heimdall

security research

A DIVISION OF ISH

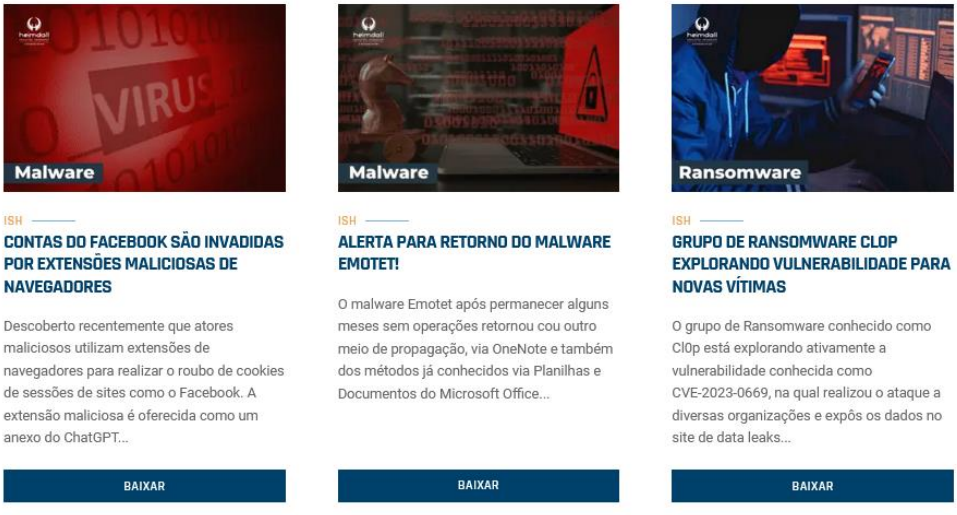
Nova campanha do ChromeLoader chamada SHAMPOO

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



Sumário

Lista de Figuras

1 NOVA CAMPANHA DO CHROMELOADER

Recentemente foi descoberto por pesquisadores de segurança uma nova campanha de malware criada em torno de uma nova extensão maliciosa do **ChromeLoader** à qual é chamada **Shampoo**.

ChromeLoader é uma família de malware de extensão do navegador **Google Chrome** analisada pela primeira vez no início de 2022 por pesquisadores de segurança. Seu objetivo é instalar uma extensão maliciosa no Google Chrome que é usada para publicidade, versões mais antigas do ChromeLoader têm uma cadeia de infecção particularmente complexa, começando com a vítima baixando arquivos ISO maliciosos de sites que hospedam conteúdo ilegal. O mesmo ganhou notoriedade por sua instalação forçada de extensões de navegador indesejadas, geralmente levando as vítimas a resultados de pesquisa indesejáveis e potencialmente prejudiciais, variando de promoções de software e jogos adultos a pesquisas enganosas, brindes falsos e sites de namoro. Acredita-se que a operação do adware seja motivada financeiramente, com o objetivo de gerar receita com os redirecionamentos de pesquisa e anúncios.

2 CADEIA DE INFECÇÃO DO CHROMELOADER SHAMPOO

De início, a vítima baixa um VBScript malicioso disfarçado como um download gratuito de filme, videogame ou conteúdo, geralmente de um site que hospeda conteúdo ilegal. Este script executa um script do PowerShell que configura uma tarefa agendada tornando a infecção persistente. A cada 50 minutos, a tarefa executa um script em loop que baixa e executa outro script do PowerShell. Este script baixa e instala a extensão maliciosa. Uma vez conectado a uma sessão do Chrome, o ChromeLoader Shampoo começa a enviar informações confidenciais de volta para um servidor de comando e controle (C2).

Essa extensão é capaz de coletar informações pessoais confidenciais, como consultas de pesquisa, bem como redirecionar pesquisas e injetar anúncios na sessão de navegação da vítima.

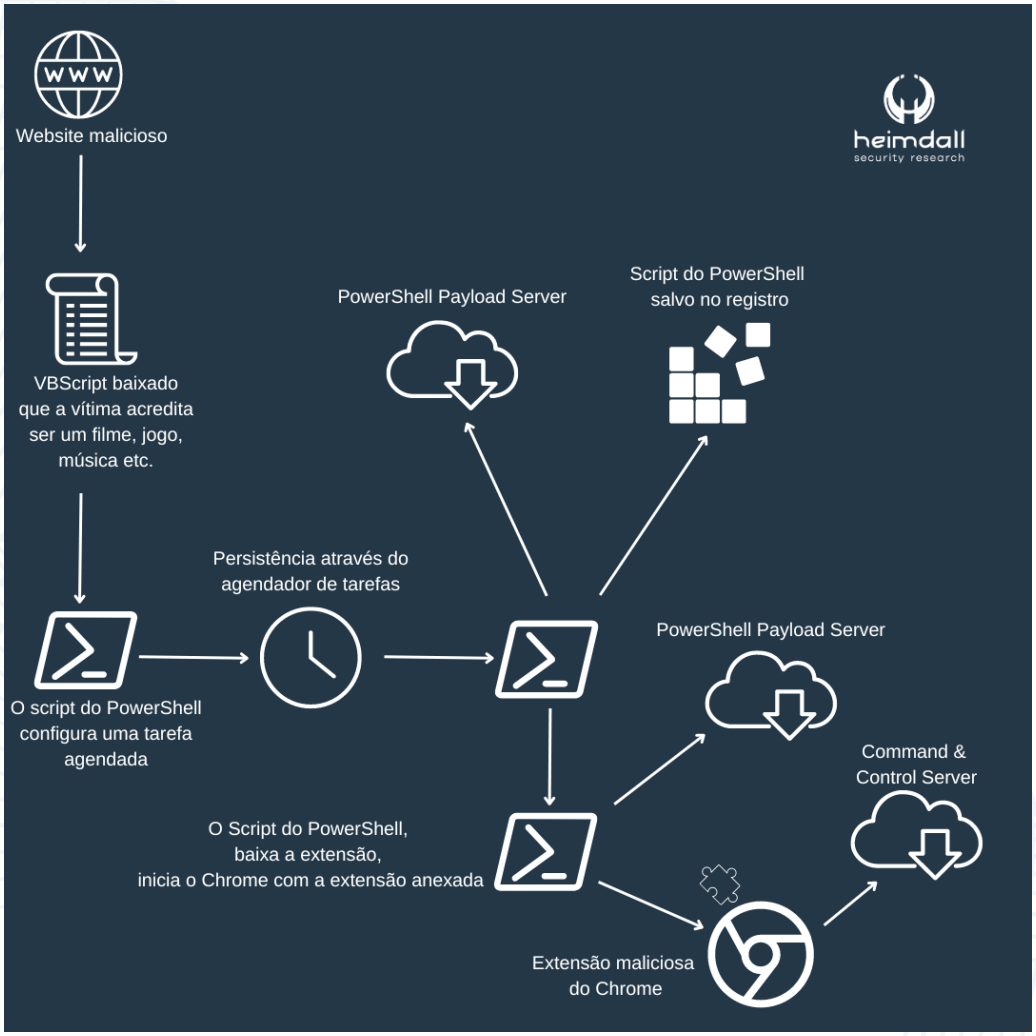


Figura 1 – Cadeia de infecção do CHROMELOADER SHAMPOO.

3 Conclusão

A instalação de extensões maliciosas no navegador Google Chrome apresenta sérios riscos para a segurança e privacidade dos usuários. Essas extensões podem roubar informações pessoais, monitorar atividades de navegação, redirecionar tráfego, exibir anúncios indesejados e criar vulnerabilidades de segurança. É crucial que os usuários adotem práticas de segurança ao instalar extensões e ficarem atentos a mudanças inesperadas em suas experiências de navegação, pois isso pode ser um sinal de um sequestrador de navegador ou outro malware.

4 TTPs – MITRE ATT&CK

Tática	Técnica	Detalhes
Execução	T1204	O shampoo exige que a vítima clique inicialmente em um link malicioso. O Shampoo exige que a vítima execute um arquivo baixado malicioso.
Evasão de defesa	T1027	O Shampoo VBScript contém um script PowerShell incorporado.
Execução	T1059	Shampoo usa VBScript para executar o código. Shampoo usa PowerShell para executar o código.
Execução, Persistência, Escalonamento de Privilégios	T1053	Shampoo configura uma tarefa agendada para persistência.
Persistência	T1176	Shampoo anexa uma extensão maliciosa ao Chrome.
Evasão de defesa	T1622	A extensão Shampoo contém várias armadilhas anti-depuração.
Comando e Controle	T1071	Os dados e arquivos enviados e recebidos pelo Shampoo utilizam HTTPS de forma padrão.
Comando e Controle	T1132	O shampoo usa um esquema xor personalizado para proteger os dados enviados e armazenados. Shampoo usa RC4 para proteger dados enviados e armazenados.

5 MITIGAÇÕES

Para remover a variante do Shampoo ChromeLoader de um dispositivo comprometido, os usuários devem desativar seu mecanismo de persistência seguindo as etapas abaixo:

- Remova todas as tarefas agendadas com o prefixo "**chrome_**". As tarefas agendadas legítimas do Chrome normalmente têm o prefixo "**Google**".
- Exclua a chave de registro "**HKCU\Software\Mirage Utilities\".**
- Em seguida, reinicie o computador.

OBS. Essas etapas devem ser executadas rapidamente antes que o script em loop possa reinstalar o malware.

6 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:

- **Utilização de fontes confiáveis**, para downloads e a manutenção de um software de segurança confiável e atualizado para proteção contra tais ameaças.
- **Ferramentas de detecção e proteção contínuas e completas**, contra worms, vírus, cavalos de Tróia, spyware, ransomware, explorações de dia zero, rootkits e outras ameaças digitais.
- **Atualizações regulares**, mantenha suas extensões atualizadas. As atualizações podem corrigir vulnerabilidades conhecidas e oferecer proteção contra ameaças emergentes.
- **Adoção de medidas de antivírus,** visando verificar e varrer constantemente toda a infraestrutura e ativos utilizados com monitoramento dos aplicativos.
- **Permissões necessárias**, verifique as permissões solicitadas pela extensão durante a instalação. Se uma extensão solicitar permissões excessivas ou permissões que não parecem necessárias para sua funcionalidade, considere isso um sinal de alerta e avalie cuidadosamente se a instalação é realmente necessária.

7 IoCs

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.

URLs de distribuição e endereços IP C2:

wedonhissw[.]com
edrubyglowe[.]com
entxviewsinterf[.]com
oftheappyri[.]com
mysitesext[.]com
worldtimesext[.]com
cesprincipledecli[.]com
dogsfanext[.]com
raconianstarvard[.]com
disguishedbriting[.]com
gingleagainedame[.]com
ebruisiaculturerp[.]com
dprivatedqualizebr[.]com
alfelixstownrus[.]com
ticalsdebaticalfelixs[.]com
edeisasbeautif[.]com
dmiredindee[.]com
sverymuchad[.]com
swordhiltewa[.]com
ndalargere[.]com
wobrightsa[.]com
yeshehadtwo[.]com
sapphiresan[.]com
oldforeyes[.]com
vesoffinegold[.]com
rwiththinlea[.]com
ildedalloverw[.]com
rincelewasgi[.]com
dthestatueof[.]com
ighabovethe[.]com
cityonatall[.]com
olumnstoo[.]com
tropicalhorizonext[.]com
herofherlittl[.]com
wedonhissw[.]com

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.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- threatresearch-hp
- bitdefender
- bleepingcomputer

heimdall
security research

A DIVISION OF ISH