Hackers chineses exploram a infraestrutura de hospedagem na web para a

Data: 2025-08-16 09:31:03

Autor: Inteligência Against Invaders

Os pesquisadores da Cisco Talos descobriram um sofisticado grupo de ameaça persistente (APT)

de língua chinesa, designada UAT-7237, que tem como alvo ativamente a infraestrutura de

hospedagem na web em Taiwan desde pelo menos 2022.

O grupo demonstra sobreposições operacionais significativas ao ator de ameaças identificado anteriormente UAT-5918, sugerindo atividades coordenadas sob um guarda-chuva mais amplo, enquanto emprega táticas distintas para estabelecer persistência a longo prazo em ambientes de alto valor.

O UAT-7237 se distingue através de uma abordagem refinada para manter o acesso persistente, divergindo do tradicional shell da web Estratégias de implantação.

O grupo explora inicialmente as vulnerabilidades conhecidas em servidores não patches da Internet antes de realizar um rápido reconhecimento para avaliar o valor-alvo.

Sua sofisticada metodologia operacional inclui vários componentes -chave:

- **Carregador de código de shell personalizado**: O grupo implanta “Soundbill”, uma ferramenta personalizada construída sobre a estrutura Vthello em língua chinesa que pode decodificar e executar várias cargas úteis, incluindo beacons de greve de cobalto.
- **Persistência baseada na VPN**: Em vez de confiar em shells da web, o UAT-7237 usa clientes VPN Softether combinados com direto Acesso ao protocolo de desktop remoto (RDP) para presença sustentada.
- **Infraestrutura em nuvem**: Operações de comando e controle utilizam URLs da AWS Lambda, indicando operações sofisticadas baseadas em nuvem.
- **Técnicas de evasão**: O Soundbill contém executáveis incorporados do software de mensagens instantâneas QQ provavelmente usadas como chamarizes, permitindo a implantação de implementações personalizadas de Mimikatz.

Isso representa uma evolução significativa nas capacidades do grupo, permitindo a execução do comando arbitrário enquanto evita a detecção por meio de mecanismos avançados de carregamento do código de shell.

Roubo de credencial e spread de rede

O UAT-7237 demonstra características avançadas de ameaça persistente por meio de técnicas sistemáticas de extração de credenciais e expansão de rede.

O grupo emprega várias ferramentas, incluindo o Juicypotato para escalada de privilégios, FSCAN para reconhecimento de rede e várias implementações de Mimikatz para a colheita de credenciais.

Suas operações incluem modificações no registro para desativar as restrições de controle da conta do usuário e ativar o armazenamento de senha ClearText, indicando um entendimento completo dos mecanismos de segurança do Windows.

Os atores de ameaças realizam um reconhecimento extenso usando binários de termos de vida e ferramentas especializadas como SharpWmi e WMICMD para execução remota baseada em instrumentação de gerenciamento do Windows.

Suas operações de colheita de credenciais têm como alvo configurações de VNC, lixões de processo LSASS e empregam o projeto SSP_DUMP_LSASS de código aberto para extração de memória.

As credenciais roubadas são sistematicamente arquivadas usando 7-ZIP antes da exfiltração, demonstrando procedimentos organizados de manuseio de dados.

Direcionando a infraestrutura de Taiwan

A análise da vitimologia do UAT-7237 revela um foco concentrado nos provedores de hospedagem na web de Taiwan e entidades críticas de infraestrutura, alinhando-se a padrões mais amplos de campanha da APT chinesa.

Pesquisadores de Talos avaliar Com alta confiança de que o UAT-7237 opera como um subgrupo do UAT-5918, que anteriormente direcionava as entidades de infraestrutura crítica em Taiwan.

A conexão é suportada por ferramentas compartilhadas, padrões de vitimologia e prazos operacionais que abrangem de 2022 a 2024.

O interesse particular do grupo em VPN e infraestrutura em nuvem sugere objetivos de coleta de inteligência além do roubo de dados tradicionais.

Sua janela operacional de dois anos usando a infraestrutura Softether VPN, com configurações simplificadas de idiomas chineses, fornece confiança de atribuição adicional.

O direcionamento estratégico dos provedores de hospedagem na web pode facilitar ataques da cadeia de suprimentos ou coleta mais ampla de inteligência contra entidades hospedadas, representando implicações significativas para a segurança da infraestrutura digital de Taiwan e o cenário regional de segurança cibernética.

Indicadores de compromisso (COI):

Hash	Caminho do arquivo / nome	Descrição / ferramenta
450FA9029C59AF9EDF2126DF1D6A657EE6EB024D0341B32E6F6BDB8DC04BAE5A	C: temp wmiscan.exe	Wmiscan
6A72E4B92D6A459FC2C6054E9DDB9819D04ED362BD847733	c: /hotfix/project1.exe	ferramenta ssp_dump_lsass

Hash	Caminho do arquivo / nome	Descrição / ferramenta
3492410B6D7BAE5AA E106716A660C751E37CFC4F4F BF2EA2F833E92C2A49A0B3F4 0FC36AD77E0A044	C: /hotfixlog/fileless.exe	FScan
B52BF5A644AE96807E6D846B0 CE203611D83CC8A782BADC68 AC46C9616649477	C: /hotfixlog/smb_version.exe	SMB_VERSION
864E67F76AD0CE6D4CC83304 AF4347384C364CA6735DF0797 E4B1FF9519689C5	FILOUST.EXE	Mimikatz
DF8497B9C37B780D6B6904A24 133131FAED8EA4CF3D75830B 53C25D41C5AEA386	Soundbill	Malware
0952E5409F39824B8A630881D 585030A1D656DB897ADF228C E27DDD9243DB20B7	Greve de cobalto	Baliza
7A5F05DA3739AD3E11414672D 01B8BCF23503A9A8F1DD3F10 BA2EAD7745CDB1F	Greve de cobalto	Baliza
cvbbonwxtgvc3isfqfc52cwzja0kvu qd.lambda-url.ap-northeast-1[.]sobre[.]AWS	(URL)	URL de lambda malicioso
http[://]141[.]164[.]50[.]141/sdksd k608/win-x64[.]rar	(URL)	Carga útil de malware (rar)
141[.]164[.]50[.]141	(IP)	Servidor C2 malicioso