Playbook de Kimsuky Hackers descoberto no despejo de dados 'Kim' expo

Data: 2025-09-08 17:33:28

Autor: Inteligência Against Invaders

Uma rara violação atribuída a um ator afiliado norte -coreano chamado “Kim” pelos vazadores

revelou uma visão sem precedentes sobre as operações de Kimsuky (APT43).

Apelidado de dump “Kim”, o conjunto de dados de 9 GB inclui históricos de bash ativos, domínios de phishing, fluxos de trabalho de OCR, estagiários personalizados e evidências de rootkit linux –revelado Uma campanha híbrida que aproveita as ferramentas e a infraestrutura da língua chinesa para direcionar redes sul-coreanas e taiwanesas.

Este vazamento destaca um modelo de intrusão focado em credenciais destinado aos sistemas PKI do governo, avançado Aitm phishinge persistência profunda do sistema.

Parte I: Análise técnica dos materiais de despejo

Desenvolvimento interativo de malware
Os arquivos de histórico de terminais demonstram montagem de malware em voo usando NASM para código de shell de baixo nível, com comandos de compilação e limpeza iterativa. Essa abordagem prática ressalta um carregador sob medida e um fluxo de trabalho da ferramenta de injeção.

Reconhecimento orientado a OCR
Os comandos OCR processaram PDFs em língua coreana nos padrões PKI e configurações de VPN. Executando ocrmypdf -l kor+eng contra documentos como *?????? _ ???? _141125.pdf*o ator extraiu dados de certificado e configuração de rede para falsificação de falsificação e credenciais.

Logs de gerenciamento de acesso privilegiado (PAM)
As entradas de log do PAM marcadas com ???? (“Alterar completas”) revelam rotações sistemáticas de contas de alto privilégio-Oracle, Svradmin, APP_ADM01-apontando para acesso de back-end sustentado.

Infraestrutura de phishing sofisticada
Uma rede de domínios falsificados (segurança nid[.]com, webcloud-noticice[.]com, Koala-App[.]com) imitou portais do governo coreano, implantando proxies do AITM para capturar credenciais em tempo real. E -mails do queimador (por exemplo, Jeder97271[@]WUZAK[.]com) Coleção de credenciais furtivas facilitadas.

Implante de rootkit Linux
O despejo contém um rootkit furtivo (vmmisc.ko) usando canais Syscall e guinchos secretos. Instalado em /usr/lib64/tracker-fs/esconde arquivos, processos e portas de rede enquanto oferece Socks5 Proxy, conchas PTY Backdoor e sessões de controle criptografadas por meio de um binário

cliente protegido por senha.

Reconnaissance de Taiwan
Os registros de rede mostram acesso direcionado ao governo de Taiwan e IPS acadêmico (domínios .tw e rastreios diretos .git), indicando reconhecimento da cadeia de suprimentos destinado a repositórios internos e portais de autenticação em nuvem.

Falsificação mais sofisticada foi vista em locais que emulam agências governamentais oficiais como o DCC.mil[.]KR, Spo.go[.]KR e MOFA.GO[.]kr.

Parte II: Motivação e objetivos do ator Apt

Domínio de credenciais e comprometimento da PKI
Central para a campanha é o roubo de certificados GPKI (por exemplo, 136???001_env.key) e senhas de texto simples, permitindo falsificação de identidade em sistemas do governo sul -coreano. Language da política e os registros da PAM extraídos com OCR confirmam uma estratégia de colheita de credenciais, abuso de certificados e persistência no nível do insider.

Mapa de conexões de domínio.

Expansão para Taiwan
Além da Coréia, o ator sondou portais corporativos de Taiwan (Tw.systexcloud[.]com, mlogin.mdfapps[.]com) e .git repositórios (caa.org[.]TW), sinalizando um mandato regional expandido para espionagem, cadeia de mantimentos infiltração e roubo de credencial.

Pegada Hybrid DPRC -PRC
Artefatos de língua coreana localizados e configurações de sistema UTC+9 apontam para a origem da RPDC, enquanto o uso extensivo de plataformas chinesas (Gitee, Baidu, Zhihu) e o comportamento simplificado da navegação chinesa indicam operação física dentro da China ou suporte à infraestrutura da PRC. Essa fusão amplifica o alcance e ofusca a atribuição.

Persistência a longo prazo
A compilação manual do código de shell, a implantação do rootkit e o phishing do AITM reflete uma mistura de táticas da velha escola com o engano moderno. A camuflagem cultural do operador – embutida em artefatos de mídia social chinesa – o escrava sua verdadeira identidade e permite iscas mais credíveis.

Parte III: compartimento de relatório CTI para analistas

Táticas, técnicas e procedimentos (TTPs)

- Desenvolvimento de código de shell baseado em NASM e resolvido por hash Chamadas de API.
- Extração de OCR da documentação coreana de PKI e VPN.
- AITM phishing via proxies TLS e e -mails de queimadores.
- Linux rootkit com syscall enganche e backdoor criptografado.
- Reconhecimento direto de repositórios de Taiwan .git.

Recomendações

- Monitore os artefatos da cadeia de ferramentas NASM nos hosts de desenvolvedores.
- Detecte o uso da ferramenta OCR contra coleções de PDF sensíveis.
- Bloco e sumidou domínios de phishing conhecidos e proxies AITM.
- Empregue o monitoramento da integração do arquivo em caminhos de rootkit suspeitos.
- Audite os logs Pam e SSH para entradas não autorizadas “????”.

Sem dúvida, uma análise mais aprofundada do dump “Kim” revelará novas idéias adicionais. Analistas e defensores devem continuar revisando e neutralizando qualquer ativo queimado restante ou infraestruturas clonadas para reduzir essa ameaça híbrida em evolução.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.