BOLETIM DE SEGURANÇA

Operadores de ransomware explorando vulnerabilidade do hipervisor ESXi em ataques

heimdall
security research
A DIVISION OF ISH

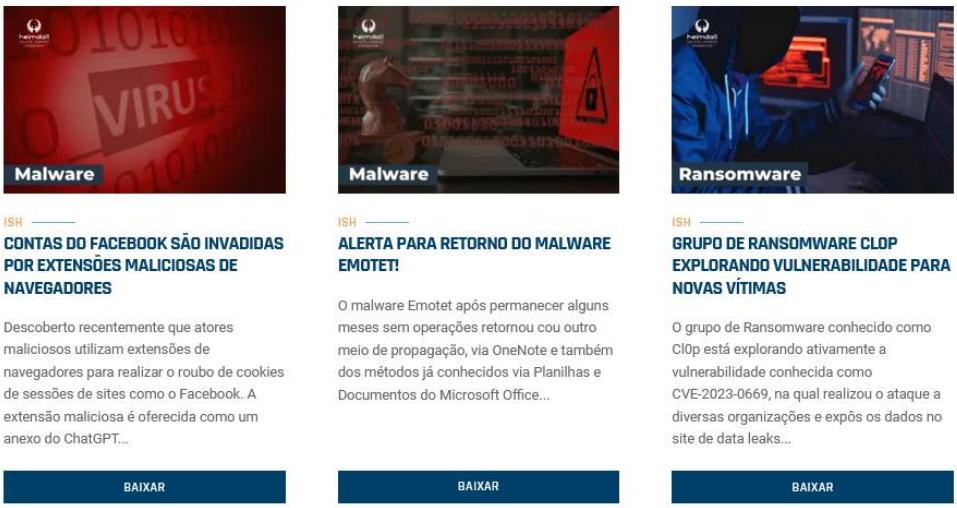
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Microsoft recentemente alertou que uma vulnerabilidade em **hipervisores ESXi** está sendo explorada por vários operadores de ransomware para obter permissões administrativas completas em hipervisores ESXi unidos a domínios. O ESXi é um hipervisor bare-metal que se instala diretamente em um servidor físico, permitindo acesso direto e controle sobre os recursos subjacentes. Os hipervisores ESXi hospedam máquinas virtuais, que podem incluir servidores críticos em uma rede. Em um ataque de ransomware, a obtenção de permissões administrativas totais em um hipervisor ESXi permite que o agente malicioso criptografe o sistema de arquivos, impactando a operação e a funcionalidade dos servidores hospedados. Além disso, isso possibilita ao atacante acessar VMs hospedadas, exfiltrar dados ou movimentar-se lateralmente pela rede.

2 FALHA EXPLORADA E TÉCNICAS UTILIZADAS PELOS ATORES

A falha do hipervisores ESXi apontada pela Microsoft é identificada como CVE-2024-37085, envolve um grupo de domínio cujos membros recebem acesso administrativo total ao hipervisor ESXi por padrão, sem validação adequada. O bug permite que invasores adicionem um novo usuário a um grupo '**ESX Admins**' que eles criam, um usuário que receberá automaticamente privilégios administrativos completos no hipervisor ESXi. Os operadores de ransomware como **Storm-0506**, **Storm-1175**, **Octo Tempest** e **Manatee Tempest** em vários ataques. Em vários casos, o uso dessa técnica levou a implantações de ransomware Akira e **Black Basta**.

- *net group "ESX Admins" /domain /add*
- *net group "ESX Admins" username /domain /add*

Ao investigar os ataques e o comportamento descrito, os pesquisadores da Microsoft descobriram que o propósito dos agentes de ameaça para usar esse comando era utilizar uma vulnerabilidade em hipervisores ESXi unidos a domínios que permite que o agente de ameaça eleve seus privilégios para acesso administrativo total no hipervisor ESXi. Em ma análise mais detalhada da vulnerabilidade revelou que os hipervisores VMware ESXi associados a um domínio do Active Directory consideram qualquer membro de um grupo de domínio denominado "ESX Admins" como possuindo acesso administrativo total por padrão. Este grupo não é um grupo interno no Active Directory e não existe por padrão. Os hipervisores ESXi não verificam a existência desse grupo ao associar o servidor a um domínio, mas ainda tratam os membros de um grupo com este nome como tendo acesso administrativo total, mesmo que o grupo não tenha existido originalmente. Além disso, a associação ao grupo é baseada no nome e não no identificador de segurança (SID).

Pesquisadores da Microsoft identificaram três métodos para explorar essa vulnerabilidade:

Adicionar o grupo "ESX Admins" ao domínio e adicionar um usuário a ele.

- Este método está sendo ativamente explorado por agentes de ameaças mencionados anteriormente. Nesse cenário, se o grupo "ESX Admins" não existir, qualquer usuário de domínio com permissão para criar um grupo pode elevar seus privilégios para obter acesso administrativo total aos hipervisores ESXi associados ao domínio. Eles fazem isso criando o grupo "ESX Admins" e, em seguida, adicionando a si mesmos ou a outros usuários sob seu controle a este grupo.

Renomear qualquer grupo no domínio para "ESX Admins" e adicionar um usuário ao grupo ou usar um membro

- Este método é similar ao anterior, mas aqui o agente da ameaça precisa de um usuário com a capacidade de renomear alguns grupos arbitrários e alterar o nome de um deles para "ESX Admins". O agente pode então adicionar um usuário ao grupo ou utilizar um usuário que já esteja no grupo para escalar privilégios e obter acesso administrativo total. A Microsoft ainda não observou esse método sendo utilizado na prática.

Atualização de privilégios do hipervisor ESXi

- Mesmo que o administrador da rede atribua outro grupo no domínio para gerenciar o hipervisor ESXi, os privilégios administrativos completos dos membros do grupo "ESX Admins" não são removidos imediatamente, permitindo que agentes de ameaças ainda possam explorá-los. A Microsoft não observou esse método sendo utilizado na prática até o momento.

A exploração bem-sucedida resulta em acesso administrativo total aos hipervisores ESXi, permitindo que os agentes maliciosos criptografem o sistema de arquivos do hipervisor, o que pode comprometer a operação e a funcionalidade dos servidores hospedados. Além disso, possibilita que os atacantes acessem as máquinas virtuais hospedadas, exfiltrem dados ou se movimentem lateralmente pela rede.

3 IMPLANTAÇÃO DO RANSOMWARE BLACK BASTA PELO STORM-0506.

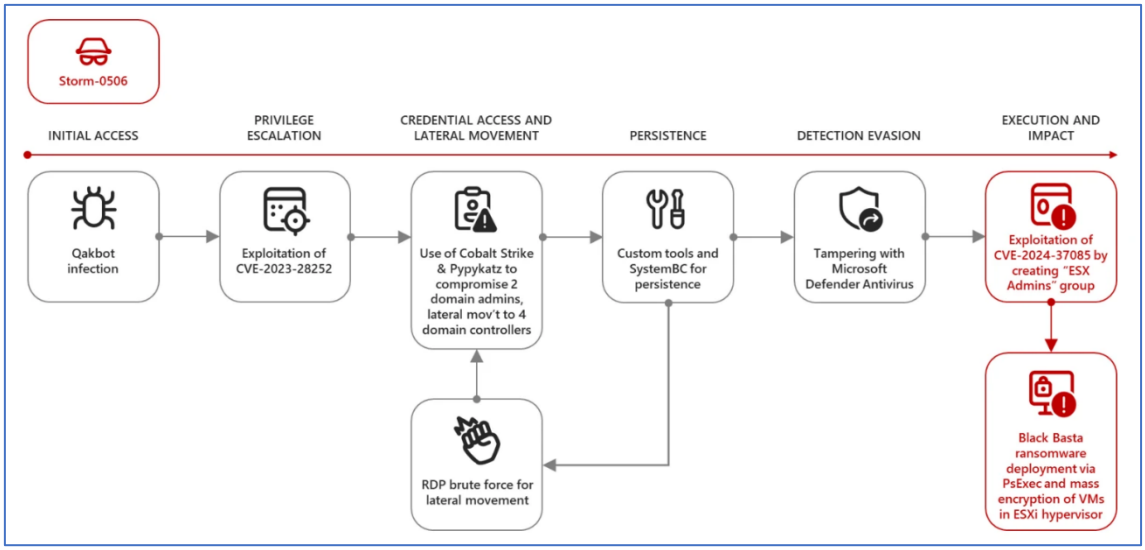


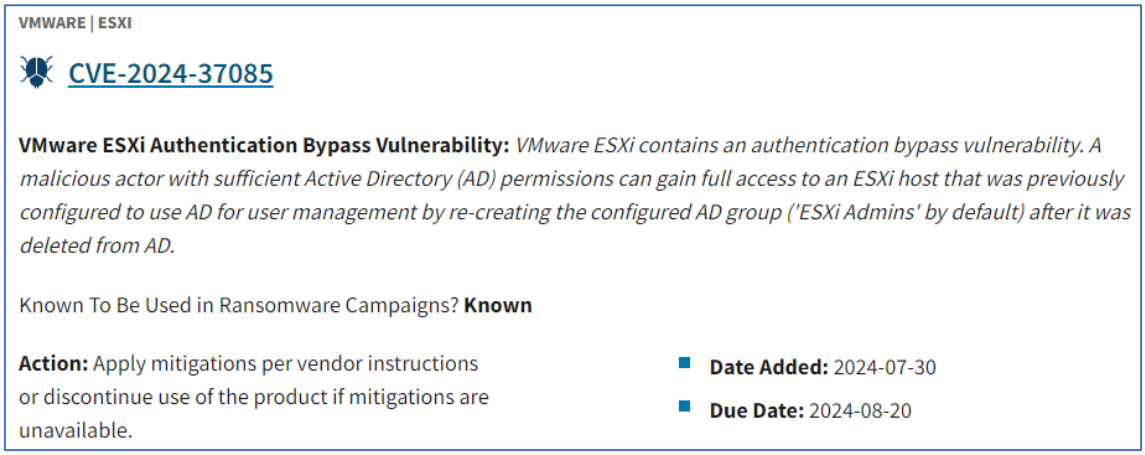
Figura 1 – Cadeia de ataque do Storm-0506 para implantação do Black Basta.

No início deste ano, uma empresa de engenharia na América do Norte foi vítima de um ataque do ransomware Black Basta, perpetrado pelo grupo **Storm-0506**. Durante o incidente, os atacantes exploraram a vulnerabilidade **CVE-2024-37085** para obter privilégios elevados nos hipervisores ESXi da organização. O acesso inicial foi conseguido através da infecção pelo malware Qakbot, seguido pela exploração da vulnerabilidade CVE-2023-28252 no Windows CLFS para elevar os privilégios nos dispositivos comprometidos. Em seguida, os atacantes utilizaram ferramentas como Cobalt Strike e Pypykatz (uma versão em Python do Mimikatz) para roubar as credenciais de dois administradores de domínio e mover-se lateralmente para quatro controladores de domínio.

Nos controladores de domínio comprometidos, os atacantes instalaram mecanismos de persistência utilizando ferramentas personalizadas e um implante SystemBC. Eles também foram observados tentando usar conexões do Remote Desktop Protocol (RDP) para se mover lateralmente e reinstalar o Cobalt Strike e o SystemBC. Além disso, tentaram desativar o Microsoft Defender Antivírus com várias ferramentas para evitar a detecção. A Microsoft identificou que os atacantes criaram o grupo "ESX Admins" no domínio e adicionaram uma nova conta de usuário a ele. Como resultado dessas ações, a criptografia do sistema de arquivos ESXi foi observada, levando à perda de funcionalidade das máquinas virtuais hospedadas no hipervisor ESXi. Além disso, os atacantes usaram o PsExec para criptografar dispositivos que não estavam hospedados no hipervisor ESXi.

4 VULNERABILIDADE ADICIONADA AO KEV-CISA

Devido estas explorações a vulnerabilidade já foi adicionada ao Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV).



VMWARE | ESXI

CVE-2024-37085

VMware ESXi Authentication Bypass Vulnerability: *VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.*

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-07-30
- **Due Date:** 2024-08-20

Figura 2 – Falha no catálogo da CISA-KEV.

5 CONCLUSÃO

Os riscos para organizações decorrentes das explorações realizadas por operadores de ransomware são significativos e multifacetados. Primeiramente, o acesso administrativo total aos hipervisores ESXi permite a criptografia do sistema de arquivos, interrompendo operações críticas e comprometendo a continuidade dos negócios. A capacidade de movimentação lateral e exfiltração de dados facilita a expansão do ataque dentro da rede, aumentando o alcance e o impacto do incidente. Além disso, a instalação de mecanismos de persistência e a desativação de soluções de segurança dificultam a detecção e a remoção das ameaças. Finalmente, a exploração de vulnerabilidades não corrigidas expõe a organização a riscos contínuos, destacando a importância de práticas robustas de segurança cibernética e manutenção regular de sistemas.

6 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1566 Phishing T1190 Exploit Public-Facing Application	Qakbot pode ser entregue através de e-mails de phishing ou exploração de aplicações expostas.
Privilege Escalation	T1068 Exploitation for Privilege Escalation	Exploração da vulnerabilidade CVE-2023-28252 para ganhar privilégios elevados.
Credential Access and Lateral Movement	T1003 Credential Dumping T1078 Valid Accounts T1071 Application Layer Protocol T1110 Brute Force	Uso de ferramentas como Cobalt Strike e Pypykatz para extrair credenciais e movimentar-se lateralmente na rede. Uso de força bruta para ganhar acesso via RDP.
Persistence	T1547 Boot or Logon Autostart Execution T1053 Scheduled Task/Job	Uso de ferramentas personalizadas e SystemBC para garantir persistência.
Detection Evasion	T1562 Impair Defenses	Manipulação do Microsoft Defender para evitar detecção.
Execution and Impact	T1486 Data Encrypted for Impact T1569 System Services	Implantação do ransomware Black Basta usando PsExec e criptografia massiva de VMs.

Tabela 1 – Tabela MITRE ATT&CK.

7 RECOMENDAÇÕES

A Microsoft recomenda as seguintes medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Instalar atualizações de software

Certifique-se de instalar as últimas atualizações de segurança lançadas pela VMware em todos os hipervisores ESXi ingressados no domínio. Se não for possível instalar atualizações de software, você pode usar as seguintes recomendações para reduzir o risco:

- Valide se o grupo "*ESX Admins*" existe no domínio e está protegido.
- Negue manualmente o acesso deste grupo alterando as configurações no próprio hipervisor ESXi . Se o acesso de administrador total para o grupo de administradores ESX do Active Directory não for desejado, você pode desabilitar esse comportamento usando a configuração avançada do host:
- '*Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd*'.
- Altere o grupo de administração para um grupo diferente no hipervisor ESXi.
- Adicione detecções personalizadas no XDR/SIEM para o novo nome do grupo.
- Configure o envio de logs do ESXi para um sistema SIEM e monitore acesso administrativo completo suspeito.

Higiene das credenciais

Para utilizar os diferentes métodos de vulnerabilidade, os agentes de ameaças exigem o controle de um usuário altamente privilegiado na organização. Portanto, nossa recomendação é garantir a proteção de suas contas altamente privilegiadas na organização, especialmente aquelas que podem gerenciar outros grupos de domínio:

- Aplique autenticação multifator (MFA) em todas as contas, remova usuários excluídos da MFA e exija estritamente a MFA de todos os dispositivos, em todos os locais, sempre.
- Habilite métodos de autenticação sem senha (por exemplo, Windows Hello, chaves FIDO ou Microsoft Authenticator) para contas que oferecem suporte a autenticação sem senha. Para contas que ainda exigem senhas, use aplicativos autenticadores como o Microsoft Authenticator para MFA.
- Isole contas privilegiadas de contas de produtividade para proteger o acesso administrativo ao ambiente.

Melhore a postura de segurança dos ativos críticos

Identifique seus ativos críticos na rede, como hipervisores ESXi e vCenters (uma plataforma centralizada para controlar ambientes VMware vSphere), e

certifique-se de protegê-los com as últimas atualizações de segurança, procedimentos de monitoramento adequados e planos de backup e recuperação.

Identifique ativos vulneráveis

Implante varreduras autenticadas de dispositivos de rede para identificar vulnerabilidades em dispositivos da rede, como ESXi, e receber recomendações de segurança.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **MITRE ATT&CK**
- **NVD**

9 AUTORES

- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH