O Confucius Hacker Group Armaniza documentos para infectar sistemas V

Data: 2025-10-03 06:58:18

Autor: Inteligência Against Invaders

O ConfuCius Hacking Group, uma operação cibernética de longa duração com suspeitos de laços patrocinados pelo Estado, desenvolveu significativamente suas metodologias de ataque ao longo do ano passado, transitando de ladrões de documentos como WooperStealer para sofisticados backdoors baseados em Python, incluindo malware de Anondoor.

A campanha de dezembro de 2024 demonstrou táticas refinadas de engenharia social de Confucius, utilizando e -mails de phishing com apresentações em PowerPoint em armas (document.ppsx) que exibiram mensagens de “página corrompida” para as vítimas.

O documento malicioso continha objetos OLE incorporados que desencadearam a execução do VBScript da infraestrutura remota em Greenxeonsr.info, iniciando uma cadeia de infecção complexa.

Análise recente da FortiGuard Labs revela Como esse ator de ameaças do sul da Ásia tem documentos de escritório em armas e arquivos LNK maliciosos para comprometer os sistemas do Windows em toda a região, particularmente visando organizações baseadas no Paquistão.

A metodologia de ataque envolve técnicas de carregamento lateral da DLL, onde o malware copia os executáveis ??legítimos do Windows como FixMapi.exe aos diretórios do usuário, renomeando-os como swom.exe para persistência.

O grupo estabelece a persistência baseada no registro em HKCU Software Microsoft Windows NT CurrentVersion Windows Load, permitindo a execução automática durante a inicialização do sistema.

Evolução para ataques baseados em LNK

Até março de 2025, Confúcio havia articulado para malicioso Arquivos LNK disfarçado como documentos legítimos como “Invoice_Jan25.pdf.lnk”.

Esses arquivos executam comandos do PowerShell que baixam DLLs maliciosos e documentos PDF de chamariz de servidores remotos, mantendo a ilusão de acesso legítimo ao arquivo ao estabelecer acesso de backdoor.

O Mapistub.dll baixado cria mecanismos adicionais de persistência e prepara endereços de host remotos codificados por base64 para entrega de carga útil.

A análise revelou que a carga útil final permaneceu WooperStealer, configurada para exfiltrar tipos

extensos de arquivos, incluindo documentos, imagens, arquivos e arquivos de email com extensões que variam de .txt e .pdf a formatos .pst e .eml.

A evolução mais significativa ocorreu em agosto de 2025, com a introdução de Anondoor, um sofisticado backdoor baseado em Python que representa uma partida acentuada das ferramentas anteriores baseadas em .NET.

O novo malware estabelece ambientes de execução baixando e configurando o Python através do Scoop Package Manager, criando arquivos .pyc ocultos nos diretórios do usuário.

A Anondoor implementa recursos avançados de reconhecimento, sistemas de vítimas de impressão digital por meio de várias técnicas, incluindo extração de hardware WMIC UUID, geolocalização pública de IP por meio de serviços como api.ipify.org e ip-api.com e enumeração abrangente de espaço em disco em todas as cartas de unidade.

Operações de comando e controle

O backdoor suporta extensos recursos de execução de comando, incluindo captura de captura de tela, listagem e download de arquivos, travessias de diretório e colheita de credenciais de navegadores como Firefox e borda.

A Anondoor se comunica com a infraestrutura de comando e controle por meio de pacotes de dados estruturados usando delimitadores específicos ($!! $ e #$$) e mantém a segurança operacional por meio de intervalos de execução de 6 minutos para reduzir a probabilidade de detecção.

Organizações utilizando FortigateAs soluções FortiMail, Forticlient e Fortiedr recebem proteção automática contra esses vetores de ataque em evolução.

A arquitetura modular do malware permite a carga dinâmica de módulos Python adicionais de servidores remotos, permitindo que os operadores expandam a funcionalidade com base em requisitos específicos de inteligência.

O direcionamento geográfico permanece focado nas regiões do sul da Ásia, particularmente no Paquistão, consistente com os padrões operacionais históricos de Confúcio.

A FortiGuard Labs implementou recursos abrangentes de detecção para esta campanha de ameaças, com o FortiGuard Antivirus identificando vários componentes, incluindo variantes de LNK/agente, amostras de msOffice/agente e classificações de Python/Agent.

A evolução tática do grupo Confucius demonstra a adaptação persistente dos atores de ameaças alinhados ao estado, enfatizando a importância crítica de abordagens de segurança de várias camadas e o monitoramento contínuo de inteligência de ameaças na defesa contra operações sofisticadas de espionagem direcionadas às organizações regionais do governo e defesa.