Iscas de credenciais baseadas em atalhos entregam implantes DLL - Agai

Data: 2025-10-02 11:28:30

Autor: Inteligência Against Invaders

Uma campanha que empacota arquivos ZIP com tema de credenciais com arquivos maliciosos de

atalho do Windows (.lnk) foi rastreada por pesquisadores de segurança cibernética.

Os arquivos ZIP prometem documentos certificados, incluindo digitalizações de passaporte e registros de pagamento. Quando um usuário clica em um atalho, ele dispara um script do PowerShell minimizado e ofuscado que baixa uma carga maliciosa.

A engenharia social encontra as táticas de evasão

O que há de novo neste ataque é a mistura de engenharia social familiar e evasão pragmática, de acordo com um novo comunicado da BlackPoint.

O dropper rotula os arquivos de teste com nomes “.ppt” enquanto os salva como DLLs localmente, constrói comandos-chave a partir de matrizes de bytes para evitar texto claro, como “Start-Process” e “rundll32.exe”, e escolhe arquivos de servidor diferentes quando detecta processos antivírus comuns. A abordagem favorece a confiabilidade operacional e a furtividade em relação à criptografia avançada.

“[The shortcuts] lançar silenciosamente o PowerShell ofuscado”, disse a BlackPoint.

Em seguida, eles buscam DLLs disfarçadas de arquivos .ppt.

A atividade foi observada visando um usuário vertical de gerenciamento, sugerindo que as iscas foram adaptadas a fluxos de trabalho executivos, como verificação de identidade e aprovação de pagamento.

Como funciona o conta-gotas

O dropper do PowerShell é iniciado de uma maneira projetada para permanecer indetectável. Ele usa os chamados sinalizadores silenciosos, permitindo que o comando seja executado sem exibir janelas visíveis ou solicitar permissão ao usuário. Ele também suprime as mensagens de progresso e limpa o console para que haja poucas, se houver, pistas na tela de que algo incomum está acontecendo.

Antes de fazer o download, o script verifica o sistema em busca de sinais de processos antivírus comuns. Se nenhum for encontrado, ele solicitará um arquivo de linha de base rotulado NORVM.ppt. Se um antivírus estiver presente, ele solicitará BD3V.ppt – uma variante destinada a ser mais furtiva.

Os .pptnames são apenas cover; O script trata os arquivos como bytes brutos em vez de slides.

Esses bytes baixados são salvos no perfil do usuário como uma DLL curta e nomeada aleatoriamente. O dropper invoca essa DLL com o utilitário do Windows rundll32.exe usando a exportação JMB, que efetivamente pede que um programa de sistema assinado carregue e execute o código do invasor.

Como o runtime usa um binário existente do Windows em vez de iniciar um executável desconhecido, a atividade pode parecer um comportamento comum do sistema. Essa abordagem de viver da terra ajuda o implante a se misturar às operações normais, dando ao invasor uma posição silenciosa na máquina, tornando a detecção e o bloqueio simples menos prováveis.

Leia mais sobre técnicas habilitadas para PowerShell: Carregador baseado em PowerShell implanta Remcos RAT em novo ataque sem arquivo

Mitigações e sinais a serem observados

A Blackpoint compartilhou várias sugestões para enfrentar ameaças como essa, incluindo:

- Bloqueie ou detone arquivos LNK em arquivos e aplique a Marca da Web
- Negar a execução de caminhos graváveis pelo usuário com o WDAC ou o AppLocker e restringir o uso de rundll32
- Instrumente o PowerShell, habilite a transcrição de log de bloco de script e AMSI e proteja a saída da Web com inspeção TLS

O relatório alertou que essas medidas são necessárias porque o ataque negocia com a confiança do usuário em conteúdo com tema de documento e usa binários de sistema assinados e verificações simples de reconhecimento de AV para reduzir a detecção precoce.