Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Rhysida Ransomware's Decryptor is Now in Action

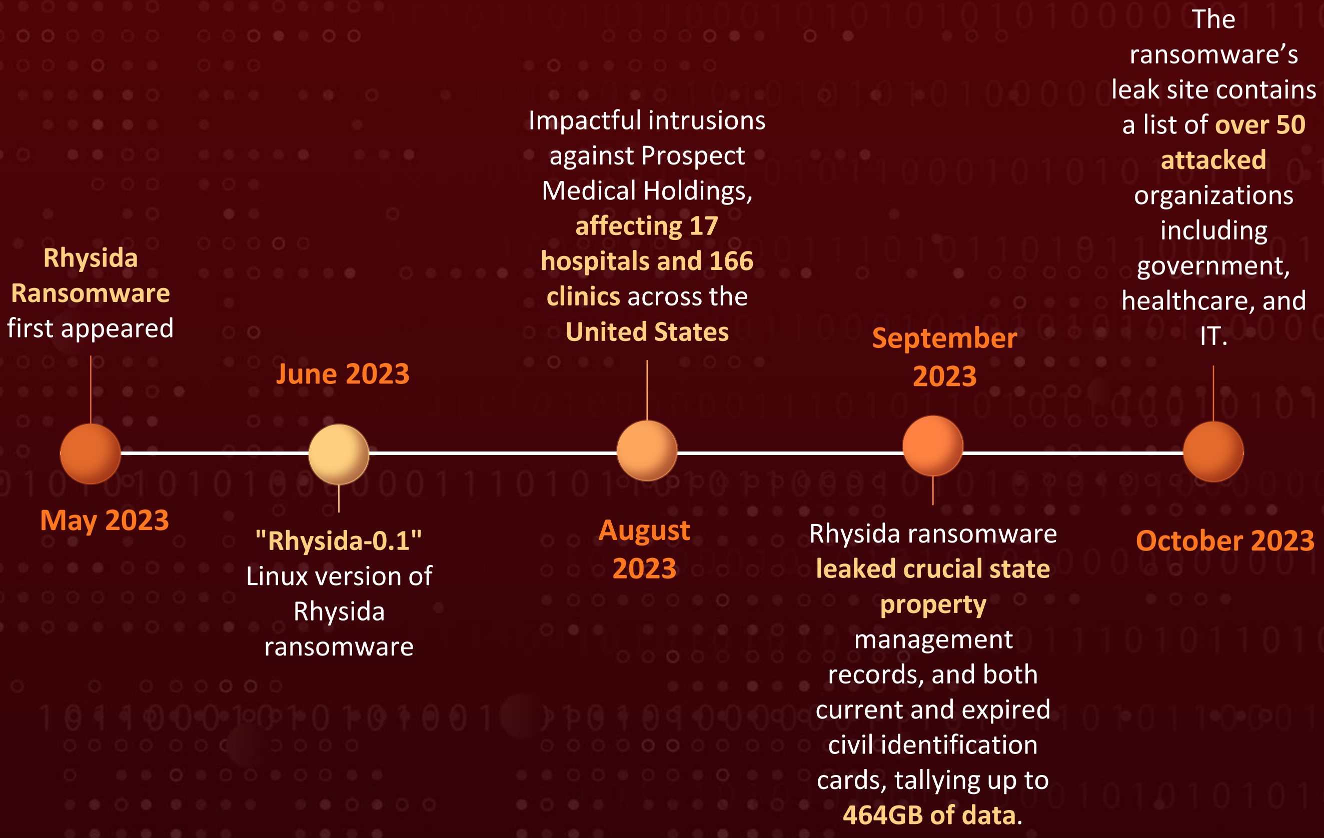
Date of Publication	Admiralty Code	TA Number
February 14, 2024	A1	TA2024058

Summary

First Seen: May 17, 2023
Malware: Rhysida Ransomware
Attack Region: Germany, Spain, United States, Malaysia, United Kingdom, Belgium, Slovenia, Thailand, Israel, Italy, Australia, Peru, Brazil, Dominican Republic, Jordan, Kuwait, Qatar, Lithuania, South Africa, Portugal, Switzerland, Denmark, China
Targeted Industries: Internet Software and services, Utilities, Financial Services, Renewable Electricity, Education, Consumer Services, Health Care Providers and services, Energy, Industrial Conglomerates, Real Estate, Government, Media, IT Services, Construction, Engineering

Attack: The Rhysida ransomware-as-a-service (RaaS) group poses a significant global threat, targeting diverse sectors. Recently, an implementation vulnerability in the source code of the Rhysida ransomware has been discovered. By exploiting this vulnerability to reconstruct encryption keys, it enables the development of a decryptor. This decryptor allows victims of the Rhysida ransomware to recover their encrypted data without any cost.

Attack Timeline



May 2023

Rhysida Ransomware first appeared

June 2023

"Rhysida-0.1" Linux version of Rhysida ransomware

August 2023

Impactful intrusions against Prospect Medical Holdings, **affecting 17 hospitals and 166 clinics** across the **United States**

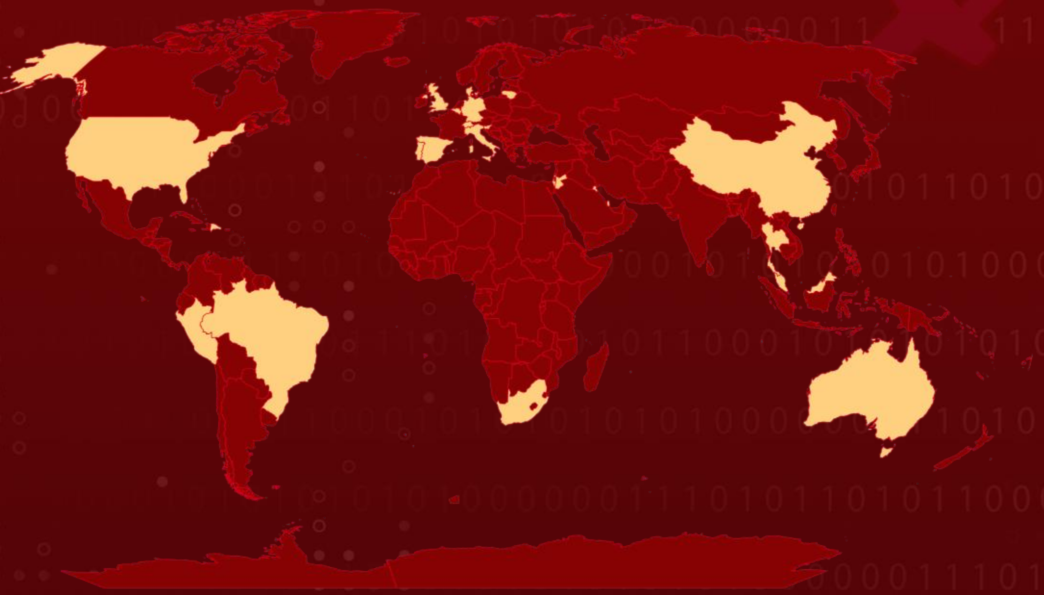
September 2023

Rhysida ransomware **leaked crucial state property** management records, and both current and expired civil identification cards, tallying up to **464GB of data**.

October 2023

The ransomware's leak site contains a list of **over 50 attacked** organizations including government, healthcare, and IT.

Attack Regions



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

Attack Details

#1 The Rhysida ransomware-as-a-service (RaaS) group emerged in May 2023, introducing a victim assistance chat platform accessible through the TOR network (.onion). Rhysida utilizes various channels for dissemination, employing notable strategies like distribution via Cobalt Strike or similar frameworks and executing meticulously orchestrated phishing campaigns.

#2 Additionally, Rhysida actors have been observed utilizing external-facing remote services to gain initial access and establish persistence within a targeted network. Since its inception, the group has documented over 80 victims globally on its website. Rhysida ransomware primarily targets sectors such as education, healthcare, manufacturing, information technology, and government. Victims of Rhysida incursions are distributed across major geopolitical regions, indicating a lack of focus on any specific country.

#3 Rhysida employs a 4096-bit RSA key with the ChaCha20 algorithm for encryption. This encryption's primary function is to initiate the overall runtime of the ransomware, including specific encryption parameters. The ransom demand appears as a "distinctive key," meticulously crafted to restore encrypted files, requiring payment from the victim.

#4 An implementation vulnerability in the ransomware's encryption scheme, specifically in the random number generator (CSPRNG), facilitates the generation of a unique private encryption key in each attack. Exploiting this flaw allows for the recovery of the internal state of the CSPRNG during the attack, enabling the creation of a valid key to reverse the data encryption.

#5 Rhysida's strategic use of intermittent encryption, selectively encrypting portions of files while leaving others in plaintext, plays a crucial role in shaping the decryption method. Although an automated decryption tool is available, it is important to note that this decryptor exclusively works for files encrypted by the Rhysida Windows encryptor and does not apply to files encrypted on VMware ESXi or through its PowerShell-based encryptor.

Recommendations

Understand Limitations: Be aware of any limitations associated with the third-party or open-source decryptor. Some decryptors may not support certain file types, operating systems, or versions of the ransomware.

Use in Isolation: Run the decryptor in an isolated environment or on a test system to prevent unintended consequences. This precaution helps minimize the risk of unintentional system changes or interactions with other software.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0040 Impact	T1595 Active Scanning	T1598 Phishing for Information
T1583 Acquire Infrastructure	T1566 Phishing	T1059.003 Windows Command Shell	T1059.001 PowerShell
T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1055 Process Injection	T1070.004 File Deletion
T1070.001 Clear Windows Event Logs	T1083 File and Directory Discovery	T1082 System Information Discovery	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1490 Inhibit System Recovery	T1486 Data Encrypted for Impact	T1491 Defacement

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f, f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab, 1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd, 2c5d3fea7ad3c9c49e9c1a154370229c86c48fbaf7044213fd85d31efcebf7f6, 3d2013c2ba0aa1c0475cab186ddf3d9005133fe5f88b5d8604b46673b96a40d8,

TYPE	VALUE
SHA256	67a78b39e760e3460a135a7e4fa096ab6ce6b013658103890c866d9401928ba5, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1, 258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595, 3518195c256aa940c607f8534c91b5a9cd453c7417810de3cd4d262e2906d24f, d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

Recent Breaches

https://www.traviangames.com
https://www.tcman.com
https://www.mhmhealth.com
https://www.iwk.com.my
https://www.smh.group
https://www.HandelsschoolAalst.be
https://www.hse.si
https://www.bu.ac.th
https://www.hermelin.ort.org.il
https://www.prosperius.it
https://www.mtsm.org
https://www.stedmundscollege.org
https://www.coredesktop.com.au
https://www.cnpc.com.pe
https://www.aspirationtraining.com
https://www.pmh.com
https://www.leespring.com
https://www.grupojosealves.com
https://www.migracion.gob.do
https://www.hse.si
https://www.abdalihospital.com
https://www.mof.gov.kw
https://www.qrec.gov.qa
https://www.doctorbruce.net
https://www.singingriverhealthsystem.com
https://www.aovr.veneto.it
https://www.ktu.edu
https://www.tut.ac.za
https://www.ufms.br
https://www.pierce.ctc.edu
https://www.insomniac.games

https://www.cm-gondomar.pt
https://www.hit.ac.il
https://www.bl.uk
https://www.lutheranworld.org
https://www.kingedwardvii.co.uk
https://www.nccu.edu
https://www.gedi.ceec.net.cn
https://www.comune.fe.it

References

https://arxiv.org/pdf/2402.06440.pdf

https://seed.kisa.or.kr/kisa/Board/166/detailView.do

https://www.hivepro.com/threat-advisory/knocking-the-surface-of-rhysida-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.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

February 14, 2024 • 7:30 PM

More at www.hivepro.com