A nova variante Toneshell usa o serviço de agendador de tarefas para mar

Data: 2025-09-12 07:56:15

Autor: Inteligência Against Invaders

A mais recente variante ToNeshell apresenta um avanço notável em sua estratégia de persistência,

aproveitando o serviço Com o Scheduler Com tarefa do Windows.

Esse backdoor leve, tradicionalmente entregue por meio de técnicas de carga de DLL, agora incorpora mecanismos de persistência aprimorados e recursos sofisticados anti-análises que apresentam desafios significativos para as equipes de segurança.

Os pesquisadores de segurança cibernética têm identificado Uma nova variante do backdoor de Toneshell, demonstrando a evolução contínua do arsenal do grupo de panda Mustang China-Nexus.

Ao contrário das versões anteriores que se basearam apenas em métodos de persistência tradicionais, essa variante estabelece uma tarefa programada chamada “Dokanctl” que executa a cada minuto de uma pasta nomeada aleatoriamente no diretório AppData do usuário.

O processo de instalação do backdoor começa com uma rotina abrangente de validação. Primeiro, ele verifica se está saindo de um caminho de sincronização do Google Drive, provavelmente uma medida anti-infecção para impedir que os atores de ameaças comprometam seus próprios sistemas.

Se essa verificação passar, o malware aplicar uma política de instância única usando a mutex “Global singleCorporation12ad8b” antes de prosseguir com sua sequência de instalação.

Depois que os pré-requisitos operacionais forem atendidos, o backdoor se copia juntamente com os arquivos DLL de suporte (msvcr100.dll, msvcp100.dll, mfc100.dll) para um diretório recém-criado com um nome de uppercase aleatório de seis caracteres.

O Agendador de tarefas Com a integração do serviço cria um mecanismo de execução persistente, definindo a tarefa para executar %AppData % svchosts.exe em intervalos de um minuto.

Arsenal sofisticado de anti-análise

Essa variante Toneshell demonstra um avanço significativo nas técnicas de evasão, implementando várias camadas de mecanismos de anti-análise e anti-areia.

O malware emprega operações repetidas de arquivos que criam, escrevem, fecham e excluem arquivos temporários em loops com atrasos de 100 milissegundos, queimando efetivamente o tempo de execução e estressando a emulação do sistema de arquivos em ambientes de análise automatizada.

As técnicas de evasão baseadas em tempo incluem loops randomizados do sono que introduzem

atrasos que variam de 800 milissegundos a mais de um segundo por iteração, acumulando mais de 20 segundos de atraso na inicialização.

Além disso, o malware usa getTickCount64 () combinado com sono estridente, esperando até pelo menos 10 segundos de tempo de parede decorridos para garantir que os emuladores sem recursos realistas de avanço do relógio fiquem presos.

Talvez mais notavelmente, a variante incorpora grandes buffers de cordas incorporadas contendo texto copiado de Openai Blog sobre geração de imagens e o site da Pega AI.

Essas strings não servem a nenhum objetivo funcional, além de inflar o tamanho binário e fornecer conteúdo sem sentido para comparações ofuscadas de string que consomem ciclos de processamento sem afetar a lógica do núcleo.

O malware mantém a comunicação com seu servidor de comando e controle em 146.70.29[.]229: 443 Usando um invólucro de protocolo do tipo TLS projetado para misturar com o tráfego legítimo de rede.

Cada pacote começa com bytes fixos “17 03 03” (dados do aplicativo TLS 1.2) seguidos por um campo de comprimento de dois bytes, embora apenas o byte baixo seja processado, limitando efetivamente as cargas úteis a 255 bytes.

O protocolo de comunicação emprega a codificação XOR com uma chave de rolagem de 256 bytes para ofuscação de carga útil. Depois que o cabeçalho do tipo TLS é despojado, a estrutura de carga útil decodificada consiste em um campo de tipo/status, um byte de código adicional e o corpo da mensagem.

Essa abordagem mantém a estrutura de comunicação estabelecida nas variantes anteriores de ToNeshell, enquanto incorpora os recursos atualizados.

O backdoor continua a gerar identificadores de máquina exclusivos por meio da criação da GUID, tentando ler os identificadores existentes de “C: ProgramData SystemRuntimelag.inc” antes de gerar novos usando o coCreateguid ou voltar a um gerador congruente linear interno quando necessário.

O direcionamento contínuo de Mianmar por Mustang Panda através dessa variante Toneshell reflete interesses geopolíticos chineses mais amplos na região.

O malware foi distribuído através de arquivos com nomes de arquivos birmaneses, especificamente “tnla ????? ??????????????????????????” (TNLA e outras forças revolucionárias), indicando foco sustentado no cenário político e de segurança de Mianmar.

Esse direcionamento persistente ressalta como as operações cibernéticas servem como ferramentas para manter a influência em estados vizinhos estrategicamente importantes, particularmente em áreas que envolvem segurança nas fronteiras, desenvolvimento de infraestrutura e monitoramento político.

Mitigações

As equipes de segurança devem se concentrar na detecção dos mecanismos de persistência

específicos empregados por essa variante, principalmente monitorando a criação de tarefas programadas denominadas “Dokanctl” e atividades suspeitas em diretórios da AppData com nomes aleatórios de seis caracteres.

O Mutex “Global SingleCorporation12ad8b” oferece outra oportunidade de detecção, juntamente com as comunicações de rede para a infraestrutura de comando e controle identificada.

As sofisticadas técnicas de anti-análise empregadas por essa variante destacam a necessidade de recursos avançados de análise dinâmica que podem explicar atrasos prolongados de execução e fluxos de controle ofuscados.

As organizações devem implementar o monitoramento comportamental que possa identificar as operações de arquivos característicos e os padrões de tempo associados a essa família de malware.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.