




Your IT Company

Principais Vulnerabilidades e Ameaças (março/26)

Sumário

1. Objetivo	2
2. Vulnerabilidades e Ameaças descobertas	2
2.1. Campanha sofisticada usa recursos anti-bot da Cloudflare para roubar credenciais do Microsoft 365 ...	2
2.2. Vulnerabilidades no Cisco IOS XR permitem execução de comandos como root e controle administrativo.....	3
2.3. Microsoft Copilot: vulnerabilidade na sumarização permite injeção de prompts e phishing confiável.....	5
2.4. Vulnerabilidade CVE-2026-3910 — V8 do Chrome permite execução remota de código	7
2.5. Malware EV-assinado se passa por Teams, Zoom e Adobe para implantar RMM e manter acesso persistente	8

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

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. Campanha sofisticada usa recursos anti-bot da Cloudflare para roubar credenciais do Microsoft 365

Uma campanha de phishing sofisticada direcionada a usuários do Microsoft 365 passou a explorar recursos legítimos da Cloudflare (como o Turnstile) para bloquear varreduras automatizadas e pesquisadores, permitindo que páginas falsas colem credenciais em tempo real. A técnica torna mais difícil a detecção e escalona o impacto, pois os ataques só apresentam o conteúdo malicioso a visitantes humanos confiáveis.

Exploração

A campanha utiliza domínios registrados via Namecheap e hospedados na infraestrutura da Cloudflare, sendo `securedsnmail[.]com` um dos domínios iniciais identificados. Essa infraestrutura é usada para hospedar páginas maliciosas e dificultar o rastreamento da operação.

Os atacantes implementam múltiplos mecanismos de filtragem para evitar análise. Entre eles estão verificação humana via Cloudflare Turnstile, checagem de IP utilizando `api.ipify[.]org` e análise de *user-agent*. Bots, crawlers e faixas de IP associadas a fornecedores de segurança ou provedores de nuvem são bloqueados antes de acessar o conteúdo real.

Caso o *user-agent* corresponda a ferramentas de indexação ou análise, como Googlebot, Bingbot, AhrefsBot ou Twitterbot — o site retorna um falso erro 404, impedindo a indexação e dificultando a investigação automatizada.


A lógica de roubo de credenciais é ofuscada dentro de uma máquina virtual JavaScript personalizada (função `e_d007dc`), que interpreta instruções codificadas para dificultar a análise estática. Se a presença de ferramentas de segurança for detectada durante a sessão, o site redireciona silenciosamente o visitante para domínios legítimos, como o Google Search, eliminando evidências da atividade maliciosa.

Usuários que passam por todos os filtros são direcionados para páginas que imitam o login do Microsoft 365, onde as credenciais são capturadas em tempo real.

O impacto potencial inclui comprometimento de contas corporativas Microsoft 365, como e-mail, documentos e identidade digital, além de acesso a dados sensíveis, movimentação lateral dentro do ambiente e uso das contas comprometidas para novas campanhas de phishing ou fraude.

Mitigação e Prevenção

- **Recomendações gerais:**
 - Habilitar autenticação multifator (MFA) forte em todas as contas Microsoft 365; preferir MFA por chave de segurança (FIDO2) ou autenticação por aplicativo em vez de SMS.


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

- **Aplicar políticas de Acesso Condicional no Azure AD:** bloqueio por localização, risco de login, requerer MFA para perspectivas anômalas.
- **Implementar detecção e resposta a credenciais comprometidas:** monitorar e bloquear logins suspeitos e forçar reset de senha quando atividade anômala for detectada.
- **Treinamento de usuários:** conscientização sobre URLs falsos, inspeção de barras de endereço, não inserir credenciais em páginas abertas a partir de links em e-mail sem verificar.
- **Recomendações para administradores e equipes de segurança:**
 - Procurar e bloquear ativamente os domínios e padrões reportados (lista de IOCs abaixo) em firewalls, proxys e soluções de filtragem de URL.
 - Procurar pelo Turnstile sitekey (0x4AAAAACG6TJhrsuzdpjsN) em serviços como Shodan, Censys e URLScan para descobrir infraestrutura maliciosa associada.
 - Monitorar logs de proxy e DNS em busca de resoluções ou conexões para os IOCs; criar alertas para conexões web a domínios listados.
 - Incluir regras de detecção para padrões URL e caminhos usados (p.ex. /KuPbXodA) e para uso atípico de api.ipify[.]org correlacionado a páginas desconhecidas.
 - Fortalecer políticas de registro/controle de novos domínios e reputação de Namecheap quando houver picos de registro em massa ou domínios com nomes similares a marcas legítimas.
 - Configurar políticas de e-mail (SPF/DKIM/DMARC) e filtros anti-phishing no gateway de e-mail; usar sandboxes de links e detecção de páginas clonadas.
 - Para equipes de resposta: coletar logs de web, proxy e autenticação ao investigar possíveis comprometimentos; preservar evidências antes que redirecionamentos posteriores as removam.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/cloudflare-anti-bot-features-microsoft-365/>.

2.2. Vulnerabilidades no Cisco IOS XR permitem execução de comandos como root e controle administrativo

Cisco divulgou um advisory de alta gravidade sobre duas vulnerabilidades de escalada de privilégios no IOS XR Software (CVE-2026-20040 e CVE-2026-20046). Um invasor autenticado e com conta de baixo privilégio pode, se explorar as falhas, executar comandos como *root* ou obter controle administrativo completo de roteadores afetados, atualização imediata é recomendada.

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

Exploração

A vulnerabilidade CVE-2026-20040 permite execução de comandos como *root* devido à validação insuficiente de argumentos fornecidos por usuários em comandos CLI específicos. Um usuário com privilégios baixos pode enviar comandos especialmente construídos no prompt e explorar essa falha para elevar privilégios, obtendo execução arbitrária no sistema operacional subjacente do Cisco IOS XR.


Já a CVE-2026-20046 é uma falha de Administrative Control Bypass causada por mapeamento incorreto de um comando CLI para grupos de tarefa (task-groups) no código-fonte. Isso permite que um usuário de baixo privilégio contorne as verificações de autorização e execute comandos que deveriam ser restritos, obtendo controle administrativo completo.

Quanto ao alcance, a CVE-2026-20040 afeta implementações do Cisco IOS XR em todas as configurações. A CVE-2026-20046 impacta especificamente roteadores Cisco IOS XRv 9000, independentemente da configuração aplicada. A Cisco confirmou que outras plataformas, como Cisco IOS, Cisco IOS XE e Cisco NX-OS, não são afetadas.

O impacto potencial inclui comprometimento total do dispositivo, com possibilidade de execução de comandos como *root*, alteração de configurações críticas, interrupção de rotas e serviços de rede, exfiltração de dados e uso do equipamento comprometido para pivot na infraestrutura. As falhas foram descobertas internamente pela equipe ASIG da Cisco e, até o momento, não há evidências públicas de exploração ativa.

Mitigação e Prevenção

- **Recomendações imediatas (administradores de rede):**
 - Atualizar imediatamente para as releases corrigidas indicadas pela Cisco (ex.: 25.2.21 ou 25.4.2) ou aplicar os Softwares Maintenance Updates (SMUs) específicos para sua plataforma.
 - Priorizar a correção de CVE-2026-20040, não existem workarounds conhecidos; a atualização é a única defesa viável.
 - **Para CVE-2026-20046:** se usa TACACS+ para AAA, configurar command authorization para restringir comandos permitidos a usuários não administrativos e negar todos os demais até a correção.
 - Rever contas administrativas e de baixo privilégio: remover acessos desnecessários, aplicar princípio do menor privilégio e rotacionar credenciais.
 - Restringir o acesso ao plano de gerenciamento: limitar via ACLs/IP Source Guard, VRFs de gerenciamento, e segmentação de rede para interfaces de administração.
 - Habilitar e exigir autenticação forte (idealmente MFA) para acesso à gestão dos dispositivos.
 - Testar atualizações em ambiente de homologação antes de aplicar em produção e manter backups das configurações.

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

- **Detecção e monitoração (operacional):**
 - Auditar logs de CLI e AAA para comandos incomuns ou tentativas de execução fora do perfil esperado.
 - Criar alertas para atividades de elevação de privilégio, criação de contas administrativas, ou mudanças críticas de configuração.
- **Recomendações para usuários finais e equipes de suporte:**
 - Evitar uso de contas com privilégios desnecessários para operações diárias.
 - Reportar imediatamente qualquer comportamento anômalo nos dispositivos de rede ao time de segurança.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/cisco-ios-xr-software-vulnerability-root/>.

2.3. Microsoft Copilot: vulnerabilidade na sumarização permite injeção de prompts e phishing confiável

Pesquisadores descobriram uma vulnerabilidade de Cross-Prompt Injection (XPIA) em superfícies de sumarização do Microsoft 365 Copilot (CVE-2026-26133) que permite inserir texto controlado por atacante dentro de um e-mail para forjar saídas confiáveis do assistente. A exploração pode produzir notificações/links convincentes dentro do painel de resumo e até exfiltrar contexto interno, representando risco imediato para usuários e organizações que usam Copilot.

Exploração


A falha pertence à classe Cross-Prompt Injection Attack (XPIA), que ocorre quando um modelo de linguagem interpreta conteúdo não confiável como o texto de um e-mail, como se fossem instruções válidas a serem executadas.

No cenário analisado, a pipeline de sumarização do Microsoft Copilot processa o conteúdo bruto do e-mail sem distinguir adequadamente entre texto informativo e possíveis comandos embutidos. Assim, um e-mail malicioso contendo um “bloco de instruções” pode induzir o assistente a gerar respostas manipuladas, incluindo texto, botões ou links falsificados, apresentados no formato e na “voz” do Copilot, o que aumenta a credibilidade da mensagem.

Os testes foram realizados em diferentes superfícies, como o botão Summarize no Microsoft Outlook, o painel Copilot no Outlook e o Copilot integrado ao Microsoft Teams. O comportamento variou entre interfaces, sendo observado que o ambiente do Teams apresentou maior probabilidade de incorporar o conteúdo malicioso nas respostas geradas.

O impacto potencial inclui a geração de phishing altamente convincente dentro da própria interface do Copilot. O assistente pode criar links que incorporam contexto interno, como mensagens do Teams ou arquivos armazenados no Microsoft OneDrive e no Microsoft SharePoint, que, ao serem acessados, podem enviar essas informações para infraestrutura controlada pelo atacante. Esse cenário possibilita exfiltração de dados com apenas um clique, sem necessidade de execução de código ou anexos maliciosos tradicionais.

A relevância do ataque está no fato de que usuários tendem a confiar em conteúdos apresentados por assistentes de IA. Como o Copilot pode acessar diversos repositórios corporativos

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

conforme as permissões do usuário, a exploração desse comportamento amplia significativamente a superfície de ataque e o risco de exposição de dados sensíveis.

Mitigação e Prevenção


- **Para administradores / equipes de segurança:**

- Aplicar o patch de março de 2026 imediatamente, Microsoft confirmou rollout completo em 11 de março de 2026.
- Auditar e reduzir o escopo de recuperação do Copilot, conceder apenas permissões estritamente necessárias (minimizar acesso a Teams, OneDrive, SharePoint quando não for essencial).
- Habilitar Microsoft Purview sensitivity labels e políticas DLP, limitar o fluxo de dados sensíveis mesmo se o Copilot tentar incorporá-los.
- Ativar Safe Links e verificação de reputação de URLs em todas as superfícies do Copilot, garantir que links gerados passem por checagens de reputação/filtragem.
- Monitorar logs e telemetria do Copilot, buscar padrões incomuns de recuperação (acesso a múltiplos repositórios, geração de links externos) que possam indicar exploração XPIA.
- 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.
- Configurar controles de acesso condicional e segmentação por dispositivo/usuário para reduzir impacto em caso de clique em links maliciosos.
- Revisar políticas de retenção e indexação que o Copilot usa para recuperação contextual (limitar índices de conteúdo sensível).

- **Para usuários finais / conscientização:**

- Treinar colaboradores para desconfiar de conteúdo em painéis/visões geradas por IA não assumir automaticamente que um resumo é “do sistema” nem clicar em botões/links sem verificação.
- Validar solicitações incomuns diretamente com remetente por um canal separado (telefone, chat corporativo) antes de tomar ações sugeridas pelo resumo.
- Reportar resumos suspeitos ao time de segurança e encaminhar o e-mail original para análise.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/microsoft-copilot-summarization-vulnerability/>.

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

2.4. Vulnerabilidade CVE-2026-3910 — V8 do Chrome permite execução remota de código

A CVE-2026-3910, é uma vulnerabilidade de alta severidade no motor V8 (JavaScript/WebAssembly) do Chrome que pode ser acionada por uma página HTML maliciosa, permitindo execução arbitrária de código dentro do sandbox do navegador. O bug já foi confirmado como explorado em ambiente real, tornando a atualização imediata do Chrome crítica para reduzir riscos de comprometimento em ambientes corporativos e pessoais.

Exploração

A vulnerabilidade decorre de uma implementação inadequada no motor V8, responsável por processar JavaScript e WebAssembly no Google Chrome. Esse tipo de falha pode levar a comportamentos inesperados durante o processamento de conteúdo web.

A exploração ocorre quando um usuário é induzido a acessar uma página HTML especialmente preparada. Ao interpretar o conteúdo, o V8 pode permitir a execução de código arbitrário dentro do processo do navegador, mesmo que ainda dentro do sandbox.

Os principais alvos são usuários que navegam na web, tanto em dispositivos pessoais quanto em estações corporativas. A exploração pode ocorrer ao visitar sites maliciosos ou páginas legítimas previamente comprometidas por atacantes.

O impacto potencial inclui execução de código no contexto do navegador, roubo de credenciais, instalação de malware e progressão do ataque quando combinado com outras vulnerabilidades ou técnicas de engenharia social, podendo levar a comprometimento mais amplo do ambiente corporativo.

Como observação adicional, a atualização também corrige a vulnerabilidade CVE-2026-3909, uma falha de out-of-bounds write no Skia, que também foi relatada como explorada ativamente. Por isso, recomenda-se aplicar a atualização completa do navegador para mitigar todos os riscos associados.

Mitigação e Prevenção

- **Atualização imediata:**
 - Atualize o Chrome para as versões corrigidas: 146.0.7680.75 e 146.0.7680.76 (Windows/macOS) ou 146.0.7680.75 (Linux).
 - Para ambientes corporativos, priorize a distribuição do patch a endpoints de usuários, estações de trabalho administrativas e sistemas compartilhados de navegação.
 - Monitore e aplique patches dos navegadores baseados em Chromium (Edge, Brave, Opera, Vivaldi), pois podem herdar a mesma exposição.
- **Para administradores de sistema / equipes de TI:**
 - Forçar atualização via solução de gerenciamento de patches (SCCM, WSUS, Intune, GPO etc.) e confirmar relançamento do navegador após a instalação.
 - Implementar políticas de gerenciamento de extensões e restringir instalações externas.

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

- Habilitar e reforçar mecanismos de mitigação do navegador: Site Isolation, Safe Browsing, sandboxing reforçado e execução de navegadores com privilégios mínimos.
- Aplicar filtragem de URL/proxy e bloqueio de domínios/malware conhecidos para reduzir a exposição a páginas maliciosas.
- Garantir EDR/antivírus com assinaturas/heurísticas atualizadas e regras de detecção para comportamentos pós-exploit (criação de processos suspeitos, injeção, conexões de comando e controle).
- **Para usuários finais:**
 - Atualize e reinicie o navegador assim que possível.
 - Evite clicar em links não solicitados e verifique URLs antes de acessar.
 - Mantenha o sistema operacional e software de segurança atualizados; não execute software de fontes não confiáveis.
- **Para equipes de segurança / SOC**
 - Priorizar a criação e aplicação de regras de detecção para padrões de exploração de navegador (comportamento anômalo no V8, processos filhos inesperados, download/execução pós-navegação).
 - Realizar caça a ameaças em endpoints com foco em sinais de execução de código a partir do navegador e movimento lateral.
 - Preparar respostas a incidentes para isolar hosts comprometidos e coletar evidências antes de restaurar.
 - Acompanhar publicações de fornecedores e feeds de inteligência (ex.: regras SIG, YARA, assinaturas EDR) para detecções específicas.


Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://socprime.com/blog/cve-2026-3910-vulnerability/>.

2.5. Malware EV-assinado se passa por Teams, Zoom e Adobe para implantar RMM e manter acesso persistente

Uma campanha de phishing ativa está distribuindo executáveis maliciosos que se disfarçam como instaladores/atualizadores do Microsoft Teams, Zoom e Adobe Reader. Os binários vêm com certificados EV legítimos (emitidos para TrustConnect Software PTY LTD), o que torna a detecção por usuários e ferramentas básicas mais difícil; ao executar, o malware instala múltiplas ferramentas RMM (ScreenConnect, Tactical RMM, Mesh Agent) para controle persistente e movimentação lateral.

Exploração

O vetor inicial da campanha consiste em e-mails de phishing contendo convites de reunião, faturas ou documentos financeiros que induzem o usuário a baixar um instalador aparentemente legítimo. A mensagem explora senso de urgência ou contexto corporativo para aumentar a probabilidade de execução do arquivo.

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

Para reforçar a credibilidade, os arquivos utilizam nomes que imitam softwares confiáveis — como msteams.exe ou adobereader.exe, e são assinados com certificados EV (Extended Validation) válidos. Essa combinação aumenta a confiança do usuário e pode contornar verificações superficiais de segurança.


Após a execução, o binário copia-se para C:\Program Files, registra-se como serviço do Windows e cria uma chave Run no registro para persistência. Em seguida, estabelece comunicação com o domínio de comando e controle trustconnectsoftware[.]com e executa comandos PowerShell codificados que utilizam msixexec para baixar e instalar ferramentas de acesso remoto.

Entre as ferramentas implantadas estão ScreenConnect, Tactical RMM e MeshCentral (por meio do agente Mesh). Esses componentes criam múltiplos backdoors e permitem controle remoto do sistema comprometido, movimentação lateral na rede, coleta de dados e instalação de payloads adicionais.

A campanha é particularmente perigosa porque combina engenharia social convincente, assinaturas digitais válidas e uso de plataformas legítimas de RMM (Remote Monitoring and Management). Essa abordagem dificulta tanto a detecção por soluções baseadas em assinatura quanto a identificação do risco pelo próprio usuário.

Mitigação e Prevenção

- **Para administradores / equipes de segurança:**
 - **Bloquear/autorizar:** implemente listas de bloqueio/permitidos para ferramentas RMM, permitir apenas soluções aprovadas. Use Windows Defender Application Control (WDAC) ou AppLocker para bloquear executáveis não autorizados.
 - **Aplicar MFA:** exigir autenticação multifator em todas as interfaces RMM aprovadas e para contas administrativas.
 - **Proteção de e-mail:** ativar Safe Links, Safe Attachments e Zero-hour Auto Purge (ZAP) no gateway/serviço de e-mail para interceptar anexos e links maliciosos.
 - **Endpoint protection:** manter proteção em nuvem ativa (cloud-delivered protection), EDR com telemetria e regras de detecção para anomalias de instalação de MSI e serviços recém-criados.
 - **Regras de redução de superfície (ASR):** habilitar regras que bloqueiem execução de binários provenientes de locais não confiáveis, bem como criação de processos via PsExec/WMI quando não autorizados.
 - **Monitoramento e detecção:** criar regras de SIEM/EDR para monitorar: criação de serviço com nomes suspeitos, chaves de Run no HKLM apontando para executáveis em Program Files não esperados, execuções de msixexec iniciadas por processos não usualmente associados, e conexões para trustconnectsoftware[.]com.
 - **Resposta a incidentes:** isolar endpoints suspeitos, coletar artefatos (binários, chaves de registro, logs de rede), buscar lateralidade por meio de contas e sessões RMM e

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

remover todos os canais RMM encontrados. Considerar solicitar revogação do certificado EV junto à autoridade certificadora se for comprovado abuso.

- **Políticas de assinatura:** validar assinaturas com políticas internas, não confiar apenas na presença de assinatura EV; verificar o contexto, reputação do assinante e cadeia de confiança.
- **Para usuários finais / colaboradores:**
 - **Treinamento:** conscientização sobre phishing, desconfiar de instaladores recebidos por e-mail ou links para “atualizações” que não venham do canal oficial da aplicação.
 - **Procedimento seguro:** nunca executar instaladores baixados de links em e-mail; preferir canais oficiais (site do fornecedor ou instalador distribuído pelo time de TI).
 - **Reporte:** encaminhar e-mails suspeitos à equipe de segurança antes de abrir anexos ou executar programas.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/signed-malware-masquerading-as-teams/>.

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