Jul 03 2023

NETMANAGEIT

Intelligence Report

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

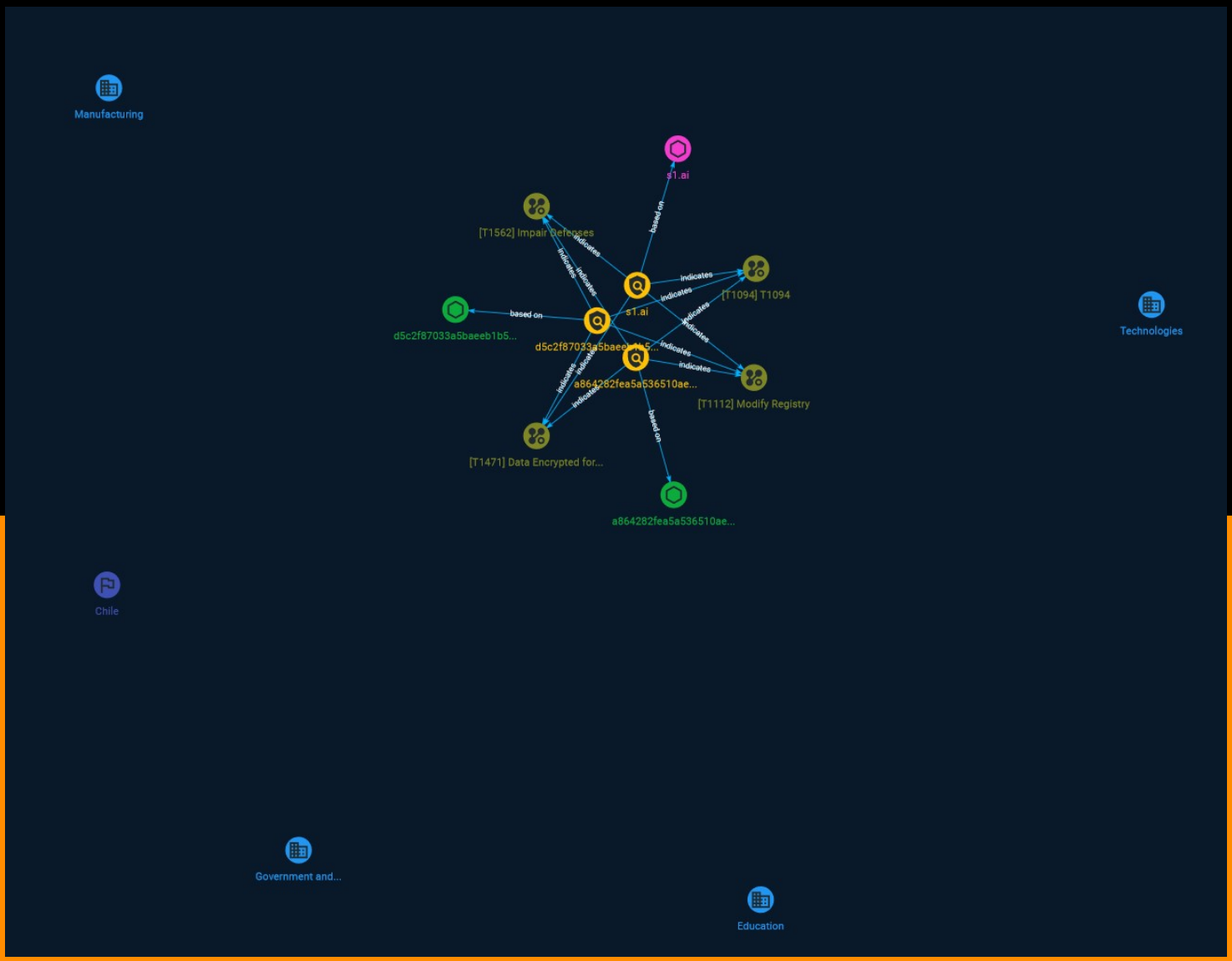

Table of contents

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
s1.ai
Pattern Type
stix
Pattern
[domain-name:value = 's1.ai']
Name
a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6']
Name

d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee']

Country

Name
Chile

Attack-Pattern

Name
T1094
ID
T1094
Name
Data Encrypted for Impact
ID
T1471
Description
An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. 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.
Name
Impair Defenses

ID

T1562

Description

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Name

Modify Registry

ID

T1112

Description

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse

these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Sector

Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

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

Domain-Name

Value
s1.ai

StixFile

Value
a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee

External References

- https://otx.alienvault.com/pulse/64a2e75f6e9cde21e9128510
- https://www.sentinelone.com/blog/rhysida-ransomware-raas-crawls-out-of-crimeware-undergrowth-to-attack-chilean-army/