Novos hackers alinhados à China atingem os setores estatal e de telecom

Data: 2025-10-01 11:00:00

Autor: Inteligência Against Invaders

Um grupo de espionagem cibernética recém-identificado tem como alvo organizações

governamentais e de telecomunicações em toda a África, Oriente Médio e Ásia há pelo menos dois

anos e meio, de acordo com a Palo Alto Networks.

O grupo foi rastreado como cluster de atividades CL-STA-0043 pela equipe de pesquisa da Unidade 42 de Palo Alto em 2022 e 2023.

Em 2024, foi-lhe atribuída uma classificação de grupo temporária, TGR-STA-0043, e codinome de campanha, Operação Espectro Diplomático.

Em Um novo relatório, publicado em 30 de setembro de 2025, os pesquisadores da Unidade 42 elevaram o TGR-STA-00043 a um grupo de ameaça distinto sob o nome de Phantom Taurus.

Como parte de suas campanhas de espionagem cibernética, o grupo tem como alvo ministérios das Relações Exteriores, embaixadas, eventos geopolíticos e operações militares. Sua atividade está alinhada com os interesses do Estado chinês.

Phantom Taurus: Técnicas de Mira e Ataque

De acordo com o relatório da Unidade 42, o Phantom Taurus normalmente conduz operações de coleta de inteligência de longo prazo contra alvos de alto valor para obter informações confidenciais e não públicas.

O grupo tem um interesse específico em comunicações diplomáticas, inteligência relacionada à defesa e operações de ministérios governamentais críticos, com campanhas que frequentemente coincidem com grandes eventos globais e assuntos de segurança regional.

Enquanto o Phantom Taurus anteriormente se concentrava na exfiltração de e-mails confidenciais de servidores de e-mail comprometidos, o grupo recentemente passou a direcionar diretamente os bancos de dados do SQL Server para roubo de dados.

As operações do grupo agora envolvem um script de lote personalizado (mssq.bat), que eles executam remotamente por meio do WMI (Instrumentação de Gerenciamento do Windows) para consultar e extrair informações de bancos de dados.

O script funciona da seguinte maneira:

1. Autenticação no SQL Server usando a conta de administrador do sistema e uma senha pré-

comprometida
2. Executar dinamicamente consultas fornecidas pelos operadores (por exemplo, pesquisar tabelas/palavras-chave relacionadas a países específicos como Afeganistão e Paquistão)
3. Exportando resultados para arquivos CSV para exfiltração antes de fechar a conexão

Essa mudança tática sugere um foco expandido em repositórios de dados estruturados, provavelmente para coletar inteligência ou documentos confidenciais com mais eficiência do que apenas o roubo baseado em e-mail.

O uso do WMI para execução remota destaca ainda mais a dependência do grupo em vivendo da terra (LotL) para evitar a detecção.

O Phantom Taurus usa uma infraestrutura operacional que tem sido usada exclusivamente por agentes de ameaças chineses, incluindo Iron Taurus (também conhecido como APT27), Starchy Taurus e Stately Taurus (também conhecido como Mustang Panda).

No entanto, os componentes específicos da infraestrutura usados pelo Phantom Taurus não foram observados em operações por outros agentes de ameaças, indicando compartimentalização operacional dentro desse ecossistema compartilhado.

Além disso, o Phantom Taurus usa um conjunto único de técnicas, táticas e procedimentos (TTPs), que o diferencia de outros grupos.

Juntamente com ferramentas comuns, como China Chopper, Potato suite e Impacket, o grupo usa algumas ferramentas e técnicas que nunca foram observadas em operações de outros grupos e outras que raramente foram usadas por outros agentes de ameaças.

Isso inclui a família de malware Spectre, Ntospy e NET-STAR, um pacote de malware recém-identificado.

NET-STAR, um novo pacote de malware personalizado

O relatório da Unidade 42 compartilhou descobertas sobre um pacote de malware .NET não documentado implantado pela Phantom Taurus para atingir servidores Web do Internet Information Services (IIS).

Essa ferramenta recém-identificada, apelidada de NET-STAR pelos pesquisadores de segurança com base no uso da string nos caminhos do banco de dados do programa (PDB) do malware, “demonstra as técnicas avançadas de evasão do Phantom Taurus e um profundo conhecimento da arquitetura .NET”, observou o relatório da Unit 42.

O pacote compreende três backdoors distintos baseados na Web, cada um desempenhando uma função específica na cadeia de ataque, mantendo a persistência no ambiente IIS do alvo:

- IIServerCore: um backdoor modular sem arquivo que dá suporte à execução na memória de argumentos de linha de comando, comandos arbitrários e cargas úteis

- AssemblyExecuter V1: uma versão mais antiga do assembly .NET personalizado projetado para uma única finalidade específica de executar outros assemblies .NET diretamente na memória sem gravá-los no disco (usado pelo Phantom Taurus em campanhas de 2024)
- assemblyexecer v2: uma versão nova e aprimorada do assemblyexecer v1 equipado comth Recursos de bypass da Interface de Verificação Antimalware (AMSI) e do Rastreamento de Eventos para Windows (ETW) (usados pelo Phantom Taurus desde o início de 2025)