BOLETIM DE SEGURANÇA

BlackByte Ransomware explora vulnerabilidade do VMware ESXi em nova onda de ataques

heimdall
security research
A DIVISION OF ISH

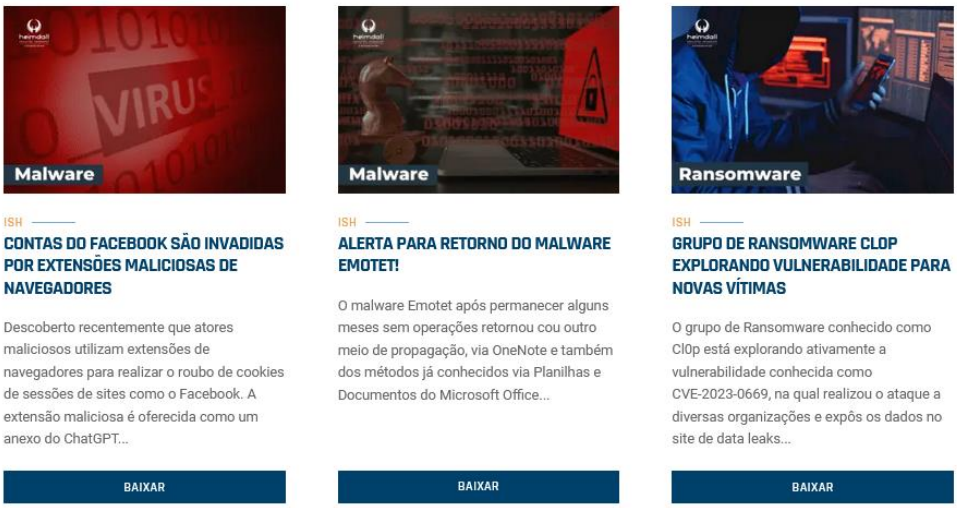
TLP: CLEAR

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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

O grupo de ransomware BlackByte continua a utilizar táticas, técnicas e procedimentos (TTPs) que têm sido a base de sua eficácia desde o início. Eles iteram continuamente o uso de drivers vulneráveis para contornar proteções de segurança e implantam um criptografador de ransomware autopropagante e com características de worm.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Em investigações recentes, o Talos IR observou o BlackByte utilizando técnicas que se afastam de sua tradição, como explorar a vulnerabilidade CVE-2024-37085 no VMware ESXi logo após sua divulgação, e usar o mecanismo de acesso remoto autorizado da vítima em vez de uma ferramenta comercial como o AnyDesk.

Foi identificada uma nova versão do criptografador BlackByte que adiciona a extensão “blackbytent_h” aos arquivos criptografados, descarta quatro arquivos de driver vulneráveis em vez de três, e usa as credenciais do Active Directory da vítima para se autopropagar. A empresa também avalia que o grupo BlackByte é mais ativo do que seu site de vazamento de dados sugere, com apenas 20 a 30 por cento dos ataques bem-sucedidos resultando em uma postagem de extorsão.

O BlackByte é um grupo de ransomware-as-a-service (RaaS) que se acredita ser um desdobramento do grupo Conti. Observado pela primeira vez em meados de 2021, seu trabalho inclui o uso de drivers vulneráveis para contornar controles de segurança, implantação de ransomware autopropagante com características de worm, e o uso de binários de sistema conhecidos como bons (LoLBins) e outras ferramentas comerciais legítimas como parte de sua cadeia de ataque. O ator reprojetou seu binário de ransomware ao longo do tempo, com versões escritas em Go, .NET, C++ ou uma combinação dessas linguagens. Os esforços do grupo para melhorar continuamente suas ferramentas, operações e até mesmo seu site de vazamento de dados estão bem documentados.

Durante a investigação de um ataque recente do BlackByte, notou-se semelhanças entre indicadores de comprometimento (IOCs) descobertos durante a investigação e outros eventos na telemetria global do Talos. Investigações mais aprofundadas revelaram que o grupo é significativamente mais ativo do que parece pelo número de vítimas publicado em seu site de vazamento de dados. Durante análise sobre um recente ataque de ransomware BlackByte, o agente da ameaça obteve acesso inicial usando credenciais válidas para acessar a VPN da organização vítima. Limitações na telemetria e perda de evidências após o evento de criptografia impediram o Talos IR de determinar se as credenciais foram obtidas por força bruta da interface VPN ou se já eram conhecidas pelo adversário antes do ataque. No entanto, o Talos IR tem confiança moderada de que a autenticação de força bruta facilitada por varredura na Internet foi o vetor de acesso inicial, com base nas seguintes observações:

A conta inicial comprometida pelo adversário tinha uma convenção de nomenclatura básica e, supostamente, uma senha fraca. A interface VPN pode ter permitido que uma conta de domínio fosse autenticada sem autenticação multifator (MFA) se a conta de destino tivesse uma configuração específica do Active Directory.

O ator tem um histórico de varredura e exploração de vulnerabilidades públicas, como a vulnerabilidade ProxyShell no servidor Microsoft Exchange. Dado o histórico do BlackByte de explorar vulnerabilidades públicas para acesso inicial, o uso de VPN para acesso remoto pode representar uma ligeira mudança na técnica ou oportunismo. O uso da VPN da vítima para acesso remoto também oferece ao adversário outras vantagens, incluindo visibilidade reduzida do EDR da organização.

Após obter acesso inicial ao ambiente, o adversário escalou privilégios comprometendo duas contas de nível de administrador de domínio. Uma dessas contas foi usada para acessar o servidor VMware vCenter da organização e, logo depois, criar objetos de domínio do Active Directory para hipervisores VMware ESXi individuais, unindo esses hosts ao domínio. A mesma conta foi usada para criar e adicionar várias outras contas a um grupo do Active Directory chamado “ESX Admins”. Foi avalidado que esse grupo foi criado para explorar a vulnerabilidade CVE-2024-37085 no VMware ESXi, conhecida por ser usada por vários grupos de ransomware. A exploração bem-sucedida dessa vulnerabilidade concede aos membros de um grupo específico do Active Directory privilégios elevados em um host ESXi, permitindo o controle sobre máquinas virtuais (VMs), a capacidade de modificar a configuração do servidor host e o acesso a logs do sistema, diagnósticos e ferramentas de monitoramento de desempenho.

O Talos IR observou o agente de ameaça alavancando essa vulnerabilidade, que inicialmente recebeu atenção limitada da comunidade de segurança, poucos dias após sua publicação. Isso destaca a velocidade com que grupos de ransomware como o BlackByte podem adaptar seus TTPs para incorporar vulnerabilidades recém-divulgadas, e o nível de tempo e esforço investidos na identificação de potenciais vias para avançar um ataque. O agente da ameaça acessou outros sistemas, diretórios e arquivos dentro do ambiente de cada vítima usando protocolos como Server Message Block (SMB) e Remote Desktop Protocol (RDP). A análise dos logs de eventos e autenticação do sistema revelou um padrão consistente em que o agente da ameaça aproveitou principalmente o NT LAN Manager (NTLM) para autenticação, enquanto os usuários organizacionais usaram principalmente o Kerberos. Essa atividade NTLM inicial pode refletir ataques de autenticação, como passar o hash para movimento lateral. A análise dinâmica do binário do ransomware revelou posteriormente o uso consistente do NTLM para autenticação por esse arquivo também.

Observou-se a execução de um arquivo chamado “atieclxx.exe” do diretório “C:\temp\sys\” em um dos servidores de arquivos. A versão legítima do “atieclxx.exe” normalmente pode ser encontrada no diretório “C:\Windows\System32”, onde ele suporta processos do sistema associados a placas de vídeo AMD. No entanto, durante a investigação de um ataque BlackByte, “atieclxx.exe” foi executado do diretório “C:\temp\sys” com o comando atieclxx.exe P@$$w0rd123!!!. Como os atores do BlackByte são conhecidos por favorecer a string “P@$$w0rd” ao definir senhas de conta e como parâmetros de entrada para ferramentas personalizadas, essa sintaxe pode indicar esforços para disfarçar malware – como sua ferramenta personalizada de exfiltração de dados, ExByte – como um arquivo conhecido ou legítimo.

Por fim, o agente da ameaça foi observado adulterando configurações de ferramentas de segurança por meio de modificações no registro do sistema, desinstalando manualmente o EDR de vários sistemas-chave e, em uma investigação, alterando a senha raiz dos hosts ESXi da organização. Imediatamente antes do primeiro sinal de criptografia de arquivo, volumes aumentados de autenticação NTLM e tentativas de conexão SMB foram observados entre dezenas de sistemas no ambiente. Essa atividade foi posteriormente entendida como característica do mecanismo de autopropagação do ransomware.

Restrições na telemetria disponível, o impacto do processo de criptografia do ransomware e o local de preparação fora da rede do adversário durante a investigação do Talos IR impediram uma avaliação de alta confiança dos métodos de exfiltração de dados e se a exfiltração ocorreu. Conforme mencionado anteriormente, o possível uso da ferramenta de exfiltração de dados personalizada da BlackByte, ExByte, foi observado, mas não pôde ser confirmado.

Em investigações recentes, o binário do ransomware BlackByte, “host.exe,” foi executado do mesmo diretório – “C:\Windows” – em todas as vítimas analisadas pelo Talos IR. A sintaxe do comando usada pelo adversário durante cada ataque – C:\Windows\host.exe -s [string numérica de 8 dígitos] svc – e o comportamento do binário do ransomware são consistentes com análises anteriores do binário BlackByteNT pela Microsoft, DuskRise, Acronis e outros. Os pontos em comum observados incluíram:

- O binário do ransomware não será executado sem a sequência numérica correta de oito dígitos passada para o parâmetro “-s”. Essa sequência de oito dígitos era a única parte da sintaxe do comando que variava entre as vítimas. Em um ataque, o adversário usou dois criptografadores diferentes sequencialmente, cada um com seu próprio valor de parâmetro “-s”, embora não estivesse claro por que vários criptografadores foram empregados.

- O parâmetro “svc” faz com que o ransomware se instale como um serviço, o que parece transformar um sistema infectado em um propagador adicional como parte do comportamento wormável do ransomware. Autenticações SMB e NTLM subsequentes foram observadas contra hosts alcançáveis após a criação do serviço de ransomware, resultando em várias ondas de criptografia horas após o evento inicial.

- O binário do ransomware cria e opera principalmente a partir do diretório “C:\SystemData”. Vários arquivos comuns são criados neste diretório em todas as vítimas do BlackByte, incluindo um arquivo de texto chamado “MsExchangeLog1.log”, que parece ser um log de rastreamento de processo onde os marcos de execução são registrados como valores “q”, “w” e “b” separados por vírgulas.

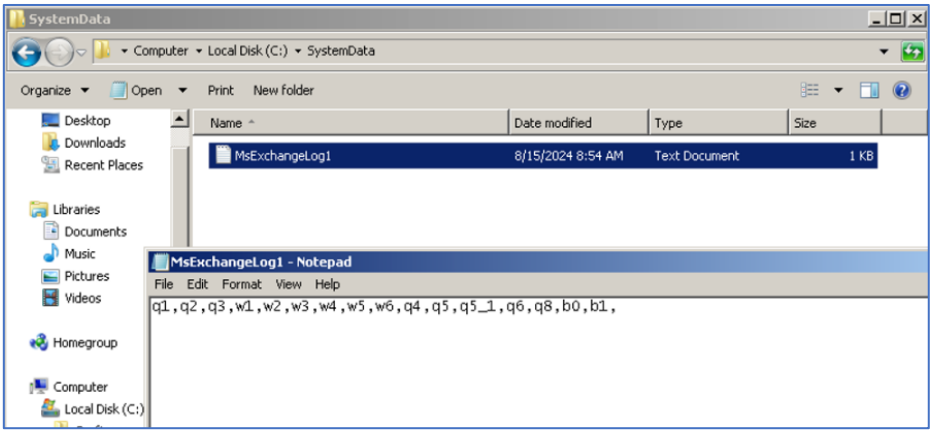


Figura 1 – Conteúdo do MsExchangeLog1.log durante a execução.

Recentes ataques do BlackByte mostraram algumas diferenças. Notavelmente, arquivos criptografados em todas as vítimas receberam a extensão “blackbytent_h”, ainda não relatada publicamente.

A versão mais recente do criptografador descarta quatro drivers vulneráveis como parte da técnica Bring Your Own Vulnerable Driver (BYOVD) do BlackByte, um aumento em relação aos dois ou três drivers mencionados anteriormente. Os quatro drivers foram descartados pelo binário do criptografador em todos os ataques investigados pelo Talos IR, cada um com uma convenção de nomenclatura semelhante – oito caracteres alfanuméricos aleatórios seguidos por um sublinhado e um valor numérico iterativo. Usando “AM35W2PH” como exemplo fictício, os drivers vulneráveis apareceriam na seguinte ordem:

- “AM35W2PH” – RtCore64.sys, um driver usado originalmente pelo MSI Afterburner, um utilitário de overclock do sistema.
- “AM35W2PH_1” – DBUtil_2_3.sys, um driver do utilitário de atualização de firmware da Dell.

- “AM35W2PH_2” – zamguard64.sys, um driver do aplicativo Zemana Anti-Malware (ZAM).
- “AM35W2PH_3” – gdrv.sys, um driver do pacote de software GIGABYTE Tools para placas-mãe GIGABYTE.

A inclusão do arquivo “zamguard64.sys”, também conhecido como “Terminator”, é particularmente interessante devido a relatórios recentes de outros pesquisadores de segurança sobre sua prevalência. Além disso, o binário do ransomware criou duas chaves de registro relacionadas ao serviço associadas a esse arquivo durante a execução, e depois as excluiu mais tarde no processo de execução. Usando a mesma sequência fictícia acima, essas chaves de registro seriam:

- HKLM\SISTEMA\CONTROLSET001\SERVIÇOS\AM35W2PH_2
- HKLM\SISTEMA\CONTROLSET001\SERVIÇOS\AM35W2PH_2\SEGURANÇA

Durante a análise dinâmica de vários binários do ransomware BlackByte, a Talos descobriu que o arquivo tentou enumerar o compartilhamento de rede por meio da função NetShareEnumAll do pipe nomeado ‘SRVSVC’ usando contas de usuário específicas associadas à vítima. Como essa análise foi conduzida em um ambiente controlado e em sandbox, essas contas só poderiam aparecer no tráfego de rede se fossem incorporadas ao próprio binário do ransomware. Essa descoberta dá à Talos alta confiança de que a personalização por vítima do BlackByte do criptografador de ransomware inclui empacotar alguma forma de credencial roubada no binário para dar suporte à sua capacidade de worm.

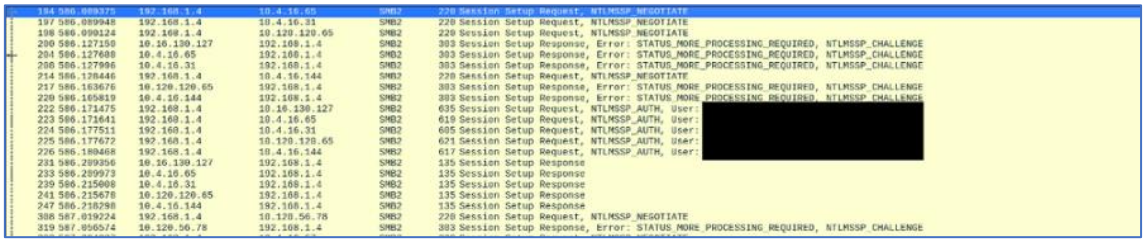


Figura 2 – Credenciais das vítima.

A análise da BlackByte confirma essa avaliação, com mais de 32% das vítimas identificadas pertencendo ao setor de manufatura.

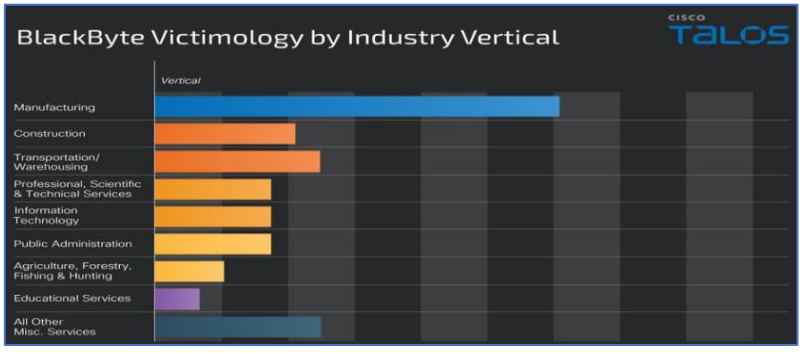


Figura 3 – Vitimização do BlackByte por setor vertical.

Provavelmente, esses números são conservadores, considerando a diferença entre o número de vítimas divulgadas no site de vazamento de dados do BlackByte nos últimos seis a nove meses e o número de vítimas identificadas na telemetria e relatadas publicamente. Não está claro por que apenas uma parte limitada — estimada entre 20 e 30 por cento — das vítimas do BlackByte é eventualmente divulgada.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1078.002 T1078.003	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Discovery	T1018 T1083	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Persistence	T1136.002	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Execution	T1204 T1569.002	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Privilege Escalation	T1543 T1484.001 T1484 T1098	Consiste em técnicas que os adversários usam para obter permissões de nível mais alto em um sistema ou rede.
Lateral Movement	T1021.002 T1021.001 T1210	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.
Resource Development	T1608	Consiste em técnicas que envolvem adversários criando, comprando ou comprometendo/roubando recursos que podem ser usados para dar suporte à segmentação.
Defense Evasion	T1562.001 T1112 T1070.004 T1211	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Impact	T1529 T1486	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Implementar MFA

- Priorizar “push verificado” como o método MFA em vez de opções menos seguras, como SMS ou chamada telefônica.

Auditar a configuração de VPN

- Confirme se as políticas de VPN legadas foram removidas e se as tentativas de autenticação que não correspondem a uma política de VPN atual são negadas por padrão.

Limitação do NTLM

- Limite ou desabilite o uso de NTLM onde possível e imponha métodos de autenticação mais seguros como Kerberos. Limite a taxa de tentativas e falhas de autenticação em interfaces públicas e internas para evitar varredura de autenticação automatizada.

Desabilitar o SMB

- Desabilite o SMBv1 e imponha a assinatura e a criptografia do SMB para proteger contra movimentação lateral e propagação de malware.

Implantação de EDR

- Implante clientes EDR em todos os sistemas em todo o ambiente . Configure uma senha de administrador em clientes EDR para impedir adulteração ou remoção não autorizada do cliente.

Criações de detecções

- Crie detecções para alterações de configuração não autorizadas que podem ser feitas em vários sistemas no ambiente, incluindo alterações nas políticas do Windows Defender, alterações não autorizadas em Objetos de Política de Grupo e criação de tarefas agendadas e serviços instalados incomuns.

Aplicações de Patches

- Fortaleça e aplique patches nos hosts ESX para reduzir a superfície de ataque desses servidores críticos na medida do possível e garantir que as vulnerabilidades recém-descobertas sejam corrigidas o mais rápido possível.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	2d8e4f38b36c334d0a32a7324832501d
sha1:	f6f11ad2cd2b0cf95ed42324876bee1d83e01775
sha256:	01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd
File name:	RtCore64.sys

Indicadores de compromisso do artefato	
md5:	c996d7971c49252c582171d9380360f2
sha1:	c948ae14761095e4d76b55d9de86412258be7afd
sha256:	0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5
File name:	DBUtil_2_3.Sys

Indicadores de compromisso do artefato	
md5:	21e13f2cb269defeae5e1d09887d47bb
sha1:	16d7ecf09fc98798a6170e4cef2745e0bee3f5c7
sha256:	543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91
File name:	zamguard64.sys

Indicadores de compromisso do artefato	
md5:	9ab9f3b75a2eb87fafb1b7361be9dfb3
sha1:	fe10018af723986db50701c8532df5ed98b17c39
sha256:	31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427
File name:	gdrv.sys

Tabela 2 – Indicadores de Compromissos de artefatos

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Talos
- Thehackernews

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH