BOLETIM DE SEGURANÇA

Hackers norte-coreanos utilizam exploit zero day no Chrome para implantar o rootkit FudModule

heimdall
security research
A DIVISION OF ISH

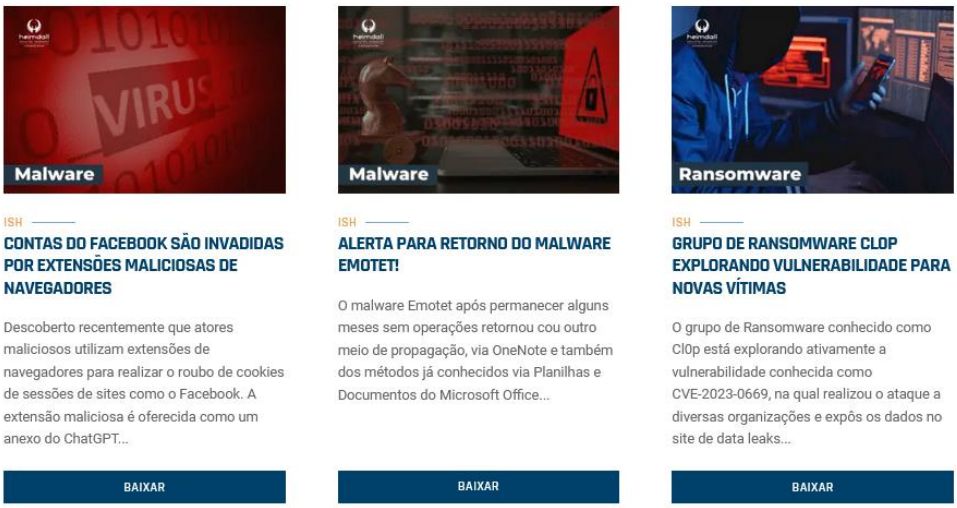
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Recentemente, foi identificada uma vulnerabilidade CVE-2024-7971 categorizada como alta no Google Chrome e outros navegadores baseados no Chromium. Essa vulnerabilidade foi explorada por agentes norte-coreanos em um ataque zero day, com o objetivo de distribuir o rootkit FudModule.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Em agosto de 2024, a Microsoft detectou que um agente de ameaça norte-coreano explorava uma vulnerabilidade de dia zero no Chromium, agora conhecida como CVE-2024-7971, com o intuito de executar remotamente código malicioso (RCE). Com elevada confiança, a empresa atribuiu a exploração a um agente de ameaça norte-coreano com foco no setor de criptomoedas, visando lucro financeiro. A análise indica que esse ataque pode estar vinculado ao grupo Citrine Sleet. Embora o rootkit FudModule também tenha sido associado ao Diamond Sleet, a Microsoft identificou similaridades nas infraestruturas e ferramentas usadas pelos dois grupos, sugerindo um possível compartilhamento do malware FudModule. Essa falha afeta o mecanismo V8 JavaScript e WebAssembly em versões do Chromium anteriores a 128.0.6613.84, permitindo que agentes mal-intencionados obtenham RCE no processo de renderização do Chromium. O Google corrigiu a falha em agosto de 2024, e usuários são fortemente aconselhados a atualizar seus navegadores.

O grupo de ameaças conhecido como Citrine Sleet, rastreado pela Microsoft, tem suas operações na Coreia do Norte e foca em instituições financeiras, especialmente no setor de criptomoedas, visando ganhos financeiros. Como parte de suas táticas, o grupo realiza um extenso reconhecimento de indivíduos e empresas envolvidas com criptomoedas. Eles criam sites falsos, que imitam plataformas legítimas de negociação, para atrair vítimas. Nessas páginas, os alvos são levados a baixar aplicativos ou carteiras de criptomoedas comprometidos. O malware mais comum utilizado pelo grupo é o trojan AppleJeus, que permite o controle sobre os ativos de criptomoeda das vítimas. Além disso, o rootkit FudModule, também utilizado pela Citrine Sleet, foi associado ao grupo Diamond Sleet.

Segundo avaliações do governo dos EUA, esses atores norte-coreanos provavelmente continuarão explorando vulnerabilidades em empresas de tecnologia de criptomoedas, jogos e bolsas, para gerar e lavar fundos que financiam o regime da Coreia do Norte. Uma das organizações que foi alvo desta vulnerabilidade já havia sido atacada anteriormente pelo grupo Sapphire Sleet. O Citrine Sleet também é rastreado por outras empresas de segurança com os nomes AppleJeus, Labyrinth Chollima, UNC4736 e Hidden Cobra, e está ligado ao Bureau 121 do Reconnaissance General Bureau norte-coreano.

O ataque explorado pelo grupo Citrine Sleet seguiu uma sequência comum em cadeias de exploração de navegadores. Os alvos foram direcionados para o domínio voyagorclub[.]space, controlado pelo grupo. Embora o método de direcionamento ainda não esteja claro, a engenharia social é uma tática frequentemente utilizada por eles. Ao se conectar ao domínio, os alvos foram expostos a um exploit de execução remota de código (RCE) relacionado à vulnerabilidade CVE-2024-7971.

Após a execução bem-sucedida do exploit no processo de renderização em sandbox do Chromium, um shellcode contendo um exploit de escape de sandbox do Windows e o rootkit FudModule foi carregado. O escape de sandbox explorou a vulnerabilidade CVE-2024-38106, corrigida pela Microsoft em agosto de 2024, antes que qualquer ligação com o grupo Citrine Sleet fosse estabelecida. Esta vulnerabilidade já havia sido reportada ao Microsoft Security Response Center (MSRC), mas ainda não foi estabelecido um vínculo direto entre essa exploração e o ataque do Citrine Sleet.

O FudModule é um rootkit sofisticado que compromete o kernel do Windows e evita detecção. Ele utiliza técnicas de manipulação de objetos do kernel (DKOM), permitindo adulterações diretas e execução de código malicioso no kernel. O grupo Diamond Sleet vem utilizando o FudModule desde 2021, com a primeira versão pública reportada em 2022, quando atacantes usaram a técnica “Bring Your Own Vulnerable Driver” (BYOVD).

Em 2024, a Avast documentou uma versão mais avançada do FudModule, que explorava a vulnerabilidade CVE-2024-21338 no driver AppLocker do Windows. Essa versão, chamada “FudModule 2.0”, introduziu uma cadeia de ataque complexa, incluindo o Kaolin RAT, um trojan de acesso remoto que carregava o rootkit e se conectava a um servidor C2 para executar comandos avançados, como transferência de arquivos e manipulação de processos.

Além disso, em agosto de 2024, o Gen Threat Labs identificou outra vulnerabilidade, CVE-2024-38193, sendo explorada pelo Diamond Sleet com o FudModule, ampliando ainda mais o nível de acesso ao kernel, conforme divulgado publicamente em agosto daquele ano.

3 RECOMENDAÇÕES

Em agosto de 2024, a Microsoft disponibilizou uma atualização de segurança voltada para corrigir a vulnerabilidade CVE-2024-38106, que estava sendo explorada pelo grupo Diamond Sleet. A atualização também bloqueia tentativas de exploração da vulnerabilidade CVE-2024-7971, garantindo proteção para sistemas que já aplicaram as correções mais recentes. Organizações que ainda não implementaram essas atualizações são fortemente recomendadas a fazê-lo com urgência, a fim de proteger seus sistemas contra potenciais ameaças e evitar que suas infraestruturas sejam comprometidas por ataques explorando essa cadeia de vulnerabilidades.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **Thehackernews**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH