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.

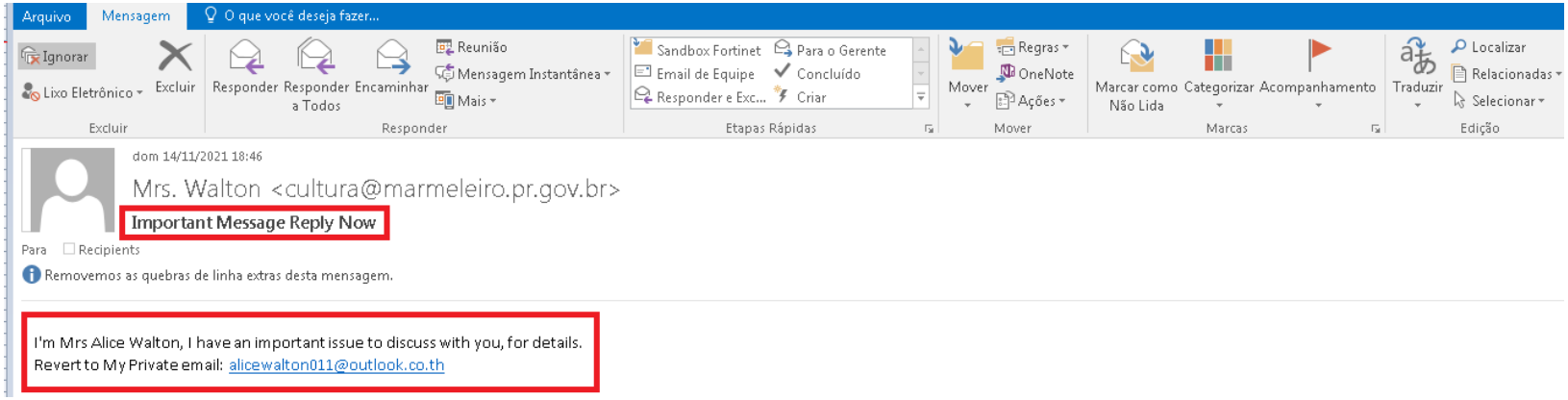
Suas definições de spam, vírus e malware são atualizadas diariamente na base de conhecimento do fabricante das respectivas ferramentas visando a eliminação de novas ameaças associadas a mensagens eletrônicas.

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.

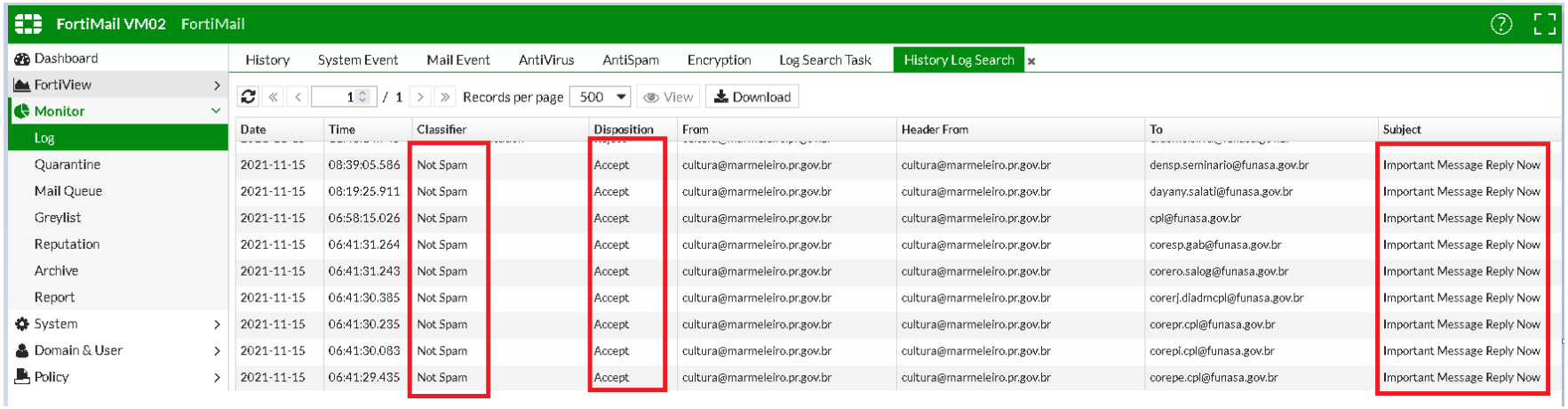
3.1. Análise de Logs associados às ferramentas InterScan Messaing Security Virtual Appliance e do Fortimail.

1º - Exemplo:

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

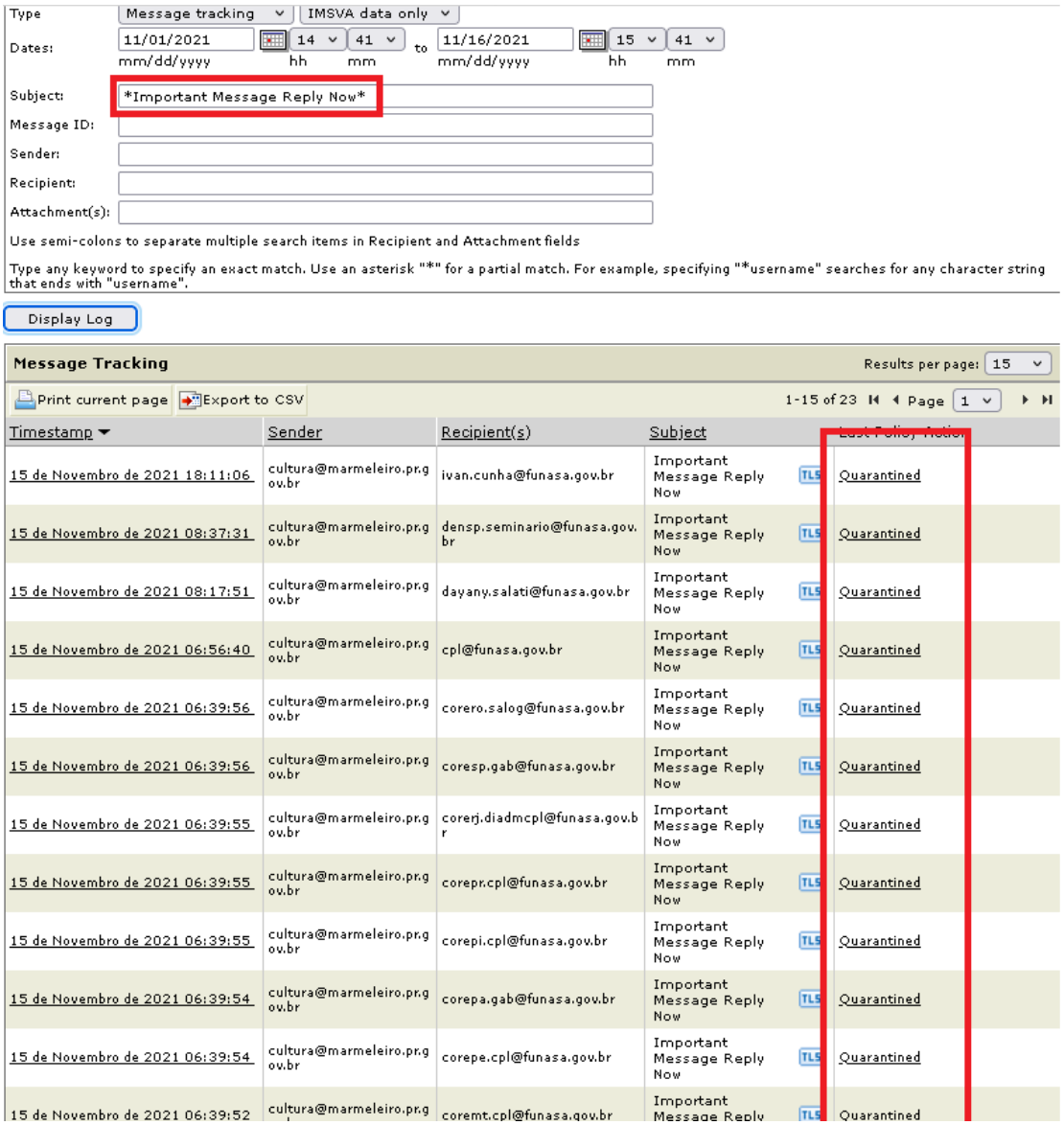


3.3. Log do Fortimail no qual a mensagem é aceita e categorizada como limpa (Not Spam).



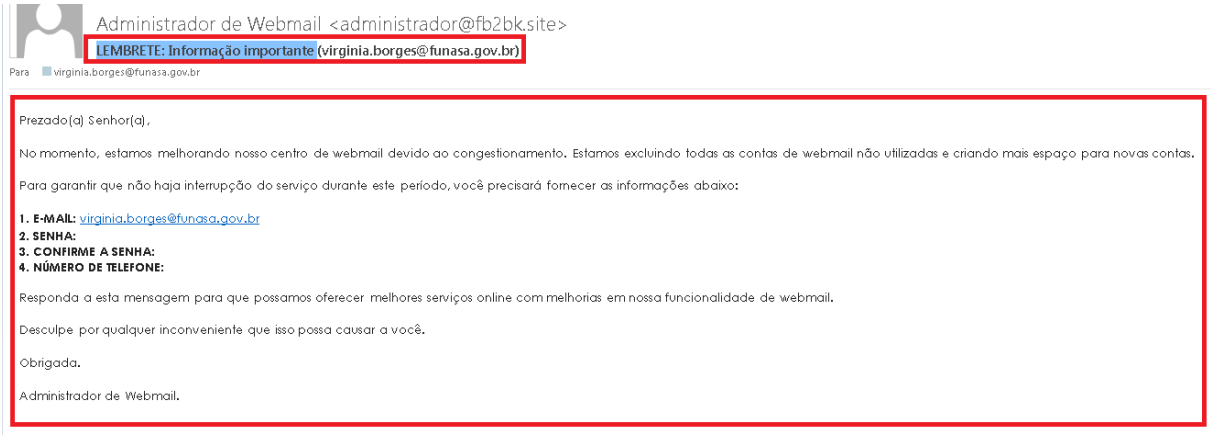
Date	Time	Classifier	Disposition	From	Header From	To	Subject
2021-11-15	08:39:05.586	Not Spam	Accept	cultura@marmeleiro.pr.gov.br	cultura@marmeleiro.pr.gov.br	densp.seminario@funasa.gov.br	Important Message Reply Now
2021-11-15	08:19:25.911	Not Spam	Accept	cultura@marmeleiro.pr.gov.br	cultura@marmeleiro.pr.gov.br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

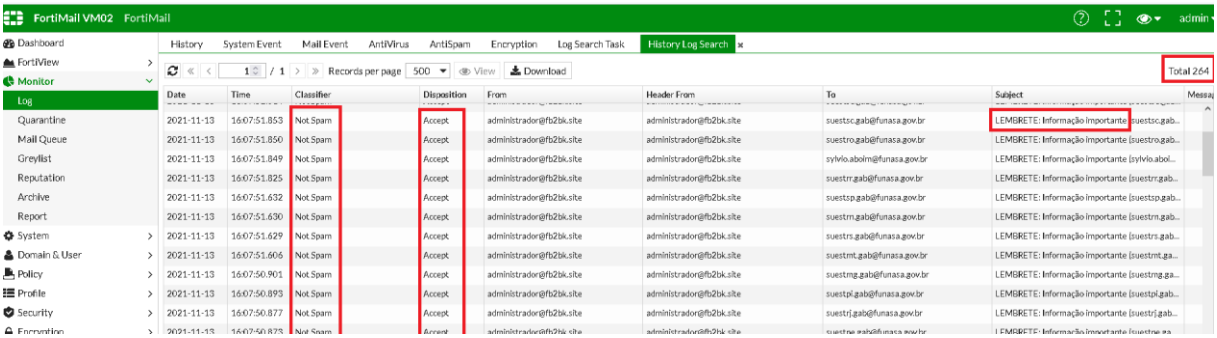


2º Exemplo:

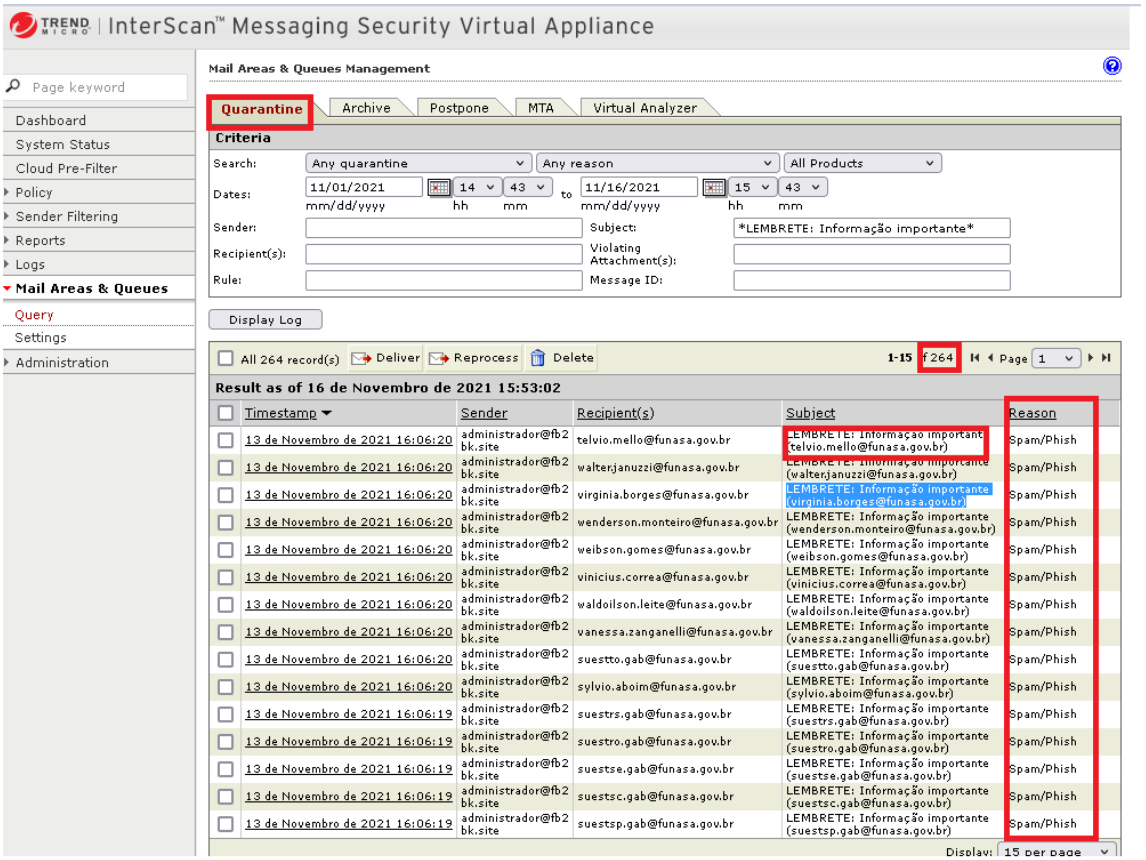
3.4. Mensagem spam com o assunto “LEMBRETE: Informação importante” enviada para vários destinatários da FUNASA.



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

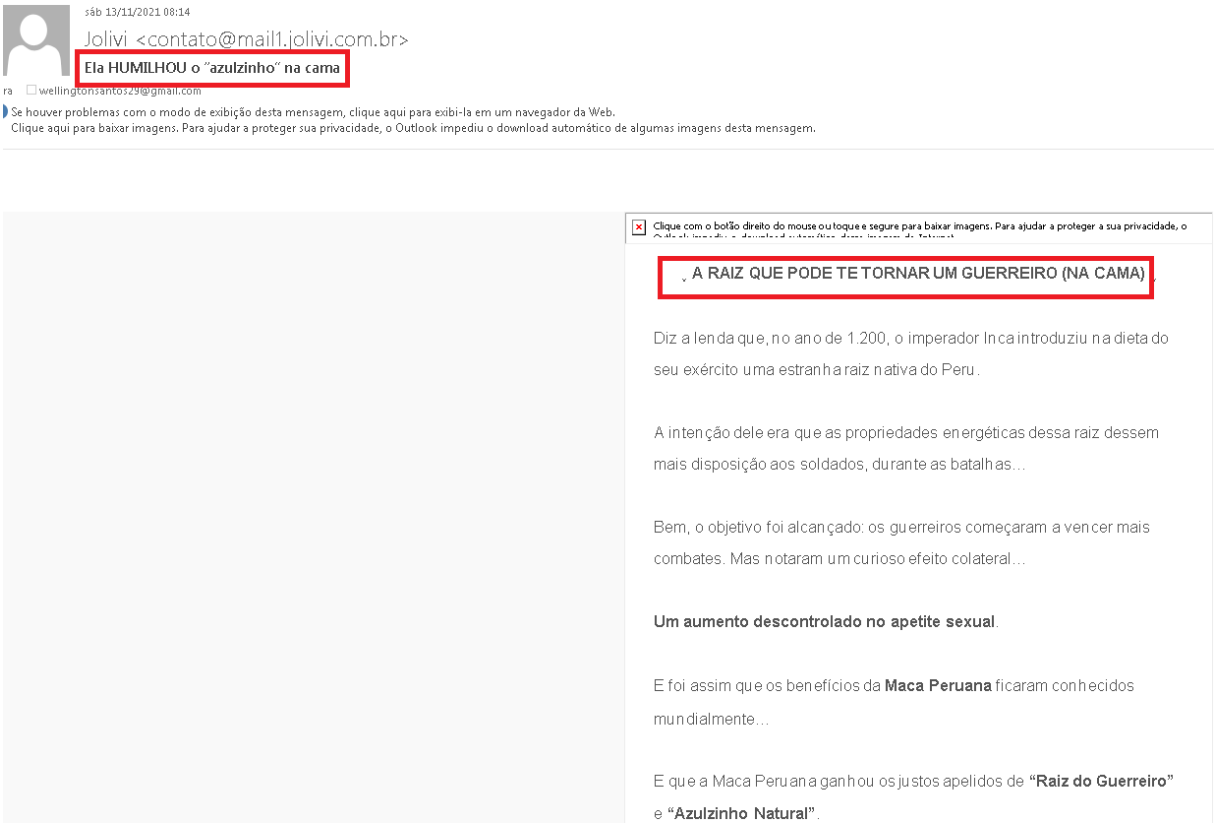


3.6. Mensagens detectadas/bloqueadas como spam e adicionadas à quarentena no InterScan Messaing Security Virtual Appliance.

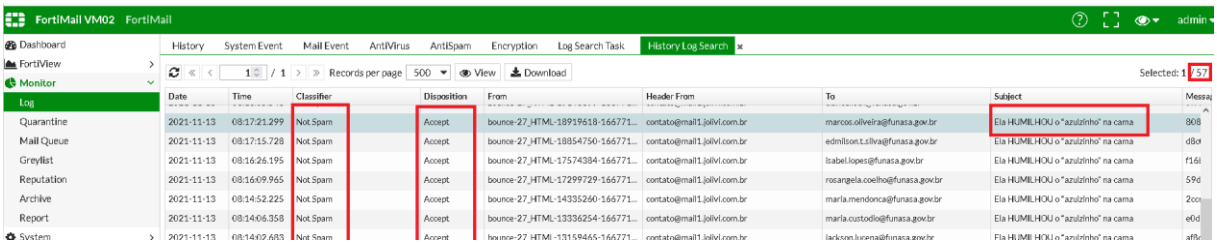


3º Exemplo:

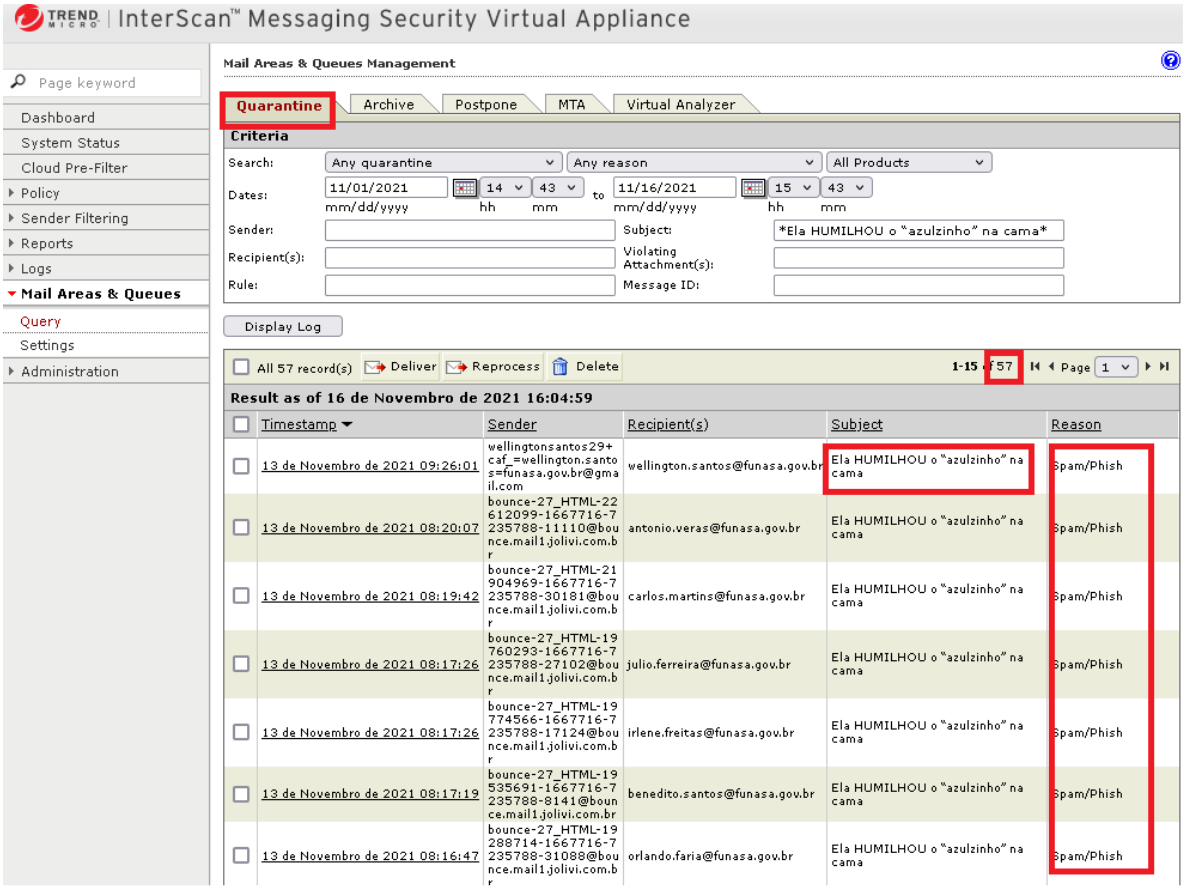
3.7. Mensagem spam com o assunto “Ela HUMILHOU o “azulzinho” na cama” enviada para vários destinatários da FUNASA.



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



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

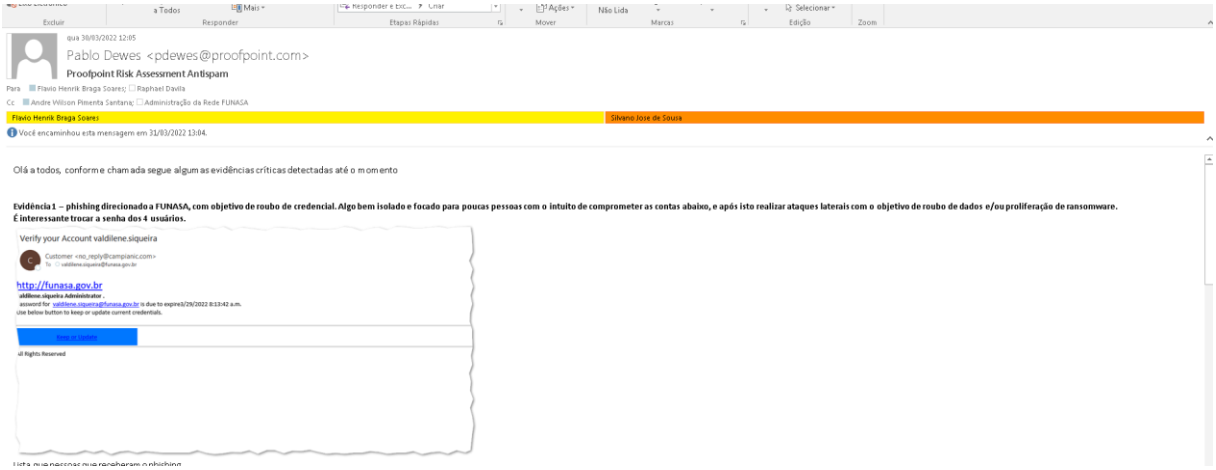


3.10. Análise de Logs associados à ferramenta da Proofpoint.

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:



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

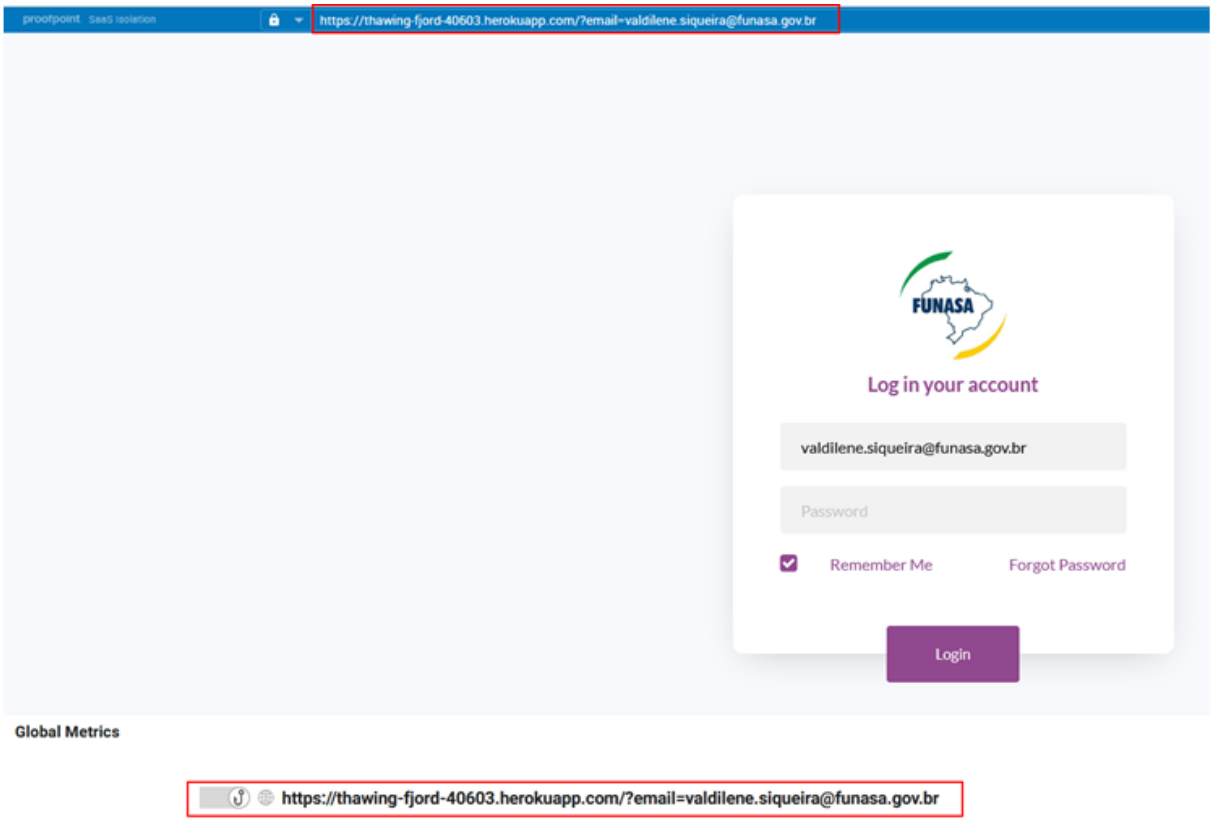
1º - Exemplo:

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	saneamentorural@funasa.gov.br	2022-03-29 05:03:51 [UTC-03:00]	Verify your Account saneamentorural
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:



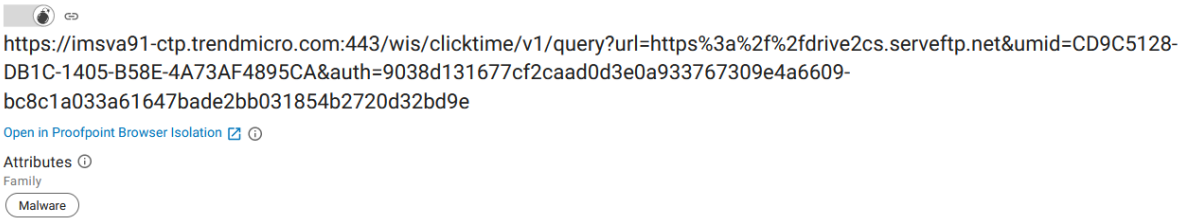
3.11.4. Origem da mensagem visualizada no cabeçalho header:

```
Authentication-Results: ppops.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 0E164AE075   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 F1911AE073   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=4hO1GRl2veO2YoyR1yklb5CFwGwDY919aDi+7UEx2s0=;
 b=LXtSCV8f8USgKEPhQXiQEQ33dyldFbSI9UTRJqjZ54wiWBzcIkYCLFBoFL85/bjE/hfySTnJp1Ir
   1ebK3ONcrZX0Ne2wXbWF8tlsSH3+ZGyvQAis1WyqFQ9SRwFUYBdefgYpuUyQAJVZjHYNzXmGzNIe
   LEeAIaYJ2drgbarDvT4=

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:

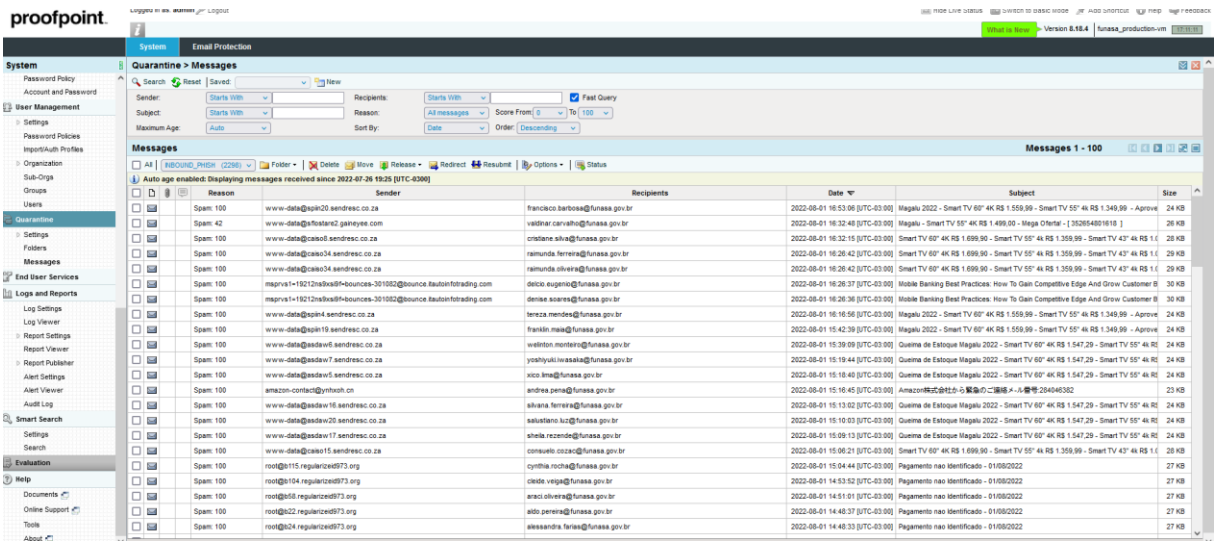
3.12. Link detectando *malware*.

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



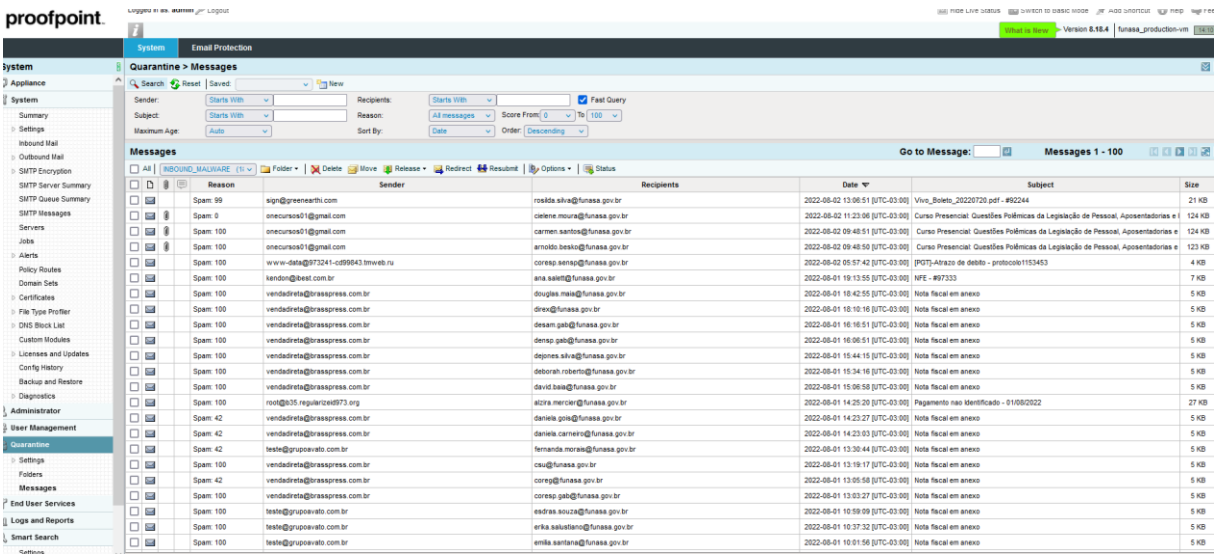
3º - Exemplo:

3.13. Mensagens categorizadas como *PHISH* bloqueadas:



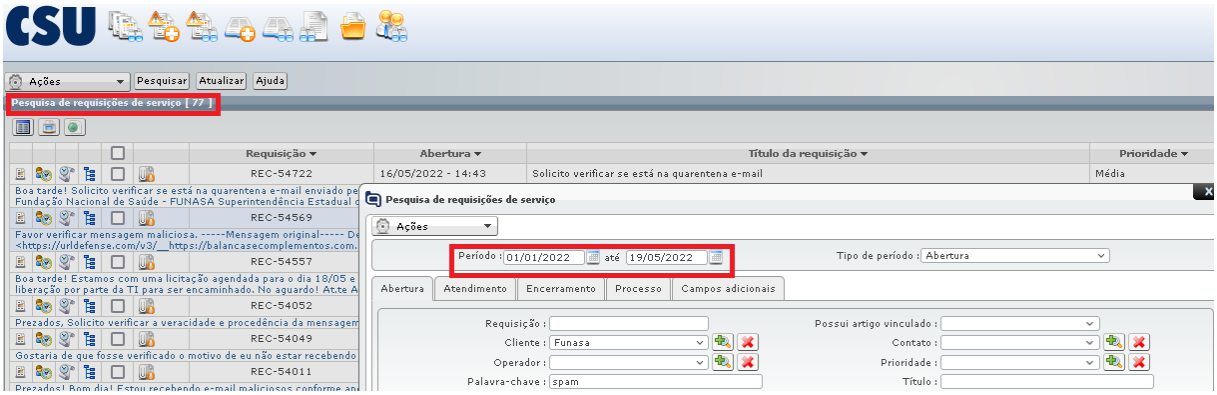
4º - Exemplo:

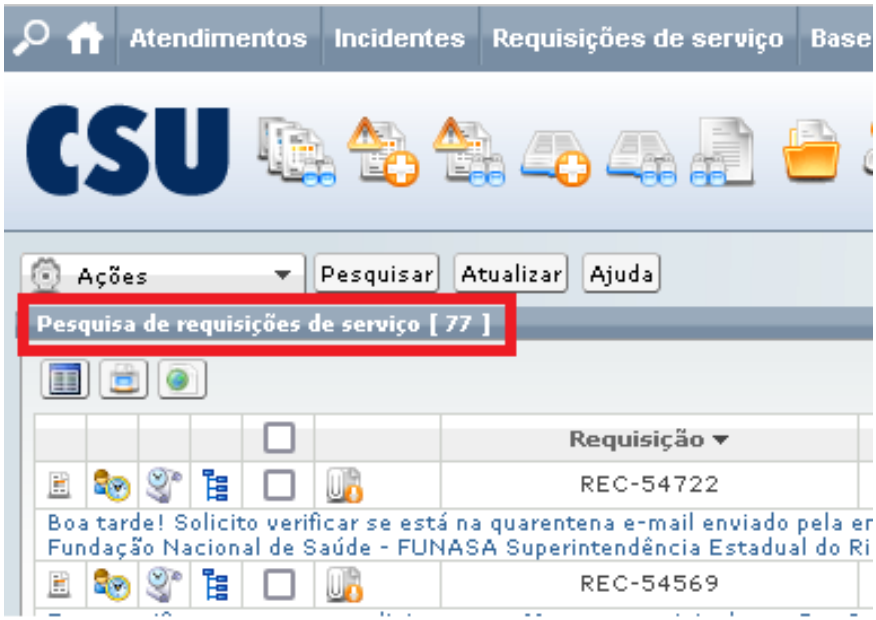
3.14. Mensagens categorizadas como *MALWARE* bloqueadas:



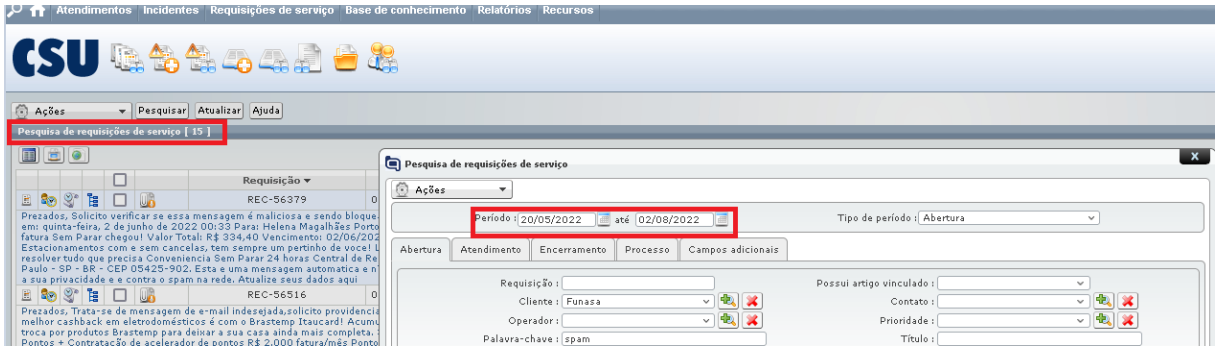
4. Comparativos de chamados abertos na ferramenta de registro de requisição e incidente (Qualitor) associados à tratativas de e-mail entres as ferramentas.

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





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 Messaing 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 Fortimal e do InterScan Messaing Security Virtual Appliance, conforme demonstrado nos logs registrados neste documento.

O melhor desempenho da ferramenta da Prooftpoint 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