de vista econômico é a melhor maneira de seguir em frente.

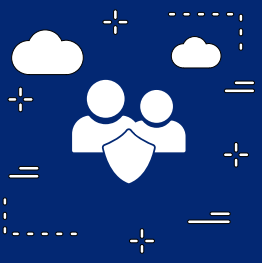


No espaço de 30 a 60 minutos a partir do contato inicial, a DigitalMint consegue efetuar o pagamento do resgate pela vítima. Isso inclui investigar o ator de ameaça para garantir que ele não esteja vinculado a um país sancionado pelos Estados Unidos da América, contatar os corretores de criptomoedas e realizar as transações necessárias para adquirir o volume de criptomoedas necessário para pagar o resgate.

# V - Ciclo de vida do incidente de *Ransomware*

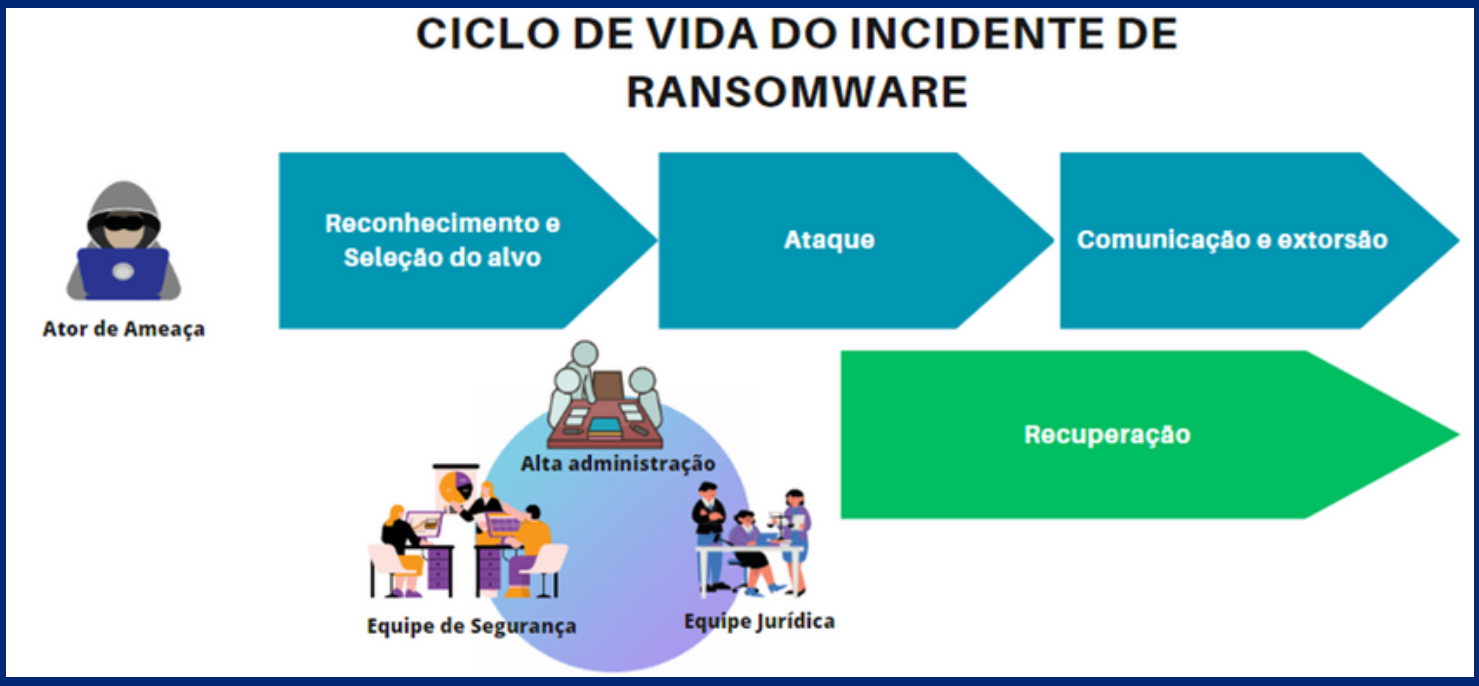
Os incidentes de *ransomware* são generalizados e devastadores, visando organizações e causando estragos em operações, finanças e reputação. Para se defender dessas ameaças, as equipes de segurança devem entender o ciclo de vida do *ransomware*.

À medida que a dependência de sistemas e redes digitais aumenta, o risco da ocorrência de um incidente de *ransomware* cresce exponencialmente. Ataques de *ransomware* podem paralisar empresas, interromper serviços, comprometer dados e levar a perdas financeiras significativas.



Os atores de ameaças evoluem continuamente suas táticas, exigindo constante adaptação das equipes de segurança. Como parte de sua operação, eles trabalham de modo a compreender o negócio que foi comprometido. Isso é para que eles possam exigir o maior resgate que acreditam que uma organização estaria disposta a pagar e distribuir seus esforços comprometendo redes com base no retorno esperado.

Apesar de existirem vários atores de ameaça conhecidos no cenário do *ransomware*, cada um com suas respectivas ferramentas, abordagens e táticas, a análise dos incidentes revela que há pontos em comum entre eles e várias oportunidades para as organizações detectarem, prevenirem e responderem a esse tipo de ameaça.



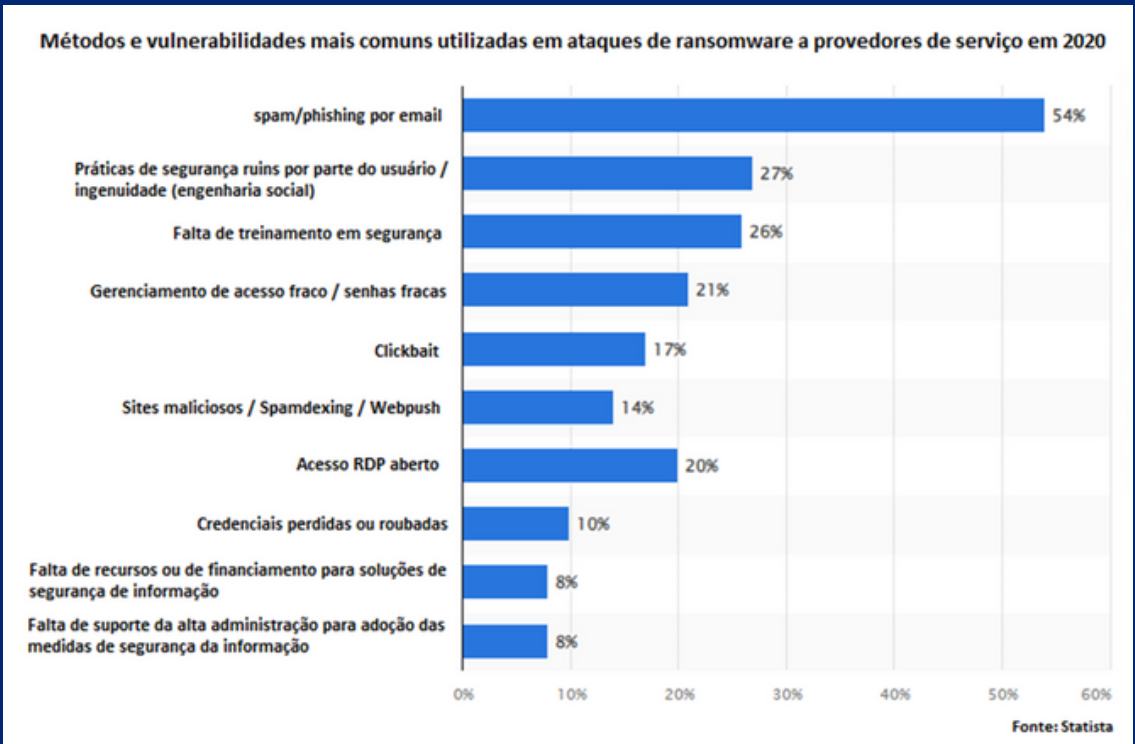

O primeiro passo para se preparar para um incidente de *ransomware* é entender o seu ciclo de vida. De maneira geral, é possível identificar 4 fases no ciclo de vida de um incidente de *ransomware*:

- Reconhecimento e seleção do alvo;
- Ataque de *ransomware*;
- Comunicação e extorsão; e
- Recuperação do incidente.

As fases de Reconhecimento e Seleção do Alvo, Ataque e Comunicação e Extorsão são realizadas pelo ator de ameaça. A fase de recuperação é de responsabilidade da organização vítima e envolve, geralmente, as equipes de segurança da informação, a equipe jurídica e a alta administração.

Cabe observar que a fase de Recuperação, realizada pela organização alvo, se inicia quando se consegue detectar o incidente. Preferencialmente, esta detecção deve ocorrer nos momentos iniciais da fase de Ataque, quando ainda é possível adotar, proativamente, medidas para conter a ameaça. Caso a organização só tome conhecimento do incidente na etapa de Comunicação e Extorsão, a fase de Recuperação se inicia de forma extremamente tardia, sendo composta basicamente de atividades reativas, pois provavelmente já ocorreu a exfiltração e a criptografia e/ou destruição dos dados pelos atores de ameaça, sendo o impacto extremamente maior.

Outro ponto importante a ser ressaltado é que a grande maioria dos incidentes de *ransomware* explora falhas humanas, conforme pode ser visto no gráfico a seguir.




Em função dos métodos utilizados e vulnerabilidades exploradas em incidentes de *ransomware*, algumas das principais medidas que podem ser adotadas imediatamente, independentemente dos métodos e técnicas de ataque são:

- Conscientizar e treinar todos os funcionários sobre as melhores práticas de segurança cibernética, dentre elas: usar proteção de senha forte, conectar-se apenas a *Wi-Fi* seguro e nunca clicar em *links* de *e-mails* não solicitados;
- Conhecer o ambiente, estabelecendo um inventário dos ativos da organização. Quando ocorre um incidente, não se quer perder tempo tentando entender a arquitetura existente ou descobrir onde os dados são armazenados. A resposta a um incidente sempre deve começar com uma compreensão clara dos ativos que compõem o escopo envolvido naquela situação;

- Manter as configurações seguras, aplicando as constantemente correções de segurança e atualizações aos sistemas operacionais e *softwares* em uso. Como os atores de ameaça estão constantemente procurando brechas e *backdoors* para explorar, a atualização constante dos ativos minimiza sua exposição a vulnerabilidades conhecidas;

- Estabelecer um modelo de controle de acesso forte aos ativos da organização;
- Implementar um modelo robusto de proteção e gerenciamento de credenciais, constantemente analisando o comportamento e os desvios de cada conta da força de trabalho (usuários humanos, contas privilegiadas, contas de serviço), detectando movimentos laterais e implementando o acesso condicional baseado em risco para detectar e impedir ameaças de *ransomware*;

- Estabelecer um plano de gerenciamento de vulnerabilidades, em especial:
    - Implementar e aprimorar a segurança de *e-mail*, com a implementação de uma solução de segurança de *e-mail* que possua filtragem de URL e *sandbox* de anexos. Para simplificar esses esforços, um recurso de resposta automatizada pode ser usado para permitir a quarentena retroativa de *e-mails* entregues antes que o usuário interaja com eles.

    - Monitorar continuamente o ambiente em busca de atividade maliciosa e indicadores de ataque (IOAs). Uma solução do tipo *Endpoint Detection and Response* (EDR) atua como uma câmera de vigilância em todos os *endpoints*, capturando eventos brutos para detecção automática de atividade maliciosa não identificada por métodos de prevenção e fornecendo visibilidade para ações proativas caça de ameaças.

    - Integrar a inteligência de ameaças à estratégia de segurança, monitorando os sistemas em tempo real e mantendo-se atualizado com a inteligência de ameaças mais recente para detectar um ataque rapidamente, entender a melhor forma de responder e impedir que ele se espalhe.

- Desenvolver estratégias de forma a possuir *backups* resistentes a *ransomware*. A ideia mais importante a ser considerada é que os agentes de ameaças visam *backups online* antes de implantar o *ransomware* no ambiente. Por esses motivos, é importante possuir *backups* resistentes *ransomware* utilizando estratégias como:
    - Testar frequentemente os *backups* de forma a garantir que os dados estão completos e não-corrompidos;

    - Manter um backup *off-line* em um dispositivo ou armazenamento criptografado, como um disco rígido separado do principal ou em um dispositivo externo;
    - Usar armazenamento imutável ou inalterável — algo que o *ransomware* não consegue danificar. Isso permite que se mantenha os dados em um estado em que não sejam excluídos ou modificados por ninguém por um período de tempo específico;

    - Aumentar a frequência de *backup*. Isso garantirá que o ponto de restauração de dados mais recente seja o mais próximo do possível; e
    - Implementar uma proteção de *endpoint* em servidores de *backup*.

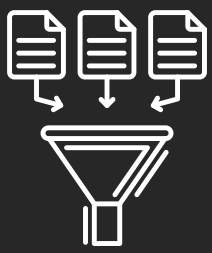
- Implementar um plano de resposta e gestão de incidentes. As equipes de resposta a incidentes devem sempre ter procedimentos bem documentados sobre como responderão a incidentes. Um manual de *ransomware* dedicado deve ser criado para entender como as investigações especificamente associadas a ataques de *ransomware* devem ser realizadas.

## VI – Fase I: Reconhecimento e seleção do alvo

A primeira fase de um incidente de *ransomware* envolve o ator da ameaça pesquisando e selecionando organizações para atacar. Durante esta fase, eles identificam alvos potenciais e coletam informações críticas sobre eles.

Atores de ameaças se envolvem em reconhecimento para identificar organizações com maior probabilidade de gerar um alto retorno em suas atividades maliciosas. Eles avaliam cuidadosamente fatores como setor, tamanho, estabilidade financeira e o valor dos dados mantidos pelos alvos em potencial. As organizações que dependem fortemente de sua infraestrutura digital e são mais propensas a pagar um resgate para recuperar o acesso a sistemas e dados críticos são os principais alvos.

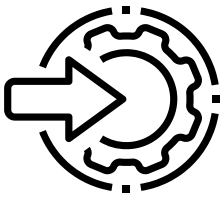
Os atores de ameaças empregam várias técnicas para coletar informações durante a fase de reconhecimento. Essas técnicas podem incluir reconhecimento passivo, onde eles coletam dados publicamente disponíveis de *sites*, plataformas de mídia social e sites de redes profissionais. Eles também podem utilizar o reconhecimento ativo, como a verificação de portas abertas e vulnerabilidades, realização de campanhas de *phishing* para coletar informações de funcionários ou alavancar fontes de terceiros, como bancos de dados vazados e fóruns da *dark web*.



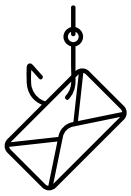
## VII – Fase II: O Ataque de *Ransomware*

De maneira geral, um ataque de ransomware segue as seguintes etapas:

# 7.1. Acesso Inicial



O acesso inicial consiste em técnicas que usam vários vetores de entrada para obter sua posição inicial dentro de uma rede. Os pontos de apoio obtidos por meio do acesso inicial podem permitir acesso contínuo, como contas válidas e uso de serviços remotos externos, ou podem ser de uso limitado devido à alteração de senhas.



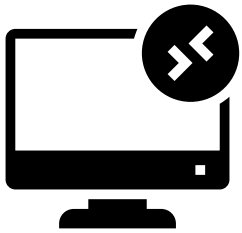
As técnicas utilizadas são bastante variadas, desde as mais comuns, como a exploração de serviços remotos e o *phishing*, até as mais sofisticadas, como o comprometimento da cadeia de suprimento (na qual se manipulam os produtos ou os mecanismos de entrega de produtos ao consumidor final com o objetivo de comprometer os dados ou sistemas).

As técnicas mais populares utilizadas pelos atores de ameaça de forma a obter o acesso inicial à vítima são:

- Exploração do *Remote Desktop Protocol* (RDP);
- Exploração de aplicações disponibilizadas ao público; e
- *Phishing*.

## 7.1.1. Exploração de serviços remotos, em especial o *Remote Desktop Protocol* (RDP)

Um dos vetores mais comuns de infecção são os serviços remotos expostos, especialmente o RDP, pois, geralmente, esses serviços não estão suficientemente protegidos.

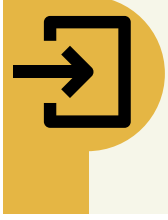


Com o aumento de organizações que optam pelo trabalho remoto, o uso de RDP pela *Internet* também aumentou. O RDP oferece aos usuários uma forma de obter uma área de trabalho remota. No entanto, é importante observar que o RDP não foi inicialmente projetado com os recursos de segurança e privacidade necessários para usá-lo com segurança na *Internet* atual. O RDP se comunica pela conhecida porta 3389, tornando-a muito fácil de descobrir por agentes de ameaças. Além disso, o método de autenticação padrão é limitado apenas a um nome de usuário e senha.

O risco de exploração do RDP exposto é ampliado, principalmente, pelos seguintes motivos:

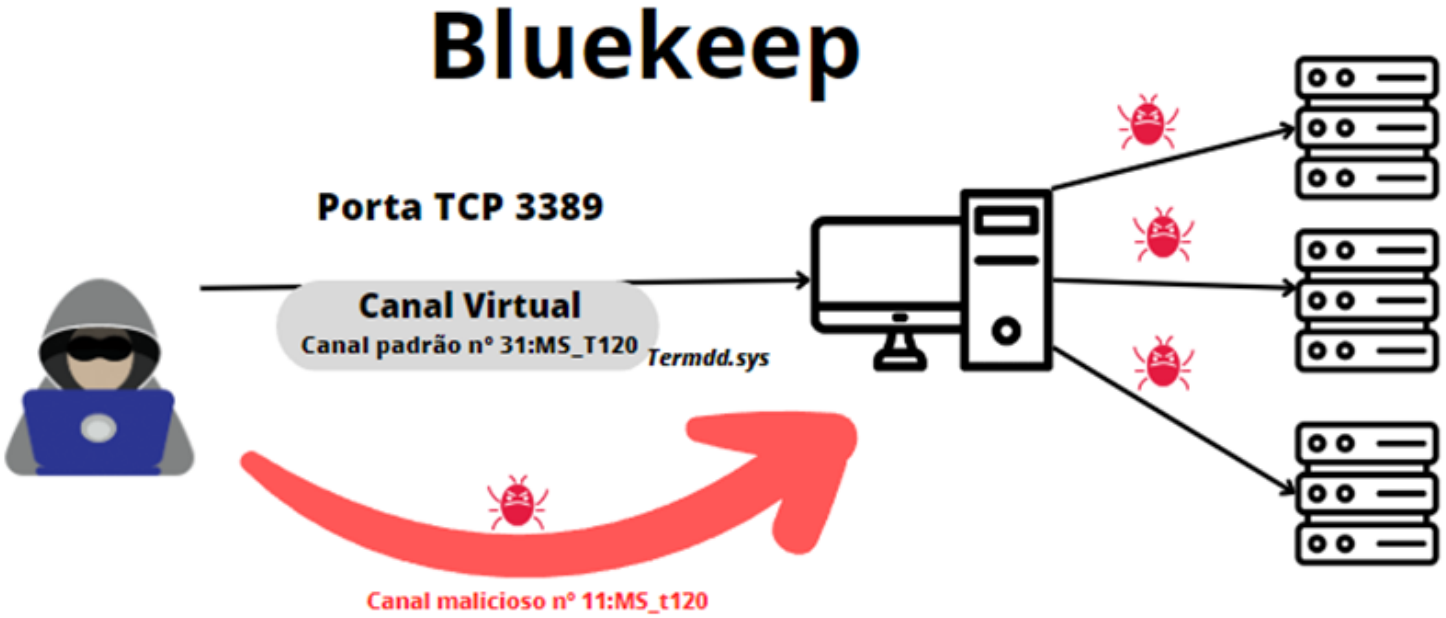
Propensão dos usuários para reutilização de senha. Diversos usuários utilizam a mesma senha tanto para acesso via RDP em sua organização como para acessar outros *sites*. Isso significa que, se um *site* for violado, os agentes de ameaças provavelmente adicionarão essa senha a uma lista para uso com tentativas de força bruta.

Política de senha ruim: uma política de senha ruim está sujeita aos mesmos problemas da reutilização de senha pelos usuários. Senhas muito curtas, pouco complexas e que sejam facilmente lembradas (como datas, nomes, etc) oferecem aos agentes de ameaças uma chance maior de sucesso na força bruta nos ataques a instâncias RDP expostas.

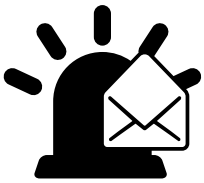


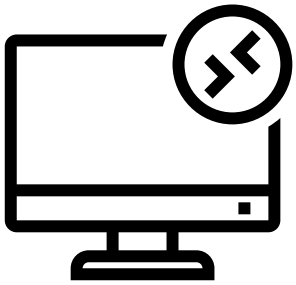
Monitoração deficiente dos *logins* RDP, permitindo que comprometimentos bem-sucedidos do RDP passem despercebidos. Caso os *logins* RDP sejam coletados, as organizações devem trabalhar para garantir que, no mínimo, *timestamps*, endereços IP e o local do *login* sejam inseridos em uma solução de gerenciamento de *log*. Infelizmente, a maioria das organizações não possui uma solução de gerenciamento de *log* ou SIEM para coletar os *logs* que podem alertar sobre seu uso indevido, aumentando o desafio para as organizações de proteger o RDP.

Os perigos da exposição do RDP - e soluções semelhantes, como TeamViewer (porta 5958) e VNC (porta 5900) - são bastante conhecidos, como o Bluekeep (CVE-2019-0708), que é uma vulnerabilidade pré-autenticação, não exige interação por parte do usuário vítima e permite ao ator de ameaça executar códigos arbitrários no *host* vítima.




Um relatório de pesquisadores da Coveware (https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority) indicou que no segundo trimestre de 2021 o *phishing* por *e-mail* e o RDP exposto à força bruta permaneceram os métodos mais baratos e, portanto, mais lucrativos e populares para os agentes de ameaças ganharem espaço inicial dentro das redes corporativas.





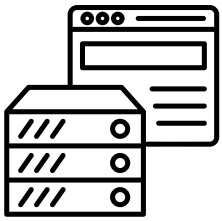
As limitações dos mecanismos de autenticação para o RDP aumentam significativamente o risco para organizações com instâncias de RDP expostas à *Internet*. Por padrão, o RDP não possui uma autenticação multifator (MFA) integrada. Para adicionar MFA aos *logins* RDP, as organizações necessitariam implementar um *gateway* de área de trabalho remota (*remote desktop gateway*) ou colocar o servidor RDP atrás de uma VPN que suporte MFA. No entanto, esses controles adicionais aumentam o custo e a complexidade que algumas organizações podem não ser capazes de suportar.

## 7.1.2.Exploração de aplicações disponibilizadas ao público

Os atores de ameaça sempre tentam encontrar falhas de configuração e vulnerabilidades não-corrigidas nas aplicações disponibilizadas ao público como uma forma de obter o acesso inicial aos sistemas. Por esse motivo, servidores MS Exchange, Apache, Sharepoint, Fortinet Fortios, Oracle Banking Payments, dentre outros, são muito visados pelos grupos de *ransomware*.

As vulnerabilidades mais comumente exploradas são as CVEs de ProxyShell.

No caso do MS Exchange, as CVE-2021-34473, CVE-2021-34523 e CVE-2021-31207 são vulnerabilidades que, quando combinadas, permitem ao ator de ameaça executar código arbitrário em um servidor vulnerável.[1] A CVE-2021-31207 permitia desviar da autenticação realizada no *Account Control List*. Já a CVE-2021-34523 permitia escalar privilégios no *Exchange PowerShell Back-end*. Por fim, a CVE-2021-34473 permitia a execução remota de código no sistema vulnerável.

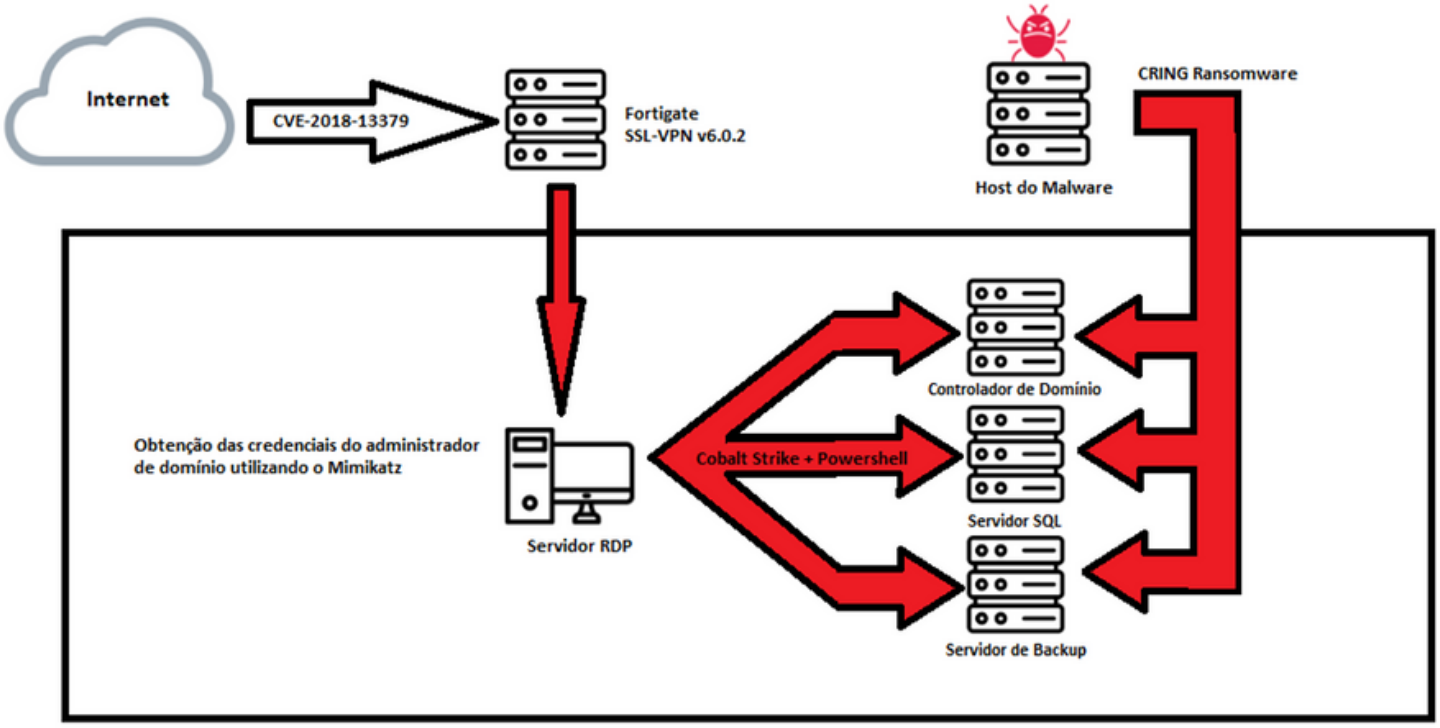


No caso do Apache, a CVE-2021-40438 era uma vulnerabilidade crítica de *server-side request forgery* (SSRF) que utilizava o *mod_proxy* e permitia forçar servidores HTTP Apache vulneráveis a encaminhar requisições a servidores arbitrários, o que dava aos atores de ameaça condições de obter ou manipular recursos que de outra forma estariam indisponíveis para eles.

Outro exemplo de exploração de vulnerabilidades conhecidas são os ataques ao FortIOS. O FortIOS é o sistema operacional da Fortinet, sendo o centro da *Fortinet Security Fabric*, considerada uma das plataformas de cibersegurança de alta performance da indústria. Apesar disso, servidores Fortinet FortIOS[2] foram atacados com sucesso por atores de ameaça que exploraram vulnerabilidades conhecidas.


Um dos ataques explorou a CVE-2018-13379, uma vulnerabilidade de *directory traversal* que permitia realizar o *download* de arquivos no sistema atacado através da utilização de uma requisição HTTP especialmente configurada.

O grupo responsável pelo ataque também utilizou o CobaltStrike associado a execução de comandos pelo Powershell para controlar o ambiente e o CRING *ransomware* para executar as ações de exfiltração e impacto.




[1] Essas vulnerabilidades afetam versões do Exchange 2013 CU23 anteriores a 15.0.1497.15, Exchange 2016 CU19 versões anteriores a 15.1.2176.12, Exchange 2016 CU20 versões anteriores a 15.1.2242.5, versões do Exchange 2019 CU8 anteriores a 15.2.792.13 e Exchange 2019 CU9 versões anteriores a 15.9.2

[2] Fortinet FortiOS 6.0.2, 5.6.7 e anteriores, FortiADC 6.1.0, 6.0.0 to 6.0.1, 5.4.0 to 5.4.4

Como pode ser visto, os atores de ameaça podem explorar vulnerabilidades existentes de formas distintas a fim de obter acesso inicial à infraestrutura. Portanto, é necessário um processo de gerenciamento de vulnerabilidades bem projetado para mitigar esse problema.

Infelizmente, nem todas as vulnerabilidades encontradas são publicadas pelos principais fornecedores em tempo hábil. Além disso, existe um número significativo de vulnerabilidades do tipo "*zero-day*".

## 7.1.3. *Phishing*

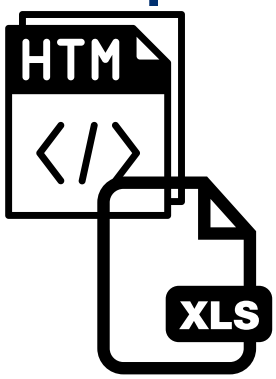
O *phishing* é considerado um dos meios mais eficientes e baratos para a obtenção do acesso inicial. Grupos de *ransomware* como o Conti, Clop, Hive e RagnarLocker utilizam constantemente a técnica de *phishing* conhecida como *Spearphishing Attachment*, na qual um *e-mail* é enviado com um arquivo anexo com o *malware* embutido (geralmente um arquivo .pdf, .doc. ou um código executável). Essa técnica depende da ação do usuário para a execução do *malware*, por esse motivo o texto do *e-mail* sempre apresenta uma razão plausível para que o usuário abra o arquivo anexo. Uma vez aberto o arquivo anexo, o *malware* é instalado e explora vulnerabilidades do sistema infectado.


Como exemplo, pode-se citar os ataques de *phishing* do grupo RagnarLocker, que exploravam a vulnerabilidade CVE-2108-0802, que permitia a execução de código remoto arbitrário no contexto do usuário logado. Se o usuário logado estivesse conectado com direitos de usuário administrativo, o ator de ameaça poderia assumir o controle do sistema afetado, sendo capaz de instalar programas, visualizar, alterar ou excluir dados, além de criar novas contas com plenos direitos de usuário.

A técnica mais clássica é utilizar um arquivo anexo do tipo documento (.doc ou .docx) ou planilha (.xls ou .xlsx). Dentro desses arquivos uma macro é utilizada para gerar um shell de linha de comando do sistema operacional e então executar comandos em lote para descarregar o *malware* que será usado no *ransomware*.

Outra técnica comum é utilizar um arquivo HTML anexo contendo o redirecionamento para um site comprometido a fim de realizar o *download* de um arquivo que será o responsável pelo *download* e instalação do *malware*.

Verifica-se, portanto, que essa técnica depende exclusivamente de fatores humanos, pois as cargas maliciosas não são iniciadas até que um usuário abra o arquivo anexo. Por esse motivo, as organizações devem realizar regularmente treinamento de conscientização, a fim de reduzir as chances de sucesso campanhas de *phishing*.



## 7.1.4. Ações de Mitigação para a Etapa de Acesso Inicial

Em relação às técnicas apresentadas, dentre as possíveis ações de mitigação temos:

- Desabilitar o serviço RDP se este for desnecessário;
- Caso o RDP seja necessário:
  - Criar um grupo específico para uso do RDP;
  - Auditar continuamente o grupo de uso do RDP, removendo usuários inativos;
  - Utilizar um *gateway* de área de trabalho remota;
  - Aplicar regras no *firewall* de forma a bloquear o tráfego RDP entre zonas de segurança da rede na rede interna;
  - Limitar o tempo máximo de duração permitido para cada sessão ativa;
  - Especificar o tempo máximo que uma sessão desconectada permanecerá ativa na sessão RDP no *host*;
  - Definir timeouts mínimos para sessões;
  - Se possível, remover o grupo de administradores locais do grupo de uso do RDP;
  - Limitar o número máximo de conexões remotas permitidas para cada usuário.
- Implementar uma política de senhas robusta;
- Implementar um programa de conscientização dos usuários;
- Isolar as aplicações e/ou executá-las em um *sandbox*;
- Desabilitar ou remover recursos e programas desnecessários, de forma a limitar o número de serviços disponíveis ao mínimo necessário;
- Segmentar a rede e os sistemas apropriadamente;
- Implementar um processo de gerenciamento de contas privilegiadas (PAM);
- Manter todos os aplicativos, serviços e programas atualizados;
- Utilizar uma solução *antimalware*;
- Utilizar um sistema de prevenção de intrusão, que são sistemas projetados para varrer e remover anexos maliciosos de *e-mails* ou *links* que podem ser usados para atividade suspeita;
- Restringir o conteúdo baseado na web, bloqueando o acesso se a atividade não puder ser devidamente monitorada ou se for identificado algum risco significativo; e
- Conscientizar e treinar os usuários.

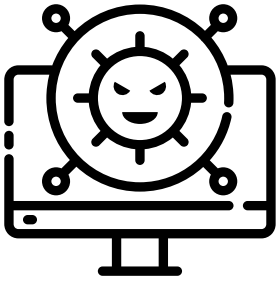
## 7.1.5. Atividades de Detecção para a Etapa de Acesso Inicial

A fim de detectar o uso das técnicas apresentadas deve-se, no mínimo, monitorar e identificar:

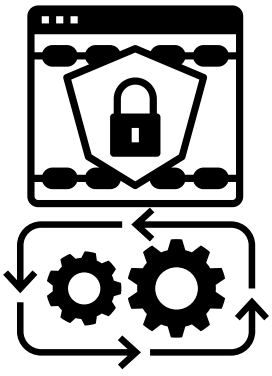
- A criação de serviços que utilizem “cmd.exe /k” ou “cmd.exe /c” em seus argumentos;
- Padrões de acesso e atividades não usuais que ocorram após o *login* remoto;
- Padrões de tráfego de rede, especialmente o SSL/TLS, e inspecionar os pacotes associados a protocolos a fim de identificar padrões não usuais de fluxo de dados;
- Fluxos de dados incomuns na rede;
- Anomalias no uso de arquivos que normalmente não iniciariam conexões com protocolos de comunicação; e
- Processos que normalmente não utilizam a comunicação por rede que estejam utilizando a rede;
- Anomalias nas operações dos aplicativos disponibilizados ao público, em especial:
  - Geração de *shell* por um processo da *Web*;
  - Surgimento de processos pai/filho não esperados durante a execução de um processo *web*;
  - Criação de arquivos incomuns, como .aspx (comuns nos casos de exploração de *ProxyShell*);
  - Argumentos/requisições suspeitas na execução de um processo *web*; e
  - Conexões de rede incomuns ou anormais durante a execução de um processo *web*.

## 7.2. Estabelecimento de ponto de apoio e C2 (Comando-e-Controle)

Após obter o acesso inicial, os atores de ameaça necessitam executar um arquivo malicioso a fim de garantir a capacidade de execução de código controlado remotamente por eles no sistema infectado.



Este estágio permite que os atores de ameaça controlem os estágios subsequentes do ataque remotamente. Durante essas comunicações de comando e controle (C2), os atores de ameaça utilizam diversos *malwares* e técnicas para estabelecer uma posição ainda mais segura no ambiente da vítima e os prepara para o mapeamento dos ativos disponíveis (descoberta) e para a expansão de suas atividades (movimento lateral, acesso a credenciais e elevação de privilégios).



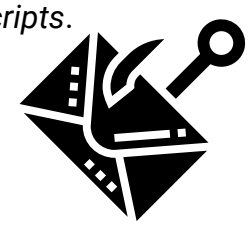
Os atores de ameaça utilizam diversas técnicas de forma a permanecerem ocultos no ambiente sem serem detectados. Ataques mais modernos e sofisticados são capazes de se adaptar ao ambiente circundante e operar de forma autônoma, misturando-se à atividade regular mesmo quando isolado de seu servidor de comando e controle. Essas variedades de *ransomware* "autossuficientes" representam um grande problema para as defesas tradicionais, que dependem de interromper as ameaças apenas com base em suas conexões externas maliciosas.

A fase de estabelecimento de ponto de apoio e C2 é composta de diversas atividades, em especial:

- Execução;
- Persistência;
- Evasão de Defesas; e
- Comando e Controle.

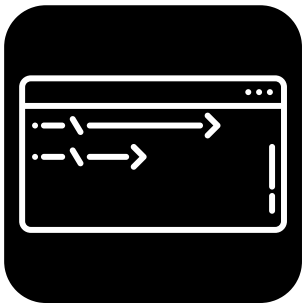
# 7.2.1. Execução

Após obter o acesso inicial, os atores de ameaça necessitam executar um arquivo malicioso a fim de garantir a capacidade de execução de código controlado remotamente por eles no sistema infectado. A principal técnica utilizada para esse fim é o uso do interpretador de comandos e *scripts*.

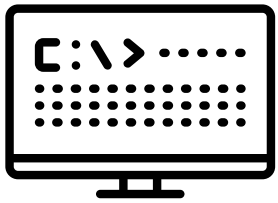


Conforme discutido anteriormente, atores de ameaça geralmente utilizam campanhas de *phishing* para descarregar código malicioso nos sistemas de suas vítimas. O arquivo malicioso geralmente contém um *script* que é executado no momento que o usuário abre o arquivo.

Em ambientes Windows, os atores de ameaça utilizam diferentes comandos do *Windows Shell* de forma a executar os *scripts* maliciosos e desviar das soluções de controle que não levam em conta o uso indevido desse utilitário Windows.



O Windows tem dois *shells* de linha de comando: o *Shell* de comando e o *PowerShell*. Cada *shell* é um programa de *software* que fornece comunicação direta entre o usuário e o sistema operacional ou o aplicativo, fornecendo um ambiente para automatizar operações de TI. O *Shell* de comando foi o primeiro *shell* integrado ao Windows para automatizar tarefas rotineiras, como gerenciamento de conta de usuário ou *backups*, utilizando os arquivos de comandos em lote (.bat). Já o *PowerShell* foi projetado para estender os recursos do *Shell* de comando para executar comandos do *PowerShell* chamados cmdlets. Os cmdlets são semelhantes aos Comandos do Windows, mas fornecem uma linguagem de *script* mais extensível.



Todos os atores de ameaça utilizam o interpretador de comandos e *scripts* (como o cmd.exe no Windows ou o *bash* no Linux) na fase de execução, pois ele é capaz de enviar pedidos reconhecíveis relativos a praticamente todos os executáveis ao sistema operacional.

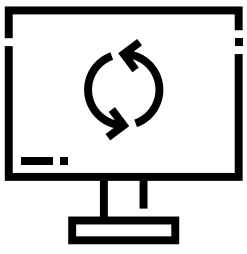
No caso do *Windows Command Shell*, por exemplo, que está presente em todas as versões do Windows, a técnica de uso do interpretador de comandos e scripts pode ser utilizada, dentre outras possibilidades:

- Execução do *shell* na técnica de execução do código malicioso pelo usuário, vista anteriormente;
- Manutenção da persistência, evasão de defesas, escalada de privilégios, descoberta de recursos e geração de impacto, utilizando utilitários como:
  - Reg.exe, que executa operações nas informações e valores em entradas do *registry*;
  - Schtasks.exe, que permite, dentre outras tarefas, agendar a execução de comandos e programas, incluir e remover tarefas do agendamento, iniciar e encerrar tarefas sob demanda, alterar as tarefas agendadas;
  - Net.exe, que gerencia praticamente qualquer aspecto da rede e suas configurações, podendo ser usado, dentre outras possibilidades, para:
    - configurar os requisitos de senha e *logon* para os usuários;
    - adicionar ou remover computadores a um domínio, além de criar e excluir grupos locais e globais;
    - apresentar a lista de arquivos abertos no servidor;

    - iniciar ou parar um serviço de rede;
    - listar os recursos compartilhados aos quais o computador está conectado e quais estão disponíveis para conexão; e
    - listar os computadores e os dispositivos de rede conectados à rede.
- Sc.exe, que se comunica com o *Service Controller* e com os serviços instalados, fornecendo capacidades similares ao *Services* no Painel de Controle. Dentre outras possibilidades, ele pode ser utilizado para:
    - recuperar e definir informações de controle sobre serviços;
    - configurar, parar ou iniciar um serviço específico; e
    - testar e debugar serviços.
- Arp.exe, que exibe e modifica entradas no cache do Protocolo de Resolução de Endereços – ARP. A cache do ARP contém tabelas – uma para adaptador de rede instalado no computador - que são usadas para armazenar endereços IPs e seus correspondentes endereços físicos resolvidos;
- Ping.exe, que verifica a conectividade no nível IP com outro computador TCP/IP e também pode ser utilizado para testar o nome de computador e o endereço IP do computador;
- Netstat.exe, que exibe conexões TCP ativas, portas nas quais o computador está em escuta, estatísticas de *Ethernet*, tabela de roteamento de IP, estatísticas de IPv4 e estatísticas de IPv6;
- Del.exe, que deleta um ou mais arquivos do computador;
- Rd.exe na sintaxe RD /S /Q <pathname>, pois o parâmetro /S pRermite deletar todos os arquivos e subdiretórios, além do próprio diretório indicado em <pathname> e o parâmetro /Q realiza a operação de forma silenciosa, ou seja, não pede confirmação do usuário. Por exemplo, o comando RD /S /Q D:\ apagaria todos os arquivos e diretórios do drive [D:];
- Vssadmin.exe, que permite deletar as cópias de sombra (*shadow copy*) de um volume;
- ftp.exe, que permite transferir arquivos de e para um computador.

Em função da grande variedade de ações possíveis, a técnica de uso do interpretador de comandos e *scripts* geralmente é adotada em todas as etapas de um ataque de *ransomware*.

## 7.2.2. Persistência



A persistência consiste em técnicas que os atores de ameaça usam para manter o acesso aos sistemas durante reinicializações, alterações de credenciais e outras interrupções que podem interromper seu acesso. As técnicas usadas para persistência incluem qualquer acesso, ação ou alterações de configuração que permitem aos atores de ameaça manter sua posição nos sistemas, como substituição ou sequestro de código legítimo ou adição de código de inicialização.

Os atores de ameça são bastante criativos em relação às técnicas utilizadas para manter a persistência, sendo alguns dos exemplos:

A modificação do *firmware* de componentes do *host*: essa técnica implica em métodos sofisticados de forma a instalar o código malicioso num componente do host. O código malicioso instalado no firmware será sempre executado antes do processo de *boot* do sistema operacional;

A exploração do protetor de tela (*screensaver*): os atores de ameaça podem estabelecer persistência executando um conteúdo malicioso acionado pela inatividade do usuário. Protetores de tela são programas executados após um tempo configurável de inatividade do usuário e consistem em arquivos do tipo *Portable Executable* (PE) com extensão [.scr]. As configurações do protetor de tela estão armazenadas no registro do sistema operacional e podem ser manipuladas para se obter persistência; e

O abuso dos processadores de impressão: no ambiente Windows, processadores de impressão são bibliotecas carregadas pelo serviço de *pool* de impressão (spoolsv.exe) durante o *boot* do sistema operacional. Os atores de ameaça podem instalar processadores de impressão (usando a API *AddPrintProcessor*, do próprio sistema operacional, por exemplo) para carregar código malicioso.

As técnicas mais comuns utilizadas para manter a persistência são:

- Agendamento de tarefas;
- Execução no carregamento (*boot*) ou *logon autostart*;
- Manipulação de contas; e
- Criação ou modificação de serviços no sistema operacional.

## 7.2.2.1. Agendamento de tarefas

O agendamento de tarefas é usado por atores de ameaça para executar seus programas na inicialização do sistema ou de forma programada.
No caso do Unix, os atores de ameça podem abusar do utilitário cron para agendar tarefas para a execução inicial ou recorrente de um código malicioso.

No caso do Windows, uma das principais formas de agendar tarefas para executar um *malware* é usar o schtasks.exe (conforme visto em 6.2.) a partir do interpretador de comandos e scripts. O *malware*, na maioria dos casos, fica localizado no diretório público.

Os atores de ameaça também podem criar tarefas agendadas "ocultas" (ou seja, ocultar artefatos) a fim de evitar sua identificação por ferramentas de defesa ou consultas manuais usadas para enumerar tarefas. Isso pode ser feito de diversas maneiras, dentre elas:

- Ocultar uma tarefa de *schtasks /query* e do Agendador de Tarefas excluindo o valor de registro do Descritor de Segurança (SD) associado (em que a exclusão desse valor deve ser concluída usando permissões do SYSTEM); e
- Alterar os metadados (por exemplo, valor do índice) nas chaves de registro associadas.

## 7.2.2.2. Execução no carregamento (*boot*) ou *logon autostart*

A instalação de *malware* como uma chave de execução no registro do computador (*Registry Run Key*) ou adicioná-lo ao diretório de inicialização (*StartUp folder*) é uma forma popular de garantir a execução do *malware* de forma automática e programada na inicialização do sistema.

No caso do Windows, por exemplo, os atores de ameaça geralmente adicionam seu *malware* como uma entrada nas seguintes chaves do registro:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

As chaves a seguir permitem controlar a inicialização automática de serviços durante o processo de *boot*:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

Além disso, eles também utilizam o seguinte diretório de inicialização:

- C:\Users\[user]\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup

Deve-se observar que existem diversas chaves de registro adicionais e outros locais do sistema onde os atores de ameaça podem instalar sua carga maliciosa.

## 7.2.2.3 Manipulação de contas

A maioria dos ataques é acompanhada por manipulações de contas. A manipulação de contas inclui a mudança de senhas de consta comprometidas, criação de contas e sua inclusão de contas em grupos privilegiados (especialmente no grupo de administradores), mudança nas políticas de senhas, dentre outras ações.

Em um caso de *ransomware* analisado, os atores de ameaça utilizaram um *script* para criar uma conta de usuário já ativa não expirável e a adicionaram a todos os grupos de administradores. Para isso, eles usaram comandos comuns, como:

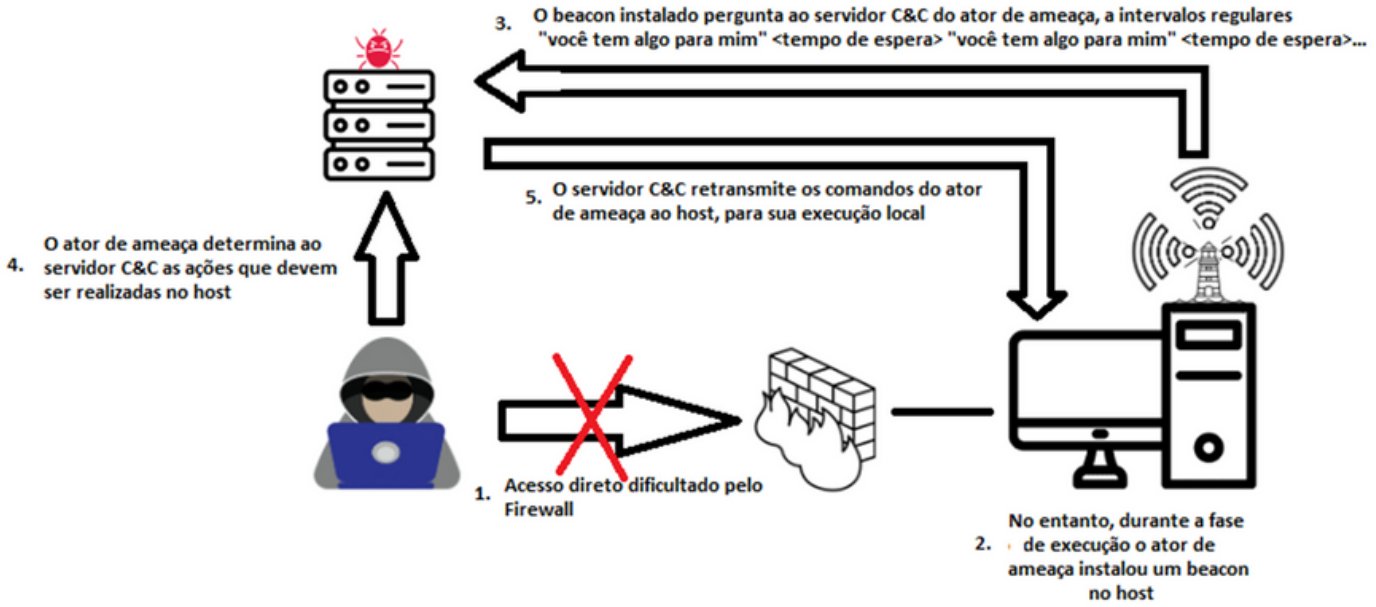
- Net user [nome_de_usuário [senha]] /add /active:yes /expires:never
- Net localgroup administrators [nome_de_usuário] /add
- Net group “Enterprise admins” [nome_de_usuário] /add
- Net group “Domain admins” [nome_de_usuário] /add

Com essa conta ativa, eles simplesmente removeram os demais usuários dos grupos de administradores. Isso permitiu ao ator de ameça executar suas atividades na infraestrutura além de bloquear as ações de resposta ao incidente.

## 7.2.2.4. Criação ou manipulação de serviços no sistema operacional

Serviços do sistema operacional são ativamente utilizados por atores de ameaça para executar sua carga maliciosa e manter a persistência, uma vez que os serviços são sempre executados em segundo plano. Além disso, os atores de ameaça utilizam diversas técnicas de mascaramento no nome ou descrição do serviço de forma a tornar o *malware* menos detectável.

Usualmente, criar um serviço é sempre acompanhado de uma escalada de privilégios pois os serviços são executados com privilégios de sistema e sua criação depende de direitos administrativos. Os beacons do CobaltStrike têm sido instalados nos servidores infectados como um serviço, o qual estabelece a conexão com os servidores Comando-e-controle (*Command-and-Control* – C2 ou C&C).




O uso de serviços apresenta muitas vantagens para os atores de ameaça, pois fornece capacidade de execução de *malware*, persistência, evasão de defesas e escalada de privilégios.

## 7.2.3. Evasão das Defesas

Os atores de ameaça utilizam diversas técnicas para evitar as medidas de segurança padrão ativas, aumentar o impacto de suas ações e ocultar suas atividades. Geralmente, as técnicas de evasão de defesas implicam na desabilitação dos produtos de segurança e na ocultação da execução do *malware* utilizado, seja pela renomeação do *malware*, pelo abuso de processos confiáveis ou pela ofuscação dos arquivos maliciosos. Além disso, os atores de ameaça tomam medidas para evitar que o *malware* não seja obtido de forma que possa ser estudado pela equipe de segurança da informação da vítima, geralmente pela autodestruição dos arquivos maliciosos utilizados no ataque.

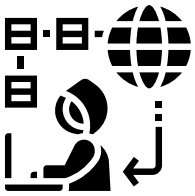
As técnicas mais comuns utilizadas para evasão de defesas são:

- *Signed binary proxy execution*;
- Injeção de processo;
- Enfraquecimento dos mecanismos de defesa:
- Mascaramento; e
- Remoção de indicador no *host*.

# 7.2.3.1. Signed Binary Proxy Execution

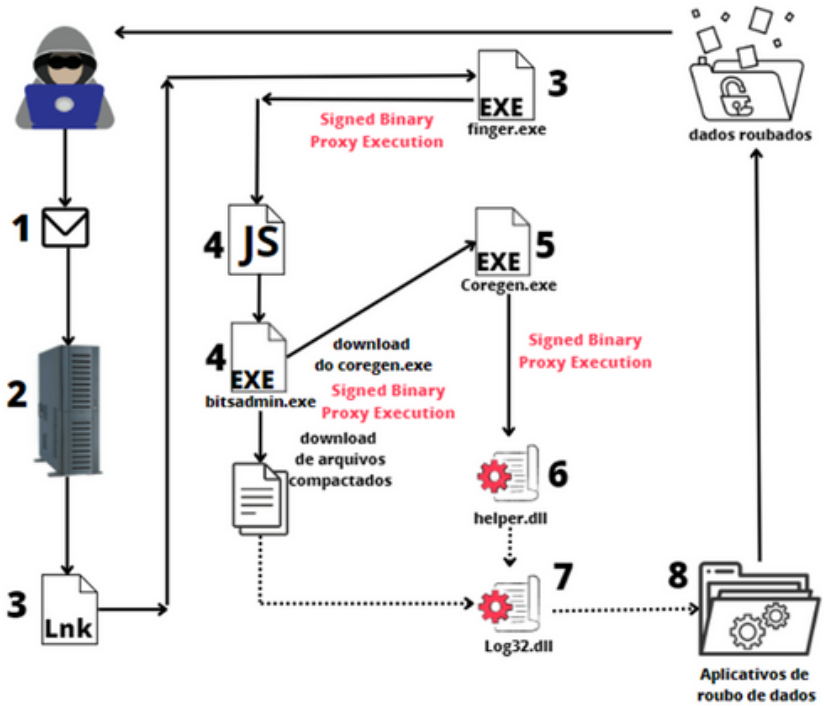
Os atores de ameaça podem desviar dos processos e das defesas baseadas em assinatura utilizando binários assinados para executar sua carga maliciosa. Binários assinados são arquivos que indicam que foram obtidos de fornecedores confiáveis ou já são nativos do próprio sistema operacional. Binários assinados com certificados digitais confiáveis normalmente podem ser executados em sistemas operacionais que possuem mecanismos de proteção baseados na validação de assinatura digital.

Esta técnica é fácil de automatizar. Ele permite que os invasores evitem o *download* de *malware* de uma só vez pois divide o processo de instalação da carga maliciosa em estágios, reduzindo a probabilidade de detecção.



Vários binários assinados pela Microsoft que são padrão nas instalações do Windows podem ser usados para executar *proxy* de outros arquivos ou comandos. Os atores de ameaça geralmente utilizam utilitários como rundll32.exe, regsvr32.exe, mshta.exe, msiexec.exe, e etc., para evitar restrições na execução de sua carga maliciosa e evadir da detecção por ferramentas de detecção, como um *antimalware*, durante o *download* ou execução das cargas maliciosas recebidas dos servidores atacantes remotos.

Da mesma forma, em sistemas Linux, os atores de ameaça podem abusar de binários confiáveis, como o Split, para executar essa técnica.



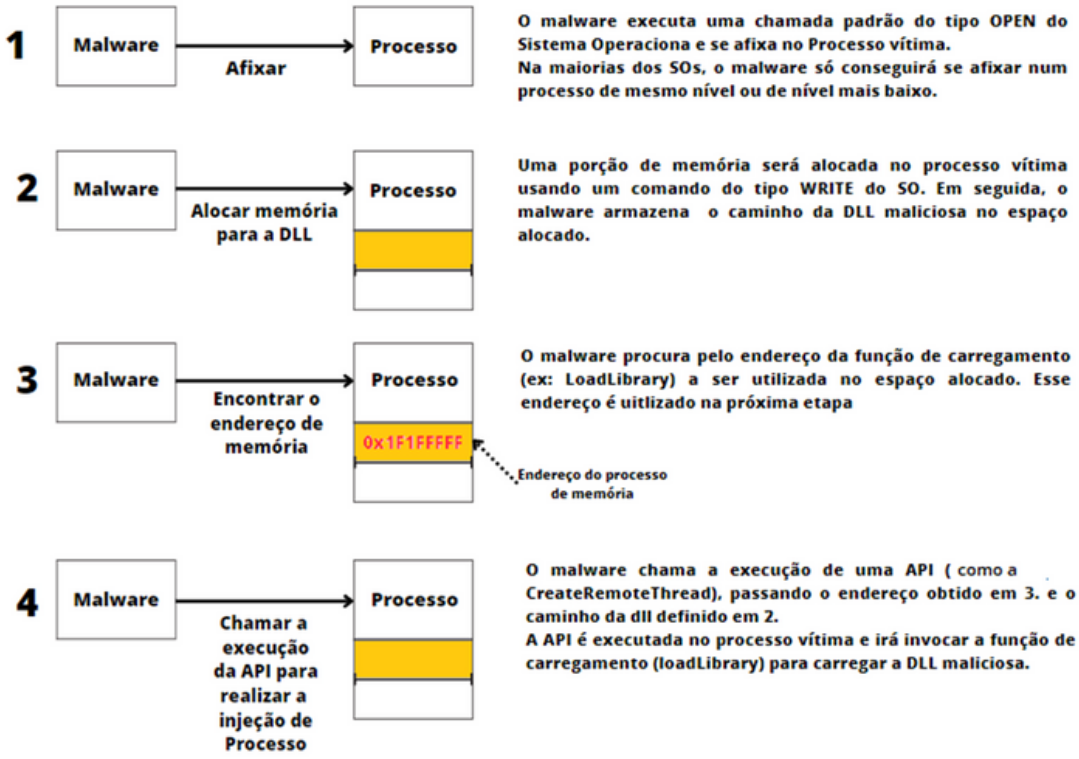

1 . O ator de ameaça envia um email com phishing
2 . A vítima abre o anexo ao phishing e obtem um arquivo .LNK
3. A vítima executa o arquivo .LNK , que executa um aplicativo como o finger.exe, binário legítimo do Windows, para recuperar o primeiro pacote de comandos maliciosos a partir de uma porta específica e os encaminhar para resolução pelo cmd.exe.
4. A execução dos comandos pelo cmd.exe cria um arquivo malicioso que contém um script (neste exemplo, um arquivo JS). A execução desse arquivo leva ao download de vários outros arquivos maliciosos. Para isso, o arquivo JS do exemplo utiliza um programa como bitsadmin.exe, que também é um binário legítimo do Windows.
5. Um dos arquivos carregados anteriormente deve ser um binário legítimo do SO. No exemplo, o arquivo será o coregen.exe, que é binário legítimo de um produto da MS, o Silverlight.
O coregen.exe então é usado para carregar um dos malwares do pacote, no nosso caso um malware chamado helper.dll
6. Uma vez carregado, o helper.dll descompacta e executa os demais arquivos enviados pelo, dentre eles o Log32.dll
7. O log32.dll executa então várias rotinas anti-debug,anti-vm (para identificar sandboxes), e uma série de verificações de sistema antes de carregar os aplicativos responsáveis pelo roubo de dados
8. Finalmente, os aplicativos de roubo de dados iniciam suas atividades e enviam os dados exfiltrados para o ator de ameaça.

# 7.2.3.2. Injeção de Processo

Atores de ameaça injetam código em processos para escapar das defesas baseadas em processos, bem como possivelmente elevar privilégios.

A injeção de processo é um método de execução de código malicioso arbitrário no espaço de endereço de um processo ativo separado. A execução de código no contexto de outro processo pode permitir acesso à memória do processo, recursos de sistema, da rede e até execução com privilégios elevados. A execução por injeção de processo também pode evitar a detecção de produtos de segurança, pois a execução é mascarada por um processo legítimo.

Existem muitas maneiras diferentes de injetar código em um processo, especialmente explorando funcionalidades legítimas. Essas implementações existem para todos os principais sistemas operacionais, mas geralmente são específicas da plataforma. Um bom artigo sobre técnicas de injeção de processo pode ser visto em https://www.elastic.co/pt/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process.




A injeção de processo permite ao ator de ameaça a oportunidade de ocultar o *malware* das ferramentas de segurança utilizando os eventos de sistema, pois é muito comum que as equipes de segurança, de forma a reduzir a carga nos sistemas de monitoramento, filtrem os eventos executados por processos de sistemas, considerando-os legítimos.

## 7.2.3.3. Enfraquecimento dos mecanismos de defesa

Nas técnicas de enfraquecimento dos mecanismos de defesa, o foco dos atores de ameaça se concentra, principalmente, em desabilitar ou modificar o *Firewall* do sistema e as ferramentas de segurança instaladas, em especial soluções *antimalware* e ferramentas de detecção que possam ser utilizadas para identificar e impedir um comportamento malicioso.

Os atores de ameaça também podem atuar para enfraquecer operações de rotina que contribuam com a segurança do ambiente, impedindo o *log out* de usuários, impedindo o *shutdown* de um determinado *host* ou desabilitando as operações de *backup*.

No caso dos *firewalls* de sistema, os atores de ameaça realizam alterações que podem desabilitar todo o mecanismo, bem como adicionar, excluir ou modificar regras específicas, a fim de contornar os controles que limitam o uso da rede. Isso pode ser feito de várias maneiras, dependendo do sistema operacional atingido.

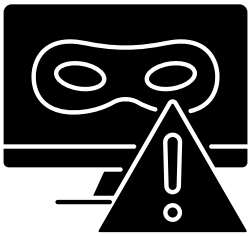
A modificação ou desativação de um *firewall* do sistema pode permitir comunicações do tipo Comando e Controle - C2 adversárias, movimentação lateral e exfiltração de dados que, de outra forma, não seriam permitidas.

Deve-se observar que os atores de ameaça agem de forma previsível: se precisarem de acesso ao RDP ou necessitarem que certas portas estejam abertas (139, 445), eles preferem adicionar uma regra ao *firewall* ao invés de tentar contornar as restrições utilizando outros métodos.

No caso das ferramentas de segurança instaladas, os atores de ameaça podem agir de diversas formas a fim garantir que as ferramentas não operem corretamente, impedindo a detecção de suas atividades, em especial:

- Matar processos ou serviços relacionados a ferramentas de segurança;
- Modificar ou excluir chaves do Registro ou arquivos de configuração das ferramentas de segurança;
- Desativar as atualizações para impedir que os *patches* de segurança mais recentes cheguem às ferramentas nos sistemas das vítimas;
- Adulterar os artefatos implantados e utilizados pelas ferramentas de segurança; e
- Explorar os *drivers* legítimos das ferramentas de segurança, especialmente *antimalware*, para ganhar acesso ao espaço do kernel.

## 7.2.3.4. Mascaramento



O mascaramento é um tipo de ação de ameaça por meio da qual uma entidade não autorizada obtém acesso a um sistema ou executa um ato malicioso ao se apresentar ilegitimamente como uma entidade autorizada.

Os atores de ameaça podem tentar manipular os recursos em seus artefatos para fazê-los parecer legítimos ou benignos para os usuários e mecanismos de segurança. O mascaramento ocorre quando o nome ou a localização de um objeto, legítimo ou malicioso, é manipulado ou abusado a fim de evitar defesas e observação.

Renomear utilitários de sistema que possam ser explorados para fugir do monitoramento de segurança também é uma forma de mascaramento.

O mascaramento de objetos para fins de evasão de defesas pode ser classificado em quatro categorias:

1. Mascaramento de extensão de arquivos, que envolve enganar um usuário ou um aplicativo para abrir um arquivo que parece um tipo de arquivo benigno por causa de sua extensão aparente. Portanto, a extensão percebida pelos usuários não reflete a extensão real do arquivo;

2

Mascaramento de nomes, onde o ator de ameaça altera:

- Nomes de arquivos, tarefas ou serviços maliciosos com nomes de arquivos, tarefas ou serviços legítimos e confiáveis, para torná-los benignos e evitar a detecção;
- Nomes de utilitários de sistema legítimos antes de usá-los de forma maliciosa (como na técnica de *signed binary proxy execution*), pois várias ferramentas de segurança monitoram esses utilitários do sistema operacional para detectar seu uso suspeito;

3

Mascaramento de localização de arquivos, no qual o ator de ameaça:

- Coloca arquivos maliciosos em diretórios confiáveis, como "C:\Windows\System32";
- Cria diretórios semelhantes aos diretórios usados por *softwares* conhecidos, como "C:\Intel\"; e
- Altera todo o caminho do *malware*, incluindo o diretório e o nome do arquivo, como "C:\NVIDIA\NvDaemon.exe";

4

Mascaramento de assinatura de arquivos, na qual o ator de ameaça copia a assinatura de código e as informações de metadados de programas válidos e assinados e os utiliza em seu *malware*.

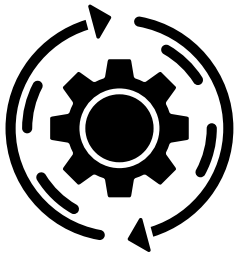
Uma das subtécnicas usadas para o mascaramento de extensão de arquivos é a *Right-To-Left-Override* (RTLO). Um ataque RTLO explora a confiança do usuário, alterando a extensão do arquivo malicioso para um arquivo executável ".exe". Um ataque RTLO é uma técnica sofisticada de *phishing* que engana os usuários utilizando o caracter UNICODE U+202E, que inverte a direção dos caracteres apresentados no texto após seu local de inserção, fazendo-os pensar que estão abrindo um arquivo inofensivo quando, na verdade, estão abrindo um executável malicioso.

Por exemplo, para esconder um arquivo.exe como se fosse um arquivo [.pdf], o ator de ameaça escolhe um nome para o arquivo malicioso cujo final seja <nome>fdp.exe. Ao aplicar o U+202E, o arquivo passará a se chamar <nome>exe.pdf.

| Texto modificado: o que o usuário vê | Texto real: o que o computador vê |
|---|---|
| ReceitaFederal_012023exe.doc | ReceitaFederal_012023[U+202E]cod.exe |

## 7.2.3.5. Remoção de indicador no *host*

Os atores de ameaça responsáveis por ataques de *ransomware*, como em qualquer ataque de *malware* sofisticado, agem de forma a dificultar as atividades das equipes de segurança. Eles compreendem que caso as amostras dos arquivos maliciosos utilizados não sejam eliminadas, elas podem ser recuperadas e analisadas utilizando engenharia reversa. Além disso, eles também sabem que eliminar os *logs* do sistema torna o processo de análise do ataque muito mais trabalhoso, senão impossível de realizar.

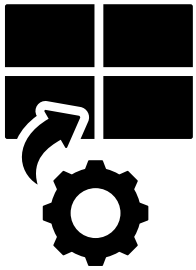


A remoção de indicador no *host* é uma atividade que pode ser realizada em todas as etapas do ataque do *ransomware*, sendo extremamente importante na etapa de exfiltração e na de impacto.

Os atores de ameaça, como forma de eliminar os arquivos maliciosos, podem apagar completamente um dispositivo ou excluir arquivos individuais para manipular resultados externos ou ocultar atividades. Para limpar completamente um dispositivo é necessário ter acesso de administrador. Já a eliminação de arquivos individuais pode não exigir permissões especiais, dependendo do local de armazenamento.

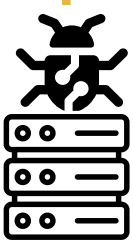
Os *logs* de eventos de um sistema operacional são um registro dos alertas e notificações de um computador. Geralmente, existem três fontes de eventos definidas pelo sistema: Sistema, Aplicativo e Segurança, com cinco tipos de eventos: Erro, Aviso, Informação, Auditoria de Sucesso e Auditoria de Falha.

No caso dos sistemas operacionais Windows, os atores de ameaça podem utilizar os seguintes comandos para apagar o *log* de eventos: Wevtutil cl system|application|security. Os logs também podem ser apagados usando a interface gráfica do visualizador de eventos (*event viewer*) e comandos do p*owershell*, como o Remove-EventLog – LogName system|application|security.



## 7.2.2.Comando e Controle – C2

Os atores de ameaça utilizam técnicas de comando-e-controle (C2) para se comunicar e controlar os sistemas vítimas de um ataque de *ransomware*. Isto permite aos atores de ameaça, dependendo da situação, alterar as técnicas de ataque ou executar ações complementares. A maioria dos métodos de comunicação utilizados tenta atuar como um tráfego normal e legítimo, como o HTTP ou ICMP, apesar de que métodos de ofuscação mais avançados, como uso de *proxy* ou tunelamento, também são possíveis. Geralmente, ferramentas de acesso remoto – ou *software* com funcionalidade similar - são utilizadas para esse objetivo.

As técnicas de C2, em especial, são constantemente utilizadas em várias etapas do ataque de *ransomware*.

Servidores C2 são amplamente utilizados pelos atores de ameaça para realizar o *download* de *malware* e *scripts* auxiliares, controlar ou comprometer os sistemas através dos canais C2 e até garantir que os servidores C2 estão ativos e aptos a executar o *ransomware*.

Vários atores de ameaça executam os códigos maliciosos vindos dos servidores C2 a partir de aplicativos legítimos do sistema operacional (utilizando técnicas vistas anteriormente como, por exemplo, uso do interpretador de comandos e *scripts*, injeção de processo e *signed binary proxy execution*).

Outra forma de utilização do C2 é para a exfiltração de dados.

## 7.2.5. Ações de Mitigação para a Etapa de Estabelecimento de Ponto de Apoio e C2

Em função das técnicas e subtécnicas apresentadas, as possíveis ações de mitigação incluem, dentre outras:

- Implementar um modelo *zero-trust*;
- Implementar um processo de gerenciamento de contas privilegiadas (PAM);
- Implementar controles de acesso de forma a, no mínimo:
  - Garantir, se possível, que apenas os administradores possam:
    - Acessar e utilizar o *shell* do sistema operacional;
    - Modificar configurações e desabilitar os serviços relacionados aos mecanismos de segurança;
    - Criar tarefas agendadas em sistemas remotos;
    - Interagir e modificar as configurações dos serviços do sistema; e
    - Visualizar e executar ações com os *logs* de eventos;
  - Limitar a execução de binários vulneráveis apenas a contas ou grupos privilegiados que efetivamente necessitem deles, de forma a reduzir as oportunidades de exploração;
  - Garantir que as permissões de acesso a arquivos e processos relacionados aos mecanismos de segurança tenham sido corretamente configuradas de forma a evitar a desabilitação ou modificação indevida desses mecanismos;
  - Proteger diretórios críticos, como o \System32; e
  - Proteger os arquivos de eventos gerados que sejam armazenados localmente com as devidas permissões de acesso e mecanismos de autenticação;
- Utilizar soluções de segurança *endpoint*, como o *Attack Surface Reduction* (ASR) da Microsoft, para:
  - Habilitar regras de forma a evitar que *scripts* possam realizar o *download* de conteúdo malicioso;
  - Identificar e bloquear:
    - A execução de arquivos potencialmente maliciosos;
    - Tentativas de injeção de processo utilizando regras baseadas em sequencias de eventos – ou em alterações de comportamento – que ocorrem durante um ataque de injeção de processo (o ASR, por exemplo, pode ser utilizado para evitar que as aplicações do MS-Office sejam usadas para injeção de processo); e
    - Métodos que utilizem binários assinados para evitar os mecanismos de segurança;

- Implementar sistemas de detecção e prevenção de intrusão em redes que utilizem assinaturas para identificar o tráfego associado a *malware*;
- Permitir somente a execução de scripts assinados (confiáveis) sempre que possível;
- Utilizar extensões que bloqueiem *scripts*, de forma a prevenir a execução de *scripts* e arquivos HTML *application* – HTA, os quais são comumente utilizados no processo de exploração;
- Desabilitar ou remover qualquer interpretador desnecessário ou inativo;
- Revisar todas as alterações realizadas nos serviços de agendamento de tarefas, como o cron e o schtasks;
- Configurar as tarefas agendadas de forma que só sejam executadas no contexto de uma conta autenticada ao invés de permitir sua execução diretamente pela conta system;
- Utilizar a autenticação multifator (MFA), quando possível, e emitir alertas sempre que um novo dispositivo, usuário, ou grupo seja registrado sem o uso de MFA;
- Segmentar a rede;
- Utilizar ferramentas de auditoria capazes de detectar e corrigir oportunidades de abuso de serviços e de privilégios nos sistemas;
- Aplicar regras de segurança de forma a impedir uma aplicação de gravar um driver assinado vulnerável no sistema;
- Impor o registro e execução de *drivers* de serviços assinados de forma legítima sempre que possível;
- Impor, quando possível, o modelo de autenticação por assinatura de forma a impedir que *drivers* não-assinados sejam instalados;
- Desabilitar os binários assinados que não sejam necessários ao funcionamento do sistema;
- Utilizar o controle de aplicações de forma a prevenir a execução de binários que sejam suscetíveis a abuso e que não sejam necessários em um sistema ou rede;
- Utilizar ferramentas *antimalware* para colocar os arquivos suspeitos em quarentena;
- Ofuscar ou encriptar os arquivos de eventos localmente e em trânsito a fim de não fornecer informações aos atores de ameaça; e
- Automaticamente encaminhar eventos para um servidor de *log* ou um repositório de dados a fim de prevenir condições nas quais os atores de ameaça possam localizar e manipular os dados de log num sistema local.

### 7.2.6. Atividades de Detecção para a Etapa de Estabelecimento de Ponto de Apoio e C2

A fim de aumentar as chances de detectar o uso das técnicas e subtécnicas apresentadas deve-se, no mínimo:

- Monitorar e identificar:
  - Os seguintes tipos de atividades realizadas por processos confiáveis como as aplicações de pacotes do tipo office (MS-Office, LibreOffice, OpenOffice etc.), aplicações de leitura de PDF (Acrobat reader, Tiny PDF, etc.) e outras aplicações que permitam a execução de macros ou scripts embutidos, dentre outras:

- execução do *Shell* do sistema operacional;
- carregamento e/ou instalação de arquivos executáveis ou *scripts*;
- carregamento e/ou instalação de bibliotecas suspeitas; e
- conexão de rede com Indicadores de Compromisso – IoCs (IP, URL, Domínio);

- Os seguintes sintomas que geralmente indicam atividade suspeita relacionada a serviços:
  - o arquivo executável do serviço se encontra num diretório aberto;
  - o executável do serviço não é assinado pelo sistema operacional; e
  - o serviço foi criado por um usuário com atividade anormal;
- O comportamento dos binários assinados em combinação com o comportamento inesperado de processos do sistema auxilia na identificação precoce do ataque. Deve-se considerar como atividade suspeita quando um binário assinado:
  - executar uma ação a partir de uma fonte externa;
  - executar uma ação a partir de um diretório público (acessível a qualquer usuário);
  - gerar um *shell*;
  - executar um arquivo com uma extensão desconhecida ou atípica; e
  - for executado com argumentos suspeitos;
- Eventos relacionados a bibliotecas de vínculo dinâmico (*dinamic-link library* – DLL), especialmente:
  - a criação de DLLs;
  - o carregamento inesperado de DLLs de forma a identificar:
    - DLLs desconhecidas;
    - DLLs que normalmente não sejam carregadas por um processo; e
    - comportamento anormal de um processo em função do carregamento de uma DLL maliciosa;
- A criação de:
  - novas chaves de registro quando da criação de uma nova tarefa;
  - programas adicionados a partir de diretórios abertos com extensões de arquivos executáveis suspeitas;
  - arquivos que possam ser utilizados para configurar atributos do sistema operacional de forma a executar programas de forma automática durante o processo de *boot* ou de *logon*;
  - novas contas e grupos no sistema; e
  - processos que possam manipular componentes no ambiente de forma a enfraquecer ou desabilitar mecanismos de defesa;
- A execução de:
  - processos que incluam comandos que possam criar ou modificar tarefas agendadas;
  - comandos, argumentos e Interfaces de Processamento de Aplicações (*Application Processing Interface* – API):
    - que tentem modificar atributos do sistema operacional de forma a executar programas de forma automática durante o processo de *boot* ou de *logon*;
    - que modifiquem contas e grupos, em especial suas configurações e permissões;
    - associados com a desabilitação ou modificação dos mecanismos de defesa; e
    - em atividades que possam levar à exclusão de *logs* de eventos;

- Modificações:
  - nas entradas relacionadas a tarefas agendadas nos armazéns do Windows Task Scheduler no %systemroot%\System32\Tasks que não estejam correlacionadas com o padrão de uso de software ou dos ciclos de alteração, em especial:
    - processos novos cujos processos pais sejam o svchost.exe ou o taskeng.exe; e
    - instâncias do schtasks.exe sendo executadas como processos, em especial com os argumentos /create, /run, /query. /delete, /change, e /end;
  - nos mecanismos do sistema operacional, como adições ao registro do sistema, que possam iniciar um processo de execução automática;
  - em arquivos ou em processos:
    - relacionados a configurações e permissões de contas e de grupos;
    - que possam injetar código em processos;
    - que possam ser utilizados para configurar atributos do sistema operacional de forma a executar programas de forma automática durante o processo de *boot* ou de *logon*;
  - na Registry do sistema que desabilitem ou alterem configurações dos mecanismos de defesa;
  - no estado de qualquer mecanismo de defesa, como interrupção do serviço ou parada do *driver*;
  - nas regras de exclusão dos mecanismos de segurança;
  - nas regras do *firewall* que:
    - permitam comunicação remota através de protocolos como o SMD e o RDP; e
    - abram portas locais e ativem serviços;
- Todos os programas adicionados ao *autorun*;
- A ocorrência de atividade incomum no kernel, especialmente a instalação de *drivers*, que possa resultar na configuração de atributos do sistema operacional de forma a executar programas de forma automática durante o processo de *boot* ou de *logon*;
- Dados contextuais sobre um arquivo, em especial informações como nome, conteúdo (ex: assinatura, cabeçalhos ou dados/mídia), usuário/propriedade, permissões etc.;
- Inconsistências no uso de memória pelos processos, em especial a ocupação de memória pelo processo analisado em comparação com os padrões esperados para o processo legítimo;
- O evento *CreatRemoteThread* no *log* do Sysmon;
- Parada não esperada de qualquer mecanismo de segurança;
- Atividade suspeita ou anormal de drivers associados aos mecanismos de defesa;
- Qualquer deleção de *logs* de eventos;
- O conteúdo do tráfego de rede e pacotes associados aos protocolos, identificando o fluxo de tráfego que não esteja aderente aos padrões de protocolo e fluxo de tráfego esperados (por exemplo, pacotes estranhos que não pertençam a fluxos estabelecidos, padrões de tráfego anômalos, sintaxes ou estruturas anômalas);
- O tráfego da *web* de-e-para domínios conhecidos como perigosos ou suspeitos, analisando os fluxos de tráfego que não seguem os padrões de protocolo e de fluxo de tráfego esperados (por exemplo, pacotes estranhos que não pertencem a fluxos estabelecidos ou padrões de tráfego anômalos);

- Coletar *hashes* de arquivos. Nomes de arquivos que não correspondam ao *hash* esperado devem ser tratados como suspeitos e postos em quarentena;
- Manter uma lista de arquivos e processos que geralmente são utilizados pelos atores de ameaça como se fossem processos legítimos do sistema operacional;
- Identificar:
  - Arquivos com nomes legítimos, mas em diretórios não-usuais;
  - O uso de caracteres comuns que possam indicar a tentativa de RTLO, como \u202E, [U+2020E] e %E2%80%AE; e
  - Arquivos que apresentem inconsistências entre o nome do arquivo em disco e o metadado do binário de seu *Portable Executable* (PE);
- Verificar que os cabeçalhos ou assinaturas dos arquivos e suas extensões correspondem usando detecção de *bytes* mágicos[3] (assinatura Hex) e/ou validação de assinaturas (Por exemplo, os *bytes* mágicos de um arquivo [.exe] são "4D 5A" enquanto um arquivo [.pdf] são "25 50 44 46 2D").

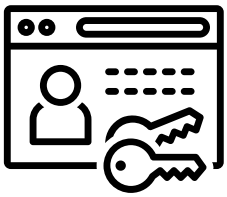
## 7.3. Mapeamento e Expansão

Uma vez que o ator de ameaça tenha estabelecido seu ponto de apoio e uma estrutura C2, ele irá tentar se movimentar através da rede. Para isso, ele precisa obter informação sobre os sistemas e infraestrutura da organização. A fim de se mover lateralmente pela rede, o ator de ameaça necessita de credenciais. Além disso, para ser capaz de executar suas ações, ele geralmente necessita elevar os privilégios da conta que estiver utilizando. O mapeamento da estrutura, a elevação de privilégios e a obtenção de credenciais têm como principal meta obter o controle da rede.

A etapa de mapeamento e expansão é composta pelas seguintes atividades:

- Elevação de privilégio;
- Acesso a credenciais;
- Descoberta; e
- Movimento lateral.

### 7.3.1. Elevação de privilégio



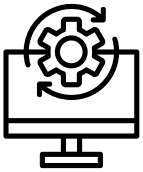
Elevação de privilégio é o processo de exploração de vulnerabilidades ou configurações incorretas em sistemas para elevar privilégios de um usuário para outro, geralmente para um usuário com acesso administrativo ou *root* em um sistema. Uma elevação de privilégio bem-sucedida permite que os atores de ameaça aumentem seu controle sobre um sistema ou grupo de sistemas que pertencem a um domínio.

[3] *Bytes* mágicos (*magic bytes*) é um termo que se refere a um bloco de valores de *byte* usado para identificar um tipo de arquivo de forma a que as aplicações de um sistema operacional possam determinar se o arquivo que pretendem consumir está no formato apropriado.

A elevação de privilégio é uma etapa lógica num ataque a um sistema e normalmente é realizada explorando vulnerabilidades e falhas de configuração nos mecanismos de autenticação e autorização, cujo objetivo é segregar contas de usuário com base em suas permissões e funções.

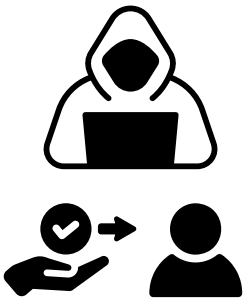

Dada a natureza dos ataques de elevação de privilégios em relação a contas e permissões de usuários, existem dois métodos principais que podem ser utilizados por invasores com base em suas intenções e objetivos, a saber:

- Elevação horizontal de privilégios; e
- Elevação vertical de privilégios.



A elevação vertical de privilégios é o processo de exploração de uma vulnerabilidade em um sistema operacional para obter acesso *root* ou administrativo em um sistema. Esse método geralmente é preferido por atores de ameaça, pois com a ampliação das permissões e funcionalidades, aumenta o acesso e controle sobre o sistema.

É importante observar que a elevação vertical de privilégios pode não ser fruto apenas da exploração de uma vulnerabilidade. É muito comum encontrar sistemas e serviços mal configurados que podem permitir que contas de usuários não administrativos executem comandos ou binários com permissões administrativas.



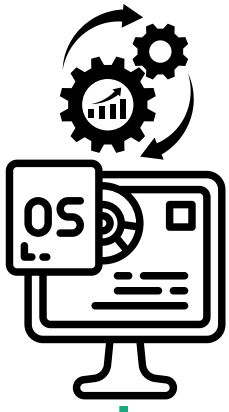
A elevação horizontal de privilégios é o processo de acessar a funcionalidade ou dados de outras contas de usuário em um sistema, em vez de obter acesso a contas com privilégios administrativos ou *root*. Envolve principalmente acessar ou autorizar uma funcionalidade em um sistema usando contas que estão no mesmo nível de permissões da conta sendo utilizada pelo ator de ameaça. Esse método é normalmente utilizado quando o ator de ameaça está mais interessado em acessar dados de contas de usuários não privilegiados, coletar credenciais de contas de usuários ou obter *hashes* de senha.

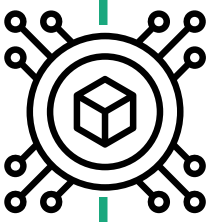
Os principais vetores de ataque que podem ser explorados em ataques de elevação de privilégio são:

- Credenciais inseguras;
- Configurações incorretas;
- Serviços e programas vulneráveis;
- Módulos do kernel e suas extensões;
- Tokens manipuláveis; e
- Não-aplicação de *patches* de segurança.

Em função desses vetores de ataque, existem diversas técnicas que podem ser utilizadas para realizar a elevação de privilégios. Podemos citar, como exemplos:

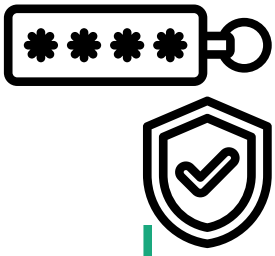
- Desviar do mecanismo de controle de elevação: A maioria dos sistemas modernos contém mecanismos nativos de controle de elevação destinados a limitar os privilégios que um usuário pode executar em uma máquina. A autorização deve ser concedida a usuários específicos para realizar tarefas que possam ser consideradas de maior risco. Um ator de ameaça pode executar vários métodos para aproveitar os mecanismos de controle integrados para escalar privilégios em um sistema.
  Por exemplo, no caso do sistema operacional Windows, caso o nível de proteção UAC (*Windows User Account Control*) não esteja configurado no nível mais alto, alguns programas podem elevar privilégios ou executar alguns objetos de nível mais elevado sem solicitar confirmação para o usuário através da caixa de notificação do UAC. Isso permitiria ao ator de ameaça injetar um *software* malicioso num processo legítimo para ganhar privilégios elevados sem que o usuário saiba.





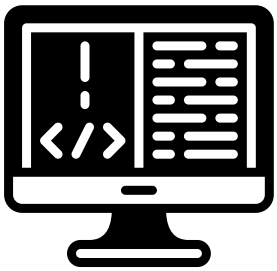
- Roubo de *token*: atores de ameaça podem duplicar e personificar o *token* existente de um usuário para aumentar os privilégios e ignorar os controles de acesso. O ator de ameaça geralmente executa o roubo de *token* quando tem acesso a um processo existente específico ao qual deseja atribuir o *token* duplicado (Por exemplo, isso pode ser útil quando o usuário de destino tiver uma sessão de *logon* fora da rede no sistema).

- Manipulação do *token* de acesso: Os atores de ameaça podem modificar os *tokens* de acesso para operar em um contexto de segurança de usuário ou de sistema diferente. O sistema operacional usa *tokens* de acesso para determinar a propriedade de um processo em execução. Um ator de ameaça pode manipular *tokens* de acesso para fazer um processo em execução parecer filho de um processo diferente ou pertencer a alguém que não seja o usuário que iniciou o processo. Quando isso ocorre, o processo também assume o contexto de segurança associado ao novo *token*.



- *Exploits* dos módulos de Kernel e suas extensões: os atores de ameaça podem modificar o kernel para que ele execute automaticamente programas durante o *boot* do sistema. *Loadable Kernel Modules* (LKMs) são pedaços de código que podem ser carregados e descarregados no kernel sob demanda. Eles ampliam as funcionalidades do kernel sem a necessidade de reinicialização do sistema (como, por exemplo, os *drivers* de dispositivos, que permitem ao kernel acessar o *hardware* conectado do sistema). Quando usados de forma maliciosa, os LKMs podem ser um tipo de *rootkit* de modo kernel executado com o privilégio mais alto do sistema operacional. Recursos comuns de *rootkits* baseados em LKM incluem: ocultar-se, ocultar seletivamente arquivos, processos e atividades de rede, bem como adulteração de *logs*, fornecer *backdoors* autenticados e permitir acesso *root* a usuários não privilegiados.

- Exploração de vulnerabilidades de *software*: os atores de ameaça podem utilizar erros de programação em um aplicativo, serviço ou no próprio sistema operacional para executar um código malicioso. Vulnerabilidades, em componentes do sistema operacional e *software* que sejam executados com permissões mais altas podem ser exploradas para obter níveis mais altos de acesso ao sistema. Esse tipo de técnica pode permitir que alguém mude de permissões não privilegiadas ou de nível de usuário para permissões SYSTEM ou *root*, dependendo do componente vulnerável. Isso também pode permitir que um ator de ameaça se mova de um ambiente virtualizado, como de dentro de uma máquina virtual ou contêiner, para o *host* subjacente. Essa pode ser uma etapa necessária para se comprometer um sistema de *endpoint* que foi configurado corretamente e esteja limitando outros métodos de escalonamento de privilégios.



Dentre as possíveis ações de mitigação pode-se destacar:

- Manter o sistema operacional atualizado;
- Implementar um processo de gerenciamento de contas privilegiadas (PAM);
- Limitar:
  - As permissões e os direitos de acessos dos usuários comuns;
  - Permissões de forma que grupos e usuários comuns não possam criar *tokens*;
  - O acesso a conta *root*; e
  - A capacidade dos usuários de carregar módulos e extensões no kernel através das devidas separações de privilégios;
- Controlar o uso das permissões e acessos dos administradores;
- Utilizar aplicações que restrinjam a carga de módulos no kernel; e
- Utilizar *antimalware* com capacidades de detecção de *rootkits*.

Em função da grande variedade de técnicas que podem ser utilizadas, a detecção desse tipo de ameaça é bastante complexa. Dentre as possíveis atividades de detecção deve-se monitorar e identificar:

O uso de comandos e argumentos em tentativas de desvio dos mecanismos de controle para ganhar privilégios elevados, especialmente quando executados por usuários não-autenticados ou não-autorizados ou fora do horário padrão;


A execução de chamadas APIs que possam ser indicativas de injeção de processo, especialmente quando executados por usuários não-autenticados ou não-autorizados ou fora do horário padrão;

Qualquer manipulação de *tokens* por comandos e argumentos do sistema operacional ou por qualquer outro aplicativo;

Arquivos recém-construídos ou modificações em arquivos existentes que possam levar o kernel a executar programas automaticamente no *boot* do sistema;

A criação e execução de processos ou serviços atípicos;
A presença ou carga de *drivers* vulneráveis conhecidos; e
Comportamento anormal ou não-esperado de aplicativos e serviços.

## 7.3.2. Acesso a credenciais

O acesso a credenciais consiste em técnicas para roubar credenciais, como nomes de contas e senhas. O uso de credenciais legítimas dá aos atores de ameaça acesso aos ativos aos quais essas credenciais tenham permissão de acesso, além de tornar a detecção de suas atividades mais difícil. Por fim, dependendo das credenciais obtidas, é possível ao ator de ameaça criar mais contas e processos para ajudá-lo a atingir seus objetivos.

As técnicas mais comuns para esse fim são:

- Despejo de Credenciais do sistema operacional;
- Obtenção de credenciais em armazéns de senhas; e
- Força bruta.

## 7.3.2.1. Despejo de Credenciais do sistema operacional

Os atores de ameaça podem tentar despejar credenciais para obter *login* de conta e material de credencial, normalmente na forma de um *hash* ou uma senha de texto não criptografado, do sistema operacional e do *software*. As credenciais podem então ser usadas para realizar o Movimento Lateral e acessar informações restritas.

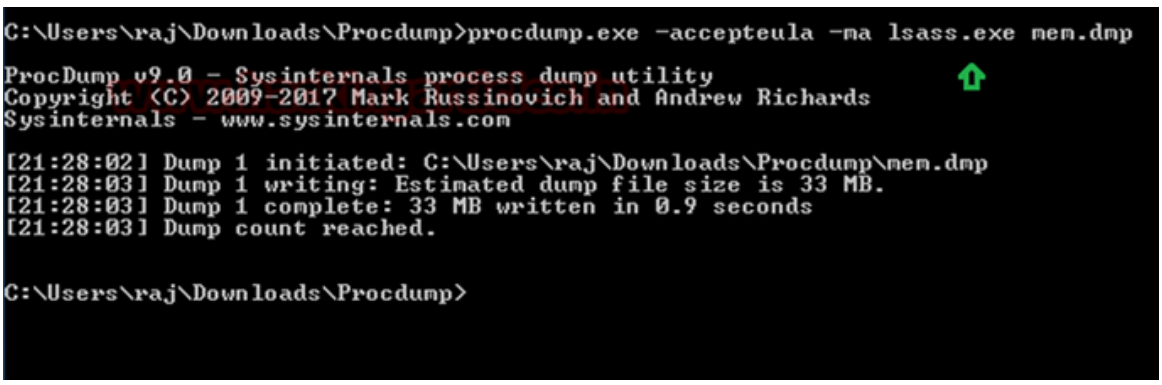
Existem diversas técnicas para realizar o despejo de credenciais do sistema operacional, como:

- Acessar os dados de credenciais armazenados na memória de processo do *Local Security Authority Subsystem Service* (LSASS);
- Acessar as credenciais de domínio em *cache*;
- Extrair os dados de credenciais da base de dados do *Security Account Manager* (SAM); e
- Acessar os segredos do *Local Security Authority* (LSA).


A técnica de despejo de credenciais do sistema operacional mais utilizada pelos atores de ameaça é acessar os dados de credenciais armazenados na memória de processo do LSASS. O LSASS é um serviço usado para gerenciar a segurança local, *login* e permissões. Ele também é o responsável por garantir a política de segurança nos sistemas operacionais Windows.

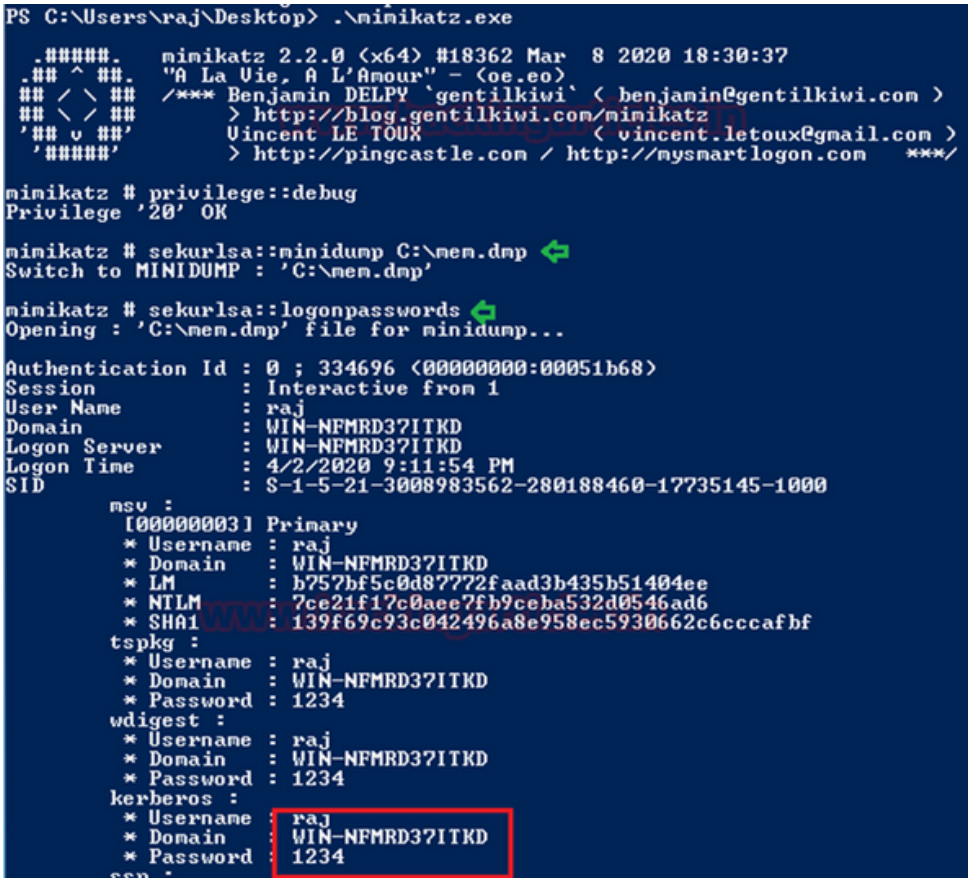
Depois que um usuário faz *logon*, o sistema gera e armazena uma variedade de dados de credenciais na memória do processo LSASS. Esses dados de credencial podem ser coletados por um usuário administrativo ou SYSTEM e usados para conduzir a movimentação lateral. Como na maioria das técnicas de acesso à memória, a memória de processo do LSASS pode ser despejada do *host* alvo e ser analisada no sistema local.

Para realizar o despejo de memória, os atores de ameaça podem se valer de utilitários ou ferramentas do próprio sistema operacional Windows, como ProcDump.exe (procdump -ma lsass.exe lsass_dump) ou o comsvcs.dll (rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full).



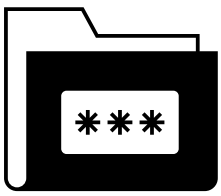

Fonte: https://www.hackingarticles.in/credential-dumping-local-security-authority-lsalsass-exe/

O mimikatz tem sido a ferramenta preferida dos atores de ameaça (sekurlsa::Minidump lsassdump.dmp e sekurlsa::logonPasswords) para analisar o arquivo com o despejo de memória localmente.




Fonte: https://www.hackingarticles.in/credential-dumping-local-security-authority-lsalsass-exe/

## 7.3.2.2. Obtenção de credenciais em armazéns de senhas



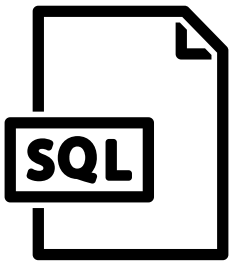

Os atores de ameaça podem procurar locais comuns de armazenamento de senhas para obter credenciais de usuário. As senhas são armazenadas em vários locais em um sistema, dependendo do sistema operacional ou aplicativo que contém as credenciais. Existem também aplicativos específicos que armazenam senhas para facilitar o gerenciamento e a manutenção dos usuários. Uma vez obtidas as credenciais, elas podem ser usadas para realizar movimentos laterais e acessar informações restritas.

Assim como ocorre no despejo de credencias, existem várias técnicas para obter credenciais a partir de armazéns de senhas, sendo as principais:

- Exploração de navegador *web*; e
- Violação da base de dados e gerenciadores de senhas.

Os atores de ameaça podem adquirir credenciais de navegadores da *Web* lendo arquivos específicos do navegador de destino. Os navegadores da *Web* geralmente salvam credenciais, como nomes de usuário e senhas de *sites*, para que não precisem ser inseridos manualmente no futuro e armazenam essas credenciais em um formato criptografado em um armazenamento de credenciais. No entanto, existem métodos para extrair credenciais em texto não-criptografado de navegadores da *web*.

Por exemplo, em sistemas Windows, as credenciais criptografadas podem ser obtidas do Google Chrome lendo um arquivo de banco de dados, AppData\Local\Google\Chrome\User Data\Default\Login Data e executando uma consulta SQL: SELECT action_url, username_value, password_value FROM logins ;. A senha em texto simples pode ser obtida passando as credenciais criptografadas para a função da API do Windows CryptUnprotectData, que usa as credenciais de *logon* em *cache* da vítima como a chave de descriptografia. Procedimentos semelhantes podem ser utilizados em navegadores como o Firefox, o Safari e o Edge, dentre outros.




Os atores de ameaça também podem adquirir credenciais de usuário a partir de aplicativos gerenciadores de senhas. Os gerenciadores de senhas são aplicativos projetados para armazenar as credenciais do usuário, normalmente em um banco de dados criptografado. As credenciais são normalmente acessíveis depois que um usuário fornece uma senha mestra que desbloqueia o banco de dados. Após o desbloqueio do banco de dados, essas credenciais podem ser copiadas para a memória.

Os atores de ameaça podem adquirir as credenciais de usuário contidas nos gerenciadores de senhas extraindo a senha mestra e/ou credenciais de texto não-criptografado da memória. Os adversários podem extrair credenciais da memória por meio da exploração de vulnerabilidades na programação da aplicação ou até por força bruta.


## 7.3.2.3. Força Bruta

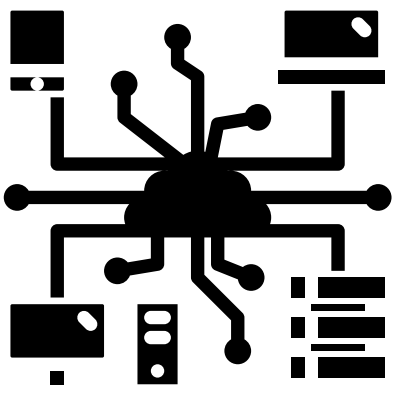

Os atores de ameaça podem usar técnicas de força bruta para obter acesso a contas quando as senhas são desconhecidas ou quando os *hashes* de senha são obtidos. Sem o conhecimento da senha de uma conta ou conjunto de contas, um ator de ameaça pode utilizar um programa repetitivo e interativo executado de forma sistemática para tentar adivinhar uma senha. A obtenção de uma senha por de força bruta pode ocorrer por meio da interação com um serviço que verificará a validade dessas credenciais ou *offline* em relação aos dados de credenciais adquiridos anteriormente, como *hashes* de senha.

## 7.3.3. Descoberta

A descoberta continua sendo uma fase inerente de um ataque. Atores de ameaça necessitam reunir o maior número de informações sobre a infraestrutura da rede alvo a fim de maximizar a superfície de ataque, navegando mais facilmente pela rede, identificando os ativos que podem ser aproveitados e, se necessário, determinando as ações subsequentes no ataque.

As principais técnicas utilizadas na etapa de descoberta são:

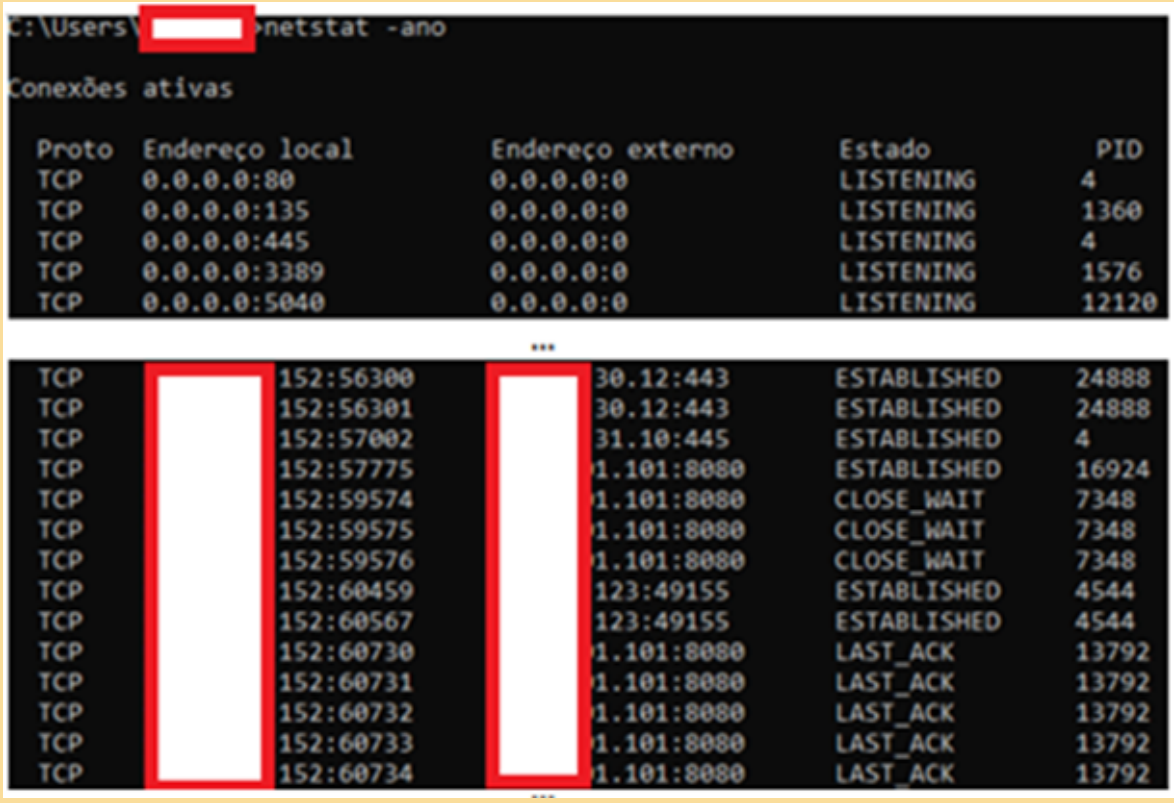
- Descoberta de conexões de rede;
- Descoberta de sistemas remotos;
- Descoberta de compartilhamentos de rede;
- Descoberta de contas;
- Descobertas de arquivos e diretórios; e
- Descoberta de processos.



# 7.3.3.1. Descoberta de conexões de redes

Atores de ameaça sempre agem de forma a obter uma lista de conexões de rede existentes no sistema comprometido, pois verificar as conexões de rede é a maneira mais fácil de encontrar ativos que possam ser explorados em sequência. Geralmente, são utilizados comandos do próprio sistema operacional para realizar essa tarefa, como:

- Net session /list: usado para listar sessões entre o *host* e outros computadores na rede;
- net use: é utilizado para apresentar informação sobre as conexões de um computador, conectar ou desconectar um computador com um recurso compartilhado e controlar conexões persistentes. Quando usado sem parâmetros, ele apresenta uma lista de conexões existentes;
- netstat –ano: o comando netstat exibe as conexões TCP ativas. O parâmetro –a inclui as portas TCP e UDP nas quais o computador está em escuta. O parâmetro –n exibe os endereços e números de portas numericamente, sem tentar determinar nomes. O parâmetro –o inclui a ID de cada processo (PID) para cada conexão; e




- query session: exibe as informações sobre as sessões num *host*. A lista pode incluir tanto informações sobre as sessões ativas como outras sessões que o *host* executa, dependendo do privilégio da conta usada para a consulta. Quando usado no formato “query session /server: <identificação_do_servidor>” traz as informações sobre todas as sessões ativas no servidor especificado.

As ações executadas são praticamente as mesmas em todos os sistemas operacionais.

# 7.3.3.2. Descoberta de sistemas remotos


Atores de ameaça podem atuar para obter uma lista de outros sistemas na rede usando endereços IP, nomes de *host* ou outro identificador lógico, de forma a realizar uma movimentação lateral a partir do sistema comprometido.

Para atingir esse fim, eles podem utilizar ferramentas como o Adfind, o backdoor.Oldrea, Bazar e Black Basta. No entanto, os utilitários disponíveis no sistema operacional também podem ser utilizados, como:

- *Ping*, que verifica a conectividade no nível de IP com outro computador TCP/IP;
- *Tracert*, que determina o caminho utilizado para atingir um destino através do envio de uma requisição ECHO;

```
C:\Users\Mike>tracert www.octanetworks.com

Tracing route to www.octanetworks.com [104.27.186.226]
over a maximum of 30 hops:

  1     *        2 ms     1 ms  192.168.1.1
  2    18 ms    11 ms    10 ms  10.248.0.1
  3    11 ms    10 ms    11 ms  125.99.55.177
  4    15 ms    11 ms    12 ms  203.212.193.30
  5    15 ms    11 ms    12 ms  202.88.130.245
  6    13 ms    11 ms    11 ms  136.232.27.245
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    92 ms   116 ms    88 ms  103.198.140.89
 12   110 ms    95 ms    91 ms  162.158.160.222
 13    94 ms    90 ms    91 ms  104.27.186.226

Trace complete.
```

Fonte: https://blog.octanetworks.com/tracert-what-is-tracert-tracert-options/

- Net view, que exibe uma lista de domínios, computadores e recursos sendo compartilhados em um *host* específico.

```
C:\Users\[redacted]>net view
Server Name                     Remark

---------------------------------------------------------
\\AIDA
\\AMYMAHRAN
\\H3R4                          H3R4
\\HANIEY-CCC5A912
\\MFP-05022234                  SMB Server
\\POLI-6C09207E7E
\\POLY-0F34242C4C
\\SITIAISHAH-PC
\\USER-PC
The command completed successfully.
```

- Arp -av: utilizado para mostrar o cache do *Address Resolution Protocol* (ARP) de um *host*, o que pode incluir resolução de endereços para sistemas remotos. O parâmetro –a exibe as entradas ARP atuais. O parâmetro –v exibe as entradas no modo detalhado.

```
C:\Users\user>arp -a

Interface: 10.10.100.131 --- 0xb
  Internet Address      Physical Address      Type
  10.10.100.1           00-50-56-c0-00-01     dynamic
  10.10.100.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Atores de ameaça podem atuar para obter uma lista de outros sistemas na rede usando endereços IP, nomes de *host* ou outro identificador lógico, de forma a realizar uma movimentação lateral a partir do sistema comprometido.

## 7.3.3.3. Descoberta de compartilhamentos de rede

As redes possuem unidades e pastas compartilhadas que permitem aos usuários acessar diretórios de arquivos em vários sistemas numa rede. Atores de ameaça procuram por essas pastas e unidades compartilhadas como um meio de identificar fontes de informações a serem coletadas na etapa de exfiltração e para identificar potenciais sistemas de interesse para a movimentação lateral.

O compartilhamento de arquivos em uma rede Windows ocorre por meio do protocolo *Server Message Block* (SMB). Computadores Unix e Linux utilizam o N*etwork File System* (NFS) para compartilhar arquivos numa rede. Uma solução para que que computadores Linux/Unix possam compartilhar arquivos com computadores Windows é usar o Samba, um *software* livre que implementa o protocolo de redes SMB/CIFS.

Atores de ameaça podem usar diversas ferramentas como o Bazar, o CrackMapExec, o Empire e o InvisiMole, para realizar essa tarefa ou apenas usar os utilitários e comandos disponíveis no próprio sistema operacional, como, por exemplo:

- *Net share*: apresenta informação sobre todos os recursos que estão compartilhados no computador local.

```
C:\Users\Brink>net share

Share name   Resource                        Remark

-------------------------------------------------------------------
C$           C:\                             Default share
D$           D:\                             Default share
E$           E:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\WINDOWS                      Remote Admin
New folder   D:\New folder
Pictures     C:\Users\Brink\Pictures
Users        C:\Users
The command completed successfully.
```

Fonte: https://www.tenforums.com/tutorials/112017-view-all-network-shares-windows-pc.html

- Net view \\Nome_do_computador /All : apresenta uma lista com todos os compartilhamentos de rede e de impressoras em um computador remoto, incluindo os compartilhamentos ocultos.

```
C:\Users\Brink>net view \\Brink-W10PC /All
Shared resources at \\Brink-W10PC


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C$          Disk           Default share
D$          Disk           Default share
E$          Disk           Default share
IPC$        IPC            Remote IPC
New folder  Disk
Pictures    Disk
Users       Disk
The command completed successfully.
```

Fonte: https://www.tenforums.com/tutorials/112017-view-all-network-shares-windows-pc.html

- *Powershell* do Windows, usando o comando Get-WmiObject –Class Win32_share

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Brink> Get-WmiObject -Class Win32_Share

Name        Path                    Description
----        ----                    -----------
ADMIN$      C:\WINDOWS              Remote Admin
C$          C:\                     Default share
D$          D:\                     Default share
E$          E:\                     Default share
IPC$                                Remote IPC
New folder  D:\New folder
Pictures    C:\Users\Brink\Pictures
Users       C:\Users
```

Fonte: https://www.tenforums.com/tutorials/112017-view-all-network-shares-windows-pc.html

## 7.3.3.4. Descoberta de Contas

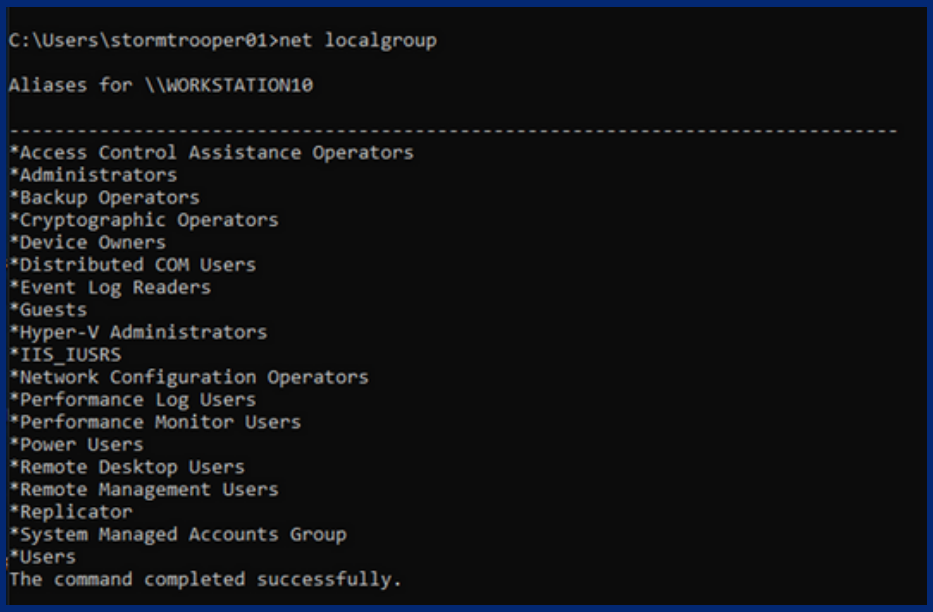
Atores de ameaça sempre tentarão obter uma lista de contas e nomes de usuário válidos no sistema ou no ambiente comprometido, pois essas informações podem ajudá-los a determinar o comportamento subsequente, como utilizar ataques de força bruta, ataques de *spear phishing* ou realizar o controle de contas.

Podem ser utilizados vários métodos para enumerar as contas existentes, incluindo uso de ferramentas de terceiros, abuso de comandos e aplicativos do próprio sistema operacional e exploração de configurações incorretas ou insuficientes.

Dentre os comandos que podem ser utilizados para esse fim, temos:

⇨ Para contas locais:

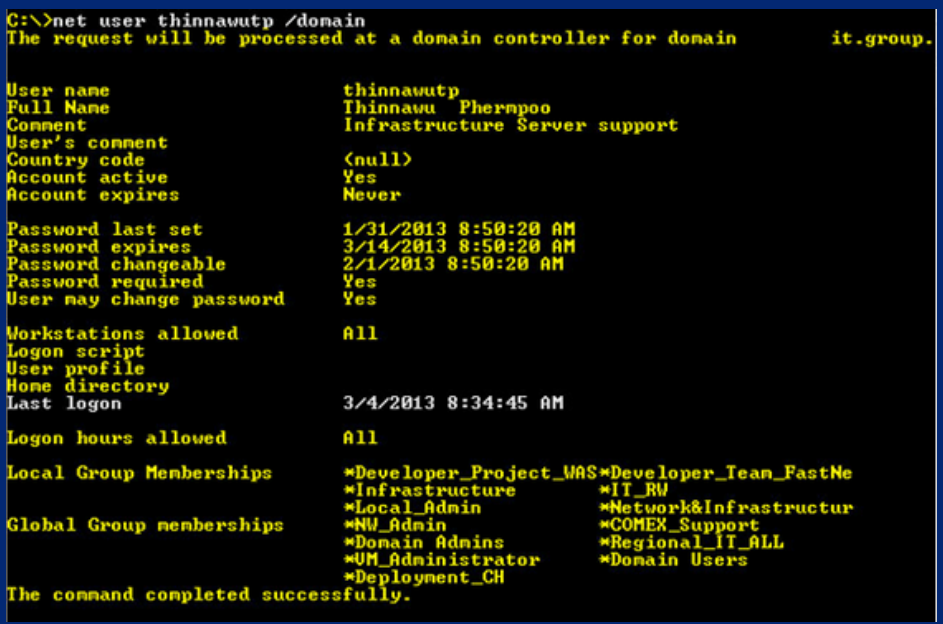
- No Windows: *net user* e *net localgroup*;
- No Linux e macOS: id e *groups*;
- No Linux, os usuários locais também podem ser enumerados através do uso de /etc/passwd; e
- No macOS, as contas locais podem ser enumeradas usando o comando dscl . list /users




Fonte: https://securitytutorials.co.uk/basic-enumeration-on-a-windows-pc/

⇨ Para contas de domínio:

- No Windows: net user /domain, net group /domain e Powershell cmdlets como o Get-ADUser ou Get-ADGroupMember;
- No macOS: dscacheutil –q group; e
- No Linux: ldapsearch.




Fonte: https://serveradmintools.blogspot.com/2013/03/details-and-examples-net-user-domain.html

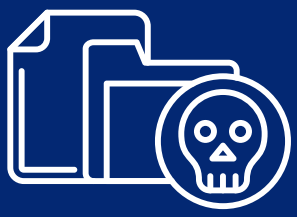
## 7.3.3.5. Descoberta de arquivos e diretórios

Atores de ameaça sempre procuram enumerar arquivos e diretórios para moldar comportamentos subsequentes, incluindo a decisão de quais objetos podem ser infectados para auxiliar na propagação das atividades, além de definir quais arquivos devem ser exfiltrados e/ou criptografados.

Ferramentas personalizadas podem ser usadas para coletar informações de arquivos e diretórios e interagir com a API nativa. No entanto, é possível utilizar apenas utilitários de *shell* de comando para obter essas informações, dentre eles o dir, tree, ls, find e locate.

## 7.3.3.6. Descoberta de processos

A descoberta de processos consiste no uso de métodos que enumerem processos ativos nos sistemas afetados de forma a permitir que os atores de ameaça possam decidir sobre as ações específicas a serem tomadas na realização do ataque. As informações obtidas podem ser usadas para entender os *softwares*/aplicativos comuns em execução nos sistemas da rede de forma a moldar comportamentos subsequentes, incluindo a decisão de infectar os sistemas afetados e encerrar os processos que possam interferir nas etapas de exfiltração e impacto.



No Linux, é possível enumerar todos os processos em um sistema usando o comando ps (com a sintaxe padrão ps –e ou a sintaxe BSD ps ax, conforme o caso). Os atores de ameaça também podem optar por enumerar processos via /proc.

```
net2_admin@net2:~$ ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:01 /sbin/init splash
    2 ?        S      0:00 [kthreadd]
    3 ?        I<     0:00 [rcu_gp]
    4 ?        I<     0:00 [rcu_par_gp]
    6 ?        I<     0:00 [kworker/0:0H-kb]
    7 ?        I      0:00 [kworker/u2:0-ev]
    8 ?        I<     0:00 [mm_percpu_wq]
    9 ?        S      0:00 [ksoftirqd/0]
   10 ?        I      0:00 [rcu_sched]
   11 ?        S      0:00 [migration/0]
   12 ?        S      0:00 [idle_inject/0]
   13 ?        I      0:00 [kworker/0:1-eve]
   14 ?        S      0:00 [cpuhp/0]
   15 ?        S      0:00 [kdevtmpfs]
   16 ?        I<     0:00 [netns]
```

Fonte: https://serveradmintools.blogspot.com/2013/03/details-and-examples-net-user-domain.html

Em ambientes Windows, os invasores podem obter detalhes sobre os processos em execução usando o utilitário Tasklist via cmd ou Get-Process via *PowerShell*. Informações sobre processos também podem ser extraídas da saída de chamadas de API nativas, como CreateToolhelp32Snapshot.

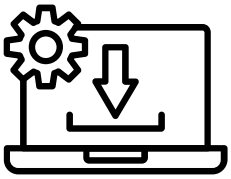
```
C:\>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         20 K
System                           4 Services                   0      1,212 K
smss.exe                       316 Services                   0      1,016 K
csrss.exe                      456 Services                   0      4,236 K
wininit.exe                    524 Services                   0      3,596 K
csrss.exe                      532 Console                    1     35,068 K
winlogon.exe                   576 Console                    1      8,368 K
services.exe                   620 Services                   0      9,344 K
lsass.exe                      628 Services                   0     14,496 K
svchost.exe                    724 Services                   0      9,064 K
svchost.exe                    764 Services                   0     12,216 K
svchost.exe                    840 Services                   0     21,384 K
dwm.exe                        880 Console                    1     40,796 K
svchost.exe                    908 Services                   0     43,676 K
svchost.exe                    372 Services                   0     81,824 K
svchost.exe                    468 Services                   0     14,376 K
svchost.exe                    964 Services                   0     18,596 K
spoolsv.exe                   1108 Services                   0     14,656 K
svchost.exe                   1136 Services                   0     22,544 K
svchost.exe                   1336 Services                   0      8,000 K
dtupdate.exe                  1456 Services                   0      7,884 K
svchost.exe                   1484 Services                   0      8,884 K
inetinfo.exe                  1528 Services                   0     16,736 K
MsDtsSrvr.exe                 1688 Services                   0     18,396 K
sqlservr.exe                  1788 Services                   0    188,192 K
msmdsrv.exe                   1876 Services                   0     53,788 K
ReportingServicesService.     1648 Services                   0     79,764 K
rundll32.exe                  1804 Console                    1     44,200 K
taskhostex.exe                1944 Console                    1     11,092 K
explorer.exe                  1156 Console                    1    104,072 K
ccSvcHst.exe                  2100 Services                   0     16,384 K
sppsvc.exe                    2256 Services                   0      3,464 K
sqlwriter.exe                 2280 Services                   0      6,144 K
svchost.exe                   2324 Services                   0      9,700 K
ccSvcHst.exe                  2848 Console                    1      4,712 K
TfsComProviderSvr.exe         1332 Console                    1     24,344 K
WmiPrvSE.exe                  3132 Services                   0     10,488 K
Smc.exe                       4532 Services                   0     10,960 K
fdlauncher.exe                8036 Services                   0      3,808 K
fdhost.exe                    3960 Services                   0      4,992 K
SearchIndexer.exe             3996 Services                   0     26,824 K
conhost.exe                   4040 Services                   0      3,076 K
svchost.exe                   4120 Services                   0      6,524 K
svchost.exe                   3752 Services                   0      5,252 K
WUDFHost.exe                  7580 Services                   0      6,244 K
unsecapp.exe                  3896 Services                   0      4,948 K
Skype.exe                     3224 Console                    1    139,972 K
```

Fonte: https://mahedee.net/which-service-is-using-which-port/

## 7.3.4. Movimento Lateral

O movimento lateral consiste em técnicas que os atores de ameaça usam para entrar e controlar sistemas remotos em uma rede. Essas técnicas abusam do conhecimento obtido sobre a estrutura da rede (conexões de rede, sistemas remotos, compartilhamentos, arquivos e diretórios acessíveis), credenciais padrão e privilegiadas existentes, contas ativas, processos em execução e serviços vulneráveis. Os atores de ameaça usam essas técnicas para deslocarem-se pelo ambiente, ampliando a superfície de ataque e determinando suas próximas ações de ataque.



Os atores de ameaça podem instalar suas próprias ferramentas remotas para realizar o movimento lateral ou aproveitar credenciais, ferramentas, programas e serviços legítimos instalados no ambiente, tornando suas ações ainda mais furtivas.

As técnicas mais populares utilizadas pelos atores de ameaça, e que serão vistas mais detalhadamente, são:

- Acesso a serviços remotos;
- Transferência lateral de ferramentas; e
- Sequestro de sessão.

Como exemplos de outras técnicas utilizadas, temos:

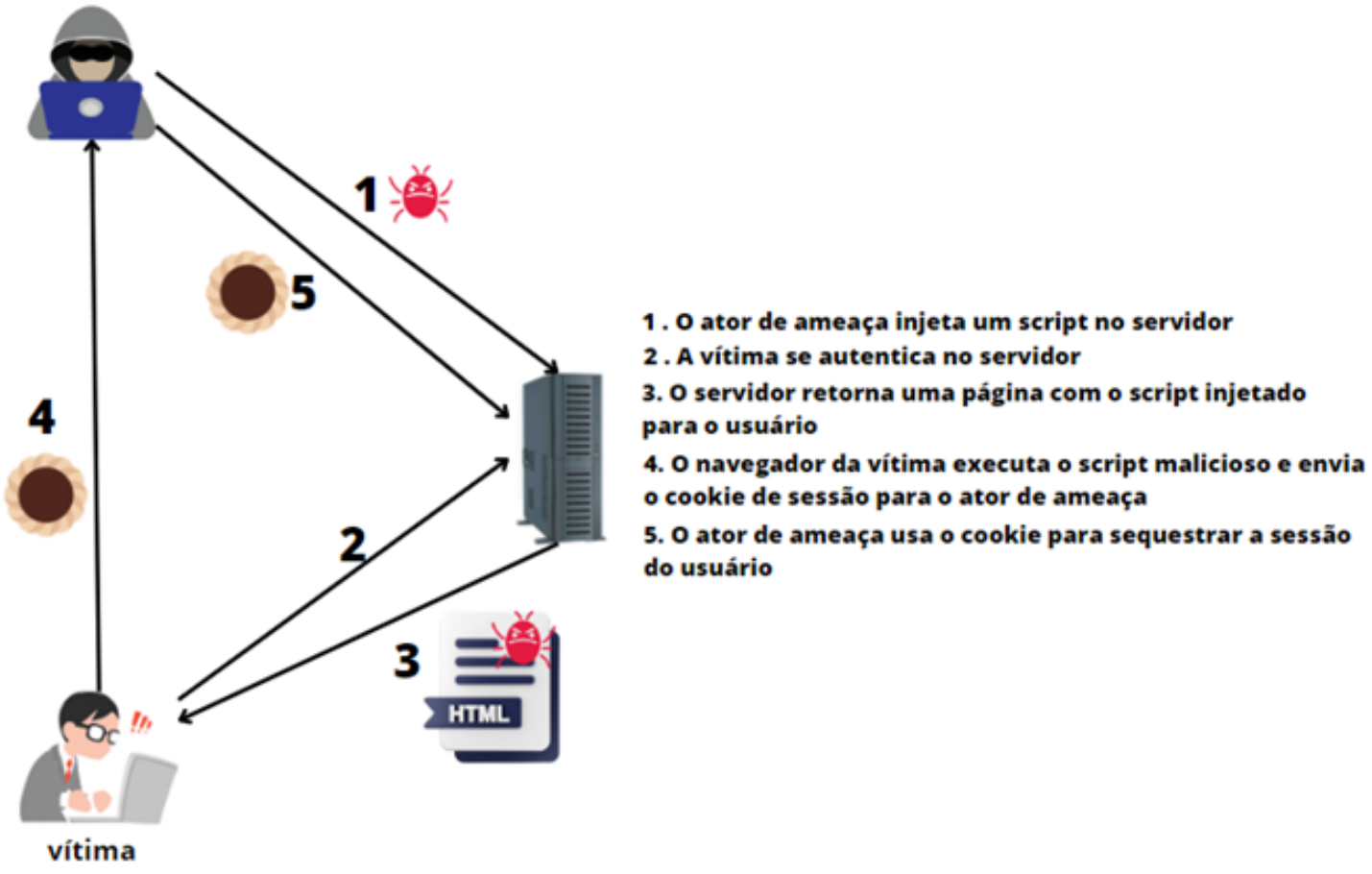
Abuso de serviços remotos, no qual os atores de ameaça exploram vulnerabilidades num programa, serviço ou no próprio *software* do sistema operacional ou no próprio kernel com o objetivo de permitir o movimento lateral no sistema. Essa técnica também é utilizada para obter o acesso inicial ao sistema alvo;

Replicação por meio de mídias removíveis, na qual atores de ameaça utilizam configurações de *autorun* sempre que uma mídia removível é conectada no sistema para implantar um *malware* num sistema (essa técnica também é utilizada na etapa de acesso inicial);

Exploração de *token* de acesso, na qual atores de ameaça utilizam *tokens* de acesso a aplicações roubados para desviar dos controles típicos de segurança;

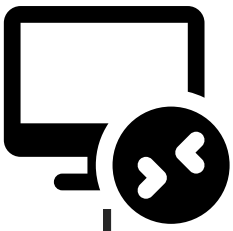
*Pass the Hash* (PtH), na qual os atores de ameaça usam *hashes* de senhas roubados para desviar dos controles normais de segurança do sistema e realizar a movimentação lateral. O PtH é um método de se autenticar como usuário em um sistema sem ter acesso à senha de texto não criptografado do usuário. Esse método ignora as etapas de autenticação padrão que exigem uma senha de texto não criptografado, movendo-se diretamente para a parte da autenticação que usa o *hash* de senha; e

Exploração de *cookies* de sessão, na qual os atores de ameaça usam *cookies* de sessão roubados ou clonados para se autenticar nos serviços e aplicações *web* disponibilizados no ambiente.



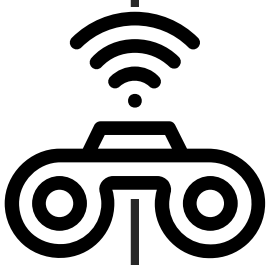
# 7.3.4.1. Acesso a serviços remotos

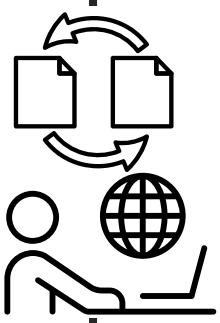
Em um ambiente corporativo, servidores e estações de trabalho geralmente estão organizados em domínios. Os domínios fornecem gerenciamento de identidade centralizado, permitindo que os usuários façam *login* usando um conjunto de credenciais em toda a rede. É justamente por esse motivo que os atores de ameaça realizam ações de descoberta de contas como parte da etapa de mapeamento e expansão.



Sempre que um ator de ameaça consegue obter um conjunto de credenciais de domínio válidas, ele geralmente se torna apto a realizar o *login* em várias máquinas diferentes usando protocolos de acesso remoto, como *Secure Shell* (SSH) ou protocolo de área de trabalho remota (RDP) e executar ações como se fosse o usuário legítimo, inclusive explorar outros aplicativos para realiza um movimento lateral, pois aplicativos legítimos podem utilizar os serviços remotos para acessar *hosts* remotos.

Por exemplo, o *Apple Remote Desktop* (ARD) no macOS é um *software* nativo usado para gerenciamento remoto. Nas versões do macOS anteriores a 10.14, um ator de ameaça poderia escalar uma sessão SSH para uma sessão ARD, o que permitiria o aceite solicitações de TCC (Transparência, Consentimento e Controle) sem a necessidade de interação do usuário, o que possibilitaria, entre outras coisas, enviar comandos diretamente pelo ARD, mantendo a sessão aberta mesmo que ocorresse a troca de senha do usuário durante a sessão.

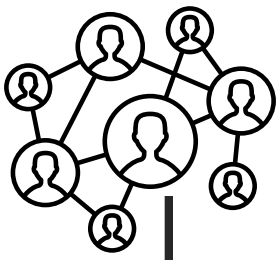




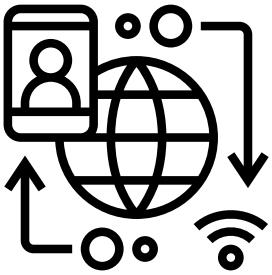
Outra técnica muito utilizada é utilizar contas válidas para interagir com os compartilhamentos remotos de rede usando *Server Message Block* (SMB) em ambiente Windows. As implementações Linux e macOS do SMB geralmente usam o Samba.

O SMB é um protocolo de compartilhamento de arquivos, impressoras e portas seriais de máquinas Windows numa mesma rede ou domínio. Isso possibilita aos atores de ameaça usar o SMB para interagir com compartilhamentos de rede para realizar o movimento lateral na rede.

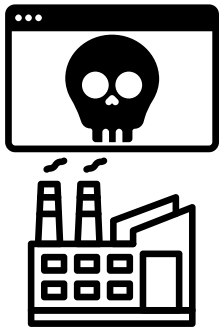
Os sistemas Windows possuem compartilhamentos de rede ocultos que são acessíveis apenas aos administradores e fornecem a capacidade de cópia remota de arquivos e outras funções administrativas. Exemplos de compartilhamentos de rede incluem C$, ADMIN$ e IPC$. Os atores de ameaça podem usar esta técnica em conjunto com contas válidas de nível de administrativo para acessar remotamente um sistema em rede por SMB, interagir com sistemas usando chamadas de procedimento remoto (RPCs), transferir arquivos e executar binários instalados por meio de execução remota.



## 7.3.4.2. Transferência lateral de ferramentas

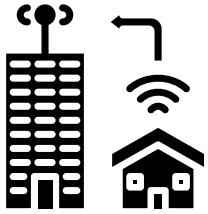


Os atores de ameaça constantemente transferem suas ferramentas e aplicativos de um sistema para outro durante uma operação para realizar o movimento lateral e ampliar a superfície de ataque. Geralmente essa transferência é realizada através de execução remota usando protocolos de compartilhamento de arquivos inerentes ao sistema operacional comprometido, como o compartilhamento de arquivos por SMB, ou usando utilitários padrão como o cmd, bitsadmin, psexec e outros.



Por exemplo, nos ataques realizados pelo *Sandworm Team* contra infraestruturas industriais na Ucrânia, em 2016 e 2017, foram usadas técnicas distintas para transferência lateral de ferramentas. No ataque ao sistema elétrico ucraniano, em 2016, foram utilizados *scripts* VBS para facilitar a transferência lateral de ferramentas. Já em 2017, no ataque realizado contra o setor ucraniano de transporte foi utilizado o *ransomware* auto propagável *Bad Rabbit*, que usa o serviço SMB para se movimentar lateralmente através das redes industriais.

## 7.3.4.3. Sequestro de sessão



É a técnica na qual os atores de ameaça assumem o controle de sessões preexistentes com serviços remotos para mover-se lateralmente em um ambiente. Quando os usuários usam credenciais válidas para fazer *login* em um serviço projetado especificamente para aceitar conexões remotas, como telnet, SSH e RDP, é estabelecida uma sessão que permite manter uma interação contínua com esse serviço.

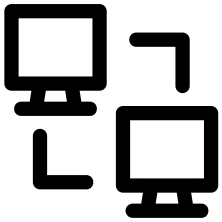
As principais técnicas utilizadas no sequestro de sessão são:

- Sequestro de sessão *Secure Shell* (SSH); e
- Sequestro de sessão *Remote Desktop Protocol* (RDP).

Os atores de ameaça podem sequestrar a sessão SSH de um usuário legítimo para se mover lateralmente no ambiente. O SSH é um meio padrão de acesso remoto em sistemas Linux e macOS. Ele permite que um usuário se conecte a outro sistema por meio de um túnel criptografado, geralmente autenticando por meio de senha, certificado ou uso de um par de chaves de criptografia assimétrica.

Para mover-se lateralmente de um *host* comprometido, os atores de ameaça podem tirar proveito das relações de confiança estabelecidas com outros sistemas por meio de autenticação de chave pública em sessões SSH ativas, sequestrando uma conexão existente com outro sistema. Isso pode ser feito comprometendo o próprio agente SSH ou acessando o soquete do agente. Se o ator de ameaça porventura conseguiu obter acesso *root* anteriormente, o sequestro de sessões SSH será trivial.

Sessões RDP também podem ser sequestradas de um usuário legítimo por atores de ameaça com a finalidade de movimentação lateral no ambiente. O RDP é um recurso comum em sistemas operacionais. Ele permite que um usuário faça *login* em uma sessão interativa com uma interface gráfica do usuário da área de trabalho do sistema em um sistema remoto. A Microsoft refere-se à sua implementação do RDP como *Remote Desktop Services* (RDS).



Normalmente, o usuário legítimo é notificado quando alguém está tentando roubar sua sessão RDP, pois geralmente é solicitada uma confirmação para permitir o acesso à sessão. No entanto, é possível ao ator de ameaça, usando apenas comandos nativos do sistema operacional ou ferramentas de *red teaming*, sequestrar uma sessão de um usuário legítimo sem a necessidade de credenciais ou confirmação da ação por parte do usuário.

No ambiente Windows, por exemplo, um ator de ameaça com permissões de SYSTEM e usando o Terminal *Services Console* c:\windows\system32\tscon.exe <número da sessão a ser roubada>|<nome_da_sessão_a_ser_roubada> pode, remotamente ou localmente e com sessões ativas ou desconectadas, sequestrar uma sessão sem a necessidade de credenciais ou *prompts* para o usuário. Isso também pode levar à descoberta de sistemas remotos e permitir o escalonamento de privilégios, caso a sessão sequestrada pertença a um administrador de domínio ou uma conta com privilégios superiores.


O sequestro de sessão difere do acesso a serviços remotos porque implica no sequestro de uma sessão existente – ativa ou desconectada - em vez de criar uma nova sessão usando contas válidas.

## 7.3.5. Ações de Mitigação para a Etapa de Mapeamento e Expansão

Dentre as possíveis ações de mitigação temos:

- Gerenciar a lista de controle de acesso por alterações nos diretórios de replicação e outras permissões associadas à replicação do controlador de domínio;
- Implementar:
  - Regras de redução de superfície de ataque para aumentar a segurança do LSASS;
  - A autenticação multifator, quando possível;
  - Um processo de gerenciamento de contas privilegiadas (PAM);
- Garantir que os *backups* dos controladores de domínio estejam seguros;
- Desabilitar:
  - O NTLM (NT LAN Manager), quando possível;
  - Os compartilhamentos administrativos do sistema operacional, quando possível;
  - O agente de encaminhamento do protocolo SSH (um mecanismo pelo qual um cliente SSH permite que um servidor SSH use o agente SSH local no servidor em que o usuário realiza o *login* como se fosse um *login* local e não remoto) nos sistemas que não necessitem dessa funcionalidade; e
  - O serviço RDP, quando possível;

- Restringir o acesso a contas privilegiadas;
- Configurar as extensões permitidas e proibidas para instalação no navegador *web*;
- Treinar e conscientizar os usuários sobre as melhores práticas para uso e armazenamento de senhas;
- Implementar políticas fortes de criação, uso e armazenamento de senhas, dentre elas:
    - Impor:
        - tamanho mínimo de senha, obrigando o uso simultâneo de letras maiúsculas, letras minúsculas, números e, quando possível, no mínimo um caractere especial;
        - troca obrigatória de senha a intervalos regulares, com a proibição de repetição da senha;
        - uso de uma senha mestra para acesso ao aplicativo gerenciador de senhas e/ou mecanismos de gerência de senhas do navegador *web*;
    - Bloquear:
        - qualquer conta após um número de tentativas falhas de *login*;
        - imediatamente uma conta que tenha sido identificada como parte de um vazamento de credenciais;
        - o acesso de qualquer conta de usuário fora do horário normal de expediente ou nos casos de afastamento do trabalho (férias, doença etc.), quando possível;
    - Garantir que as contas de administradores tenham senhas complexas e únicas através de todos os sistemas na rede;
    - Limitar a sobreposição de credenciais em contas e sistemas da rede, que ocorre principalmente pelo uso da mesma senha em diversas contas, através do treinamento e conscientização de usuários e administradores;
    - Proibir a reutilização de senhas de administradores locais entre sistemas;
- Utilizar um *firewall* para limitar comunicações de compartilhamento de arquivos, como o SMB;
- Limitar:
    - As contas que podem utilizar serviços remotos;
    - As permissões de todos os usuários que necessitem usar acesso remoto ao mínimo estritamente necessário para a realização de suas atividades. Quando possível:
        - Remover o *root*, o grupo de administradores locais, e todas as contas privilegiadas dos grupos com permissão de realizar acesso remoto através do SSH ou do RDP;
        - Negar o acesso remoto a qualquer usuário utilizando credencias de administrador local;
- Garantir que o par de chaves SSH possuam senhas fortes e evitar usar tecnologias de armazenamento de chaves, como o SSH agente, a menos que estejam devidamente protegidas;
- Utilizar *gateways* de trabalho de área remota;
- Configurar regras no *firewall* de forma a bloquear o tráfego RDP entre zonas de segurança dentro da rede; e
- Reduzir o tempo de *timeout* permitido para qualquer sessão, limitar o tempo máximo permitido que qualquer sessão poderá permanecer ativa e especificar o tempo máximo que uma sessão desconectada permanecerá ativa no *host*.

Cabe observar que:

- Reduzir o tempo de *timeout* permitido para qualquer sessão, limitar o tempo máximo permitido que qualquer sessão poderá permanecer ativa e especificar o tempo máximo que uma sessão desconectada permanecerá ativa no *host*.
  - No caso das técnicas de descoberta de compartilhamentos, uma ação que pode ser realizada para mitigar o problema é não permitir a enumeração anônima de contas e compartilhamentos, o que pode limitar as contas que serão capazes enumerar compartilhamentos de rede; e
  - No caso das técnicas de descoberta de contas, uma das poucas ações de mitigação que pode ser adota é não permitir a enumeração de contas administrativas, pois isso pode levar à descoberta de nomes de contas.
- Uma das poucas ações de mitigação possíveis em relação à técnica de transferência lateral de ferramentas é o uso de sistemas de detecção e prevenção de intrusão que usam assinaturas de rede para identificar o tráfego de *malware* adversário específico ou transferência de dados incomum por meio de ferramentas e protocolos conhecidos, como FTP. Seu uso pode atenuar a atividade no nível da rede. Infelizmente, assinaturas geralmente são para indicadores exclusivos dentro de protocolos e podem ser baseadas na técnica de ofuscação usada por um ator de ameaça ou ferramenta específica, o que significa que provavelmente serão diferentes em várias famílias e versões de *malware*. Isso também significa que os atores de ameaça provavelmente mudarão as assinaturas da ferramenta C2 ao longo do tempo ou construirão protocolos de forma a evitar a detecção por ferramentas defensivas comuns.

## 7.3.6. Atividades de Detecção para a Etapa de Mapeamento e Expansão

Em função da grande variedade de técnicas que podem ser utilizadas e em relação às técnicas e sub técnicas discutidas, algumas das possíveis atividades de detecção incluem monitorar e identificar:

- A execução, especialmente quando realizada por contas não-autenticadas ou fora do horário padrão:
  - De comandos, argumentos e APIs:
    - em atividades que resultem no despejo de memória;
    - que tentem acessar as credenciais de domínio em *cache*;
    - que possam resultar no mapeamento das conexões de-e-para a rede;
    - que tentem listar outros sistemas através de endereços IP, nome de *host* ou outro identificador lógico;
    - que procurem por arquivos e pastas compartilhadas;
    - associados à enumeração de contas;
    - que enumerem processos em execução no sistema;
    - que possam ser utilizados para sequestrar sessões legítimas;
  - Dos comandos ping.exe e tracert.exe, especialmente quando ocorridas em rápida sucessão;

- De processos criados recentemente que procurem enumerar:
  - arquivos e pastas, compartilhadas ou não, ou procurem por locais específicos no *host* ou na rede por uma informação específica no sistema de arquivos;
  - processos em execução no sistema;
- De linhas de comando que possam invocar o SAM;
- De *hash dumpers* abrindo o SAM;
- De qualquer tipo de ação realizadas através de conexões remotas, como RDP, telnet, SSH e VNC, mesmo quando realizadas por contas válidas;

⇒ As interações:

- De processos e ferramentas não esperados (como o mimikatz, procdump, gerenciador de tarefas, e outros) com o LSASS;
- Com compartilhamentos de rede ou transferência de arquivos usando serviços remotos, especialmente o SMB;

⇒ As tentativas de acesso e o acesso realizado:

- À chave de registro do SAM, especialmente para a criação de um arquivo de despejo;
- Aos Locais de armazenamento de senhas realizados por processos, comandos, argumentos e chamadas APIs que normalmente não realizem essa atividade, especialmente quando executados por usuários não-autenticados ou não-autorizados ou fora do horário padrão;
- Aos Aplicativos de gerenciamento de senhas realizados por processos, comandos, argumentos e chamadas APIs que normalmente não realizem esse tipo de atividade, especialmente quando executados por usuários não-autenticados ou não-autorizados ou fora do horário padrão;
- De contas fora dos horários e dias normais de atividade da conta;

⇒ A criação de:

- Serviços por contas válidas que não façam parte do SYSTEM;
- Conexões de rede especificamente para aceitar conexões remotas, especialmente as conexões envolvendo protocolos de gerenciamento remoto comuns, como o tcp:3283 (ARD) e tcp:5900 (VNC – usado pelo ARD), bem como as portas tcp:3389 (RPD) e tcp:22 (SSH) para *login* remoto;
- Serviços usando cmd.exe /k ou cmd.exe /c nos seus argumentos;
- Arquivos associada ao uso de serviços remotos (por exemplo, transferência de arquivos usando serviços remotos);
- Processos que possam auxiliar na transferência lateral de ferramentas, como programas de transferência de arquivos;
- Compartilhamentos de rede não-usuais ou acesso incomum a compartilhamentos de rede usando protocolos como o SMB;

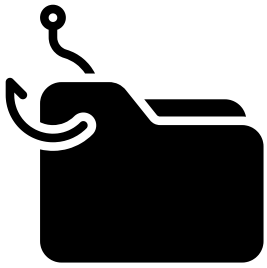
⇒ As tentativas de acesso e o acesso bem-sucedido:

- A arquivos como o /etc/hosts;
- A recursos de arquivos que contenham informação de contas, como /etc/passwd e /users, além das bases de dados de segurança, como a SAM, especialmente por contas e processos sem privilégios administrativos;
- Ao *log* de eventos que possam sugerir a obtenção de listas de contas;

- O tráfego:
  - De rede e conteúdo de pacotes, especialmente os associados ao LDAP e ao MSRPC, que não sigam os padrões esperados de protocolo e fluxo de tráfego;
  - Da *web* de-e-para domínios conhecidos como perigosos ou suspeitos e analisar os fluxos de tráfego que não seguem os padrões de protocolo e de fluxo de tráfego esperados (por exemplo, pacotes estranhos que não pertencem a fluxos estabelecidos ou padrões de tráfego anômalos);
  - Não usual de-e-para *hosts* desconhecidos ou não-esperados;
- A instalação e atividades de extensões em navegadores *web*, especialmente quando executados por usuários não-autenticados ou não-autorizados ou fora do horário padrão;
- Os arquivos dos navegadores *web* que armazenem credenciais, monitorando eventos de leitura a esses arquivos, especialmente quando o processo responsável pela leitura não está normalmente associado a essa atividade;
- Os *logs* de tentativas de autenticação, especialmente as falhas de *login* em contas válidas. Geralmente, uma taxa elevada de falhas de autenticação indica um ataque de força bruta;
- As conexões recentemente construídas associadas a *pings* ou outras ações de varredura que tentem listar outros sistemas através de endereços IP, nome de *host* ou outro identificador lógico;
- Qualquer atividade fora do padrão de contas válidas através de conexões remotas;
- O uso anormal de utilitários ou argumentos de linha de comando que possam ser utilizados para transferir arquivos remotamente;
- A replicação de arquivos por vários *hosts*;
- O uso do tscon.exe por processos ou serviços, especialmente os criados por contas não-administrativas; e
- Os padrões de acesso ou atividades não usuais que ocorram após um *login* remoto, especialmente os acessos de contas a sistemas aos quais geralmente não têm acesso ou as tentativas de uma conta de acessar múltiplos sistemas num intervalo relativamente curto de tempo.

## 7.4. Exfiltração

A exfiltração consiste em técnicas que os atores de ameaça podem usar para roubar dados de uma rede. Depois de coletar os dados, os criminosos costumam empacotá-los para evitar a detecção durante a remoção.



A exfiltração de dados auxilia os atores de ameaça nas ações de chantagem da vítima, aumentando as possibilidades do pagamento do resgate a fim de evitar o vazamento de dados, sendo parte integrante de todos os esquemas de extorsão dupla. Alguns grupos, inclusive, passaram a tratar as atividades de criptografação de dados como secundárias, concentrando-se basicamente na exfiltração dos dados.

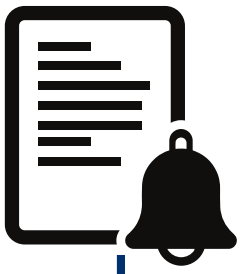
As técnicas para obter dados de uma rede de destino geralmente incluem ações de transferência por meio de seu canal de comando e controle ou um canal alternativo, podendo incluir a colocação de limites de tamanho na transmissão, a compactação e a criptografia.

Dentre as técnicas utilizadas, destacam-se:

- Evasão de defesas, em especial:
  - Transferência agendada;
  - Limitação do tamanho da transferência de dados;
  - Transferência de dados entre contas na nuvem; e
- Exfiltração para fora do ambiente comprometido.

## 7.4.1. Evasão de Defesas

Mecanismos como o *Microsoft Sentinel Fusion engine* são usados para detectar ataques avançados em múltiplos estágios, como abuso dos recursos do computador, acesso a credenciais, destruição de dados e exfiltração de dados. Em especial, no caso de exfiltração de dados, a ferramenta é capaz de identificar e emitir alertas sobre grandes transferências de dados, utilizando como parâmetro um limite (*treshhold*) esperado de volume de dados transferido por operação, por usuário ou por período de tempo, dentre outras possibilidades.

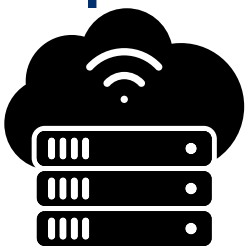


A fim de mascarar os padrões de tráfego gerados pela exfiltração de dados para fora do ambiente comprometido com as atividades normais de rede, os atores de ameaça podem utilizar técnicas como a transferência agendada e a limitação do tamanho da transferência de dados.

Na transferência agendada, os atores de ameaça geralmente utilizam o agendador de tarefas do próprio sistema comprometido de forma a realizar a exfiltração de dados apenas em determinados horários ou a certos intervalos de tempo.

Na limitação do tamanho da transferência de dados, como forma de evitar mecanismos de alerta de violação dos limites de transferência de dados (*data transfer threshold*), os atores de ameaça geralmente exfiltram os dados em pacotes menores, ao invés de extrair um conjunto de dados como um pacote único.

Tanto a transferência agendada como a limitação do tamanho da transferência de dados são aplicadas em conjunto a outras técnicas fim de efetuar a transferência da informação para os atores de ameaça, como a exfiltração usando o canal C2 ou a exfiltração usando protocolos alternativos.
Já na técnica de transferência de dados entre contas na nuvem, ao invés de transferir os dados para fora do ambiente comprometido, os atores de ameaça realizam a exfiltração transferindo os dados – incluindo os *backups* do ambiente em nuvem – para outra conta que eles controlem no mesmo serviço de nuvem, evitando muitos dos mecanismos de detecção de exfiltração.



É possível encontrar casos nos quais equipes de segurança que estão monitorando grandes transferências de dados para fora do ambiente de nuvem, seja por meio de transferências normais de arquivos ou através de canais de comando e controle, não estão monitorando transferências de dados para outra conta dentro do próprio provedor do serviço de nuvem. Essas transferências podem utilizar tanto as APIs existentes como o espaço de endereço interno do próprio provedor de nuvem para misturar a transferência dos dados entre as contas de nuvem ao tráfego normal do ambiente, evitando transferências de dados por interfaces de rede externas.

## 7.4.2. Exfiltração para fora do ambiente comprometido

Normalmente, os atores de ameaça exfiltram os dados do ambiente comprometido para um ambiente sob seu controle. A exfiltração pode ser realizada de diversas formas, dentre elas:

Usando o canal C2: quando os atores de ameaça transferem os dados utilizando o canal C2 estabelecido. Os dados roubados são codificados no canal de comunicações normal usando o mesmo protocolo de comunicações do canal C2;


Usando protocolos alternativos: quando a exfiltração ocorre utilizando um protocolo diferente daquele sendo utilizado pelo ator de ameaça em seu canal C2;

Usando outras mídias de rede: quando a exfiltração ocorre usando uma mídia de rede diferente daquela do canal C2. Por exemplo, se o canal C2 foi estabelecido sobre a rede cabeada, a exfiltração pode ocorrer sobre a conexão *WiFi*, modem, *bluetooth*, ou outro canal de frequência de rádio;

Usando mídias físicas: quando a exfiltração é feita utilizando mídias removíveis, como HDs externos e dispositivos USB, dentre outros; e

Usando serviços *Web*: quando os atores de ameaça utilizam um serviço da *Web* externo legítimo para exfiltrar dados em vez de seu canal principal de comando e controle. Os serviços da *Web* - geralmente repositórios de código (como o GitHub) ou serviços de armazenamento em nuvem (como o Dropbox e o OneDrive) - que são utilizados no processo de exfiltração fornecem uma cobertura significativa para as ações maliciosas pois é grande a probabilidade de que os *hosts* dentro de uma rede já estejam se comunicando com esses serviços antes do comprometimento. Também é comum que existam regras de *firewall* permitindo o tráfego para esses serviços.

## 7.4.3. Ações de Mitigação para a Etapa de Mapeamento e Expansão

Dentre as possíveis ações de mitigação temos:

Utilizar mecanismos de prevenção de perda de dados, que podem detectar e bloquear dados sensíveis sendo:

- Enviados para fora do ambiente utilizando protocolos não criptografados; e
- Copiados para dispositivos de armazenamento removíveis;

Utilizar *proxies web* a fim de fortalecer as políticas de comunicação com a rede externa de forma a evitar o uso de serviços externos não autorizados;

Limitar a criação de novos adaptadores de redes às contas administrativas;

Limitar o uso de dispositivos de armazenamento removível na rede;

Implementar restrições no tráfego de rede de forma a impedir transferências de dados para nuvens privadas virtuais (*Virtual Private Cloud* – VPC) não confiáveis;

Rotacionar as chaves de acesso constantemente, se possível, de forma a reduzir a efetividade do uso de credenciais roubadas; e

Utilizar sistemas de detecção e prevenção de intrusão que usam assinaturas de rede para identificar o tráfego direcionado a uma infraestrutura C2 adversária. Infelizmente, as assinaturas geralmente são para indicadores exclusivos dentro de protocolos e podem ser baseadas na técnica de ofuscação usada por um ator de ameaça ou ferramenta específica, o que significa que provavelmente serão diferentes em várias famílias e versões de *malware*. Isso também significa que os atores de ameaça provavelmente mudarão as assinaturas da ferramenta C2 ao longo do tempo ou construirão protocolos de forma a evitar a detecção por ferramentas defensivas comuns;

## 7.4.4. Atividades de Detecção para a Etapa de Evasão de Defesas

Dentre as possíveis ações de mitigação temos:

Monitorar a criação de novas conexões de rede originadas ou sendo destinadas a *hosts* não confiáveis;

Monitorar o tráfego de rede originário de dispositivos de *hardware* incomuns ou não esperados. Metadados do tráfego da rede local, como o endereço MAC da fonte, assim como o uso dos protocolos de gerenciamento de rede, como o DHCP, são úteis para identificar o *hardware* envolvido;

Monitorar o conteúdo do tráfego de rede e a inspeção de pacotes associados aos protocolos e analisar o fluxo de tráfego que não esteja aderente aos padrões de protocolo e fluxo de tráfego esperados (por exemplo, pacotes estranhos que não pertençam a fluxos estabelecidos, padrões de tráfego anômalos, sintaxes ou estruturas anômalas);

Monitorar o tráfego de dados de-e-para domínios conhecidos como perigosos ou suspeitos e analisar os fluxos de tráfego que não seguem os padrões de protocolo e de fluxo de tráfego esperados (por exemplo, pacotes estranhos que não pertencem a fluxos estabelecidos ou padrões de tráfego anômalos);

Monitorar tentativas de criação e compartilhamento de dados, como *snapshots* e *backups*, a partir de contas não confiáveis ou não usuais;

Estabelecer, periodicamente, uma linha de base para as atividades no ambiente, de forma a identificar comportamentos maliciosos;
Monitorar transferências de dados anormais entre contas;

Monitorar a criação de novas conexões de rede originadas ou sendo destinadas a:

- *Hosts* não confiáveis; ou
- Serviços *Web* ou em nuvem associados a processos anormais ou que não sejam executados a partir de um navegador *Web*;

Monitorar a criação de novas conexões por processos que normalmente não utilizam comunicação de rede;

Monitorar a criação de novas letras para *drives* na rede ou novos pontos de montagem de dispositivos de armazenamento removíveis;

Monitorar o acesso a arquivos por serviços *Web* externos;

Monitorar a transferência de arquivos para dispositivos de armazenamento removíveis; e


Monitorar a execução de APIs, comandos e argumentos que possam ser utilizados para o roubo de dados através da exfiltração de dados para fora do ambiente.

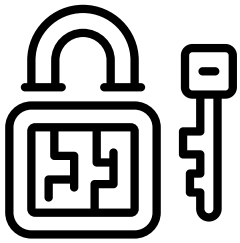
## 7.5 Impacto

As verdadeiras consequências do ataque começam a se desenrolar durante a fase de impacto. Durante esta fase, os atores de ameaças criptografam realizam diversas atividades com a finalidade de:

- Destruir as evidências e programas usados durante as etapas do ataque de *ransomware*, dificultando as atividades de recuperação das operações e análise forense do incidente;
- Interromper as atividades da vítima e dificultar a recuperação dos dados sem o pagamento de resgate;
- Interromper a disponibilidade ou comprometer a integridade por meio da manipulação de processos comerciais e operacionais; e
- Fornecer cobertura para uma violação de confidencialidade.

Em alguns casos, os processos comprometidos podem aparentemente estar em perfeito funcionamento, mas podem ter sido alterados para beneficiar os objetivos dos atores de ameaça.

A criptografia de dados é a técnica de impacto mais utilizada em ataques de *ransomware*. Os atores de ameaça geralmente criptografam dados em sistemas de destino ou em um grande número de sistemas em uma rede para interromper a disponibilidade de recursos do sistema e da rede. A criptografia também é utilizada para tornar os dados armazenados inacessíveis a fim de extrair compensação monetária de uma vítima em troca de descriptografia ou uma chave de descriptografia, com a ameaça de tornar os dados permanentemente inacessíveis nos casos de não-pagamento.

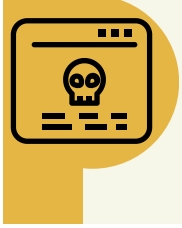


Outras técnicas muito utilizadas são:

Remoção do acesso a contas, causando indisponibilidade de recursos do sistema e da rede pela inibição do acesso a contas utilizadas por usuários legítimos. As contas podem ser excluídas, bloqueadas ou manipuladas (alterando credenciais, por exemplo) para remover o acesso às contas;

Destruição de dados, causando a interrupção e a indisponibilidade de sistemas, serviços e recursos de rede pela destruição sistemática de dados e arquivos em sistemas específicos ou em grande número. A destruição de dados geralmente torna os dados armazenados irrecuperáveis por técnicas forenses por meio da substituição de arquivos ou dados em unidades locais e remotas;

Manipulação de dados, na qual os atores de ameaça inserem, excluem ou manipulam dados para influenciar resultados externos ou ocultar atividades, ameaçando assim a integridade dos dados. Ao manipular dados, os atores de ameaça podem tentar afetar um processo de negócios, entendimento organizacional ou tomada de decisão;



*Defacement*, na qual ocorre a modificação do conteúdo visual disponível interna ou externamente a uma rede corporativa, afetando assim a integridade do conteúdo original. Os motivos para desfiguração incluem envio de mensagens, intimidação ou reivindicação (muitas vezes falsa) de crédito por uma invasão. Imagens perturbadoras ou ofensivas podem ser usadas como parte do *defacement* para causar desconforto ao usuário ou para pressionar o cumprimento das mensagens que o acompanham.

Infelizmente, é importante observar que a maioria das técnicas utilizada para impacto não podem ser facilmente mitigadas usando apenas controles preventivos uma vez que se baseiam no abuso de componentes do próprio sistema operacional. Dessa forma, as principais maneiras de mitigar os impactos de um ataque de *ransomware* são:

- Implementar um plano de recuperação de desastres; e
- Realizar *backups* seguros periodicamente, armazenando os *backups* em locais separados e protegidos.

Dentre as possíveis ações de detecção, temos:

Monitorar modificações em constas de usuários como deleções inesperadas de contas e alterações atributos de contas (como alterações de senha, de credenciais ou de *status*), especialmente quando realizadas por contas ou processos incomuns ou não esperados;

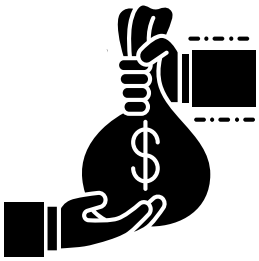
Monitorar a execução de comandos que possam ser envolvidos em atividades de destruição de dados. Em ambiente Linux, deve-se monitorar comandos como o wipe (usado em *disk wipe*), shred (usado para a destruição de dados de partição, pasta ou arquivos), dd (usado para apagar o disco, substituindo o disco inteiro por sequencias de zeros), especialmente quando realizadas por contas ou processos incomuns ou não esperados;

Monitorar a modificação de grande volume de arquivos e diretórios (como deleções ou alterações em atributos/conteúdo/formato), especialmente quando realizadas por contas ou processos incomuns ou não esperados. A criptografia de dados se inclui nesse tipo de monitoração;

Monitorar a deleção de *snapshots* do ambiente, especialmente quando realizadas por contas ou processos incomuns ou não esperados; e

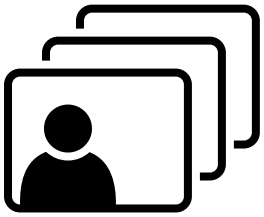
Monitorar alteração em todo conteúdo visual do ambiente, especialmente quando realizadas por contas ou processos incomuns ou não esperados.

## VIII – Fase 3: Comunicação e Extorsão



Nesta fase, os atores de ameaça estabelecem um canal de comunicação com a vítima e iniciam o processo de extorsão. Durante esta fase, os agentes de ameaças iniciam o contato com a vítima para transmitir suas demandas e estabelecer uma linha de comunicação. Eles costumam usar tecnologias de anonimato, como a rede Tor, para mascarar suas identidades e dificultar o rastreamento de suas atividades. A comunicação pode ocorrer por meio de vários canais, incluindo *e-mail*, plataformas de mensagens instantâneas ou mesmo portais de negociação de resgate dedicados configurados pelos invasores.

Em incidentes tradicionais de *ransomware*, que implicam apenas na criptografia de dados sensíveis da vítima, os atores de ameaça vão exigir pagamentos de resgate em troca de fornecer as chaves de descriptografia ou acesso aos sistemas da vítima.



Em incidentes de extorsão dupla, quando ocorre tanto a criptografia como a exfiltração de dados sensíveis, além da exigência de pagamento em troca das chaves de descriptografia, também ocorre a ameaça da publicação dos dados exfiltrados como forma adicional de pressionar a vítima. Muitas vezes os atores de *ransomware* enviam prova da exfiltração (alguns dos arquivos exfiltrados) para garantir a veracidade de suas ameaças.

Em alguns incidentes mais recentes, a extorsão se concentrou apenas na exfiltração de dados, com a ameaça de sua divulgação pública caso o pagamento da extorsão não fosse realizado.

Os atores de ameaças empregam métodos diferentes para exigir pagamentos de resgate de suas vítimas. Estes geralmente incluem:

- Exigência de pagamentos em Criptomoeda: Os agentes de ameaças geralmente exigem pagamentos de resgate em criptomoedas devido à natureza descentralizada e anônima das transações desses ativos, o que as torna difíceis de rastrear;
- Definição de prazos de pagamento rígidos: os atores de ameaças geralmente impõem prazos rígidos de pagamento, acompanhados de ameaças de exclusão permanente das chaves de descriptografia, aumento do valor do resgate e/ou divulgação dos dados exfiltrados se o prazo não for cumprido. Essas táticas visam pressionar as vítimas a cumprirem suas demandas; e
- Exigência do sigilo da transação, especialmente de sua comunicação às autoridades competentes.

A decisão de atender as demandas dos atores de ameaças durante a fase de extorsão deve levar em contas diversas considerações legais e éticas. As organizações devem avaliar cuidadosamente suas opções, observando, especialmente:

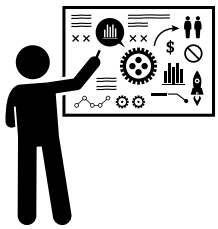
- Considerações legais:
  - Pagar o resgate pode ser ilegal em algumas jurisdições (De acordo com o *International Emergency Economic Powers Act and Trading with the Enemy Act*, empresas e pessoas nos EUA geralmente são proibidas de se envolver em transações, direta ou indiretamente, com indivíduos ou entidades contidas na *Specially Designated Nationals And Blocked Persons List do Office Foreign Assets Control* – OFAC e aquelas cobertas por embargos abrangentes de país ou região) ou ser contra as próprias políticas organizacionais.
  - Manter o sigilo da operação pode ser impossível caso a organização tenha obrigações legais de relatar o incidente, principalmente se dados pessoais ou confidenciais tiverem sido comprometidos, como ocorre em função da Lei Geral de Proteção de Dados - LGPD no Brasil e da *General Data Protection Regulation* – GDPR, na Europa.
- Considerações éticas: pagar o resgate pode contribuir para financiar outras atividades criminosas, pois o dinheiro pode ser usado para financiar ataques futuros. Apoiar cibercriminosos por meio de pagamentos de resgate perpetua o ecossistema de *ransomware*;
- Sem garantia de descriptografia: não há garantia de que os agentes de ameaças fornecerão as chaves de descriptografia ou restaurarão o acesso aos sistemas da vítima, mesmo após o pagamento do resgate. As organizações devem considerar o risco de pagar o resgate e não receber o resultado prometido;
- Sem garantia da preservação do sigilo dos dados: apesar dos principais grupos afirmarem que não divulgarão os dados exfiltrados no caso do pagamento da extorsão, não existe nenhuma garantia que posteriormente esses dados sejam utilizados em novo processo de extorsão ou simplesmente sejam vendidos a terceiros; e
- Cobertura de seguro cibernético: as organizações com apólices de seguro cibernético devem consultar seus provedores de seguros sobre sua cobertura e as implicações de pagar o resgate.

É crucial que as organizações consultem advogados, agências de aplicação da lei e profissionais experientes em resposta a incidentes antes de tomar qualquer decisão sobre o pagamento do resgate. Cada situação é única e é necessária uma avaliação completa dos riscos, obrigações legais e considerações éticas.

# IX – Fase 4: Recuperação do incidente

Durante a fase de recuperação do incidente a organização age de forma a conter o incidente, preservar as evidências necessárias para análise futura, restaurar os sistemas afetados e implementar medidas para evitar incidentes futuros.

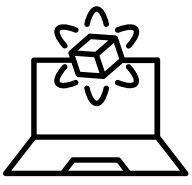

A recuperação correta de qualquer incidente cibernético depende da existência de um planejamento que defina um método sistemático a ser adotado. Isso quer dizer que as fases de recuperação de um incidente de *ransomware* dependem da organização ter realizado uma fase de preparação para responder a incidentes cibernéticos.



A fase de preparação é o ponto de partida de um Plano de Resposta a Incidentes e, em última análise, talvez a fase mais importante para proteger a organização como um todo. É preciso garantir que seus colaboradores estejam devidamente capacitados acerca de suas responsabilidades e funções, caso ocorra um incidente. O plano deve ser bem fundamentado, detalhando as funções e responsabilidades de todos.

De maneira geral, o Plano de Resposta a Incidentes definirá:

- Quem fará parte do time de resposta, estabelecendo papéis e responsabilidades de cada um;
- O fluxo de processos e descrever as atividades de tratamento de incidentes de segurança, dentre elas:
  - Estabelecer critérios para uma triagem inicial de todos os incidentes, definindo:
    - O que é considerado um incidente de segurança e quais gatilhos acionam o time de resposta;
    - Os critérios de classificação de criticidade;
  - As medidas de contenção, com a devida preservação de evidência;
  - O plano de comunicação do incidente às partes interessadas;
  - As ações de tratamento do incidente, dentre elas:
  - A forma de verificação de danos ao titular dos dados;
  - Medidas de erradicação dos vetores de ataque;
  - Medidas de recuperação dos sistemas afetados;
  - Atividades para a análise pós-incidentes.



É importante ressaltar que de forma a garantir que cada ator envolvido desempenhe o papel que lhe foi atribuído é preciso colocar o plano à prova. Para isso, é preciso avaliar o nível de preparação em termos de proteção e resposta conduzindo testes de segurança, simulando invasões ou violações de dados.

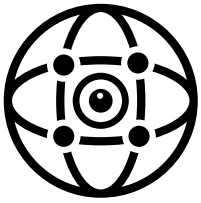

Para que o Plano de Resposta a Incidente seja realmente efetivo é necessário que todos os seus aspectos sejam aprovados pela Alta Administração e que sejam disponibilizados os recursos necessários para sua operacionalização e devido funcionamento antecipadamente.

Por fim, a inexistência de um Plano de Resposta a Incidentes implica, basicamente, na incapacidade da organização em agir de forma coerente, coordenada e eficiente para se recuperar de um incidente cibernético.

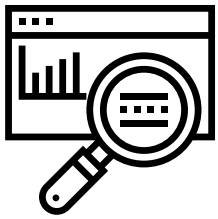
Por fim, a inexistência de um Plano de Resposta a Incidentes implica, basicamente, na incapacidade da organização em agir de forma coerente, coordenada e eficiente para se recuperar de um incidente cibernético.

**Fases da recuperação de um incidente de cibernético**


## 9.1. Detecção e Análise



Durante esta fase, a equipe de segurança monitora a rede em busca de atividades suspeitas e ameaças em potencial. São analisados dados, notificações e alertas coletados de *logs* de dispositivos e de várias ferramentas de segurança (*software* antivírus, *firewalls*) instalados na rede, filtrando os falsos positivos e fazendo a triagem dos alertas reais por ordem de gravidade.



Atualmente, a maioria das organizações usa uma ou mais soluções de segurança, como SIEM (Gerenciamento de eventos e informações de segurança) e EDR (*endpoint detection and response*) para ajudar as equipes de segurança a monitorar e analisar eventos de segurança em tempo real, além de automatizar processos de detecção de e reposta a incidentes.

Uma vez determinado que está ocorrendo um incidente cibernético, a primeira atividade da equipe de segurança deve ser determinar, dentre outros:

- O momento em que o incidente ocorreu;
- A forma de detecção do incidente;
- O responsável pela detecção; e
- As áreas afetadas.

Um dos problemas recorrentes em incidentes de *ransomware* é que não ocorre uma detecção prévia do problema (durante as etapas de acesso inicial, estabelecimento do ponto de apoio e C2, mapeamento e expansão do ambiente, ou do ataque propriamente dito), e sim uma reação ao comunicado e extorsão do grupo responsável por um ataque bem-sucedido. Nesse caso, as equipes de segurança, no primeiro momento, apenas atuam para confirmar que o incidente está realmente ocorrendo.

Uma vez confirmado o incidente e seu escopo, é necessário avaliar o impacto e aplicar um nível de gravidade para o incidente, determinando, dentre outros aspectos:

- O total de clientes (internos e externos) afetados;
- O alcance do comprometimento; e
- O impacto do incidente em termos:
  - Funcionais;
  - Informacionais; e
  - De Recuperação.

O impacto funcional pode ser:

| | |
|---|---|
| Nulo | Nenhum efeito na capacidade da organização em continuar prestando o serviço a todos os usuários |
| Baixo | Efeito mínimo, a organização pode continuar a prestar os serviços críticos a todos os usuários, mas com uma perda de eficiência |
| Médio | A organização perdeu a capacidade de prestar os serviços críticos a um grupo de usuários |
| Alto | A organização não tem mais capacidade de prestar os serviços críticos a nenhum usuário |

O impacto informacional pode ser:

| | |
|---|---|
| Nenhum | Nenhuma informação foi exfiltrada, modificada, apagada ou comprometida de qualquer forma |
| Vazamento de dados privados | Informação pessoal sensível de usuários, empregados etc., foi acessada ou exfiltrada |
| Vazamento de dados proprietários | Informação proprietária sensível, como informações da infraestrutura crítica da organização, foi acessada ou exfiltrada |
| Perda de integridade | Informação classificada ou sensível, privada ou proprietária, foi modificada, apagada ou comprometida de qualquer forma (por exemplo, criptografada por um ator de ameaça) |

O impacto de recuperação pode ser:

| | |
|---|---|
| Regular | O tempo de recuperação é previsível com os recursos disponíveis |
| Suplementado | O tempo de recuperação é previsível com recursos adicionais |
| Estendido | O tempo de recuperação é imprevisível, recursos adicionais e auxílio externo são necessários |
| Não recuperável | A recuperação do incidente não é possível (exemplo: dados pessoais sensíveis forma exfiltrados e publicados), uma investigação será necessária |

Os níveis de gravidade de incidentes são uma medição do impacto que eles têm nos negócios. Em geral, quanto menor o número de gravidade, maior é o impacto do incidente. Por exemplo, uma possível classificação de nível de gravidade seria:

Gravidade 1: incidente crítico com impacto crítico, como, por exemplo, um incidente de impacto funcional Alto, com perda de integridade e/ou vazamento de dados privados/proprietário e não recuperável;

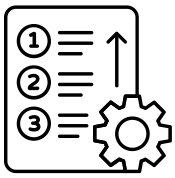
Gravidade 2: incidente crítico com alto impacto, como, por exemplo, um incidente de impacto funcional Alto, com perda de integridade e/ou vazamento de dados privados/proprietário, com impacto de recuperação Estendido;

Gravidade 3: incidente grave com impacto significativo, como, por exemplo, um incidente de impacto funcional médio, com vazamento de dados privados/proprietários, com impacto de recuperação Estendido ou Suplementado;

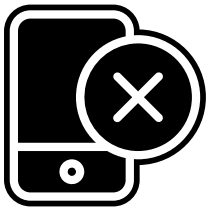
Gravidade 4: incidente médio com médio impacto, como, por exemplo, um incidente de impacto funcional Médio ou Baixo, nenhum vazamento informacional, com impacto de recuperação Suplementado ou Regular;

Gravidade 5: incidente leve com baixo impacto, como, por exemplo, um incidente de impacto funcional Baixo, nenhum vazamento de informação e tempo de recuperação Regular.

Esse tipo de classificação pode variar entre organizações. Por exemplo, uma organização pode entender que qualquer vazamento de informação ou perda de integridade deve ser classificada como um incidente crítico.



Da mesma forma, a gravidade de um incidente (o impacto que ele tem sobre usuários e organização) também está relacionada com a prioridade do incidente (a rapidez com que o problema deve ser corrigido). Às vezes, essas duas medidas estão completamente alinhadas, como, por exemplo, num incidente que cause a paralisação de todas as atividades da organização. Porém, muitas vezes a prioridade e a gravidade não se alinham.



Por exemplo, pode ocorrer de um incidente causar a paralisação completa de um aplicativo. Ele é de alta gravidade porque impede que os seus usuários realizem suas atividades. No entanto, se o incidente estiver afetando apenas 1% dos usuários, não estiver relacionado a uma atividade crítica para a organização e se houver outros incidentes com impacto mais amplo ele pode não ser considerado de alta prioridade.

Apesar das dificuldades que certamente surgem na classificação de nível de gravidade, é importante ressaltar que usar um sistema de numeração para níveis de gravidade ajuda a definir e comunicar o incidente com rapidez, o que auxilia na definição de prioridades e ações que devem ser adotadas na contenção, erradicação e recuperação do incidente.

## 9.2. Contenção

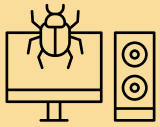
Nesta fase, a organização age para impedir que a violação cause mais danos à rede. As atividades de contenção podem ser divididas em:

- Medidas de curto prazo, que se concentram em impedir que o incidente atual se espalhe, por meio do isolamento dos sistemas afetados, com ações como:

  - No caso de vários sistemas ou sub-redes parecerem afetados, colocar a rede *offline*, pois pode não ser viável desconectar sistemas individuais durante um incidente;
  - Priorizar o isolamento de sistemas críticos para as operações diárias;
  - Remover fisicamente da rede – pela desconexão do cabo de rede e/ou desabilitação do *wifi/bluetooth* – os dispositivos afetados, caso não seja possível colocar a rede *offline*;

  - Somente desligar os sistemas afetados caso não seja possível desconectá-los da rede a fim de evitar a propagação do incidente. Cabe ressaltar que essa ação impedirá a organização de recupera o *malware* e demais artefatos utilizados pelos atores de ameaça que estejam armazenados apenas na memória volátil;

- Preservação de evidências, com a criação de uma imagem do sistema e da memória dos dispositivos afetados, a fim de auxiliar nas atividades de identificação do *malware*, mecanismos e técnicas utilizados, indicadores de compromisso (IoCs) e outros arquivos e binários relevantes;
- Triagem dos sistemas impactados para restauração e recuperação, identificando e priorizando os sistemas críticos de acordo com o mapeamento de ativos existentes;
- Exame dos sistemas de detecção e prevenção (como, por exemplo, *antimalware*, EDR, IDS, IPS) e *logs* de forma a encontrar evidências sobre as causas e execução do incidente e mecanismos adicionais que podem ter sido utilizados no ataque;
- Identificação e bloqueio das contas envolvidas no acesso inicial, incluindo contas de *e-mail*, e credenciais privilegiadas comprometidas;
- Documentação detalhada do incidente;
- Proteção dos sistemas que não foram afetados, aplicando controles de segurança mais restritos, como isolar os bancos de dados críticos e alterar todas as credenciais de acesso de usuários e administrativos.

É crucial também que a organização tenha um bom sistema de *backup* para ajudar a restaurar suas operações. Assim, qualquer dado ou ativo comprometido não será perdido definitivamente.

## 9.3. Relatório e Notificação

Uma vez que um incidente cibernético é confirmado, é necessário comunicar aos interessados internos e externos o mais rápido possível. O objetivo da comunicação interna é focar a resposta a incidentes em um só lugar e reduzir a confusão. O objetivo da comunicação externa é contar aos clientes que a equipe tem conhecimento que algo não está funcionando e que já está sendo investigado.

Um Plano de Comunicação de Resposta a Incidentes é um componente crucial do Plano de Resposta a Incidentes de uma organização, orientando e direcionando corretamente os esforços de comunicação. Tentar fazer boas escolhas rapidamente, no ambiente de alta pressão em torno de um incidente de segurança, é uma receita para o desastre.

A primeira comunicação crucial que ocorre após um incidente de segurança é a ativação da equipe de resposta a incidentes. Nos casos em que o incidente de segurança foi confirmado e que a ativação da equipe é necessária, o tempo se torna essencial. As organizações devem considerar a adoção de um mecanismo de alerta que utilize múltiplos canais de comunicação a fim de acelerar esse processo.

Assim que a notícia de um incidente de segurança vazar, as partes interessadas, internas e externas, começarão a clamar por informações. A equipe de resposta a incidentes será bombardeada por consultas de clientes, mídia, reguladores e outras partes interessadas. A comunicação de um incidente requer uma resposta coordenada para controlar os rumores e garantir que a organização apresente uma mensagem clara e consistente nos canais de comunicação.

Por este motivo, é recomendável que o Plano de Comunicação determine quais os atores que ficarão responsáveis por fornecer uma visão consistente e coordenada do incidente às partes interessadas externas por meio de atualizações regulares. Esses atores devem ter familiaridade suficiente com os conceitos técnicos para servir tanto como tradutor quanto como filtro para as informações técnicas que surgem da equipe de resposta. Um glossário pode ajudar a garantir que o vocabulário usado nas comunicações escritas e verbais seja correto e consistente.


O Plano de Comunicação também deve determinar duas decisões cruciais envolvendo o incidente:

- Quando é apropriado envolver as outras organizações, autoridades policiais e agências reguladoras, especialmente para auxiliar nas atividades de recuperação do incidente; e
- Quando é obrigatório comunicar e envolver autoridades policiais, agências reguladoras e/ou outras organizações e indivíduos.

Essas são decisões difíceis porque o envolvimento policial muitas vezes muda a natureza de uma investigação e aumenta a probabilidade de chamar a atenção do público. Por outro lado, as autoridades policiais têm acesso a ferramentas de investigação, como mandados de busca e apreensão, que não estão disponíveis para as equipes internas. Por esse motivo, o Plano de Comunicação deve abordar esse dilema, delineando critérios claros para quando é apropriado para a equipe notificar as autoridades policiais. O plano também deve identificar quem na equipe tem autoridade para fazer essa determinação e quais notificações internas devem ocorrer antes de envolver a aplicação da lei. Por exemplo, a equipe provavelmente deve consultar a Alta Administração e o conselho jurídico antes de envolver as autoridades.

O Plano de Comunicação também deve determinar quando é obrigatório a comunicação a agências reguladoras e autoridades policiais, dentre outros.

Por exemplo, de acordo com a Lei Geral de Proteção de Dados – LGPD, caso o incidente envolva dados pessoais sujeitos à LGPD que possam gerar risco ou danos relevantes aos titulares, é obrigatória a comunicação do incidente tanto à ANPD como aos titulares dos dados. A comunicação aos titulares deverá conter, no mínimo, as seguintes informações:


- Resumo e data da ocorrência do incidente;
- Descrição dos dados pessoais afetados;
- Riscos e consequências aos titulares de dados;
- Medidas tomadas pelo controlador e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis; e
- Dados de contato do encarregado do controlador para que os titulares possam solicitar informações adicionais a respeito do incidente.

Por fim, é conveniente que o Plano de Comunicação defina os modelos (*templates*) de comunicação que devem ser utilizados.

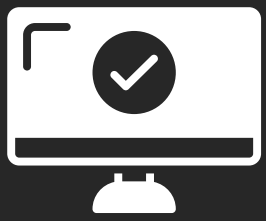
Todos os incidentes de segurança exigem um nível de comunicação adequado com Alta Administração, conselho jurídico, usuários internos, usuários externos e, muitas vezes, com a mídia e o público em geral, com informações completas, corretas e com a utilização de um vocabulário adequado ao seu público-alvo.

É por isso que os modelos de comunicação são tão críticos para um Plano de Comunicação. É extremamente difícil elaborar uma mensagem de notificação criteriosa e cuidadosa em um momento de crise, além da dificuldade de coordenar as informações e considerações de diversas pessoas de áreas distintas, desde gerentes de contas e executivos a advogados e especialistas em relações públicas.

O desenvolvimento de modelos de comunicação de resposta a incidentes pré-aprovados pode eliminar esses obstáculos com antecedência, deixando a equipe de resposta a incidentes simplesmente preencher os espaços em branco e ajustar a linguagem do modelo, conforme necessário.

## 9.4. Erradicação

Uma vez contida a situação, é preciso encontrar e eliminar a causa do incidente. Portanto, os sistemas devem ser corrigidos, as vulnerabilidades exploradas devem ser eliminadas e as atualizações de segurança existentes devem ser aplicadas. Esse trabalho tem de ser realizado de modo minucioso, para que não persistam vestígios do *malware*, mecanismos ou das vulnerabilidades que foram utilizadas no ataque.

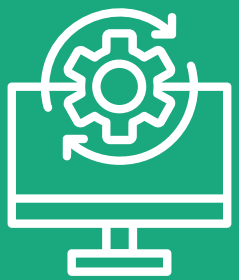


Dentre as ações possíveis nessa fase, estão:

- Conduzir uma análise profunda para identificar e eliminar os mecanismos de persistência existentes;
- Reconstruir os sistemas considerando a priorização de sistemas críticos, realizando as seguintes atividades:
  - Restauração completa das imagens de unidades de armazenamento, implicando na exclusão de todos os dados atuais;
  - Realizar o *reset* de senhas e credenciais para todos os sistemas afetados; e
  - Corrigir as vulnerabilidades existentes pela aplicação de patches de segurança, atualizações de segurança, ou aplicação de novas políticas de segurança ou outras ações relacionadas.

## 9.5. Recuperação e Atividade Pós-Incidente

Quando a equipe de resposta a incidentes estiver confiante que a ameaça foi completamente erradicada, ela irá restaurar o funcionamento normal dos sistemas afetados. O tipo de recuperação depende, principalmente, da natureza e da magnitude do incidente.



Caso o incidente não tenha afetado dados e tenha sido detectado em seus estágios iniciais, pode ser possível restaurar as atividades rapidamente apenas pela remoção dos artefatos maliciosos e substituição dos arquivos comprometidos por versões limpas (esse tipo de atividade teria o tempo de resposta mais rápido, mas corre-se o risco de deixar artefatos maliciosos ainda dormentes nos sistemas afetados).

Caso os *backups* não tenham sido afetados, a restauração é possível com uma perda mínima de dados. No entanto, caso os *backups* mais recentes também tenham sido afetados, haverá uma perda considerável de dados e a operação, além de demandar um tempo significativo (é necessário identificar a partir de qual momento os *backups* foram comprometidos, restaurar os dados a partir de *backups* defasados e elaborar uma estratégia para repor os dados perdidos no processo) implicará em custos muito maiores.

A ação de recuperação poderá envolver as seguintes atividades, dentre outras:

- Definição de cronograma para a restauração das operações pelos responsáveis pelos ativos de informação afetados;
- Recuperar os dados a partir de *backups* seguros existentes;
- Realização de varredura completa do ambiente recuperado, de forma a garantir que este esteja apto para uso seguro;
- Realização de testes de funcionamento do ambiente recuperado, validando os resultados com as linhas de base definidas, à medida em que forem disponibilizados para uso;
- Monitoramento do ambiente recuperado, a ser executado num período após o incidente cibernético, de forma a verificar comportamentos atípicos ou anormalidade nas operações.

Após o término do processo de recuperação, as equipes envolvidas devem documentar as lições aprendidas do incidente e das atividades de resposta associadas, de forma a determinar a necessidade de refinamento da Política de Segurança, do Plano de Gerenciamento de Riscos e do Plano de Resposta a Incidentes.

As lições aprendidas devem responder perguntas como:

- As falhas de segurança que foram exploradas pelo incidente e que não estavam previstas nas políticas, planos e procedimentos de segurança;
- As falhas na execução do Plano de Resposta a Incidente, em especial:
  - As etapas do planejamento de resposta a incidentes que foram seguidas, mas não apresentaram o resultado esperado;
  - As etapas do planejamento de resposta a incidentes que não foram seguidas e o que motivou essa decisão; e
  - Atividades que poderiam ter sido realizadas para auxiliar na recuperação do incidente, mas que não estavam previstas;
- Medidas preventivas que devem ser adotadas para evitar a ocorrência de eventos similares.

É importante lembrar que, de acordo com o Plano de Gestão de Incidente Cibernéticos para a Administração Pública Federal, publicado pela Portaria GSI/PR nº 120, de 21 de dezembro de 2022, após o término do processo de recuperação, os participantes da Rede Federal de Gestão de Incidentes Cibernéticos (Regic) deverão encaminhar ao Centro Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governos (CTIR Gov) um relatório do incidente, contendo as seguintes informações:

- Atores atacantes e atacados;
- Atores envolvidos no tratamento e resposta do incidente;
- Evidências coletadas;
- Indicadores de comprometimento (IoCs), bem como táticas, técnicas e procedimentos (TTPs) utilizadas pelos atores de ameaça durante o incidente;
- Ativos de infraestrutura, serviços e total de usuários afetados;
- Volume de dados exfiltrados;
- Cronologia dos fatos;
- Medidas de contenção, erradicação e recuperação adotadas; e
- Medidas preventivas propostas para ocorrências similares.

# X - Considerações Finais

Nos últimos anos o *ransomware* evoluiu dramaticamente desde suas origens iniciais, bastante primitivas, para se transformar em um modelo de negócio, com os atores de ameaça sendo capazes de lançar ataques de *ransomware* contra grandes empresas, organizações e até mesmo governos, causando danos incalculáveis.

O apelo do *ransomware* para os atores de ameaça é claro. Além de ser um processo relativamente simples, pode causar muitos danos e as recompensas em potencial costumam ser substanciais, com as demandas de *ransomware* muitas vezes rendendo aos cibercriminosos um significativo retorno financeiro. Além disso, embora algumas vítimas consigam mitigar os ataques e restaurar seus arquivos ou sistemas sem pagar resgates, basta apenas uma pequena porcentagem de ataques bem-sucedidos para produzir receita substancial – e incentivo – para os cibercriminosos.

Não é nenhuma surpresa, portanto, ouvir que os incidentes de *ransomware* estão aumentando.

As operações de *ransomware* continuam a se tornar mais criativas na monetização de seus esforços, especialmente com os surgimentos de esquemas de *ransomware* como serviço (RaaS). O potencial de lucro para os autores e operadores de *ransomware* também impulsiona a inovação rápida e a concorrência acirrada entre os cibercriminosos, com cada grupo oferecendo descontos para o uso de suas ferramentas.

No entanto, para as vítimas, a fonte do código malicioso utilizado não importa – se a organização está infectada com Petya ou PetrWrap. O resultado final é o mesmo: os dados são exfiltrados e os arquivos são criptografados ou corrompidos de tal forma que as operações críticas da organização não podem continuar.

Existem diversas atividades que as organizações podem seguir para reduzir significativamente o risco de serem vítimas de *ransomware*, em especial, seguir as melhores práticas de segurança cibernética para minimizar os danos do incidente cibernético, dentre elas:

- Realizar e testar os *backups* corporativos regularmente;
- Aplicar as atualizações de segurança quando disponíveis;
- Aplicar uma política de *zero-trust*; e
- Realizar o gerenciamento de contas privilegiadas.

Apesar dessas práticas recomendadas serem bastante conhecidas, muitas organizações ainda não realizam regularmente o *backup* de seus dados, e algumas organizações o fazem apenas dentro de suas próprias redes, o que significa que os *backups* podem ser comprometidos por um único ataque de *ransomware*.

A defesa eficaz contra *ransomware* depende, em última análise, da educação. Usuários e empresas devem reservar um tempo para aprender sobre suas melhores opções para *backups* automatizados de dados e atualizações de *software*. A educação sobre os sinais reveladores de táticas de distribuição de *ransomware*, como campanhas de *phishing* e *links* em *sites* comprometidos, deve ser uma prioridade máxima para qualquer pessoa que use um dispositivo conectado atualmente.

As organizações também devem implementar soluções de segurança que permitam proteção avançada contra ameaças, como soluções *antimalware* e ferramentas do tipo *Endpoint Detection and Response* (EDR), que monitoram atividades em *endpoints* e redes para identificar e mitigar ameaças. Essas soluções de segurança podem auxiliar a organização a detectar e mitigar os efeitos que um incidente *ransomware* pode ter sobre suas atividades.

**TLP:CLEAR**