

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## **EstateRansomware Leverages Veeam Backup Vulnerability**

Date of Publication

July 15, 2024

Admiralty Code

A1

TA Number

TA2024272

# Summary

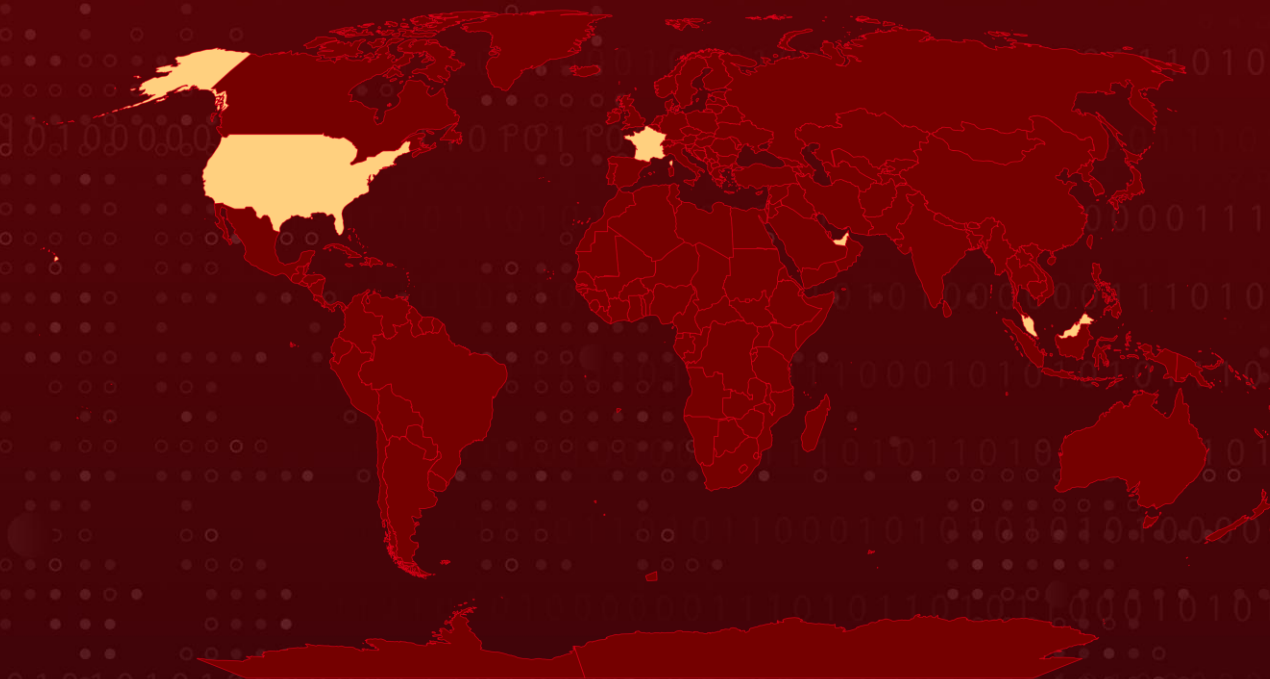
**Attack Commenced:** April 2024

**Malware:** EstateRansomware

**Targeted Countries:** UAE, France, Hong Kong, Malaysia, US




**Attack:** EstateRansomware is a newly identified ransomware group exploiting a vulnerability in Veeam Backup & Replication software to deploy file-encrypting malware and extort payments. The attack began in early April 2024.

## 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-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication			

# Attack Details

## #1

EstateRansomware is a newly emerged ransomware gang exploiting a vulnerability in Veeam Backup & Replication software to deploy file-encrypting malware and extort payments from victims. The attack began in early April 2024, with initial access to the target environment by brute-forcing a dormant account on a Fortinet FortiGate firewall SSL VPN appliance.

## #2

Next, the EstateRansomware gang proceeded to establish RDP connections from the firewall. They further utilized this remote desktop access to install a backdoor on the failover server, scheduling it to execute daily to ensure persistent access to the victim's environment. The group leverages the Veeam vulnerability to activate the xp\_cmdshell stored procedure and create a rogue user account named "VeeamBkp" to conduct further malicious activities.

## #3

This enables the attackers to disable security defenses, move laterally within the network, and ultimately deploy the ransomware payload to encrypt files. While the vulnerability CVE-2023-27532 was disclosed in March 2023 and subsequently patched by Veeam for versions 12/11a and later of the Veeam Backup & Replication software, it had previously been exploited by threat actors such as [FIN7](#) and the [Cuba ransomware](#) group (aka Fidel, COLDDRAW) in their attacks.

# Recommendations



**Patch Management Policy:** Establish a robust patch management policy to ensure all firmware and software are promptly updated with the latest security patches. Regularly apply updates to Veeam Backup & Replication software and other critical systems to protect against known vulnerabilities like CVE-2023-27532.



**Network Segmentation and Firewall Rules:** Segment the network to isolate critical systems and enforce strict firewall rules between segments to limit lateral movement. Disable unnecessary Remote Desktop Protocol (RDP) access and restrict it to specific, trusted IP addresses.



**Application Control and Whitelisting:** Implement application control measures on hosts to prevent the execution of unauthorized programs. Use whitelisting to specify which applications are allowed to run on enterprise systems, reducing the risk of malware execution.



**Monitor and Audit Accounts Regularly:** Conduct regular audits of user accounts to identify and disable any dormant accounts. Implement a policy to delete or disable accounts that are no longer in use to prevent unauthorized access.



**Implement Multi-Factor Authentication (MFA):** Enable MFA for VPN and other remote access services to add an extra layer of security. Ensure that MFA is enforced for all users accessing sensitive systems or data.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0005</u></b> Defense Evasion
<b><u>TA0006</u></b> Credential Access	<b><u>TA0007</u></b> Discovery	<b><u>TA0008</u></b> Lateral Movement	<b><u>TA0011</u></b> Command and Control
<b><u>TA0010</u></b> Exfiltration	<b><u>TA0040</u></b> Impact	<b><u>T1078</u></b> Valid Accounts	<b><u>T1204</u></b> User Execution
<b><u>T1204.002</u></b> Malicious File	<b><u>T1569</u></b> System Services	<b><u>T1569.002</u></b> Service Execution	<b><u>T1053</u></b> Scheduled Task/Job
<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1136</u></b> Create Account	<b><u>T1136.001</u></b> Local Account	<b><u>T1505</u></b> Server Software Component
<b><u>T1505.001</u></b> SQL Stored Procedures	<b><u>T1070</u></b> Indicator Removal	<b><u>T1070.001</u></b> Clear Windows Event Logs	<b><u>T1070.004</u></b> File Deletion
<b><u>T1562</u></b> Impair Defenses	<b><u>T1562.001</u></b> Disable or Modify Tools	<b><u>T1555</u></b> Credentials from Password Stores	<b><u>T1018</u></b> Remote System Discovery

<b>T1087</b> Account Discovery	<b>T1087.002</b> Domain Account	<b>T1021</b> Remote Services	<b>T1021.001</b> Remote Desktop Protocol
<b>T1571</b> Non-Standard Port	<b>T1071</b> Application Layer Protocol	<b>T1071.001</b> Web Protocols	<b>T1041</b> Exfiltration Over C2 Channel
<b>T1486</b> Data Encrypted for Impact	<b>T1110</b> Brute Force		

## ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IPv4</b>	149[.]28[.]106[.]252, 149[.]28[.]99[.]61, 45[.]76[.]232[.]205
<b>IPv4:Port</b>	77[.]238[.]245[.]11[:]30001
<b>SHA1</b>	cb704d2e8df80fd3500a5b817966dc262d80ddb8, 2c56e9beea9f0801e0110a7dc5549b4fa0661362, 5e460a517f0579b831b09ec99ef158ac0dd3d4fa, 107ec3a7ed7ad908774ad18e3e03d4b999d4690c
<b>File Name</b>	DC.exe, DC.ini, Svchost.exe, LB3.exe, netscan.exe, veeam-creds-main, CVE-2023-27532.exe, VeeamHax, BulletsPassView64.exe, netpass64.exe, PasswordFox64.exe, ChromePass.exe, WirelessKeyView64.exe, mypass.exe, VNCPassView.exe, WebBrowserPassView.exe, mailpv.exe, RouterPassView.exe, PstPassword.exe,



TYPE	VALUE
File Name	OperaPassView.exe, Dialupass.exe, ExtPassword.exe, pspv.exe, iepv.exe, SniffPass64.exe, rdpv.exe

## Patch Link

<https://www.veeam.com/kb4424>

## References

<https://www.group-ib.com/blog/estate-ransomware/>

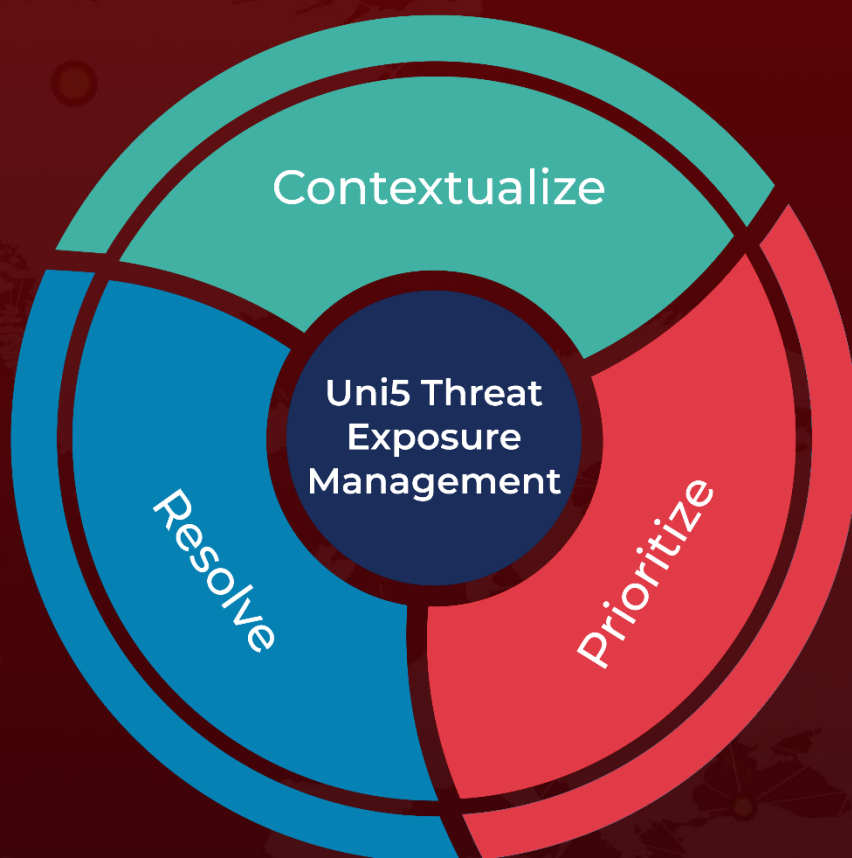
<https://hivepro.com/threat-advisory/fin7-affiliated-hackers-exploit-flaws-in-veeam-backup-servers/>

<https://hivepro.com/threat-advisory/cuba-ransomware-targets-u-s-with-veeam-exploit/>

# 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

**July 15, 2024 • 6:45 AM**

© 2024 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)