UNC5518 Grupo Hacks Sites legítimos com Captcha falso para entregar m

Data: 2025-08-23 18:39:17

Autor: Inteligência Against Invaders

O grupo de ameaças motivado financeiramente UNC5518 tem se infiltrando sites confiáveis ??para

instalar as iscas clickfix, que são as páginas falsas de captcha, como parte de uma complexa

campanha cibernética que é monitorada desde junho de 2024.

Essas páginas maliciosas levam os usuários a executar scripts de download que iniciam cadeias de infecção, geralmente levando à implantação de malware por atores afiliados.

A Defesa de Ameaças da Mandiant observou a UNC5518 operando como um fornecedor de acesso como serviço, permitindo que grupos como UNC5774 explorassem o acesso a implantar backdoors avançados como o Cornflake.v3.

Essa colaboração destaca a natureza modular das ameaças modernas, onde os corretores de acesso inicial facilitam intrusões mais profundas de atores especializados focados em ganhos financeiros por meio de reconhecimento, roubo de credenciais e movimento lateral.

Quebra técnica de cornflake.v3

O backdoor de cornflake.v3, atribuído à UNC5774, representa uma evolução de variantes anteriores, fazendo a transição de downloaders baseados em C para implementações de JavaScript ou PHP que suportam comunicações de comando e controle baseadas em HTTP (C2) com codificação XOR.

Ao contrário do Cornflake.v2, que não possuía persistência, a V3 incorpora chaves de execução do registro para longevidade e lida com diversas cargas úteis, incluindo executáveis, DLLs, JavaScript, scripts em lote e comandos de PowerShell.

Infecções geralmente começam com os usuários interagindo com as páginas clickfix, que copiam maliciosas Scripts PowerShell Para a área de transferência via JavaScript, solicitando a execução através da caixa de diálogo Run Windows.

Isso leva ao download do Node.JS ou PHP RunTimes de fontes legítimas, extraindo -as para %AppData %e executando o código incorporado.

Verificações anti-VM nos scripts do conta-gotas detectam caixas de areia analisando o uso da memória, nomes de computadores e fabricantes como o Qemu, garantindo evasão em ambientes controlados.

Uma vez ativo, o cornflake.v3 executa reconhecimento de host usando ferramentas como

SystemInfo, Tasklist e ARP, enquanto tentam Kerberoasting para a colheita de credenciais por meio de nomes principais de serviço (SPNS).

Nos casos observados, ele executou scripts em lote para consultas do Active Directory, contando computadores de domínio, enumiando relações de confiança, listando controladores e identificando grupos de administração se o host é realizado ou não.

Uma variante de PHP refina ainda mais usando túneis Cloudflare para proxy de C2, nomes de chave de registro aleatório para persistência e manuseio de carga útil alterada, como salvar DLLs como arquivos .png e integrar downloads node.js para execução de Javascript.

Essa variante também introduziu comandos como ativos para batimentos cardíacos e autorun para configuração, demonstrando melhorias iterativas contra a detecção.

Cargas úteis adicionais

Análise adicional revelado Cornflake.v3 implantando o backdoor windytwist.sea, um implante baseado em C que suporta retransmissão de TCP, conchas reversas e execução de comando, configurada com vários servidores C2 para resiliência.

As árvores de processo mostram que a desova do explorador.exe PowerShell, que, por sua vez, lança Node.exe ou Php.exe, levando ao reconhecimento e execução do RUNDLL32.EXE de cargas de DLL.

Para combater essas ameaças, as organizações devem desativar a caixa de diálogo Run Windows quando viável, conduzir simulações de engenharia social e implementar um registro robusto para atividades suspeitas, como o PowerShell, lançando o Node.js de %AppData %.

Consultas de detecção no Google Operações de segurança Indicadores de destino, como lançamentos incomuns de processos e conexões de rede com nodejs.org ou windows.php.net.

Em conclusão, esta campanha ressalta os riscos de engenharia social na entrega de malware versátil, com UNC5518 e UNC5774 exemplificando o ator de ameaças simbiose. O monitoramento proativo e a educação do usuário são essenciais para interromper essas cadeias.

Indicadores -chave de compromisso (IOCs)

Tipo	Artefato	Descrição	SHA-256/IP/domínio
Arquivo	C: Usuários Appdata roaming node-v22.11.0-win-x64 ckw8ua56.log	Arquivo de persistência de cornflake.v3 (node.js)	000B24076CAE8DBB00B46BB59188A0DA5A940E325EAAC7D86854006EC071AC5B
Registro	HKCU Software Microsoft Windows CurrentVersion Run ChromeUpDater	Cornflake.v3 (node.js) Chave de execução	N / D
Arquivo	C: Usuários AppData Roaming php config.cfg	Amostra de cornflake.v3 (php)	A2D4E8C3094C959E144F46B16B40ED29CC4636B886166615B699979

Tipo	Artefato	Descrição	SHA-256/IP/domínio
			F0A44F9A2D1
Arquivo	C: Usuários AppData roaming shift194340 78g0zrqi.png	Windytwist.sea backdoor	14F9FBBF7E82888BDC 9C314872BF0509835A4 64D1F03CD8E1A629D0 C4D268B0C
Rede	138.199.161.141	IP5518 IP de distribuição	N / D
Rede	159.69.3.151	Cornflake.v3 (node.js) c2	N / D
Rede	Vários e rentais-calgary-predict.trycloudflare.com	Cornflake.v3 (php) c2	N / D
Rede	167.235.235.151; 128.140.120.188; 177.136.225.135	Servidores windytwist.sea c2	N / D

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**