TAG-144: atores atacando entidades governamentais com novas táticas, t

Data: 2025-08-27 14:23:46

Autor: Inteligência Against Invaders

O ator de ameaças conhecido como TAG-144, também chamado de águia cega ou APT-C-36, foi vinculado a cinco aglomerados de atividades distintos que operam de maio de 2024 a julho de 2025, direcionando principalmente as entidades governamentais colombianas nos níveis locais, municipais e federais.

Este grupo de ameaças cibernéticas, ativo desde pelo menos 2018, emprega uma mistura sofisticada de ciber-spionagem e táticas de motivação financeira, concentrando-se em roubo e vigilância de credenciais por meio de commodities de acesso remoto de Trojans (ratos) como Asyncrat, DCRAT, Remcos Rat, Xworm e Limerat.

Os clusters demonstram táticas, técnicas e procedimentos (TTPs) sobrepostos, mas variados, incluindo cadeias de infecção em vários estágios que aproveitam os serviços legítimos da Internet (LIS) como Discord, Github e Archive.org para preparação de carga útil, juntamente com a Steganografia para incorporar códigos maliciosos dentro de arquivos de imagem para evasão.

Análise de infraestrutura revela Uso extensivo de servidores privados virtuais (VPS), endereços IP do ISP colombiano e fornecedores dinâmicos de DNS como DuckDNs.org e Noip.com, com alguns clusters incorporando serviços de VPN como o Torguard para obscurecer operações de comando e controle (C2).

Os dados da vitimologia indicam uma forte ênfase nas instituições governamentais, com intrusões adicionais em setores como educação, saúde e energia, destacando o foco regional da TAG-144 na América do Sul, particularmente na Colômbia, Equador, Chile e Panamá.

Estratégias de implantação de malware

A resiliência operacional da TAG-144 é evidente na diferenciação em seus clusters, cada um adaptado com métodos exclusivos de infraestrutura e implantação, mantendo os principais TTPs.

Por exemplo, o cluster 1, ativo de fevereiro a julho de 2025, depende de servidores Torguard VPN e domínios estáticos do DuckDNS.org com algoritmo de geração de domínio (DGA), como padrões de nomeação, como “Envio16-05.duckdns.orng”, para demitir dcrat, como asnCrat e Rato Remcos.

Este cluster apresenta um novo abuso de LIS, incluindo a plataforma de hospedagem gratuita lovestoblog.com, onde os scripts codificados do PowerShell buscam cargas úteis ocultas de seganograficamente de imagens JPG no Archive.org, geralmente acompanhadas por comentários de português que resumem a colaboração em potencial.

O cluster 2, abrangendo setembro a dezembro de 2024, incorpora como colocrossing e vultr hospedando com domínios com temas espanhóis como “pesosdepesoSlibras.duckdns.org” e implanta variantes de assíncrados rachados provenientes de origem de origem Canais de telegrama resultando em infecções entre setores de governo, educação, defesa e varejo.

Enquanto isso, o cluster 3 utiliza o ISP colombiano UNE EPM para implantações assíncradas e remcos, o cluster 4 combina malware com infraestrutura de phishing que representa bancos como Bancolombia e o cluster 5 emprega Glesys que hospeda para domínios e dinâmicos.

Sobreposições na infraestrutura, como resoluções de IP compartilhadas e comunicações de vítimas, confirmam esses clusters como facetas interconectadas das campanhas do TAG-144.

Outros vínculos com o ator de ameaças Red Akodon, por meio de repositórios compartilhados do GitHub e contas de email do governo comprometidas usadas no Spearphishing, destacam o ecossistema adaptativo do TAG-144, misturando ferramentas de código aberto com crypters como CreptCrypt e Geo-Gente para restringir o acesso externo regiões direcionadas.

Linhas de crime cibernético embaçador

Para combater as ameaças do TAG-144, as equipes de segurança são aconselhadas a implementar o bloqueio de IP e domínio de C2s de ratos associados, implantar regras de detecção, incluindo YARA, Sigma e Snort para assinaturas de malware e monitorar conexões LIS para atividade anômala.

Filtragem de email, monitoramento de exfiltração de dados e atualizações contínuas de inteligência de ameaças são cruciais, dado o uso do grupo de roteadores comprometidos como proxies reversos e direcionamento persistente de entidades de alto valor.

Olhando para o futuro, o TAG-144 deve sustentar seu foco nos ativos do governo colombiano, potencialmente integrando ferramentas emergentes e expandindo a exploração do LIS, enquanto embakando linhas entre crimes cibernéticos e espionagem no cenário digital em evolução da América do Sul.

Essa persistência ressalta a necessidade de defesas regionais aprimoradas e colaboração para mitigar essas ameaças regionalmente sintonizadas.

Indicador de compromisso (COI)

Tipo de IOC	Exemplos
Endereços IP (Cluster 1)	45.133.180.26, 146.70.137.90, 181.235.4.255
Domínios (cluster 1)	Envio16-05.duckdns.org, trabajonuevos.duckdns.org
Endereços IP (Cluster 2)	64.188.9.172, 179.14.8.131
Domínios (cluster 2)	pesoSdepesoSlibras.Duckdns.org, DeadPoolstart2064.duckdns.org
SHA256 HASHES	04878A5889E3368C2CF093D42006BA18A87C5054F1464900094E6864F4919899, AEE42A6D8D22A421FD445695D8B8C8B3311FA0DC0476461AEA649A08236587EDD

Encontre esta notícia interessante! Siga -nosGoogle NewsAssim,LinkedIneXPara obter atualizações instantâneas!