Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Cuba Ransomware Targets U.S. with Veeam Exploit

Date of Publication	Admiralty Code	TA Number
August 21, 2023	A1	TA2023338

Summary

Attack Began: June 2023
Malware: Cuba ransomware (aka Fidel, COLDDRAW), BUGHATCH, and BURNTCIGAR
Attack Region: Bolivia, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Nicaragua, Panama, Paraguay, Puerto Rico, Uruguay, USA
Targeted Industry: Critical Infrastructure and IT.

Attack: The Cuba ransomware has targeted attacks on critical infrastructure organizations in the United States and IT enterprises across Latin America. In order to acquire credentials, it employs a blend of old and contemporary tools and leverages CVE-2023-27532 to extract credentials.

Attack Regions

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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-27532	Veeam Missing Authentication for Critical Function	Veeam Backup & Replication & Veeam Cloud Connect	✗	✗	✓
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	✗	✓	✓

Attack Details

#1

The Cuba ransomware has targeted attacks against critical infrastructure organizations in the United States and IT firms in Latin America. These attacks employ a combination of both outdated and modern tools, incorporating distinctive resources like BUGHATCH, a specialized downloader, and BURNTCIGAR an anti-malware utility. Moreover, the attackers have harnessed established frameworks like Metasploit and Cobalt Strike, in conjunction with a variety of Living-off-the-Land Binaries (LOLBINS).

#2

Emerging on the threat landscape in 2019, the Cuba ransomware, (aka COLDDRAW or Fidel) has garnered attention. In its latest campaign, this ransomware variant has capitalized on the vulnerability CVE-2023-27532 to retrieve credentials from configuration files. This weakness focuses on Veeam Backup & Replication (VBR) products, an exploit that had been previously utilized by the Russian threat group **FIN7**.

#3

The Cuba ransomware gains initial access through compromised administrative credentials via Remote Desktop Protocol (RDP), avoiding the need for brute force methods. The attack starts with BUGHATCH, a custom downloader exclusively linked to the Cuba ransomware group. This tool establishes a connection to a command-and-control (C2) server, fetching a payload, usually small PE files or PowerShell scripts. The Metasploit DNS stager is then employed to establish a foothold within the target environment, executing shellcode directly in memory.

#4

Cuba ransomware uses the Bring Your Own Vulnerable Driver (BYOVD) technique to bypass endpoint protection tools. The 'BurntCigar' tool terminates kernel processes tied to security products. Alongside the recent Veeam vulnerability, Cuba exploits CVE-2020-1472 Zerologon—a flaw in Microsoft's NetLogon protocol, enabling privilege escalation against Active Directory (AD) domain controllers. Further, the Cuba ransomware maintains a ".onion" webpage within the dark web, accessible only via the TOR network. The driving force behind the Cuba ransomware exhibits motivations rooted in financial gain.

Recommendations

Ensure that operating systems and software are up to date. Implement a security approach based on the principle of least privilege, which involves limiting unnecessary access to administrative shares and other services.

Employing segmented networks and monitoring the network activities for anomalous behavior. Strengthening all endpoints, encompassing employee workstations and servers, involves adjusting permissions, and eliminating unnecessary services. This proactive approach diminishes the susceptibility to attacks reminiscent of the 'living off the land' (LOTL) technique.

Establish regular backups for all assets to guarantee their comprehensive security. Employ the 3-2-1-1 backup framework and utilize specialized tools to enhance backup durability and accessibility.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control
T1133 External Remote Services	T1078.003 Local Accounts	T1106 Native API	T1204.002 Malicious File
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1569.002 Service Execution	T1218.011 Rundll32
T1211 Exploitation for Defense Evasion	T1548.002 Bypass User Account Control	T1140 Deobfuscate/Decode Files or Information	T1562.001 Disable or Modify Tools
T1036.005 Match Legitimate Name or Location	T1543.003 Windows Service	T1068 Exploitation for Privilege Escalation	T1124 System Time Discovery
T1135 Network Share Discovery	T1018 Remote System Discovery	T1083 File and Directory Discovery	T1057 Process Discovery
T1570 Lateral Tool Transfer	T1212 Exploitation for Credential Access	T1090.003 Multi-hop Proxy	T1105 Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	58ba30052d249805caae0107a0e2a5a3cb85f3000ba5479fafb7767e2a5a78f3, 3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0, cf87a44c575d391df668123b05c207eef04b91e54300d1cbbec2f48f5209d4a4, 765d84ae85561bf5dbc1187da2b2cef91da9f222bcc6cf2c12cacd36e44bcffd, 1c2d7f19f8c12e055e1ba8cdf5334e6cb5510847783fbe36121a35ad70f09eb3, 9b1b15a3aacb0e786a608726c3abfc94968915cedcbd239ddf903c4a54bfcf0c, 4b5229b3250c8c08b98cb710d6c056144271de099a57ae09f5d2097fc41bd4f1, 075de997497262a9d105afeadaaefc6348b25ce0e0126505c24aa9396c251e85, Bd93d88cb70f1e33ff83de4d084bb2b247d0b2a9cec61ae45745f2da85ca82d2

Patch Links

https://www.veeam.com/kb4424

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

References

https://blogs.blackberry.com/en/2023/08/cuba-ransomware-deploys-new-tools-targets-critical-infrastructure-sector-in-the-usa-and-it-integrator-in-latin-america

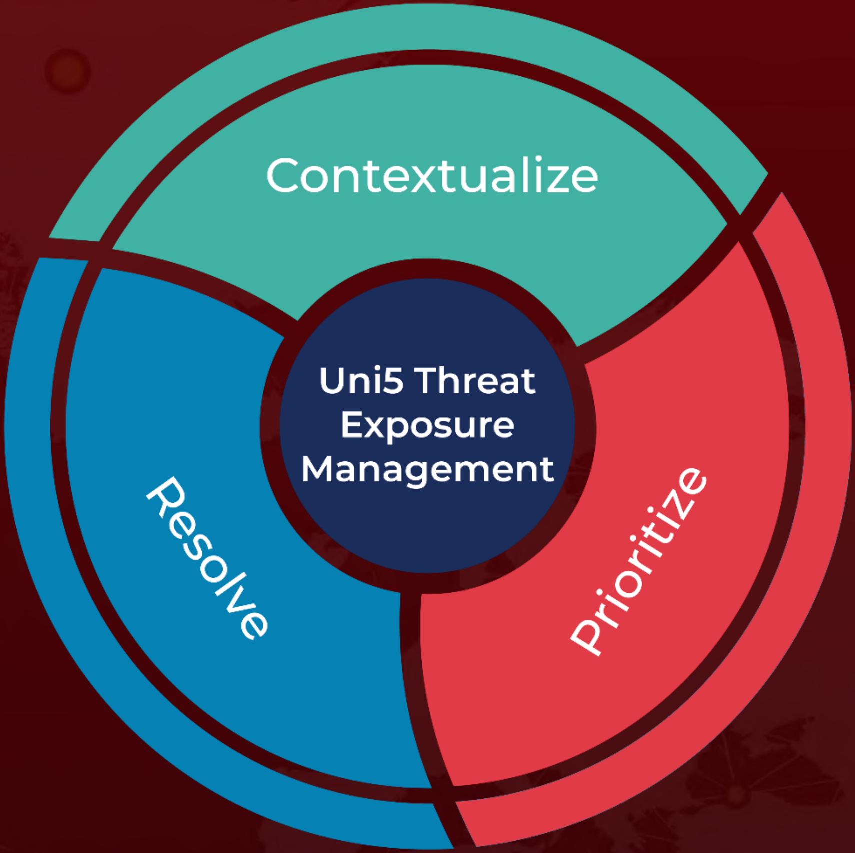
https://www.hivepro.com/zero-day-vulnerability-leveraged-to-deploy-cuba-ransomware/

https://www.hivepro.com/fin7-affiliated-hackers-exploit-flaws-in-veeam-backup-servers/

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 21, 2023 • 7:00 AM

More at www.hivepro.com