Aug 24 2023

NETMANAGEIT

Intelligence Report

Lazarus Group's infrastructure reuse leads to discovery of new malware

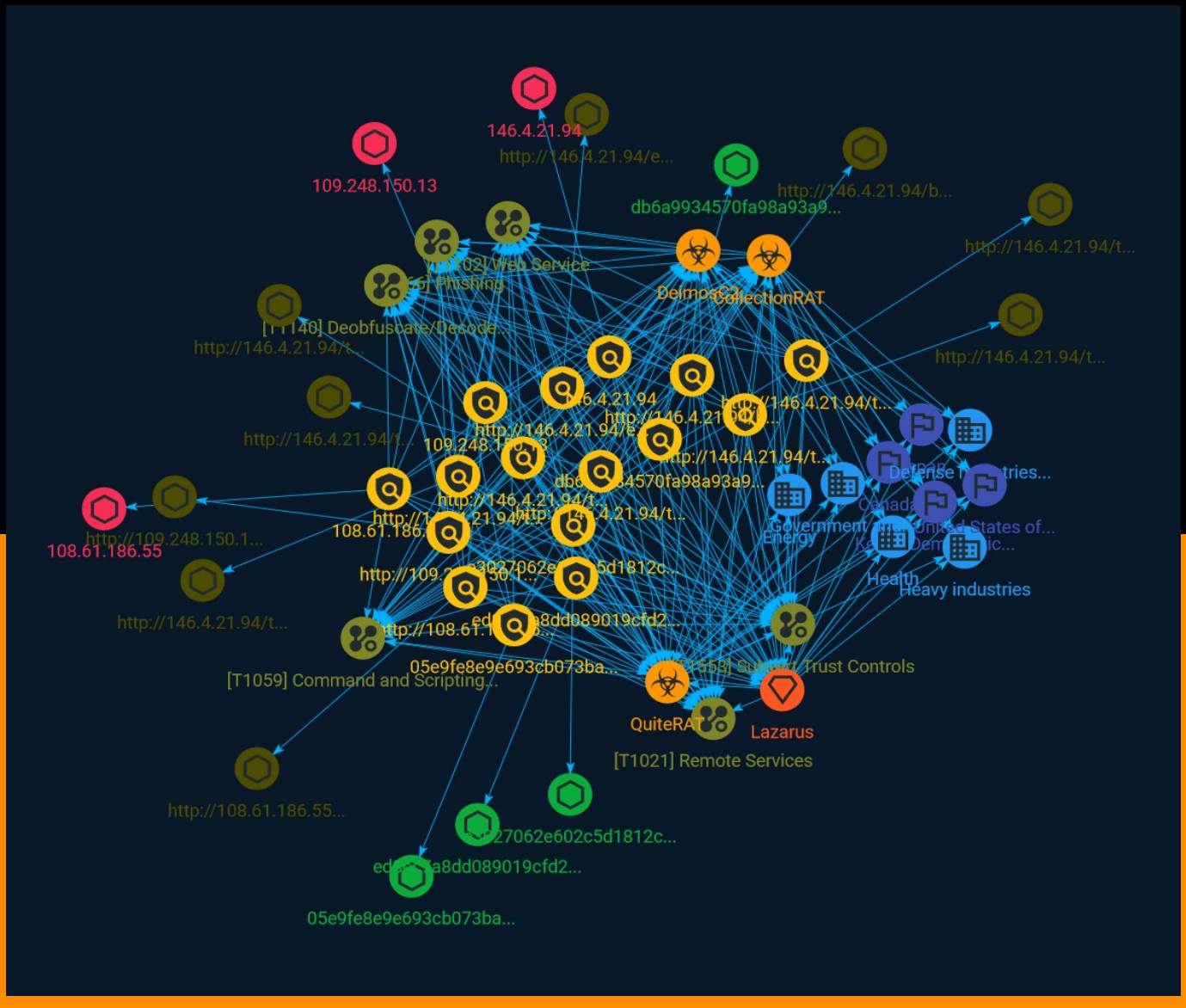

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In the Lazarus Group's latest campaign, which is detailed in a recent blog, the North Korean state-sponsored actor is exploiting CVE-2022-47966, a ManageEngine ServiceDesk vulnerability to deploy multiple threats. In addition to their "QuiteRAT" malware, which is covered in the blog, it was also discovered Lazarus Group is using a new threat called "CollectionRAT."

Confidence

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

15 / 100

Indicator

Name
http://146.4.21.94/tmp/tmp/logs.php
Pattern Type
stix
Pattern
[url:value = 'http://146.4.21.94/tmp/tmp/logs.php']
Name
e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe']
Name

http://146.4.21.94/tmp/tmp/comp.dat

Pattern Type

stix

Pattern

[url:value = 'http://146.4.21.94/tmp/tmp/comp.dat']

Name

http://146.4.21.94/tmp/tmp/

Pattern Type

stix

Pattern

[url:value = 'http://146.4.21.94/tmp/tmp/']

Name

108.61.186.55

Pattern Type

stix

Pattern

[ipv4-addr:value = '108.61.186.55']

Name

db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984']

Name

http://109.248.150.13/EsaFin.exe

Pattern Type

stix

Pattern

[url:value = 'http://109.248.150.13/EsaFin.exe']

Name

http://146.4.21.94/editor/common/cmod

Pattern Type

stix

Pattern

[url:value = 'http://146.4.21.94/editor/common/cmod']

Name
http://146.4.21.94/tmp/data_preview/
Pattern Type
stix
Pattern
[url:value = 'http://146.4.21.94/tmp/data_preview/']
Name
http://108.61.186.55:443
Pattern Type
stix
Pattern
[url:value = 'http://108.61.186.55:443']
Name
http://146.4.21.94/boards/boardindex.php
Pattern Type
stix
Pattern
[url:value = 'http://146.4.21.94/boards/boardindex.php']

Name

ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6

Description

TA430

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6']

Name

109.248.150.13

Description

CC=NL ASN=AS203557 DataClub S.A.

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.248.150.13']

Name

http://146.4.21.94/tmp/tmp/log.php

Pattern Type

stix

Pattern

[url:value = 'http://146.4.21.94/tmp/tmp/log.php']

Name

05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d

Description

ELF:Agent-BGN\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d']

Name

146.4.21.94

Description

CC=CH ASN=AS3303 Bluewin

Pattern Type
stix
Pattern
[ipv4-addr:value = '146.4.21.94']

Malware

Name
CollectionRAT
Name
QuiteRAT
Name
DeimosC2

Country

Name
Korea, Democratic People's Republic of
Name
Canada
Name
Japan
Name
United States of America

Intrusion-Set

Name
Lazarus

Sector

Name
Heavy industries
Description
Private entities working to transform raw materials into manufactured products (Chemicals, metal etc.).
Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.

Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

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

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

StixFile

Value
05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d
ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe

IPv4-Addr

Value
109.248.150.13
108.61.186.55
146.4.21.94

Url

Value
http://146.4.21.94/editor/common/cmod
http://146.4.21.94/boards/boardindex.php
http://146.4.21.94/tmp/tmp/logs.php
http://146.4.21.94/tmp/tmp/log.php
http://146.4.21.94/tmp/tmp/comp.dat
http://109.248.150.13/EsaFin.exe
http://108.61.186.55:443
http://146.4.21.94/tmp/data_preview/
http://146.4.21.94/tmp/tmp/

External References

- https://otx.alienvault.com/pulse/64e76f372e57767067edc4dd
- https://blog.talosintelligence.com/lazarus-collectionrat/