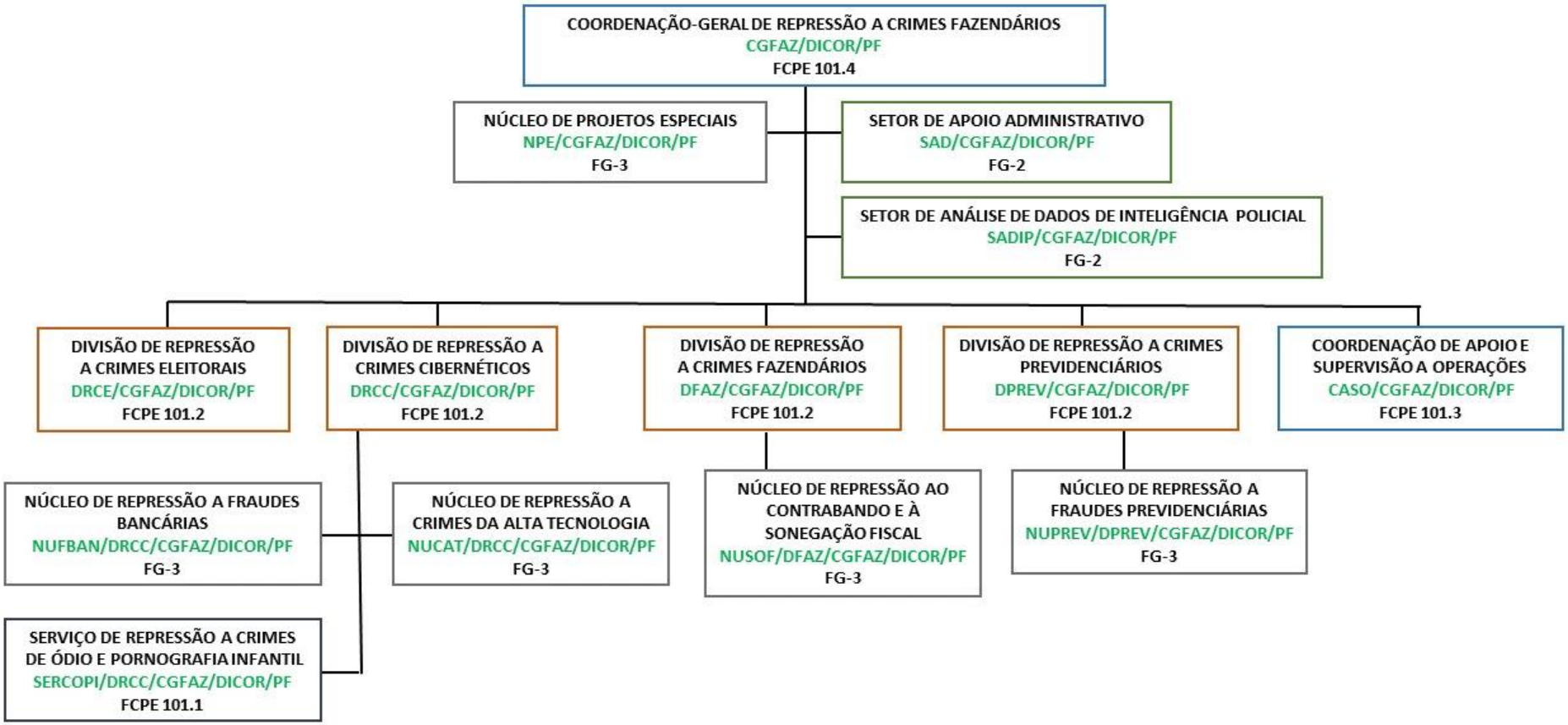
Investigação, Perícia e Respostas Cibernéticas

Escola Superior de Guerra – RJ 2022

Polícia Federal
DIVISÃO DE REPRESSÃO A CRIMES CIBERNÉTICOS

Introdução



COORDENAÇÃO-GERAL DE REPRESSÃO A CRIMES FAZENDÁRIOS – CGFAZ/DICOR/PF

DRCC

- Criada em 2003 e formalizada em 2011
- Atribuição de coordenação das ações de:
  - Combate às fraudes eletrônicas (NUFBAN 2011)
  - Combate aos crimes de Alta Tecnologia (NUCAT 2015)
  - Combate à crimes de ódio e abuso sexual infantil (SERCOPI)
    - Criada em 2003 e incorporada à DRCC em 2014
  - Unidade Especial de Investigação de Crimes Cibernéticos (UEICC)
    - Criada em 2022
    - Atuação em casos sensíveis e complexos
- **GRCC's nas unidades descentralizadas**

NUCAT/DRCC

Crimes de Alta Tecnologia

Prospecção de novas tecnologias

Capacitação

Crimes de Alta Tecnologia

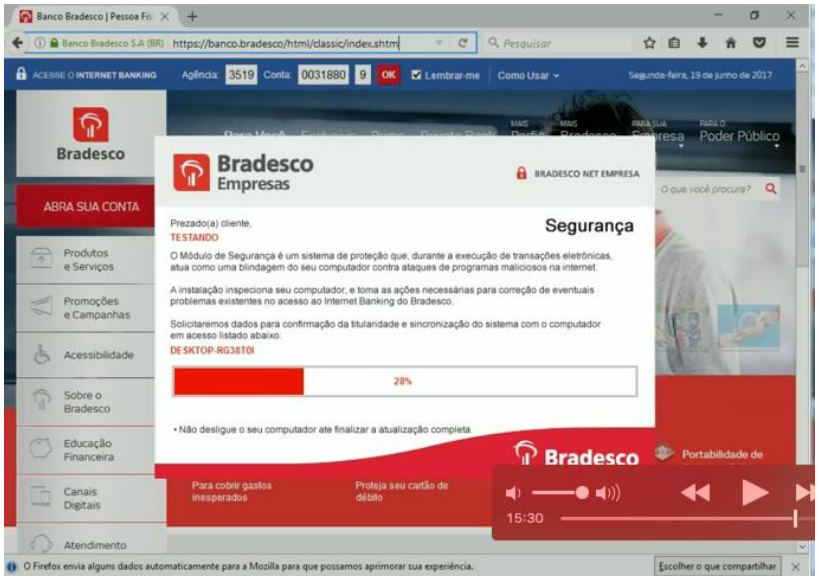
- Crimes cibernéticos que usam tecnologia eletrônica ou digital para atacar computadores ou redes de computadores (Europol)
- Crimes usando códigos maliciosos
  - Fraude bancária eletrônica (em conjunto com o NUFBAN)
  - *Ransomware*
- Crime de invasão de dispositivos e redes
- Ataques de negação de serviço (DDoS)
- Mineração Clandestina de Criptomoedas

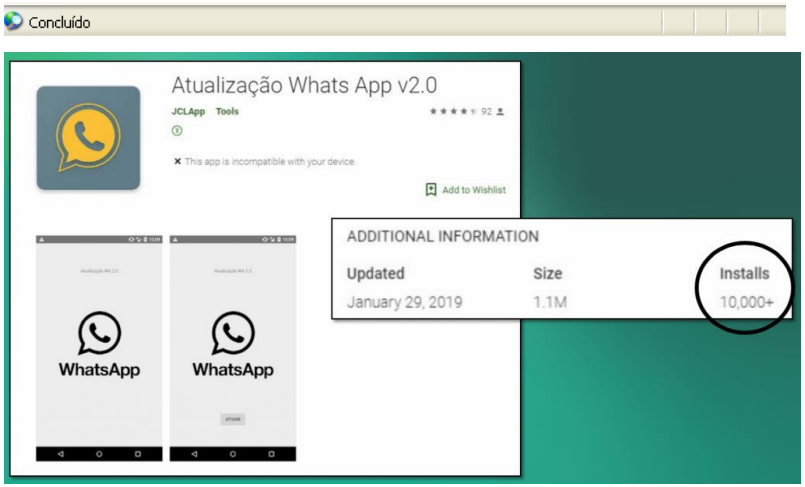
Crimes de Alta Tecnologia

- Fraude bancária usando *malware*
  - Diversas técnicas usadas desde 1998
    - *Keyloggers*
    - Captura de cliques de mouse (teclados virtuais)
    - Captura de segundo fator de autenticação (token, cartão "batalha naval", etc)
    - Contorno de soluções de segurança (Antivírus, plug-ins, etc.)
    - **RAT/KL REMOTA (Cadastro de computadores)**
    - **RAT em celulares**
    - **Smishing**
  - Ataques *"low tech"*
    - Desvio de cartões
    - Engenharia social (URA)
    - Boletos falsos

https://www.cbsi.net.br/2017/10/a-cidade-paraense-que-e-considerada-berco-dos-hackers-criminosos-do-brasil.html

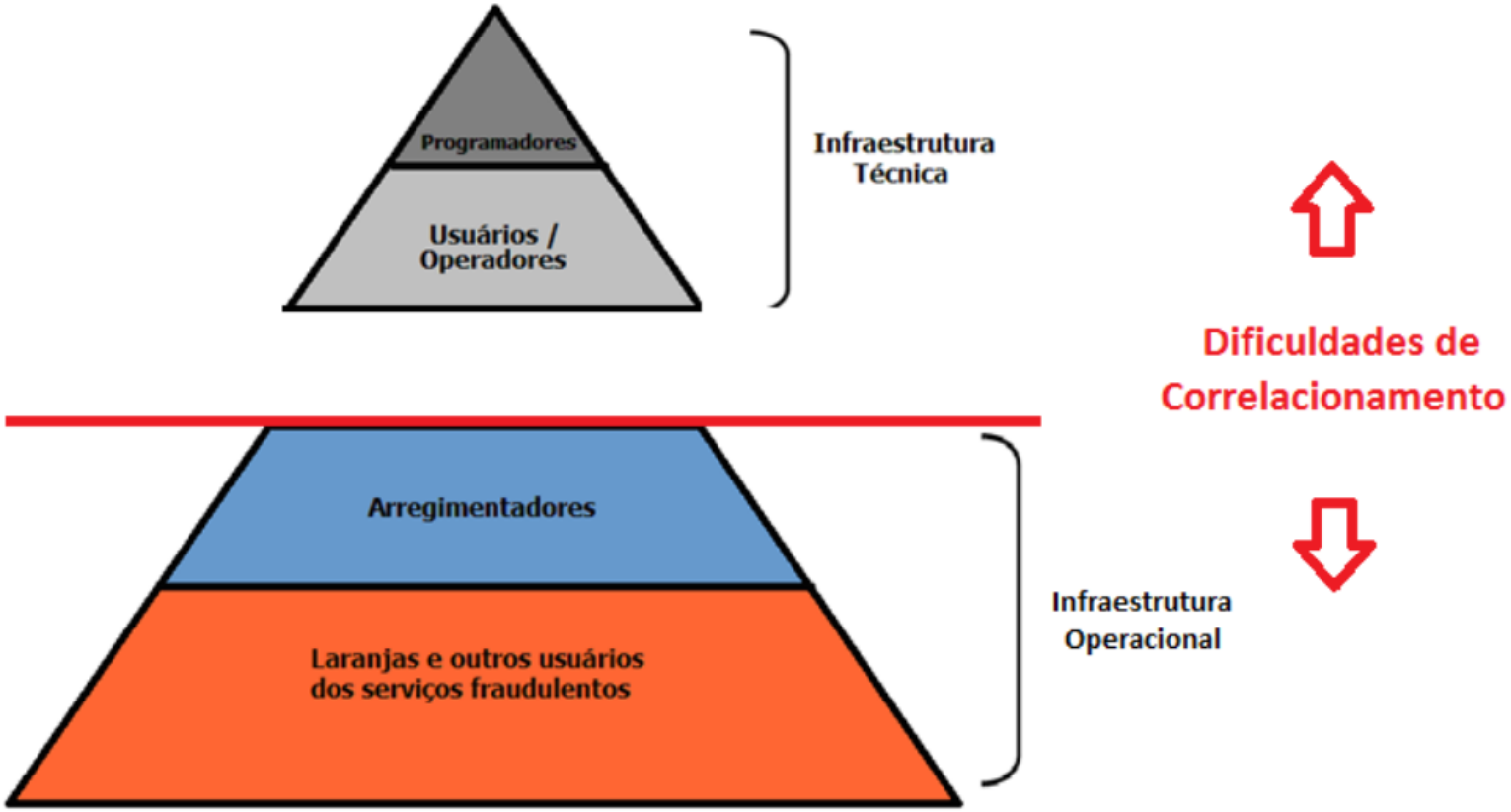
Fraude bancária usando *malware*





Fraude bancária eletrônica

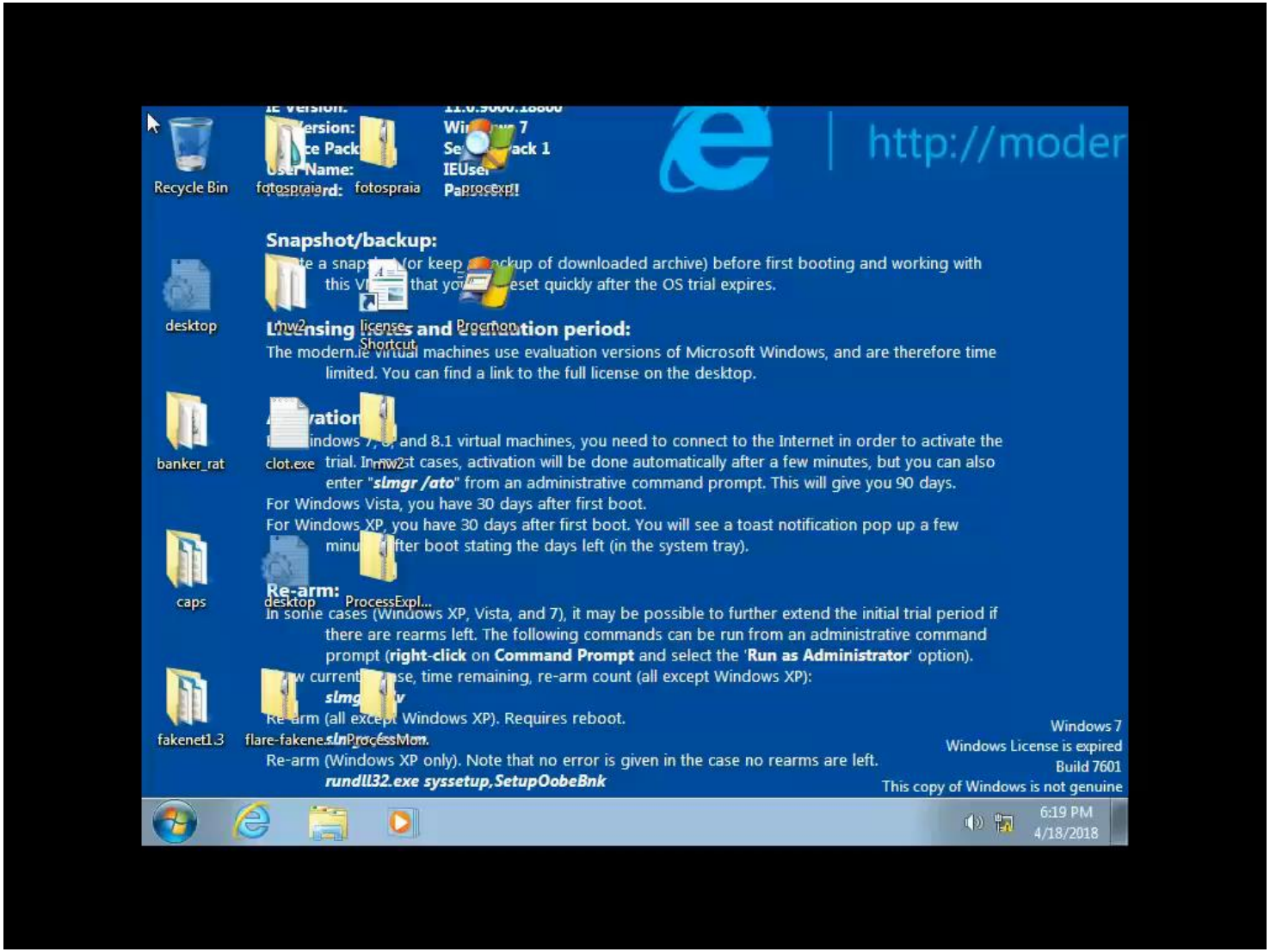
Fraude bancária eletrônica



Operação Código Reverso

- Iniciada a partir de uma fraude na CEF
  - Vítima aceitou fornecer o computador para análise
  - Encontrado código malicioso usado na fraude
  - Análise de *malware* apontou o destino do controle remoto
    - Operador da Fraude
  - Investigação apontou restante da quadrilha
    - Movimentação financeira
    - Interceptação telefônica e telemática
    - Busca e apreensão: Tocantins, São Paulo, Goiás e Pernambuco

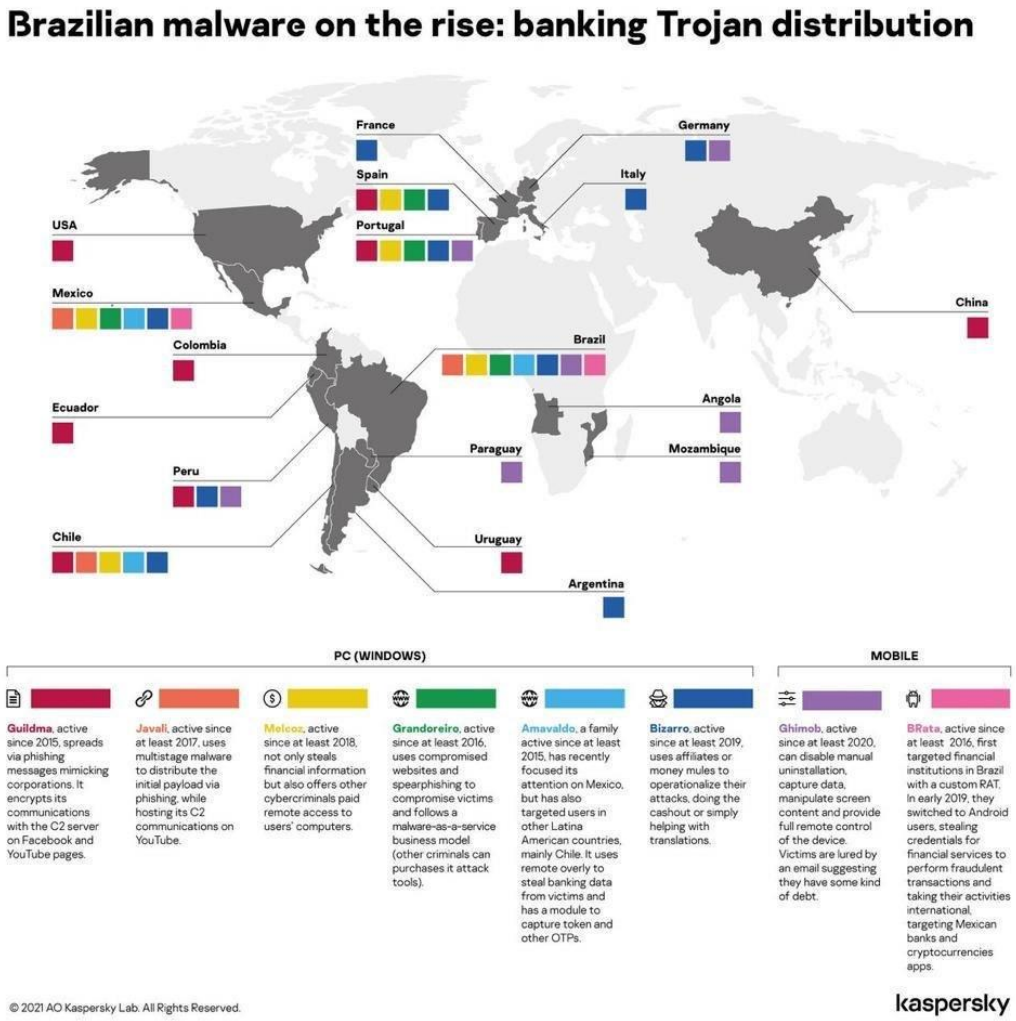
Operação Código Reverso



Malware bancário

- Aprendizados
  - Evidência no computador da vítima (C2)
    - Caminho até o operador da fraude
  - Criação de procedimento padrão na CEF
    - Coleta de artefatos mediante autorização
    - Análise e busca do C2
    - Correlação das fraudes via projeto tentáculos
  - Análise automatizada em lote de binários
    - Ferramenta customizada para *malware* bancário
    - Envio para ferramenta de correlação
  - Investigação em duas frentes – *malware* e fraudes
    - Cooperação entre NUFBAN e NUCAT

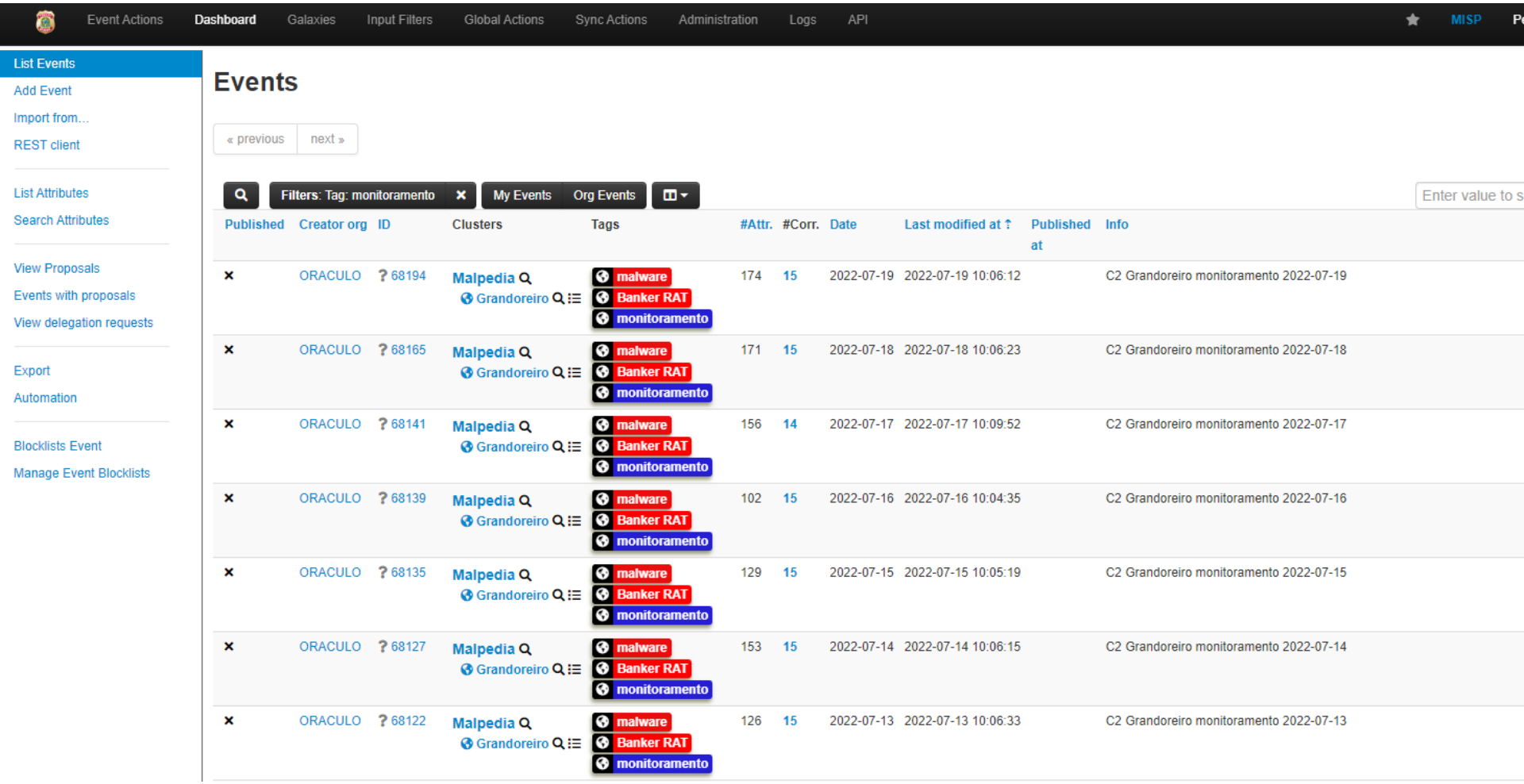
Famílias de malware bancário



Monitoramento de *malware*

- Campanhas de *malware*
  - Atuações diferentes de uma mesma família
  - Operadores diferentes
  - Infraestrutura de comando e controle (C2)
    - Monitoramento dos IP's
    - Engenharia reversa dos DGA (domain generaton algorithm)
- Famílias de malware
  - Classificação pelos antivírus
    - Conflitos de classificação
  - Malpedia como fonte de classificação
    - https://malpedia.caad.fkie.fraunhofer.de
    - Integrado ao MISP (Galaxies)
  - Regras YARA para classificação
- Base Nacional de Crimes Cibernéticos - BNCC

Monitoramento de *malware*



Invasão a sites públicos

- Motivações
  - Hacktivismo
    - *Defacement (*Zone-h*)*
    - Doxing
    - Vazamento de bancos de dados
  - **Acessos a bancos de dados da APF**
    - Ataque mais direcionado
    - Atores mais sofisticados
    - Comprometimento de credenciais
    - Acesso continuado
    - Ligação com fraudes (ex: carders)
  - Ação posterior (ex: *Ransomware*)
    - Comércio de acesso em fóruns

Invasão a sites públicos

- Hacktivismo

Invasão a sites públicos

- Invasores motivados
- Correlação de diferentes casos
  - Base Nacional de Crimes Cibernéticos
- Monitoramento de vazamentos e comércio de dados
  - Parceiros nacionais e internacionais
  - LGPD
- Apoio às unidades descentralizadas
  - Ex: uso de *big data*, *malware*, *dark web*.

Ransomware

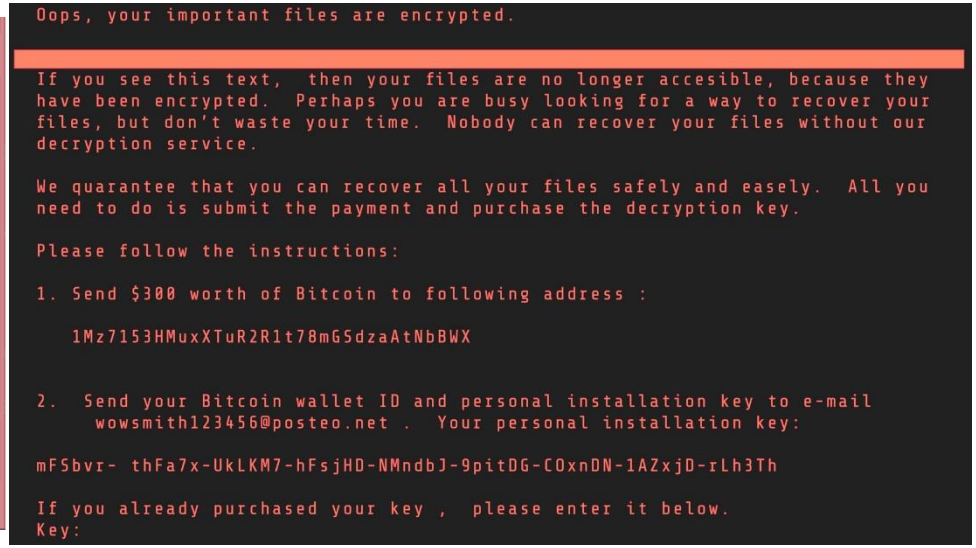
- Ataques de extorsão digital
- Invasão seguido de *malware*
- Evolução desde 1989:
  - 2010: Uso de criptografia assimétrica
  - 2016: Ransomware em massa – RaaS
  - 2017: Wannacry (ransomware + worm)
  - 2018-2019: Transporte, água, energia, saúde
  - 2020: Dupla extorsão (vazamento de dados)
  - Fonte: https://www.kaspersky.com.br/blog/history-of-ransomware/17280/
- Primeiro caso registrado na PF: 2013

Ransomware


PRESS ANY KEY!


You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a spec
key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three eas
steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need
help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://petya37h5tbhyvki.onion/QFg6S2
http://petya5koahtsf7sv.onion/QFg6S2
3. Enter your personal decryption code there:
85Q9MB-fQR2BE-ADiFHL-Tk6Bf9-8P2aSS-umQLcu-tgGTUV-hVogSi-oAd6RH-nkVWjm-
7zvEq8-WqBRUV-MHBVB2-5WN2Mi-c1aVrh
If you already purchased your key, please enter it below.
Key:

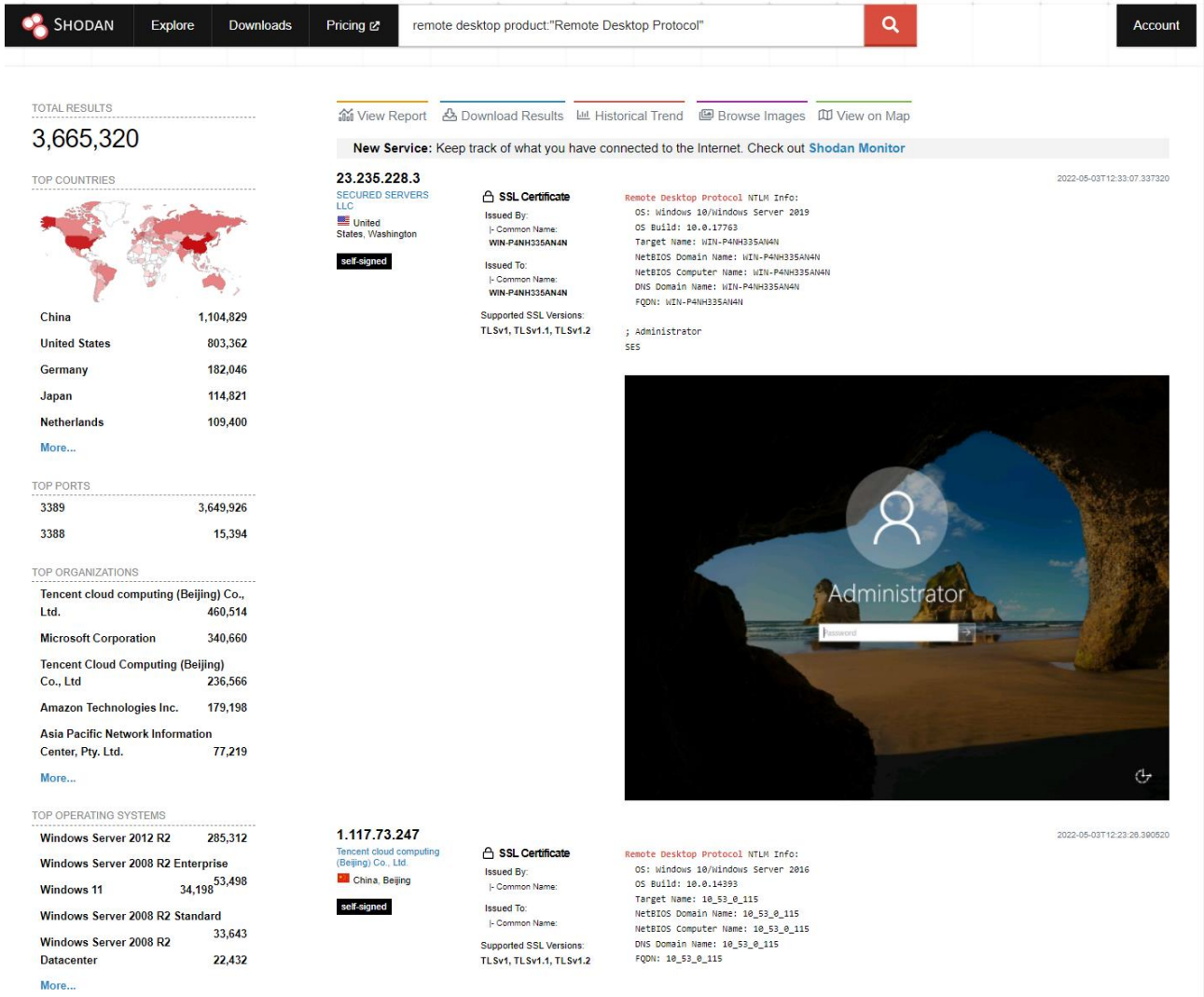

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Oops, your important files are encrypted.
If you see this text, then your files are no longer accesible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easely. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address :
1Mz7153HMuxXTuR2R1t78mG5dzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net . Your personal installation key:
mF5bvr- thFa7x-UkLKM7-hFsjHD-NMndbJ-9pitDG-COxnDN-1AZxjD-rLh3Th
If you already purchased your key , please enter it below.
Key:

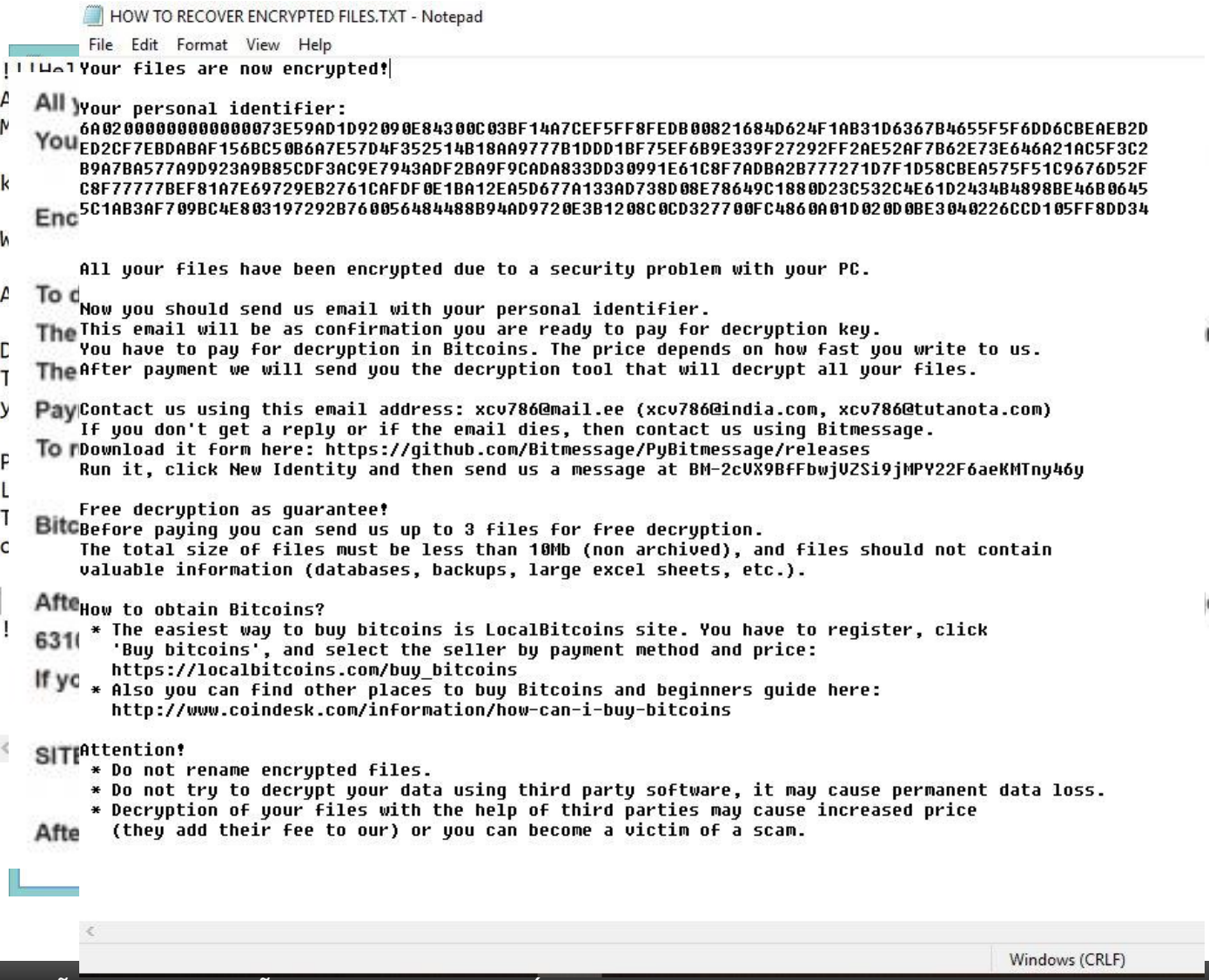
Ransomware

- Antes (até 2020) – ataques oportunistas
  - RDP aberto
  - Credenciais vazadas
  - Vítimas aleatórias
  - *Malware* genérico
    - Dados de contato idênticos
    - Dificuldade de investigação
  - Uso de redes de anonimização (VPN, Tor, etc)
  - Uso de contatos difíceis de rastrear (protonmail, tutanota, etc)
  - Uso de criptomoedas para pagamento
  - Cooperação internacional insuficiente

Ransomware


SHODAN
Explore
Downloads
Pricing
remote desktop product:"Remote Desktop Protocol"
Account
TOTAL RESULTS
3,665,320
TOP COUNTRIES
China 1,104,829
United States 803,362
Germany 182,046
Japan 114,821
Netherlands 109,400
More...
TOP PORTS
3389 3,649,926
3388 15,394
TOP ORGANIZATIONS
Tencent cloud computing (Beijing) Co., Ltd. 460,514
Microsoft Corporation 340,660
Tencent Cloud Computing (Beijing) Co., Ltd 236,566
Amazon Technologies Inc. 179,198
Asia Pacific Network Information Center, Pty. Ltd. 77,219
More...
TOP OPERATING SYSTEMS
Windows Server 2012 R2 285,312
Windows Server 2008 R2 Enterprise 53,498
Windows 11 34,198
Windows Server 2008 R2 Standard 33,643
Windows Server 2008 R2 Datacenter 22,432
More...
View Report
Download Results
Historical Trend
Browse Images
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
23.235.228.3
SECURED SERVERS LLC
United States, Washington
self-signed
SSL Certificate
Issued By:
|- Common Name:
WIN-P4NH335AN4N
Issued To:
|- Common Name:
WIN-P4NH335AN4N
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
2022-05-03T12:33:07.337320
Remote Desktop Protocol NTLM Info:
OS: Windows 10/Windows Server 2019
OS Build: 10.0.17763
Target Name: WIN-P4NH335AN4N
NetBIOS Domain Name: WIN-P4NH335AN4N
NetBIOS Computer Name: WIN-P4NH335AN4N
DNS Domain Name: WIN-P4NH335AN4N
FQDN: WIN-P4NH335AN4N
; Administrator
SES
Administrator
1.117.73.247
Tencent cloud computing (Beijing) Co., Ltd.
China, Beijing
self-signed
SSL Certificate
Issued By:
|- Common Name:
Issued To:
|- Common Name:
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
2022-05-03T12:23:26.390520
Remote Desktop Protocol NTLM Info:
OS: Windows 10/Windows Server 2016
OS Build: 10.0.14393
Target Name: 10_53_0_115
NetBIOS Domain Name: 10_53_0_115
NetBIOS Computer Name: 10_53_0_115
DNS Domain Name: 10_53_0_115
FQDN: 10_53_0_115

Ransomware


HOW TO RECOVER ENCRYPTED FILES.TXT - Notepad
File Edit Format View Help
Your files are now encrypted!
Your personal identifier:
6A02000000000000073E59AD1D92090E84300C03BF14A7CEF5FF8FEDB00821684D624F1AB31D6367B4655F5F6DD6CBEAEB2D
ED2CF7EBDABAF156BC50B6A7E57D4F352514B18AA9777B1DDD1BF75EF6B9E339F27292FF2AE52AF7B62E73E646A21AC5F3C2
B9A7BA577A9D923A9B85CDF3AC9E7943ADF2BA9F9CADA833DD30991E61C8F7ADBA2B777271D7F1D58CBEA575F51C9676D52F
C8F77777BEF81A7E69729EB2761CAFDF0E1BA12EA5D677A133AD738D08E78649C1880D23C532C4E61D2434B4898BE46B0645
5C1AB3AF709BC4E80319729 2B760056484488B94AD9720E3B1208C0CD327700FC4860A01D020D0BE3040226CCD105FF8DD34
All your files have been encrypted due to a security problem with your PC.
Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.
Contact us using this email address: xcv786@mail.ee (xcv786@india.com, xcv786@tutanota.com)
If you don't get a reply or if the email dies, then contact us using Bitmessage.
Download it form here: https://github.com/Bitmessage/PyBitmessage/releases
Run it, click New Identity and then send us a message at BM-2cVX9BfFbwjVZSi9jMPY22F6aeKMTny46y
Free decryption as guarantee!
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 10Mb (non archived), and files should not contain
valuable information (databases, backups, large excel sheets, etc.).
How to obtain Bitcoins?
* The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
'Buy bitcoins', and select the seller by payment method and price:
https://localbitcoins.com/buy_bitcoins
* Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price
(they add their fee to our) or you can become a victim of a scam.
Windows (CRLF)

Investigação cibernética

- Investigações de invasão/*ransomware*
  - Polícia dificilmente atua como *first responder*
    - Impossível prever *a priori* tudo que deve ser preservado
  - ETIR (Norma Complementar nº 05/IN01/DSIC/GSIPR) ou equipe de TI
  - Preservação de evidências (Norma Complementar nº 21/IN01/DSIC/GSIPR)
  - Comunicação para a autoridade competente
  - **Tempo como fator crucial de sucesso**
  - Evidências em disco
    - Logs, *malware*, arquivos cifrados
  - Evidências em memória
    - Requer preservação mais especializada
  - Ransomware por *atacado*
    - Mesmos dados de contato em vários ataques
    - Dificuldade de investigação (endereços já reportados e desativados)
    - Eventualmente há *decrypters* disponíveis (projeto No More Ransom)
  - Ransomware direcionado
    - Artefato e técnicas sofisticadas
    - Altos valores de resgate
    - Dupla extorsão

Investigação cibernética

- Local de crime diferenciado
  - Alta volatilidade dos vestígios
  - Necessidade de pronto atendimento – *first responder*
  - Equipe de Tratamento de Incidentes de Redes (ETIR)
  - Preservação de evidências x restauração do ambiente
  - Investigação x perícia x resposta
- Investigação diferenciada
  - Cooperação internacional
  - “Crime Global”

Investigação cibernética

- Perícia em ataques cibernéticos
  - Altamente dependente da preservação de evidências
  - Alta volatilidade dos vestígios
  - Prioridade na atuação
- Resposta a incidentes cibernéticos
  - Requer equipe dedicada e especializada
  - Conhecimento do ambiente afetado
  - Preservação de evidências – First Responder
  - Orientação na restauração do ambiente

Investigação cibernética

Investigação cibernética

- **Integração** investigação, perícia e resposta
  - Preservação de evidências
  - Cooperação e canal direto
  - Força-tarefa
  - Dinâmica do incidente importante para prevenir novos incidentes
  - Comunicação conjunta
  - Diligências antecipadas

ALERTA 19/2022

Campanha do Malware "Symbiote"

Publicado em 15/07/2022 16h59 | Atualizado em 19/07/2022 11h55

[TLP:WHITE]

1. Este Alerta foi confeccionado pelo Departamento de Polícia Federal (DPF) em parceria com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). O trabalho conjunto visa fornecer informações oportunas e indicar ações preventivas relativas à campanha massiva de ataques com o Malware Symbiote.

2. Foram encontrados indícios de uma campanha sofisticada com o objetivo de manter acesso remoto e coletar informações sensíveis em entes do setor financeiro e órgãos públicos do Brasil. O atacante usa um artefato bastante sofisticado (rootkit) que se esconde em computadores com o sistema operacional Linux e se comunica através de um canal encapsulado que se usa do protocolo de resolução de nomes da Internet (DNS).

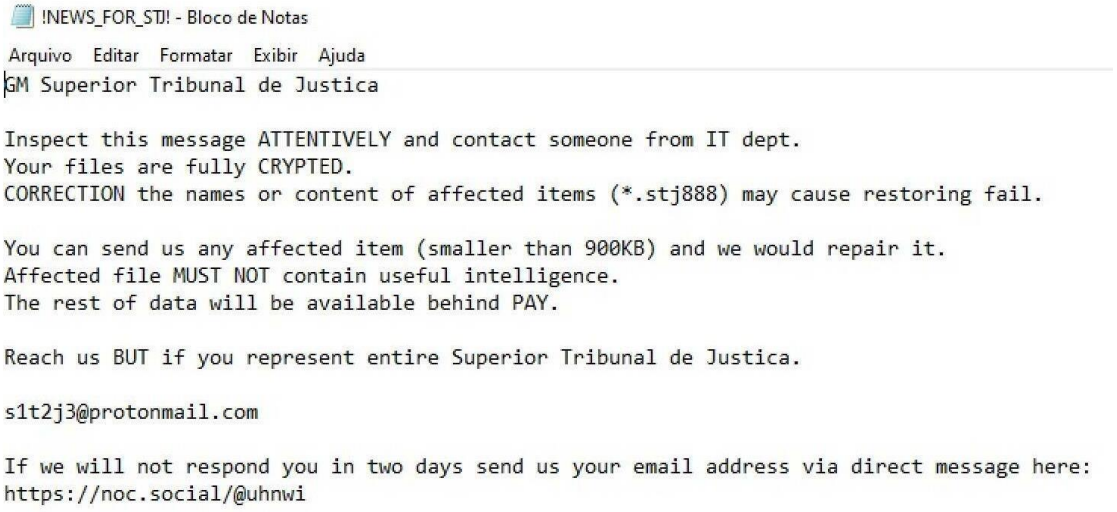
3. Não há informações claras de como o ataque se inicia, mas há suspeitas de que o atacante se valha de credenciais de acesso remoto válidas (VPN) e que explore uma vulnerabilidade chamada "Dirty COW" (CVE-2016-5195). Há indícios que a campanha foi efetivada entre outubro de 2021 e março de 2022.

4. O artefato permite ao atacante acessar servidores da rede com uma credencial própria (uma espécie de chave mestra). Permite ainda copiar informação sensível como usuários e senhas, documentos e outros dados da rede da vítima e enviar para o atacante usando o canal camuflado DNS. Há indícios ainda de que o atacante é capaz de escalar privilégios e obter acesso de administrador (root) no sistema afetado.

5. Sistemas vulneráveis: Linux (todas as versões e distribuições).

Ransomware

- Caso STJ – 3/11/2020
  - Divisor de águas
  - Ataque altamente sofisticado
    - Ultra high-net-worth individual (UHNWI)
    - Uso de ferramentas customizadas
    - Living off the land e persistência em memória
  - *Ransomware* personalizado
    - Sem dados de criptomoedas para transferência
    - Contato personalizado – s1t2j3@protonmail.com
  - Versão Linux / ESXi (cifragem das máquinas virtuais)


!NEWS_FOR_STJ! - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

GM Superior Tribunal de Justica

Inspect this message ATTENTIVELY and contact someone from IT dept.
Your files are fully CRYPTED.
CORRECTION the names or content of affected items (*.stj888) may cause restoring fail.

You can send us any affected item (smaller than 900KB) and we would repair it.
Affected file MUST NOT contain useful intelligence.
The rest of data will be available behind PAY.

Reach us BUT if you represent entire Superior Tribunal de Justica.

s1t2j3@protonmail.com

If we will not respond you in two days send us your email address via direct message here:
https://noc.social/@uhnwi

10 de novembro de 2020

Alerta Especial nº 07/2020
Nova campanha de ataques de Ransomware

Atualização: 11 de novembro de 2020 - 10:00

Por favor, entre em contato com o **CTIR Gov**, caso tenha alguma dúvida relacionada a esta publicação em sua Coordenação ou pelos

Ataques relacionados

- Ataque Embraer
  - Atendido pelo GRCC/SP com apoio do NUCAT/DRCC
  - Mesmo grupo (RansomExx)
  - Empresa privada prestou serviço de resposta incidentes
  - Coleta de *dumps* de memória
  - Análise do SETEC/SP
  - Evidências adicionais
    - *Pyxie* server
    - Artefato .NET (túnel *Socks*)
    - Propagador

Ataques relacionados

- Caso EIGSI (general engineering school in La Rochelle)
  - Dia anterior do caso STJ
  - Descoberto via *retrohunt* no VirusTotal
  - Acionada adidância na França
  - Empresa não cooperou com a investigação

```
%s/%s
!NEWS_FOR_EIGSI!.txt
.31gs1
Greetings EIGSI!!!
Study this message REGARDFULLY and call administrator from technical division.
Yours information is securely ENCRYPTED.
CHANGING content or names of crypted files (*.31gs1) can make recovering failure.
You can mail us one crypted document (not bigger than 700KB) and we would restore it.
Encrypted file MUST NOT have rich data.
All other data will be your behind the PAYMENT.
Reach us SOLELY if you represent all affected network.
france.eigs@protonmail.com
```

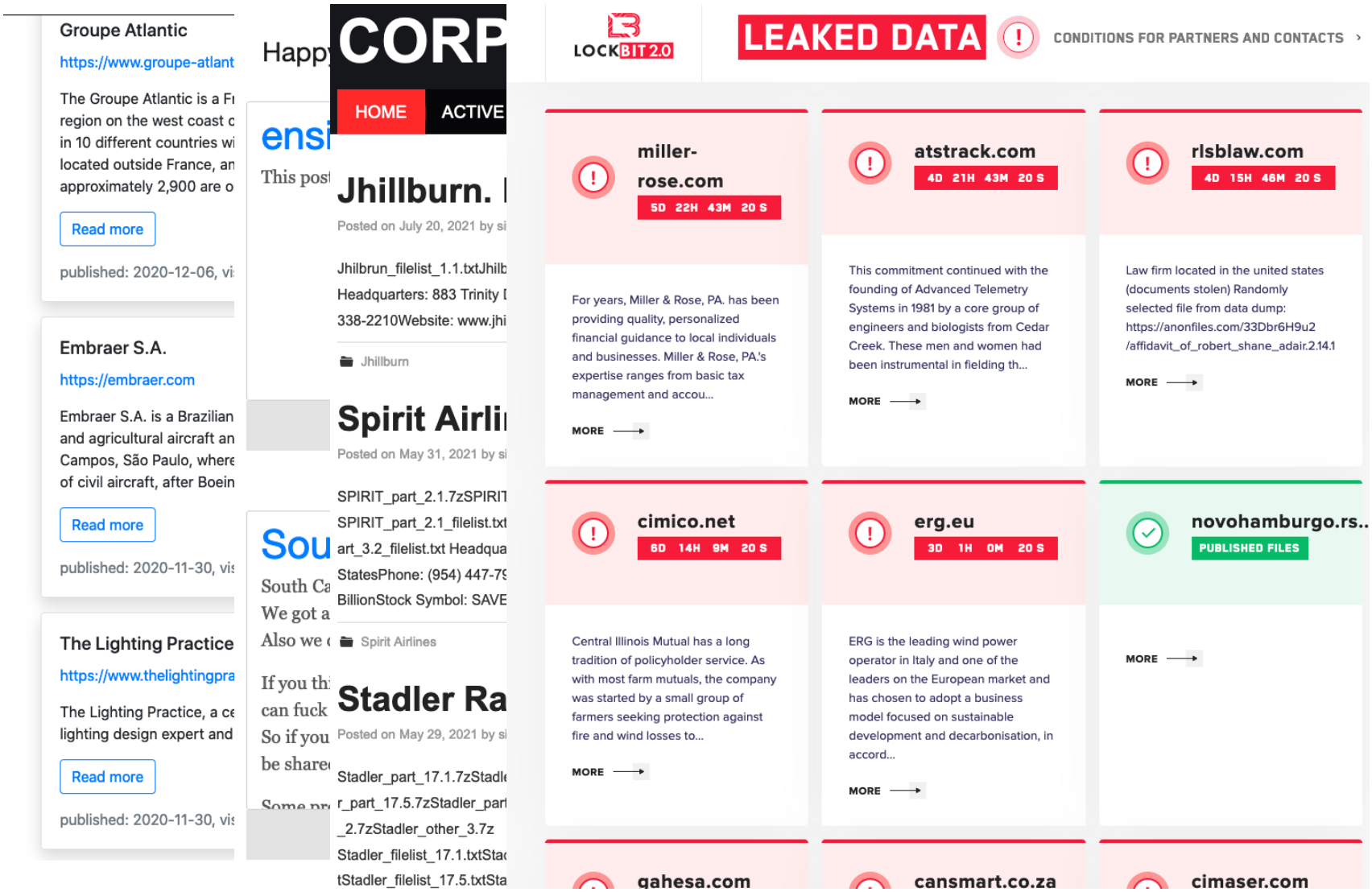
Aprendizados

- Modelo de força tarefa
- Agilidade na análise das evidências
- Cooperação nacional e internacional
  - Ataques não reportados para forças policiais
- Presença de ETIR capacitada melhora muito a preservação de evidências
- Evidências em memória são fundamentais
- Compartilhamento de informações fundamental para prevenir novos ataques

Ransomware

- Dupla extorsão
  - “Blogs” dark web com vazamento de dados
- Grupos
  - RansomExx
  - Lockbit
  - Nefilm
  - REvil
- Possibilidades
  - Ransomware para esconder outra ação?
  - Ataque interno? (RaaS)
- Cifragem incompleta (desempenho)
  - Ex: 8mb RansomExx, 4kb Lockbit 2.0 (https://threatpost.com/lockbit-ransomware-proliferates-globally/168746/)
- Proteção contra localidades específicas

Ransomware

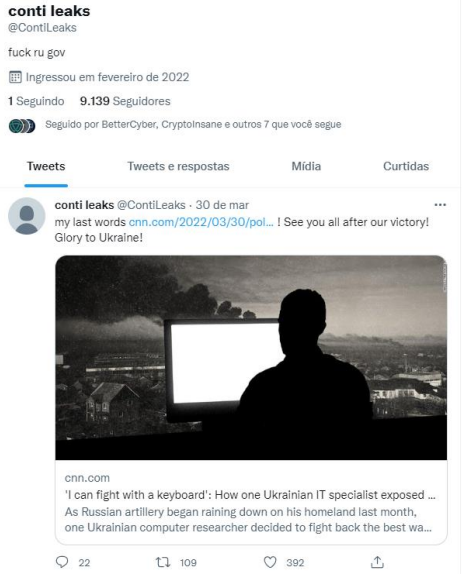

Groupe Atlantic
https://www.groupe-atlant
The Groupe Atlantic is a Fr
region on the west coast c
in 10 different countries wi
located outside France, an
approximately 2,900 are o
Read more
published: 2020-12-06, vi
Embraer S.A.
https://embraer.com
Embraer S.A. is a Brazilian
and agricultural aircraft an
Campos, São Paulo, where
of civil aircraft, after Boein
Read more
published: 2020-11-30, vis
The Lighting Practice
https://www.thelightingpra
The Lighting Practice, a ce
lighting design expert and
Read more
published: 2020-11-30, vis
CORP
HOME
ACTIVE
Jhillburn.
Posted on July 20, 2021 by si
Jhilbrun_filelist_1.1.txtJhilb
Headquarters: 883 Trinity
338-2210Website: www.jhi
Jhillburn
Spirit Airli
Posted on May 31, 2021 by si
SPIRIT_part_2.1.7zSPIRIT
SPIRIT_part_2.1_filelist.txt
art_3.2_filelist.txt Headqua
StatesPhone: (954) 447-79
BillionStock Symbol: SAVE
Spirit Airlines
Stadler Ra
Posted on May 29, 2021 by si
Stadler_part_17.1.7zStadle
r_part_17.5.7zStadler_part
_2.7zStadler_other_3.7z
Stadler_filelist_17.1.txtSta
tStadler_filelist_17.5.txtSta
LOCKBIT 2.0
LEAKED DATA
CONDITIONS FOR PARTNERS AND CONTACTS
miller-rose.com
5D 22H 43M 20 S
For years, Miller & Rose, PA. has been providing quality, personalized financial guidance to local individuals and businesses. Miller & Rose, PA.'s expertise ranges from basic tax management and accou...
MORE
atstrack.com
4D 21H 43M 20 S
This commitment continued with the founding of Advanced Telemetry Systems in 1981 by a core group of engineers and biologists from Cedar Creek. These men and women had been instrumental in fielding th...
MORE
rlsblaw.com
4D 15H 46M 20 S
Law firm located in the united states (documents stolen) Randomly selected file from data dump: https://anonfiles.com/33Dbr6H9u2 /affidavit_of_robert_shane_adair.2.14.1
MORE
cimico.net
6D 14H 9M 20 S
Central Illinois Mutual has a long tradition of policyholder service. As with most farm mutuals, the company was started by a small group of farmers seeking protection against fire and wind losses to...
MORE
erg.eu
3D 1H 0M 20 S
ERG is the leading wind power operator in Italy and one of the leaders on the European market and has chosen to adopt a business model focused on sustainable development and decarbonisation, in accord...
MORE
novohamburgo.rs..
PUBLISHED FILES
MORE
gahesa.com
cansmart.co.za
cimaser.com

Ransomware

- Desafios (investigação)
  - Redes de Anonomização
  - Cooperação nacional
  - Cooperação internacional
  - **Investigação mundial por grupo**
  - **Atuação conjunta perícia e investigação de forma célere**
  - **Parte não visível da estrutura criminosa**
- Prevenção
  - Backups off-line
  - Correção de vulnerabilidades conhecidas
  - Controle de acessos externos
  - MFA
  - Bloqueio na borda de redes de anonimização

Ransomware

- Estrutura criminosa
  - Initial Access Brokers
  - Data Exfiltration Brokers
  - Financial Handlers
  - Counter Anti-Virus Services (CAV Services)
  - Virtual Private Network Services (VPN services)
  - Anonymous communication platforms
- Conti Leaks
  - https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/
  - https://therecord.media/conti-leaks-the-panama-papers-of-ransomware/
  - https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/
  - https://www.forescout.com/resources/analysis-of-conti-leaks/



Ransomware

File name	File size	Date	Category	Description
Conti Chat Logs 2020.7z	2417273	01-03-22 2:46	Chats	Chats from June until November 2020
Conti Documentation Leak.7z	234714	01-03-22 5:29	Docs	Various documents such as technical guidelines and instructions for managers
Conti Internal Software Leak.7z	3911885	01-03-22 2:57	Tools	12 git repositories of internal software used by Conti
Conti Jabber Chat Logs 2021 - 2022.7z	1160294	02-03-22 13:10	Chats	Additional chats spanning 2021 and 2022
Conti Locker Leak.7z	6852466	05-03-22 4:29	Tools	The ransomware component used by Conti
Conti Pony Leak 2016.7z	62014991	01-03-22 2:51	Docs	Collection of credentials and certificates stolen from multiple organizations by the Pony malware
Conti Rocket Chat Leaks.7z	3370574	01-03-22 2:47	Chats	Chat logs
Conti Screenshots December 2021.7z	452894	01-03-22 2:46	Docs	Several screenshots of Cobalt strike toolkit used by Conti
Conti Toolkit Leak.7z	94186791	01-03-22 2:42	Tools	Source code of Chimaera.Ngrok and Chimaera.Sugarlogic toolkits. Also contains manuals for file-and-rank employees that have been leaked earlier last year.
Conti Trickbot Forum Leak.7z	8542211	01-03-22 2:50	Chats	Messages from the Trickbot forum.
Conti Trickbot Leaks.7z	955850	01-03-22 6:52	Tools	Two backend components written in Erlang for data dispatcher and collection
Training Material Leak (267-part zip file)	-	31-12-69 18:00	Docs	Educational text and video materials, as well as code examples.

Alias	Role
stern	Boss 1
tramp	Boss 2
hof	sysadmin, oversees botnets
zevs	sysadmin, oversees botnets
max	Alla Witte, the Trickbot developer
revers	Hacker, manager
professor	Negotiates ransom with companies, creates darknet blogs
Hors	Sysadmin
Bentley	Sysadmin
Swift	hacker
Buza	Developers' teamlead / OSINT research
pumba	Negotiates ransom with companies, creates darknet blogs
bio	Negotiates ransom with companies, creates darknet blogs
skippy	HR / Legal
many	works on cryptolocker, decrypts data for victims
starfall	Sysadmin
reshaev	top hacker
Salamandra	HR
kagas	HR
viper	HR
elvira	HR
ford	HR
jaime	Developer
mango	technical manager, QA, side projects (blockhain, hackers' social network)
cybergangster	works on cryptolocker, decrypts data for victims
dollar	Hacker, works as intermediary between the group and the victims
pin	works on cryptolocker, decrypts data for victims
paranoik	works on cryptolocker, decrypts data for victims

Ransomware

Necessidade de junção de evidências do ataque com inteligência cibernética

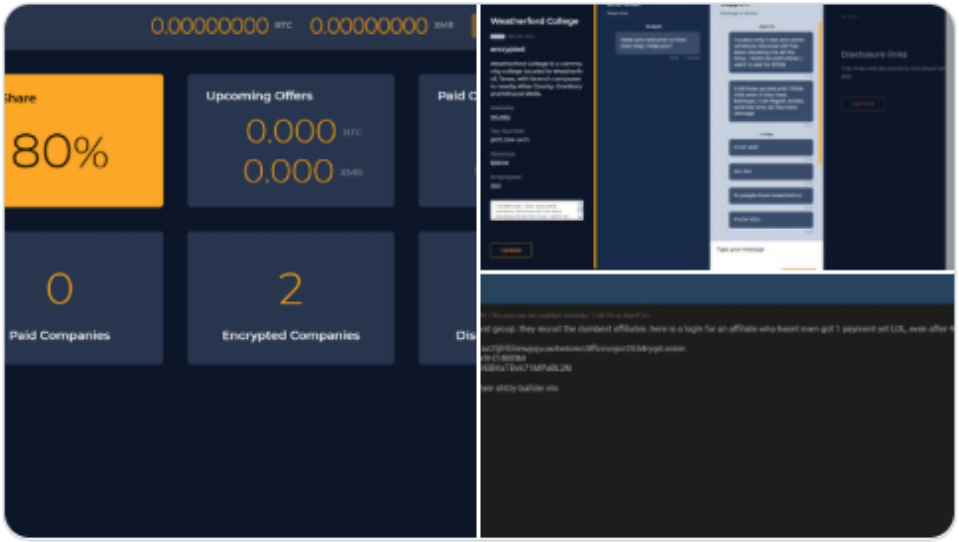
OSINT
Rastreamento de Criptomoedas
Dark Web
Fóruns de compra e venda de produtos criminosos

Ransomware

vx-underground
@vxunderground

Yesterday an individual on Breached, the successor to the infamous RaidForums, proclaimed their disdain for HIVE ransomware group and leaked login credentials for an affiliate in HIVE.

Traduzir Tweet



10:47 AM · 5 de mai de 2022 · Twitter Web App

64 Retweets **2** Tweets com comentário **219** Curtidas

Iniciativas Polícia Federal (DRCC)

- Entrada no projeto “no more ransom”
  - Europol, Polícia Holanda, Kaspersky e Mcafee
  - Mais de 100 instituições participantes (polícias, CSIRTS e empresas de segurança)
  - Maior iniciativa do gênero conhecida
- Participação na *International Counter-Ransomwrare Initiative* (CRI)
  - Captaneada pelos EUA
  - Brasil no grupo Disruption (Australia)
- Parcerias nacionais e internacionais
  - Europol, Interpol, FBI, entre outras
- Inciativa de bloqueio de redes anônimas
  - Tratativas com SERPRO e outras entidades

Novas Tecnologias

- Base Nacional de Crimes Cibernéticos
  - Base de indicadores cibernéticos
  - Organização da inteligência cibernética interna
    - Laudos periciais
    - Relatórios de investigação
    - Relatórios de inteligência
- Cybertools
  - Ferramenta de consulta de informações na Internet
    - Whois/RDAP
    - GeoIP
    - Protonmail
    - Passive DNS
- LUNES
  - Ferramenta de consulta de chats de casos passados
  - Em desenvolvimento
  - Integrante do projeto P.A.T.R.I.A Digital

Capacitação

- Curso básico de crimes cibernéticos – EAD (DRCC)
- Disciplina crimes cibernéticos ANP (DRCC)
- Curso básico de malware (NUCAT)
- AMB – Análise de Malware Básico EAD
  - Em desenvolvimento
  - Parceria com a Perícia de Informática
- Curso avançado de malware
  - Previsto para 2022
- Curso de investigação de crimes de alta tecnologia
  - Previsto para 2022

Conclusões

- Crimes cibernéticos em expansão
  - Brasil exportando tecnologia criminosa
  - Necessidade de aumentar a capacidade de resposta
- Ataques cada vez mais sofisticados (APT)
  - **Ação global** empresas + justiça
  - Ataques em cadeia de suprimento
- **Tempo de resposta é um fator crucial de sucesso**
  - Modelo de investigação/perícia integrado e mais eficiente
- **Integração** nacional e internacional

Obrigado

Ivo de Carvalho Peixinho
Perito Criminal Federal

E-mail: peixinho.icp@pf.gov.br