Confúcio muda de ladrões de documentos para backdoors Python

Data: 2025-10-02 14:45:00

Autor: Inteligência Against Invaders

Um grupo de espionagem cibernética de longa data conhecido como Confúcio introduziu novas técnicas em suas campanhas contra usuários do Microsoft Windows.

Identificado pela primeira vez em 2013, o grupo tem visado consistentemente agências governamentais, empreiteiros de defesa e indústrias críticas em todo o sul da Ásia, particularmente no Paquistão.

De ladrões a ataques Python

De acordo com descobertas recentes do FortiGuard Labs, o que há de novo é a mudança do Confucius de ladrões focados em documentos, como o WooperStealer, para backdoors baseados em Python mais avançados, como o AnonDoor.

“Este último relatório do FortiGuard Labs destaca que os agentes de ameaças estão constantemente adaptando suas técnicas para ficar à frente da comunidade de pesquisa de segurança, que desenvolve novas técnicas para detectá-los”, disse John Bambenek, presidente da Bambenek Consulting.

“Em particular, o uso de ferramentas Python explora a dificuldade persistente em detectar atividades maliciosas em linguagens de script, onde você tem uma infinidade de técnicas de ofuscação. O Python é usado rotineiramente em todos os lugares, o que significa que os invasores são livres para aproveitar seu poder sem precisar instalar novas ferramentas ou binários também.”

Os pesquisadores do FortiGuard observaram várias cadeias de ataque entre dezembro de 2024 e agosto de 2025.

As primeiras operações dependiam de spear-phishing com documentos maliciosos do Office e arquivos LNK para entregar o WooperStealer, uma ferramenta que exfiltrava uma ampla variedade de arquivos confidenciais, incluindo documentos, planilhas, imagens e e-mails.

Em meados de 2025, no entanto, Confúcio adotou uma nova abordagem. Em vez de depender apenas do roubo de dados, o grupo começou a implantar o backdoor AnonDoorPython que fornece recursos de persistência e execução de comandos de longo prazo. O AnonDoor permite ações como capturar capturas de tela, listar arquivos, baixar dados e despejar senhas do navegador.

Leia mais sobre espionagem cibernética no sul da Ásia: 20.000 IPs e domínios asiáticos desmantelados na repressão ao infostealer

Técnicas de evasão e persistência

O FortiGuard Labs detalhou como o grupo colocou vários métodos em camadas para obter persistência e evitar a detecção.

Estes incluíram:

- Sideload de DLL por meio de executáveis legítimos
- Scripts do PowerShell ofuscados para instalar ambientes de execução
- Tarefas agendadas para executar repetidamente cargas ocultas
- Rotinas de exfiltração furtivas para minimizar o ruído da rede

Esses métodos permitiram que o grupo mantivesse a flexibilidade operacional e evitasse ferramentas de segurança que dependessem da detecção baseada em assinatura.

Expandindo recursos

Ao contrário das campanhas anteriores que se concentravam estritamente no roubo de documentos, o AnonDoor é capaz de criar perfis completos de host. Ele coleta detalhes do sistema, geolocaliza IPs públicos e inventaria volumes de disco antes de receber tarefas de seus servidores de comando e controle (C2).

Os pesquisadores descobriram que suas operações foram adaptadas para alvos no Paquistão, sugerindo objetivos com foco regional.

“Esta campanha ressalta a agilidade técnica de Confúcio”, escreveu o FortiGuard, observando que o grupo pode alternar rapidamente entre diferentes famílias de malware e métodos de entrega para sustentar o acesso.

O relatório conclui que a cadeia de ataque em camadas de Confúcio demonstra uma clara evolução em direção a operações de espionagem mais duráveis e furtivas.

Analistas alertam que a vigilância contra tais táticas continua sendo crucial, pois os grupos ligados ao Estado continuam a refinar seus métodos.