Oct 28 2023

NETMANAGEIT

Intelligence Report

Analysis Report on Lazarus Threat Group's Volgmer and Scout Malware

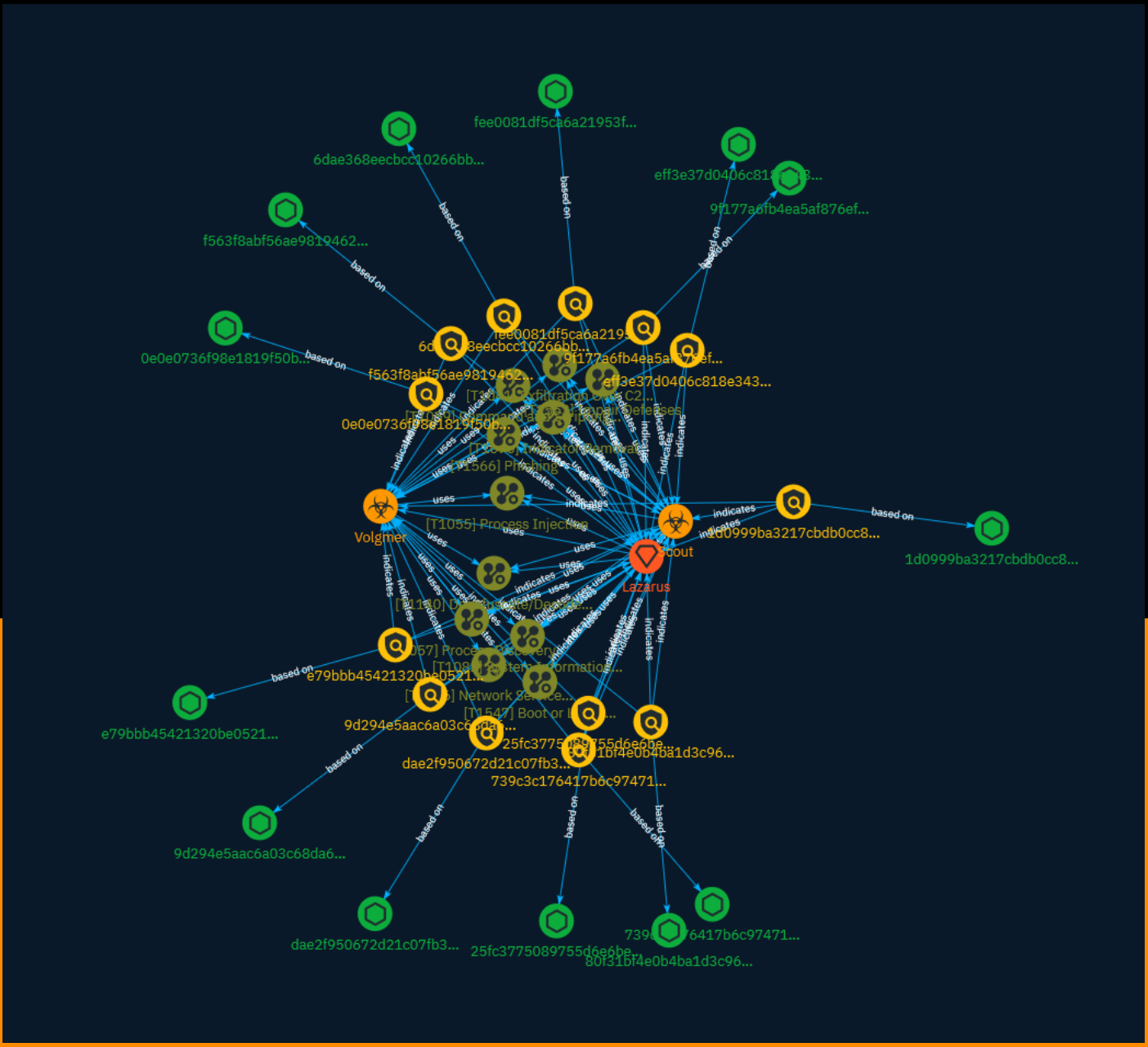

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The AhnLab Security Emergency Response Center (ASEC) is tracking attacks by the seemingly state-sponsored Lazarus threat group, and in this blog post, they examine the two major malware strains used in their attacks.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment

modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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

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

Network Service Discovery

ID

T1046

Description

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021) Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well. Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as `dns-sd -B _ssh._tcp .`) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

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

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)

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)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name
dae2f950672d21c07fb34fd4f1c415d9bf6e9a5f70f040980074f9eebcfe1b04
Description
SHA256 of 5473fa2c5823fbab2b94e8d5c44bc7b4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'dae2f950672d21c07fb34fd4f1c415d9bf6e9a5f70f040980074f9eebcfe1b04']
Name
6dae368eecbcc10266bba32776c40d9ffa5b50d7f6199a9b6c31d40dfe7877d1
Description
Backdoor:Win32/Joanap.I!dha SHA256 of 35f9cfe5110471a82e330d904c97466a
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6dae368eecbcc10266bba32776c40d9ffa5b50d7f6199a9b6c31d40dfe7877d1']

Name

eff3e37d0406c818e3430068d90e7ed2f594faa6bb146ab0a1c00a2f4a4809a5

Description

SHA256 of 1ecd83ee7e4cfc8fed7ceb998e75b996

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eff3e37d0406c818e3430068d90e7ed2f594faa6bb146ab0a1c00a2f4a4809a5']

Name

739c3c176417b6c974714a7469f16cb1db3b689fcf34c98c5b185d37e77ceeb0

Description

Armadillov1xxv2xx SHA256 of 64965a88e819fb93dbabafc4e3ad7b6c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '739c3c176417b6c974714a7469f16cb1db3b689fcf34c98c5b185d37e77ceeb0']

Name

0e0e0736f98e1819f50b6f05fa59b19296ea7a61042be94c46eb03012b42ea49

Description

SHA256 of 570a4253ae80ee8c2b6b23386e273f3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e0e0736f98e1819f50b6f05fa59b19296ea7a61042be94c46eb03012b42ea49']

Name

1d0999ba3217cbdb0cc85403ef75587f747556a97dee7c2616e28866db932a0d

Description

SHA256 of 5dd1ccc8fb2a5615bf5656721339efed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d0999ba3217cbdb0cc85403ef75587f747556a97dee7c2616e28866db932a0d']

Name

e79bbb45421320be05211a94ed507430cc9f6cf80d607d61a317af255733fcf2

Description

Backdoor:Win32/Joanap.I!dha SHA256 of e3d03829cbec1a8cca56c6ae730ba9a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e79bbb45421320be05211a94ed507430cc9f6cf80d607d61a317af255733fcf2']

Name

fee0081df5ca6a21953f3a633f2f64b7c0701977623d3a4ec36fff282ffe73b9

Description

Armadillov1xxv2xx SHA256 of eb9db98914207815d763e2e5cfbe96b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fee0081df5ca6a21953f3a633f2f64b7c0701977623d3a4ec36fff282ffe73b9']

Name

80f31bf4e0b4ba1d3c963cf37dd7cefb5517b6454f7809fe3a1703e8b5941b41

Description

SHA256 of 72756e6ebb8274d9352d8d1e7e505906

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '80f31bf4e0b4ba1d3c963cf37dd7cefb5517b6454f7809fe3a1703e8b5941b41']

Name

f563f8abf56ae9819462e21635fbd4c790b2f7d69ae8c02d042a3510209694a9

Description

SHA256 of 4753679cef5162000233d69330208420

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f563f8abf56ae9819462e21635fbd4c790b2f7d69ae8c02d042a3510209694a9']

Name

25fc3775089755d6e6be30d3aad35cba2942760355a82cd585fb085e89ef82fa

Description

SHA256 of b517e7ad07d1182feb4b8f61549ff233

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25fc3775089755d6e6be30d3aad35cba2942760355a82cd585fb085e89ef82fa']

Name

9d294e5aac6a03c68da6fe8d81b06aee322940182e9d7533acb91be319807a38

Description

SHA256 of b1225fa644eebafba07f0f5e404bd4fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d294e5aac6a03c68da6fe8d81b06aee322940182e9d7533acb91be319807a38']

Name

9f177a6fb4ea5af876ef8a0bf954e37544917d9aaba04680a29303f24ca5c72c

Description

Armadillov1xxv2xx SHA256 of 9a5fa5c5f3915b2297a1c379be9979f0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f177a6fb4ea5af876ef8a0bf954e37544917d9aaba04680a29303f24ca5c72c']

Intrusion-Set

Name
Lazarus

Malware

Name
Volgmer

Description
[Volgmer](https://attack.mitre.org/software/S0180) is a backdoor Trojan designed to provide covert access to a compromised system. It has been used since at least 2013 to target the government, financial, automotive, and media industries. Its primary delivery mechanism is suspected to be spearphishing. (Citation: US-CERT Volgmer Nov 2017)

Name
Scout

StixFile

Value
9f177a6fb4ea5af876ef8a0bf954e37544917d9aaba04680a29303f24ca5c72c
e79bbb45421320be05211a94ed507430cc9f6cf80d607d61a317af255733fcf2
739c3c176417b6c974714a7469f16cb1db3b689fcf34c98c5b185d37e77ceeb0
25fc3775089755d6e6be30d3aad35cba2942760355a82cd585fb085e89ef82fa
fee0081df5ca6a21953f3a633f2f64b7c0701977623d3a4ec36fff282ffe73b9
80f31bf4e0b4ba1d3c963cf37dd7cefb5517b6454f7809fe3a1703e8b5941b41
f563f8abf56ae9819462e21635fbd4c790b2f7d69ae8c02d042a3510209694a9
9d294e5aac6a03c68da6fe8d81b06aee322940182e9d7533acb91be319807a38
0e0e0736f98e1819f50b6f05fa59b19296ea7a61042be94c46eb03012b42ea49
eff3e37d0406c818e3430068d90e7ed2f594faa6bb146ab0a1c00a2f4a4809a5
1d0999ba3217cbdb0cc85403ef75587f747556a97dee7c2616e28866db932a0d
dae2f950672d21c07fb34fd4f1c415d9bf6e9a5f70f040980074f9eebcfe1b04
6dae368eecbcc10266bba32776c40d9ffa5b50d7f6199a9b6c31d40dfe7877d1

External References

- https://otx.alienvault.com/pulse/652d5e396771a72c6468d3cc
- https://asec.ahnlab.com/en/57685/