Mustang Panda adota um novo método de carregamento lateral da DLL pa

Data: 2025-10-07 06:17:35

Autor: Inteligência Against Invaders

A sofisticada ameaça ligada à China Actormustang Pandahas refinou seu arsenal de espionagem cibernética com uma técnica avançada de carregamento lateral da DLL direcionada especificamente à comunidade tibetana, de acordo com a recente análise de uma campanha identificada pela primeira vez pelo X-Force da IBM em junho de 2025.

Esta operação politicamente motivada demonstra como os atores de ameaças evoluem continuamente seus métodos de ofuscação para ignorar os controles de segurança e manter a persistência em sistemas comprometidos.

O vetor de ataque começa com um cuidadosamente trabalhado.

O SingleLoader descriptografa e executa um comando criando uma tarefa programada chamada “Adobeexperiencemanager” que é executada a cada dois minutos:

```
textschtasks /F /Create /TN "AdobeExperienceManager" /SC minute /MO 2 /TR
"C:ProgramDataAdobeLicensingPluginWF_Adobe_licensing_helper.exe Licensing"
```

Essa abordagem de persistência redundante complica os esforços de resposta a incidentes e aumenta a probabilidade de manter o acesso, mesmo que um mecanismo de persistência seja descoberto e removido.

Quando executado com o argumento correto, a reivindicação transita para sua fase de implantação de carga útil primária. O malware aloca a memória executável usando virtualAllocwithpage_execute_readWritePermissions e copia o código de shell descriptografado para este buffer.

Em vez de executar diretamente o código shell, o malware abusa doEnumfontswapi Mecanismo de retorno de chamada passando o endereço do código shell como o ponteiro da função de retorno de chamada – uma técnica que evita muitas soluções de monitoramento de segurança.

O shellcode implantado, identificado AspublOader, implementa o hash da API usando o algoritmo ROR13 para resolver dinamicamente as APIs do Windows necessárias.

Este componente executa o Bloco de Ambiente de Processo (PEB) caminhando para localizar e carregar os módulos necessários, estabelecendo a comunicação com a infraestrutura de comando e

controle para exfiltrar as informações do sistema.

A campanha demonstra a evolução contínua de Mustang Panda na segmentação de metodologias, combinando elementos de engenharia social específicos para interesses tibetanos com técnicas avançadas de ofuscação técnica.

As equipes de segurança devem implementar o monitoramento abrangente para padrões incomuns de carregamento de DLL, criação de tarefas programadas e modificações suspeitas de registro para detectar campanhas semelhantes de maneira eficaz.

Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas e definir GBH como uma fonte preferida em**Google**.**