Hackers abusam de certificados de EV para assinar malware DMG comple

Data: 2025-10-01 13:37:29

Autor: Inteligência Against Invaders

Os pesquisadores de segurança descobriram uma nova campanha de malware do MacOS na qual

os atores de ameaças estão abusando de certificados de assinatura de código de validação (EV)

para distribuir cargas de pagamento de disco completamente indetectáveis ??(FUD) (DMG).

Embora o abuso de certificado de EV tenha atormentado o ecossistema do Windows, sua expansão no malware do MACOS marca uma escalada significativa na exploração de assinatura de código.

Uma amostra DMG fresca (SHA-256: A031BA81111D0C11ACFEDE9AB83B4BE8274584DA71BCCC88FF72E2D51957DD7) foi identificada por um novo ID do desenvolvedor: Thomas Boulay Duval (J97GLQ5).

Os certificados de EV exigem verificação rigorosa da identidade e investimento financeiro substancial por desenvolvedores legítimos. Na plataforma da Apple, os certificados de EV são concedidos com moderação e a alto custo e representam o padrão-ouro para a confiança de assinatura de código.

No entanto, os adversários obtiveram esses certificados – seja por roubo, compra através de canais ilícitos ou abuso de documentos de identidade comprometidos – para assinar seu malware. Uma vez assinado, as cargas úteis da DMG parecem legítimas para macos verificações de segurança e são prontamente instaladas pelos usuários.

Os operadores de campanha anexam fragmentos do nome do signatário ao identificador do pacote em uma tentativa grosseira de fingir legitimidade – a Balaban.sudoku imita “Alina Balaban” e Thomas.parfums ecoa “Thomas Boulay Duval”. Apesar dessa manobra, a inspeção mais profunda revela facilmente comportamentos maliciosos.

Descobrindo o lançador malicioso

Análise do executável Mach-O dentro do DMG revela Várias referências à palavra francesa “Parfums” incorporadas em tabelas de cordas.

O AppleScript incorporado é buscado em tempo de execução de um URL remoto (FranceParfumes[.]org/parfume), semelhante às técnicas descritas por @osint_barbie em um tópico recente do Twitter.

Depois de executado, o AppleScript cai e executa uma carga útil em segundo estágio identificada como ladrão de Odyssey, um Trojan de colheita de credenciais visto anteriormente nas implantações do Windows.

O script chama as APIs do sistema via Swift dataTaskWithURL:completionHandler: Método para baixar o roubo binário e executá -lo sob o contêiner assinado sem arrecadar alertas.

Impacto operacional e COI

O uso indevido dos atores de ameaças dos certificados de EV mina Maçã Modelo de confiança de assinatura de código. Assim que esses certificados forem relatados e adicionados à lista de revogação, as campanhas subsequentes de malware não serão lançadas em sistemas atualizados.

No entanto, a janela de oportunidade para a implantação não detectada pode durar dias ou semanas – o tempo suficiente para comprometer inúmeras vítimas.

Indicadores de compromisso:

- SHA-256: A031BA8111DED0C11ACFEDE9AB83B4BE8274584DA71BCC88FF72E2D51957DD7.
- Domínio: FranceParfumes[.]org/parfume.
- Endereço IP: 185.93.89.62.

As equipes de segurança podem monitorar os certificados de EV abusados ??pelo Odyssey Stealer através da pesquisa pública da CertCentral em certCentral.org/LOOKUP?DETAIL_TYPE=Malware&Query=odyssey+Stealer, mantida pelo @SquableDoBlog.

O uso de certificados EV para assinar malware macOS representa uma mudança preocupante na exploração de assinatura de código.

As organizações e os usuários finais devem permanecer vigilantes-verificando a legitimidade do certificado além dos avisos do gatekeeper e alavancar feeds de inteligência de ameaças para bloquear domínios maliciosos e certificados revogados.

Relatórios rápidos e revogação de certificados de EV abusados ??são essenciais para interromper essas campanhas e proteger os ambientes de MacOS de ameaças assinadas de maneira semelhante.