Hive Pro®

Threat Level

Red

CISA: AA23-319A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

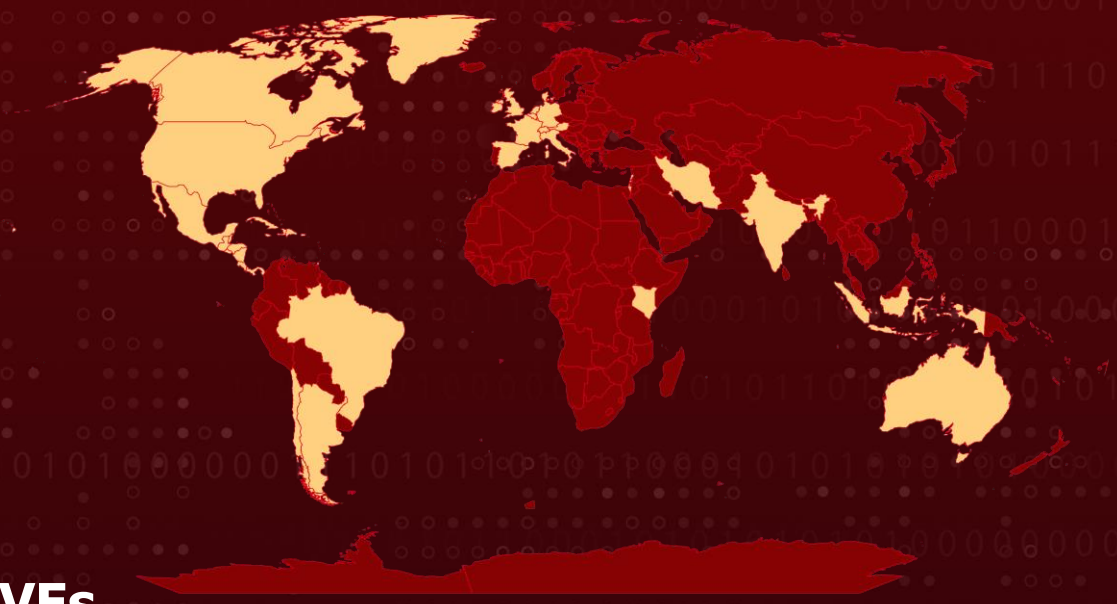
Knocking the Surface of Rhysida Ransomware

Date of Publication	Last Update Date	Admiralty Code	TA Number
August 10, 2023	November 16, 2023	A1	TA2023329

Summary

First Seen: May 17, 2023
Malware: Rhysida Ransomware
Attack Region: Israel, Kuwait, United States, Brazil, Dominican Republic, Australia, Denmark, Italy, Argentina, Indonesia, Mexico, France, Iran, United Kingdom, Spain, Germany, Martinique, Switzerland, Kenya, Austria, Netherlands, Chile, Lebanon, Singapore, India, Western Europe, North and South America
Targeted Sectors: Consumer Services, Healthcare, Education, Government, IT Services, Construction, Engineering, Electrical Equipment, Industrial Conglomerates, Media, Food Products, Transportation, Professional Services, Aerospace, Defense, Manufacturing, Insurance, Banking, Retail, and Technology
Attack: The Rhysida ransomware campaign is rapidly gaining notoriety, driven by a series of successful infiltrations into various sectors. Employing an array of dissemination techniques such as Cobalt Strike, phishing campaigns, and a victim assistance chat platform accessible via TOR.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability (Zerologon)	Microsoft Netlogon	✗	✓	✓

Attack Details

#1

The Rhysida ransomware-as-a-service (RaaS) emerged in May 2023, in parallel with the launch of their victim assistance chat platform, accessible via the TOR network (.onion). Rhysida disseminated via various channels, with notable methods including distribution via Cobalt Strike or similar frameworks, as well as execution through meticulously organized phishing campaigns. Rhysida has been observed exploiting Zerologon, a critical vulnerability that facilitates the elevation of privileges within Microsoft's Netlogon Remote Protocol.

#2

Notably, Rhysida has initiated a series of targeted attacks against healthcare and public health organizations. When initiated, the Rhysida ransomware displays a cmd.exe interface while meticulously searching all data on local discs. Rhysida, who only facilitates transactions in BTC (Bitcoin), offers victims detailed instructions on how to acquire and use BTC via a dedicated victim webpage. Rhysida is a 64-bit Portable Executable (PE) Windows cryptographic ransomware executable that was painstakingly developed using the MINGW/GCC toolchain.

#3

This ransom note deviates from the norm, foregoing the standard blatant ransom ultimatum found in the majority of ransom notes linked with other malware lineages. The Rhysida ransom letter, on the other hand, takes the form of an alert distributed by the Rhysida "cybersecurity team," informing victims of their compromised system status and the subsequent encryption of their information.

#4

The ransom demand takes the form of a "distinctive key," carefully created to restore encrypted files, the acquisition of which involves payment by the victim. Aside from technical resembles such as the deployment of NTDSUtil, the implementation of local firewall regulations to facilitate C2 communications via SystemBC, and the adoption of the PortStarter utility—a tool primarily associated with **Vice Society**—another noteworthy aspect is the correlation between the emergence of Rhysida and a significant decline in Vice Society operations.

#5

The Kuwaiti government fell victim to a targeted Rhysida ransomware attack on its Ministry of Finance. The cyber attack commenced on September 18, 2023, and the hacking group publicized their success on their leaked website on September 25, 2023. The disclosed information includes crucial state property management records, such as agreements for chalet rentals, land rental contracts, and both current and expired civil identification cards, tallying up to 464GB of data. This signifies the successful infiltration of the government organization's intricate systems by the hacking group.

#6 The auction for this stolen data is starting with a substantial initial price of 15BTC, equivalent to approximately $400,000. Notably, the individuals behind the Rhysida ransomware have implemented a dedicated form on their website, allowing potential clients to provide their email addresses and state their bidding prices. This gutsy move underscores the increasing boldness of cybercriminals, who are progressively resorting to extortion as a means to achieve financial gains.

Recommendations

- Create an inventory of assets and data. Examine the event and incident records thoroughly. Supervise hardware and software configurations. Allocate administrative powers and access exclusively based on a privilege. Set strict security parameters for network infrastructure devices such as firewalls and routers. Create a software whitelist to only allow legitimate applications.
- 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.
- Prioritize system **patching** to address the CVE-2020-1472 vulnerability (ZeroLogon) and prevent unauthorized access. Implement network segmentation to contain potential breaches and restrict lateral movement.

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	**T1491.001** Internal Defacement
T1069.001 Local Groups	**T1003.002** Security Account Manager	**T1069** Permission Groups Discovery	**T1055.002** Portable Executable Injection
T1021.004 SSH	**T1657** Financial Theft	**T1018** Remote System Discovery	**T1033** System Owner/User Discovery
T1112 Modify Registry	**T1482** Domain Trust Discovery	**T1564.003** Hidden Window	**T1078.002** Domain Accounts

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	67a78b39e760e3460a135a7e4fa096ab6ce6b013658103890c866d9401928ba5, a78fa1ecadc46870c17e458ab427bad6586b74c7d3e8472f6d8448832ccb20f1, 258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595, 294dce4ba0235538be2a8fb2347383bc9f2443f0edcef8a0e7de93c274474c8e, 97d24b71bf0232c738773173221c0cba5f92cede31876b71b51fd23501d54841, 02d54bd9a044d476f70a825e694e6c3c2e67c41bfdc27a3a7fc15682fcdd33c5, 76bf0dcb758ffa3415927d22ac2fb08db7684162a4de6b576efa92f9ab8d1100, 21e128e8e4633a87dd797ce8a8d46fc83758b2f757ffc1dc6ef7ebb71d6bc09d, 167e9daa1b1923e9115755ad674e08184487b7a02f1f717e5b9aadcafad95e17, cceb160f11c42b427f019f69d13521d6370d12c0cf43b85e9e781b396d6ac2f4, 94c45dede070df365fae5360c408e3c04f55d6dd923e25ba7941631d2e24060c,

TYPE	VALUE
SHA256	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b, 1c4978cd5d750a2985da9b58db137fc74d28422f1e087fd77642faa7efe7b597, 4e34b9442f825a16d7f6557193426ae7a18899ed46d3b896f6e4357367276183, 97766464d0f2f91b82b557ac656ab82e15cae7896b1d8c98632ca53c15cf06c4, 918784e25bd24192ce4e999538be96898558660659e3c624a5f27857784cd7e1, 48f559e00c472d9ffe3965ab92c6d298f8fb3a3f0d6d203cd2069bfca4bf3a57, edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef, 201d8e77ccc2575d910d47042a986480b1da28cf0033e7ee726ad9d45ccf4daa, a48ac157609888471bf8578fb8b2aef6b0068f7e0742fccf2e0e288b0b2cfdfb, de73b73eeb156f877de61f4a6975d06759292ed69f31aaf06c9811f3311e03e7, 951b1b5fd5cb13cde159cebc7c60465587e2061363d1d8847ab78b6c4fba7501, fdadb6e15c52c41a31e3c22659dd490d5b616e017d1b1aa6070008ce09ed27ea, d689cb1dbd2e4c06cd15e51a6871c406c595790ddcdcd7dc8d0401c7183720ef, 554f523914cdbaed8b17527170502199c185bd69a41c81102c50dbb0e5e5a78d, d3a816fe5d545a80e4639b34b90d92d1039eb71ef59e6e81b3c0e043a45b751c, 8329bcbadc7f81539a4969ca13f0be5b8eb7652b912324a1926fc9bfb6ec005a, be922312978a53c92a49fefd2c9f9cc098767b36f0e4d2e829d24725df65bc21, 4243dc8b991f5f8b3c0f233ca2110a1e03a1d716c3f51e88faf1d59b8242d329, 7ba47558c99e18c2c6449be804b5e765c48d3a70ceaa04c1e0fae67ff1d7178d, 5ef168f83b55d2cbd2426afc5e6fa8161270fa6a2a312831332dc472c95dfa42, d3247f03dcd7b9335344ebba76a0b92370f32f1cb0e480c734da52db2bd8df60, ed05f5d462767b3986583188000143f0eb24f7d89605523a28950e72e6b9039a, 5e55b4caf47a248a10abd009617684e969dbe5c448d087ee8178262aaab68636,

TYPE	VALUE
SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de, 3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96, 2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1, 6633fa85bb234a75927b23417313e51a4c155e12f71da3959e168851a600b010, dcdb9bd39b6014434190a9949dedf633726fdb470e95cc47cdaa47c1964b969f, 8d950068f46a04e77ad6637c680cccf5d703a1828fbd6bdca513268af4f2170f, 6ed5d50cf9d07db73eaa92c5405f6b1bf670028c602c605dfa7d4fcb80ef0801, d1f718d219930e57794bdadf9dda61406294b0759038cef282f7544b44b92285, 355b4a82313074999bd8fa1332b1ed00034e63bd2a0d0367e2622f35d75cf140, 4226738489c2a67852d51dbf96574f33e44e509bc265b950d495da79bb457400, 13fd3ad690c73cf0ad26c6716d4e9d1581b47c22fb7518b1d3bf9cfb8f9e9123, 4bf8fbb7db583e1aacbf36c5f740d012c8321f221066cc68107031bd8b6bc1ee, 95a922e178075fb771066db4ab1bd70c7016f794709d514ab1c7f11500f016cd, a9ca77dfe03ce15004157727bb43ba66f00ceb215362c9b3d199f000edaa8d61, 2813b6c07d17d25670163e0f66453b42d2f157bf2e42007806ebc6bb9d114acc, 8e43d1ddbd5c129055528a93f1e3fab0ecdf73a8a7ba9713dc4c3e216d7e5db4
SHA1	5b1bb39d0caa11e4ce62248ff2d031dae28725fc, f875ebf4c6809e76775d54f389840da67d236b36, 69b3d913a3967153d1e91ba1a31ebed839b297ed, 338d4f4ec714359d589918cee1adad12ef231907, b07f6a5f61834a57304ad4d885bd37d8e1badba8, 7abc07e7f56fc27130f84d1c7935a0961bd58cb9, 2543857b275ea5c6d332ab279498a5b772bd2bd4, eda3a5b8ec86dd5741786ed791d43698bb92a262
MD5	59a9ca795b59161f767b94fc2dece71a

TYPE	VALUE
URLs	hxxps://ipapi[.]com/json/, http[:]//5.255.127[.]20:443
TOR Address	rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad[.]onion, rhysidafc6lm7qa2mkiukbezh7zuth3i4wof4mh2audkymscjm6yegad[.]onion
IPv4	5.39.222[.]67, 5.255.99[.]59, 51.77.102[.]106, 108.62.118[.]136, 108.62.141[.]161, 146.70.104[.]249, 156.96.62[.]58, 157.154.194[.]6, 23.52.156[.]13, 23.108.57[.]83, 5.255.113[.]37
Emails	rhysidaeverywhere@onionmail[.]org, rhysidaofficial@onionmail[.]org
File Names	conhost.exe, psexec.exe, S_0.bat, 1.ps1, S_1.bat, S_2.bat, Sock5.sh, PsExec64.exe, PsGetsid64.exe, PsGetsid.exe, PsInfo64.exe, PsInfo.exe, PsLoggedon64.exe, PsLoggedon.exe, PsService64.exe, PsService.exe, Eula.txt, psfile64.exe, psfile.exe, pskill64.exe, pskill.exe, pslist64.exe, pslist.exe, psloglist64.exe, psloglist.exe, pspasswd64.exe,

TYPE	VALUE
File Names	pspasswd.exe, psping64.exe, psping.exe, psshutdown64.exe, psshutdown.exe, pssuspend64.exe, pssuspend.exe, PSTools.zip, Pstools.chm, psversion.txt, psexesvc.exe

Patch Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

Recent Breaches

https://www.pmh.com/
https://pierce.ctc.edu/
https://singingriverhealthsystem.com/
https://prosperius.it/
https://www.ufms.br/
http://www.mof.gov.kw/
https://coredesktop.com.au/
https://www.migracion.gob.do/
http://www.hermelin.ort.org.il/
https://www.hit.ac.il/
https://www.comune.fe.it/
http://pami.org.ar/
https://opt.net.au/
https://www.ramtha.com/
https://www.unitedtractors.com/
https://rouzbeh.info/
https://axity.com/
https://www.uws.ac.uk/
http://esmod.com/
https://www.eska-fuses.de/
https://web.unisa.it/
http://lumbertonisd.org/
https://iris-info.com/
https://www.thebiglifegroup.com/
https://roc-teraa.nl/ict/
https://www.ziegel-eder.de/
https://www.sapros.de/

http://www.imatica.com/
https://www.ejercito.cl/
http://www.tyconz.com/
https://www.eder.co.at/
https://www.polytec.bmgroup.com/
https://www.amstutz.ch/
http://ecaterham.net/
https://www.cittanuova.it/
https://www.haemokinesis.com/
https://www.koper-it.nl/
https://www.nsuok.edu/
https://thomas-hardye.net/
https://www.fassi.com/
https://www.ayto-arganda.es/
https://www.pchs.k12.il.us/
https://www.kebs.org/
https://www.collectivitedemartinique.mq/
https://www.hs-kl.de/
https://www.enfieldgrammar.org/
https://avannubo.com/
https://www.sfasu.edu/
https://www.hollywoodforever.com/

References

https://www.cisa.gov/sites/default/files/2023-11/aa23-319a-stopransomware-rhysida-ransomware_1.pdf

https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/rhysida-ransomware-intrusion.pdf?utm_source=blog&utm_medium=blog&utm_campaign=rhysida-ransomware

https://www.trendmicro.com/en_us/research/23/h/an-overview-of-the-new-rhysida-ransomware.html

https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf

https://www.sentinelone.com/blog/rhysida-ransomware-raas-crawls-out-of-crimeware-undergrowth-to-attack-chilean-army/

https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/

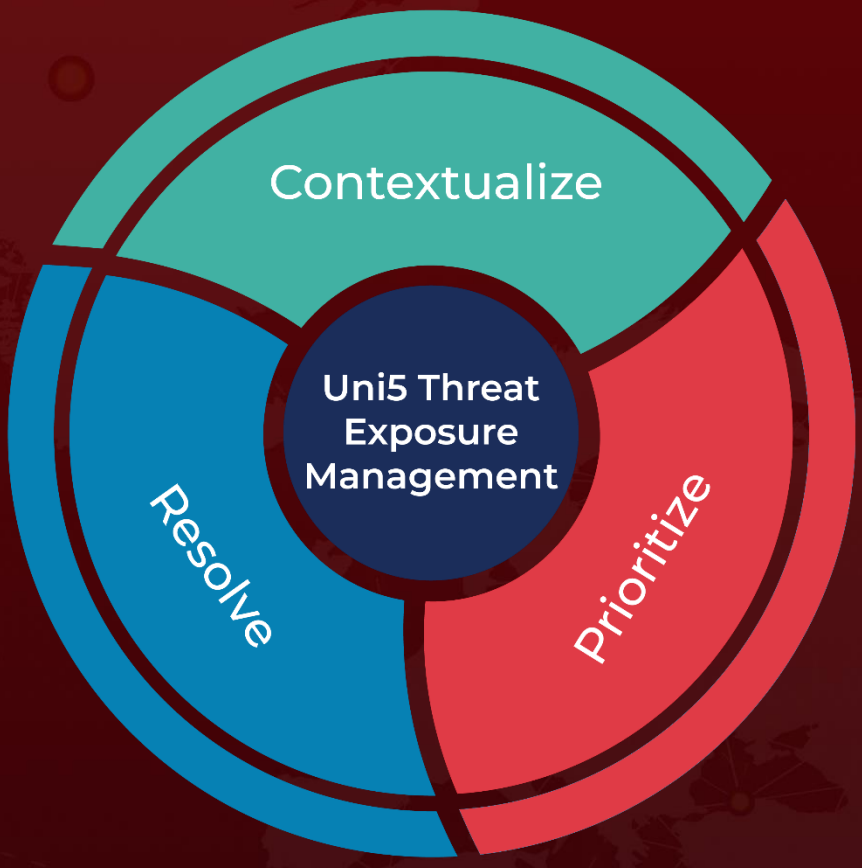
https://izoologic.com/2023/09/28/kuwaits-finance-ministry-faces-attack-from-rhysida-ransomware/

https://www.hivepro.com/threat-advisory/vice-society-actors-target-k-12-institutions-in-us/

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

August 10, 2023 • 7:00 AM

More at www.hivepro.com