

# Cyber Threat Intelligence

## Aplicada à Análise de Phishing Corporativo

Évora da Ibéria Leite

### Resumo

Este trabalho apresenta uma investigação prática de Cyber Threat Intelligence aplicada à análise de um e-mail de phishing voltado ao ambiente corporativo, com foco em empresas do setor de energia industrial. Foram usadas diversas ferramentas consolidadas (VirusTotal, Hybrid-Analysis, Burp Suite) para identificar indicadores de comprometimento, padrões de pretexto e infraestrutura maliciosa.

Os resultados revelaram uma campanha estruturada com e-mail spoofing, com landing pages de login clonadas do provedor de e-mail da empresa, hospedadas em subdomínios de plataforma gratuita (Weebly), uso de P2P via IPFS ou uso de AJAX e requests do tipo POST para coleta de credenciais. Foi revelada também a ausência de DKIM e DMARC, o que permite a mitigação deste tipo de ataque.

Conclui-se que a implementação adequada de políticas de autenticação de e-mail (SPF, DKIM, DMARC), aliada a monitoramento contínuo de relatórios DMARC e a integração de ferramentas CTI, é essencial para mitigar riscos de phishing e proteger a privacidade, disponibilidade e integridade dos dados e serviços das organizações.

## 1 Introdução

No contexto atual da digitalização de processos corporativos, o e-mail permanece como um dos principais vetores de comunicação e ao mesmo tempo um dos mais explorados por agentes maliciosos. A engenharia social, aliada a técnicas cada vez mais sofisticadas de spoofing e clonagem de páginas legítimas, permite que atacantes influenciem usuários a revelar credenciais críticas ou a executar ações que comprometam a segurança organizacional.

Este relatório apresenta a aplicação prática de Cyber Threat Intelligence (CTI) para a análise de um e-mail de phishing direcionado a uma empresa de pequeno porte do setor de energia. Com base em ferramentas consolidadas como VirusTotal, Hybrid-Analysis e MITRE ATT&CK, aliado ao uso de BurpSuite para inspeção manual, busquei identificar padrões de ataque, indicadores de comprometimento e vulnerabilidades exploradas.

Ao explorar tanto o design do e-mail (pretexto, entrega e técnicas de spoofing), quanto o comportamento dinâmico de páginas clonadas e back-end malicioso, o documento tem como objetivo demonstrar os riscos inerentes à ausência de controles de autenticação de origem (SPF, DKIM, DMARC) e propõe um procedimento replicável de mitigação. Dessa forma, esta análise serve de base para fortalecer a postura de defesa contra campanhas de phishing futuras.

## 2 Contexto

**M Solutions** (por motivos de confidencialidade usaremos um nome fictício) é uma empresa de automação e controle com foco em programação e comissionamento de ICS/SCADA. Há 10 anos usa um domínio e um provedor de email associado a este domínio. Até então nunca havia sofrido uma tentativa de phishing.

A empresa recebeu um email com características de phishing durante o mês de março de 2025. Este email foi direcionado ao CEO da empresa, não foi detectado spam pelo provedor e tinha como motivo informar ao alvo que várias tentativas de acesso à sua conta de email haviam sido detectadas.

No primeiro dia de junho de 2025, mais um email foi recebido. Desta vez, informando que a conta de email do alvo iria ser desativada, e que seria necessário que o alvo acessasse um link para verificar a conta para que isto não ocorresse. Aqui temos um detalhe importante, o email foi enviado do mesmo domínio de email do alvo, mudando apenas o usuário.

### 3 Objetivos

Este relatório tem como objetivo principal usar ferramentas de Cyber Threat Intelligence (CTI) para pontuar os indicativos de *phishing* resultantes da análise do design do e-mail e da análise dos relatórios gerados pelas seguintes ferramentas:

- Virus Total
- Hybrid-Analysis
- Mitre ATT&CK
- UrlScan.io
- BurpSuite

A partir do relatório gerado, estratégias de mitigação serão expostas para os possíveis problemas associados ao e-mail, como:

- Verificação dos registros dos domínios;
- Atualização do registro SPF;
- Implementação do DKIM;
- Implementação da política DMARC;
- Monitoramento contínuo do servidor de e-mail.

Além disso, o relatório pode ser adotado como um procedimento a ser usado nas análises de phishing que a empresa possa, por ventura, receber futuramente.

## 4 Análise do Email

### 4.1 Pretextos

Os atacantes usaram técnicas psicológicas de engenharia social como **urgência**, ao tratar de assuntos sensíveis como acesso indevido e inativação de conta, e **autoridade** ao se direcionar ao alvo como RH (primeira tentativa de phishing, março-2025 Figura 1), e como o suporte da própria plataforma de email da empresa (segunda tentativa, junho-2025, Figura 2).

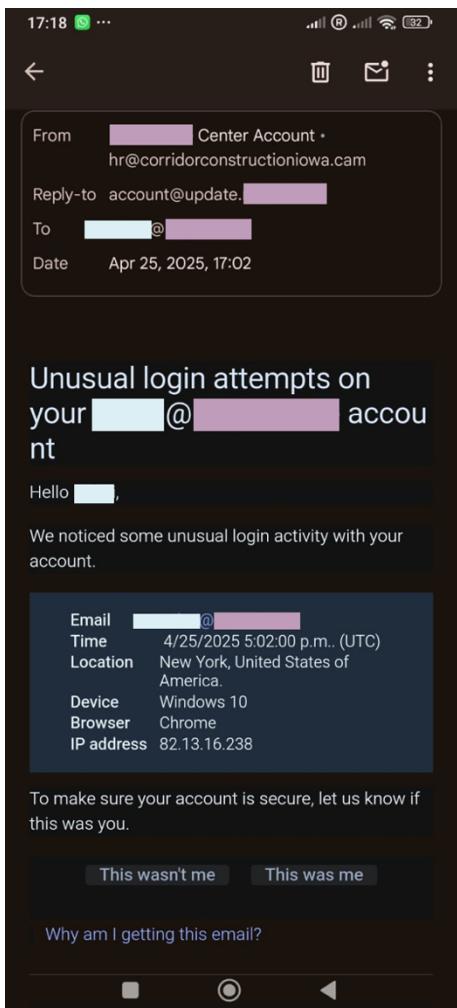


Figura 1: Pretexto do primeiro email

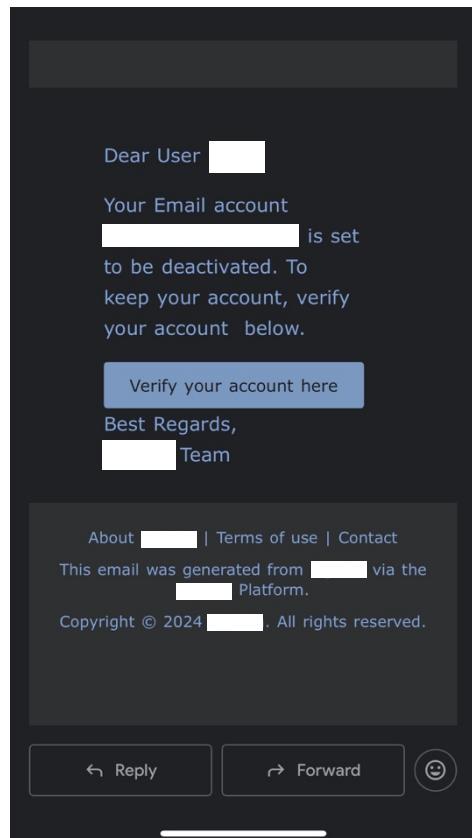


Figura 2: Pretexto do segundo email

#### 4.3 Páginas clonadas

Neste tópico veremos as páginas clonadas do **primeiro** e do **segundo** ataque, em contraste com a **página oficial**.

Na **página oficial**, logo abaixo, podemos notar que a URL está correta e o site usa https.

No **primeiro** clone, nota-se uma URL completamente diferente da original, e o email do usuário já está populado. Os idiomas abaixo também estão mal escritos. No **segundo** clone, o atacante usou um provedor de sites web, nota-se o mesmo problema na apresentação dos idiomas, além das caixas de input não parecerem profissionais.

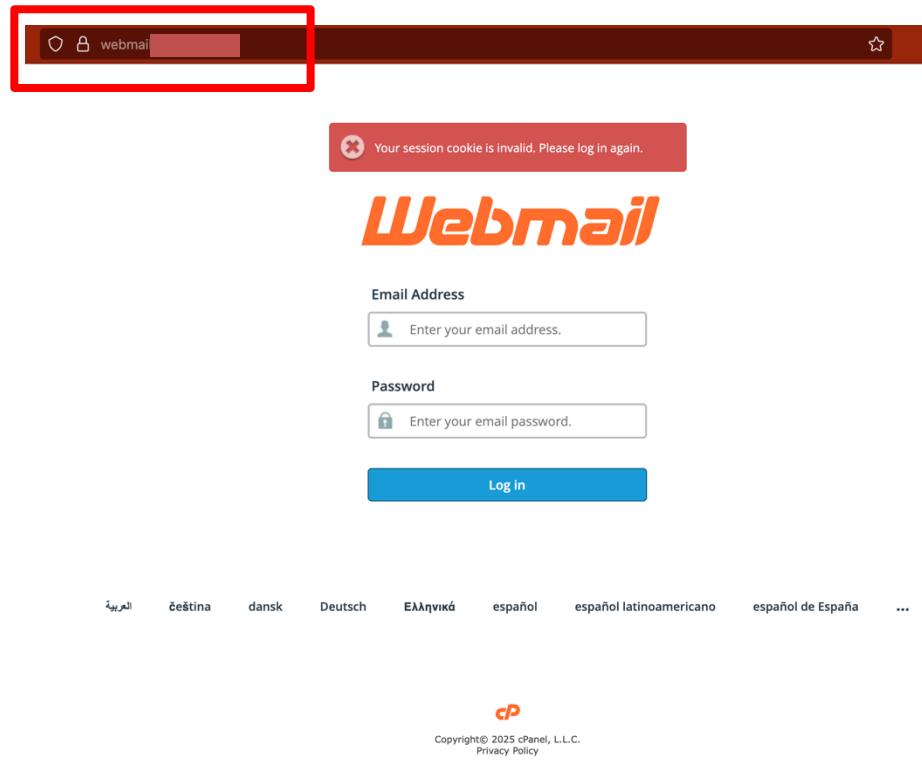


Figura 3: Página original

The image displays two cloned login pages side-by-side. Both pages have their URLs highlighted with red boxes. The left page's URL is 'ipfs.io/ipfs/bafybeibdiuiycafjy2s7w56...', and the right page's URL is 'webmailsecureonlinelogin83kksdmsmsm.weebly.com'. Both pages feature the 'Webmail' logo at the top. The left page has a 'Email address' field containing a redacted email and a 'Password' field with placeholder text. It includes a 'Login' button and a 'Reset Password' link. Language links at the bottom are: English, Deutsch, español de España, Dansk, Deutsch, italiano, and español. The right page has similar fields for 'Username' and 'Password', a 'Log in' button, and a 'Reset Password' link. Language links at the bottom are: العربية, čeština, dansk, Deutsch, Ελληνικά, español, español latinoamericano, español de España, and ...

Figura 4: Primeira página clonada

Figura 5: Segunda página clonada

### 4.3 Objetivo do Atacante

Com base no clone das páginas de login e na análise feita com o software BurpSuite, o phishing tinha como objetivo coletar as credenciais do alvo. O spoofing do email e seu uso como remetente facilita a exposição de credenciais e possível vazamento de dados em cadeia, comprometendo tanto a privacidade do alvo, quanto a dos clientes para os quais o alvo fornece serviços.

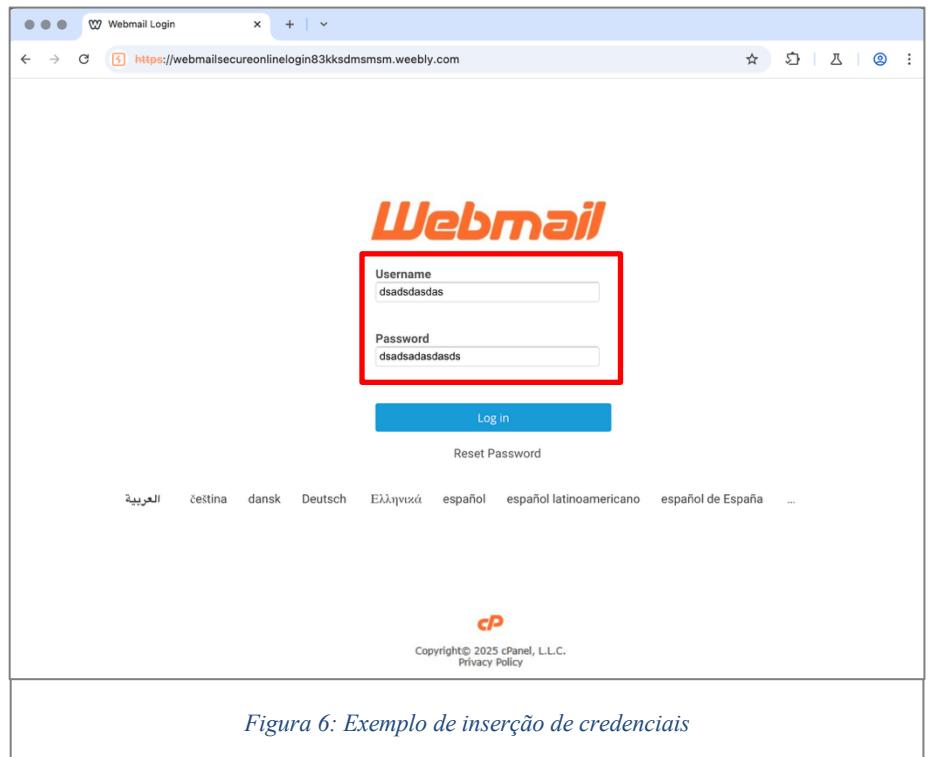


Figura 6: Exemplo de inserção de credenciais

Na Figura 7, observa-se que, ao clicar no botão Log in, as credenciais são enviadas em um request do tipo POST para um servidor malicioso, também identificado na imagem. Detalhe que as informações são enviadas em *plaintext*, ou seja, completamente sem criptografia.

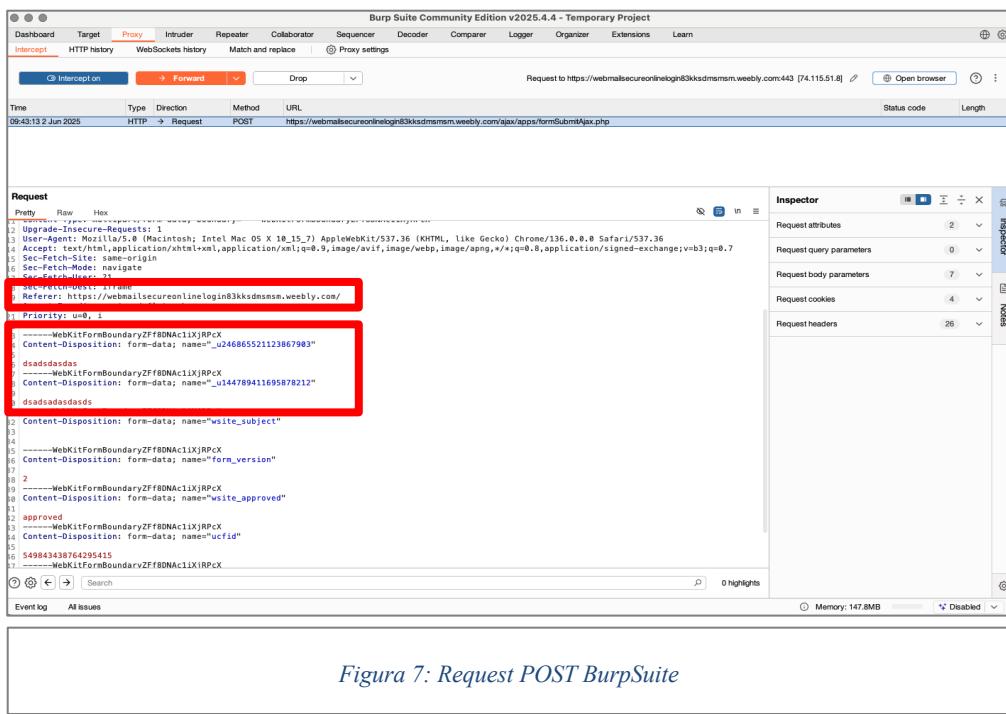


Figura 7: Request POST BurpSuite

## 5 Análise do Source Code – Primeira Tentativa de Phishing

Aqui será analisado o *source code* da primeira tentativa de phishing, onde será feita uma análise mais aprofundada das partes relevantes do header.

### 5.1 Cadeia de Recebimento

A cadeia de recebimento (*received chain*) é formada pelos servidores que manipularam o e-mail, incluindo o servidor do destinatário. Podemos fazer um rastreamento percorrendo o source code do e-mail na direção *top → bottom*.

No **top** está a conexão mais recente (geralmente o servidor do destinatário), enquanto que no **bottom** está a conexão mais antiga, ou seja, a do servidor que originou a comunicação.

A importância destes elementos reside no fato de que todos os endereços de IP dos servidores estão no *source code*, o que nos permite analisar o caminho feito pelo e-mail. Porém, isso nos dará apenas uma ideia do que pode ter ocorrido, já que os IPs não são uma fonte confiável de *intel*.

No **primeiro bloco** do email temos o último ponto de contato (servidor mais recente): cpanel-003-fra.hostingww.com, usando o protocolo LMTP. Este contato é o servidor do provedor de email do cliente.

```
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <hr@corridorconstructioniowa.cam>
Delivered-To: [REDACTED]
Received: from cpanel-003-fra.hostingww.com
        by cpanel-003-fra.hostingww.com with LMTP
        id EGKZEk+WC2jNvzYA2p0M4Q
        (envelope-from <hr@corridorconstructioniowa.cam>)
        for <[REDACTED]>; Fri, 25 Apr 2025 14:03:59 +0000
Return-path: <hr@corridorconstructioniowa.cam>
Envelope-to: [REDACTED]
Delivery-date: Fri, 25 Apr 2025 14:03:59 +0000
```

No **segundo bloco** temos outro servidor, de IP 148.113.172.133 e URL vps-58680c2d.vps.ovh.ca. Neste bloco o servidor de envio vps-58680c2d.vps.ovh.ca se anuncia ao servidor de recebimento usando o helo=mail.corridorconstructioniowa.cam, neste caso o servidor de recebimento aceitou receber o email. O helo funcionaria como um “handshake” e é uma parte essencial no protocolo SMTP, já que ele verifica a saúde dos servidores.

```

Received: from vps-58680c2d.vps.ovh.ca ([148.113.172.133]:46792
helo=mail.corridorconstructioniowa.cam)
    by cpanel-003-fra.hostingww.com with esmtps (TLS1.3) tls
TLS_AES_256_GCM_SHA384
    (Exim 4.98)
    (envelope-from <hr@corridorconstructioniowa.cam>)
    id 1u8Jep-0000000FOHA-1KmS
    for [REDACTED];
    Fri, 25 Apr 2025 14:03:59 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
    d=corridorconstructioniowa.cam; s=202502; t=1745589723;
    bh=27SJj8BZJ81+ac4w7EED3uS3UQaeMwpWWY+B6MYbbRw=;
    h=Reply-To:From:To:Subject:Date:From;
    b=FAC2py1yVLMWN9ryPZ2h9Argv0wFwdTBoyVrJVJdGURbFd0UVvg3e5ksvSTL7vg
Jz
8sFFfqSWvMdIGHzsF8nsO2ZbTjjts8Zfs5X3LdedHbrvTGdtM7R3Lcr5PnU4DFBdNv
5k/71bd4SzQ7nBr+6Zv5GIcBlyrynnUXWWY0+DQtJghyX/UtrwBmzYQXHnntiFjWi
hGkzuPxC99ekXfXs7+YyxaldUecvXG94sfhtl0QobsVgS0skIDuKZniOL5XJzFW2NG
JUGMv//or1NCpd/qWG6S179ChoIC8HOYFUNwsq59HO6CHiokaKqsZUp4i4Wde7z0px
6BPt3grCuM5Cw==
```

Neste caso, a ferramenta **virustotal** não sinalizou o domínio nem o IP, porém temos um achado importante relacionado ao IP 148.113.172.133:

```

Last HTTPS Certificate

Version: V3
Serial Number: 44b7fa66fb131cc97692a8cf0eb4bfe7ef3
Thumbprint: b3c9900fa0b35cfb1e3dede8df0a24496a1de2ab
Signature Algorithm:
Issuer: C=US O=Let's Encrypt CN=E5
Validity
Not Before: 2024-06-12 11:21:39
Not After: 2024-09-10 11:21:38
Subject: CN=referidos.packsporno.com
...
Authority Information Access:

OCSP - http://e5.o.lencr.org
CA Issuers - http://e5.i.lencr.org/
```

Aqui temos três pontos interessantes:

1. O CN está associado a um site duvidoso;
2. As autoridades certificadoras não são confiáveis;
3. O certificado está vencido.

Além disso, o email passou por outro país antes de chegar no servidor final, o WHOIS indica que o hosting está sendo feito no Canadá.

Um achado interessante é que o subdomínio que aparece no CN não retorna nenhuma flag maliciosa na inspeção com o **virustotal**, porém se fizermos uma busca pelo domínio, teremos algumas flags associadas aos IPs reconhecidos pelo pDNS (passive DNS, que é uma gravação histórica das resoluções DNS do domínio).

Passive DNS Replication (51) ⓘ			
Date resolved	Detections	Resolver	IP
2024-03-24	1 / 94	VirusTotal	45.139.122.160
2022-09-24	0 / 94	VirusTotal	172.67.135.234
2022-09-24	0 / 94	VirusTotal	104.21.7.87
2021-09-27	0 / 94	VirusTotal	103.224.212.219
2020-01-05	4 / 94	VirusTotal	70.32.1.32
2020-01-04	1 / 94	VirusTotal	170.178.168.203
2019-11-28	2 / 94	VirusTotal	103.224.212.222

Figura 8: Ips reconhecidos pelo pDNS

No **terceiro bloco**, e último contendo a tag Received, temos o primeiro servidor, o servidor que provavelmente gerou o email. O **virustotal** não tem nenhuma informação sobre a URL ip-134-38.dataclub.info, porém temos informações sobre o IP 84.38.134.38. O servidor está na Latvia, porém nenhum vendor sinalizou o IP nem como malicioso nem como não malicioso, o que é estranho.

```
Received: from ip-134-38.dataclub.info (unknown [84.38.134.38])
      by mail.corridorconstructioniowa.cam (Postfix) with ESMTPSA id
154A88D745
      for <[REDACTED]>; Fri, 25 Apr 2025 14:02:02 +0000 (UTC)
```

Também temos estas informações na aba DETAILS do **virustotal**, associadas ao IP:

```
role: DATCLUB SIA
address: Kraslavas iela 14 - 2
address: LV1003
address: Riga, Latvia
phone: +371 60-00-77-98
```

Uma breve pesquisa OSINT usando google maps nos retorna o seguinte:



Lembrando que não é possível dar certeza do endereço do servidor, pois o atacante poderia estar usando uma VPN, Tor, etc.

Ainda sobre o IP 84.38.134.38, temos uma informação importante: foram detectados mais de 10 arquivos incorporando este IP. Na aba RELATIONS do site **virustotal** temos 23 arquivos que fazem referência ao IP, sempre relacionados a arquivos de email, como mostra a imagem abaixo.

Scanned	Detections	Type	Name
2020-08-08	22 / 59	Email	2020-07-21-12:14:06:577948.qs
2020-08-08	22 / 60	Email	2020-07-21-13:10:32:137784.qs
2020-08-08	23 / 59	Email	2020-07-21-11:56:10:209775.qs
2020-08-08	23 / 59	Email	2020-07-21-12:42:07:288676.qs
2020-08-08	23 / 60	Email	2020-07-21-11:20:33:101137.qs
2020-08-08	23 / 60	Email	2020-07-21-12:15:29:548319.qs
2020-08-08	24 / 58	Email	2020-07-21-11:46:23:794601.qs
2020-08-08	24 / 59	Email	2020-07-21-12:09:16:998593.qs
2020-08-08	22 / 59	Email	1595402296.S.112140.2421.pro-236-98.eml
2020-08-08	23 / 59	Email	2020-07-21-11:10:02:268298.qs
2020-08-08	24 / 58	Email	2020-07-21-11:44:891716.qs
2020-07-24	18 / 59	Email	2020-07-21-13:11:59:028827.qs
2020-07-24	17 / 58	Email	2020-07-21-12:50:08:947100.qs
2020-08-08	21 / 57	Email	2020-07-21-12:50:32:320575.qs
2020-08-08	23 / 59	Email	2020-07-21-12:19:24:775183.qs
2020-08-08	23 / 58	Email	2020-07-21-12:10:47:801167.qs
2020-07-22	14 / 57	Email	mail_1595318480_23254.eml
2020-07-24	17 / 59	Email	2020-07-21-11:11:30:420038.qs
2020-07-24	17 / 59	Email	2020-07-21-11:21:57:838596.qs
2020-07-22	2 / 58	Email	문서.eml

**Figura 10: Arquivos que incorporam o IP 84.38.134.38**

Todos os arquivos estão relacionados à detecção de trojan. Infelizmente não podemos ter certeza de qual trojan estaria sendo usado, pois as flags abaixo são generalistas, são flags levantadas quando um arquivo possui um comportamento parecido a um trojan. Também não podemos inferir que algum malware está associado ao link do e-mail.

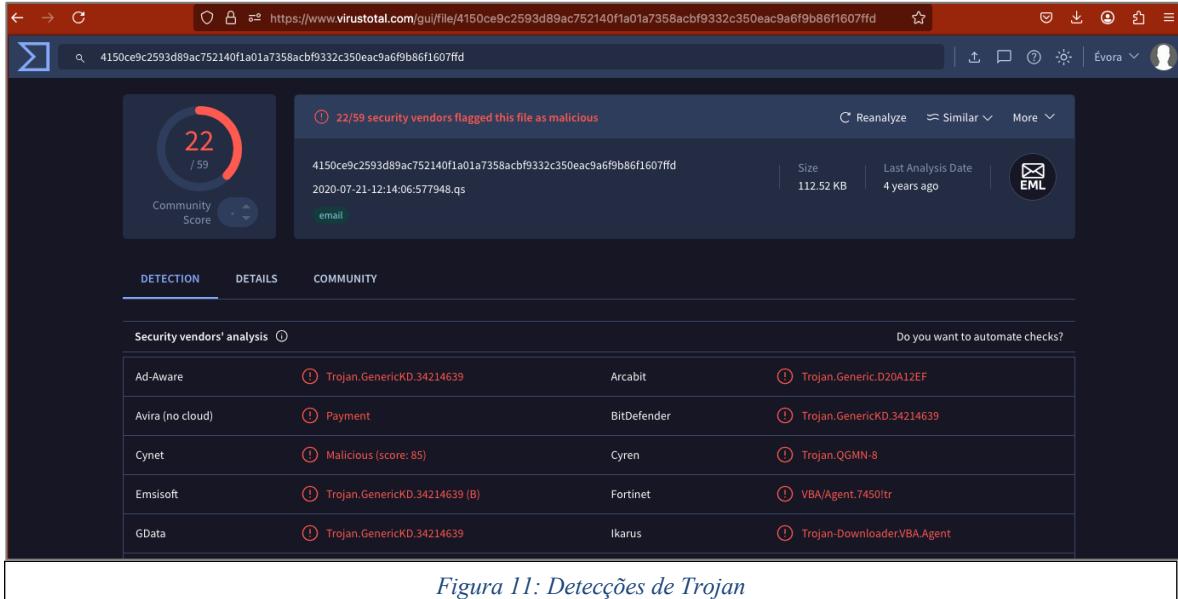


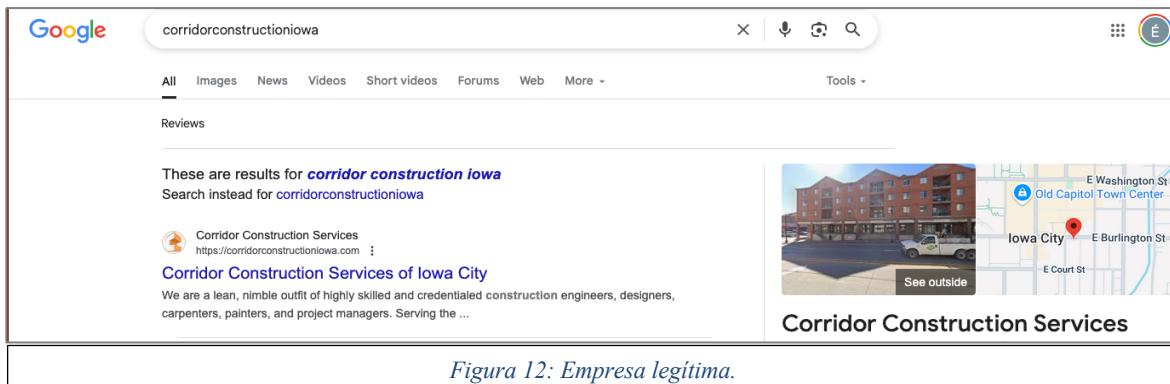
Figura 11: Detecções de Trojan

## 5.2 Caminho de Retorno

O caminho de retorno (Return-path) é o endereço usado para enviar o email. Podemos vê-lo no **primeiro bloco** do *source code*, em verde.

```
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <hr@corridorconstructioniowa.cam>
Delivered-To: [REDACTED]
Received: from cpanel-003-fra.hostingww.com
        by cpanel-003-fra.hostingww.com with LMTP
        id EGKZEk+WC2jNvzYA2p0M4Q
        [(envelope-from <hr@corridorconstructioniowa.cam>)]
        for <[REDACTED]>; Fri, 25 Apr 2025 14:03:59 +0000
Return-path: <hr@corridorconstructioniowa.cam>
Envelope-to: [REDACTED]
Delivery-date: Fri, 25 Apr 2025 14:03:59 +0000
```

O e-mail `hr@corridorconstructioniowa.cam` pode até existir, mas o site `corridorconstructioniowa.cam` não. O interessante é que a empresa existe e é legítima, mas parece que sofreu um TLD-squatting e estão usando o domínio de forma maliciosa.



*Figura 12: Empresa legítima.*

### 5.3 Conclusão da Análise do Source Code

Com os indicativos que temos, o atacante usou **pretexto** como tática de engenharia social, **autoridade** ao usar um email supostamente do RH e **urgência**, ao enviar um email de acesso indevido.

Adicionalmente, a mudança no **TLD** é uma técnica conhecida como **combo-squatting** ou **TLD-squatting**, onde se utiliza o nome do domínio legítimo, neste caso corridorconstructioniowa, mas se altera o **TLD**, no nosso caso para .cam. Isso pode induzir o usuário ao erro, e interagir com o link potencialmente malicioso.

## 6 Análise do Link Usando Hybrid Analysis – Primeira Tentativa de Phishing

Como já explicado no tópico “4 Análise do Design”, os botões redirecionavam para um link, no caso:

ipfs[.]io/ipfs/bafybeibdiuiyka... (o link está *defanged*, ou seja, inválido para evitar um clique acidental, para torná-lo ativo usar o [cyberchef](#)).

Neste tópico foi usado a ferramenta [Hybrid-Analysis](#), a qual foi criada pela Payload Security e agora faz parte do CrowdStrike. Serve para análise de arquivos e URLs e usa ambientes do tipo *sandbox* com o objetivo de detectar comportamentos maliciosos sem comprometer a infraestrutura local.

O usuário faz o upload de um arquivo ou link, a ferramenta o executa em uma VM controlada e registra os resultados da interação com o arquivo/link, como:

- Análise comportamental (mudanças no registry, conexões de rede, processos, criações de arquivos);

- Indicadores de Comprometimento (IoCs);
- Comportamento de rede (resquests DNS, tráfego HTTP/HTTPS, IPs contactados);
- Mapeamento das Táticas, Técnicas e Procedimentos (TTPs) usando o Mitre ATT&CK;
- Resultados de escaneamento de antivírus usando o virustotal.

Foram examinadas as seguintes sessões da página carregada após o envio do link:

- Analysis Overview
- Anti-virus (AV) Scanner Results
- Falcon Sandbox Reports
- Relations
- Incident Response
- Additional Context

## 6.1 Analysis Overview

A primeira análise foi feita em março. Até 29 de abril a análise retornava a *flag no specific threat*, como podemos observar na figura abaixo:

**Analysis Overview**

**no specific threat**

AV Detection: Marked as clean

X Post ⌂ Link ⌂ E-Mail

[Overview](#) [Copy Sample SHA256](#) [Copy Sample Name/URL](#) [Downloads](#) [External Reports](#) [Re-analyze](#) [Hash Not Seen Before](#) [Request Report Deletion](#)

Figura 13: Link do primeiro phishing.

Em 26 de maio foi realizada uma nova análise e a *flag* mudou para **malicious**. A depender do ambiente da sandbox, a flag muda para *ambiguous*. Neste último caso o antivírus detecta o link como malicioso, mas a sandbox não encontra nenhum comportamento estranho.

**Analysis Overview**

**malicious**

AV Detection: 22%

X Post ⌂ Link ⌂ E-Mail

[Request Report Deletion](#)

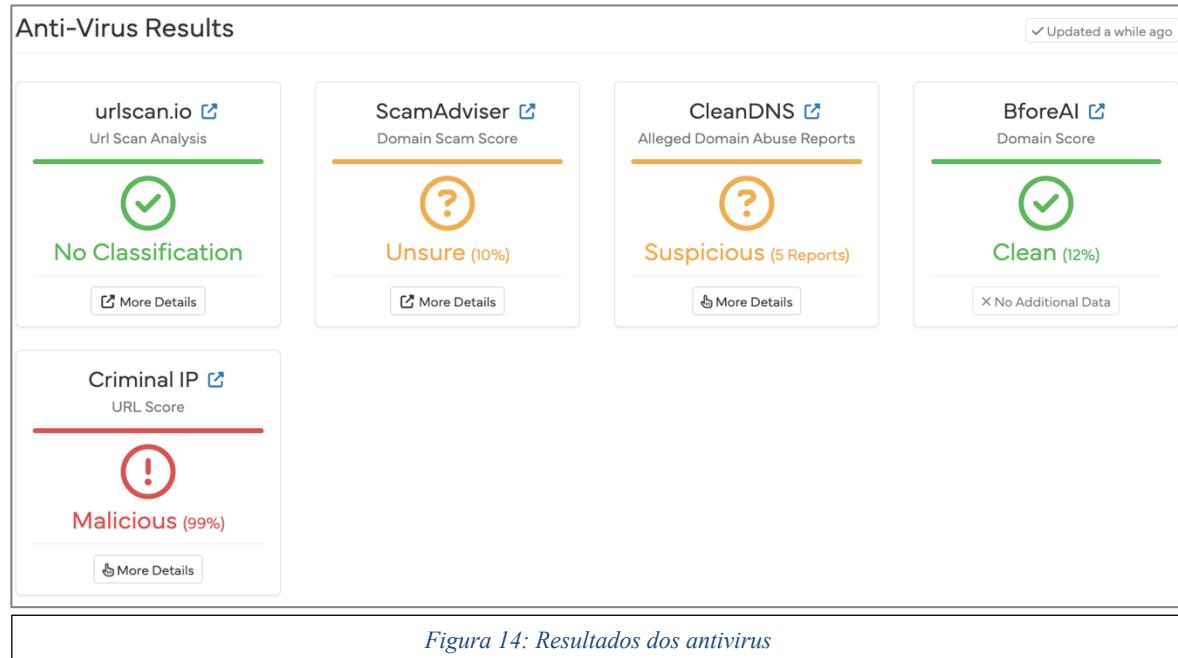
Submission name:	hxps://ipfs.io/ipfs/bafybeibdiuiykafjy2s7w56jqreby4xbp4mzmpupbchz5spu6tsbitera u
Size:	104B
Type:	url
Mime:	application/x-mswinurl
Submitted At:	2025-04-29 13:39:50 (UTC)
Last Anti-Virus Scan:	2025-05-26 07:50:35 (UTC)
Last Sandbox Report:	2025-04-30 10:29:56 (UTC)

0 Community Score 0

Figura 14: Análise do dia 26 de maio.

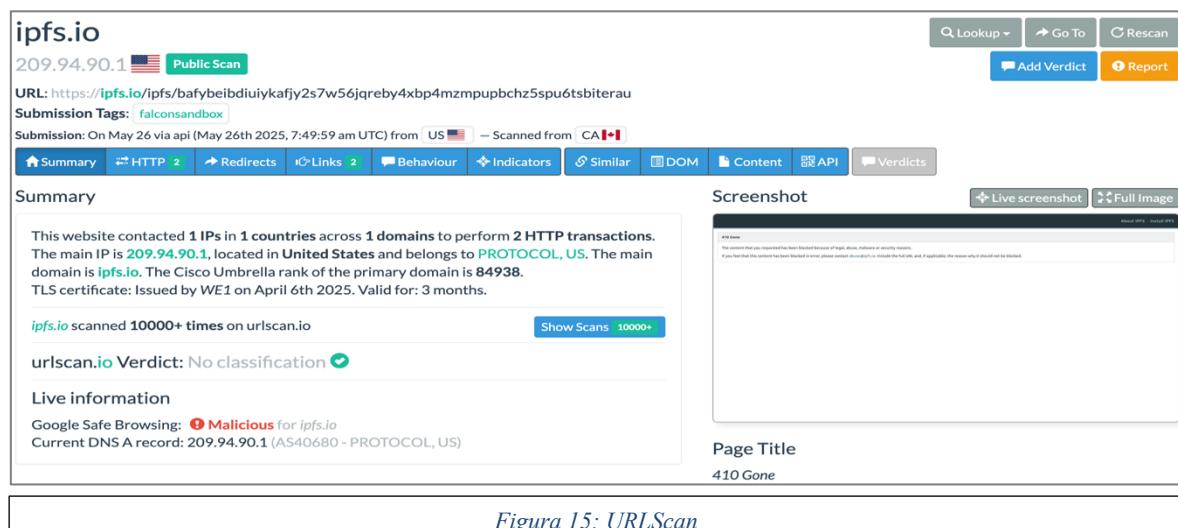
## 6.2 AV Scanner Results

A ferramenta faz o escaneamento da URL usando cinco ferramentas, são elas urlscan.io, ScamAdviser, CleanDNS, BforeAI e Criminal IP.



### 6.2.1 Urlscan.io

Esta ferramenta registra a atividade de rede do IP, o conteúdo da página, os metadados e também faz uma análise comportamental com o objetivo de detectar phishing. Neste caso, Hybrid-Analysis retorna a flag **No Classification**, mas se clicarmos em **More Details** teremos duas informações: o Google Safe Browsing sinalizou o domínio como **malicioso** e a página tem status HTTP 410:



## 6.2.2 ScamAdviser

Esta ferramenta é baseada em votos da comunidade. Os reports de que é um scam são recentes, por isso a flag Unsure (10%).

## 6.2.3 CleanDNS

The screenshot shows a modal window titled "Alleged User-Reported Domain Abuse from CleanDNS (5)". It displays a table of abuse reports with columns "Alleged User-Reported Domain Abuse" and "Reported At". The data is as follows:

Alleged User-Reported Domain Abuse	Reported At
Alleged Phishing	2025-03-13 00:00:00 (UTC)
Alleged Phishing	2024-10-20 00:00:00 (UTC)
Alleged Phishing	2024-10-11 00:00:00 (UTC)
Alleged Phishing	2024-10-10 20:49:04 (UTC)
Alleged Phishing	2024-06-10 00:00:00 (UTC)

At the bottom right of the modal is a "Close" button.

*Figura 16: Relatório do CleanDNS*

Os usuários do CleanDNS reportaram que o domínio está sendo abusado.

## 6.2.4 Criminal IP

The screenshot shows a modal window titled "URL Scan Report Summary for Criminal IP". It displays the following information:

- URL**:
  - DGA Score: 1.264
  - Probability of Phishing: 99.97%
- Common**:
  - Fake Domain: No
  - Invalid SSL: No
  - MITM Attack: No
  - Abuse Record: -
  - Phishing Record: ① 2
- HTML**:
  - Suspicious Program: 0
  - Suspicious HTML Element: 0
  - Credential Input Form: Safe
- Network**:
  - Suspicious Cookie: No

At the bottom right of the modal is a "Close" button.

*Figura 17: Relatório Criminal IP*

O scan do Criminal IP sugere que existe uma probabilidade de 99,97% do link estar relacionado a ataques de phishing.

## 6.3 Falcon Sandbox Reports

Por *default*, Hybrid-Analysis usa três sandboxes:

- Windows 7 32bit (Win7)
- Windows 10 64bit (Win10)

- Windows 11 64bit (Win11)

Farei uma análise crítica comparativa dos indicadores encontrados nos três Sistemas Operacionais (OS), a partir disso será discutida a análise relacionada ao OS mais provável como alvo do ataque.

### 6.3.1 Indicadores Suspeitos

Na primeira parte do relatório gerado pelo Hybrid-Analysis, temos a sessão *Indicators*. Nesta sessão encontramos os indicadores que apontam para uma possível tática, técnica e procedimento (TTP) usados. Estes resultados vêm da execução da URL dentro do ambiente da sandbox, então podemos acompanhar o que ocorre ao clicar no link.

Na tabela da próxima página, é possível ver que **os três OS tiveram alertas do Suricata**. O Suricata é uma ferramenta de análise de rede e detecção de ameaças *open source*, é um software de IDS/IPS. Neste caso o alerta tem relação com compartilhamento de arquivos via P2P, ou seja, existe um tráfego IPFS.

Para além dos alertas do Suricata, o Win7 não gera nenhum outro alerta inicial, então continuaremos com o próximo sistema, o Win10.

O Win10 gerou um alerta interessante associado ao Att&ck ID T1114, que se relaciona à tática de “Coleta” e mais especificamente à “Coleta de Email”. Na matriz Mitre ATT&CK, esta tática está relacionada à coleta de informações sensíveis usando o e-mail de um alvo qualquer.

#### WINDOWS 7 32

<b>Detected suricata alert</b>
Details
Detected alert "et file_sharing observed peer-to-peer file sharing service domain (ipfs .io in tls sni)" (sid: 2036874, rev: 3, severity: 2) categorized as "potentially bad traffic" detected alert "et file_sharing peer-to-peer file sharing service domain in dns lookup (ipfs .io)" (sid: 2036873, rev: 5, severity: 2) categorized as "potentially bad traffic"
Source
Suricata alerts
Relevance
10/10

#### WINDOWS 10 64

<b>Detected suricata alert</b>
Details
Detected alert "et file_sharing peer-to-peer file sharing service domain in dns lookup (ipfs .io)" (sid: 2036873, rev: 5, severity: 2) categorized as "potentially bad traffic" detected alert "et file_sharing observed peer-to-peer file sharing service domain (ipfs .io in tls sni)" (sid: 2036874, rev: 3, severity: 2) categorized as "potentially bad traffic"
Source
Suricata alerts
Relevance
10/10
<b>Found a potential e-mail address in binary/memory</b>
Details

	Pattern match: "abuse@ipfs.jo"
Source	File/memory
Relevance	3/10
Att&ck id	T1114

## WINDOWS 11 64

### Detected suricata alert

Details	Detected alert "et file_sharing observed peer-to-peer file sharing service domain (ipfs .io in tls sni)" (sid: 2036874, rev: 3, severity: 2) categorized as "potentially bad traffic" detected alert "et file_sharing peer-to-peer file sharing service domain in dns lookup (ipfs .io)" (sid: 2036873, rev: 5, severity: 2) categorized as "potentially bad traffic"
Source	Suricata alerts
Relevance	10/10

### Posts data to a webserver

Details	"post /api/report?cat=bingbusiness http/1.1 host: bzip.netreports.net connection: keep-alive content-length: 461 content-type: application/reports+json user-agent: mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/121.0.0.0 safari/537.36 edg/121.0.0.0 accept-encoding: gzip, deflate, br accept-language: en-us,en;q=0.9" with payload:<=> [{"age":5,"body":{"elapsed_time":1875,"method":"get","phase":"application","protocol":"h2","referrer":"","sampling_fraction":1.0,"server_ip":"13.107.6.158","status_code":401,"type":"http.error"},"type":"network-error","url":"https://business.bing.com/work/api/v2/tenant/my/settingswithflights?&clienttype=edge-omnibox","user_agent":"mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/121.0.0.0 safari/537.36 edg/121.0.0.0"}]" http/1.1 200 ok content-length: 0 server: kestrel date: wed 30 apr 2025 10:30:38 gmt connection: keep-alive pmuser_format_qs: x-cdn-traceid: 0.65a13617.1746009038.113389c access-control-allow-headers: * access-control-allow-credentials: false access-control-allow-methods: get options post access-control-allow-origin: * with no response body "post /api/report?cat=bingbusiness http/1.1 host: bzip.netreports.net connection: keep-alive content-length: 456 content-type: application/reports+json user-agent: mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/121.0.0.0 safari/537.36 edg/121.0.0.0 accept-encoding: gzip, deflate, br accept-language: en-us,en;q=0.9" with payload:<=> [{"age":60003,"body":{"elapsed_time":1883,"method":"get","phase":"application","protocol":"h2","referrer":"","sampling_fraction":1.0,"server_ip":"13.107.6.158","status_code":401,"type":"http.error"},"type":"network-error","url":"https://business.bing.com/api/v1/user/token/microsoftgraph?&clienttype=edge-omnibox","user_agent":"mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/121.0.0.0 safari/537.36 edg/121.0.0.0"}]" http/1.1 200 ok
---------	---

```
content-length: 0
server: kestrel
date: wed
30 apr 2025 10:31:38 gmt
connection: keep-alive
pmuser_format_qs:
x-cdn-traceid: 0.65a13617.1746009098.114a192
access-control-allow-headers: *
access-control-allow-credentials: false
access-control-allow-methods: get
options
post
access-control-allow-origin: * with no response body
Source
Network traffic
Relevance
5/10
Att&ck id
T1041
```

Agora seguimos com o Win11, que demonstrou ter um comportamento mais avançado, em se tratando de um ataque. **E quais os indicadores deste comportamento?**

O Att&ck ID T1041 está relacionado à “Exfiltração de dados através de canais C2”. Vale ressaltar que C2 é um acrônimo para *Command and Control*, e está associado às ferramentas e técnicas que atacantes usam para manter a comunicação com a infraestrutura alvo.

Ao clicar no link usando o Win11, a rede do alvo faz um request do tipo POST, usando JSON, para um servidor web: host: bzib.nelreports.net. O que isso significa? Como mostrado no início desse relatório, a página era uma cópia exata da página de login do webmail da empresa. Se o usuário colocasse suas credenciais, provavelmente elas iriam para o servidor do atacante.

---

## 7 Nova Série de Ataques, junho | 2025 – Segunda Tentativa de Phishing

No início de junho, a empresa recebeu o mesmo tipo de ataque. Em um único dia receberam 7 emails de phishing com o mesmo pretexto. Um detalhe muito importante, o atacante usou o **mesmo** domínio do e-mail corporativo do alvo, um indicativo de spoofing de e-mail do seu próprio domínio. Mas, diferente do ataque passado que usou um e-mail com TLD squatting de outra empresa, neste caso não houve indícios de typosquatting nem nenhuma outra técnica, era realmente um spoofed e-mail se passando por um e-mail de suporte.

A análise com a sandbox do Hybrid-Analysis não retornou nada, provavelmente por ser uma campanha de phishing recente. Os atacantes tem a tendência de criar novos domínios com tempo de vida curto para não serem rastreados, não dando tempo das ferramentas de análise sinalizarem o link como malicioso.

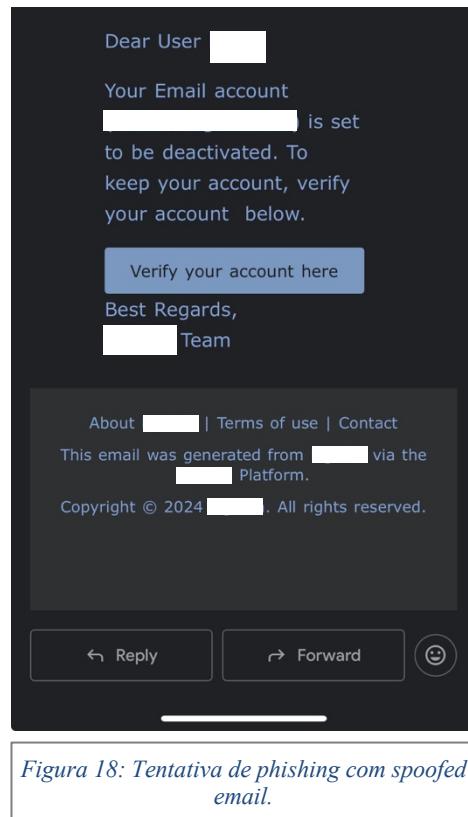


Figura 18: Tentativa de phishing com spoofed email.

Até o dia 03 de junho o link funcionava, agora, além da página não existir mais, já está sendo sinalizada pelo Google Safe Browsing como um site malicioso.

O link do botão `Verify your account here` desta vez não é um link de compartilhamento via IFPS, mas sim um provedor de domínio legítimo, o Weebly. Este provedor possui um [histórico](#) de ser host para sites de phishing, assim como [vários outros](#).

Link do botão

```
http://webmailsecureonline[.]com/login83kksdmsmsm[.]weebly[.]com/
```

A análise do link no **virustotal** retornou que duas plataformas sinalizaram como url maliciosa. Porém, não tinha nenhuma informação importante, já que os DETAILS estavam associados ao provedor usado, e não ao atacante.

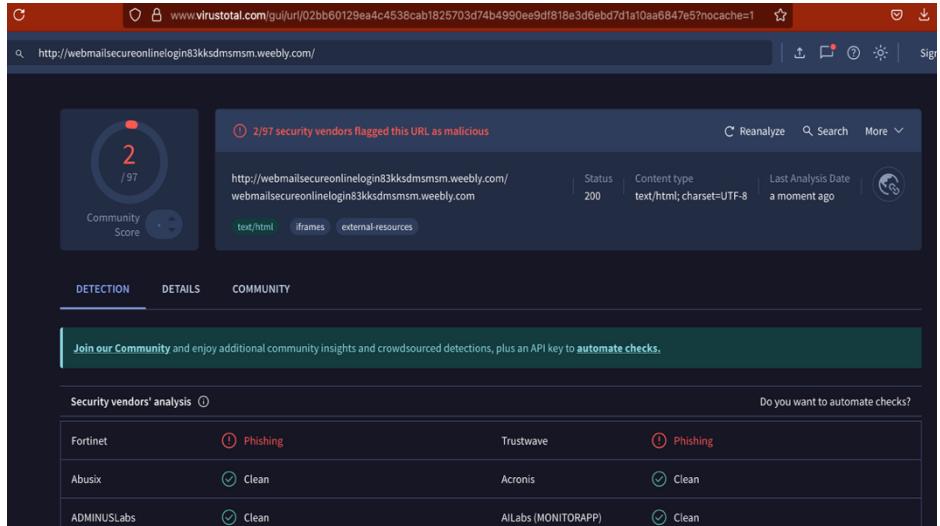


Figura 19: Análise do link no virustotal

## 7.1 Análise com BurpSuite

Como nada foi encontrado nas ferramentas **virustotal** e **Hybrid-Analysis**, resolvi fazer a análise dos *requests* feitos via HTTP usando o **BurpSuite**.

Assim que a página do link malicioso é carregada, o request abaixo é feito. Na linha 09, é um request do tipo XMLHttpRequest é um tipo de AJAX/XHR call, carregam geralmente payloads do tipo JSON via função Javascript, os quais são enviados no background da aplicação, sem que a página carregue. Foi feito uma conexão com a api do servidor do atacante.

```

09 X-Requested-With: XMLHttpRequest
10 vUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
    AppleWebKit/537.36. (KHTML, Like Gecko) Chrome/136.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript. /: 9=0.01
12 Content-Type: application/json; charset=UTF-8
13 Origin: https://webmailsecureonlinelogin83kksdmsmsm.weebly.com
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://webmailsecureonlinelogin83kksdmsmsm.weebly.com/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20
21 }
"jsonrpc": "2.0",
"method": "CustomerAccounts::getAccountDetails", v
"params": [
],
"id": 0
}

```

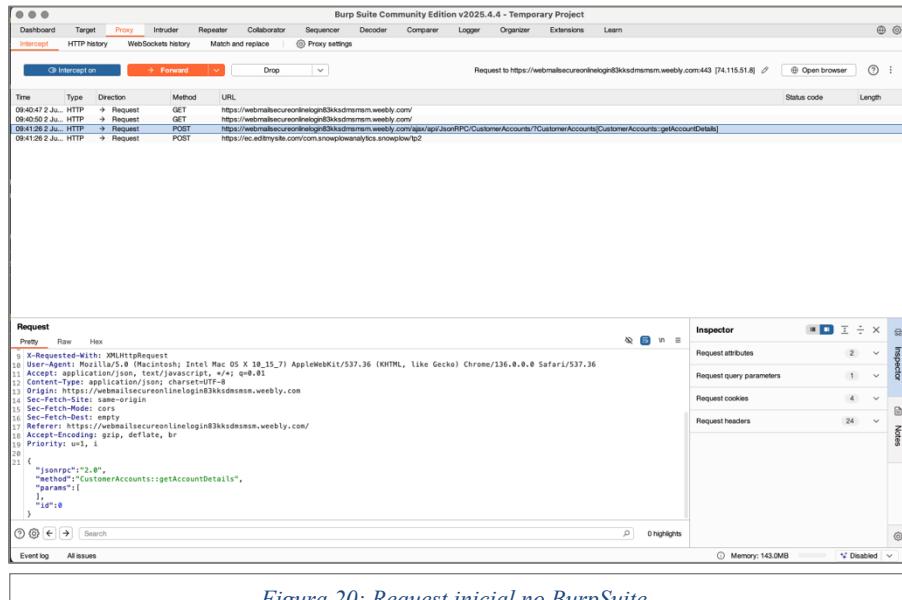


Figura 20: Request inicial no BurpSuite.

Na página, foram colocadas as credenciais **usuário** e **senha** com o objetivo de detectar algo no backend da aplicação. Como mostrado na figura abaixo, foi feito um request POST para o servidor AJAX do site malicioso, contendo as credenciais em *plaintext*. Aqui, fica óbvio que o objetivo do ataque era a coleta de credenciais.

```
-----WebKitFormBoundaryn0bKEInDC04Bsm9e
Content-Disposition: form-data; name="__U246865521123867903"
usuario
-----WebKitFormBoundaryn0bKEInDC04Bsm9e
Content-Disposition: form-data; name=__U144789411695,878212"
senha
```

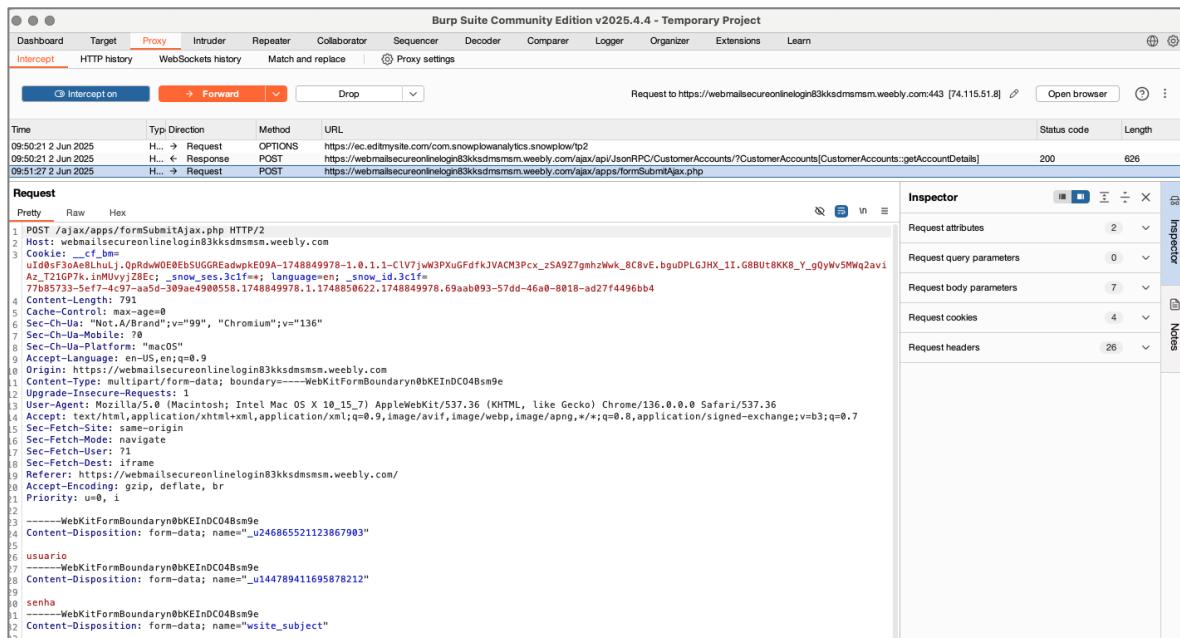


Figura 21:POST request com credenciais falsas.

## 8 Rastreamento de Vulnerabilidades

### 8.1 Email Spoofing

O e-mail spoofing ocorre quando um atacante envia um e-mail se passando por um e-mail ou domínio legítimo. Diferente da técnica de TLD squatting que vimos no primeiro caso de phishing, neste caso o atacante forja o `From:` ou outros campos do header do e-mail.

Para exemplificar o ocorrido, como usamos MSolutions como o codinome da empresa, vamos supor que o domínio da empresa seja `msolutions.com`. O atacante usou um email [no-reply@msolutions.com](mailto:no-reply@msolutions.com), ou seja, cai na característica de ser um spoofed mail. Este email não foi reconhecido pelo servidor do alvo como spam. Existe aí uma falha do próprio domínio e webserver do alvo, pois se o domínio tivesse as proteções necessárias, o servidor do usuário iria reconhecer este spoofed mail como ilegítimo e o recebimento seria rejeitado, no mínimo. Mas, como isso não ocorreu, é prova suficiente para supor que o webmail nem o domínio do alvo estavam protegidos. Então, quais proteções são necessárias para evitar um spoofing de email corporativo?

Existem mecanismos de defesa a serem implementados para que o uso indevido de um domínio seja evitado, são eles: Sender Policy Framework - SPF, DomainKeys Identified Mail - DKIM e Domain-based Message Authentication, Reporting & Conformance - DMARC. Veremos em seguida com detalhes cada um.

The screenshot shows the cPanel Email Deliverability interface. On the left sidebar, there are links for Tools, Sitejet Builder, WordPress Management, and Manage Team. The main content area has a title 'Email Deliverability' and a sub-section 'List Domains'. A search bar is at the top right. Below it, a message says: 'Use this interface to reduce the number of emails sent from this server that end up in spam folders. For more information, read our [Email Deliverability](#) documentation.' A large red box covers most of the content area. At the bottom, a yellow warning message reads: '⚠ Problems Exist (DMARC and DKIM)'. There are 'Repair' and 'Manage' buttons next to it. The footer includes the cPanel logo and version 126.0.16, along with links for Home, Trademarks, Privacy Policy, Documentation, and Give Feedback.

Figura 22: Servidor do alvo, com problemas de configuração de DKIM e DMARC.

## 8.2 SPF

Este framework funciona como um mecanismo de autenticação. Ele permite que o proprietário do domínio publique, no DNS, uma especificação de quais endereços de IP ou hostnames podem enviar emails em nome do domínio. Por *default*, o protocolo de envio de email SMTP não verifica o remetente do email, então um atacante com acesso a qualquer servidor de email pode, simplesmente, usar o campo `From:` do header do email com qualquer email criado usando o domínio do alvo. Como isto é possível?

No nosso caso, o atacante colocou um endereço arbitrário no `From`, usando o domínio do próprio alvo `no-reply@msolutions.com`, lembrando que este endereço na verdade não existe. Esta **vulnerabilidade** na configuração do SPF do servidor web do alvo foi explorada pelo atacante. A “sorte” do alvo é que a empresa é pequena e o CEO, quem recebeu o email, sabe quais emails existem na empresa.

O SPF é colocado na configuração do DNS no registro TXT-Record do domínio principal, que seria, em nosso caso `msolutions.com`.

**Na plataforma do domínio o SPF estava configurado:**

```
v=spf1 +mx +a +ip4:3.X.X.X +include:mail.dominio.com ~all
```

## 8.3 DKIM

O DKIM é um método de autenticação de email, onde o destinatário verifica que um servidor de email autorizado “assinou”, com uma chave criptográfica, a mensagem recebida. Também garante a integridade da mensagem contra adulteração.

O servidor de email gera um par de chaves pública/privada. A chave pública deve ser publicada no servidor DNS, também no registro TXT-record, mas desta vez no sub-domínio correspondente: `default._domainkey.msolutions.com`. Com um DKIM registrado, o cliente quando envia um email do seu servidor de email autorizado, tem esse email assinado com a chave privada. Quando este email chega ao servidor de destino, este extrai o domínio que está no header e busca via DNS a chave DKIM pública deste domínio, recalculando assim o hash gerado pela assinatura e verificando que a mensagem é legítima.

**Na plataforma DNS do domínio o DKIM não estava configurado.** Isso torna o spoofing do domínio de email muito mais fácil para o atacante, e foi o que aconteceu.

Além disso, o atacante pode usar spoofed emails para clientes, se passando pelo proprietário do domínio. Alguns servidores de email não entregam emails sem o DKIM configurado, então isso pode impedir também o envio de emails legítimos.

Figura 24: Configuração DKIM

O DKIM foi implementado no domínio da empresa da seguinte maneira. Foi gerado uma chave DKIM no provedor de email e no domínio DNS, no registro, foi adicionado um domínio default.\_domainkey e nele adicionado um registro TXT com o valor da chave pública. Com a configuração correta, o provedor de email retorna que o domínio agora possui um DKIM válido.

## 8.4 DMARC

O DMARC é uma política publicada no DNS, avisando aos servidores de email dos destinatários como lidar com emails que falham na checagem do SPF e/ou do DKIM. É uma política que deve ser publicada no DNS do cliente.

As políticas usadas no DMARC são `none`, para que quando algum email recebido falhe as checagens o servidor não faça nada; `quarantine`, neste caso o email vai para caixa de spam; e `reject`, para que o email seja recebido.

Para possuir uma política DMARC, o DNS precisa ter SPF e DKIM configurados. Como neste caso o alvo não possuía registro DKIM, o **DMARC também não estava configurado**.

O uso do DMARC também possibilita adicionar emails para enviar resumos diários (parâmetro `rua`) e relatórios forense (parâmetro `ruf`) caso o DMARC encontre uma falha, como no exemplo:

```
v=DMARC1; p=quarantine; rua=mailto:dmarc-aggregate@msolutions.com;
ruf=mailto:dmarc-forensic@msolutions.com
```

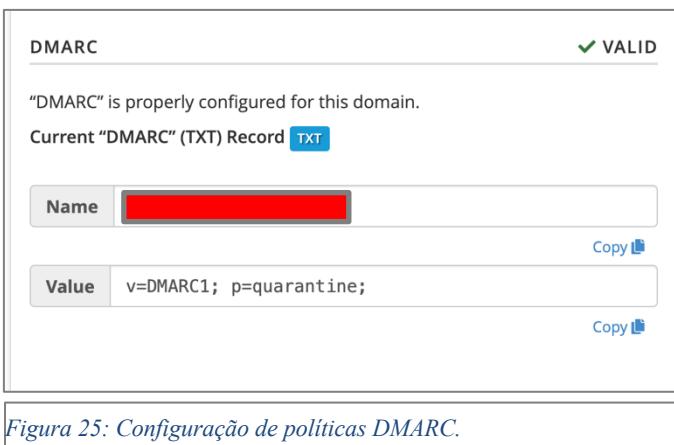


Figura 25: Configuração de políticas DMARC.

Também foi configurada a política DMARC no registro DNS do domínio, neste caso foi usado o padrão acima. A imagem ao lado ilustra que uma política simples também retorna como válido. Para que o DMARC seja registrado, é necessário que o domínio tenha primeiro o DKIM válido.

## 9 Conclusão

Todas as empresas, pequenas e grandes, estão sujeitas a um ataque de spoofing. Com o propósito de evitar o vazamento de credenciais via phishing, protegendo assim a privacidade dos usuários/clientes e também a integridade da empresa, devem ser implementados controles de autenticação de email (SPF, DKIM e DMARC) e monitoramento.

Estes controles reforçam a **confidencialidade, integridade e disponibilidade**, pilares da segurança da informação, na empresa. E, ao impedir o spoofing de emails e domínios, estes controles reduzem a probabilidade de vazamento de credenciais da empresa, impediendo que:

- Os colaboradores tenham seus dados expostos por ataques de phishing (confidencialidade);
- Os sistemas fiquem indisponíveis em caso de invasão ocasionada por credenciais vazadas (disponibilidade);
- Garante a integridade dos emails enviados pela empresa (integridade);
- E garante que atacantes não usem o domínio da empresa para ataques futuros, que podem inclusive comprometer os clientes da empresa.

## Bibliografia

SpamHaus Project. **Understanding the source code of a malicious email.** Disponível em:  
<https://www.spamhaus.org/resource-hub/email-security/understanding-the-source-code-of-a-malicious-email/#lessstronggreatermore-email-source-code-elementslessstronggreater>

<https://www.virustotal.com/gui/domain/cpanel-003-fra.hostingww.com>

<https://www.virustotal.com/gui/domain/vps-58680c2d.vps.ovh.ca>

<https://www.virustotal.com/gui/ip-address/148.113.172.133/details>

<https://www.virustotal.com/gui/ip-address/84.38.134.38/details>

<https://www.virustotal.com/gui/ip-address/84.38.134.38/relations>

Cyber Security Ventures. **Top-level domain squatting victims and how to combat the threat.** Disponível em: <https://cybersecurityventures.com/top-level-domain-squatting-victims-and-how-to-combat-the-threat/>

EclecticIQ, G. Rafael. **Financially motivated threat actor leveraged google docs and weebly services to target telecom and financial sectors.** Disponível em:  
<https://blog.eclecticiq.com/financially-motivated-threat-actor-leveraged-google-docs-and-weebly-services-to-target-telecom-and-financial-sectors>

Palo Alto Networks. **Legitimate saas platforms being used to host phishing attacks.** Disponível em: <https://unit42.paloaltonetworks.com/platform-abuse-phishing/>

<https://www.virustotal.com/gui/url/02bb60129ea4c4538cab1825703d74b4990ee9df818e3d6ebd7d1a10aa6847e5/community>