Your IT Company

Principais Vulnerabilidades e Ameaças (Março/25)

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. Hackers estão abusando do Microsoft Teams & Quick Assist para obter acesso remoto

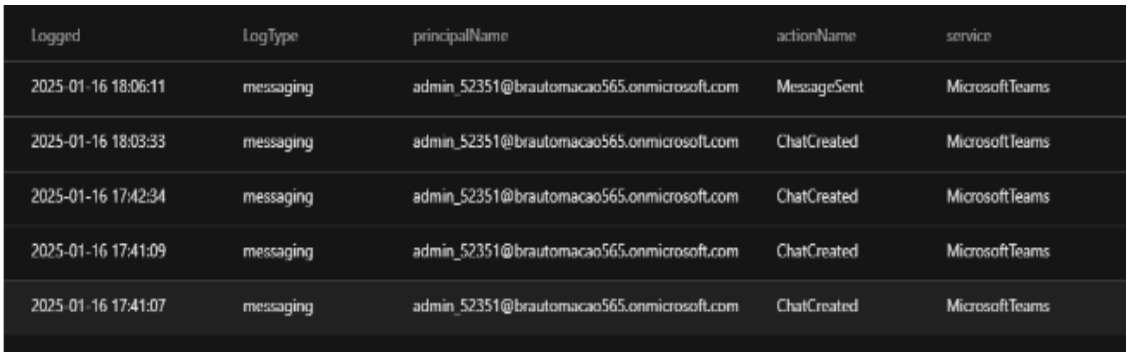
O Microsoft Teams é uma plataforma unificada de comunicação e colaboração que combina bate-papo, videoconferências, armazenamento de arquivos e integração de aplicativos e serviços da Microsoft e de terceiros. Já o Microsoft Quick Assist é uma ferramenta que permite aceder remotamente a um computador Windows ou macOS para fornecer suporte técnico. Ambas as ferramentas estão sofrendo ataques de Ransomwares que exploram o Microsoft Teams e o Quick Assist para sequestrar redes corporativas, com isso, os ataques têm preocupado especialistas em segurança cibernética, pois os agentes de ameaças vêm arrecadando mais de US$ 107 milhões em resgates pagos em Bitcoin desde outubro de 2024.

As equipes de XDR gerenciado e de resposta a incidentes da Trend Micro detectaram recentemente campanhas orquestradas pelos grupos de ransomware Black Basta e Cactus, que utilizam uma variante compartilhada do malware BackConnect (QBACKCONNECT) para garantir acesso persistente aos sistemas comprometidos.

Esses ataques representam uma ameaça sofisticada ao combinar engenharia social, uso indevido de ferramentas legítimas e exploração da infraestrutura em nuvem de forma altamente estratégica.

Exploração

A cadeia de ataque tem início com uma sobrecarga intencional de e-mails, inundando as caixas de entrada das vítimas para distraí-las e dificultar a identificação de comunicações maliciosas. Em seguida, os invasores recorrem a técnicas de falsificação de identidade no Microsoft Teams para enganar alvos e obter acesso não autorizado. Os agentes de ameaças se passam por suporte de TI usando contas falsificadas como **admin_52351@brautomacao565[.]onmicrosoft[.]com**



Logged	LogType	principalName	actionName	service
2025-01-16 18:06:11	messaging	admin_52351@brautomacao565.onmicrosoft.com	MessageSent	MicrosoftTeams
2025-01-16 18:03:33	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams
2025-01-16 17:42:34	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams
2025-01-16 17:41:09	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams
2025-01-16 17:41:07	messaging	admin_52351@brautomacao565.onmicrosoft.com	ChatCreated	MicrosoftTeams

Figura 1 - Endereço de e-mail usado pelo invasor – Fonte: https://cybersecuritynews.com/hackers-abusing-microsoft-teams-quick-assist/

As vítimas são coagidas a conceder acesso remoto através da ferramenta Quick Assist, integrada ao Windows, permitindo que os invasores obtenham controle total sobre o dispositivo. Uma vez concedido o acesso, os atacantes baixam arquivos .bpx maliciosos de buckets de armazenamento em nuvem comprometidos. Em um exemplo específico, os arquivos kb052117-01.bpx e kb052123-02.bpx foram concatenados em um único arquivo, denominado pack.zip. Ao ser extraído usando o utilitário tar.exe, esse arquivo implanta DLLs e executáveis maliciosos diretamente no diretório do OneDrive, facilitando a execução de ações mal-intencionadas.

Os invasores abusam do OneDriveStandaloneUpdater.exe, um binário legítimo da Microsoft, para fazer o sideload de uma DLL maliciosa (winhttp.dll). Essa DLL descriptografa cargas úteis de settingsbackup.dat, implantando o malware BackConnect.

O comando e controle persistente (C2) é estabelecido por meio de IPs como 38.180.25[.]3, conectado na chave do registro. A Trend Micro atribui esses IPs à infraestrutura C2 da Black Basta. O BackConnect permite a execução remota de código, roubo de credenciais e movimentação lateral via Server Message Block (SMB) e Windows Remote Management (WinRM).

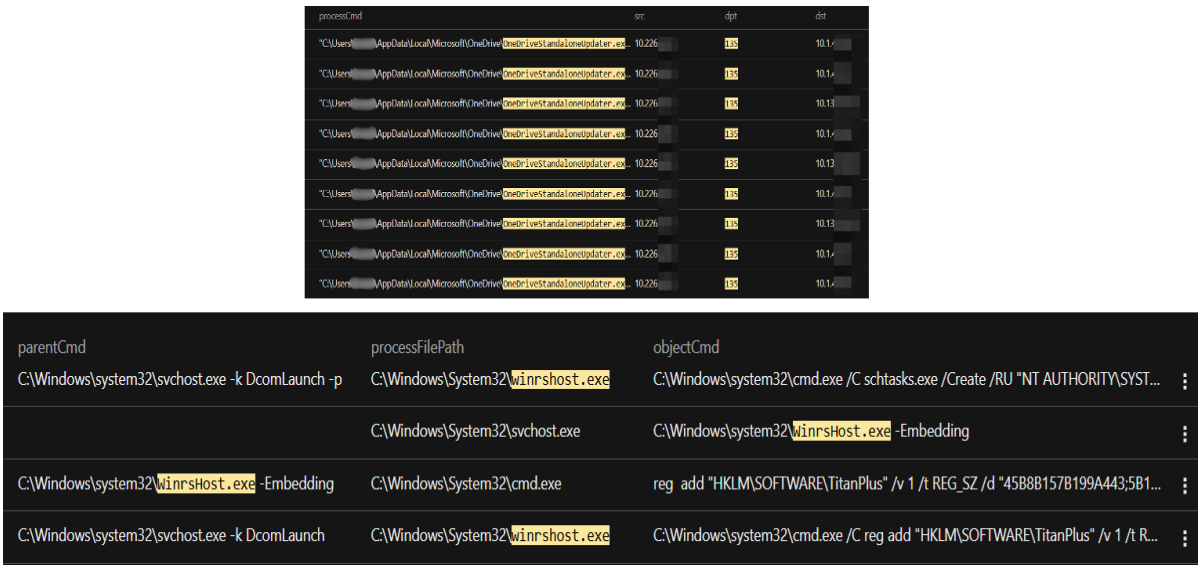


Figura 2 - Acesso SMB via 'OneDriveStandaloneUpdater.exe' (parte superior)
WinRM utilizado para execução remota de comandos e criação de tarefas agendadas (parte inferior) – Fonte: https://cybersecuritynews.com/hackers-abusing-microsoft-teams-quick-assist/

Mitigação e prevenção

A Trend Micro recomenda as seguintes medidas:

• Restringir o Quick Assist: Desative ferramentas remotas não autorizadas e exija autenticação multifator para todas as solicitações de TI.

• Monitorar a atividade do Teams: Aplique as práticas recomendadas de segurança da Microsoft e trate o Teams com o mesmo nível de vigilância que o e-mail.

• Bloquear IPs maliciosos: Coloque na lista negra IPs C2, como 45.8.157[.]199 e 5.181.3[.]164.

• Procurar por sideload de DLL: Utilize a consulta do Trend Vision One, como eventSubId: 603 AND (request:filters*.s3.us-east-*), para identificar atividades maliciosas relacionadas a arquivos.

Essas campanhas ressaltam a urgência de adotar defesas em camadas robustas para enfrentar as ameaças da engenharia social e as táticas de "Living off the Land" (LotL).

Com a possível desintegração do Black Basta após o vazamento de dados e a ascensão do Cactus, é importante que as organizações fortaleçam suas estratégias de segurança, priorizando a implementação de políticas Zero Trust e promovendo treinamentos comportamentais contínuos para capacitar seus funcionários a identificar e mitigar ataques sofisticados de forma proativa.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/hackers-abusing-microsoft-teams-quick-assist/

2.2. Alerta de Segurança: CISA emite alerta sobre vulnerabilidade crítica no Palo Alto Firewall CVE-2025-0108

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) emitiu um alerta urgente em 4 de março de 2025, adicionando três vulnerabilidades críticas da VMware ao seu catálogo de Vulnerabilidades Exploradas Conhecidas (KEV) após a exploração confirmada.

As vulnerabilidades CVE-2025-22224, CVE-2025-22225 e CVE-2025-22226 permitem que invasores com acesso privilegiado a máquinas virtuais (VMs) escalem privilégios, executem código em hipervisores e exfiltrem dados confidenciais de memória.

Essas falhas, descobertas pelo Microsoft Threat Intelligence Center (MSTIC), afetam os produtos VMware ESXi, Workstation, Fusion, Cloud Foundation e Telco Cloud Platform.

O comunicado da CISA coincide com o lançamento de patches da Broadcom, enfatizando a necessidade de agências federais e organizações privadas priorizarem a correção sob a Diretiva Operacional Vinculativa (BOD).

Exploração

Falha crítica de TOCTOU permite a aquisição do hipervisor (CVE-2025-22224)

CVE-2025-22224, o mais grave do trio com uma pontuação CVSS de 9,3, é uma condição de corrida de tempo de verificação de tempo de uso (TOCTOU) no VMware ESXi e no Workstation.

Os invasores com privilégios administrativos em uma VM podem explorar essa vulnerabilidade de estouro de heap para executar código arbitrário no processo VMX — o componente do hipervisor que gerencia as operações da VM.

A exploração bem-sucedida concede controle sobre o sistema host, permitindo o movimento lateral entre infraestruturas virtualizadas.

Escape de sandbox por meio de gravação arbitrária (CVE-2025-22225)

O CVE-2025-22225 (CVSS 8.2) permite que invasores autenticados gravem dados arbitrários em hosts ESXi por meio do processo VMX, facilitando escapes de sandbox. Ao manipular a memória do kernel, os adversários obtêm privilégios elevados para implantar malware ou interromper serviços.

Essa falha é particularmente perigosa em ambientes de nuvem multilocatários, onde uma única VM comprometida pode comprometer clusters inteiros.

Vazamento de memória do hipervisor (CVE-2025-22226)

A terceira vulnerabilidade, CVE-2025-22226 (CVSS 7.1), decorre de uma leitura fora dos limites no Host Guest File System (HGFS) da VMware.

Os invasores que aproveitam essa falha podem extrair dados confidenciais do processo VMX, incluindo chaves de criptografia ou credenciais armazenadas na memória do hipervisor. Embora menos grave do que os outros, ele fornece dados críticos de reconhecimento para orquestrar novos ataques.

Mitigação e prevenção

A Broadcom lançou correções para todos os produtos afetados, incluindo:

- ESXi 8.0/7.0: Patches ESXi80U3d-24585383 e ESXi70U3s-2458529;
- Workstation 17.x: a versão 17.6.3 aborda o CVE-2025-22224/22226;
- Fusion 13.x: a atualização 13.6.3 resolve o CVE-2025-22226.

As organizações que usam o VMware Cloud Foundation ou o Telco Cloud Platform devem aplicar patches assíncronos ou atualizar para versões fixas do ESXi.

- Aplicação imediata de patches: priorize atualizações para ESXi, Workstation e Fusion.
- Monitorar a atividade da VM: detecte padrões incomuns de escalonamento de privilégios ou acesso à memória.
- Aproveite as estruturas BOD 22-01: alinhe os fluxos de trabalho de correção com os cronogramas KEV da CISA.

Com a exploração já observada, a correção atrasada corre o risco de violações em grande escala semelhantes aos incidentes do vCenter Server de 2024. Como a virtualização sustenta a infraestrutura crítica, a defesa proativa é fundamental para frustrar os adversários do estado-nação que buscam acesso persistente.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/cisa-warns-vmware-vulnerabilities/

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: Comitê Editorial de Segurança da Service Sec