




heimdall
security research

A DIVISION OF ISH



Stealer para Google Chrome, Rilide



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

[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](#)



ISH
CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH
ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH
GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

Sumário

1	Infecção por meio de PowerPoint.....	6
2	Campanha V3 Rilide com bypass no Manifest.....	11
3	Referências.....	13

Lista de Figuras

Figura 1 – Exemplo de página de phishing do HSBC.....	7
Figura 2 – Documento de ppt criado para orientar os usuários na instalação do Rilide.	8
Figura 3 – Cadeia de infecção para campanhas do Rilide.	9
Figura 4 – Adaptação para distribuição do malware.....	12

1 INFECÇÃO POR MEIO DE POWERPOINT

Recentemente foi descoberta uma extensão maliciosa do navegador **Rilide Stealer Chrome** retornando em novas campanhas direcionadas a usuários criptográficos e funcionários corporativos para roubar credenciais e carteiras criptográficas.

O malware Rilide é uma extensão de navegador maliciosa para navegadores baseados em Chromium, incluindo Chrome, Edge, Brave e Opera na qual a Trustwave SpiderLabs descobriu inicialmente em abril de 2023.

A referida empresa descobriu que uma nova versão do Rilide que agora suporte a Chrome Extension Manifest V3, permitindo superar as restrições introduzidas pelas novas especificações de extensão do Google e adicionando ofuscação de código adicional para evitar a detecção.

Ocorre que a versão mais recente do malware Rilide agora também visa contas bancárias, sendo possível agora exfiltrar os dados roubados por meio de um canal do Telegram ou capturando telas em intervalos pré-determinados e enviando-os ao servidor C2.

O referido malware está se espalhando em várias campanhas e, como o malware é vendido em fóruns de hackers, é provável que acabam sendo utilizados por diferentes agentes de ameaças. A campanha visa vários bancos, provedores de pagamentos, provedores de serviços de e-mail, plataforma de criptomoedas, VPNs e provedores de serviços em nuvem, utilizando scripts de injeção, com foco principalmente em usuários na Austrália e Reino Unido.

A referida campanha utilizou mais de 1.500 páginas de phishing utilizando domínios *typosquatting*, promovidos por envenenamento de SEO em mecanismos de pesquisa confiáveis e personificando os bancos e provedores de serviços para induzir as vítimas a inserir suas credenciais de contas em formulários de phishing.

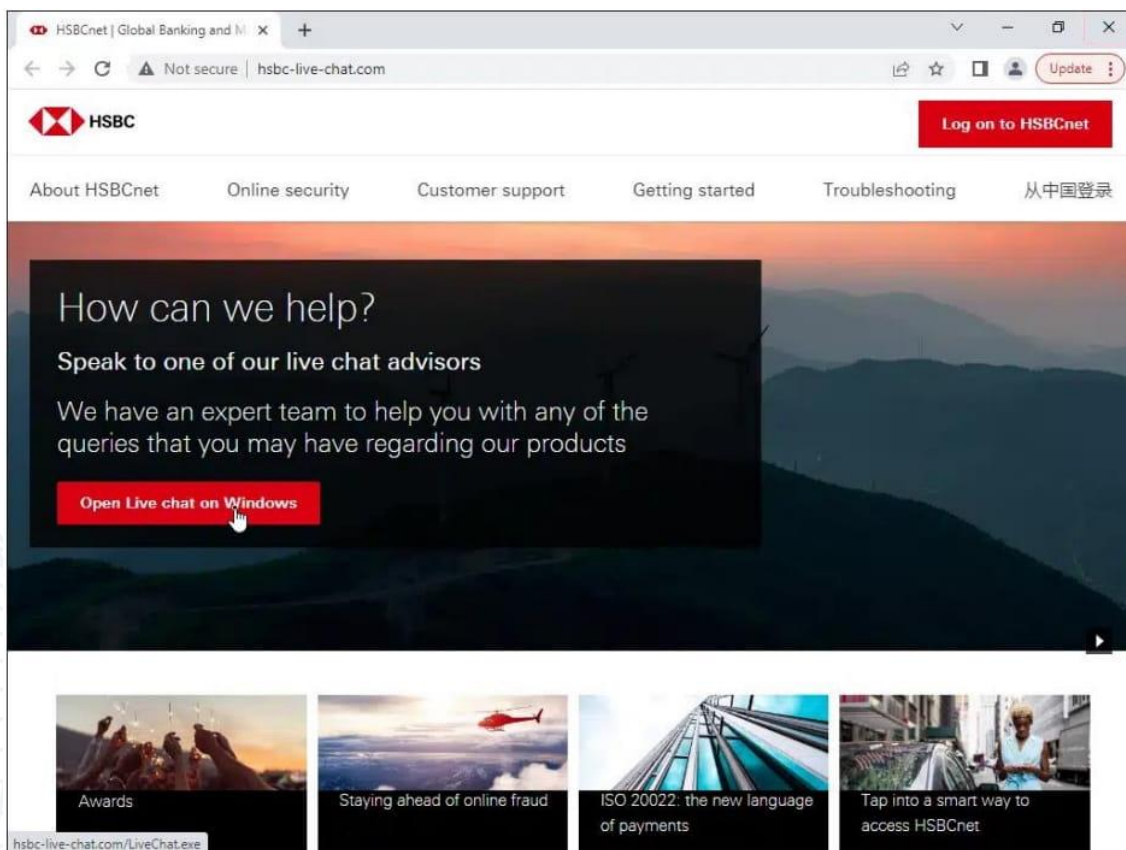


Figura 1 – Exemplo de página de phishing do HSBC.

Além disso, a Trustwave encontrou uma apresentação do PowerPoint direcionada aos funcionários da ZenDesk que habilmente finge ser um aviso de segurança, orientando os usuários a instalar a extensão. A referida apresentação inclui slides que avisam que os agentes de ameaças estão se passando pela GlobalProtect para distribuir malware e fornece etapas que o usuário deve seguir as etapas do guia para instalar o software correto.

Fake GlobalProtect (VPN) Pages – Identifying them

As well as the Okta phishing pages, there are also bad actors which leverage accesses via GlobalProtect. It is very important you do not enter your login information anywhere except the GlobalProtect application on your work machines.

Before you can access any of Zendesk's internal systems such as Okta, Slack and Zendesk Corporate you will need to add GlobalProtect to your browser.



In the next slide, Evie (Head of Product) will guide you on how to add this to Chrome.



Figura 2 – Documento de ppt criado para orientar os usuários na instalação do Rilide.

Por fim, a Trustwave detectou outra campanha que é executada no Twitter, levando as vítimas a sites de phishing para jogos falsos de blockchain P2E (Play To Earn). No entanto, os instaladores desses sites instalam a extensão Rilide, permitindo que os agentes de ameaças roubem as carteiras de criptomoedas das vítimas.

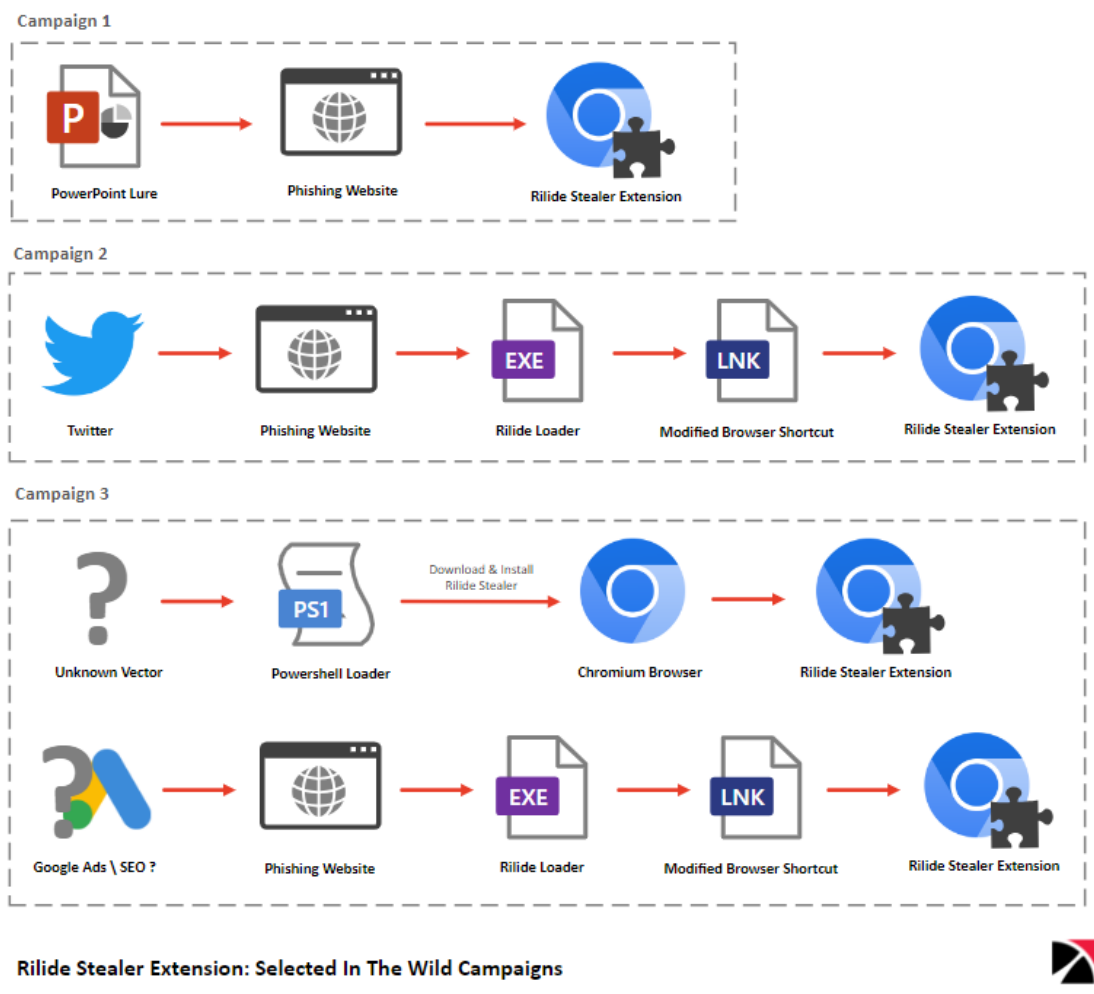


Figura 3 – Cadeia de infecção para campanhas do Rilide.

Independente do tipo de distribuição, após a instalação, a extensão se comunica com o servidor do invasor e recebe um dos seguintes comandos:

- Extension: Ativa ou desativa uma extensão da lista de extensões instaladas.
- Info: Envia informações do sistema e do navegador para o servidor C2. Obtenha todas as definições de configuração.
- Push: Cria uma notificação com mensagem, título e ícone especificados. Ao clicar na notificação, uma nova aba com a URL do servidor C2 será aberta.
- Cookies: Obtenha todos os cookies do navegador e envie-os para o servidor C2.
- Screenshot: Captura a área visível da guia atualmente ativa na janela atual.

- url: Crie uma guia com o URL fornecido.
- current_url: Recupere a URL da guia ativa.
- History: Obtenha o histórico de navegação dos últimos 30 dias.
- Injects: Recupera o código de injeção para aplicar as URLs específicas.
- Settings: Recupera configurações de proxy, grabbers e telegrams.
- Proxy: Ativa ou desativa o proxy. Atores de ameaças utilizam a implementação de proxy da ferramenta "CursedChrome", permitindo navegar na Web autenticado como vítima.
- Screenshot_rules: Atualiza as listas de regras para captura de tela do módulo em intervalos de tempo especificados.

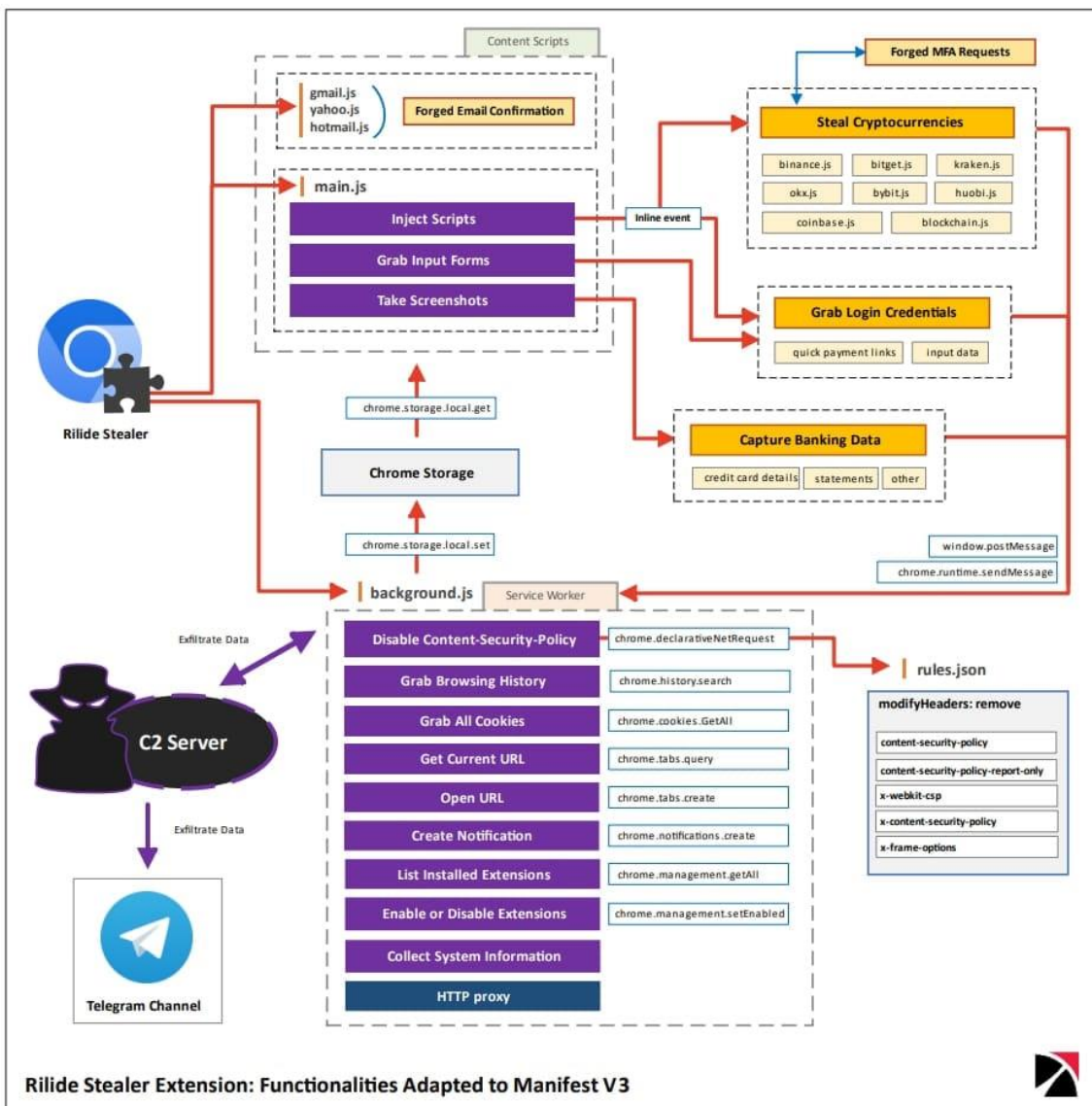
Vale salientar que a quantidade de comandos acima, poderá permitir que os atores roubem uma variedade de informações que podem ser utilizadas para carteiras criptográficas e obtenção de acesso a contas online.

2 CAMPANHA V3 RILIDE COM BYPASS NO MANIFEST V3

A campanha está sendo adaptada para conseguir aplicar o “bypass” na solução do Google Manifest v3, a qual impede que extensões mais antigas parem de funcionar desde janeiro de 2023.

O Manifest v3 limita o acesso da extensão as solicitações de rede do usuário, impedindo o carregamento de código fontes remotas e move todas as modificações de solicitações de rede das extensões para o navegador.

Isso acaba por afetar o Rilide, pois depende da injeção de scripts JS hospedados remotamente, porém, os autores do malware implementaram uma combinação de técnicas divulgadas publicamente que contornam os requisitos do Google.



Rilide Stealer Extension: Functionalities Adapted to Manifest V3

Figura 4 – Adaptação para distribuição do malware.

Como o Rilide não é distribuído pela Chrome Web Store, onde as políticas do Manifest V3 são aplicadas, seus autores podem implementar soluções alternativas para executar o código hospedado remotamente.

Além disso, foi verificado que o malware está sendo comercializado amplamente na Dark Web, já que é realizada a venda por US\$5.000 para outros cibercriminosos, os quais devem criar o próprio método de propagação e infecção.

Podemos acrescentar ainda que houve vários vazamentos de códigos-fontes do Rilide potencialmente autênticos em fóruns clandestinos, expondo o código-fonte a muitos cibercriminosos, os quais podem realizar as suas adaptações.

3 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [BleepingComputer](#) – Malware Rilide



heimdall
security research

A DIVISION OF ISH