

HiveForce Labs

THREAT ADVISORY

**ATTACK REPORT**

BlackByte Ransomware Exploits VMware Flaw and Beyond

Date of Publication

August 30, 2024

Admiralty Code

A1

TA Number

TA2024336

Summary

First Seen: July 2021

Malware: BlackByte Ransomware

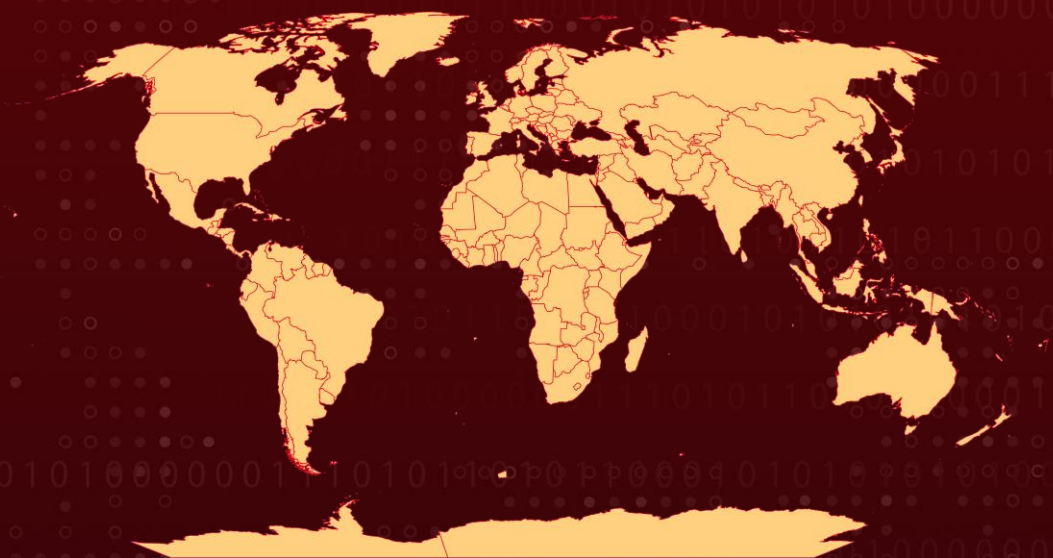
Targeted Region: Worldwide

Targeted Industries: Manufacturing, Construction, Transportation, Professional Services, Agriculture, Education, Technology, Government

Affected Product: VMware ESXi hypervisors




Attack: BlackByte, a ransomware-as-a-service (RaaS) group believed to have originated from the infamous Conti ransomware, first appeared in 2021. The group rapidly gained notoriety for exploiting security vulnerabilities, including the recently patched CVE-2024-37085, which affects VMware ESXi hypervisors.

Attack Regions



CVE

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi			

Attack Details

#1

BlackByte is a ransomware-as-a-service (RaaS) group that likely evolved from the notorious Conti ransomware group, first emerging in 2021. This group has been observed exploiting a recently patched security vulnerability, tracked as CVE-2024-37085, which affects VMware ESXi hypervisors.

#2

Additionally, BlackByte leverages vulnerable drivers to bypass security defenses and deploys a self-propagating, ransomware encryptor with worm-like capabilities. Over time, BlackByte has refined its ransomware binary, developing versions in Go, .NET, C++, or a combination of these languages.

#3

In recent attacks, the group's tactics involve gaining initial access using valid credentials, often obtained through brute-forcing VPN interfaces. Once inside, they escalate privileges, frequently targeting Domain Admin-level accounts to further infiltrate the victim's network.

#4

BlackByte's attack chain includes reconnaissance and enumeration, using protocols like SMB and RDP. The group is also known for tampering with security configurations, including uninstalling EDR from critical systems and altering essential passwords. Before executing the ransomware, they typically exfiltrate data using tools like their custom ExByte tool.

#5

A notable aspect of BlackByte's tactics is their use of the Bring Your Own Vulnerable Driver (BYOVD) technique, where they drop vulnerable drivers to complicate detection and removal. Encrypted files across all victims are rewritten with the file extension "blackbytent_h."

Recommendations



Harden and Patch VMware ESXi Host: Harden and patch ESXi hosts to minimize their attack surface. Ensure that all newly discovered vulnerabilities specifically CVE-2024-37085 are patched promptly to protect these critical systems from exploitation.



Audit and Strengthen VPN Configurations: Regularly audit your VPN configurations to ensure that outdated or legacy VPN policies are removed. Any authentication attempts that do not match current VPN policies should be automatically denied. Limit VPN access to essential network segments and services only. This approach minimizes the exposure of critical assets, such as Domain Controllers, reducing the attack surface.



Enhance Authentication Security: Where possible, limit or disable the use of NTLM (NT LAN Manager) and enforce more secure authentication methods like Kerberos. Implement rate limiting on authentication attempts and failures for both public-facing and internal interfaces to prevent automated scanning and brute-force attacks.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0004</u> Privilege Escalation	<u>TA0005</u> Defense Evasion	<u>TA0007</u> Discovery	<u>TA0008</u> Lateral Movement
<u>TA0010</u> Exfiltration	<u>TA0040</u> Impact	<u>T1078.002</u> Domain Accounts	<u>T1078.003</u> Local Accounts
<u>T1078</u> Valid Accounts	<u>T1018</u> Remote System Discovery	<u>T1083</u> File and Directory Discovery	<u>T1136</u> Create Account
<u>T1136.002</u> Domain Account	<u>T1204</u> User Execution	<u>T1569.002</u> Service Execution	<u>T1543</u> Create or Modify System Process
<u>T1484.001</u> Group Policy Modification	<u>T1484</u> Domain Policy Modification	<u>T1098</u> Account Manipulation	<u>T1021.002</u> SMB/Windows Admin Shares

T1021.001 Remote Desktop Protocol	T1210 Exploitation of Remote Services	T1608 Stage Capabilities	T1562.001 Disable or Modify Tools
T1112 Modify Registry	T1070.004 File Deletion	T1211 Exploitation for Defense Evasion	T1529 System Shutdown/Reboot
T1486 Data Encrypted for Impact			

🔗 Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd, 0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5, 543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91, 31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427
File Name	RtCore64.sys, DBUtil_2_3.sys, zamguard64.sys, gdrv.sys
TOR Address	tj3ty2q5jm5au3bmd2embtjscd3qjt7nfio2o7cr6moyy5kgil5pieqd[.]onion

🔗 Patch Link

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505>

🔗 Recent Breaches

<https://www.modernauto.com/>

<https://cityofnewburgh-ny.gov/>

References

<https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/>

<https://github.com/SpiderLabs/BlackByteDecryptor>

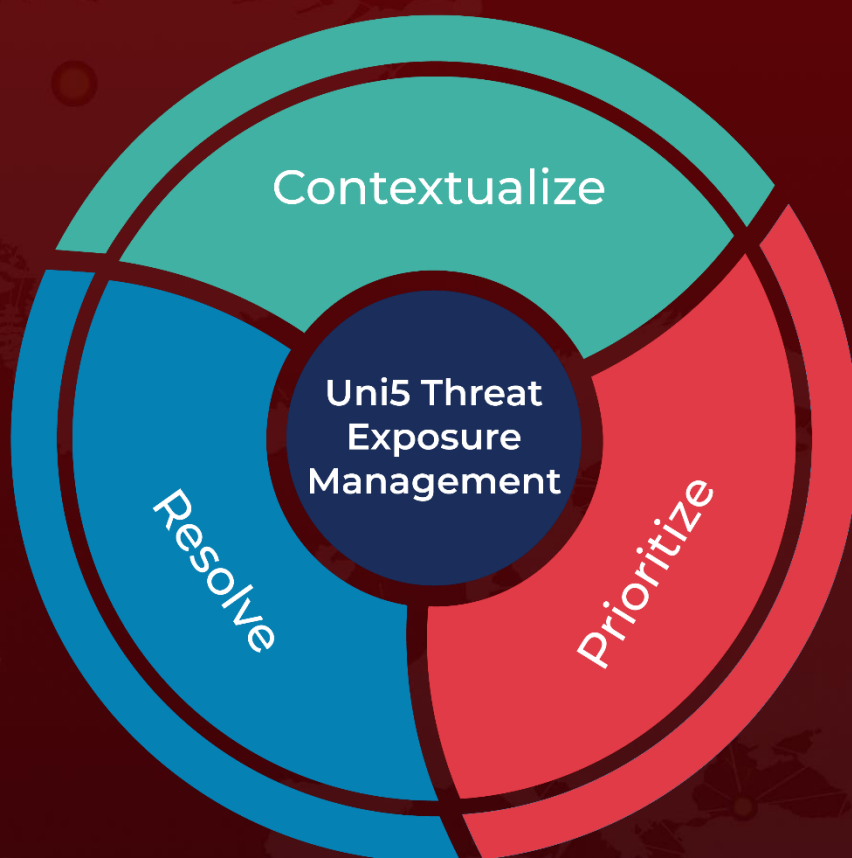
<https://hivepro.com/threat-advisory/blackbyte-uses-a-new-attack-technique-to-target-vulnerable-windows-drivers/>

<https://hivepro.com/threat-advisory/vmware-esxi-fatal-flaw-cve-2024-37085-opens-doors-for-ransomware-havoc/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

August 30, 2024 • 7:00 AM

© 2024 All Rights are Reserved by HivePro



More at www.hivepro.com