



Your IT Company

Principais Vulnerabilidades e Ameaças (outubro/26)

Sumário

1. Objetivo	2
2. Vulnerabilidades e Ameaças descobertas	2
2.1. CISA: Ransomware SafePay atingiu mais de 600 organizações de infraestrutura crítica	2
2.2. Chaves roubadas do UpdraftCentral usadas em sites WordPress backdoor	4
2.3. Múltiplas Vulnerabilidades no NGINX Permitem Negação de Serviço e Possível Execução Remota de Código	6
2.4. Hackers registraram novos domínios baseados no Teams e usaram uma página de login para roubar seus logins	8
2.5. DNS: vulnerabilidade no BIND 9 pode causar corrupção de memória e execução remota de código ...	10
2.6. Hackers Abusam de 20.000 Domínios de Páginas da Cloudflare para Divulgar Alertas de Segurança Falsos da Microsoft	12

	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. CISA: Ransomware SafePay atingiu mais de 600 organizações de infraestrutura crítica

O SafePay é uma operação de ransomware identificada em agosto de 2024 que combina criptografia de arquivos, roubo de informações e extorsão. O grupo foi associado a ataques contra mais de 600 organizações de diferentes setores de infraestrutura crítica desde agosto de 2024, segundo um alerta conjunto da CISA, do FBI e de outras autoridades internacionais. A operação emprega a estratégia de dupla extorsão: além de tornar arquivos inacessíveis, os invasores ameaçam divulgar publicamente os dados exfiltrados caso a vítima não atenda às exigências financeiras.

Exploração

O acesso inicial pode ocorrer por meio de credenciais expostas, ataques de força bruta, phishing, vulnerabilidades em VPNs e outros dispositivos expostos à internet.

Após invadir o ambiente, os atacantes podem:

- Realizar reconhecimento de contas, servidores e compartilhamentos de rede.
- Utilizar ferramentas administrativas para movimentação lateral.
- Coletar credenciais e identificar informações de alto valor.
- Compactar e transferir dados para infraestrutura externa.
- Interromper mecanismos de recuperação, incluindo cópias de sombra do Windows.
- Criptografar arquivos e exigir pagamento para suposta recuperação e não divulgação dos dados.

Impactos potenciais

- Indisponibilidade operacional: interrupção de sistemas, aplicações e serviços essenciais.
- Exposição de informações: vazamento de dados pessoais, financeiros, comerciais e estratégicos.
- Comprometimento de backups: redução da capacidade de recuperação após o ataque.

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

- Movimentação lateral: expansão do comprometimento para outros servidores e segmentos.
- Impactos em infraestrutura crítica: interrupção de operações essenciais.
- Prejuízos financeiros: custos de resposta, restauração, investigação e paralisação.
- Danos reputacionais: perda de confiança de clientes, fornecedores e parceiros.
- Extorsão continuada: ameaças de divulgação mesmo após o início da recuperação.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Investigar autenticações suspeitas em VPNs, firewalls e servidores.
 - Isolar sistemas comprometidos, preservando evidências para análise forense.
 - Revogar sessões e credenciais comprometidas e verificar possíveis acessos persistentes.
 - Bloquear indicadores maliciosos confirmados nos controles de rede e endpoint.
 - Proteger backups contra exclusão, alteração e acesso não autorizado.
 - Acionar a equipe de resposta a incidentes e avaliar obrigações de comunicação.
- **Recomendações para Administradores de Sistema:**
 - Corrigir vulnerabilidades aplicáveis em VPNs, firewalls e dispositivos de borda.
 - Exigir MFA, preferencialmente resistente a phishing, para acessos administrativos.
 - Aplicar o princípio do menor privilégio e segmentar redes críticas.
 - Manter backups offline ou imutáveis e testar a restauração periodicamente.
 - Monitorar ferramentas de transferência, descoberta de rede e administração remota.
 - Correlacionar eventos do EDR, SIEM, VPN, Active Directory e infraestrutura de backup.
- **Recomendações para usuários finais:**
 - Não executar anexos ou arquivos recebidos de fontes não verificadas.
 - Comunicar mensagens suspeitas e solicitações inesperadas de autenticação.
 - Utilizar senhas exclusivas para serviços corporativos.
 - Não instalar ferramentas de suporte remoto sem autorização da equipe de TI.

IoCs e artefatos

A análise publicada pela Cyber Security News, com referência ao alerta das autoridades, apresenta os seguintes indicadores.

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

- 5.255.11[.]134
- 88.119.167[.]239
- 37.10.71[.]188
- 167.235.225[.]149
- SHA-256 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae soc.dll
- SHA-256 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917 locker.dll

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [CISA: Ransomware SafePay atingiu mais de 600 organizações de infraestrutura crítica](#)

2.2. Chaves roubadas do UpdraftCentral usadas em sites WordPress backdoor

TeamUpdraft identificou acesso não autorizado à sua infraestrutura. O incidente pode ter exposto dados de clientes, hashes de senhas, configurações de autenticação multifator e chaves de conexão dos serviços UpdraftCentral, UpdraftVault e UpdraftClone.

O UpdraftCentral permite gerenciar remotamente várias instalações WordPress. Assim, o comprometimento de chaves válidas pode permitir o envio de comandos a sites conectados sem a necessidade de explorar individualmente uma vulnerabilidade em cada instalação.

Segundo a notícia, os arquivos de distribuição do plugin UpdraftPlus não foram diretamente afetados, mas as chaves comprometidas criaram risco para instalações conectadas ao serviço de gerenciamento.

Exploração

A campanha explorou o canal legítimo de administração remota:

- O invasor obteve acesso à infraestrutura da fornecedora.
- Chaves de conexão foram potencialmente expostas.
- Chaves válidas foram utilizadas para enviar comandos aos sites conectados.
- Plugins maliciosos foram instalados para criar backdoors.
- Em determinadas variantes, os plugins permitiam criar contas administrativas ou acessar contas de administradores existentes.

A Patchstack identificou pelo menos 99 nomes distintos de plugins maliciosos disfarçados de ferramentas de manutenção e otimização, incluindo Site Health Cache.

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

O caso é especialmente relevante porque a atividade relatada não dependia necessariamente da exploração da CVE-2026-10795: o atacante abusou de chaves válidas do canal de gerenciamento remoto.

Impacto

- Controle administrativo não autorizado de sites.
- Comprometimento de múltiplas instalações gerenciadas centralmente.
- Roubo de dados e acesso a bancos de dados.
- Instalação de backdoors e mecanismos de persistência.
- Alteração de conteúdo e redirecionamento de visitantes.
- Distribuição de phishing ou malware por sites comprometidos.
- Comprometimento de credenciais e conexões usadas para backups.
- Danos à reputação de proprietários de sites e provedores de hospedagem

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o UpdraftPlus para a versão 1.26.13 ou posterior (gratuita) ou 2.26.13 ou posterior (Premium), conforme orientação publicada.
 - Remover as chaves UpdraftCentral existentes em cada instalação WordPress potencialmente afetada.
 - Revogar sessões e substituir credenciais e chaves de armazenamento que possam ter sido expostas.
 - Inspecionar plugins, contas administrativas, arquivos PHP e tarefas agendadas.
 - Revisar logs para localizar comandos remotos e instalações não autorizadas.
 - Se houver comprometimento confirmado, restaurar a partir de backups limpos e verificar a integridade do site.
- **Recomendações para Administradores de Sistema:**
 - Inventariar todos os sites conectados ao UpdraftCentral.
 - Aplicar MFA às contas de gerenciamento e restringir acessos administrativos.
 - Separar credenciais do WordPress das credenciais de backup e hospedagem.
 - Monitorar instalação e ativação de plugins fora do processo de mudança autorizado.
 - Manter cópias de segurança isoladas, com credenciais independentes.
 - Auditar usuários administrativos e arquivos alterados após o período do incidente.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Chaves roubadas do UpdraftCentral usadas em sites WordPress backdoor](#)

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

2.3. Múltiplas Vulnerabilidades no NGINX Permitem Negação de Serviço e Possível Execução Remota de Código

O CAIS/RNP publicou, em 21 de outubro de 2026, um alerta sobre cinco vulnerabilidades no NGINX Open Source, NGINX Plus e produtos relacionados, identificadas como CVE-2026-15176, CVE-2026-93479, CVE-2026-97205, CVE-2026-95101 e CVE-2026-97629.

As falhas podem permitir negação de serviço (DoS), possível execução remota de código (RCE), injeção de dados em requisições HTTP/3 e contorno de mecanismos de autenticação TLS, conforme a vulnerabilidade, a versão e a configuração do ambiente.

Exploração

As vulnerabilidades apresentam diferentes mecanismos de exploração:

- **CVE-2026-15176:** falha de heap buffer overflow associada ao uso conjunto das diretivas alias e rewrite com referências à variável \$request_filename. Requisições HTTP especialmente manipuladas podem provocar falhas nos processos do NGINX.
- **CVE-2026-93479:** falha de heap buffer overflow relacionada à avaliação de expressões e variáveis, incluindo determinadas configurações da diretiva map com expressões regulares e grupos de captura.
- **CVE-2026-97205:** vulnerabilidade use-after-free que pode ocorrer com operações assíncronas de entrada e saída (AIO) combinadas com Server Side Includes (SSI), causando corrupção de memória e interrupção do serviço.
- **CVE-2026-95101:** falha no processamento de requisições HTTP/3 que pode permitir a injeção de dados em requisições encaminhadas a servidores de backend quando proxy_request_buffering está habilitada.
- **CVE-2026-97629:** falha relacionada à rotação automática de chaves de sessões TLS, que pode possibilitar falsificação de sessões e, em determinadas condições, contorno da verificação de certificados de clientes.

As três primeiras vulnerabilidades podem permitir execução remota de código em determinadas condições, especialmente quando o ASLR (Address Space Layout Randomization) está desabilitado ou pode ser contornado. Até a publicação do alerta, não havia confirmação de exploração ativa dessas cinco falhas em ataques reais.

Impacto

- **Indisponibilidade de serviços:** falhas e reinicializações dos processos do NGINX podem interromper sites, aplicações, APIs e serviços de proxy reverso.

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

- **Execução remota de código:** possibilidade de execução de código no contexto do processo vulnerável, dependendo das condições de exploração.
- **Comprometimento de aplicações de backend:** a injeção de dados em requisições HTTP/3 pode afetar aplicações que recebem as requisições encaminhadas pelo NGINX.
- **Contorno de autenticação TLS:** determinadas condições podem comprometer a validação de sessões ou certificados de clientes.
- **Exposição de ambientes críticos:** servidores públicos, balanceadores de carga, gateways e ambientes de contêineres podem representar pontos de risco para a disponibilidade e a segurança das aplicações.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o NGINX para versões corrigidas: 1.30.6 ou superior na linha Stable e 1.31.7 ou superior na linha Mainline, conforme a recomendação do fabricante.
 - Priorizar servidores expostos à Internet, proxies reversos, balanceadores de carga, gateways e aplicações críticas.
 - Aplicar as atualizações correspondentes do NGINX Plus e dos demais produtos relacionados, conforme os avisos oficiais da F5.
 - Quando a atualização imediata não for possível, aplicar as medidas temporárias específicas para cada vulnerabilidade e monitorar possíveis sinais de exploração.
- **Recomendações para Administradores de Sistema:**
 - Inventariar as instalações do NGINX em servidores, contêineres, appliances e ambientes Kubernetes.
 - Verificar a versão efetivamente instalada e confirmar a aplicação dos patches, considerando que distribuições Linux podem disponibilizar correções por meio de backports.
 - Revisar as configurações afetadas, especialmente as diretivas alias, rewrite e map, além do uso combinado de AIO e SSL.
 - Avaliar a desativação temporária de HTTP/3 quando aplicável e até que a correção correspondente seja instalada.
 - Manter o ASLR habilitado como camada adicional de proteção contra exploração de falhas de memória.
 - Monitorar os logs do NGINX e do sistema operacional em busca de requisições suspeitas, erros anormais e reinicializações recorrentes.

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

- Caso haja suspeita de comprometimento, preservar evidências, coletar logs e iniciar os procedimentos internos de resposta a incidentes.

- **Recomendações para Usuários Finais:**

- Comunicar à equipe de TI eventuais indisponibilidades ou comportamentos anormais em sites e aplicações corporativas.
- Evitar ignorar alertas de segurança apresentados pelos sistemas e navegadores.
- Utilizar os canais oficiais de suporte para relatar falhas de acesso ou suspeitas de comprometimento.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [CAIS-Alerta 21/10/2026: Múltiplas vulnerabilidades no NGINX permitem negação de serviço e possível execução remota de código | RNP](#)

2.4. Hackers registraram novos domínios baseados no Teams e usaram uma página de login para roubar seus logins

Em outubro de 2026, um pesquisador de segurança identificou o domínio teams-cloud[.]live, que imitava a página de login e elementos da interface do Microsoft Teams. O domínio foi reportado como recém-registrado e apresentava características compatíveis com uma tentativa de phishing direcionada a usuários corporativos. A notícia também menciona o subdomínio amgen[.]teams-cloud[.]live.

A publicação não confirma quantas vítimas acessaram o site, se as credenciais foram efetivamente capturadas ou quem controlava a infraestrutura. Portanto, o caso deve ser tratado como uma ameaça de phishing reportada, e não como prova de comprometimento de uma organização específica.

Exploração

A técnica se baseia na imitação visual de um serviço legítimo para induzir o usuário a fornecer suas credenciais.

A sequência potencial é:

- A vítima recebe um link por e-mail, mensagem ou outro canal.
- A página fraudulenta imita o ambiente de autenticação do Teams.
- O usuário insere suas credenciais acreditando estar em um serviço oficial.
- Os dados podem ser coletados pelo operador da página.
- O atacante pode tentar reutilizar as credenciais para acessar outros serviços corporativos.

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

Impacto

- Roubo de credenciais corporativas.
- Acesso indevido a mensagens, reuniões e arquivos.
- Uso de contas comprometidas para disseminar novos ataques.
- Exposição de informações de clientes e colaboradores.
- Fraudes por personificação de funcionários.
- Comprometimento de serviços integrados ao Microsoft 365.
- Instalação de arquivos não autorizados, caso o usuário execute conteúdo baixado.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Bloquear o domínio e os subdomínios confirmados nos filtros corporativos.
 - Pesquisar acessos à página nos registros de DNS, proxy e navegador.
 - Caso credenciais tenham sido inseridas, redefinir as senhas afetadas e revogar sessões e tokens.
 - Investigar arquivos baixados durante a interação.
 - Revisar tentativas de autenticação e regras de caixa de correio suspeitas.
- **Recomendações para administradores de sistema:**
 - Reforçar a proteção contra phishing em e-mail e navegador.
 - Aplicar políticas de acesso condicional e MFA resistente a phishing.
 - Monitorar domínios recém-registrados que imitam serviços corporativos.
 - Restringir execução de arquivos baixados e instalações não autorizadas.
 - Correlacionar alertas do Microsoft Entra ID com os registros de endpoint.
 - Disponibilizar um canal simples para reportar URLs suspeitas.
- **Recomendações para usuários finais:**
 - Conferir o domínio completo antes de inserir credenciais.
 - Acessar o Teams pelo aplicativo corporativo ou por um endereço oficial conhecido.
 - Não confiar exclusivamente no cadeado HTTPS ou na aparência da página.
 - Não baixar supostas atualizações a partir de links inesperados.
 - Informar a equipe de TI caso tenha fornecido credenciais em uma página suspeita.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Hackers registraram novos domínios baseados em Teams e usaram a página de login para roubar seus logins](#)

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

2.5. DNS: vulnerabilidade no BIND 9 pode causar corrupção de memória e execução remota de código

A vulnerabilidade CVE-2026-94300 afeta o BIND 9, software amplamente utilizado para resolução de nomes DNS e gerenciamento de zonas. Classificada como Alta, com pontuação CVSS 8.1, a falha está relacionada ao processamento concorrente de mensagens assinadas por GSS-TSIG, mecanismo de autenticação que pode utilizar Kerberos.

A vulnerabilidade permite que mensagens UDP previamente assinadas sejam reproduzidas (replay) durante o período de validade da chave negociada, causando corrupção de memória no processo named, responsável pelo serviço DNS. Em determinadas condições, a exploração pode levar à interrupção do serviço ou à execução remota de código.

Exploração

A exploração envolve o mecanismo GSS-TSIG, utilizado para autenticar transações DNS, incluindo atualizações dinâmicas em ambientes integrados ao Active Directory. Um invasor capaz de capturar uma mensagem UDP legítima previamente assinada pode retransmiti-la enquanto a chave TSIG negociada ainda estiver válida. Essa atividade pode provocar uma condição de concorrência no estado compartilhado da sessão Kerberos, resultando em corrupção de memória e possível encerramento inesperado do processo named.

Ao combinar essa técnica com consultas especialmente elaboradas para uma zona DNS sob seu controle, o invasor pode, em determinadas condições, transformar a corrupção de memória em execução remota de código. A exploração é remota, não exige interação do usuário nem privilégios prévios, mas possui alta complexidade, pois depende da captura de uma mensagem válida e da exploração dentro do período de validade da chave.

Impacto

- **Negação de serviço (DoS):** encerramento inesperado do processo named, comprometendo a resolução de nomes DNS.
- **Execução remota de código (RCE):** possibilidade de execução de código no sistema que hospeda o BIND, dependendo das condições de exploração.
- **Corrupção de memória:** comprometimento da integridade do processo DNS, podendo afetar sua estabilidade e segurança.
- **Interrupção de serviços corporativos:** indisponibilidade de resolução de nomes pode afetar aplicações, autenticação, comunicação interna e acesso a serviços externos.

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

- **Risco para ambientes integrados ao Active Directory:** organizações que utilizam GSS-TSIG para atualizações dinâmicas de DNS podem estar mais expostas a cenários relevantes de exploração.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o BIND 9 para uma versão corrigida, conforme a orientação oficial do ISC.
 - Priorizar servidores DNS expostos a redes não confiáveis e ambientes que utilizam GSS-TSIG.
 - Verificar a disponibilidade de pacotes atualizados fornecidos pela distribuição Linux ou pelo fornecedor responsável.
 - Como o ISC informa que não existem soluções alternativas conhecidas, priorizar a atualização do software vulnerável.
 - Monitorar reinicializações inesperadas e interrupções no serviço DNS até que a correção seja aplicada.
- **Recomendações para Administradores de Sistema:**
 - Identificar instalações do BIND 9 e verificar se estão nas versões afetadas:
 1. 9.11.0 até 9.18.50;
 2. 9.20.0 até 9.20.29;
 3. 9.21.0 até 9.21.26.
 - Verificar também as versões afetadas do BIND Supported Preview Edition, quando utilizadas.
 - Atualizar para as versões corrigidas indicadas pelo ISC: 9.20.30 ou 9.21.27, conforme a linha utilizada. Para a edição Supported Preview, a correção correspondente é a 9.20.30-S1.
 - Organizações que utilizam a linha 9.18 devem planejar a migração para uma versão suportada, pois essa linha chegou ao fim de vida e não recebe a correção indicada para esta vulnerabilidade.
 - Restringir o tráfego DNS e o uso de atualizações dinâmicas aos sistemas autorizados, conforme os requisitos do ambiente.
 - Centralizar e correlacionar logs do BIND, do sistema operacional e dos mecanismos de autenticação para identificar possíveis atividades suspeitas.
 - Após a atualização, validar a resolução de nomes, as transferências de zona e as atualizações dinâmicas de DNS.

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

- **Recomendações para Usuários Finais:**

A correção depende principalmente dos administradores responsáveis pelos servidores DNS. Aos usuários finais, recomenda-se:

- Comunicar à equipe de TI falhas recorrentes de resolução de nomes ou indisponibilidade de serviços internos.
- Evitar contornar controles corporativos de rede e autenticação.
- Seguir as orientações da equipe técnica durante eventuais períodos de manutenção ou recuperação dos serviços DNS.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [CVE-2026-94300: Concurrent GSS-TSIG messages corrupt memory](#)

2.6. Hackers Abusam de 20.000 Domínios de Páginas da Cloudflare para Divulgar Alertas de Segurança Falsos da Microsoft

Uma campanha identificada em 2026 abusou de domínios hospedados no Cloudflare Pages para distribuir alertas falsos de segurança e direcionar visitantes a centrais fraudulentas de suporte técnico. A investigação da Infoblox citada pela publicação identificou mais de 20 mil domínios associados à operação Help Traffic Distribution System (Help TDS) ao longo de seis meses. A infraestrutura legítima do Cloudflare Pages não é maliciosa por natureza. A ameaça está no uso indevido da plataforma para hospedar páginas fraudulentas, redirecionar visitantes e explorar a confiança em serviços conhecidos.

Exploração

A campanha combina distribuição de tráfego, engenharia social e abuso de serviços legítimos de hospedagem. O fluxo potencial é:

- O visitante chega a uma página por meio de publicidade maliciosa, spam, redes sociais ou um site comprometido.
- Um sistema de direcionamento decide quais visitantes serão encaminhados ao golpe.
- A página exibe um alerta falso alegando que o computador foi bloqueado ou apresenta um problema grave.
- Mensagens alarmistas, sons e elementos visuais simulam um incidente de segurança.
- A vítima é incentivada a telefonar para um número de suporte fraudulento.
- O falso atendente tenta persuadi-la a instalar uma ferramenta legítima de acesso remoto, como o UltraViewer.

Impacto

- Fraude financeira e cobrança por serviços inexistentes.
- Roubo de dados pessoais e corporativos.

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

- Acesso remoto não autorizado a estações de trabalho.
- Instalação de softwares indesejados ou maliciosos.
- Exposição de credenciais armazenadas no navegador.
- Comprometimento da rede corporativa a partir de uma estação.
- Ampliação da distribuição de golpes por meio de sites comprometidos.
- Custos de suporte, investigação e recuperação.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Bloquear domínios maliciosos confirmados.
 - Revisar o histórico de navegação dos equipamentos afetados.
 - Se houve acesso remoto suspeito, desconectar o equipamento da rede conforme o procedimento de resposta a incidentes.
 - Encerrar sessões remotas e investigar arquivos transferidos e comandos executados.
 - Revogar credenciais expostas e preservar os registros de navegador, EDR, DNS e proxy.
- **Recomendações para Administradores de Sistema:**
 - Implementar filtragem DNS, proteção de navegação e análise de URLs.
 - Monitorar ferramentas de acesso remoto, incluindo UltraViewer e outras aplicações não autorizadas.
 - Restringir instalações por usuários sem privilégios administrativos.
 - Correlacionar redirecionamentos suspeitos com eventos de endpoint e conexões externas.
 - Proteger sites corporativos e CMS contra alterações não autorizadas.
 - Utilizar inteligência de ameaças para identificar infraestrutura associada à campanha.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Hackers Abusam de 20.000 Domínios de Páginas da Cloudflare para Divulgar Alertas de Segurança Falsos da Microsoft](#)

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