Lazarus Group tem como alvo o Windows 11 com táticas clickfix e ofertas

Data: 2025-08-30 00:29:53

Autor: Inteligência Against Invaders

A notória organização de ameaça persistente avançada de Lazarus (APT), que qi'anxin rastreia

internamente como APT-Q-1, foi vista usando a técnica Clickfix para penetrar nos sistemas Windows

11 e MacOS em uma sofisticada progressão de ataques de engenharia social.

Conhecido por incidentes de alto perfil como o Sony Pictures Hack de 2014, Lazarus mudou de roubo de inteligência para extração de ativos financeiros desde 2014, direcionando entidades como trocas de criptomoedas e instituições financeiras.

Esta campanha mais recente aproveita as ofertas falsas de emprego divulgadas por meio de contas falsas de mídia social para atrair as vítimas a armadilhas de phishing, implantando malware como Beavertail e InvisibleFerret.

Análises recentes do Centro de Inteligência de Ameaças Qi'anxin revela Um script em lote que se disfarça de atualização de software da NVIDIA, facilitando a implantação dessas cargas úteis nas plataformas.

Implantação de malware

O ataque começa com as vítimas que encontram um site de entrevista de emprego enganoso que os leva a resolver uma falha de configuração de câmera fabricada.

Isso leva à execução do clickfix-1.bat (md5: f9e18687a38e968811b93351e9fca089), que baixará a Arquivo de Zip maliciosonvidiarElease.zip (md5: a4e58b91531d199f268c5ea02c7bf456), de hxxps: //driverServices.store/visiodrive/nvidiarelase.zip.

Após a descompressão, o arquivo é executado.

Se correspondido, ele inicia o drvupdate.exe backdoord (MD5: 6175EFD148A89CA61B6835C77ACC7A8D), enquanto simultaneamente a verificando um ambiente Node.js.

O node.js ausente aciona shell.bat (md5: 983a8a6f4d0a8c887536f5787a6b01a2) para baixá -lo e instalá -lo, seguido por comandos npm) para executar main.js (md5: b52e105bd040bda639e9e951f (md5: b52e105bd040bda639e9e9e951f (md5: b52e105bd040bda639e95e951f (md5: b52e105bd040bda639e9e95e951F (b52e105bd040bda639e9e95en.

Beavertail, um Infotealer de plataforma cruzada preferida por Lazarus, se comunica com servidores de comando e controle (C2), como hxxp: //45.159.248.110, e prossegue para buscar cargas pagas

adicionais. (MD5: 17EB90AC00007154A6418A91BF8DA9C7). A persistência é alcançada por meio de modificações de registro, incorporando comandos em %userprofile %.pyppythonw.exe para garantir acesso a longo prazo.

Para variantes do macOS, scripts como Arm64-Fixer (md5: cdf296d7404bd6193514284f021bfa54) imitam correções de arquitetura do braço, implantando similar Beavertail Instâncias através de arquivos Drivfixer.sh e Launchagents Plist para persistência, com C2 em HXXP: //45.89.53.54.

O backdoor drvupdate.exe, conectando -se a 103.231.75.101:888, suporta várias funções, incluindo a execução de comandos via cmd.exe (instrução 0x6), operações de leitura/gravação de arquivo (0x8 e 0x18) e as informações do dispositivo, o sedimento (0x4), como usernames, hostnoms, hostn, hostn, hostn, hostn, hostn, hostn.

Ele autentica a conectividade C2 por meio de mecanismos de resposta a desafios, permitindo que os invasores emitam comandos do sono (0x9) ou manipule arquivos com subcomandos para abertura, escrita e fechamento de operações.

A rastreabilidade vincula esses artefatos a Lazarus devido a semelhanças de scripts com relatórios anteriores e o uso consistente de Beavertail e InvisibleFerret, estendendo o alcance da campanha aos ecossistemas Windows e MacOS.

Implicações mais amplas

Esta campanha Clickfix ressalta a exploração adepta de vulnerabilidades psicológicas de Lazarus, ignorando as defesas técnicas, induzindo as vítimas a malware auto-excluído sob o pretexto de correções de rotina.

As organizações devem aplicar a verificação estrita de comunicações relacionadas ao trabalho e evitar executar scripts ou atualizações não solicitadas de fontes não confiáveis.

A suíte de Qi’anxin, incluindo a plataforma de inteligência de ameaças (TIP) e o sistema de detecção de ameaças avançadas de Tianyan, fornece detecção robusta contra tais ameaças.

O backup de dados críticos, aplicando patches oportunos e utilizando plataformas de análise de arquivos para executáveis ??desconhecidos são defesas essenciais.

Como grupos adequados como Lazarus refinam a engenharia social com táticas de plataforma cruzada, a vigilância contra interações on-line enganosas permanece primordial para impedir a inteligência e operações de roubo financeiro.

Indicadores de compromisso (COI)

Categoria	Detalhes do COI
MD5 (Windows)	F9E18687A38E9688811B93351E9FCA089, A4E58B91531D199F268C5EA02C7BF456, 3EF7717C8BCB26396FC50ED92E812D13, 98. B73FD8F21A2ED093F8CAF0CF4B41AA4D
MD5 (macOS)	CDF296D7404BD6193514284F021BFA54, CBD183F5E5ED7D295D83E29B62B15431,

Categoria	Detalhes do COI
	A009CD35850929199EF60E71BCE8830, 13400D5C844B7AB9AACC81822B1E7F02
MD5 (Beavertail)	B52E105BD040BDA6639E958F7D9E3090, 15E48AEF2E26F2367E5002E6C3148E1F
C & c	driverServices.Store, Block-Digital.Online, hxxp: //45.159.248.110, hxxp: //45.89.53.54, 103.231.75.101:8888
Url	hxxps: //driverServices.store/visiodrive/nvidiarelase.zip, hxxps: //diverservices.store/visiodrive/nvidiareleasenew.zip, hxxps: //drivers.store/visiodrive/arm64-fixer, //drivers.store/visiodrive/arm64-fixer, hxxps: //driverServices.store/visiodrive/arm64-fixernew, hxxps: //block-digital.online/drivers/cam_driver

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