O New Shamos Malware tem como alvo macOS através de sites de ajuda f

Data: 2025-08-24 12:59:03

Autor: Inteligência Against Invaders

Pesquisadores de segurança cibernética da CrowdStrike identificaram e frustraram uma sofisticada

campanha de malware que implantou Shamos, uma variante avançada do malware atômico de

moradia de macos (AMOS), orquestrado pela aranha de biscoitos do grupo cibercriminal.

Operando sob um modelo de malware como serviço, a Spider Spider aluga esse ladrão de informações para afiliados que têm como alvo as vítimas para coletar dados confidenciais, incluindo Credenciais de logincarteiras de criptomoeda e outras informações pessoais.

A campanha tentou comprometer mais de 300 ambientes de clientes, mas foi bloqueada com sucesso pela plataforma Crowdstrike Falcon, destacando a crescente ameaça de malware específico do MacOS no ecossistema Ecrime.

Esta operação se baseou em táticas de malvertismo, onde os sites de ajuda de MacOS fraudulentos foram promovidos nos resultados dos mecanismos de pesquisa, atraindo usuários que buscam soluções para problemas comuns, como lavar o cache do resolvedor.

Descoberta de campanha

Vítimas de países como Estados Unidos, Reino Unido, Japão, China, Colômbia, Canadá, México e Itália foram direcionados, com uma exclusão notável da Rússia e da Commonwealth of Independent States, alinhando -se com proibições nos fóruns russos de ecris contra o ataque doméstico.

O Malvertising instruiu os usuários a sites falsificados imitando páginas de suporte legítimas de macOS, como Mac-Safer[.]com e resgate-MAC[.]com, que forneceu instruções enganosas para executar um comando de instalação de uma linha malicioso no terminal.

Este comando, muitas vezes codificado por Base64, baixou um Script Bash Isso capturou a senha do usuário e buscou o executável Shamos Mach-O.

Ao explorar essa técnica, os atacantes ignoraram as verificações de segurança do MacOS Gatekeeper, permitindo a instalação direta do malware sem acionar proteções padrão.

Táticas semelhantes foram observadas em campanhas anteriores envolvendo ladrões de cuco e shamos, incluindo o Malvertising para Homebrew entre maio de 2024 e janeiro de 2025, bem como repositórios oportunistas do GitHub que posam como ferramentas gratuitas do MacOS, como editores de vídeo, software CAD e aplicativos de IA.

Mecanismos de persistência

Após a execução, o malware shamos é baixado para o diretório / tmp /, onde remove atributos de arquivo estendidos usando o XATTR para evitar a detecção, atribui permissões executáveis ??via CHMOD e executa verificações anti-VM para evitar ambientes de caixa de areia.

Em seguida, ele aproveita o AppleScript para reconhecimento, digitalizando arquivos de carteira de criptomoeda, dados de chaveiro, notas da Apple e credenciais do navegador.

Os dados coletados são arquivados em um arquivo zip nomeado.zip e exfiltrado via comandos CURL para servidores controlados por atacantes.

Outras cargas úteis, incluindo um aplicativo de carteira Live Ledger Ledger e um módulo de botnet, são implantadas como arquivos ocultos no diretório inicial do usuário.

Se houver privilégios de sudo, Shamos estabelecerá persistência criando um arquivo PLIST (com.finder.helper.plist) no diretório de lançamento, garantindo acesso a longo prazo.

Observações de Crowdstrike observado Múltiplas invocações de curl indicativas de atividade de botnet, ressaltando o design modular do malware para compromisso prolongado.

Os relatórios de código aberto corroboraram essas descobertas, detalhando uma campanha relacionada por meio de um repositório falso do GitHub imitando o ITERM2, um popular emulador de terminal do MacOS.

Este repositório instruiu os usuários a executar um comando de uma linha semelhante, buscando shamos de domínios como o Macostutorial[.]com, demonstrando a preferência dos atores por misturar engenharia social com evasão técnica.

Crowdstrike avalia com alta confiança de que os atores do ECRIME persistirão no uso de comandos de instalação de Malvertising e de uma linha para a distribuição de roubos de macos, dada sua eficácia comprovada em ignorar o gatekeeper e impulsionar o tráfego das vítimas.

O aprendizado de máquina e os indicadores de ataque da plataforma Falcon (IOAs) fornecem detecção em camadas, impedindo os estágios de download, execução e exfiltração.

Para proteção, os usuários devem permitir a prevenção suspeita de processos e a prevenção de ameaças de origem da inteligência nas políticas do Falcon Insight XDR.

Os caçadores de ameaças podem utilizar as consultas do SiEM da próxima geração do Falcon para detectar comportamentos de risco, como scripts de bash chamando DSCL, CURL, XATTR e CHMOD ou execuções de AppleScript de / tmp / binários.

Indicador de compromisso (COI)

Tipo de IOC	Descrição	Valor
Sites de Malvertising	Sites contendo instruções para baixar Shamos	Mac-Safer[.]com Resgate-Mac[.]com https[:]// github[.]com/jeryrymoore/iterm2
Bash Script SHA256 Hashes	Hashes de scripts de festas maliciosas	231C4BF14C4145BE77AA4FEF 36C208891D818983C520BA067

Tipo de IOC	Descrição	Valor
Hashes shamos mach-o sha256	Hashes of Shamos executáveis	DDA62D3BBBF547F EB7ED285ABA687661AD13F22 F8555AAB186DEBBADF2C1162 51CB269E913EF68 4549E2599DE3011973FDE6105 2A55E5CDB770348876ABC82D E14C2D99575790F B01C13969075974F555C8C880 23F9ABF891F72865CE07EFBC EE6C2D906D410D5 A4E47FD76DC8ED8E147EA817 65EDC32ED1E11CFF27D13826 6E3770C7CF953322 95B97A5DA68FCB73C98CD931 1C56747545DB5260122DDF6FA E7B152D3D802877
URLs de host de scripts bash	URLs hospedando scripts de bash maliciosos	https[:]// iCloudServers[.]com/gm/install[.]sh https[:]// Macostutorial[.]com/iterm2/install[.]sh
URLs de host shamos	URLs que hospedam cargas úteis de Shamos	https[:]// iCloudServers[.]com/gm/atualização https[:]// Macostutorial[.]com/iterm2/atualização

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**