KPMG Cyber Threat Intelligence Platform

CACTUS Ransomware – Concealed Binary Wrecking Havoc

The CACTUS ransomware has emerged as a significant cybersecurity threat since March 2023. This new strain of ransomware capitalizes on known vulnerabilities of VPN to breach targeted networks, employing UPX packing and self encryption to avoid detection. The utilization of double extortion tactics intensifies the risk landscape for organizations, posing an additional layer of threat. Particularly, large commercial organizations are the primary targets of this ransomware.

CACTUS exploits known vulnerabilities in VPN appliances to gain initial access. It deploys an SSH backdoor to connect to C2 & sets persistence for the same via scheduled tasks. It conducts network recon through scanner tools and uses PowerShell to gather endpoint information, identify user accounts, and save the data locally. It leverages remote access tools for persistence and deploys proxy tool like Chisel for C2 traffic tunneling and script transfer. The malware dumps credentials from browsers & LSASS for privilege escalation & lateral movement. Also, local admin accounts are added via batch script and antivirus software is uninstalled. Data exfiltration is achieved through Rclone, a cloud storage tool. Post exfiltration, the 'TotalExec.ps1 ' script automates the deployment of an encryptor, setting autorun, extracting compressed ransomware binary & executing it remotely using PsExec. It's encryptor binary supports arguments such as '-s' to set persistence and writing encoded configuration; '-r' to read configuration from 'ntuser.dat' file and spawning; '-i' to proceed to encryption. Cactus utilizes multi-threaded encryption with a '.cts\d' file extension.

CACTUS ransomware exploits the vulnerability and utilizes self-encryption technique to beat security checks that poses significant risk. To prevent this, it is crucial to always update the patches and monitor the network for data exfiltration tasks.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

CACTUS Ransomware – Concealed Binary Wrecking Havoc

Indicators of Compromise: IP Addresses	
104.86.182[.]8	23.216.147[.]76
20.99.184[.]37	163.123.142[.]213
23.216.147[.]64	

Indicators of Compromise: Domains
progetecloud[.]online

Indicators of Compromise: Hashes
d9f15227fefb98ba69d98542fbe7e568
3adc612b769a2b1d08b50b1fb5783bcf
be7b13aee7b510b052d023dd936dc32f
26f3a62d205004fbc9c76330c1c71536
d5e5980feb1906d85fbd2a5f2165baf7
78aea93137be5f10e9281dd578a3ba73
5737cb3a9a6d22e957cf747986eeb1b3
e28db6a65da2ebcf304873c9a5ed086d
949d9523269604db26065f002feef9ae
eba1596272ff695a1219b1380468293a
1add9766eb649496bc2fa516902a5965
2611833c12aa97d3b14d2ed541df06b2
de6ce47e28337d28b6d29ff61980b2e9
4baf3066aec9851b1acb05cecc093562
45ebcb76574ba953a69ccb2bb92f5aea
2d1e815c8486f9123276cc942638fc73
a892940cdc8d3bbc58a8a0fb814b7c9e
7ce6d2015647765528fa314c0e349d42
f63627cd5490822768a105c67cd410b5
6462b5463a50154b5a7c3b89d6b6db76
de8e875dbba6089a6a1d0944c5f4fea6
97dcabd4a3ca1a2d8f1f0dbdb0bd7721
c1bcacf47e8739936b40547c9a184d1e
bca9143bf5e45cb88f90dd44dc3bb63b

KPMG

KPMG Cyber Threat Intelligence Platform

CACTUS Ransomware – Concealed Binary Wrecking Havoc

Indicators of Compromise: Hashes
d41d8cd98f00b204e9800998ecf8427e
daf1853a8f44f3a1c7ff93325c822c57
c0ba7bc46af92c6c76af76a3df5f46a1
889c2b60da0d185980147695bd94df5a
aacd397ed77c6eb124a962279a4f24a9
c9a3d53476fc8955db591270dc4280d0
8528ec904911fa809f0bd0661b78d57f
323d6765a3119658be056731627ff02c
248795453ceb95e39db633285651f7204813ea3a
6715b888a280d54de9a8482e40444087fd4d5fe8
63d13dac006666bdc298ba5b1e8bcd23a331cf12
11a93a6c270d6d189fa857f03a001b347a679654
cb570234349507a204c558fc8c4ecf713e2c0ac3
3b8ae803f281ab7fc93577b79562bd7819e068bd
00086dd2271c0de3d1ec5bb70fada4d84bf522e0
48d1971ec7b17adaa8189089a97503afa705ae14
c9f3de8b5457c040d507a4abd4d6439766d3a0a0
173f9b0db97097676a028b4b877630adc7281d2f
5b70972c72bf8af098350f8a53ec830ddbd5c2c7809c71649c93f32a8a3f1371
b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b
ebce70ec427279c0717b899bdba48ced38c4a70933035c6b936d89e00d1cfe16
9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a
78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17
d7429c7ecea552403d8e9b420578f954f5bf5407996afaa36db723a0c070c4de
509a533ade43406eb50fa9cb8984b2e10d008ad0ea8c22d0652f3ee101125bb7
0933f23c466188e0a7c6fab661bdb8487cf7028c5cec557efb75fde9879a6af8
69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc
c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd