Mar 19 2024

NETMANAGEIT

Intelligence Report

Ransomware Roundup – RA World

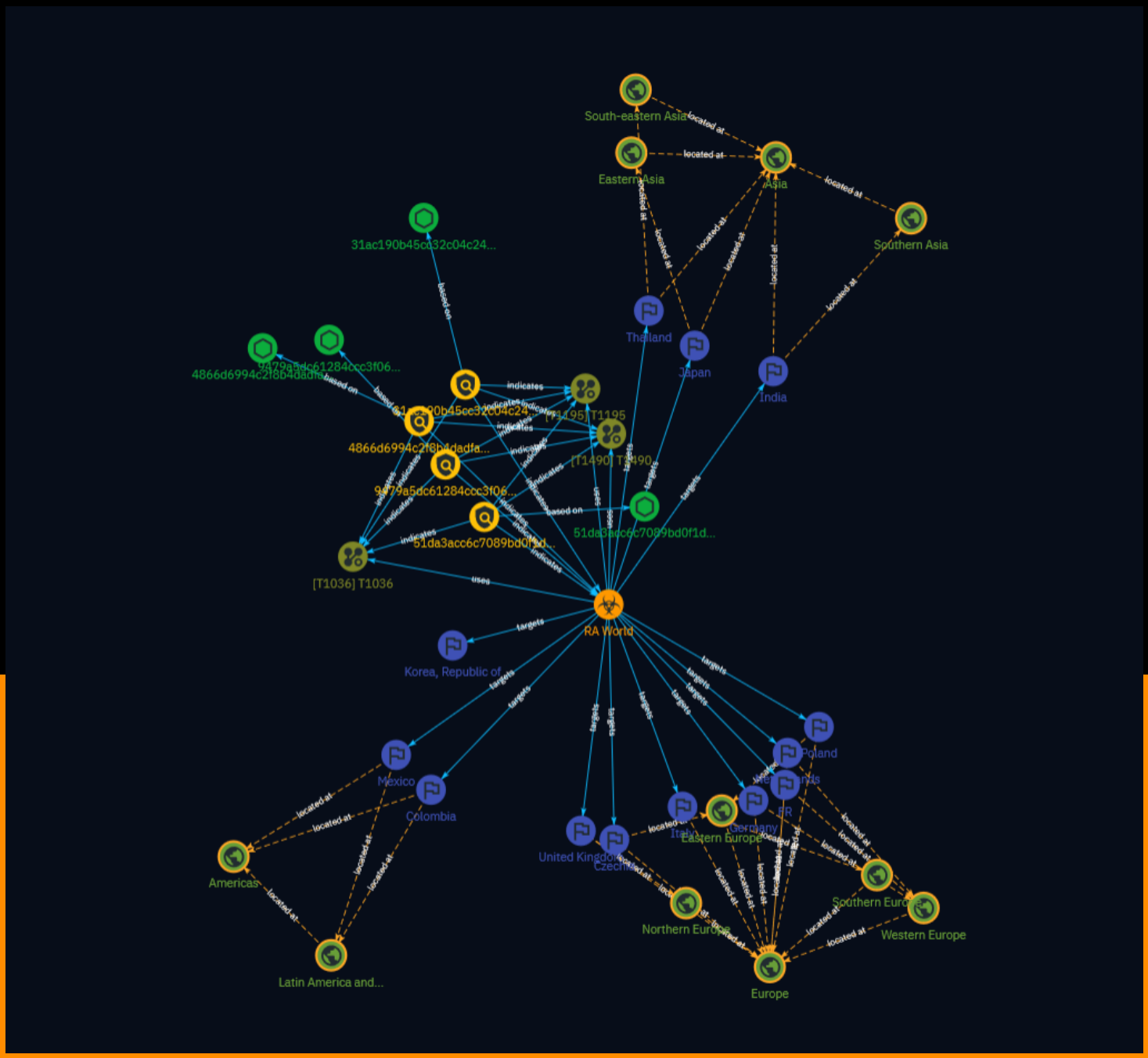

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 8
- Attack-Pattern 9
- Country 12
- Region 14

Observables

- StixFile 16

External References

- External References 17

Overview

Description

The blog provides an overview of the RA World ransomware, which encrypts files and steals data before demanding ransom for decryption and not leaking stolen files. The ransomware disables backups and deletes shadow copies to prevent recovery. It encrypts files and adds the .RAWLD extension, and drops a ransom note with contact info. The group operates TOR and non-TOR sites to publish stolen data. The blog covers infection vectors, victims, attack methods, protections, and mitigations.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc']
Name
4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801']
Name

31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4']

Name

9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

Description

Ransom:Win32/Babuk.SIB!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de']

Malware

Name
RA World

Attack-Pattern

Name
T1490
ID
T1490
Description
Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact] (https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete

backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Country

Name
Korea, Republic of
Name
Netherlands
Name
Germany
Name
FR
Name
Italy
Name
United Kingdom
Name
Poland

Name
Czechia
Name
India
Name
Thailand
Name
Japan
Name
Colombia
Name
Mexico

Region

Name
Western Europe
Name
Southern Europe
Name
Northern Europe
Name
Eastern Europe
Name
Europe
Name
Southern Asia
Name
South-eastern Asia

Name
Eastern Asia
Name
Asia
Name
Latin America and the Caribbean
Name
Americas

StixFile

Value
51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc
4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801
31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4
9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

External References

- https://www.fortinet.com/blog/threat-research/ransomware-roundup-ra-world
- https://otx.alienvault.com/pulse/65f80d8dee114f8093e5b5b8