Mustang Panda, ligado à China, implanta worm USB SnakeDisk avançado

Data: 2025-09-16 07:54:13

Autor: Inteligência Against Invaders

Mustang Panda, ligado à China, implanta worm USB SnakeDisk avançado

O grupo APT Mustang Panda, vinculado à China, foi flagrado usando um novo worm USB chamado SnakeDisk, juntamente com uma nova versão de malware conhecido

Grupo APT vinculado à China Mustang Panda (também conhecido como Hive0154,Camaro Dragão, VermelhoDeltaouPresidente Bronze)foi detectado usando uma versão atualizada do CONCHA DE TOM backdoor e um worm USB não documentado anteriormente chamado SnakeDisk.

O Mustang Panda está ativo desde pelo menos 2012, visandoAmericanoeEuropeuentidades como organizações governamentais, think tanks,ONGs, e até mesmoOrganizações católicasno Vaticano. As campanhas anteriores se concentraram em países asiáticos, incluindo Taiwan, Hong Kong, Mongólia, Tibete e Mianmar. Nas campanhas de 2022, os agentes de ameaças usaram relatórios da União Europeia sobre o conflito na Ucrânia e relatórios do governo ucraniano como iscas. Ao abrir os relatórios, o processo de infecção começa a levar à implantação de malware no sistema da vítima.

Em fevereiro de 2024, os pesquisadores da Trend Micro observaram o grupo visando países asiáticos, incluindo Taiwan, Vietnã e Malásia. Em abril de 2025, o grupo APT Mustang Panda implantou um novo backdoor personalizado, denominado MQsTTang, em ataques direcionados à Europa, Ásia e Austrália.

Em meados de 2025, o IBM X-Force observou o malware Toneshell e Pubload se espalhando por meio de arquivos armados carregados principalmente de Cingapura e Tailândia. A versão mais recente, Toneshell9, não foi detectada pelas varreduras do VirusTotal, usava proxies locais para se esconder dentro do tráfego corporativo e executava dois shells reversos ao mesmo tempo. Os pesquisadores da X-Force também observaram o SnakeDisk, um worm USB que só foi empregado em ataques contra dispositivos na Tailândia. O SnakeDisk infectou unidades, se espalhou por elas e derrubou o backdoor Yokai, que abriu um shell reverso para os invasores. Yokai já havia sido ligado a ataques a autoridades tailandesas no final de 2024.

“Em meados de agosto, a X-Force também descobriu o SnakeDisk, um novo worm USB que compartilha sobreposição com as variantes anteriores do Tonedisk. O worm só é executado em dispositivos localizados na Tailândia, conforme determinado por seu endereço IP público.” lê o relatório *publicado pela IBM X-Force. “A SnakeDisk distribui o backdoor Yokai, que foi publicamente vinculado a vários outros*Campanhas segmentadas pela Tailândia*pela Netskope em dezembro de 2024.”*

O novo worm USB usando o backdoor Yokai parece estar ligado às recentes tensões geopolíticas envolvendo a Tailândia.

Em meados de 2025, eclodiram confrontos fronteiriços entre a Tailândia e o Camboja, aumentando com artilharia, ataques aéreos e fogo naval. Uma ligação vazada derrubou o primeiro-ministro da Tailândia, e as tensões atingiram o pico com o Camboja acusando a Tailândia de planejar um assassinato. Com a China apoiando o Camboja, o Hive0154 provavelmente explorou a crise, implantando o SnakeDisk para atingir as redes do governo tailandês.

Em agosto de 2025, a X-Force encontrou um **Disco de cobra** Ele espelha a 01.datS.A. **Toneshell9** usando o sideload de DLL, resolução de API quase idêntica e dois modos de execução: **“-Incorporação”** (infectar USB na remoção e, em seguida, executar a carga incorporada) e **“-esperança”** (solte e corra imediatamente).

O SnakeDisk procura um arquivo de configuração em seu diretório pai, valida os candidatos por tamanho e CRC32, depois descriptografa o arquivo selecionado com uma rotina XOR de duas fases e analisa 18 valores de configuração que controlam caminhos USB, nomes de arquivos e opções de persistência. Os pesquisadores notaram que o código malicioso visa apenas a Tailândia. Antes de ativar suas rotinas USB, o worm chama http://ipinfo.io/json e prossegue somente se a máquina relatar seu país como Tailândia (“THA” ou “TH”) e impor a execução de instância única por meio de um mutex derivado da configuração.

O SnakeDisk verifica as letras da unidade para encontrar USBs hotplug. Quando encontra um, ele gera um thread e verifica se há infecções anteriores, atualizando apenas versões mais antigas. Ele move todos os arquivos USB para uma pasta oculta, tornando os usuários mais propensos a clicar no executável malicioso recém-descartado, que se disfarça como o nome do volume do USB. Após o lançamento, ele coloca os arquivos originais de volta, ocultando seus rastros.

Quando o SnakeDisk detecta a remoção de um dispositivo USB ou inicia com o argumento “-hope”ent, ele verifica um arquivo de marcador para ver se o sistema já está infectado; em caso afirmativo, ele sai. Caso contrário, ele cria suas cargas na memória, descriptografa-as com XOR e grava vários arquivos em C:UsersPublic. Esses arquivos são combinados em duas cargas finais, uma DLL e um executável com um nome aleatório. Ele exclui os arquivos originais e, em seguida, executa o EXE com um argumento project-mod. O EXE é um aplicativo assinado que carrega a DLL maliciosa, ativando a funcionalidade principal do SnakeDisk.

O backdoor Yokai DLL descartado pelo SnakeDisk verifica “-project-mod” e estabelece persistência por meio de uma tarefa agendada para não administradores. Ele cria um mutex e carrega sua configuração, usando a string de versão “1.0.0”. O backdoor se conecta a um C2 codificado por meio de solicitações POST, enviando dados criptografados. Yokai abre um shell reverso por meio de pipes anônimos, permitindo que seus operadores executem comandos arbitrários. O Yokai compartilha sobreposições técnicas com outras famílias de backdoor do Hive0154, como Toneshell e Pubload, e se aproxima da propagação, configuração e técnica de sideload do Tonedisk. Os pesquisadores apontaram que os subclusters geralmente reutilizam e compartilham código entre famílias de worms e backdoor.

“O Hive0154 continua sendo um agente de ameaças altamente capaz, com vários subclusters ativos e ciclos de desenvolvimento frequentes. A X-Force avalia com alta confiança que grupos alinhados à China, como o Hive0154, continuarão a refinar seu grande arsenal de malware e atingir

organizações públicas e privadas em todo o mundo", conclui o relatório. "O malware discutido no relatório acima provavelmente ainda está em desenvolvimento inicial, permitindo que os defensores adotem mecanismos de detecção antes de seu uso generalizado."

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,SnakeDisk)