




Your IT Company

Principais Vulnerabilidades e Ameaças (março/26)

Sumário

1. Objetivo	2
2. Vulnerabilidades e Ameaças descobertas	2
2.1. Linux rootkits usam eBPF avançado e io_uring para se esconder — ameaça crescente.....	2
2.2. Nova campanha ClickFix explora Windows Terminal para instalar o Lumma Stealer	3
2.3. Transparent Tribe usa IA para produzir em massa “vibeware” mirando governos, embaixadas e empresas.....	5
2.4. Atores vinculados à China atacam provedores de telecomunicações na América do Sul com três novos malwares	7
2.5. Vulnerabilidade crítica no plugin WordPress “User Registration & Membership” permite criação de administradores sem autenticação	9
2.6. Phishing finge ChatGPT e Gemini e empurra apps falsos na App Store para roubar credenciais do Facebook	11

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		2 de 13

1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

2. Vulnerabilidades e Ameaças descobertas

2.1. Linux rootkits usam eBPF avançado e io_uring para se esconder — ameaça crescente

Linux rootkits evoluíram para explorar recursos de kernel como eBPF e io_uring, permitindo que implantes maliciosos se escondam sem carregar módulos tradicionais. Essa técnica torna detecção e remoção muito mais difíceis, representando risco imediato para ambientes em nuvem, provedores e infraestruturas críticas.

Exploração


Rootkits têm como objetivo principal manter persistência e permanecer invisíveis no sistema, ocultando processos, arquivos e conexões de rede para evitar detecção por ferramentas de segurança e administradores.

Com a evolução do ecossistema Linux, atacantes passaram a explorar tecnologias como eBPF, originalmente criada como uma máquina virtual segura dentro do kernel para filtragem de pacotes e observabilidade. Nesse cenário, invasores carregam bytecode eBPF que, após passar pelo verificador e pelo mecanismo de JIT, é executado como código nativo no kernel sem necessidade de módulos LKM. Isso permite interceptar syscalls, tracepoints e hooks de LSM sem modificar diretamente tabelas ou o código do kernel.

Os principais alvos incluem servidores em nuvem, ambientes containerizados, infraestrutura de telecomunicações, sistemas governamentais e ambientes de computação de alto desempenho (HPC). O impacto potencial envolve persistência de longo prazo, movimentação lateral silenciosa, coleta de dados sensíveis e controle remoto do sistema, frequentemente sem detecção por scanners tradicionais que se baseiam apenas na busca por módulos de kernel carregados.

Mitigação e Prevenção

- **Recomendações gerais:**
 - **Auditoria e inspeção eBPF:** use bpftool para listar programas e mapas carregados (ex.: bpftool prog show, bpftool map show). Procure programas inesperados anexados a tracepoints ou LSM hooks.
 - **Monitoramento de io_uring:** registre e alerte uso anômalo dos syscalls io_uring_enter e io_uring_register.
 - **Restringir eBPF para não privilegiados:** se não for necessário, defina kernel.unprivileged_bpf_disabled=1 via sysctl para impedir carga de eBPF por usuários não privilegiados.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		3 de 13

- **Políticas de kernel e assinatura de módulos:** habilite lockdown do kernel, exija assinatura de módulos e mantenha Secure Boot configurado corretamente.
- **Atualização e hardening:** mantenha kernels atualizados (corrija rapidamente vulnerabilidades e aplique versões que endurecem mecanismos de hooking).
- **Telemetria abaixo do SO:** invista em soluções de monitoramento com visibilidade abaixo do kernel (ex.: instrumentação hipervisor/VM introspection, hardware-assisted telemetry) e em memory forensics para detectar rootkits que se ocultam da userland.
- **Controle de capacidades e princípio do menor privilégio:** para containers e processos, remova capacidades como CAP_BPF/CAP_SYS_ADMIN quando não necessárias; evite executar containers como root; use políticas de runtime que limitem recursos.
- **Resposta e forense:** ao suspeitar de comprometimento, capture memória e imagens de disco para análise offline (memory forensics), verifique integridade do kernel e compare com hashes/assinaturas conhecidas.
- **Recomendações por público:**
 - **Administradores de sistema:** habilitar logs/auditoria dos syscalls io_uring, usar bpftool rotineiramente, aplicar políticas de kernel lockdown, assinar módulos, restringir eBPF e atualizar kernels.
 - **Equipes de segurança/EDR:** adicionar detecção de padrões de eBPF suspeitos, integrar telemetria de baixo nível e regras de auditoria para io_uring; validar ferramentas EDR frente a técnicas que reduzem eventos de syscall.
 - **Usuários finais/Desenvolvedores:** evite executar binários não confiáveis; seguir boas práticas em containers (não rodar como root, usar imagens mínimas); reportar comportamento anômalo aos administradores.


Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/linux-rootkits-using-advanced-ebpf/>.

2.2. Nova campanha ClickFix explora Windows Terminal para instalar o Lumma Stealer

A campanha ClickFix agora instrui vítimas a abrir o Windows Terminal e colar um comando malicioso, permitindo a execução de um payload sem prompts visíveis. O objetivo final é entregar o Lumma Stealer para roubo de credenciais em navegadores; a técnica explora comportamento humano e contorna detecções tradicionais focadas no diálogo Run.

Exploração

A técnica ClickFix é uma forma de engenharia social que surgiu em 2024 e teve forte crescimento em 2025. O método engana usuários para executar comandos manualmente no sistema sob o pretexto de resolver um erro técnico ou completar uma verificação.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		4 de 13

Na variante observada em fevereiro de 2026, páginas comprometidas utilizam JavaScript para copiar automaticamente um comando PowerShell codificado (hex + XOR) para a área de transferência da vítima, sem qualquer aviso. Em seguida, a página exibe CAPTCHAs falsos ou alertas de verificação, muitas vezes imitando serviços como Cloudflare ou Microsoft, instruindo o usuário a abrir o Windows Terminal (atalho Windows + X seguido de “I”) e colar o comando para “corrigir” o suposto problema.

Quando o usuário executa o comando, o PowerShell decodifica o script diretamente em memória, conecta-se a servidores controlados pelos atacantes e baixa componentes adicionais. Entre eles estão um executável disfarçado (um 7-Zip renomeado) e um arquivo ZIP contendo o estágio seguinte do malware, que é extraído e executado silenciosamente no sistema.


A persistência é obtida por meio da criação de uma tarefa agendada. O malware é armazenado em C:\ProgramData\app_config\ctjb e injeta código em processos de navegadores utilizando a técnica QueueUserAPC. Em seguida, extrai dados sensíveis de arquivos como Login Data e Web Data de navegadores baseados em Chromium (como Chrome e Edge) para roubo de credenciais.

A campanha apresenta alta evasão porque utiliza componentes legítimos do sistema, como wt.exe (Windows Terminal). Como o PowerShell é iniciado a partir desse processo confiável, algumas regras de detecção focadas em execução via Run dialog ou outros vetores comuns podem não gerar alertas.

Mitigação e Prevenção

- **Recomendações gerais:**

- **Treinamento de usuários:** nunca colar comandos vindos de sites, pop-ups ou fontes não verificadas; desconfiar de CAPTCHAs/alertas que exigem execução de comandos.
- **Política de privilégios:** limitar acesso ao Windows Terminal e ao PowerShell apenas a contas administrativas via Group Policy.
- **Controle de execução:** aplicar AppLocker/Windows Defender Application Control para bloquear executáveis renomeados e impedir execução de binários não autorizados (incluindo 7-Zip renomeados).
- **Monitoramento e detecção:** configurar EDR/antimalware para alertar em atividades de PowerShell iniciadas por wt.exe; habilitar ScriptBlockLogging e Module Logging do PowerShell para detectar decodificação em memória.
- **Auditoria de persistência:** revisar HKCU\Software\Microsoft\Windows\CurrentVersion\Run e entradas no Agendador de Tarefas para tarefas desconhecidas; remover o que for malicioso.
- **Resposta e recuperação:** isolar sistemas suspeitos, executar varredura completa com EDR e antimalware, redefinir credenciais impactadas e forçar MFA onde aplicável.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		5 de 13

- **Atualizações e regras de rede:** manter definições antimalware atualizadas e bloquear conexões de saída para infraestrutura maliciosa conhecida (quando identificada).
- **Hardening de navegador:** restringir capacidade de páginas web de escrever na área de transferência quando possível; usar políticas de navegador e extensões que limitem ações de clipboard iniciadas por sites.
- **Recomendações por público:**
 - **Administradores de sistema:** aplicar GPOs para restringir wt.exe/PowerShell, implementar AppLocker/WDAC, habilitar logging PowerShell, revisar tarefas agendadas e chaves Run periodicamente, integrar regras EDR para PowerShell→wt.exe.
 - **Usuários finais:** não colar/rodar comandos de sites; ao receber instruções técnicas por site/telefone, validar com suporte interno; reportar prompts suspeitos ao time de segurança.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/new-clickfix-attack-leverages-windows-terminal/>.

2.3. Transparent Tribe usa IA para produzir em massa “vibeware” e mira governos, embaixadas e empresas


Transparent Tribe (também identificado como APT36) passou a empregar ferramentas de codificação assistidas por IA para gerar em grande volume implantes descartáveis, o chamado “vibeware”, escritos em linguagens menos comuns (Nim, Zig, Crystal, Rust, Go). A campanha visa principalmente o governo indiano, suas embaixadas e outras vítimas regionais, usando vetores de phishing (LNKs em ZIP/ISO e PDFs) e serviços confiáveis (Slack, Discord, Supabase, Google Sheets/Drive) para dificultar a detecção.

Exploração

Vibeware, também descrito como Distributed Denial of Detection (DDoD), refere-se a uma estratégia em que atacantes distribuem grande quantidade de binários descartáveis e variados para dificultar a detecção baseada em assinaturas ou telemetria tradicional. Ao utilizar amostras diferentes entre si, os operadores reduzem a eficácia de mecanismos de segurança que dependem de padrões estáticos.

A campanha geralmente começa com phishing. As vítimas recebem e-mails contendo arquivos ZIP ou ISO com atalhos do Windows (.LNK) ou PDFs com botões como “Download Document”, que redirecionam para o download de novos arquivos ZIP. Ao executar o .LNK, um comando PowerShell é disparado em memória, responsável por baixar e iniciar o backdoor principal no sistema comprometido.

Após o acesso inicial, os atacantes utilizam backdoors e *loaders* desenvolvidos em linguagens menos comuns, como Crystal, Nim, Zig, Rust e Go, além de integrar serviços legítimos como canais de comando e controle. Entre esses serviços estão plataformas amplamente utilizadas, como Slack, Discord, Firebase e Google Drive, o que ajuda a camuflar o tráfego malicioso. Também

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		6 de 13

foram observadas ferramentas de pós-exploração, como Cobalt Strike e Havoc, usadas para ampliar o controle após a intrusão inicial. Diversos artefatos específicos foram identificados, incluindo loaders como Warcode (Crystal), NimShellcodeLoader, CreepDropper (.NET), além de implantes como SHEETCREEP, MAILCREEP, SupaServ e LuminousStealer.

Os principais alvos identificados incluem órgãos do governo indiano, embaixadas, entidades governamentais do Afeganistão e empresas privadas. O impacto potencial envolve execução remota de código, persistência no ambiente comprometido, movimentação lateral na rede, exfiltração de documentos e credenciais, além da ampliação das capacidades de ataque por meio de ferramentas avançadas de pós-exploração.


Mitigação e Prevenção

- **Recomendações gerais:**

- Bloquear e analisar anexos compactados e imagens ISO recebidas por e-mail; filtrar ou bloquear LNK dentro de anexos.
- Bloquear/inspecionar downloads iniciados por PDFs que contenham botões de “Download Document” e redirecionamentos externos suspeitos.
- Impedir execução de PowerShell invocado por atalhos e processos de usuário sem justificativa; aplicar políticas de execução restritivas (constrain PowerShell, habilitar ConstrainedLanguage, registrar/inspecionar comandos em memória).
- Implementar proteção comportamental e EDR com detecção de reflective loading, execução in-memory e uso anômalo de APIs do sistema.
- Aplicação de allowlisting (AppLocker, WDAC) para reduzir execução de binários não aprovados, inclusive de linguagens raras.
- Monitorar e controlar acesso a serviços de terceiros (Slack, Discord, Supabase, Firebase, Google Sheets/Drive); aplicar proxies/filtragem para tráfego API e controles de DLP para uploads a serviços de nuvem.
- Ativar MFA em todas as contas e restringir privilégios de conta; segmentar rede para limitar movimento lateral.
- Atualizar e aplicar hardening: EDR, AV com heurística moderna, monitoramento de telemetria baseada em comportamento, correções e inventário de software.
- Preparar e executar caçadas por sinais de comprometimento (hunt) após aplicar patches: procurar processos/execuções atípicas, contas administrativas adicionadas, conexões incomuns ao banco.

- **Recomendações para administradores:**

- **Criar regras de detecção em SIEM/EDR para:** execução de PowerShell a partir de .LNK; processos que reflitam carregamento de shellcode; criação/execução de

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		7 de 13

binários de linguagens não usuais; uso massivo e heterogêneo de executáveis por endpoints.

- Realizar threat hunting por sinais de Cobalt Strike/Havoc e loaders reflectivos; capturar imagem de memória para análise se houver suspeita.
- Bloquear execução de binários em pastas temporárias e em perfis de usuário públicos; restringir montagem de imagens ISO e execução direta dessas imagens.
- **Recomendações para usuários finais:**
 - Não abrir anexos de remetentes desconhecidos; desconfiar de arquivos ZIP/ISO e atalhos (.LNK).
 - Evitar clicar em links de fontes não verificadas (especialmente PDFs que iniciem downloads automáticos).
 - Reportar e-mails suspeitos ao time de segurança imediatamente.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://thehackernews.com/2026/03/transparent-tribe-uses-ai-to-mass.html>.

2.4. Atores vinculados à China atacam provedores de telecomunicações na América do Sul com três novos malwares


Um grupo APT ligado à China, rastreado como UAT-9244, vem atacando provedores de telecomunicações na América do Sul desde 2024, usando três implantes (TernDoor, PeerTime e BruteEntry) para obter acesso profundo à infraestrutura de rede.

A campanha mira endpoints Windows e Linux e dispositivos de borda da rede, permitindo persistência, movimentação lateral e expansão por força bruta contra serviços como SSH, PostgreSQL e Apache Tomcat — representando risco real à disponibilidade e confidencialidade das comunicações.

Exploração

O ator de ameaça UAT-9244 tem como principal alvo provedores de telecomunicações, com o objetivo de coletar inteligência e comprometer sistemas de roteamento e gerenciamento de comunicações. Pesquisadores da Cisco Talos apontam sobreposição de ferramentas e alvos que sugerem possível ligação com os grupos FamousSparrow e Tropic Trooper.

Entre as ferramentas utilizadas está o **TernDoor**, um backdoor para Windows entregue por meio de DLL side-loading. Nesse método, um executável legítimo (wsprint.exe) carrega uma DLL maliciosa (BugSplatRc64.dll). O loader lê um arquivo codificado, descriptografa seu conteúdo com a chave hardcoded qwiozpVngruhg123 e executa o shellcode diretamente em memória. O payload é então injetado no processo msiexec.exe, de onde passa a ler sua configuração (IP e porta do C2, tentativas de reconexão e User-Agent), executar comandos remotos, manipular arquivos e estabelecer persistência. Para garantir execução após reinicialização, o malware cria uma tarefa agendada chamada WSPrint, altera chaves de registro para ocultá-la, adiciona uma entrada em Registry Run e instala o driver WSPrint.sys como serviço para controlar ou pausar processos, o que pode ser usado para desabilitar ferramentas de segurança.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		8 de 13

No ambiente Linux, foi identificado o PeerTime, um backdoor que utiliza o protocolo BitTorrent para comunicação e execução de comandos remotos. Esse método permite que o tráfego malicioso se misture ao tráfego P2P legítimo, dificultando a detecção em redes que já utilizam esse tipo de protocolo. O binário também contém strings de depuração em chinês simplificado, fornecendo um possível indicativo linguístico sobre os operadores.


Outra ferramenta observada é o BruteEntry, responsável por transformar dispositivos de borda comprometidos em Operational Relay Boxes (*ORBs*). Esses sistemas passam a executar ataques automatizados de força bruta contra serviços como SSH, PostgreSQL e Apache Tomcat, expandindo gradualmente a infraestrutura controlada pelos atacantes.

Na infraestrutura de comando e controle, a Talos identificou um certificado SSL compartilhado associado a 18 endereços IP diferentes, indicando uma operação estruturada e com presença distribuída.

O impacto potencial inclui comprometimento de sistemas de gerenciamento de rede, exfiltração de dados sensíveis, interrupção de serviços de telecomunicações e uso da infraestrutura comprometida como ponto de pivot para atacar outras redes críticas.

Mitigação e Prevenção

- **Para administradores de sistemas / equipes de segurança:**
 - **Auditar imediatamente:** verifique tarefas agendadas com nomes suspeitos (ex.: *WSPrint*), entradas em Registry Run e alterações recentes em chaves relacionadas a tarefas agendadas.
 - **Detectar DLL side-loading:** monitorar carregamento de DLLs por executáveis em diretórios de aplicação e exigir assinaturas digitais válidas.
 - Monitorar processos legítimos alterados: alertar para *msiexec.exe* (e outros processos de instalação) com injeção de código, rede ativa não esperada ou carregamento de módulos anômalos.
 - **Controlar drivers de kernel:** aplicar política para aceitar apenas drivers assinados e conhecidos; bloquear instalação de drivers não assinados e auditar *WSPrint.sys* ou drivers desconhecidos. Habilitar mitigação de kernel signing enforcement (Device Guard/HVCI onde aplicável).
 - **Endpoints e detecção:** implantar/atualizar EDR e regras de detecção para execuções em memória, shellcode e assinaturas ClamAV indicadas (*Win.Malware.TernDoor*, *Unix.Malware.BruteEntry*, *Unix.Malware.PeerTime*). Ativar SNORT/IDS com a SID 65551 recomendada.
 - **Hardening de serviços alvo de brute force:** aplicar autenticação forte/MFA para administrações, desabilitar autenticação por senha em SSH (usar chaves), aplicar rate limiting e fail2ban para SSH/PostgreSQL/Tomcat, revisar políticas de senha e bloquear IPs maliciosos conhecidos.


	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		9 de 13

- **Segmentar redes e isolar borda:** separar planos de controle da rede de produção; limitar acesso administrativo remoto; restringir comunicação de dispositivos de borda a servidores essenciais.
- **Monitorar tráfego P2P e BitTorrent:** gerar alertas para anomalias em tráfego BitTorrent em segmentos onde não é esperado; inspecionar padrões de comunicação que possam ocultar C2 (peers incomuns, portas/swarms não usuais).
- **Monitoramento de certificados:** detectar certificados SSL/TLS compartilhados e uso massivo do mesmo certificado em IPs divergentes; revogar/rotacionar quando detectar abuso.
- **Resposta a incidentes:** isolar hosts infectados, coletar memória/artefatos (dump de memória, imagens de disco), preservar logs, resetar credenciais comprometidas, reinstalar hosts críticos quando necessário e conduzir análise forense para identificar escopo.
- **Para usuários finais / operadores:**
 - Evitar execução de binários não confiáveis; não executar instaladores ou arquivos recebidos sem validação.
 - Manter sistemas e firmware atualizados; aplicar atualizações de segurança para OS, serviços (PostgreSQL, Tomcat) e dispositivos de borda.
 - Usar autenticação multifator para contas administrativas e rotacionar credenciais periodicamente.
 - Reportar comportamentos incomuns (lentidão, reinícios inesperados, tarefas agendadas estranhas) à equipe de TI.
- **Passos imediatos recomendados:**
 - Procurar por presença de arquivos/nome de tarefa/driver mencionados abaixo; isolar e coletar amostras.
 - Aplicar assinaturas ClamAV indicadas e SNORT SID 65551.
 - Auditar logs de autenticação e tentativas de força bruta em SSH/PostgreSQL/Tomcat e bloquear padrões recorrentes.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/china-nexus-hackers-attacking-telecommunication/>.

2.5. Vulnerabilidade crítica no plugin WordPress “User Registration & Membership” permite criação de administradores sem autenticação

O plugin User Registration & Membership para WordPress apresenta uma falha crítica (CVE-2026-1492) que permite a atacantes não autenticados criar contas com privilégios de administrador,

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		10 de 13

possibilitando a tomada total do site. A exploração já foi observada em ambiente real e há bloqueios de ataques, portanto a atualização imediata é necessária.

Exploração

A vulnerabilidade decorre de má gestão de privilégios no processo de registro de usuários. Em versões até 5.1.2, o sistema aceita o valor do parâmetro role enviado pelo próprio usuário no momento do cadastro, sem aplicar uma allowlist ou validação adequada no lado do servidor.

Um atacante pode explorar a falha enviando uma requisição ao endpoint de registro com o parâmetro role=adminstrator. Como não há validação server-side, o plugin cria automaticamente uma conta com privilégios administrativos.


O impacto é crítico, pois permite a criação de contas administrativas sem autenticação prévia. Com esse acesso, um invasor pode roubar dados, modificar conteúdo do site, instalar backdoors e assumir controle total da aplicação.

A falha possui pontuação CVSS 9.8 e foi descoberta pelo pesquisador Foxyyy. O relatório também menciona tentativas ativas de exploração, com dezenas de ataques bloqueados em um curto período.

Como agravante, a mesma versão (5.1.2) apresenta outra vulnerabilidade de Authentication Bypass (CVE-2026-1779), aumentando significativamente o risco para instalações não atualizadas. A correção foi disponibilizada pelo fornecedor na versão 5.1.3.

Mitigação e Prevenção

- **Ações imediatas:**
 - Atualize o plugin para a versão 5.1.3 ou superior imediatamente. Esta é a medida mais importante.
 - Se a atualização não for possível imediatamente, desative o plugin temporariamente ou desabilite o registro de novos usuários até aplicar o patch.
- **Recomendações de remediação e detecção pós-comprometimento:**
 - Realize uma revisão completa de contas (access review) e remova/análise quaisquer administradores recém-criados ou desconhecidos.
 - Altere senhas de contas administrativas legítimas e rotacione chaves/segregos sensíveis.
 - Habilite autenticação multifator (2FA) para todas as contas administrativas.
 - Verifique logs de acesso e registros de registro (registration endpoint) em busca de requisições suspeitas contendo parâmetros de role ou picos de registros.
 - Procure por arquivos e comportamentos anômalos (webshells, scripts desconhecidos) e verifique integridade de arquivos do WordPress.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		11 de 13

- Aplique regras de WAF (Web Application Firewall) para bloquear solicitações que tentem definir roles via parâmetro de registro e rate-limit para endpoints de registro.
- Implante validações server-side para qualquer formulário de registro (allowlist de roles) e use CAPTCHAs para reduzir registros automatizados.
- Mantenha backups recentes e planeje restauração caso haja evidência de comprometimento.
- Remova plugins não utilizados e mantenha core, temas e plugins sempre atualizados.
- Considere auditoria por ferramenta de segurança (ex.: Wordfence, Sucuri) e varredura de malware.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/wordpress-membership-plugin-vulnerability/>.

2.6. Phishing finge ChatGPT e Gemini e empurra apps falsos na App Store para roubar credenciais do Facebook

Uma campanha sofisticada de phishing que mira usuários de iPhone, usando e-mails que se passam por ChatGPT (OpenAI) e Gemini (Google) para induzir vítimas a baixar apps falsos na App Store. Os aplicativos exibem uma tela de login falsa do Facebook para colher credenciais em tempo real, permitindo acesso a perfis pessoais, contas de anúncios e páginas empresariais.

Exploração


O vetor de ataque consiste no envio de e-mails cuidadosamente elaborados que simulam comunicações legítimas de plataformas de inteligência artificial. Essas mensagens direcionam as vítimas para páginas de aplicativos na Apple App Store, explorando a confiança que usuários normalmente têm em marketplaces oficiais.

A campanha utiliza uma forte estratégia de engenharia social baseada em uma “cadeia de confiança”: o e-mail parece legítimo, o link leva à loja oficial e o aplicativo aparenta ser confiável. Essa sequência reduz a suspeita do usuário e aumenta significativamente a probabilidade de instalação.

Durante a análise, foram identificados dois aplicativos fraudulentos publicados na loja australiana: GeminiAI Advertising (id6759005662) e Ads GPT (id6759514534). Ambos se apresentavam como ferramentas de suporte para marketing e automação com IA.

Ao abrir o aplicativo, no entanto, nenhuma funcionalidade real é oferecida. Em vez disso, o usuário é imediatamente apresentado a uma página falsa de login do Facebook. As credenciais inseridas são capturadas e enviadas diretamente para a infraestrutura controlada pelos atacantes.


O alvo principal da campanha são profissionais de marketing digital, gerentes de redes sociais e responsáveis por contas empresariais do Facebook. Uma vez comprometidas, essas contas podem ser usadas para assumir o controle de páginas, modificar campanhas de anúncios, realizar fraudes financeiras e causar danos reputacionais.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		12 de 13

O caso demonstra uma mudança tática relevante: em vez de depender exclusivamente de sites falsos, os atacantes passam a explorar marketplaces oficiais como vetor de distribuição e elemento de legitimidade para aumentar o sucesso das campanhas de phishing.

Mitigação e Prevenção

- **Ações diretas para usuários finais:**
 - Verificar o remetente real do e-mail (não confiar apenas no display name).
 - **Antes de instalar, abrir a App Store diretamente (não clicar no link do e-mail) e checar:** nome do desenvolvedor, avaliações, número de downloads, capturas de tela e inconsistências na descrição.
 - Habilitar autenticação multifator (2FA) no Facebook e em outras contas sociais.
 - **Se houver suspeita de comprometimento:** alterar a senha do Facebook, ativar 2FA, encerrar sessões ativas, revisar dispositivos conectados e revogar acessos de aplicativos de terceiros.
 - Evitar reutilizar senhas e utilizar gerenciador de senhas.
- **Ações para administradores de TI / segurança:**
 - Implementar filtragem de e-mail e regras de anti-phishing (SPF/DKIM/DMARC, análise de links).
 - Bloquear ou monitorar URLs de apps maliciosos em proxies e gateways (adicionar as URLs/IDs à blacklist).
 - Usar MDM/EMM para restringir instalação de apps em dispositivos corporativos (bloquear instalações não gerenciadas, exigir apps aprovados).
 - Exigir dispositivos gerenciados e IDs corporativos para acesso a contas sensíveis; considerar SSO para acessos corporativos.
 - Treinamento contínuo de usuários sobre phishing e procedimentos para reportar emails suspeitos.
 - Monitorar logs e alertas de login do Facebook (tentativas de acesso de IPs/geolocalizações incomuns, mudanças de administrador em páginas, atividades incomuns em contas de anúncios).
 - **Preparar playbooks de resposta a incidentes:** isolar dispositivo, coletar evidências, forçar reset de credenciais, revisar permissões de contas, notificar fornecedores (ex: Facebook) e reportar a Apple sobre os apps fraudulentos.
- **Passos imediatos de resposta:**
 - Resetar senhas afetadas e habilitar 2FA.
 - Revogar todas as sessões ativas e tokens.

	<p align="center">Inteligência de Ameaças Cibernéticas</p> <p align="center">Comite Editorial</p>	Código
		SGSI-081
		Página
		13 de 13

- Revisar histórico de faturamento e alterações em campanhas.
- Coletar e preservar logs de e-mail, dispositivos e rede para análise forense.
- Reportar a app maliciosa à Apple e às equipes de segurança da plataforma afetada (Facebook).

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/phishing-emails-push-fake-chatgpt/>.

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

A publicação do documento de Inteligência de Ameaças será realizada quinzenalmente.

Produzido por: Equipe de Threat Intelligence da Service IT Security