BOLETIM DE SEGURANÇA

Malware Azorult sendo usado para roubo de credenciais

heimdall
security research
A DIVISION OF ISH

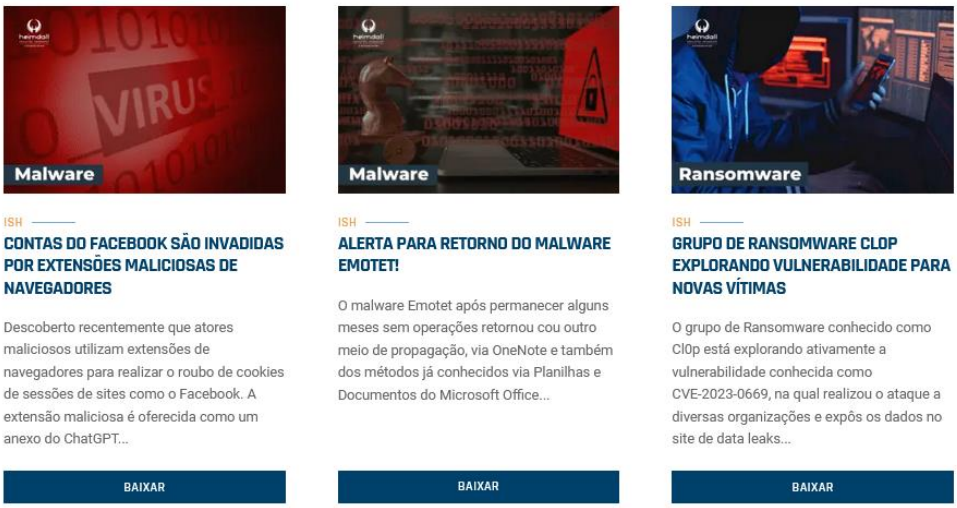
TLP: CLEAR

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

Recentemente foi identificada uma nova onda de ataques de malware, esta campanha utiliza páginas fraudulentas do Google Sites e infiltração de HTML para disseminar um malware comercial conhecido como AZORult. O objetivo principal dessa ação é facilitar a apropriação indevida de informações. De acordo com Jan Michael Alcantara, pesquisador do *Netskope Threat Labs*, o malware emprega uma estratégia de infiltração de HTML. Nessa técnica, o conteúdo malicioso é inserido em um arquivo JSON distinto, que é armazenado em um site externo.

2 INFORMAÇÕES SOBRE A CAMPANHA

A campanha de phishing não foi vinculada a um agente ou grupo específico de ameaças. Foi caracterizada como uma operação ampla, com o objetivo de reunir informações sensíveis para serem comercializadas em fóruns ocultos.

O AZORult, conhecido também como *PuffStealer* e *Ruzalto*, é um software malicioso que rouba informações, identificado inicialmente em 2016. Sua disseminação ocorre geralmente através de campanhas de phishing e malspam, softwares ou mídias piratas com instaladores trojanizados, e malvertising. Após a instalação, o malware tem a capacidade de coletar credenciais, cookies e históricos de navegadores da web, realizar capturas de tela e obter documentos que se enquadram em uma lista específica de extensões **(.TXT, .DOC, .XLS, .DOCX, .XLSX, .AXX e .KDBX**), além de dados de 137 carteiras de criptomoedas. Os arquivos com extensão **AXX** são arquivos criptografados gerados pelo *AxCrypt*, enquanto os arquivos **KDBX** correspondem a um banco de dados de senhas criado pelo gerenciador de senhas *KeePass*.

TXT	axx	documento	xls
kdbx	docx	xlsx	

Figura 1 – Extensões dos arquivos.

A mais recente ação de ataque envolve o autor da ameaça criando páginas do Google Docs falsas no Google Sites, que posteriormente empregam a técnica de contrabando de HTML para distribuir o malware. O contrabando de HTML é uma técnica furtiva que utiliza recursos legítimos de HTML5 e JavaScript para montar e disparar o malware, através do “contrabando” de um script malicioso codificado.

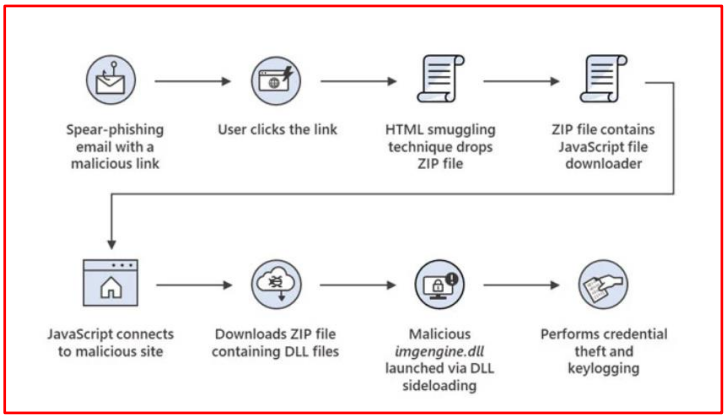


Figura 2 – Contrabando de HTML .

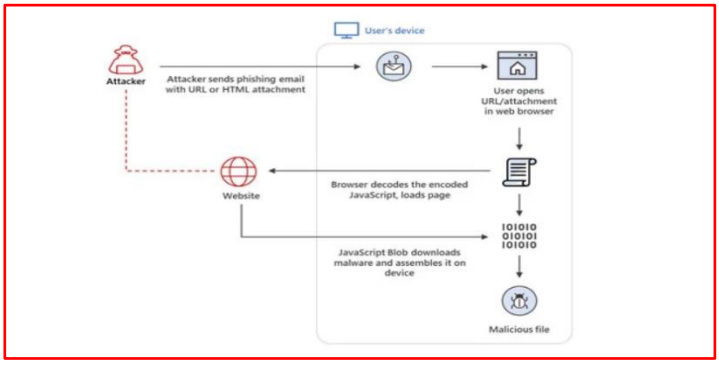


Figura 3 – Técnica furtiva.

Dessa forma, quando um visitante é levado a abrir uma página não autorizada a partir de um e-mail de phishing, o navegador decifra o script e descarrega a carga maliciosa no dispositivo do usuário, burlando eficazmente os controles de segurança comuns, como os gateways de e-mail, que geralmente inspecionam apenas anexos suspeitos. A campanha AZORult aprimora essa estratégia ao incluir uma barreira **CAPTCHA**, uma tática que não apenas confere uma aparência de autenticidade, mas também atua como uma camada extra de proteção contra scanners de URL. O arquivo que é baixado é um atalho (**.LNK**) que se passa por um extrato bancário em PDF, desencadeando uma sequência de ações para executar uma série de lotes intermediários e scripts do **PowerShell** a partir de um domínio previamente comprometido.

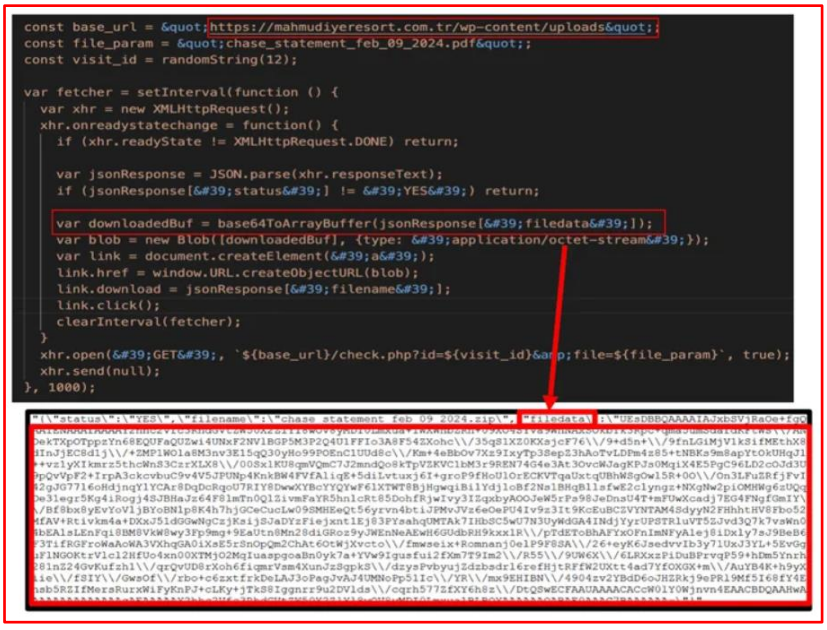


Figura 4 – Script em Powershell.

Um dos scripts do PowerShell, denominado "**agent3.ps1**", foi criado para localizar o carregador AZORult ("service.exe"). Este, por sua vez, baixa e executa um segundo script do PowerShell ("**sd2.ps1**") que contém o malware stealer. O AZORult infostealer é executado de forma furtiva, sem arquivo, utilizando o carregamento de código reflexivo, evitando a detecção baseada em disco e minimizando artefatos", ele emprega uma técnica de evasão AMSI para evitar ser

detectado por uma gama de produtos anti-malware baseados em host, incluindo o Windows Defender. Diferentemente dos arquivos de smuggling comuns, onde o blob já está embutido no código HTML, esta campanha obtém uma carga codificada de um site comprometido separado. O uso de domínios legítimos como o Google Sites pode enganar a vítima, levando-a a acreditar que o link é legítimo.

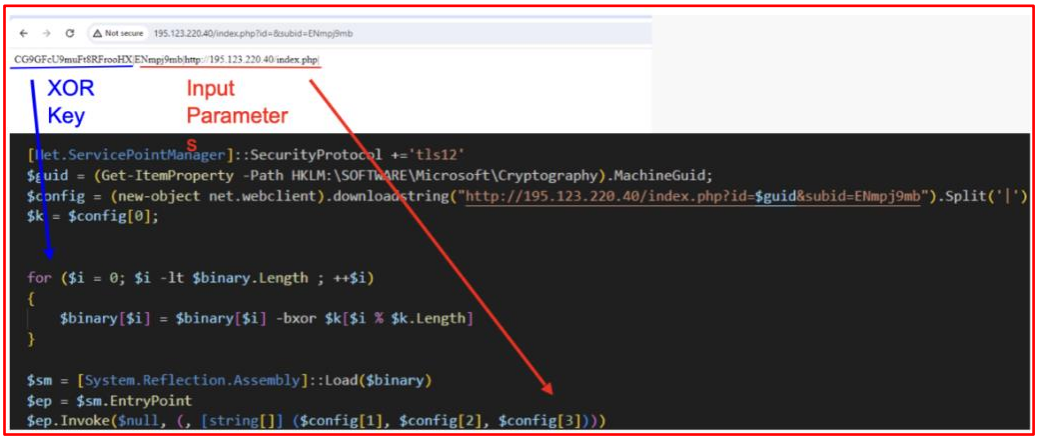


Figura 5 – Script sd2.ps1

O AutoSmuggle captura um arquivo, como um exe ou um arquivo, e o desvia para um arquivo SVG ou HTML. Assim, quando o arquivo SVG ou HTML é aberto, o arquivo desviado é entregue. Foram observadas campanhas de phishing que utilizam arquivos de atalho compactados para disseminar o LokiBot, um ladrão de informações similar ao AZORult, capaz de coletar dados de navegadores da web e carteiras de criptomoedas.

O arquivo LNK executa um script PowerShell para baixar e executar o executável do carregador LokiBot a partir de uma URL. O malware LokiBot foi visto utilizando esteganografia de imagem, empacotamento multicamadas e técnicas de vida fora da terra (**LotL**) em campanhas anteriores. Também foram identificados arquivos de atalho maliciosos que iniciam uma série de downloads de carga útil e, finalmente, implantam um malware baseado em AutoIt. Porém isso não é tudo. Usuários na região da América Latina estão sendo alvo de uma campanha contínua em que os atacantes se passam por agências governamentais colombianas para enviar e-mails com documentos PDF armadilhados que acusam os destinatários de violarem as regras de trânsito. No arquivo PDF, há um link que, quando clicado, resulta no download de um arquivo ZIP contendo um VBScript. Quando executado, o VBScript descarta um script do PowerShell responsável por buscar um dos trojans de acesso remoto, como **AsyncRAT**, **njRAT** e **Remcos**.

Além de ser usado em operações de espionagem, o contrabando de HTML também tem sido empregado em ataques de malware bancário que envolvem o trojan Mekotio. Nesses casos, os adversários enviam e-mails de spam com um link malicioso. Quando esse link é clicado, inicia-se o download de um arquivo ZIP. Esse arquivo contém um Downloader de arquivo JavaScript, que é capaz de recuperar binários utilizados para roubo de credenciais e registro de teclas digitadas.

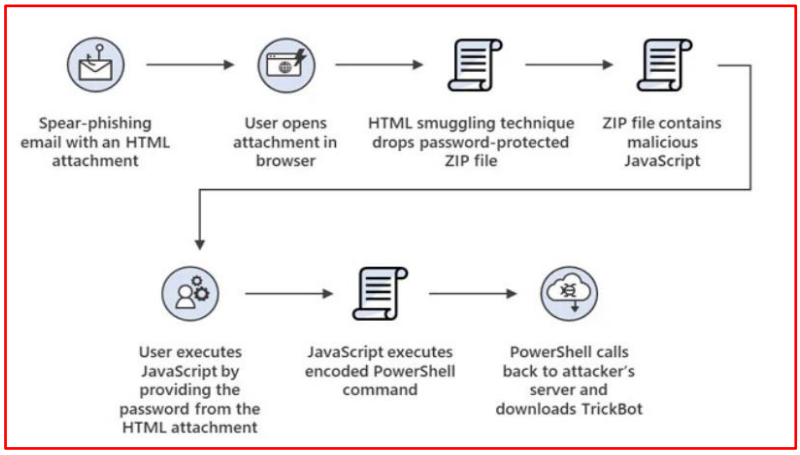


Figura 6 – Cadeia de ataque de spear-phishing

3 CONCLUSÃO

A proteção contra o Azorult é crucial para as organizações, pois este malware é capaz de roubar informações confidenciais e dados de pagamento. Ele utiliza técnicas sofisticadas de evasão para ocultar sua atividade, tornando a detecção e a prevenção um desafio. A exposição a esse tipo de ameaça pode resultar em perdas financeiras significativas e danos à reputação da organização. Portanto, é essencial que as organizações implementem medidas de segurança robustas e mantenham seus sistemas atualizados para se protegerem contra a ameaça e outros malwares semelhantes.

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:

Autenticação de múltiplos fatores

- Implemente a autenticação de múltiplos fatores para todos os serviços críticos, especialmente aqueles associados a contas bancárias online e contas de criptomoedas.

Software autorizado

- Certifique-se de que apenas softwares autorizados e assinados digitalmente sejam instalados em todos os endpoints. Realize varreduras regulares para identificar e bloquear qualquer software não autorizado.

Restrição de acesso a sites suspeitos

- Utilize um proxy de conteúdo para monitorar o uso da internet e restringir o acesso do usuário a sites suspeitos ou arriscados.

Uso de antivírus

- Execute uma varredura completa do sistema usando um software antivírus atualizado para detectar e remover o Azorult.

Restauração do sistema

- Em caso de infecção, delete tudo no seu dispositivo, restaure as configurações de fábrica e comece do zero.

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 compromisso do artefato	
md5:	7b33a1c3deb68cfc25352c8a115dc36d
sha1:	84423e34be5662534893f9726435e93ecc9f04ff
sha256:	18a72a5f52e9da32098cb60b38a3b07e311428bb379f1f6d438031337f855d95
File name:	green.exe

Indicadores de compromisso do artefato	
md5:	de9ac539a377e4fff611ca08073eeced
sha1:	02d43cc92ce09d883e0832897f36ce038bf54534
sha256:	52a0ca6fec42896245bb3b6a7caa876a44779c98102c5e28781cca46bfaf2ed9
File name:	getimages

Indicadores de compromisso do artefato	
md5:	c0f677a29c5f71d2c7766a45ae4329cf
sha1:	e3319ce3809a8a703a4ec41ef438f0264d0ee6d7
sha256:	350dae93066ddd84327e87f2bb784dfc0b70178629afd1fae298ee1376d42450
File name:	getimages

Indicadores de compromisso do artefato	
md5:	c32e590f5676fdb28a61df82fa9a6603
sha1:	9d78561603992742d38b451cb4955db1766efa9e
sha256:	380f9784f4b3db7a711f48baaa2864161ad88b66eec79521011ab8e5871c387a
File name:	google-files

Indicadores de compromisso do artefato	
md5:	2f086cbcb711ffc5597341cca9e38854
sha1:	c504265e7f161a7ad91908cdb0ab9e70992d7ed6
sha256:	030b3d76a054d5a48cbb595d49e7e1cbc6dfdddbccd676f9642640f0429bd8c4
File name:	google-scanner

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps://sites.google[.]com/view/scan-files-2/google files?file=chase_statement_feb_09_2024.pdf&fid=13141718 hxxps://sites.google[.]com/view/pixel-screencapture/getimages?mutli=screenshot_05_02_2024.zip&hid=47584359868716391 hxxps://sites.google[.]com/view/pixel-screencapture/getimages?mutli=screenshot_05_02_2024.zip&hid=47584359868716391 hxxps://sites.google[.]com/view/scan-files-1/google-files?file=chase_statement_feb_05_2024.pdf&fid=57980442 hxxps://sites.google[.]com/view/scan2web/google-scanner?sharedfile=transactions_5841MC_30_01_2024.pdf&hidfile=48483668291021154 hxxps://sites.google[.]com/view/scan-to-mail/google-scanner?sharedfile=transactions_4341VISA_31_01_2024.pdf&hidfile=48978593810214
Domínio	hxxp://sqjeans[.]com hxxp://195.123.220.40/index.php hxxp://mayanboats[.]com

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.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Netscope
- Thehackernews

heimdall
security research
A DIVISION OF ISH