




Your IT Company

## Principais Vulnerabilidades e Ameaças (Outubro/25)

### Sumário

1. Objetivo .....	2
2. Vulnerabilidades e Ameaças descobertas .....	2
2.1. Ataques de phishing no LinkedIn miram executivos financeiros com convites falsos .....	2
2.2. Airstalk: Nova família de malware Windows exfiltra credenciais de navegador .....	3
2.3. Múltiplas vulnerabilidades em plugins do Jenkins expostas: Ataques de bypass e credenciais expostas .....	4
2.4. Ataque na nuvem: AzureHound, ferramenta legítima usada para reconhecimento malicioso .....	5
2.5. Nova vulnerabilidade Brash no motor Blink afeta milhões de usuários em navegadores Chromium....	5
2.6. Vulnerabilidade crítica no plugin Anti-Malware para WordPress expondo mais de 100.000 Sites.....	6
2.7. CISA alerta sobre exploração ativa de vulnerabilidade crítica no WSUS .....	7
2.8. Gunra Ransomware: Vulnerabilidade crítica descoberta em versão Linux permite decifração .....	8
2.9. Vulnerabilidade no Kernel Linux: Risco de referências nulas em processos de Bind VM.....	8

	<b>Inteligência de Ameaças Cibernéticas</b>  <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		2 de 9

## 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. Ataques de phishing no LinkedIn miram executivos financeiros com convites falsos

Hackers estão usando o LinkedIn para enviar mensagens de phishing direcionadas a executivos financeiros, disfarçadas de convites para conselhos de administração. O objetivo é roubar credenciais Microsoft. A campanha usa links maliciosos e páginas de login falsas, evidenciando uma mudança nos vetores de ataque.

#### Exploração


A ameaça se inicia com mensagens diretas no LinkedIn que simulam convites para conselhos de fundos de investimento. As vítimas são direcionadas a links que levam a uma série de redirecionamentos, passando por páginas falsas que imitam o Microsoft login, e usam CAPTCHA e Cloudflare Turnstile para evitar a detecção por ferramentas automatizadas. O ataque visa roubar credenciais e cookies de sessão, aproveitando-se da confiança depositada na rede social profissional.

#### Mitigação e Prevenção

- **Para usuários:**
  - Tenha cautela com mensagens inesperadas no LinkedIn, especialmente aquelas que oferecem oportunidades de negócios ou convites para conselhos.
  - Não clique em links enviados em mensagens diretas sem verificar a autenticidade do remetente e da oferta.
  - Verifique a legitimidade de domínios e URLs, desconfiando de TLDs incomuns (.icu, .xyz, etc.).
- **Para administradores de sistema:**
  - Implemente soluções de segurança que monitorem e filtrem links suspeitos em mensagens de redes sociais.
  - Eduque os usuários sobre as táticas de phishing e a importância de verificar a autenticidade das mensagens.
  - Monitore os logs de acesso para detectar atividades incomuns em contas de usuários.

#### IOCs

- payrails-canaccord[.]icu
- boardproposalmeet[.]com

	<b>Inteligência de Ameaças Cibernéticas</b>  <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		3 de 9

- sqexclusiveboarddirect[.]jicu
- login.kggpho[.]jicu

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://www.bleepingcomputer.com/news/security/linkedin-phishing-targets-finance-execs-with-fake-board-invites/>.

## **2.2. Airstalk: Nova família de malware Windows exfiltra credenciais de navegador**


Descoberta recentemente, a família de malware Airstalk, que visa sistemas Windows, se destaca pela sua capacidade de roubar credenciais de navegadores. A ameaça utiliza um canal de comunicação encoberto e sofisticado, explorando a infraestrutura legítima de gerenciamento de dispositivos móveis para manter suas operações secretas.

### **Exploração**

O Airstalk opera em variantes PowerShell e .NET, empregando técnicas avançadas como comunicação multi-thread e o uso indevido da API AirWatch (Workspace ONE Unified Endpoint Management). O malware se aproveita dos atributos de dispositivos personalizados dentro da API MDM para criar um mecanismo de "dead drop", trocando informações criptografadas sem uma conexão direta entre o atacante e a vítima. A principal função do malware é coletar dados de navegadores, como cookies, histórico e capturas de tela, utilizando endpoints específicos para controle e exfiltração de dados. A variante .NET inclui suporte a versionamento e uma arquitetura multi-thread para execução simultânea de tarefas e comunicação com os atacantes.

### **Mitigação e Prevenção**

- **Para Administradores de Sistema:**
  - Monitore o tráfego de rede em busca de atividades incomuns associadas à API AirWatch.
  - Implemente sistemas de detecção de intrusão que possam identificar padrões de comunicação suspeitos.
  - Revise logs de eventos em busca de atividades anormais, como o uso de certificados digitais revogados.
  - Mantenha os softwares e sistemas operacionais atualizados para corrigir vulnerabilidades conhecidas.
- **Para Usuários Finais:**
  - Esteja atento a e-mails e links suspeitos, evitando clicar em links de fontes não confiáveis.
  - Use senhas fortes e únicas para cada conta online.
  - Habilite a autenticação de dois fatores (2FA) sempre que possível.
  - Mantenha o software antivírus atualizado e execute verificações regulares.

	<b>Inteligência de Ameaças Cibernéticas</b> <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		4 de 9

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/new-windows-based-airstalk-malware/>.

### **2.3. Múltiplas vulnerabilidades em plugins do Jenkins expostas: Ataques de bypass e credenciais expostas**

O Jenkins, popular servidor de automação de código aberto, foi alvo de múltiplas vulnerabilidades em seus plugins. As falhas variam de bypass de autenticação de alta gravidade a configurações incorretas de permissões e exposição de credenciais, representando riscos significativos para pipelines CI/CD corporativos. Este artigo destaca as principais vulnerabilidades, suas implicações e as medidas de mitigação recomendadas.


#### **Exploração**

O projeto Jenkins divulgou um alerta de segurança em 28 de outubro de 2025, revelando múltiplas vulnerabilidades em 13 plugins. A mais preocupante é a vulnerabilidade de replay no plugin SAML (CVE-2025-64131), que permite que invasores se passem por usuários legítimos ao interceptar e reproduzir solicitações de autenticação SAML. O plugin MCP Server também sofre com verificações de permissão ausentes (CVE-2025-64132), permitindo que atacantes acessem configurações SCM e iniciem construções não autorizadas. Outras vulnerabilidades incluem CSRF (Cross-Site Request Forgery), XXE (XML External Entity) e exposição de credenciais em plugins como Extensible Choice Parameter, JDepend, OpenShift Pipeline, ByteGuard Build Actions, Curseforge Publisher e azure-cli.

#### **Mitigação e Prevenção**

- **Atualização Imediata:** Aplique as correções para os plugins SAML e MCP Server imediatamente.
- **Auditoria de Plugins:** Realize uma auditoria completa dos plugins instalados, removendo ou desativando os não utilizados.
- **Proteção CSRF:** Habilite as proteções CSRF em todas as instâncias do Jenkins.
- **Monitoramento:** Monitore ativamente a atividade do Jenkins em busca de atividades suspeitas.
- **Restrição de Permissões:** Revise e restrinja as permissões de acesso aos usuários e grupos no Jenkins.
- **Armazenamento Seguro de Credenciais:** Evite o armazenamento de credenciais em texto simples. Utilize as opções de armazenamento seguro oferecidas pelo Jenkins e seus plugins.
- **Validação de Entradas:** Implemente validação rigorosa de entradas para mitigar ataques como XXE e injeção de comandos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/multiple-jenkins-vulnerability/>

	<b>Inteligência de Ameaças Cibernéticas</b>  <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		5 de 9

## 2.4. Ataque na nuvem: AzureHound, ferramenta legítima usada para reconhecimento malicioso

Alerta sobre o uso malicioso da ferramenta AzureHound por atores de ameaças para reconhecimento em ambientes Azure e Microsoft Entra ID. A ferramenta, originalmente para testes de segurança, é explorada para mapear e comprometer infraestruturas na nuvem. A sua utilização por grupos como Curious Serpens e Void Blizzard demonstra a sua crescente importância nos ataques.

### Exploração

O AzureHound é uma ferramenta de coleta de dados do BloodHound, projetada para identificar vulnerabilidades em infraestruturas de nuvem, que explora as APIs do Microsoft Graph e Azure REST para coletar informações sobre usuários, grupos, permissões e recursos. Atores de ameaças utilizam essa ferramenta para acelerar seus ataques, mapeando caminhos de ataque, identificando alvos de alto valor e descobrindo oportunidades de escalonamento de privilégios após a obtenção do acesso inicial. A ferramenta não requer posicionamento especial na rede, tornando-a acessível remotamente.

### Mitigação e Prevenção


- Implantar mecanismos de autenticação fortes, como autenticação multifator (MFA).
- Monitorar a atividade da API do Azure em busca de consultas de enumeração incomuns.
- Monitorar comandos específicos do AzureHound, como "list users", "list groups", "list role-assignments" e "list storage-accounts".
- Aplicar o princípio do menor privilégio, garantindo que as contas tenham apenas as permissões necessárias.
- Utilizar plataformas de detecção de ameaças focadas em nuvem, como Palo Alto Networks Cortex XDR e XSIAM.
- Manter uma boa prática de registro da atividade do Azure e responder rapidamente a incidentes.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://gbhackers.com/threat-actors-abuse-azurehound-tool/>.

## 2.5. Nova vulnerabilidade Brash no motor Blink afeta milhões de usuários em navegadores Chromium

Pesquisadores descobriram uma vulnerabilidade crítica, chamada Brash, no motor de renderização Blink, utilizado em navegadores baseados em Chromium (Chrome, Edge, Brave, Opera). A falha permite ataques de negação de serviço (DoS), travando os navegadores em questão de segundos através da injeção de código. A vulnerabilidade explora a ausência de limitação de taxa na API document.title, afetando mais de 3 bilhões de usuários.

### Exploração

	<b>Inteligência de Ameaças Cibernéticas</b>  <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		6 de 9

A vulnerabilidade Brash explora a ausência de limitação de taxa na API document.title. O ataque funciona em três fases: pré-carregamento de strings hexadecimais, injeção de milhões de atualizações de document.title por segundo e sobrecarga do processamento do navegador. Isso leva ao esgotamento dos recursos do sistema e ao travamento total do navegador em questão de segundos. A falha afeta as versões do Chromium 143.0.7483.0 e anteriores.

### Mitigação e Prevenção

- **Usuários Finais:**
  - Evitar clicar em links suspeitos que prometem documentos vazados, alertas de segurança urgentes ou informações sensíveis.
  - Manter os navegadores atualizados, assim que as correções forem lançadas.
- **Administradores de Sistema/Organizações:**
  - Monitorar interrupções baseadas em navegadores e manter backups de sistemas críticos.
  - Acompanhar as atualizações de segurança dos navegadores Chromium e aplicar os patches assim que disponíveis.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://gbhackers.com/critical-blink-vulnerability/>.

## 2.6. Vulnerabilidade crítica no plugin Anti-Malware para WordPress expando mais de 100.000 Sites


Um defeito crítico de segurança foi descoberto no plugin Anti-Malware Security and Brute-Force Firewall para WordPress, afetando mais de 100.000 sites. A vulnerabilidade, identificada como CVE-2025-11705, permite que atacantes autenticados com acesso básico de assinante leiam arquivos arbitrários no servidor, potencialmente expondo dados sensíveis como credenciais de banco de dados e chaves de segurança. A atualização imediata para a versão corrigida é crucial.

### Exploração

A vulnerabilidade reside na falta de uma verificação de autorização no código do plugin, especificamente na função GOTMLS\_ajax\_scan(), usada para exibir os resultados da verificação de malware. Apesar da proteção nonce, atacantes com contas de nível de assinante podem contornar essas proteções e explorar a falha para ler arquivos arbitrários no servidor. Isso possibilita o acesso a arquivos críticos como wp-config.php, que contém credenciais de banco de dados e chaves criptográficas.

### Mitigação e Prevenção

- Atualizar imediatamente o plugin Anti-Malware Security and Brute-Force Firewall para a versão 4.23.83 ou posterior.
- Verificar regularmente a versão dos plugins instalados.
- Monitorar as notificações de segurança para estar ciente de novas vulnerabilidades e atualizações de plugins.

	<b>Inteligência de Ameaças Cibernéticas</b>  <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		7 de 9

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://gbhackers.com/wordpress-plugin-vulnerability-4/>.

## 2.7. CISA alerta sobre exploração ativa de vulnerabilidade crítica no WSUS


A CISA (Cybersecurity and Infrastructure Security Agency) emitiu um alerta urgente sobre a exploração ativa da vulnerabilidade CVE-2025-59287 no Windows Server Update Service (WSUS). A falha de segurança permite a execução remota de código, concedendo aos invasores controle total sobre os servidores afetados. É crucial que as organizações tomem medidas imediatas para identificar, corrigir e monitorar seus sistemas.

### Exploração

A vulnerabilidade CVE-2025-59287, presente em múltiplas versões do Windows Server (2012, 2016, 2019, 2022 e 2025), permite que atacantes não autenticados executem código remotamente com privilégios de nível de sistema. Essa falha foi explorada ativamente após uma correção anterior não ter resolvido completamente o problema, expondo os sistemas a ataques. A exploração bem-sucedida pode levar ao comprometimento total do sistema e à movimentação lateral na rede.

### Mitigação e Prevenção

- **Identificar servidores vulneráveis:** Verifique se a função WSUS está habilitada e se as portas TCP 8530 ou TCP 8531 estão abertas. Use comandos PowerShell ou o Gerenciador do Servidor para confirmar a instalação do WSUS.
- **Aplicar a atualização de segurança:** Instale a atualização fora de banda lançada em 23 de outubro de 2025 em todos os servidores WSUS identificados.
- Reiniciar os servidores: Reinicie os sistemas após a instalação da atualização para completar a mitigação.
- **Medidas temporárias:** Se a atualização não puder ser aplicada imediatamente, desabilite temporariamente a função WSUS ou bloqueie o tráfego de entrada nas portas padrão do WSUS.
- **Atualizar outros servidores:** Aplique as atualizações em todos os servidores Windows restantes e reinicie-os.
- **Monitorar sinais de exploração:** Monitore atividades suspeitas, incluindo processos filhos com permissões de nível de sistema, especialmente aqueles originados de wsusservice.exe ou w3wp.exe. Monitore também por processos PowerShell aninhados usando comandos codificados em base64.
- **Configurar plataformas de segurança:** Configure plataformas de segurança de endpoint para alertar sobre comportamentos incomuns de processos e tentativas de escalonamento de privilégios.

	<b>Inteligência de Ameaças Cibernéticas</b> <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		8 de 9

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse:

<https://gbhackers.com/cisa-alerts-on-of-wsus-vulnerability/>.

## **2.8. Gunra Ransomware: Vulnerabilidade crítica descoberta em versão Linux permite decifração**

O ransomware Gunra, que ataca sistemas Windows e Linux, apresenta uma vulnerabilidade crítica em sua versão Linux. Pesquisadores descobriram que a falha no processo de geração de chaves de criptografia ChaCha20, torna possível a decifração dos arquivos por meio de ataques de força bruta.

### **Exploração**

O Gunra opera com um modelo comum de ransomware, criptografando arquivos e exigindo resgate, mas se destaca por ter versões específicas para Windows (EXE) e Linux (ELF). A vulnerabilidade reside na versão ELF, onde a geração da chave de criptografia ChaCha20 utiliza a função `time()` para gerar valores previsíveis, resultando em chaves fracas. A versão Windows, por outro lado, usa a API `CryptGenRandom()`, que é criptograficamente segura.

### **Mitigação e Prevenção**

- **Administradores de sistema:**

- Verifique e atualize as medidas de segurança, especialmente em servidores Linux.
- Monitore o tráfego de rede em busca de atividades suspeitas, como comunicação com servidores C&C.
- Implemente um sistema de detecção de intrusão (IDS) para identificar tentativas de acesso não autorizado.
- faça backups regulares dos dados e garanta que esses backups estejam armazenados offline.

- **Usuários finais:**


- Mantenha os sistemas operacionais e softwares atualizados.
- Tenha cuidado ao abrir anexos de e-mail e clicar em links de fontes desconhecidas.
- Instale e mantenha um software antivírus atualizado.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse:

<https://cybersecuritynews.com/gunra-ransomware-leveraging-attacking-windows/>.

## **2.9. Vulnerabilidade no Kernel Linux: Risco de referências nulas em processos de Bind VM**

Uma nova vulnerabilidade, identificada como CVE-2025-40086, foi descoberta no kernel Linux. Essa falha pode levar a referências de ponteiros nulos em determinadas situações durante o processo de `bind` de máquinas virtuais (VMs), comprometendo a estabilidade e segurança do sistema.

	<b>Inteligência de Ameaças Cibernéticas</b> <b>Comite Editorial</b>	<b>Código</b>
		SGSI-081
		<b>Página</b>
		9 de 9

### Exploração

A vulnerabilidade reside na função *drm/x* do kernel, onde um array de *binds* de VM pode, sob certas condições, desalocar outros objetos de buffer (BOs) dentro da mesma VM. Essa desalocação pode resultar em referências a ponteiros nulos mais tarde no pipeline, causando travamentos ou comportamentos inesperados. A correção implementada no código impede essa desalocação indevida, protegendo o sistema contra a exploração da falha.

### Mitigação e Prevenção

- Manter seus sistemas Linux atualizados, aplicando as últimas atualizações de segurança do kernel.
- Monitorar regularmente os logs do sistema em busca de erros relacionados a falhas de memória ou comportamento incomum de VMs.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse:

<https://www.tenable.com/cve/CVE-2025-40086>,

<https://git.kernel.org/stable/c/7ac74613e5f2ef3450f44fd2127198662c2563a9>,

<https://git.kernel.org/stable/c/5aa0ab0ba7d94549cfe17d6ef7a4f33ba1de8384>.

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