

NOTA TÉCNICA

Cliente: Fundação Nacional de Saúde - FUNASA

Assunto: Comparativo entre os filtros de spam InterScan Messaing Security Virtual Appliance - TREND Micro, Fortimail da Fortigate e ProofPoint.

INTERESSADO: COINT/CGMTI/DEADM

1. Introdução

O documento apresentado tem como objetivo demonstrar um comparativo entre os filtros de spam InterScan Messaing Security Virtual Appliance - TREND Micro, Fortimail da Fortigate e ProofPoint em prova de conceito - POC solicitada pela FUNASA.

2. Descrição dos filtros de spam e comportamento das ferramentas dentro do ambiente da Funasa

2.1. A ferramenta **InterScan Messaing Security Virtual Appliance** utilizada na POC está na versão “9.1.0.2025”, utilizando o sistema operacional 2.6.32, foi executado em modo virtualizado.

2.2. **Fortimail** utilizado na POC está na versão 7.0.1 e também foi executado em modo virtualizado.

2.3. **Proofpoint** utilizado na POC está na versão 8.18.4 e está sendo executado em modo virtualizado.

As ferramentas, possuem funções de detecção e bloqueio de spam, de anti-malware, de antivírus, proteção contra perda de dados, detecção de ameaças, Sandboxing, portal de gerenciamento centralizado entre outras.

As referidas ferramentas, também possibilitam criar regras customizadas, restauração de mensagens em quarentena e executam atualizações diárias de definições associadas a antispam e antivírus em suas respectivas bases de conhecimento.

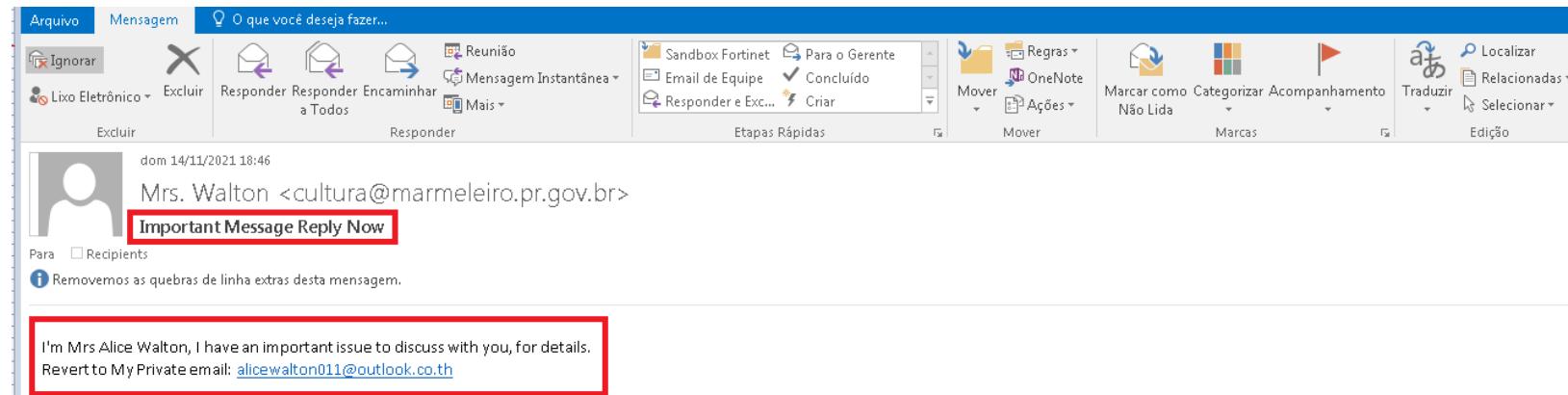
Suas definições de spam, vírus e malware são atualizadas diariamente na base de conhecimento do fabricante das respectivas ferramentas visando a eliminação de novas ameaças associadas a mensagens eletrônicas.

3. Análise de Logs de detecção de mensagem SPAM nas ferramentas do InterScan Messaing Security Virtual Appliance e do Fortimail à época e no Proofpoint a partir de março de 2022.

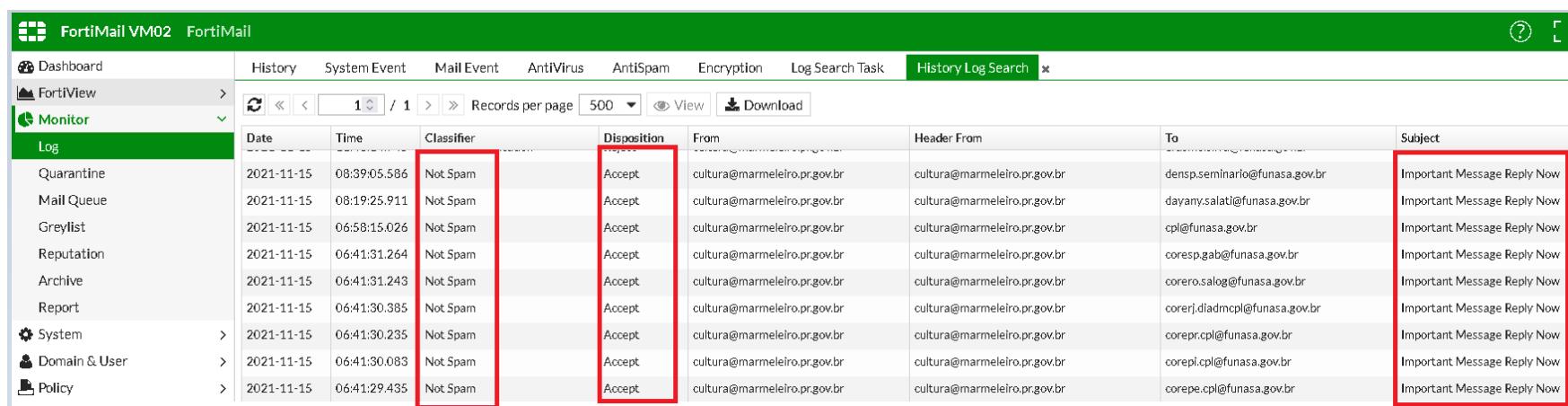
3.1. Análise de Logs associados às ferramentas InterScan Messaing Security Virtual Appliance e do Fortimail.

1º - Exemplo:

3.2. Mensagem de spam com o assunto “Important Message Reply Now” enviada para vários destinatários da FUNASA.



3.3. Log do Fortimail no qual a mensagem é aceita e categorizada como limpa (Not Spam).



Date	Time	Classifier	Disposition	From	Header From	To	Subject
2021-11-15	08:39:05.586	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	densp.seminario@funasa.gov.br	Important Message Reply Now
2021-11-15	08:19:25.911	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	dayany.salati@funasa.gov.br	Important Message Reply Now
2021-11-15	06:58:15.026	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	cpl@funasa.gov.br	Important Message Reply Now
2021-11-15	06:41:31.264	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	coresp.gab@funasa.gov.br	Important Message Reply Now
2021-11-15	06:41:31.243	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	corero.salog@funasa.gov.br	Important Message Reply Now
2021-11-15	06:41:30.385	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	corerj.diadmcp@funasa.gov.br	Important Message Reply Now
2021-11-15	06:41:30.235	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	corepr.cpl@funasa.gov.br	Important Message Reply Now
2021-11-15	06:41:30.083	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	corepi.cpl@funasa.gov.br	Important Message Reply Now
2021-11-15	06:41:29.435	Not Spam	Accept	cultura@marmeiro.pr.gov.br	cultura@marmeiro.pr.gov.br	corepe.cpl@funasa.gov.br	Important Message Reply Now

3.3. Mensagens detectadas/bloqueadas como spam e adicionadas à quarentena no InterScan Messaging Security Virtual Appliance.

Type: Message tracking | IMSVA data only

Dates: 11/01/2021 14:41 to 11/16/2021 15:41
mm/dd/yyyy hh mm mm/dd/yyyy hh mm

Subject: *Important Message Reply Now*

Message ID:

Sender:

Recipient:

Attachment(s):

Use semi-colons to separate multiple search items in Recipient and Attachment fields

Type any keyword to specify an exact match. Use an asterisk "*" for a partial match. For example, specifying "*username" searches for any character string that ends with "username".

Display Log

Message Tracking					Results per page: 15
				1-15 of 23	
Timestamp	Sender	Recipient(s)	Subject	Last Policy Action	
15 de Novembro de 2021 18:11:06	cultura@marmeleiro.prg.ov.br	ivan.cunha@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 08:37:31	cultura@marmeleiro.prg.ov.br	densp.seminario@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 08:17:51	cultura@marmeleiro.prg.ov.br	dayany.salati@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:56:40	cultura@marmeleiro.prg.ov.br	cpl@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:56	cultura@marmeleiro.prg.ov.br	corero.salog@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:56	cultura@marmeleiro.prg.ov.br	coresp.gab@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:55	cultura@marmeleiro.prg.ov.br	corenj.diadmcpl@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:55	cultura@marmeleiro.prg.ov.br	corepr.cpl@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:55	cultura@marmeleiro.prg.ov.br	corepi.cpl@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:54	cultura@marmeleiro.prg.ov.br	corepa.gab@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:54	cultura@marmeleiro.prg.ov.br	corepe.cpl@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>
15 de Novembro de 2021 06:39:52	cultura@marmeleiro.prg.ov.br	coremt.cpl@funasa.gov.br	Important Message Reply Now		<u>Quarantined</u>

2º Exemplo:

3.4. Mensagem spam com o assunto “LEMBRETE: Informação importante” enviada para vários destinatários da FUNASA.

Administrador de Webmail <administrador@fb2bk.site>

LEMBRETE: Informação importante (virginia.borges@funasa.gov.br)

Para : virginia.borges@funasa.gov.br

Prezado(a) Senhor(a),

No momento, estamos melhorando nosso centro de webmail devido ao congestionamento. Estamos excluindo todas as contas de webmail não utilizadas e criando mais espaço para novas contas.

Para garantir que não haja interrupção do serviço durante este período, você precisará fornecer as informações abaixo:

1. E-MAIL: virginia.borges@funasa.gov.br
2. SENHA:
3. CONFIRME A SENHA:
4. NÚMERO DE TELEFONE:

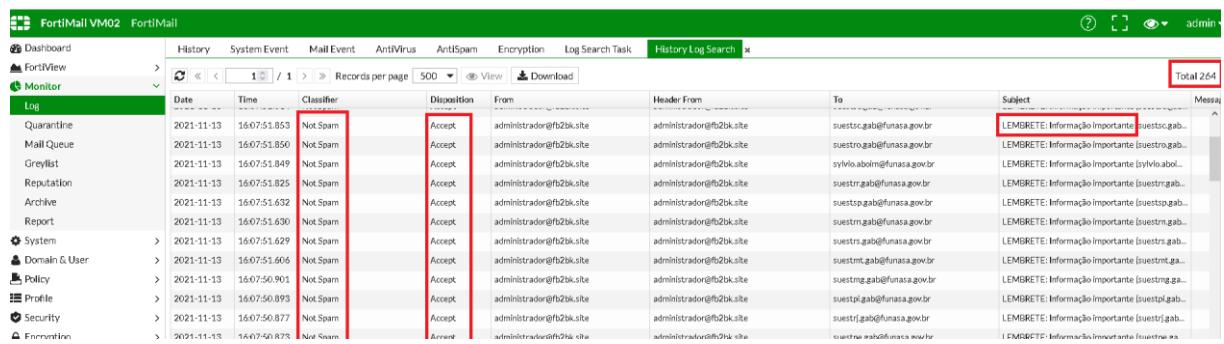
Responda a esta mensagem para que possamos oferecer melhores serviços online com melhorias em nossa funcionalidade de webmail.

Desculpe por qualquer inconveniente que isso possa causar a você.

Obrigada,

Administrador de Webmail.

3.5. Log do Fortimail no qual a mensagem é aceita e categorizada como limpa (Not Spam).



Date	Time	Classifier	Disposition	From	Header From	To	Subject	Message
2021-11-13	16:07:51.853	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestr.gab@funasa.gov.br	LEMBRETE: Informação importante (suestr.gab...	
2021-11-13	16:07:51.856	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestro.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestro.gab...	
2021-11-13	16:07:51.849	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	syvio.abolim@funasa.gov.br	LEMBRETE: Informação Importante (syvio.abol...	
2021-11-13	16:07:51.826	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestr.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestr.gab...	
2021-11-13	16:07:51.632	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestro.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestro.gab...	
2021-11-13	16:07:51.630	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestm.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestm.gab...	
2021-11-13	16:07:51.629	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestr.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestr.gab...	
2021-11-13	16:07:51.603	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestmt.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestmt.gab...	
2021-11-13	16:07:50.901	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestng.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestng.gab...	
2021-11-13	16:07:50.893	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestpl.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestpl.gab...	
2021-11-13	16:07:50.877	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestri.gab@funasa.gov.br	LEMBRETE: Informação Importante (suestri.gab...	
2021-11-13	16:07:50.878	Not Spam	Accept	administrator@fb2bk.site	administrator@fb2bk.site	suestre.gab@funasa.gov.br	I RMS&CTE: Informação Importante (suestre.gab...	

3.6. Mensagens detectadas/bloqueadas como spam e adicionadas à quarentena no InterScan Messaging Security Virtual Appliance.

TREND MICRO | InterScan™ Messaging Security Virtual Appliance

Mail Areas & Queues Management

Quarantine Archive Postpone MTA Virtual Analyzer

Criteria

Search: Any quarantine Any reason All Products

Dates: 11/01/2021 14:43 to 11/16/2021 15:43

Sender: Subject: *LEMBORETE: Informação importante*

Recipient(s): Violating Attachment(s):

Rule: Message ID:

Display Log

All 264 record(s) Deliver Reprocess Delete 1-15 of 264 Page 1

Result as of 16 de Novembro de 2021 15:53:02

Timestamp	Sender	Recipient(s)	Subject	Reason
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	telvio.mello@funasa.gov.br	LEMBORETE: Informação importante (telvio.mello@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	walterjanuzzi@funasa.gov.br	LEMBORETE: Informação importante (walterjanuzzi@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	virginia.borges@funasa.gov.br	LEMBORETE: Informação importante (virginia.borges@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	wenderson.monteiro@funasa.gov.br	LEMBORETE: Informação importante (wenderson.monteiro@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	weibson.gomes@funasa.gov.br	LEMBORETE: Informação importante (weibson.gomes@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	vinicius.correa@funasa.gov.br	LEMBORETE: Informação importante (vinicius.correa@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	waldoilson.leite@funasa.gov.br	LEMBORETE: Informação importante (waldoilson.leite@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	vanessa.zanganelli@funasa.gov.br	LEMBORETE: Informação importante (vanessa.zanganelli@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	suestto.gab@funasa.gov.br	LEMBORETE: Informação importante (suestto.gab@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:20	administrador@fb2.bk.site	sylvio.aboin@funasa.gov.br	LEMBORETE: Informação importante (sylvio.aboin@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:19	administrador@fb2.bk.site	suestrs.gab@funasa.gov.br	LEMBORETE: Informação importante (suestrs.gab@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:19	administrador@fb2.bk.site	suestro.gab@funasa.gov.br	LEMBORETE: Informação importante (suestro.gab@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:19	administrador@fb2.bk.site	suestse.gab@funasa.gov.br	LEMBORETE: Informação importante (suestse.gab@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:19	administrador@fb2.bk.site	suestsc.gab@funasa.gov.br	LEMBORETE: Informação importante (suestsc.gab@funasa.gov.br)	Spam/Phish
13 de Novembro de 2021 16:06:19	administrador@fb2.bk.site	suestsp.gab@funasa.gov.br	LEMBORETE: Informação importante (suestsp.gab@funasa.gov.br)	Spam/Phish

Disponível: 15 por página

3º Exemplo:

3.7. Mensagem spam com o assunto “Ela HUMILHOU o “azulzinho” na cama” enviada para vários destinatários da FUNASA.

sáb 13/11/2021 08:14

Jolivi < contato@mail1.jolivi.com.br>

Ela HUMILHOU o "azulzinho" na cama

ra wellington.santos29@gmail.com

Se houver problemas com o modo de exibição desta mensagem, clique aqui para exibi-la em um navegador da Web.
Clique aqui para baixar imagens. Para ajudar a proteger sua privacidade, o Outlook impedi o download automático de algumas imagens desta mensagem.

A RAIZ QUE PODE TE TORNAR UM GUERREIRO (NA CAMA)

Diz a lenda que, no ano de 1.200, o imperador Inca introduziu na dieta do seu exército uma estranha raiz nativa do Peru.

A intenção dele era que as propriedades energéticas dessa raiz dessem mais disposição aos soldados, durante as batalhas...

Bem, o objetivo foi alcançado: os guerreiros começaram a vencer mais combates. Mas notaram um curioso efeito colateral...

Um aumento descontrolado no apetite sexual.

E foi assim que os benefícios da **Maca Peruana** ficaram conhecidos mundialmente...

E que a Maca Peruana ganhou os justos apelidos de "**Raiz do Guerreiro**" e "**Azulzinho Natural**".

3.8. Log do Fortimail no qual a mensagem é aceita e categorizada como limpa (Not Spam).

FortiMail VM02 - FortiMail										
Dashboard		History	System Event	Mail Event	AntiVirus	AntiSpam	Encryption	Log Search Task		
FortView		History Log Search								
Monitor										
Log		Date	Time	Classifier	Disposition	From	Header From	To	Subject	Message
Quarantine		2021-11-13	08:17:21.299	Not Spam	Accept	bounce-27.HTML-18919618-166771...	contato@mail1.jolivi.com.br	marcos.oliveira@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	808
Mail Queue		2021-11-13	08:17:15.728	Not Spam	Accept	bounce-27.HTML-18954750-166771...	contato@mail1.jolivi.com.br	edmilson.t.silva@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	48d
Greylist		2021-11-13	08:16:26.195	Not Spam	Accept	bounce-27.HTML-17574394-166771...	contato@mail1.jolivi.com.br	labeled.lopes@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	16d
Reputation		2021-11-13	08:16:09.965	Not Spam	Accept	bounce-27.HTML-17299729-166771...	contato@mail1.jolivi.com.br	rosangela.coe@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	59d
Archive		2021-11-13	08:14:52.225	Not Spam	Accept	bounce-27.HTML-14335260-166771...	contato@mail1.jolivi.com.br	maria.mendonca@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	20d
Report		2021-11-13	08:14:06.358	Not Spam	Accept	bounce-27.HTML-13336254-166771...	contato@mail1.jolivi.com.br	maria.custodio@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	60d
System		2021-11-13	08:14:19.4R3	Not Spam	Accept	bounce-27.HTML-13159465-166771...	contato@mail1.jolivi.com.br	larkicon.luanadifunasa@whe...	Ela HUMILHOU o "azulzinho" na cama	afif

3.9. Mensagens detectadas/bloqueadas como spam e adicionadas à quarentena no InterScan Messaging Security Virtual Appliance.

TREND MICRO | InterScan™ Messaging Security Virtual Appliance

Mail Areas & Queues Management

Quarantine **Archive** **Postpone** **MTA** **Virtual Analyzer**

Criteria

Search: Any quarantine **Any reason** All Products

Dates: 11/01/2021 14:43 to 11/16/2021 15:43

Sender: *Ela HUMILHOU o "azulzinho" na cama*

Recipient(s): Violating Attachment(s):

Rule: Message ID:

Display Log

All 57 record(s) **Deliver** **Reprocess** **Delete** 1-15 of 57 Page 1

Result as of 16 de Novembro de 2021 16:04:59

Timestamp	Sender	Recipient(s)	Subject	Reason
<u>13 de Novembro de 2021 09:26:01</u>	wellington.santos+29+caf_=wellington.santos@funasa.gov.br@gmail.com	wellington.santos@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish
<u>13 de Novembro de 2021 08:20:07</u>	bounce-27_HTML-22612099-1667716-7235788-11110@bounce.mail1.jolivi.com.br	antonio.veras@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish
<u>13 de Novembro de 2021 08:19:42</u>	bounce-27_HTML-21904969-1667716-7235788-30181@bounce.mail1.jolivi.com.br	carlos.martins@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish
<u>13 de Novembro de 2021 08:17:26</u>	bounce-27_HTML-19760293-1667716-7235788-27102@bounce.mail1.jolivi.com.br	julio.ferreira@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish
<u>13 de Novembro de 2021 08:17:26</u>	bounce-27_HTML-19774566-1667716-7235788-17124@bounce.mail1.jolivi.com.br	irlene.freitas@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish
<u>13 de Novembro de 2021 08:17:19</u>	bounce-27_HTML-19505691-1667716-7235788-81418@bounce.mail1.jolivi.com.br	benedicto.santos@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish
<u>13 de Novembro de 2021 08:16:47</u>	bounce-27_HTML-19288714-1667716-7235788-31088@bounce.mail1.jolivi.com.br	orlando.faria@funasa.gov.br	Ela HUMILHOU o "azulzinho" na cama	Spam/Phish

3.10. Análise de Logs associados à ferramenta da Proofpoint.

3.10.1. Em março de 2022 foram iniciadas as configurações para que o tráfego externo encaminhado à FUNASA e filtrado pelas ferramentas de spam da FORTIMAIL e, posteriormente pela da Trend, fosse analisado pela ferramenta da Proofpoint.

3.10.2. Após a análise dos dados, a heurística e controles do Proofpoint detectaram o *phishing* que não foi detectado pela heurística e controles das aplicações da FORTIMAIL e TREND, conforme descrito abaixo.

3.10.3. E-mail de análise enviado pela equipe da Proofpoint:

Sair | Excluir | a Todos | Mais | Responder | responder e encaminhar | Encaminhar | Etapas Rápidas | Agendar | Marca | Não Lida | Marcas | Edição | Zoom

qua 30/03/2022 12:05

Pablo Dewes <pdewes@proofpoint.com>
Proofpoint Risk Assessment Antispam

Para: Pablo Dewes <pdewes@proofpoint.com>
Cc: André Willian Pimenta Santana <Administrador da Rede FUNASA>

Fábio Henrique Braga Soares
Você encaminhou esta mensagem em 31/03/2022 13:04.

Gilvane José de Souza

Olá a todos, conforme chamada segue algumas evidências críticas detectadas até o momento.

Evidência 1 – phishing direcionado à FUNASA, com objetivo de roubo de credencial. Algo bem isolado e focado para poucas pessoas com o intuito de comprometer as contas abaixo, e após isto realizar ataques laterais com o objetivo de roubo de dados e/ou proliferação de ransomware. É interessante trocar a senha dos 4 usuários.

Verify your Account valdilene.siqueira

Customer <no_reply@campianic.com>
To: valdilene.siqueira@funasa.gov.br

<http://funasa.gov.br>
valdilene.siqueira Administrator.
assword for valdilene.siqueira@funasa.gov.br is due to expire 3/29/2022 8:13:42 a.m.
Use below button to keep or update current credentials.

All Rights Reserved

3.11. Detalhamento das evidências detectadas após a análise na ferramenta da Proofpoint:

1º - Exemplo:

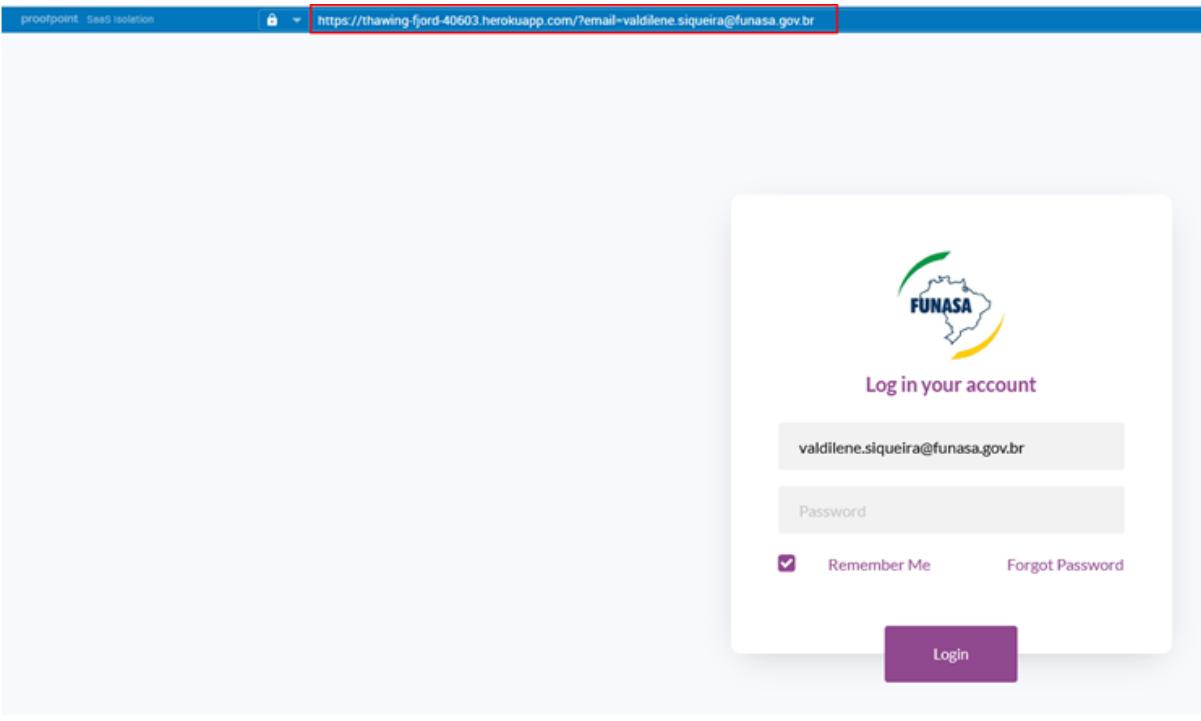
3.11.1. *Phishing* direcionado à FUNASA, com o objetivo de roubo de credencial. Algo bem isolado e focado em poucas pessoas, com o intuito de comprometer as contas abaixo, e após isto, realizar ataques laterais com o objetivo de roubo de dados e/ou proliferação de *ransomware*.



3.11.2. Lista de pessoas que receberam o *phishing*:

Reason	Sender	Recipients	Date	Subject
Spam: 100	no_reply@campianic.com	valdilene.siqueira@funasa.gov.br	2022-03-29 05:13:56 (UTC-03:00)	Verify your Account valdilene.siqueira
Spam: 100	no_reply@pupalizes.com	saneamentoral@funasa.gov.br	2022-03-29 05:03:51 (UTC-03:00)	Verify your Account saneamentoral
Spam: 100	no_reply@pupalizes.com	michelle.correia@funasa.gov.br	2022-03-29 04:57:34 (UTC-03:00)	Verify your Account michelle.correia
Spam: 100	no_reply@pupalizes.com	juliana.zancul@funasa.gov.br	2022-03-29 04:53:03 (UTC-03:00)	Verify your Account juliana.zancul

3.11.3. A imagem abaixo ilustra a página *phishing* utilizada para o roubo das credenciais:



Global Metrics

  <https://thawing-fjord-40603.herokuapp.com/?email=valdilene.siqueira@funasa.gov.br>

3.11.4. Origem da mensagem visualizada no cabeçalho header:

```

Authentication-Results: pprops.net;
spf=neutral smtp.mailfrom=no_reply@campianic.com;
dkim=fail header.d=campianic.com header.s=default;
dmarc=fail header.from=campianic.com

Received: from omalley.funasa.gov (unknown [127.0.0.1]) by IMSVA (Postfix)
with ESMTP id 0E164AB075 for <valdilene.siqueira@funasa.gov.br>; Tue, 29 Mar
2022 05:09:29 -0300 (-03)
Received: from omalley.funasa.gov (unknown [127.0.0.1]) by IMSVA (Postfix)
with ESMTP id F1911AB073 for <valdilene.siqueira@funasa.gov.br>; Tue, 29 Mar
2022 05:09:28 -0300 (-03)
Received: from nowzaradan.funasa.gov (unknown [10.15.2.100]) by
omalley.funasa.gov (Postfix) with ESMTPS for
<valdilene.siqueira@funasa.gov.br>; Tue, 29 Mar 2022 05:09:28 -0300 (-03)
Received: from mta0.campianic.com (hwsrv-949437.hostwindsdns.com
[23.254.129.221]) by nowzaradan.funasa.gov with ESMTP id
22T8DlmF019190-22T8DlmH019190 (version=TLSv1.2
cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO) for
<valdilene.siqueira@funasa.gov.br>; Tue, 29 Mar 2022 05:13:49 -0300

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=default; d=campianic.com;
h=From:To:Subject:Date:Message-ID:MIME-Version:Content-Type:
Content-Transfer-Encoding; i=no_reply@campianic.com;
bh=4hO1GRl2veO2YoyRlyk1b5CFwGwDY919aDi+7UEx2s0=;
b=LxtSCV8f8USgKEPhQX1QEQQ33dyldPbSI9UTRJqjZ54wiWBzcIkYCLFBoFL85/bjE/hfySTnJp1Ir
1ebK3ONcrZX0Ne2wXbWF8t1ssH3+2GyvQAis1WyqFQ9SRwFUYBdefgYpuUyQAJVZjHYNzXmGzN1e
LEeA1aYJ2drgrbarDvT4=
```

From: Customer <no_reply@campianic.com>
To: <valdilene.siqueira@funasa.gov.br>
Subject: Verify your Account valdilene.siqueira
Date: Tue, 29 Mar 2022 08:13:42 +0000
Message-ID: <20220329081342.40C279E3A7552A07@campianic.com>
Content-Type: text/html; charset="iso-8859-1"

2º - Exemplo:

3.12. Link detectando *malware*.

3.12.1. Seria interessante validar, na solução da TREND, se a mesma foi efetiva no bloqueio desta página.

<https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdrive2cs.serveftp.net&umid=CD9C5128-DB1C-1405-B58E-4A73AF4895CA&auth=9038d131677cf2caad0d3e0a933767309e4a6609-bc8c1a033a61647bade2bb031854b2720d32bd9e>

[Open in Proofpoint Browser Isolation](#) ⓘ

Attributes ⓘ

Family

Malware

3º - Exemplo:

3.13. Mensagens categorizadas como *PHISH* bloqueadas.

propoint. running in ex. monitor | Logout

System Email Protection Quarantine > Messages

Search

Sender: Recipients: Fast Query

Subject: Reason: Score From: To:

Maximum Age: Set By: Order:

Messages

Auto age enabled: Displaying messages received since 2022-07-26 19:25 (UTC-000)

Reason	Sender	Recipients	Date	Subject	Size
Span: 100	www-data@apj2.sendreco.co.za	francisco.barbosa@funasa.gov.br	2022-08-01 16:53:06 UTC-03:00	Magalu 2022 - Smart TV 60" 4K RS 1.559,99 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 42	www-data@faustao.ganeye.com	vestidor.carrasco@funasa.gov.br	2022-08-01 16:32:48 UTC-03:00	Magalu - Smart TV 55" 4K RS 1.499,00 - Mega Oferta! 3103654801618	26 KB
Span: 100	www-data@as34.sendreco.co.za	cristiane.silva@funasa.gov.br	2022-08-01 16:23:15 UTC-03:00	Smart TV 60" 4K RS 1.699,90 - Smart TV 55" 4K RS 1.355,99 - Smart TV 55" 4K RS 1.25	28 KB
Span: 100	www-data@as34.sendreco.co.za	remunda.ferreira@funasa.gov.br	2022-08-01 16:26:42 UTC-03:00	Smart TV 60" 4K RS 1.699,90 - Smart TV 55" 4K RS 1.355,99 - Smart TV 47" 4K RS 1.1	29 KB
Span: 100	magalu19212@outlooksources-261082@bounce fautontrading.com	decko.eugenio@funasa.gov.br	2022-08-01 16:26:42 UTC-03:00	decko.eugenio@funasa.gov.br	30 KB
Span: 100	magalu19212@outlooksources-301082@bounce fautontrading.com	dene.sousa@funasa.gov.br	2022-08-01 16:26:38 UTC-03:00	Mobile Banking Best Practices: How To Gain Competitive Edge And Grow Customer B	30 KB
Span: 100	www-data@as19.sendreco.co.za	teresa.mendes@funasa.gov.br	2022-08-01 16:16:56 UTC-03:00	Magalu 2022 - Smart TV 60" 4K RS 1.559,99 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as19.sendreco.co.za	franklin.maria@funasa.gov.br	2022-08-01 16:15:39 UTC-03:00	Magalu 2022 - Smart TV 60" 4K RS 1.559,99 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as19.sendreco.co.za	welinton.monterrey@funasa.gov.br	2022-08-01 15:59:09 UTC-03:00	Magalu 2022 - Smart TV 60" 4K RS 1.547,29 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as19.sendreco.co.za	yashayuki.watanabe@funasa.gov.br	2022-08-01 15:45:44 UTC-03:00	Questo é Estoque Magalu 2022 - Smart TV 60" 4K RS 1.547,29 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as19.sendreco.co.za	xico.lima@funasa.gov.br	2022-08-01 15:40:40 UTC-03:00	Questo é Estoque Magalu 2022 - Smart TV 60" 4K RS 1.547,29 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	amazon-connect@yuhong.cn	andrea.pereira@funasa.gov.br	2022-08-01 15:45:45 UTC-03:00	Amazon広告で見るべき二つの問題 202404530	23 KB
Span: 100	www-data@as19.sendreco.co.za	silvana.ferreira@funasa.gov.br	2022-08-01 15:11:02 UTC-03:00	Questo é Estoque Magalu 2022 - Smart TV 60" 4K RS 1.547,29 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as19.sendreco.co.za	slalislano.kuz@funasa.gov.br	2022-08-01 15:03:13 UTC-03:00	Questo é Estoque Magalu 2022 - Smart TV 60" 4K RS 1.547,29 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as19.sendreco.co.za	shelia.rezende@funasa.gov.br	2022-08-01 15:00:13 UTC-03:00	Questo é Estoque Magalu 2022 - Smart TV 60" 4K RS 1.547,29 - Smart TV 55" 4K RS 1.349,99 - Approve	24 KB
Span: 100	www-data@as15.sendreco.co.za	consuelo.coza@funasa.gov.br	2022-08-01 15:00:21 UTC-03:00	Smart TV 60" 4K RS 1.699,90 - Smart TV 55" 4K RS 1.355,99 - Smart TV 47" 4K RS 1.1	26 KB
Span: 100	root@15.replace0973.org	cynthia.rocha@funasa.gov.br	2022-08-01 15:04:44 UTC-03:00	Pagamento não identificado 018002022	27 KB
Span: 100	root@104.replace0973.org	claudia.vega@funasa.gov.br	2022-08-01 14:53:52 UTC-03:00	Pagamento não identificado 018002022	27 KB
Span: 100	root@68.replace0973.org	araci.oliveira@funasa.gov.br	2022-08-01 14:51:01 UTC-03:00	Pagamento não identificado 018002022	27 KB
Span: 100	root@22.replace0973.org	ado.pereira@funasa.gov.br	2022-08-01 14:48:37 UTC-03:00	Pagamento não identificado 018002022	27 KB
Span: 100	root@24.replace0973.org	alessandro.ferraz@funasa.gov.br	2022-08-01 14:46:33 UTC-03:00	Pagamento não identificado 018002022	27 KB

more live status

Version 8.18.4 funasa_production.vim

4º - Exemplo:

3.14. Mensagens categorizadas como *MALWARE* bloqueadas:

proofpoint.

System Email Protection Quarantine > Messages

Search Reset Saved New

Sender: Starts With Recipients: Starts With Score From: 0 To: 100 Fast Query

Subject: Starts With Reason: All messages Sort By: Date Order: Descending

Maximum Age: Auto

Messages

All INBOUND_MALWARE (1)

Reason:

Sender	Recipients	Date	Subject	Size
sign@greenearth.com	rosalba.silva@funasa.gov.br	2022-08-02 13:06:51 [UTC-03:00]	Vibe_Boletos_20220720.pdf - #92244	21 KB
oncursado1@gmail.com	cleusa.moura@funasa.gov.br	2022-08-02 11:23:06 [UTC-03:00]	Cursa Presencial: Questões Polêmicas da Legislação de Pessoal, Aposentadorias e i	124 KB
oncursado1@gmail.com	carmen.santos@funasa.gov.br	2022-08-02 09:48:51 [UTC-03:00]	Cursa Presencial: Questões Polêmicas da Legislação de Pessoal, Aposentadorias e i	124 KB
oncursado1@gmail.com	arnoldo.besko@funasa.gov.br	2022-08-02 08:48:50 [UTC-03:00]	Cursa Presencial: Questões Polêmicas da Legislação de Pessoal, Aposentadorias e i	123 KB
www-data@972241-cd99643.lmweb.ru	coresp.sensu@funasa.gov.br	2022-08-02 05:57:42 [UTC-03:00]	[PTG]-Atrazo de debito - protocolo1153453	4 KB
kendong@eet.com.br	ana.santos@funasa.gov.br	2022-08-01 19:13:55 [UTC-03:00]	NFE - #97333	7 KB
vendadireta@braspress.com.br	douglas.maria@funasa.gov.br	2022-08-01 18:42:55 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	dirne@funasa.gov.br	2022-08-01 18:10:16 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	desam.pab@funasa.gov.br	2022-08-01 16:16:51 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	desusp.pab@funasa.gov.br	2022-08-01 16:06:51 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	deponse.silva@funasa.gov.br	2022-08-01 15:44:15 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	deborah.roberta@funasa.gov.br	2022-08-01 15:34:16 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	david.tsu@funasa.gov.br	2022-08-01 15:06:58 [UTC-03:00]	Nota fiscal em anexo	5 KB
root@globalcertified973.org	alzira.morais@funasa.gov.br	2022-08-01 14:25:20 [UTC-03:00]	Pagamento não identificado - 01/08/2022	27 KB
vendadireta@braspress.com.br	daniela.pois@funasa.gov.br	2022-08-01 14:23:27 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	daniela.carrerengos@funasa.gov.br	2022-08-01 14:23:03 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	fernanda.moreira@funasa.gov.br	2022-08-01 13:30:44 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	casu@funasa.gov.br	2022-08-01 13:19:17 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	coresp.gab@funasa.gov.br	2022-08-01 13:05:58 [UTC-03:00]	Nota fiscal em anexo	5 KB
vendadireta@braspress.com.br	coresp.pab@funasa.gov.br	2022-08-01 13:03:27 [UTC-03:00]	Nota fiscal em anexo	5 KB
teste@grupavelveto.com.br	eduardo.sousa@funasa.gov.br	2022-08-01 10:59:09 [UTC-03:00]	Nota fiscal em anexo	5 KB
teste@grupavelveto.com.br	erika.silveirang@funasa.gov.br	2022-08-01 10:37:32 [UTC-03:00]	Nota fiscal em anexo	5 KB
teste@grupavelveto.com.br	emilia.santos@funasa.gov.br	2022-08-01 10:01:56 [UTC-03:00]	Nota fiscal em anexo	5 KB

4. Comparativos de chamados abertos na ferramenta de registro de requisição e incidente (Qualitor) associados à tratativas de e-mail entre as ferramentas.

4.1. Chamados abertos durante a vigência das ferramentas da FORTIMAIL e do InterScan Messaging Security Virtual Appliance.

CSU

Ações Pesquisar Atualizar Ajuda

Pesquisa de requisições de serviço [77]

Requisição Abertura Título da requisição Prioridade

REC-54722 16/05/2022 - 14:43 Solicito verificar se está na quarentena e-mail enviado pelo Fundação Nacional de Saúde - FUNASA Superintendência Estadual de Saúde

REC-54569

Favor verificar mensagem maliciosa. -----Mensagem original----- De: <https://uldefense.com/v3f/_https://balancasecomplementos.com>

REC-54557

Boa tarde! Estamos com uma licitação agendada para o dia 18/05 e liberação por parte da TI para ser encaminhado. No aguardo! Atte A

REC-54052

Prezados, Solicito verificar a veracidade e procedência da mensagem

REC-54049

Gostaria de que fosse verificado o motivo de eu não estar recebendo

REC-54011

Prezados! Bom dia! Estou recebendo e-mail maliciosos conforme an

Pesquisa de requisições de serviço

Ações

Período: [01/01/2022] até [19/05/2022]

Periodo: [01/01/2022] até [19/05/2022]

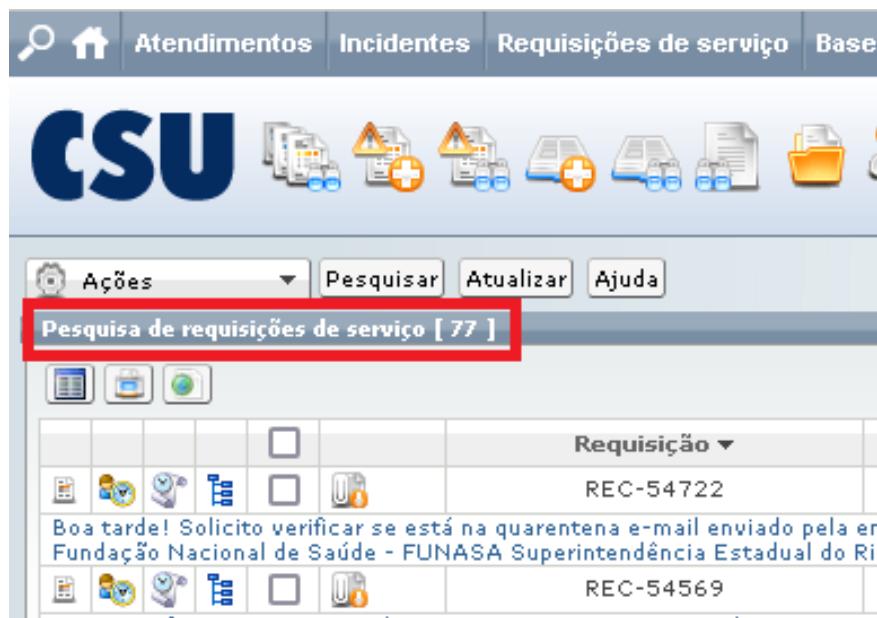
Abertura Atendimento Encerramento Processo Campos adicionais

Réquisição: Cliente: Funasa

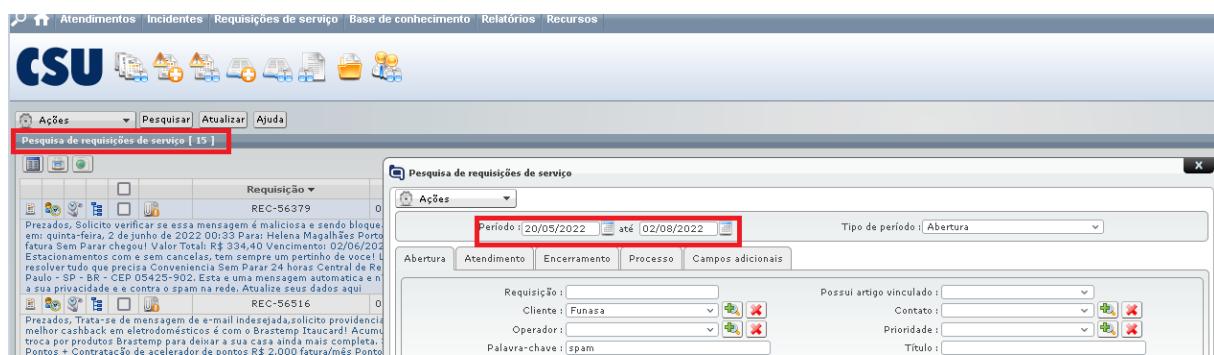
Possui artigo vinculado: Contato:

Operador: Prioridade:

Palavra-chave: spam Título:



4.2. Chamados abertos durante a vigência da ferramenta da Proofpoint.



5. Conclusão

As ferramentas de spam descritas neste documento podem ser utilizadas para filtrar e-mails recebidos e enviados, visando manter a segurança da rede em relação ao fluxo de mensagens. Possuem funções de detecção e bloqueio de spam, de anti-malware, de antivírus, proteção contra perda de dados, detecção de ameaças, sandboxing, portal de gerenciamento centralizado entre outras. Suas definições de spam, vírus e malware são atualizadas diariamente na base de conhecimento do fabricante das respectivas ferramentas, visando a eliminação de novas ameaças associadas à mensagens eletrônicas.

Com relação ao uso das ferramentas, o InterScan Messaging Security Virtual Appliance, Fortimail e Proofpoint foram semelhantes, porém, na análise dentro do ambiente da FUNASA, a ferramenta Proofpoint, apresentou um melhor resultado nas funções de heurística e na detecção de spam, phishing e malware. A mesma detectou os sinais do ataque de phishing e



malware nos logs das mensagens que já haviam sido analisadas pelas ferramentas da Fortimail e do InterScan Messaing Security Virtual Appliance e que não foram detectados por ambas. Dessa forma, promovendo um melhor bloqueio desse tipo de mensagem em comparação com o filtro de spam da Fortimail e do InterScan Messaing Security Virtual Appliance, conforme demonstrado nos logs registrados neste documento.

O melhor desempenho da ferramenta da Proofpoint ocasionou, também, uma redução de chamados referentes à problemas de envio e recebimento de mensagens e, consequentemente, das tratativas necessárias para bloqueio ou liberação de falsos positivos que passavam ou ficavam retidos na quarentena das ferramentas da FORTIMAIL e do InterScan Messaing Security Virtual Appliance.

Diante do exposto, ressaltamos que até a presente data, 02/08/2022, a ferramenta de filtro de spam da Proofpoint foi a que apresentou os melhores resultados nas suas funções dentro do ambiente da FUNASA.

Silvano José de Souza
Especialista em Segurança da
Informação
Qintess

Flavio Henrik Braga Soares
Especialista de Infraestrutura
Qintess