Mar 05 2024

NETMANAGEIT

Intelligence Report

New variant of SupermanMiner mining malware continues to be active

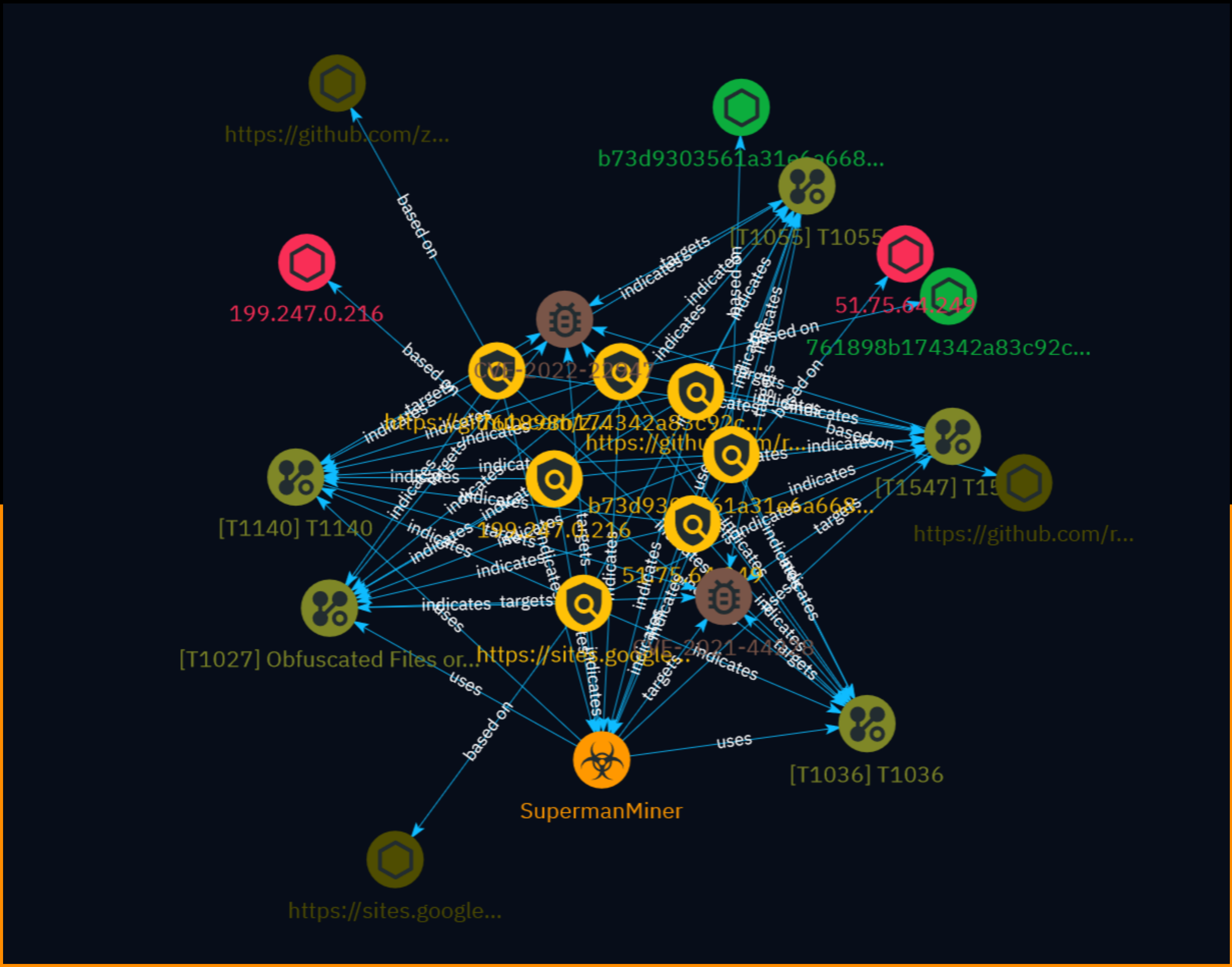

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new variant of the SupermanMiner cryptocurrency mining malware has been active for over 2 years, using techniques like vulnerability exploitation, SSH brute force, web shell injection and others to infect systems. It has evolved into multiple new branches, with heavy obfuscation and complex persistence mechanisms, posing a serious threat. Users should apply security patches, use strong passwords and limit external access to prevent infection.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

https://sites.google.com/view/2022luckyboy/2022

Description

- **Unsafe:** False - **Server:** ESF - **Domain Rank:** 1 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:** {'human': '26 years ago', 'timestamp': 874296000, 'iso': '1997-09-15T00:00:00-04:00'} - **IPQS: Domain:** sites.google.com - **IPQS: IP Address:** 172.253.115.99

Pattern Type

stix

Pattern

[url:value = 'https://sites.google.com/view/2022luckyboy/2022']

Name

https://github.com/zh/five/xdaemon

Description

- **Unsafe:** False - **Server:** GitHub.com - **Domain Rank:** 30 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Computers & internet - **Domain

Age:** {'human': '16 years ago', 'timestamp': 1191954050, 'iso': '2007-10-09T14:20:50-04:00'} - **IPQS: Domain:** github.com - **IPQS: IP Address:** 140.82.114.3

Pattern Type

stix

Pattern

[url:value = 'https://github.com/zh/five/xdaemon']

Name

https://github.com/robfig/cron/v3

Description

- **Unsafe:** False - **Server:** GitHub.com - **Domain Rank:** 30 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '16 years ago', 'timestamp': 1191954050, 'iso': '2007-10-09T14:20:50-04:00'} - **IPQS: Domain:** github.com - **IPQS: IP Address:** 140.82.114.3

Pattern Type

stix

Pattern

[url:value = 'https://github.com/robfig/cron/v3']

Name

b73d9303561a31e6a668a3546ba85b841965fea24f5989efa7aabeafaa6ea9ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b73d9303561a31e6a668a3546ba85b841965fea24f5989efa7aabeafaa6ea9ba']

Name

761898b174342a83c92c5a565019fa60bdd4022c251dd45bea7c27fb9ebcf18a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '761898b174342a83c92c5a565019fa60bdd4022c251dd45bea7c27fb9ebcf18a']

Name

199.247.0.216

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** Europe/Berlin - **Mobile:** False - **Host:** 199.247.0.216.vultrusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** DE - **Region:** Hesse - **City:** Frankfurt am Main - **Latitude:** 50.11029816 - **Longitude:** 8.71469975

Pattern Type

stix

Pattern

[ipv4-addr:value = '199.247.0.216']

Name

51.75.64.249

Description

- **Zip Code:** N/A - **ISP:** OVH SAS - **ASN:** 16276 - **Organization:** OVH SAS - **Is Crawler:** False - **Timezone:** Europe/Berlin - **Mobile:** False - **Host:** vps-ee13a4e4.vps.ovh.net - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** DE - **Region:** Hessen - **City:** Limburg an der Lahn - **Latitude:** 50.38359833 - **Longitude:** 8.05029964

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.75.64.249']

Malware

Name
SupermanMiner

Vulnerability

Name
CVE-2022-22947
Description
Spring Cloud Gateway applications are vulnerable to a code injection attack when the Gateway Actuator endpoint is enabled, exposed and unsecured.
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.

Attack-Pattern

Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [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) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1055

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

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1140

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

T1547

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.

Url

Value
https://sites.google.com/view/2022luckyboy/2022
https://github.com/zh/five/xdaemon
https://github.com/robfig/cron/v3

StixFile

Value
b73d9303561a31e6a668a3546ba85b841965fea24f5989efa7aabeafaa6ea9ba
761898b174342a83c92c5a565019fa60bdd4022c251dd45bea7c27fb9ebcf18a

IPv4-Addr

Value
199.247.0.216
51.75.64.249

External References

- https://cert.360.cn/warning/detail?id=65deee7fc09f255b91b17e0f
- https://otx.alienvault.com/pulse/65e6f2c8f044bef9fde9041f