Rewterz Threat Alert – KONNI APT Group – Active IOCs

rewterz.com/rewterz-news/rewterz-threat-alert-konni-apt-group-active-iocs-11

October 4, 2022

- Solutions

- Resources

Resources

February 15, 2024

February 15, 2024

Rewterz Threat Advisory – Multiple Adobe Acrobat and Adobe Reader Vulnerabilities

Severity High Analysis Summary CVE-2024-20726, CVE-2024-20727 Adobe Acrobat and Adobe Reader could allow a remote attacker to execute arbitrary code on the system, caused by an […]

February 15, 2024

February 15, 2024

Rewterz Threat Advisory – ICS: Multiple Siemens Products Vulnerabilities

Severity High Analysis Summary CVE-2024-23813 CVSS: 7.3 Siemens Polarion ALM could allow a remote attacker to bypass security restrictions, caused by improper authentication in the REST […]

February 15, 2024

February 15, 2024

Rewterz Threat Advisory – Multiple Dell PowerProtect Data Manager Vulnerabilities

Severity High Analysis Summary CVE-2024-22454 CVSS: 8.8 Dell PowerProtect Data Manager could allow a remote attacker to gain elevated privileges on the system, caused by the […]

Get in Touch

- Solutions

- Resources

Resources

February 15, 2024

February 15, 2024

Rewterz Threat Advisory – Multiple Adobe Acrobat and Adobe Reader Vulnerabilities

Severity High Analysis Summary CVE-2024-20726, CVE-2024-20727 Adobe Acrobat and Adobe Reader could allow a remote attacker to execute arbitrary code on the system, caused by an […]

February 15, 2024

February 15, 2024

Rewterz Threat Advisory – ICS: Multiple Siemens Products Vulnerabilities

Severity High Analysis Summary CVE-2024-23813 CVSS: 7.3 Siemens Polarion ALM could allow a remote attacker to bypass security restrictions, caused by improper authentication in the REST […]

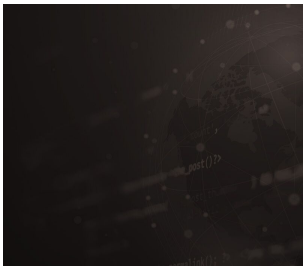
February 15, 2024

February 15, 2024

Rewterz Threat Advisory – Multiple Dell PowerProtect Data Manager Vulnerabilities

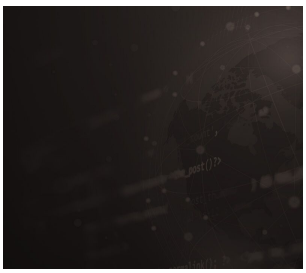
Severity High Analysis Summary CVE-2024-22454 CVSS: 8.8 Dell PowerProtect Data Manager could allow a remote attacker to gain elevated privileges on the system, caused by the […]

Get in Touch



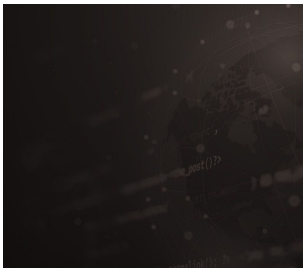
Rewterz Threat Alert – Kimsuky APT Group – Active IOCs

October 4, 2022



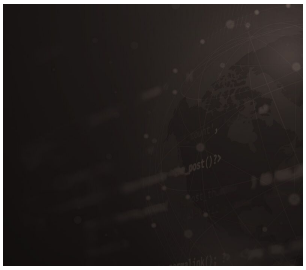
Rewterz Threat Advisory – CVE-2022-39266 – Node.js isolated-vm module Vulnerability

October 4, 2022



Rewterz Threat Alert – Kimsuky APT Group – Active IOCs

October 4, 2022



Rewterz Threat Advisory – CVE-2022-39266 – Node.js isolated-vm module Vulnerability

October 4, 2022

Severity

High

Analysis Summary

KONNI is a remote access tool that North Korean cyber attackers have been using since at least 2014. The North Korean hacker group distributes Konni RAT via phishing messages or emails. The infection chain begins when the victim accesses a weaponized file. Adversaries employ Konni RAT to gather information from victims, capture screenshots, steal files, and build a remote interactive shell. KONNI has been linked to various alleged North Korean attacks targeting political groups in Russia, East Asia, Europe, and the Middle East. KONNI shares a significant code overlap with the NOKKI malware family. Konni's APT Group continues to attack malicious documents written in Russian. This threat actor group conducts attacks with Russian-North Korean trade and economic investment documents.

This APT group was detected targeting the Russian diplomatic sector in January 2022, employing a spear phishing theme for New Year's Eve festivities as a bait. When the malicious email attachment is opened and processed, a series of events occur, allowing the actor to install an implant from the Konni RAT family as the final payload.

The latest campaign includes filename:보상명부.xlam

Impact

Information Theft and Espionage

Indicators of Compromise

IP

92[.]38[.]160[.]152

MD5

d306925713baf2d7410e26deb7f157bc

SHA-256

593811e53cfa8aa655fc5bbf5e27c76e372e7d715b5b4e0e3f36f947d66a70f6

SHA-1

f0f00aed4052bbbe4eb4d1f990dccb2986ea169c

URL

http[:]//rq7592[.]c1[.]biz/dn[.]php?name=065367&prefix=cc%20(0)

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.
- Always be suspicious about emails sent by unknown senders.
- Never click on the link/attachments sent by unknown senders.