Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

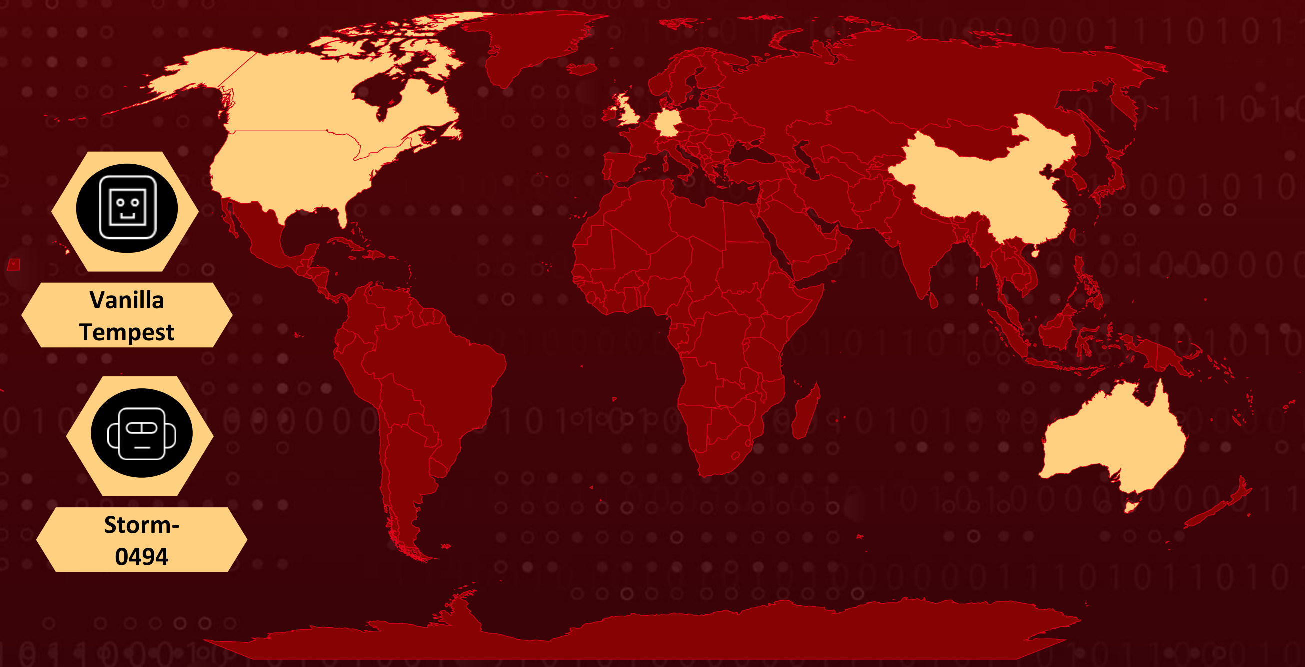
Vanilla Tempest Targets Healthcare with INC Ransomware

Date of Publication	Admiralty Code	TA Number
September 20, 2024	A1	TA2024365

Summary

First Appearance: June 2021
Threat actors: Vanilla Tempest (DEV-0832, Vice Society), Storm-0494
Malware: INC Ransomware, Gootloader, Supper backdoor
Targeted Countries: United States, United Kingdom, Canada, Australia, Germany, China
Targeted Industries: Education, Healthcare, IT, and Manufacturing
Attack: Vanilla Tempest, also known as Vice Society, is a cyber threat actor actively targeting sectors like healthcare and education using INC ransomware. They gain entry via Gootloader malware, deployed by Storm-0494, and use tools like AnyDesk and MEGA for lateral movement and data exfiltration. Their opportunistic attacks highlight ongoing cybersecurity challenges, particularly for healthcare organizations.

Attack Regions



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

Attack Details

#1

Vanilla Tempest is a sophisticated cyber threat actor, is actively targeting U.S. healthcare organizations using a new strain of ransomware called INC. This marks the first time Vanilla Tempest has employed INC ransomware in its attacks, which have been ongoing since at least July 2023. The group is also recognized under the alias Vice Society, DEV-0832 and has been linked to various ransomware families, including BlackCat, Quantum Locker, Zeppelin, and Rhysida.

#2

The group gains entry into networks through the Gootloader malware, which is deployed by another threat actor known as Storm-0494. After gaining access, attackers utilize tools such as the Supper backdoor, along with legitimate software like AnyDesk for remote management and MEGA for data synchronization. The attackers then move laterally within the network using techniques like Remote Desktop Protocol (RDP) and Windows Management Instrumentation (WMI) to deploy the INC ransomware across connected systems.

#3

Vanilla Tempest primarily focuses on sectors such as education, healthcare, IT, and manufacturing. Their recent activities have notably impacted healthcare institutions, including a cyberattack on Regent Care Center hospitals, which disrupted IT systems and forced rescheduling of appointments due to compromised access to patient databases.

#4

Active since at least June 2021, Vanilla Tempest has evolved from its earlier identity as Vice Society. In their attacks, Vanilla Tempest uses custom PowerShell scripts, exploits disclosed vulnerabilities, and employs Windows-native binaries to escalate privileges, exfiltrate data, and eventually deploy ransomware. The group has demonstrated a pattern of opportunistic attacks and is known for leveraging existing ransomware tools rather than developing custom variants. This development highlights ongoing challenges in cybersecurity, particularly within critical sectors like healthcare that are increasingly targeted by financially motivated cybercriminals.

Recommendations

Implement Multi-Factor Authentication (MFA): Strengthen access control by using MFA, especially for Remote Desktop Protocol (RDP) and privileged accounts, to reduce the risk of unauthorized access.

Regular Patching and Vulnerability Management: Apply patches for known vulnerabilities promptly, particularly for software and systems often targeted by threat actors like Vanilla Tempest (e.g., vulnerabilities in Windows binaries).Network Segmentation and Least Privilege: Limit lateral movement by segmenting networks and applying the principle of least privilege, ensuring that users and systems only have access to necessary resources.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a INC ransomware attack, up-to-date backups enable recovery without paying the ransom.

Endpoint Detection and Response (EDR): Deploy advanced threat detection tools to monitor for unusual activity, including the use of legitimate tools like AnyDesk and WMI for malicious purposes.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0042 Resource Development	TA0002 Execution	TA0005 Defense Evasion
TA0003 Persistence	TA0008 Lateral Movement	TA0040 Impact	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1068 Exploitation for Privilege Escalation
T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1047 Windows Management Instrumentation	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced, b939ec9447140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988, c853d91501111a873a027bd3b9b4dab9dd940e89fcfec51efbb6f0db0ba6687b
MD5	0b175136f48d88e094318cc78792b876, 032bf67c14d00b5468ce0aeab927c86c, 7ca12616c3e964dcf3dccb30f8ee6a18, F176d8ee8c58223c3a1ca5b1dff274b8, c1cd52785f2ca5ef177e259c7ae3596f

Recent Breaches

https://www.nusser-mineraloel.de

https://erokodistributors.com

https://onepointpatientcare.com

https://e-zpack.com

https://regentcarecenter.com

https://erokodistributors.com

https://dontwastegroup.com

https://hl-lawsonandsons.com

References

https://x.com/MsftSecIntel/status/1836456406276342215

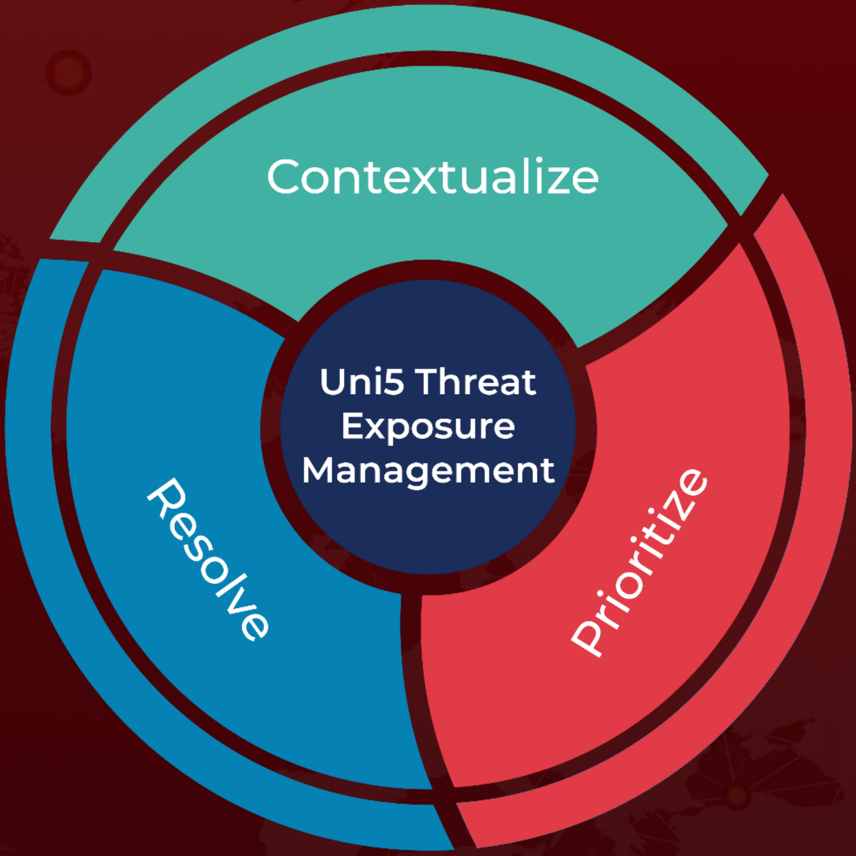
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/

https://hivepro.com/threat-advisory/vice-society-gang-switches-to-new-custom-ransomware/

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

September 20, 2024 • 6:30 AM

More at www.hivepro.com