Your IT Company

Principais Vulnerabilidades e Ameaças (dezembro/25)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Ataques de força bruta em massa visam portais GlobalProtect da Palo Alto Networks 2
2.2. Phishing no Microsoft Teams: Ataques usam notificações falsas para roubar dados 3
2.3. Vulnerabilidade crítica no Apache Tika permite ataques via arquivos PDF maliciosos 3
2.4. CastleRAT: Nova ameaça RAT mirando sistemas Windows com técnicas sofisticadas 4
2.5. AWS SageMaker: Vulnerabilidade permite escalada de privilégios em instâncias 5
2.6. Alerta Crítico: Vulnerabilidades de permissão no Splunk Enterprise e Universal Forwarder para Windows 6
2.7. Nova ameaça: Malware Linux combina ataques DDoS e mineração clandestina 6
2.8. BRICKSTORM: Nova ameaça cibernética ataca VMware ESXi e Windows 7

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 força bruta em massa visam portais GlobalProtect da Palo Alto Networks

Pesquisadores detectaram uma nova campanha que está mirando portais GlobalProtect da Palo Alto Networks com tentativas de login e varreduras em endpoints da API SonicWall SonicOS. A atividade, iniciada em 2 de dezembro de 2025, envolveu milhares de endereços IP de uma empresa alemã de TI, indicando um esforço direcionado a credenciais e possíveis vulnerabilidades.

Exploração

A campanha usa tentativas de força bruta e login contra portais GlobalProtect, o componente de VPN da Palo Alto Networks. Os atacantes mudaram para a varredura de endpoints da API SonicWall SonicOS em busca de vulnerabilidades e configurações incorretas. A atividade se originou de mais de 7.000 endereços IP da 3xK GmbH, que opera sua própria rede BGP. A Palo Alto Networks confirmou que os ataques visam credenciais e não exploram vulnerabilidades de softwares.

Mitigação e Prevenção

- **Para administradores de sistema:**
  - Monitore as superfícies de autenticação para detectar tentativas repetidas e falhas anormais.
  - Monitore e bloqueie os IPs associados a essa atividade maliciosa.
  - Considere o uso de bloqueio dinâmico e com reconhecimento de contexto em vez de listas de reputação estáticas.
  - Implemente a autenticação multifator (MFA) para proteger contra o uso indevido de credenciais.
- **Para usuários finais:**
  - Use senhas fortes e exclusivas para suas contas.
  - Habilite a MFA sempre que disponível.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.bleepingcomputer.com/news/security/new-wave-of-vpn-login-attempts-targets-palo-alto-globalprotect-portals/.

Classificação: Público

2.2. Phishing no Microsoft Teams: Ataques usam notificações falsas para roubar dados

Pesquisadores de cibersegurança descobriram uma sofisticada campanha de phishing que utiliza notificações do Microsoft Teams para enganar usuários e levá-los a ligar para números de suporte fraudulentos. Os criminosos exploram a confiança nas plataformas de comunicação legítimas para contornar defesas de segurança e filtros de e-mail.

Exploração

Os atacantes estão utilizando o Microsoft Teams para adicionar usuários a grupos com nomes falsos e conteúdos financeiros enganosos, como cobranças de faturas, avisos de renovação automática ou taxas não autorizadas do PayPal. As vítimas recebem notificações por e-mail, que parecem vir de infraestrutura legítima do Microsoft Teams, solicitando que entrem em contato com um número de suporte falso. Como os e-mails vêm de um domínio oficial da Microsoft, eles geralmente passam pelos filtros de e-mail e parecem confiáveis. Ao ligar para os números fraudulentos, os usuários fornecem informações confidenciais aos criminosos.

Mitigação e Prevenção

- **Para Administradores de Sistema:**
  - Implemente uma análise mais rigorosa nas notificações do Teams.
  - Ajuste as políticas de entrega para exigir aprovação manual para convites do Teams de grupos desconhecidos.
  - Implemente autenticação multifator (MFA).
  - Mantenha uma forte segurança no gateway de e-mail.
  - Eduque os funcionários sobre esse tipo de ataque.
- **Para Usuários Finais:**
  - Verifique solicitações de pagamento urgentes através dos canais oficiais da empresa.
  - Desconfie de notificações do Teams com nomes de grupos relacionados a finanças, especialmente as que usam linguagem de urgência.
  - Revise regularmente as suas associações a grupos no Teams.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/microsoft-teams-phishing-attack/.

2.3. Vulnerabilidade crítica no Apache Tika permite ataques via arquivos PDF maliciosos

Uma vulnerabilidade crítica no Apache Tika, uma ferramenta amplamente utilizada para extrair texto e metadados de documentos, permite que atacantes comprometam sistemas ao enviar arquivos PDF especialmente criados. A falha, causada por uma injeção de entidade externa XML (XXE), afeta diversas versões do Tika e exige ação imediata para mitigar o risco de execução de código malicioso, roubo de informações e acesso não autorizado.

Classificação: Público

Exploração

O Apache Tika é uma ferramenta de código aberto essencial para muitas organizações, utilizada para processar documentos como PDFs, arquivos do Word e imagens. A vulnerabilidade reside em uma falha de injeção XXE que permite a execução de código arbitrário. Atacantes exploram essa falha ao criar arquivos PDF com arquivos XFA (XML Forms Architecture) maliciosos, que, quando processados pelo Tika, acionam a vulnerabilidade. Isso pode levar à execução de código, roubo de informações sensíveis e acesso não autorizado aos sistemas. A falha afeta as versões 1.13 a 3.2.1 do Tika-core, as versões anteriores a 2.0.0 do Tika-parsers e as versões 2.0.0 a 3.2.1 do módulo parser PDF do Tika.

Mitigação e Prevenção

- **Atualização Imediata:** A ação mais importante é atualizar o Tika-core para a versão 3.2.2 ou posterior, que corrige a vulnerabilidade em todos os componentes.
- **Verificação de Versões:** As organizações devem verificar as versões do Tika-core, Tika-parsers e do módulo parser PDF do Tika instaladas em seus sistemas.
- **Contate o Fornecedor:** Usuários de versões 1.x devem entrar em contato com seus fornecedores de software para obter versões corrigidas.
- **Restrição Temporária:** Como medida de segurança temporária, restrinja o envio de arquivos PDF de fontes externas não confiáveis até que a correção seja implementada.
- **Monitoramento:** Monitore a atividade do sistema em busca de sinais de exploração da vulnerabilidade.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/apache-tika-core-vulnerability/.

2.4. CastleRAT: Nova ameaça RAT mirando sistemas Windows com técnicas sofisticadas

Uma ameaça crescente, CastleRAT, um Trojan de Acesso Remoto (RAT) recente, está infectando sistemas Windows globalmente. Este malware permite que invasores controlem máquinas comprometidas remotamente, utilizando versões em Python e C, com recursos avançados de coleta de dados e comunicação encriptada. A sua capacidade de se infiltrar e exfiltrar dados através do monitoramento da área de transferência (clipboard) o torna particularmente perigoso.

Exploração

O CastleRAT opera em duas versões principais, uma leve em Python e outra mais robusta em C. A versão em C oferece funcionalidades como captura de keystrokes, screenshots e métodos de instalação persistentes. O malware coleta informações do sistema, como nome do computador, nome de usuário, GUID da máquina e endereço IP, e se comunica com o servidor de comando e controle (C2) usando criptografia RC4 com uma chave fixa. A técnica de coleta de dados da área de transferência é um dos seus principais vetores de ataque, onde dados sensíveis são roubados simulando ações de "colar" em aplicativos aparentemente inofensivos.

Classificação: Público

Mitigação e Prevenção

- **Para Administradores de Sistema**: Monitore conexões de saída incomuns, downloads via PowerShell de linha única e a presença de binários inesperados em pastas de usuários. Fique atento a sinais de tráfego criptografado com RC4.
- **Para Usuários Finais**: Tenha cuidado ao copiar e colar informações sensíveis, como senhas e dados de carteiras de criptomoedas. Mantenha seus sistemas operacionais e softwares atualizados. Utilize softwares de segurança com proteção de clipboard.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/hackers-using-castlerat-malware/.

2.5. AWS SageMaker: Vulnerabilidade permite escalada de privilégios em instâncias

Uma nova vulnerabilidade em instâncias AWS SageMaker permite a escalada de privilégios, dando a atacantes com permissões limitadas a capacidade de executar código com maiores privilégios em instâncias EC2 e SageMaker. A falha reside na capacidade de modificar configurações de inicialização e configurações de ciclo de vida, possibilitando a injeção de payloads maliciosos e o acesso não autorizado a dados sensíveis.

Exploração

A técnica explora a modificação de atributos de instâncias EC2 e SageMaker, como userData e configurações de ciclo de vida, para injetar código malicioso que é executado durante a inicialização ou reinicialização. Atacantes com permissões de ec2:StartInstances, ec2:StopInstances e ec2:ModifyInstanceAttribute ou permissões semelhantes no SageMaker, podem parar a instância, modificar a configuração para incluir código malicioso (como roubo de credenciais) e reiniciar a instância. O código malicioso é executado no contexto do perfil da instância, concedendo ao atacante acesso aos seus privilégios completos.

Mitigação e Prevenção

- **Restrição de Permissões:** Limitar o uso da permissão ec2:ModifyInstanceAttribute a administradores confiáveis. No SageMaker, restringir as permissões de sagemaker:StopNotebookInstance, sagemaker:UpdateNotebookInstance e sagemaker:StartNotebookInstance.
- **Monitoramento:** Implementar monitoramento contínuo do CloudTrail para detectar padrões suspeitos, como sequências de "Stop → Update → Start" em instâncias de computação, especialmente de identidades não operacionais.
- **Políticas de Controle de Serviço (SCPs):** Utilizar SCPs para negar a passagem ampla de funções de execução, restringindo o acesso e o uso de recursos.
- **Fluxos de Aprovação:** Implementar fluxos de trabalho de aprovação para reinicializações e modificações de configurações críticas.

Classificação: Público

- **Auditoria:** Realizar auditorias regulares das funções de execução assumidas para identificar e corrigir possíveis brechas de segurança.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/aws-sagemaker-vulnerability/.

2.6. Alerta Crítico: Vulnerabilidades de permissão no Splunk Enterprise e Universal Forwarder para Windows

Uma vulnerabilidade de alta gravidade foi descoberta no Splunk, afetando as versões Enterprise e Universal Forwarder para Windows. A falha, identificada como CVE-2025-20386 e CVE-2025-20387, permite que usuários não administradores acessem diretórios de instalação sensíveis, abrindo portas para ataques de escalonamento de privilégios. É crucial atualizar para as versões corrigidas ou aplicar as medidas de mitigação recomendadas.

Exploração

A vulnerabilidade reside na configuração incorreta das permissões de arquivo durante a instalação ou atualização do Splunk em sistemas Windows. A falha concede acesso de leitura e escrita a usuários locais não privilegiados nos diretórios de instalação padrão, como "C:\Program Files\Splunk" e "C:\Program Files\SplunkUniversalForwarder". Essa permissão inadequada permite que um atacante modifique configurações do sistema, insira código malicioso ou eleve seus privilégios ao nível de administrador. A pontuação CVSS é 8.0 (Alta).

Mitigação e Prevenção

- **Atualização:** A ação prioritária é atualizar para as versões corrigidas do Splunk Enterprise (10.0.2, 9.4.6, 9.3.8 ou 9.2.10) e Universal Forwarder (10.0.2, 9.4.6, 9.3.8 ou 9.2.10).
- **Mitigação (se a atualização imediata não for possível):** Utilize o comando icacls para reconfigurar as permissões dos diretórios, removendo acessos inadequados e reaplicando os controles de herança corretos.
- **Recomendação:** Administradores de sistema devem verificar regularmente as permissões de arquivos e diretórios críticos para garantir que apenas usuários autorizados tenham acesso.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/splunk-enterprise-permission-vulnerabilities/.

2.7. Nova ameaça: Malware Linux combina ataques DDoS e mineração clandestina

Pesquisadores descobriram um malware Linux sofisticado, o V3G4, que integra as capacidades de uma botnet DDoS derivada do Mirai com um minerador de criptomoedas furtivo. Essa combinação permite ataques em larga escala contra servidores Linux e dispositivos IoT, visando tanto a interrupção de serviços quanto a mineração de criptomoedas.

Classificação: Público

Exploração

O malware V3G4 inicia com um script shell que identifica a arquitetura da CPU da vítima para baixar a versão correta do bot. Após a execução, o bot entra em modo furtivo, se disfarçando como um processo legítimo do sistema. Ele estabelece uma infraestrutura de comando e controle (C2) usando tanto varredura de sockets TCP quanto consultas DNS para se comunicar com o servidor C2. A parte final do ataque envolve a implantação de um minerador de Monero (XMRig) que busca dinamicamente as configurações de mineração, evitando a criação de arquivos no disco e dificultando a análise forense.

Mitigação e Prevenção

- **Administradores de sistema**:
  - Monitore o tráfego de rede em busca de atividade suspeita, como tráfego intenso para portas incomuns e tentativas de conexão SSH bruteforce.
  - Implemente firewalls e sistemas de detecção de intrusão para bloquear o tráfego malicioso e identificar tentativas de acesso não autorizado.
  - Mantenha os sistemas atualizados com as últimas correções de segurança para mitigar vulnerabilidades exploradas pelo malware.
  - Faça uma análise de logs de sistema em busca de atividades anômalas, como a execução de scripts suspeitos ou a criação de processos incomuns.
- **Usuários finais**:
  - Certifique-se de que seus dispositivos IoT e servidores estejam executando softwares atualizados.
  - Use senhas fortes e únicas para todos os seus dispositivos e contas.
  - Monitore regularmente seus dispositivos em busca de atividades estranhas, como lentidão ou comportamento incomum.

IOCs

- 103.149.93.224
- 159.75.47.123
- baojunwakuang.asia

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/linux-malware-combines-mirai-derived-ddos-botnet/.

2.8. BRICKSTORM: Nova ameaça cibernética ataca VMware ESXi e Windows

A CISA, a NSA e o Centro de Segurança Cibernética do Canadá alertam sobre a campanha BRICKSTORM, um sofisticado backdoor desenvolvido por agentes cibernéticos patrocinados pela China. Esta ameaça visa ambientes VMware vSphere e Windows, buscando persistência de longo prazo em redes críticas, com o objetivo de obter controle total sobre os sistemas comprometidos.

Classificação: Público

Exploração

BRICKSTORM é um malware customizado em Go, projetado para se integrar profundamente em infraestruturas virtualizadas, como VMware vCenter e ESXi. Ele emprega mecanismos de C2 (comando e controle) resilientes, usando DNS-over-HTTPS (DoH) para se comunicar de forma disfarçada. Após a conexão, o malware estabelece uma conexão HTTPS que é então convertida em uma conexão WebSocket com várias camadas de criptografia TLS. Essa técnica permite que os atacantes executem múltiplas ações, como shells interativos e transferência de arquivos, dentro de uma única conexão criptografada.

Os atacantes exploram vulnerabilidades para comprometer servidores web, movendo-se lateralmente para controladores de domínio internos e servidores ADFS, onde instalam o BRICKSTORM para roubar dados, criar VMs falsas e exportar chaves criptográficas.

Mitigação e Prevenção

- **Atualização:** Atualize os servidores VMware vSphere para as versões mais recentes.
- **Restrição de Rede:** Limite a conectividade de dispositivos de borda a recursos internos.
- **Bloqueio de Tráfego DoH:** Bloqueie o tráfego DoH não autorizado para impedir a resolução da infraestrutura C2 do malware.
- **Monitoramento:** Aumente o monitoramento em contas de serviço, pois foram amplamente abusadas nos ataques.
- **Análise Abrangente:** Realize análises em disco, além de exames forenses padrão, para detectar mecanismos de persistência estática.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/brickstorm-attacking-vmware-esxi-and-windows/.

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

Classificação: Público