Jan 05 2024

NETMANAGEIT

Intelligence Report

Three New Malicious PyPI Packages Deploy CoinMiner on Linux Devices

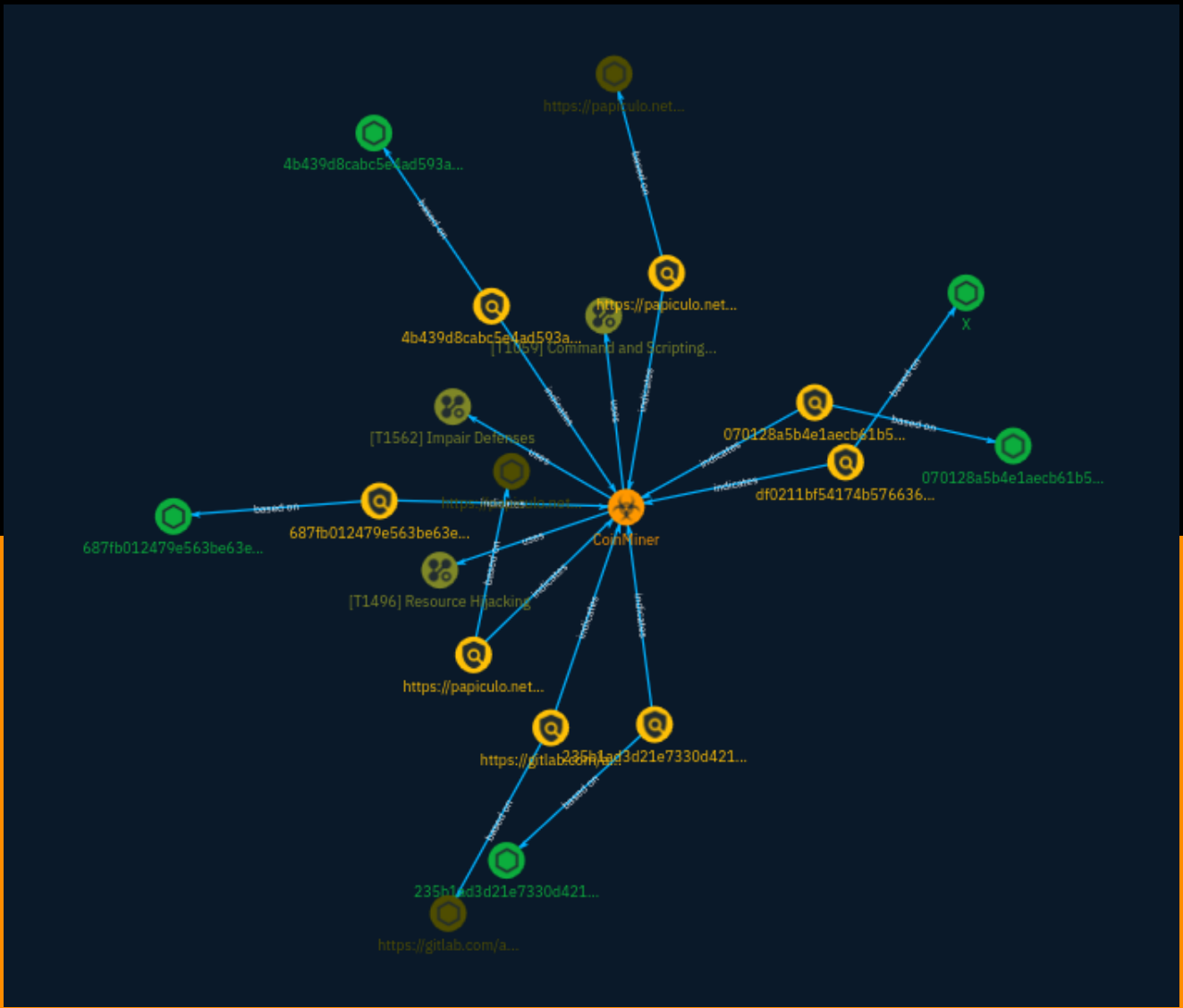

Table of contents

Overview

Entities

Observables

External References

Overview

Description

FortiGuard has identified three new malicious PyPI packages that deploy a CoinMiner executable on Linux devices, in an analysis published in the Security Research Review (PSIRT) journal on Wednesday.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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
Resource Hijacking
ID
T1496

Description

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster. (Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR) Alternatively, they may engage in proxyjacking by selling use of the victims' network bandwidth and IP address to proxyware services.(Citation: Sysdig Proxyjacking)

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)

Indicator

Name
https://papiculo.net/unmi.sh
Pattern Type
stix
Pattern
[url:value = 'https://papiculo.net/unmi.sh']
Name
https://gitlab.com/ajo9082734/Mine/-/raw/main/X
Pattern Type
stix
Pattern
[url:value = 'https://gitlab.com/ajo9082734/Mine/-/raw/main/X']
Name
070128a5b4e1aecb61b59f3f8ef2602e63cd1e5357f1314080a7c8a4960b0bee

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '070128a5b4e1aecb61b59f3f8ef2602e63cd1e5357f1314080a7c8a4960b0bee']
Name
235b1ad3d21e7330d421c9a03b6b822fcdddacaa707bed9d67dabd43d4401fc6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '235b1ad3d21e7330d421c9a03b6b822fcdddacaa707bed9d67dabd43d4401fc6']
Name
687fb012479e563be63e02718eb7be7ee81974193c952777ca94234c95b25115
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '687fb012479e563be63e02718eb7be7ee81974193c952777ca94234c95b25115']

Name
df0211bf54174b5766366eecfb0a04c4a59346478e1507b6685fbaed6b2d2aca
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'df0211bf54174b5766366eecfb0a04c4a59346478e1507b6685fbaed6b2d2aca']
Name
https://papiculo.net/unmiconfig.json
Pattern Type
stix
Pattern
[url:value = 'https://papiculo.net/unmiconfig.json']
Name
4b439d8cabc5e4ad593a26065e6d374efdddf41c8d91744b077a69812df170d2
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4b439d8cabc5e4ad593a26065e6d374efdddf41c8d91744b077a69812df170d2']

Malware

Name
CoinMiner

StixFile

Value
070128a5b4e1aecb61b59f3f8ef2602e63cd1e5357f1314080a7c8a4960b0bee
235b1ad3d21e7330d421c9a03b6b822fcdddacaa707bed9d67dabd43d4401fc6
df0211bf54174b5766366eecfb0a04c4a59346478e1507b6685fbaed6b2d2aca
687fb012479e563be63e02718eb7be7ee81974193c952777ca94234c95b25115
4b439d8cabc5e4ad593a26065e6d374efdddf41c8d91744b077a69812df170d2

Url

Value
https://papiculo.net/unmi.sh
https://papiculo.net/unmiconfig.json
https://gitlab.com/ajo9082734/Mine/-/raw/main/X

External References

- https://otx.alienvault.com/pulse/65980fc667b79d999df25ec4
- https://www.fortinet.com/blog/threat-research/malicious-pypi-packages-deploy-coinminer-on-linux-devices