Sep 22 2023

NETMANAGEIT

Intelligence Report

Sandman APT | A Mystery Group Targeting Telcos with a LuaJIT Toolkit

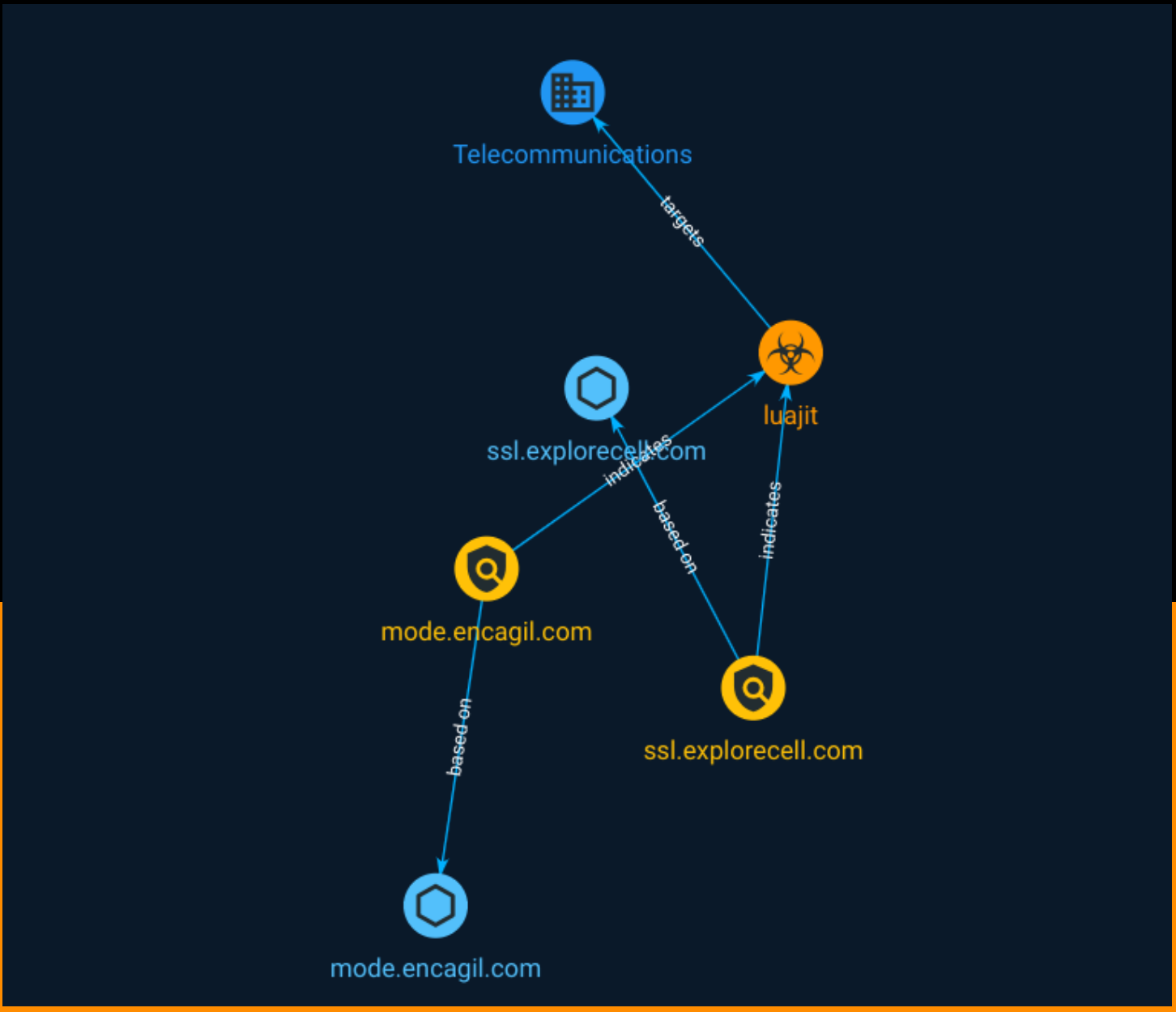

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Sophisticated threat actor deploys high-end malware utilizing the LuaJIT platform to backdoor telcos in Europe, Middle East and South Asia.

Confidence

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

15 / 100

Sector

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Indicator

Name
mode.encagil.com
Pattern Type
stix
Pattern
[hostname:value = 'mode.encagil.com']
Name
ssl.explorecell.com
Pattern Type
stix
Pattern
[hostname:value = 'ssl.explorecell.com']

Malware

Name
luajit

Hostname

Value
ssl.explorecell.com
mode.encagil.com

External References

- https://otx.alienvault.com/pulse/650d48259c180c1a4f592ab7
- https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/