Shadowsilk alvos de teste de penetração e explorações públicas para viol

Data: 2025-08-29 22:01:33

Autor: Inteligência Against Invaders

Especialistas em segurança cibernética descobriram um cluster de ameaça persistente (APT)

chamado Shadowsilk em uma pesquisa completa publicada pelo Grupo-IB. Desde pelo menos 2023,

esse grupo violou ativamente as instituições governamentais na Ásia Central e na área da Ásia-

Pacífico.

As operações do grupo, em andamento em julho de 2025, concentram-se principalmente na exfiltração de dados, alavancando uma mistura sofisticada de explorações publicamente disponíveis, utilitários de teste de penetração e malware personalizado.

A infraestrutura e o conjunto de ferramentas da Shadowsilk exibem sobreposições significativas com as campanhas iorotrooper previamente documentadas, incluindo scripts compartilhados do PowerShell para entrega de carga útil e mecanismos de comando e controle baseados em telegrama (C2).

No entanto, a análise expandida revelou um escopo mais amplo da vítima e perfis operacionais diferenciados, levando o Grupo-IB a classificar Shadowsilk como um ator de ameaça distinto.

Uma operação conjunta com o CERT-KG permitiu a aquisição de uma imagem do servidor, expondo as táticas, técnicas e procedimentos do grupo (TTPs), incluindo evidências de operadores de língua chinesa e russa colaborando em subgrupos.

Essa composição bilíngue sugere potenciais alianças transversais, embora a natureza exata de sua cooperação permaneça incerta.

Mais de 35 vítimas, predominantemente no setor governamental, foram identificadas, com ataques envolvendo acesso inicial por meio e -mails de phishing que fornecem arquivos protegidos por senha contendo executáveis.

Esses binários estabelecem persistência por meio de modificações do registro e facilitam a execução do comando remoto, ressaltando a ênfase do grupo na infiltração furtiva e de longo prazo.

Operações bilíngues de Shadowsilk

Um exame forense mais forense da imagem do servidor apreendida destacou o diversificado arsenal de Shadowsilk, que integra ferramentas de teste de penetração de código aberto, como SQLMAP, WPSCAN, FSCAN, GOBUSTER e Pesquisa de Reconhecimento e Vulnerabilidade.

O grupo explora vulnerabilidades conhecidas, como CVE-2018-7600 (DrupalgedDon2), CVE-2018-7602 e CVE-2024-27956, juntamente com estruturas como metasploit e Greve de cobalto para escalada de privilégios e movimento lateral.

Os elementos personalizados incluem bots telegrama para C2, permitindo emissão de comando em tempo real, exfiltração de dados e ofuscação de tráfego como atividade legítima do mensageiro.

As capturas de tela das estações de trabalho dos operadoras revelaram interfaces em língua chinesa, incluindo ferramentas como Struts2VulStools e Godzilla Webshells, apontando para membros de língua chinesa que lidam com a penetração de rede e reconhecimento interno.

Por outro lado, os operadores de língua russa parecem focados no desenvolvimento de malware, evidenciados pelos layouts do teclado russo, erros de comando (por exemplo, “???? –??” para “Screen -ls”) e testes de belisões de cobalto em seus próprios dispositivos.

Redes de vítimas compartilhadas, como as de organizações Uzbeque, indicam esforços coordenados entre subgrupos, com notas de reconhecimento idênticas aparecendo em ambos os contextos.

A persistência é mantida por meio de chaves de registro como HKCU Software Microsoft Windows CurrentVersion Run, enquanto o acesso de credenciais envolve roubar lojas de senha do Chrome e descriptografá -las usando chaves locais.

Scripts de exfiltração, geralmente ofuscando o código do PowerShell, arquivam sistematicamente arquivos sensíveis (por exemplo, .docx, .xlsx, .pdf) para domínios como pweobmxdlboi[.]com, comprimindo dados em arquivos ZIP para transmissão.

O grupo também adquiriu painéis da Web como o JRAT e o Morf Project nos fóruns da DarkWeb, usando -os para gerenciar dispositivos infectados sem desenvolver construtores de malware personalizados, reduzindo assim a sobrecarga operacional.

Campanhas em evolução

De acordo com o relatórioAs campanhas de Shadowsilk demonstram adaptabilidade, com a infraestrutura atualizando após exposições, como a divulgação de “lince silencioso” de janeiro de 2025 que levou a abandono de servidores antigos.

Até junho de 2025, surgiram novos bots de telegrama e endereços IP, mantendo semelhanças processuais como comandos PowerShell modificados para implantação de carga útil (por exemplo, downloads baseados em curl para caminhos como C: Usuários Public $$.

Uma fração de dados exfiltrados surgiu para venda em fóruns DarkWeb, sugerindo possíveis motivos de monetização além da espionagem.

Para a defesa, as organizações devem implementar a filtragem robusta de email para bloquear os vetores de phishing, aplicar controles estritos de aplicativos e aplicar patches para CVEs explorados.

A caça proativa de ameaças, combinada com soluções gerenciadas de detecção e resposta (MXDR), é crucial para detectar anomalias como mudanças incomuns no registro ou tráfego de

telegrama.

Monitorar os vazamentos de DarkWeb e alavancar as plataformas de inteligência de ameaças podem fornecer avisos precoces, garantindo a resiliência contra ameaças tão persistentes.

Indicadores de compromisso (IOCs)

Categoria	Indicador	Descrição
Domínio	pweobmxdlboi[.]com	Exteration de Exfiltração
Domínio	documento[.]Hometowncity[.]nuvem	Entrega da carga útil
IP	141[.]98[.]82[.]198	Hospedagem em painel
Hash	471E1DE3E1A7B0506F6492371A687CDE4E278ED8	Amostra de malware
Hash	CA12E8975097D1591CDA08D095D4AF09B05DA83F	Amostra de malware

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