Rewterz Threat Alert – Leaked Conti Ransomware Used to Target Russia – Active IOCs

rewterz.com/rewterz-news/rewterz-threat-alert-leaked-conti-ransomware-used-to-target-russia-active-iocs

April 11, 2022

- Solutions

- Resources

Resources

January 7, 2024

January 7, 2024

Rewterz Threat Advisory – CVE-2023-6690 – GitHub Enterprise Server Vulnerability

Severity Low Analysis Summary CVE-2023-6690 GitHub Enterprise Server could allow a remote authenticated attacker to gain elevated privileges on the system, caused by a race condition. […]

January 7, 2024

January 7, 2024

Rewterz Threat Advisory – CVE-2023-51441 – Apache Axis Vulnerability

Severity High Analysis Summary CVE-2023-51441 Apache Axis is vulnerable to server-side request forgery, caused by a improper input validation by the service admin HTTP API. By […]

January 6, 2024

January 6, 2024

Rewterz Threat Update – 4.5 Million Patients Impacted Due to Healthcare Tech Company Data Breach

Severity High Analysis Summary A health management solutions provider, HealthEC LLC, recently suffered a data breach that has impacted almost 4.5 million patients who received healthcare […]

Get in Touch

- Solutions

- Resources

Resources

January 7, 2024

January 7, 2024

Rewterz Threat Advisory – CVE-2023-6690 – GitHub Enterprise Server Vulnerability

Severity Low Analysis Summary CVE-2023-6690 GitHub Enterprise Server could allow a remote authenticated attacker to gain elevated privileges on the system, caused by a race condition. […]

January 7, 2024

January 7, 2024

Rewterz Threat Advisory – CVE-2023-51441 – Apache Axis Vulnerability

Severity High Analysis Summary CVE-2023-51441 Apache Axis is vulnerable to server-side request forgery, caused by a improper input validation by the service admin HTTP API. By […]

January 6, 2024

January 6, 2024

Rewterz Threat Update – 4.5 Million Patients Impacted Due to Healthcare Tech Company Data Breach

Severity High Analysis Summary A health management solutions provider, HealthEC LLC, recently suffered a data breach that has impacted almost 4.5 million patients who received healthcare […]

Get in Touch

Rewterz Threat Advisory – Multiple IBM Vulnerabilities

April 11, 2022

Rewterz Threat Alert – Lazarus APT Group – Active IOCs

April 11, 2022

Rewterz Threat Advisory – Multiple IBM Vulnerabilities

April 11, 2022

Rewterz Threat Alert – Lazarus APT Group – Active IOCs

April 11, 2022

Severity

High

Analysis Summary

Conti ransomware was discovered in December 2019 and is delivered via TrickBot. It's been utilized against large companies and government institutions across the world, especially in North America. Conti steals important files and information from targeted networks and threatens to disseminate it unless the ransom is paid. Conti ransomware enhances performance by utilizing "up to 32 simultaneous encryption operations," and is very likely directly controlled by its controllers. This ransomware can target network-based resources while ignoring local files. This feature has the noticeable impact of being able to create targeted harm in an environment in a way that might hinder incident response actions.

During the Russian-Ukrainian cyber warfare, threat groups and hacktivists have taken sides in support of either party. Russian originator Conti announced their support for Russia, but shortly after their data was breached and code for the ransomware was leaked. Similarly, NB65 group took Ukraine's side and retaliated with attacks on VGTRK and the Russian Space Agency 'Roscosmos'.

The group has created a unique ransomware from the leaked conti code and changed the ransomware note, added **.**NB65 extension to the encrypted file's names, and the encryption process was also modified to change the decryptor.

Impact

- Sensitive File Theft
- File Encryption

Indicators of Compromise

Domain Name

- thulleultinn[.]club
- vaclicinni[.]xyz
- tapavi[.]com
- oxythuler[.]cyou
- dictorecovery[.]cyou
- contirecovery[.]best

IP

- 83[.]97[.]20[.]160
- 82[.]118[.]21[.]1
- 68[.]183[.]20[.]194
- 23[.]82[.]140[.]137

Remediation

- Block the threat indicators at their respective controls.
- Search for IOCs in your environment.