Malware LNK Aproveita os arquivos legítimos do Windows para deslizar as

Data: 2025-09-25 14:01:35

Autor: Inteligência Against Invaders

Em uma campanha recentemente observada emergindo de Israel, os atores de ameaças reviveram

o uso de arquivos de atalho do Windows (.LNK) para fornecer um potente Trojan de acesso remoto

(rato).

Esses arquivos de atalho aparentemente inócuos exploram os binários de Living-Off-the-Land (LOLBins), como ODBCCONF.EXE para registrar silenciosamente e executar DLLs maliciosos, fugir de ferramentas de segurança e complicando os esforços de detecção.

O ataque começa quando as vítimas são atraídas para baixar um arquivo chamado “cyber security.lnk” de um canal Discord. Ao clicar, o atalho abre um PDF de engodo intitulado “Cyber Security.pdf ”para distrair o usuário, enquanto uma sequência oculta do PowerShell é executada em segundo plano.

Para evitar qualquer janelas de console visível, o script inicia o Conhost.exe no modo sem cabeça, resolve dinamicamente o caminho para o PowerShell e o executa sem janela.

Execução inicial de comando.

Em seguida, o script do PowerShell cria um diretório de trabalho em C: Usuários public Nuget e define várias variáveis:

- Moq.zip: o arquivo malicioso.
- Cyber ??Security.pdf: O chamariz.
- Cyber ??Security.lnk: O atalho malicioso.
- $ Env: Temp e $ Env: Public: para estadiamento de arquivos.

Os bytes LNK brutos são digitalizados para o cabeçalho do %PDF Magic, permitindo a extração do PDF incorporado.

O Arquivo lnk é excluído para cobrir as faixas e o arquivo zip é extraído na pasta Nuget. Após um breve atraso, emergem o moq.dll e as bibliotecas de suporte (Dapper.dll, newtonsoft.dll e um arquivo chamado Nunit), enquanto o zip é removido para manter furtividade.

Execução da DLL e rato central

Para ativar o rato sem acionar alarmes, o script abusa de odbcconf.exe, um binário legítimo do Windows, usando o comando:

```
textodbcconf.exe /a {regsvr "C:UsersPublicNugetmoq.dll"}
```

Isso registra e executa o MOQ.DLL como uma DLL, invocando sua exportação DLLRegisterServer. Em vez de incorporar toda a lógica da carga útil, o moq.dll carrega dinamicamente o Dapper.dll e o newtonsoft.dll, aumentando a complexidade para os engenheiros reversos.

Durante a análise dinâmica, o MOQ.DLL foi observado para:

- Carregue AMSI.dll e patch amsiscanBuffer para retornar sempre a falha, ignorando a interface de varredura anti-malware.
- Patch etweventwrite em ntdll.dll para desativar o rastreamento de eventos do Windows, frustrando o registro de segurança.
- Invoque a WideChartomultibyte para processar a carga útil da “Nunit”, que é decodificada e passada para a função NowyouNeMeeMe () da Dapper.dll.
- Use o ClrcreateInstance para hospedar o .NET Runtime e executar o script PowerShell decodificado.

O script PowerShell resultante, uma vez desusado, revela Os módulos criptografados da AES descriptografam em tempo de execução, armazenando o texto simples em uma variável para execução. Para segurança, os analistas redirecionaram essa saída para um arquivo em vez de executá -lo.

Após a execução, o malware garante a persistência modificando a chave do registro

```
textHKCUSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonShell
```

Para anexar seu comando de lançamento ao lado do Explorer.exe, garantindo a ativação no login.

O rato gera ou lê um identificador exclusivo de ID e máquina a partir de arquivos no diretório Temp antes de chegar a um URL C2 codificado (por exemplo, hotchichenfly.info).

Se o servidor primário não for alcançado, ele calcula um endereço de fallback com base no ID do bot e no nome de usuário. Os comandos do C2 são codificados e armazenados em arquivos temporários, depois decodificados e executados conforme necessário.

Os principais recursos de rato incluem:

- Métricas do sistema de coleta, como produtos antivírus, detalhes do sistema operacional, endereço IP e nome de usuário.
- Captura de capturas de tela, codificando -as na base64 e exfiltrando -as a um servidor remoto.
- Carregando arquivos arbitrários através do Dropbox API usando tokens roubados.
- Digitando um loop perpétuo para buscar e executar novos comandos C2.

Esse conjunto de recursos abrangente ressalta a versatilidade do rato como uma ferramenta de espionagem multifuncional.

Mitigações

As equipes de segurança devem implementar as seguintes medidas defensivas:

- Bloqueie ou monitore de perto a execução de lolbins como Odbcconf.exe para parâmetros não padrão.
- Aplicar a lista de permissões da aplicação para impedir os registros desconhecidos da DLL.
- Habilite e proteja o registro AMSI e ETW para detectar tentativas de remendo na memória.
- Eduque os usuários sobre os riscos de abrir atalhos e baixar arquivos de plataformas de bate -papo não confiáveis.

Dada a sofisticação deste rato baseado em LNK e o uso de componentes legítimos do Windows, implantando uma solução de segurança respeitável-como a segurança total do K7-e garantir assinaturas, heurísticas e detecções comportamentais estão atualizadas é crucial para frustrar ataques futuros. Patching contínuo, separação estrita de privilégio e monitoramento vigilante de execuções anormais de processo permanecem essenciais para manter uma postura segura.

COI

Hash	Nome da detecção
7391C3D895246DBD5D26BF70F1D8CBAD	Trojan (0001140E1)
2956EC73EC77757271E612B81CA122C4	Trojan (0001140E1)
5A1D0E023F696D094D6F7B25F459391F	Trojan (0001140E1)
92FC7724688108D3AD841F3D2CE19DC7	Trojan (0001140E1)