BLACKSWAN
CYBERSECURITY

# THREAT ADVISORY

July 17, 2024

## EstateRansomware Threat Group Exploiting Veeam Backup Software Vulnerability (CVE-2023-27532)

### SUMMARY

A flaw in Veeam Backup & Replication software (CVE-2023-27532) is being exploited by the EstateRansomware group, as observed by Group-IB through a dormant Fortinet FortiGate SSL VPN account. The attackers establish RDP connections, deploy backdoors, and disable defenses before executing ransomware.

### THREAT INTELLIGENCE

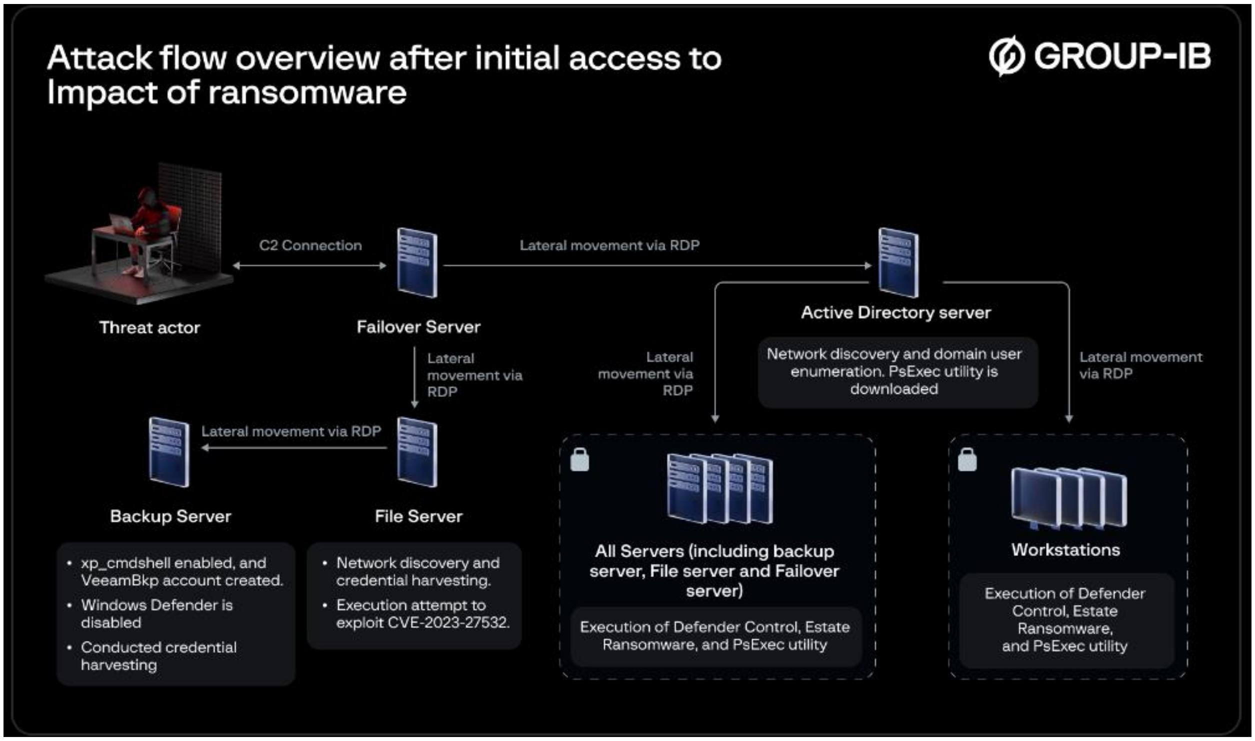
Exploits actively observed.

### TECHNICAL DETAILS

EstateRansomware is exploiting a security flaw (CVE-2023-27532) in Veeam Backup & Replication software. Initial access is obtained via a dormant account named 'Acc1' on a Fortinet FortiGate firewall SSL VPN appliance, then pivoting laterally and establishing RDP connections to a failover server. They then deploy a persistent backdoor named "svchost.exe" connected to a command-and-control (C2) server, enabling the execution of arbitrary commands.

The Veeam flaw is exploited to enable xp_cmdshell on the backup server, create a rogue user account named "VeeamBkp," and conduct network discovery, enumeration, and credential harvesting using tools like NetScan, AdFind, and NitSoft. They then move laterally across the network, disable Windows Defender using DC.exe, and deploy the ransomware with PsExec.exe.

The attack follows a double extortion model, where data is exfiltrated before encryption. This requires long-term access to explore the environment, elevate privileges, and identify valuable data.


Attack flow overview after initial access to Impact of ransomware
GROUP-IB
C2 Connection
Lateral movement via RDP
Threat actor
Failover Server
Active Directory server
Network discovery and domain user enumeration. PsExec utility is downloaded
Lateral movement via RDP
Lateral movement via RDP
Lateral movement via RDP
Lateral movement via RDP
Backup Server
File Server
• xp_cmdshell enabled, and VeeamBkp account created.
• Windows Defender is disabled
• Conducted credential harvesting
• Network discovery and credential harvesting.
• Execution attempt to exploit CVE-2023-27532.
All Servers (including backup server, File server and Failover server)
Execution of Defender Control, Estate Ransomware, and PsExec utility
Workstations
Execution of Defender Control, Estate Ransomware, and PsExec utility

## INDICATORS OF COMPROMISE (IOCS)

### Executable files:

- DC.exe: CB704D2E8DF80FD3500A5B817966DC262D80DDB8
- DC.ini: 2C56E9BEEA9F0801E0110A7DC5549B4FA0661362
- Svchost.exe: 5E460A517F0579B831B09EC99EF158AC0DD3D4FA
- LB3.exe: 107EC3A7ED7AD908774AD18E3E03D4B999D4690C
- netscan.exe
- veeam-creds-main
- CVE-2023-27532.exe
- VeeamHax
- BulletsPassView64.exe
- netpass64.exe
- PasswordFox64.exe
- ChromePass.exe
- WirelessKeyView64.exe
- mspass.exe
- VNCPassView.exe
- WebBrowserPassView.exe
- mailpv.exe
- RouterPassView.exe
- PstPassword.exe
- OperaPassView.exe
- Dialupass.exe
- BulletsPassView64.exe
- ExtPassword.exe
- pspv.exe
- iepv.exe
- SniffPass64.exe • rdpv.exe

### IPv4:

- 149.28.106[.]252
- 149.28.99[.]61
- 45.76.232[.]205
- 77.238.245[.]11:30001

## RECOMMENDATIONS

- Regularly update and patch all software, especially public-facing applications and critical systems.
- Implement multi-factor authentication (MFA) for all remote access points to prevent unauthorized access.
- Regularly review and disable dormant or unused accounts to minimize potential entry points.
- Segment networks to limit lateral movement and isolate critical systems from general user access.
- Implement application control on hosts to prevent execution of unauthorized programs.
- Deploy endpoint detection and response (EDR) solutions to monitor and respond to malicious activities in real-time.
- Maintain regular, secure backups and test restoration processes to ensure data recovery.
- Implement strict access controls and least privilege principles to limit access to critical systems.
- Use intrusion detection systems (IDS) to monitor network traffic for signs of intrusion and unauthorized activity.
- Conduct regular security awareness training for employees to recognize phishing attempts and other social engineering attacks.
- Turn off unnecessary services, ports, and protocols to reduce attack surfaces.
- Continuously monitor and audit network activity for suspicious behavior and signs of compromise.
- Implement advanced defensive measures, such as deception technologies, to detect and mislead attackers.
- Ensure network edge devices are securely configured and regularly updated.
- Restrict the use of built-in administrative tools and monitor their usage to detect living-off-the-land (LotL) techniques.

## REFERENCES

- https://thehackernews.com/2024/07/new-ransomware-group-exploiting-veeam.html
- https://www.group-ib.com/blog/estate-ransomware/
- https://nvd.nist.gov/vuln/detail/cve-2023-27532
- https://www.veeam.com/kb4424