Invasores Adotando Novas Técnicas de LOTL para Evitar a Detecção - Aga

Data: 2025-09-14 21:47:47

Autor: Inteligência Against Invaders

Os agentes de ameaças estão usando novas táticas de viver fora da terra (LOTL) para evitar melhor a detecção, de acordo com a HP Wolf *Relatório de insights de ameaças do 2º trimestre de 2025*.

Essas táticas incluem o uso crescente de vários binários, muitas vezes incomuns, em uma única campanha e novos usos de arquivos de imagem, tornando mais difícil para as equipes de segurança distinguir entre atividades maliciosas e legítimas.

Alex Holland, pesquisador principal de ameaças do HP Security Lab, explicou: “Estamos vendo mais encadeamento de ferramentas vivas e uso de tipos de arquivos menos óbvios, como imagens, para evitar a detecção. Tome os shells reversos como exemplo – você não precisa descartar um Trojan de acesso remoto (RAT) completo quando um script simples e leve alcançará o mesmo efeito. É simples, rápido e muitas vezes passa despercebido porque é muito básico.”

Malware XWorm executado por meio do MSBuild

Em um incidente observado, os invasores encadearam várias ferramentas LOTL, incluindo as menos conhecidas, para fornecer o malware XWorm, um RAT que contém recursos para roubo de dados e controle remoto.

Notavelmente, a carga final foi ocultada nos pixels de uma imagem baixada de um site confiável, decodificada via PowerShell e executada por meio do MSBuild.

O ataque começou com os invasores distribuindo arquivos maliciosos de Ajuda HTML Compilada (.chm) como anexos de e-mail, disfarçados de documentação do projeto – algo que os usuários geralmente exigem quando precisam de ajuda para usar aplicativos do Windows.

Os arquivos maliciosos não continham documentação, apenas scripts maliciosos projetados para iniciar uma infecção em vários estágios.

O script inserido usa vários binários LOTL do Windows para evitar a detecção e executar a carga. Isso inclui o uso do extrac32.exe para copiar o executável legítimo do Windows Script Host (cscript.exe) do System32 para o diretório de usuário público.

A campanha soltou um arquivo VBScript no diretório Public, com o PowerShell usado para executar o script.

O arquivo em lotes, também executado por meio do PowerShell, baixou um arquivo JavaScript para

o diretório ProgramData e o executa usando o interpretador de script nativo do Windows

O script do PowerShell baixou uma imagem de um site de gerenciamento de ativos digitais chamado Tagbox. Como este domínio de site era confiável e o arquivo uma imagem válida, ele ignora a maioria dos filtros de segurança.

No entanto, essa imagem continha dados ocultos, que são carregados em um objeto bitmap. Isso desencadeia uma sequência de eventos que baixa, decodifica e executa a carga final, XWorm, no processo legítimo do MSBuild.

PDF atrai para entregar malware

O Lobo HP relatório, publicado em 12 de setembro, também destacou novos usos de Gráficos vetoriais escaláveis (SVG) para entregar malware.

Os SVGs contêm instruções de texto semelhantes a XML (Extensible Markup Language) para desenhar imagens redimensionáveis baseadas em vetores em um computador.

Os arquivos fornecem um Gama de vantagens para agentes de ameaças, incluindo o fato de que eles abrem no navegador padrão em computadores Windows e podem ser usados para desenhar uma variedade de formas e gráficos, permitindo a representação de várias entidades.

Eles também costumam se comportar como documentos HTML, permitindo que os invasores abusem de tecnologias padrão da Web, como incorporar JavaScript ou fazer referência a recursos externos hospedados em servidores controlados por invasores.

Em novos incidentes observados no segundo trimestre, os invasores distribuíram arquivos SVG extremamente pequenos que não eram maliciosos por conta própria.

Quando aberto em um navegador, o SVG exibia uma imitação convincente de uma interface do Adobe Acrobat Reader, completa com uma animação de upload de documento falso e uma barra de carregamento que se preenchia gradualmente. Isso deu à vítima a impressão de um aplicativo da web legítimo.

Depois que o upload falso foi concluído, o usuário foi solicitado a recuperar o suposto envolvimento. No entanto, clicar no botão de download acionou uma solicitação em segundo plano para um URL externo, que serviu um arquivo ZIP.

Esse arquivo ZIP continha um arquivo JavaScript ofuscado por meio da substituição de strings, concedendo aos invasores controle básico sobre o sistema infectado.

Os invasores também usaram geofencing para restringir downloads a regiões específicas – uma tática projetada para evitar análises automatizadas e atrasar a detecção.

Lumma Stealer Spread via arquivos IMG

O Lumma Stealer emergiu como uma das famílias de malware mais ativas observadas pelos pesquisadores no segundo trimestre de 2025.

Em uma campanha notável, o infostealer foi incorporado em arquivos IMG em e-mails de phishing para evitar a detecção.

A imagem de disco continha um arquivo de aplicativo HTML (HTA) disfarçado de fatura. Se um usuário tentar inspecionar o arquivo em um editor de texto, o script incorporado ficará oculto atrás de longas sequências de espaços em branco para evitar análises casuais.

Quando executado, o script compilou e executou um comando do PowerShell, que baixou um executável de uma URL predefinida. Este executável era um instalador do Windows construído usando o Nullsoft Scriptable Install System (NSIS), uma ferramenta de código aberto para a criação de instaladores.

Ele executa um script de instalação personalizado, que cria várias chaves do Registro que fazem referência a vários caminhos de arquivo e tenta abrir vários arquivos inexistentes, provavelmente com a intenção de enganar os analistas.

Por fim, o instalador do NSIS iniciou outro comando do PowerShell, que executou um arquivo descartado da pasta AppData local.

O PowerShell executou dois códigos de shell, que após vários estágios de descompactação, implantou e executou o Lumma Stealer.

Os pesquisadores observaram que, apesar da derrubada da aplicação da lei de Infraestrutura do Lumma Stealer em maio de 2025, as campanhas continuaram em junho e as operadoras começaram a reconstruir sua infraestrutura.