Jan 22 2024

NETMANAGEIT

Intelligence Report

Mimo CoinMiner and Mimus Ransomware Installed via Vulnerability Attacks

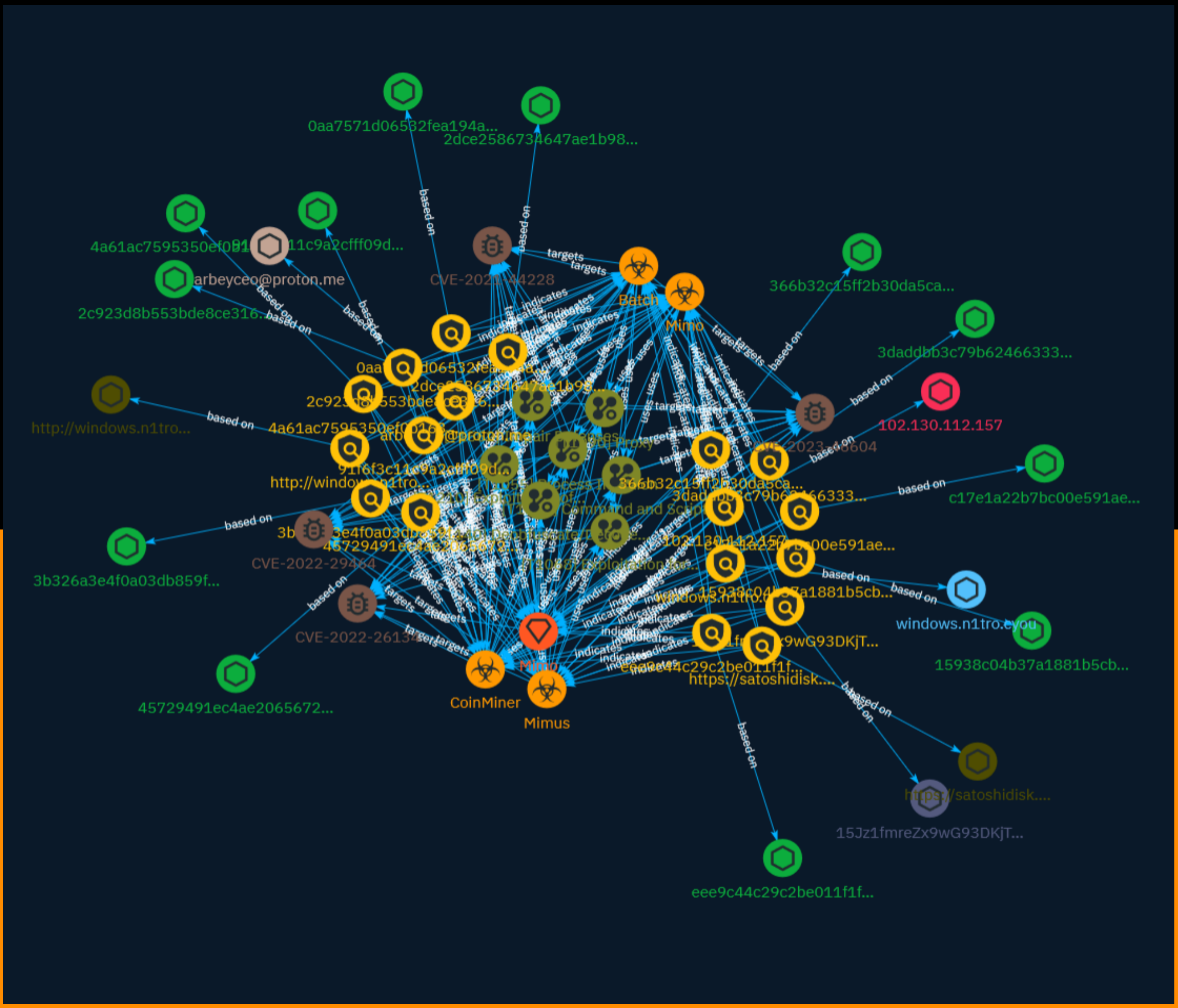

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat actor called Mimo has been exploiting vulnerabilities to install CoinMiners and other malware.

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 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

Exploitation of Remote Services

ID

T1210

Description

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

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

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)

Indicator

Name

windows.n1tro.cyou

Pattern Type

stix

Pattern

[hostname:value = 'windows.n1tro.cyou']

Name

arbeyceo@proton.me

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 3 - **Overall Score:** 4 - **First Name:** Unknown - **Generic:** False - **Common:** True - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** True - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** arbeyceo@proton.me - **Domain Age:** {'human': '3 years ago', 'timestamp': 1611884794, 'iso': '2021-01-28T20:46:34-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1705674587, 'iso': '2024-01-19T09:29:47-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'arbeyceo@proton.me']

Name

15Jz1fmreZx9wG93DKjTXMhuLpPpCgvEQk

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = '15Jz1fmreZx9wG93DKjTXMhuLpPpCgvEQk']

Name

91f6f3c11c9a2cfff09dd7be94c2c82314d341d6fb9bc7ac3be04cb235bafc55

Description

SUSP_ENV_Folder_Root_File_Jan23_1 SHA256 of 5e0f18dfe16f274d34716d011e0a3f39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'91f6f3c11c9a2cfff09dd7be94c2c82314d341d6fb9bc7ac3be04cb235bafc55']

Name

366b32c15ff2b30da5cafc1407e6dc49aa4bbecffc34c438302022acd1c00b8e

Description

ALF:Trojan:Win32/CoinMiner.D SHA256 of 3edcde37dcecb1b5a70b727ea36521de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '366b32c15ff2b30da5cafc1407e6dc49aa4bbecffc34c438302022acd1c00b8e']

Name

102.130.112.157

Description

CC=ZA ASN=AS328364 Host-Africa-AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '102.130.112.157']

Name

4a61ac7595350ef0b163787b175cecc4e7ee9774d288770fa0ea0289b1d83548

Description

SHA256 of c25972604121f4c6a7f8025e4e575c7c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a61ac7595350ef0b163787b175cecc4e7ee9774d288770fa0ea0289b1d83548']

Name

15938c04b37a1881b5cb16c4ad66a40a97fb0e28fd26e42d4f1a10826d12e26e

Description

SUSP_ENV_Folder_Root_File_Jan23_1 SHA256 of 618680a68eb6ac79f530a0291ad29d9f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15938c04b37a1881b5cb16c4ad66a40a97fb0e28fd26e42d4f1a10826d12e26e']

Name

45729491ec4ae2065672e6d93a3aa7533a8058cecb8fcdb79ecd5d10cfa2aeca

Description

Script:SNH-gen\ [Trj] SHA256 of 5d32f0eee7adf20e0766d5481a1953a5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45729491ec4ae2065672e6d93a3aa7533a8058cecb8fcdb79ecd5d10cfa2aeca']

Name

0aa7571d06532fea194a62091a812557a8f8b8d616ffd923df766a4871f4a918

Description

___FilesToHash_17jun SHA256 of dd6931fda2df843249a5df40b8808387

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0aa7571d06532fea194a62091a812557a8f8b8d616ffd923df766a4871f4a918']

Name

https://satoshidisk.com/pay/CIIRg6

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 540483 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Downloads - **Domain Age:** {'human': '6 years ago', 'timestamp': 1511717546, 'iso': '2017-11-26T12:32:26-05:00'} - **IPQS: Domain:** satoshidisk.com - **IPQS: IP Address:** 172.67.221.90

Pattern Type

stix

Pattern

[url:value = 'https://satoshidisk.com/pay/CIIRg6']

Name

http://windows.n1tro.cyou:4544

Description

ASCII text, with no line terminators
565339bc4d33d72817b583024112eb7f5cdf3e5eef0252d6ec1b9c9a94e12bb3

Pattern Type

stix

Pattern

[url:value = 'http://windows.n1tro.cyou:4544']

Name

3daddbb3c79b624663339a9603e685a469e92b4c889e6a8a7b8625f769c7c661

Description

ALF:Trojan:Win32/CoinMiner.D SHA256 of 7ef97450e84211f9f35d45e1e6ae1481

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3daddbb3c79b624663339a9603e685a469e92b4c889e6a8a7b8625f769c7c661']

Name

eee9c44c29c2be011f1f1e43bb8c3fca888cb81053022ec5a0060035de16d848

Description

SHA256 of 1136efb1a46d1f2d508162387f30dc4d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'eee9c44c29c2be011f1f1e43bb8c3fca888cb81053022ec5a0060035de16d848']

Name

2c923d8b553bde8ce3167fe83f35a40a712e2bed2b76ebaf5e3e63642d551389

Description

SHA256 of 61def7b3b98458a40fffa42a19ddf258

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2c923d8b553bde8ce3167fe83f35a40a712e2bed2b76ebaf5e3e63642d551389']

Name

c17e1a22b7bc00e591aede9d101b843ff2e47d5b582bb0628406bbd53b7dac78

Description

SHA256 of bfa626e053028f9adbfaceb5d56086c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c17e1a22b7bc00e591aede9d101b843ff2e47d5b582bb0628406bbd53b7dac78']

Name

3b326a3e4f0a03db859feeed7e4e3a832acdaeaf8b2cd69ecc0dce73c1a225c9

Description

SUSP_ENV_Folder_Root_File_Jan23_1 SHA256 of a3ffb336aee9f01275c92ac529c8f70e

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3b326a3e4f0a03db859feeed7e4e3a832acdaeaf8b2cd69ecc0dce73c1a225c9']
Name
2dce2586734647ae1b9811e59281583f72c5c624c30a49380e006b0dbb8370c9
Description
SUSP_ENV_Folder_Root_File_Jan23_1 SHA256 of 958dd3e767b32a28c199d59ce01ffb6c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2dce2586734647ae1b9811e59281583f72c5c624c30a49380e006b0dbb8370c9']

Intrusion-Set

Name
Mimo

Malware

Name
Mimo

Name
CoinMiner

Name
Batch

Name
Mimus

Vulnerability

Name

CVE-2022-26134

Description

Atlassian Confluence Server and Data Center contain a remote code execution vulnerability that allows for an unauthenticated attacker to perform remote code execution.

Name

CVE-2021-44228

Description

Apache Log4j2 contains a vulnerability where JNDI features do not protect against attacker-controlled JNDI-related endpoints, allowing for remote code execution.

Name

CVE-2023-46604

Description

Apache ActiveMQ contains a deserialization of untrusted data vulnerability that may allow a remote attacker with network access to a broker to run shell commands by manipulating

serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath.
Name
CVE-2022-29464
Description
Multiple WSO2 products allow for unrestricted file upload, resulting in remote code execution.

Cryptocurrency-Wallet

Value
15Jz1fmreZx9wG93DKjTXMhuLpPpCgvEQk

Email-Addr

Value
arbeyceo@proton.me

StixFile

Value
4a61ac7595350ef0b163787b175cecc4e7ee9774d288770fa0ea0289b1d83548
3daddbb3c79b624663339a9603e685a469e92b4c889e6a8a7b8625f769c7c661
2c923d8b553bde8ce3167fe83f35a40a712e2bed2b76ebaf5e3e63642d551389
0aa7571d06532fea194a62091a812557a8f8b8d616ffd923df766a4871f4a918
45729491ec4ae2065672e6d93a3aa7533a8058cecb8fcdb79ecd5d10cfa2aeca
c17e1a22b7bc00e591aede9d101b843ff2e47d5b582bb0628406bbd53b7dac78
366b32c15ff2b30da5cafc1407e6dc49aa4bbecffc34c438302022acd1c00b8e
eee9c44c29c2be011f1f1e43bb8c3fca888cb81053022ec5a0060035de16d848
91f6f3c11c9a2cfff09dd7be94c2c82314d341d6fb9bc7ac3be04cb235bafc55
15938c04b37a1881b5cb16c4ad66a40a97fb0e28fd26e42d4f1a10826d12e26e
3b326a3e4f0a03db859feeed7e4e3a832acdaeaf8b2cd69ecc0dce73c1a225c9
2dce2586734647ae1b9811e59281583f72c5c624c30a49380e006b0dbb8370c9

Hostname

Value
windows.n1tro.cyou

IPv4-Addr

Value
102.130.112.157

Url

Value
http://windows.n1tro.cyou:4544
https://satoshidisk.com/pay/CIIRg6

External References

- https://otx.alienvault.com/pulse/65aa819dfed4b47f5aaebe94
- https://asec.ahnlab.com/en/60440/