Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

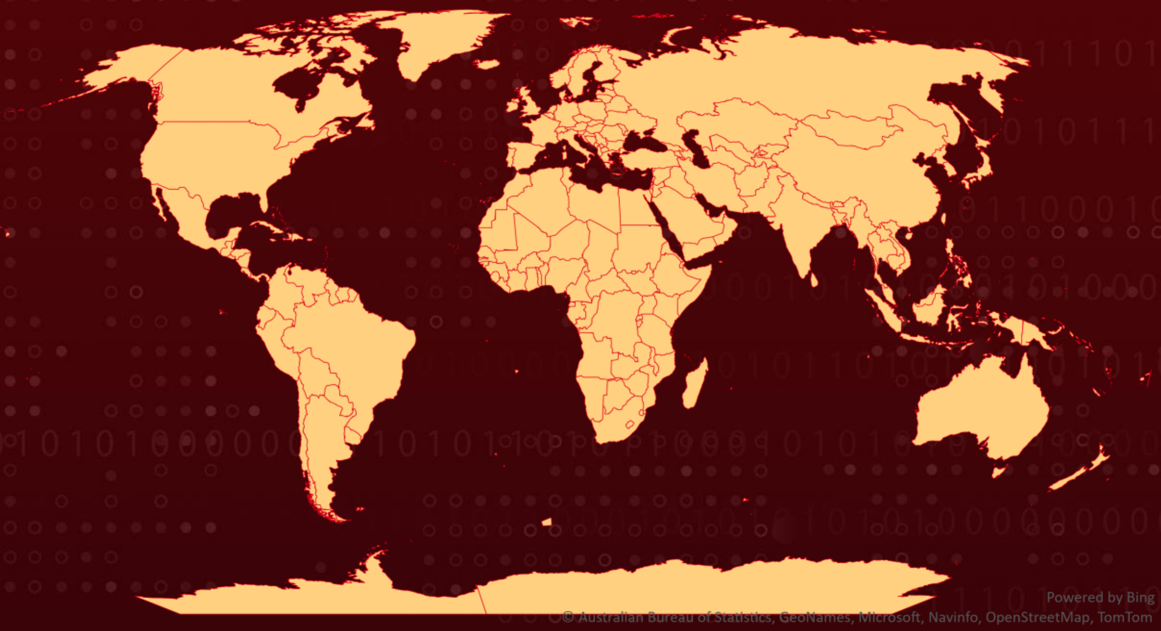
CACTUS Ransomware Emerges as New Threat Targeting Large Enterprises

Date of Publication	Admiralty Code	TA Number
May 12, 2023	A1	TA2023225

Summary

Attack began: March 2023
Attack Regions: Worldwide
Malware: CACTUS Ransomware
Attack: CACTUS is a new strain of ransomware that targets large commercial entities, gains initial access to networks through VPN vulnerabilities, creates new user accounts, exfiltrates sensitive data, and communicates with victims through Tox, using a variety of tools and tactics to distribute the ransomware binary and maintain persistence within the environment, while attempting to obtain credentials and escalate privileges through lateral movement.

Attack Regions


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

Attack Details

#1

CACTUS is a new type of ransomware that has been discovered recently. It targets large commercial entities since March 2023 and gains initial access to networks by exploiting documented vulnerabilities in VPN appliances. Once inside the network, the ransomware actors create new user accounts and deploy the ransomware encryptor via scheduled tasks. The ransomware encryptor requires a key to decrypt the binary for execution, which is provided within a file named ntuser.dat. The actors behind CACTUS ransomware also exfiltrate sensitive data and communicate with victims through the peer-to-peer messaging service called Tox.

#2

The ransom note filename is cAcTuS.readme.txt, and encrypted files have an extension of .cts1, although the number at the end of the extension may vary. CACTUS ransomware uses various tactics, techniques, and procedures (TTPs), including the use of tools such as Chisel, Rclone, TotalExec, Scheduled Tasks, and custom scripts to distribute the ransomware binary. The initial exploit used by CACTUS is via the exploitation of vulnerable VPN appliances. CACTUS uses legitimate remote access tools like Splashtop, AnyDesk, and SuperOps RMM, along with Cobalt Strike and the use of Chisel, a SOCKS5 proxy tool, to maintain persistence within the environment.

#3

The ransomware actors attempt to obtain credentials from user web browsers and search for files containing passwords for escalation. They use valid or created accounts, RDP, and remote management tools such as SuperOps to move laterally within the environment. They also exfiltrate sensitive data to increase the pressure of extortion and use common exfiltration tools such as Rclone to automatically extract files to cloud storage. CACTUS utilizes a script called TotalExec.ps1, which automates the deployment of the encryptor and is often used by another ransomware called BLACKBASTA.

Recommendations

Patch and update VPN Devices: The CACTUS ransomware has been observed exploiting known vulnerabilities in VPN appliances to gain initial access to networks. It is critical for organizations to regularly patch and update their VPN devices to prevent such exploits. Timely installation of security patches is a crucial aspect of ensuring that the organization is protected from the latest threats.

Implement Password Managers and Monitor PowerShell Execution: The CACTUS ransomware has been observed extracting credentials from web browsers to gain further access to the network. Therefore, implementing password managers can help to mitigate the risks of password theft. Additionally, monitoring PowerShell execution and ensuring PowerShell is logged can help detect and prevent the execution of malicious scripts. Creating detections for encoded script execution can also help identify attempts by the threat actor to obfuscate their actions.

Audit User, Administrator and Service Accounts and Implement Multi-factor Authentication: The CACTUS ransomware has been observed using highly privileged accounts to escalate privileges and move laterally within the network. Therefore, it is important to audit user, administrator, and service accounts to ensure that they have the appropriate level of access and privileges. Implementing the principle of least privilege can help reduce the risk of unauthorized access. Additionally, implementing multi-factor authentication can help prevent lateral movement and restrict access to sensitive areas of the network.

Review Backup Strategies: The CACTUS ransomware is designed to encrypt files and demand payment in exchange for a decryption key. Therefore, it is important to ensure that an organization's backup strategy is effective and that backups are taken regularly. At least one backup should be isolated from the network to prevent it from being encrypted by the ransomware. Having a solid backup strategy can help organizations quickly recover from a ransomware attack without having to pay the ransom.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0040 Impact	T1190 Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1072 Software Deployment Tools
T1136 Create Account	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1003 OS Credential Dumping
T1049 System Network Connections Discovery	T1087 Account Discovery	T1087.002 Domain Account	T1018 Remote System Discovery
T1021 Remote Services	T1021.001 Remote Desktop Protocol	T1570 Lateral Tool Transfer	T1119 Automated Collection
T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage	T1219 Remote Access Software	T1090 Proxy
T1486 Data Encrypted for Impact			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	163[.]123[.]142[.]213

TYPE	VALUE
MD5	d9f15227fefb98ba69d98542fbe7e568 3adc612b769a2b1d08b50b1fb5783bcf be7b13aee7b510b052d023dd936dc32f 26f3a62d205004fbc9c76330c1c71536 d5e5980feb1906d85fbd2a5f2165baf7 78aea93137be5f10e9281dd578a3ba73

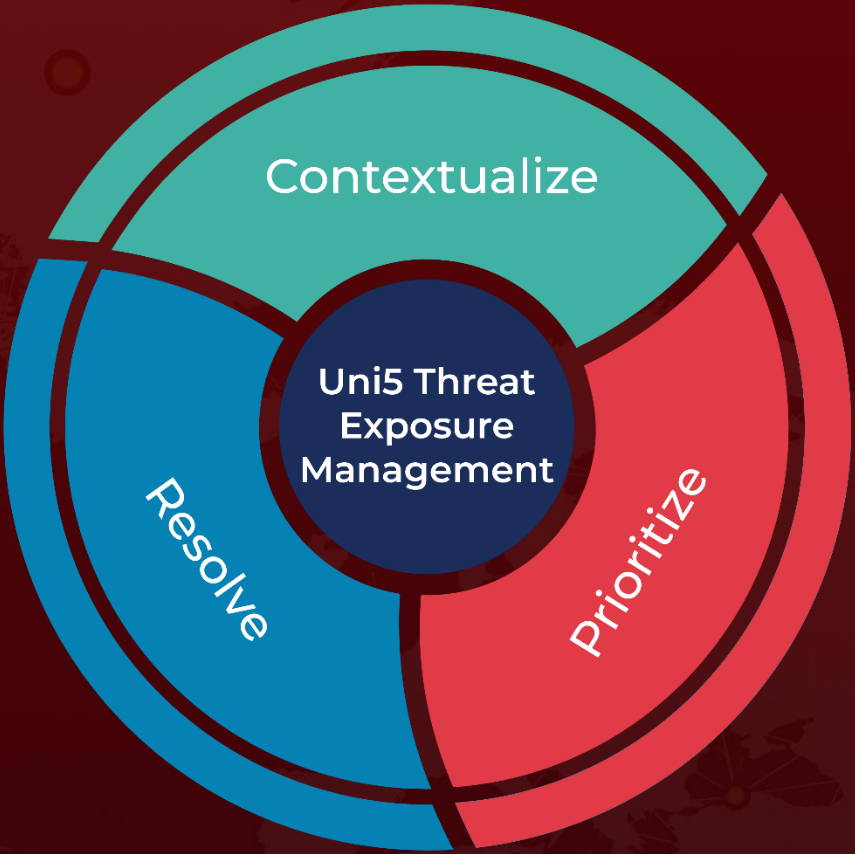
References

https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection

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

May 12, 2023 • 2:00 AM

More at www.hivepro.com