Patchwork lança campanha de spear-phishing contra a defesa turca

Data: 2025-09-21 18:53:59

Autor: Inteligência Against Invaders

Redazione RHC**:21 Setembro 2025 20:53**

O **Patchwork** grupo, também conhecido pelos pseudônimos *APT-C-09, APT-Q-36, Chinastrats, Elefante Dropado, Operação Ressaca, Tigre Acolchoado e Zinco Emerson* , lançou um novo **spear-phishing** visando o setor de defesa turco. O objetivo principal dos invasores, de acordo com analistas, era **para obter informações confidenciais sobre desenvolvimentos em plataformas não tripuladas e armas hipersônicas.**

De acordo com Laboratórios de lobos do Ártico , a cadeia de ataque consiste em cinco etapas e começa com a distribuição de arquivos LNK (atalho do Windows) disfarçados de convites para uma conferência internacional sobre veículos não tripulados. Esses e-mails foram *dirigido a funcionários de empresas que operam no complexo militar-industrial turco* , incluindo um **fabricante de mísseis de alta precisão** .

O contexto geopolítico torna o ataque particularmente significativo: o seu lançamento coincidiu com o aprofundamento da cooperação técnico-militar entre os Estados-Membros. **Turquia e Paquistão** , bem como a escalada do conflito entre o Paquistão e a Índia. De acordo com vários analistas, *A Patchwork está agindo no interesse do Estado indiano e tem atacado sistematicamente alvos políticos e militares em países do sul da Ásia desde 2009.*

No início de 2025, o mesmo grupo lançou uma campanha *contra universidades chinesas usando documentos relacionados à energia como isca* . Ele usou um **Ferrugem-** baseado **downloader** que descriptografou e executou um **Trojan C# conhecido como Protego** , projetado para coletar dados de computadores infectados.

O último ataque às organizações de defesa turcas mais uma vez usa **LNK** Incorporação de arquivos **PowerShell** Comandos. Os scripts iniciam uma conexão com um servidor remoto, expouav[.]org—o domínio foi registrado em 25 de junho de 2025 e *é usado como um ponto de distribuição de carga. Além do código malicioso* , o site contém um documento PDF que imita uma conferência internacional, referindo-se ostensivamente a um evento real realizado na plataforma WASET. Isso permite que o usuário se distraia com um ” **capa** ” enquanto os scripts são executados em segundo plano.

Outras ações levam ao carregamento de uma biblioteca DLL, iniciada por meio do método de sideload de DLL, ou seja, substituindo um componente legítimo em um processo confiável. Sua execução é iniciada por ***uma tarefa agendada no Agendador de Tarefas do Windows*** , que inicia o código shell incorporado. Este módulo realiza reconhecimento ambiental: ele coleta informações do sistema, faz capturas de tela e envia dados para o servidor C2.

Uma característica distintiva das novas operações é a utilização de **Arquivos PE de 32 bits em vez das DLLs de 64 bits usadas anteriormente** . Isso indica uma evolução da base técnica e uma tentativa de aumentar o nível de ofuscação: binários x86 compactos são mais fáceis de injetar em processos confiáveis e a mudança arquitetônica complica a detecção automática de ameaças.

Os pesquisadores também encontraram evidências de sobreposição entre a infraestrutura do Patchwork e elementos anteriormente associados ao **Grupo de equipe DoNot (APT-Q-38, Bellyworm**), o que pode indicar cooperação tática ou logística entre os dois grupos de APT indianos.

A campanha contra a indústria de defesa turca marca uma expansão do foco da Patchwork, anteriormente focada no sul da Ásia. Tendo em conta o papel fundamental da Turquia no mercado dos drones (*O país responde por aproximadamente 65% das exportações globais*) e a sua ambição de desenvolver armas hipersónicas, **as atividades do grupo indiano de ciberespionagem parecem estrategicamente motivadas.**

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli