Jul 03 2023

NETMANAGEIT

Intelligence Report

Analysis of attack activities of APT-C-26 (Lazarus) organization using fake VNC software

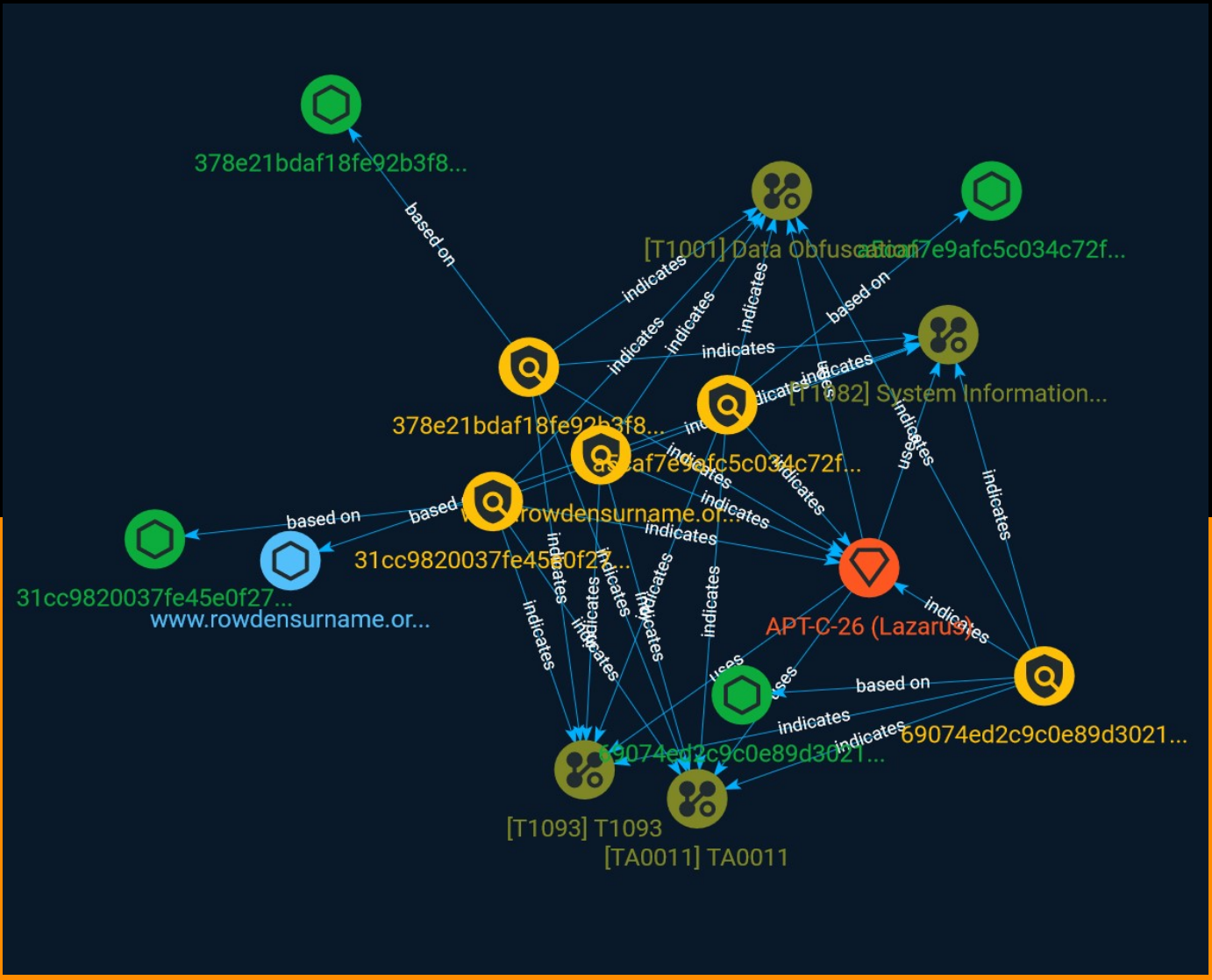

Table of contents

Overview

Entities

Observables

External References

Overview

Description

APT-C-26 (Lazarus) is an active APT organization whose main targets are financial institutions and cryptocurrency exchanges, and its attack methods include phishing, network attacks, and ransomware attacks. Their attacks have a high degree of technical complexity and concealment. The main purpose of the Lazarus group is to obtain funds, and may also be involved in activities such as theft of sensitive information.

Confidence

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

15 / 100

Indicator

Name
378e21bdaf18fe92b3f8ad9bef04dadd57a4271a4a5d4e00c9d73174695a07a2
Description
SHA256 of f6989d0c87f55fd9796c01a85a47896d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '378e21bdaf18fe92b3f8ad9bef04dadd57a4271a4a5d4e00c9d73174695a07a2']
Name
www.rowdensurname.org
Pattern Type
stix
Pattern

[hostname:value = 'www.rowdensurname.org']

Name

69074ed2c9c0e89d30217ef872e0ee96c34e7bbbd5aaf3380d9ce5acb45c1041

Description

SHA256 of ce1792fd716579823b33ac3c085ad742

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '69074ed2c9c0e89d30217ef872e0ee96c34e7bbbd5aaf3380d9ce5acb45c1041']

Name

31cc9820037fe45e0f27ea594b9f4c85ce4eaa9b95ae2a802cf7753e142afe85

Description

SHA256 of 6299bac300f45a37280a3503e6fdf0e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31cc9820037fe45e0f27ea594b9f4c85ce4eaa9b95ae2a802cf7753e142afe85']

Name
a5caf7e9afc5c034c72f50c831822ee54a307a04fef2d75a21094ef28ff1b306
Description
cotx_te SHA256 of 64bb5cff965553c0802e6d01c724b79c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a5caf7e9afc5c034c72f50c831822ee54a307a04fef2d75a21094ef28ff1b306']

Intrusion-Set

Name
APT-C-26 (Lazarus)

Attack-Pattern

Name
T1093
ID
T1093
Name
TA0011
ID
TA0011
Name
Data Obfuscation
ID
T1001
Description
Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in

an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

StixFile

Value
69074ed2c9c0e89d30217ef872e0ee96c34e7bbbd5aaf3380d9ce5acb45c1041
a5caf7e9afc5c034c72f50c831822ee54a307a04fef2d75a21094ef28ff1b306
31cc9820037fe45e0f27ea594b9f4c85ce4eaa9b95ae2a802cf7753e142afe85
378e21bdaf18fe92b3f8ad9bef04dadd57a4271a4a5d4e00c9d73174695a07a2

Hostname

Value
www.rowdensurname.org

External References

- https://otx.alienvault.com/pulse/64a2f58febf38755c4240c34
- https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA%3D%3D&mid=2247492789&idx=1&sn=a991e6c5ed7388515d75f02e9c33428f