Jul 04 2023

NETMANAGEIT

Intelligence Report

Rhysida Ransomware RaaS Crawls Out of Crimeware Undergrowth to Attack Chilean Army

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Rhysida ransomware-as-a-service (RaaS) group has gone from a dubious newcomer to a fully-fledged ransomware operation. Despite the developer's partial implementation of some features, the group emerged onto the scene at the end of May with a high-profile attack against the Chilean Army, continuing the ongoing trend of ransomware groups targeting Latin American government institutions. On June 15, the group leaked the files stolen from the Chilean Army.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name

0220083d724fdb8a406d3e780497561590804281

Description

Rhysida ransomware detection.

Pattern Type

yara

Pattern

rule rw_rhysida { meta: author = "Alex Delamotte" description = "Rhysida ransomware detection." sample = "69b3d913a3967153d1e91ba1a31ebed839b297ed" reference = "https://s1.ai/rhys" strings: $typo1 = { 63 6D 64 2E 65 78 65 20 2F 63 20 72 65 67 20 64 65 6C 65 74 65 20 22 48 4B 43 55 5C 43 6F 6E 74 74 6F 6C 20 50 61 6E 65 6C 5C 44 65 73 6B 74 6F 70 22 } $cmd1 = { 63 6D 64 2E 65 78 65 20 2F 63 20 72 65 67 20 61 64 64 20 22 48 4B 43 55 5C 53 6F 66 74 77 61 72 65 5C 4D 69 63 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 43 75 72 72 65 6E 74 56 65 72 73 69 6F 6E 5C 50 6F 6C 69 63 69 65 73 5C 41 63 74 69 76 65 44 65 73 6B 74 6F 70 } $cmd2 = { 63 6D 64 2E 65 78 65 20 2F 63 20 72 65 67 20 61 64 64 20 22 48 4B 4C 4D 5C 53 6F 66 74 77 61 72 65 5C 4D 69 63 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 43 75 72 72 65 6E 74 56 65 72 73 69 6F 6E 5C 50 6F 6C 69 63 69 65 73 5C 53 79 73 74 65 6D 22 20 2F 76 20 57 61 6C 6C 70 61 70 65 72 20 2F 74 20 52 45 47 5F 53 5A 20 2F 64 20 22 43 3A 5C 55 73 65 72 73 5C 50 75 62 6C 69 63 5C 62 67 2E 6A 70 67 22 20 2F 66 } $byte1 = { 48 8D 05 72 AA 05 00 48 8B 00 8B 95 } $byte2 = { 48 8D 15 89 CF 03 00 48 89 C1 E8 F9 1C 03 00 44 } condition: 2 of them }

Name

250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1

Description

stack_string SHA256 of b07f6a5f61834a57304ad4d885bd37d8e1badba8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1']

Name

a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6

Description

stack_string SHA256 of 69b3d913a3967153d1e91ba1a31ebed839b297ed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6']

Name

d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

Description
RareEquities_LibTomCrypt SHA256 of 338d4f4ec714359d589918cee1adad12ef231907
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee']

Intrusion-Set

Name
Rhysida

Malware

Name
Rhysida

Country

Name
Chile

Attack-Pattern

Name
Proxy
ID
T1090
Description
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.
Name
Data Encrypted for Impact
ID
T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python]

(https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Clipboard Data

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

StixFile

Value
250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1
a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

External References

- https://www.sentinelone.com/blog/rhysida-ransomware-raas-crawls-out-of-crimeware-undergrowth-to-attack-chilean-army/
- https://otx.alienvault.com/pulse/64a40a14c7d9619f336a8ea3