Feb 18 2024

NETMANAGEIT

Intelligence Report

RCE to Sliver: IR Tales from the Field

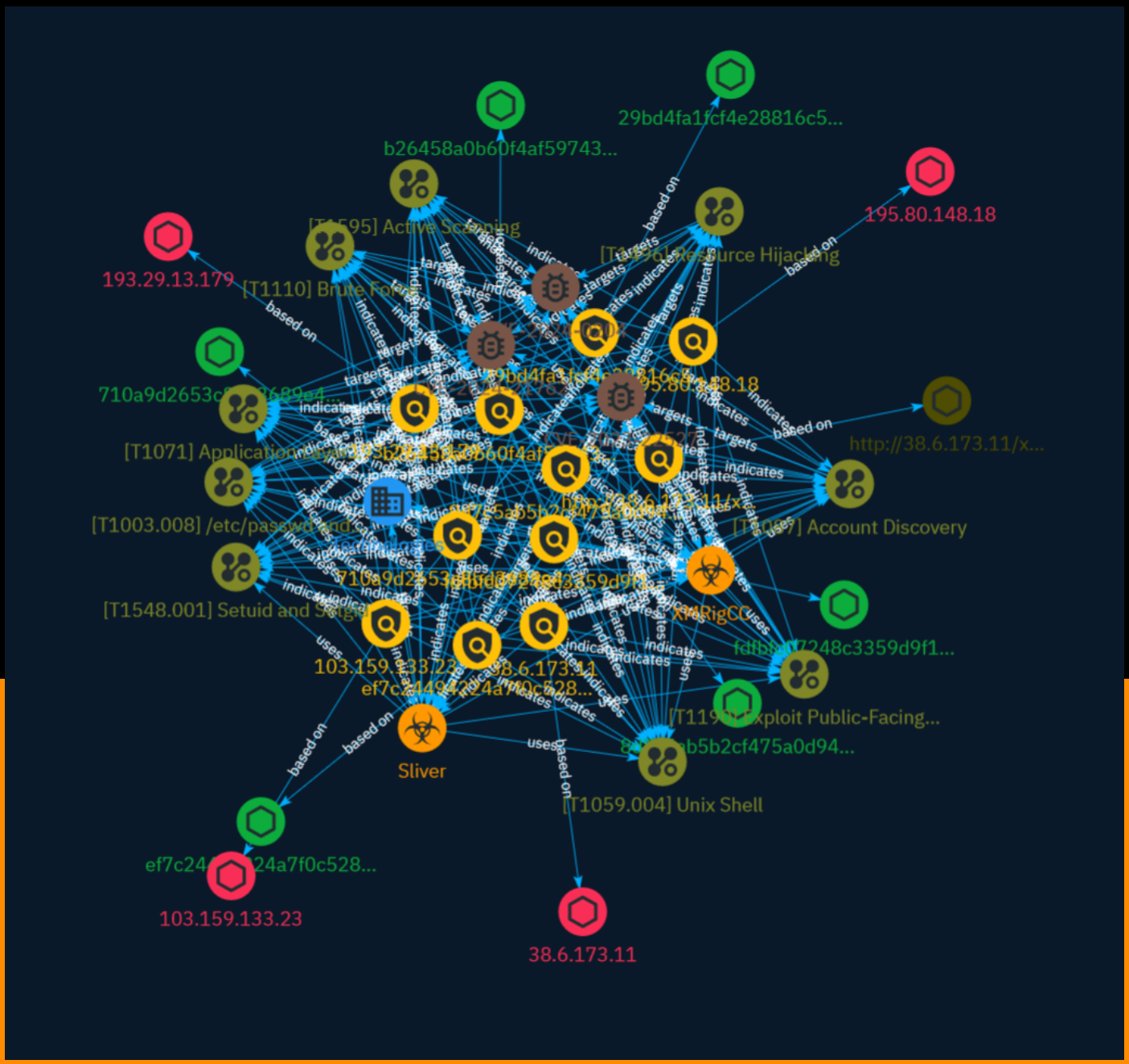

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Rapid7 Incident Response was engaged to investigate unauthorized access to two publicly-facing Confluence servers exploited via CVE-2023-22527. Cryptomining software and a Sliver C2 payload were identified. Sliver was used to action further objectives like Kerbrute enumeration and scanning. Rapid7 performed analysis to extract IOCs and implemented containment.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

http://38.6.173.11/xmrigCC-3.4.0-linux-generic-static-amd64.tar.gz

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 38.6.173.11 - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://38.6.173.11/xmrigCC-3.4.0-linux-generic-static-amd64.tar.gz']

Name

103.159.133.23

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 103.159.133.23 - **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:** MY - **Region:** Kelantan - **City:** Kota Bharu - **Latitude:** 6.1257 - **Longitude:** 102.23290253

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.159.133.23']

Name

fdfbfc07248c3359d9f1f536a406d4268f01ed63a856bd6cef9dccb3cf4f2376

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fdfbfc07248c3359d9f1f536a406d4268f01ed63a856bd6cef9dccb3cf4f2376']

Name

ef7c24494224a7f0c528edf7b27c942d18933d0fc775222dd5fffd8b6256736b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ef7c24494224a7f0c528edf7b27c942d18933d0fc775222dd5fffd8b6256736b']

Name

b26458a0b60f4af597433fb7eff7b949ca96e59330f4e4bb85005e8bbcfa4f59

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b26458a0b60f4af597433fb7eff7b949ca96e59330f4e4bb85005e8bbcfa4f59']

Name

8d7c5ab5b2cf475a0d94c2c7d82e1bbd8b506c9c80d5c991763ba6f61f1558b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8d7c5ab5b2cf475a0d94c2c7d82e1bbd8b506c9c80d5c991763ba6f61f1558b0']

Name

710a9d2653c8bd3689e451778dab9daec0de4c4c75f900788ccf23ef254b122a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '710a9d2653c8bd3689e451778dab9daec0de4c4c75f900788ccf23ef254b122a']

Name

29bd4fa1fcf4e28816c59f9f6a248bedd7b9867a88350618115efb0ca867d736

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29bd4fa1fcf4e28816c59f9f6a248bedd7b9867a88350618115efb0ca867d736']

Name

38.6.173.11

Description

- **Zip Code:** N/A - **ISP:** Cnservers LLC - **ASN:** 40065 - **Organization:** Cnservers LLC - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 38.6.173.11 - **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:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.0544014 - **Longitude:** -118.24410248

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.6.173.11']

Name

193.29.13.179

Description

- **Zip Code:** N/A - **ISP:** Bunea TELECOM - **ASN:** 42397 - **Organization:** Bunea TELECOM - **Is Crawler:** False - **Timezone:** Europe/Bucharest - **Mobile:** False - **Host:** 193.29.13.179 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RO - **Region:** Bucuresti - **City:** Bucharest - **Latitude:** 44.43230057 - **Longitude:** 26.10606956

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.29.13.179']

Name

195.80.148.18

Description

- **Zip Code:** N/A - **ISP:** EstNOC-Global - **ASN:** 206804 - **Organization:** EstNOC OY - **Is Crawler:** False - **Timezone:** Asia/Taipei - **Mobile:** False - **Host:** 195.80.148.18 - **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:** TW - **Region:** Taipei City - **City:** Taipei - **Latitude:** 25.05039978 - **Longitude:** 121.53240204

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.80.148.18']

Vulnerability

Name
CVE-2024-0204
Name
CVE-2024-21762
Description
Fortinet FortiOS contains an out-of-bound write vulnerability that allows a remote unauthenticated attacker to execute code or commands via specially crafted HTTP requests.
Name
CVE-2023-22527
Description
Atlassian Confluence Data Center and Server contain an unauthenticated OGNL template injection vulnerability that can lead to remote code execution.

Malware

Name
XMRigCC

Name
Sliver

Attack-Pattern

Name
/etc/passwd and /etc/shadow
ID
T1003.008
Description
Adversaries may attempt to dump the contents of `/etc/passwd` and `/etc/shadow` to enable offline password cracking. Most modern Linux operating systems use a combination of `/etc/passwd` and `/etc/shadow` to store user account information including password hashes in `/etc/shadow`. By default, `/etc/shadow` is only readable by the root user.(Citation: Linux Password and Shadow File Formats) The Linux utility, unshadow, can be used to combine the two files in a format suited for password cracking utilities such as John the Ripper:(Citation: nixCraft - John the Ripper) `# /usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db`
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

Unix Shell

ID

T1059.004

Description

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution. (Citation: DieNet Bash)(Citation: Apple ZShell) Unix shells can control every aspect of a system, with certain commands requiring elevated privileges. Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during

lateral movement such as with [SSH](https://attack.mitre.org/techniques/T1021/004). Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Account Discovery

ID

T1087

Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Name

Setuid and Setgid

ID

T1548.001

Description

An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively.(Citation: setuid man page) Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications (i.e. [Linux and Mac File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222/002)). The `chmod` command can set these bits with bitmasking, `chmod 4777 [file]` or via shorthand naming, `chmod u+s [file]`. This will enable the setuid bit. To enable the setgid bit, `chmod 2775` and `chmod g+s` can be used. Adversaries can use this mechanism on their own malware to make sure they're able to execute in elevated contexts in the future.(Citation: OSX Keydnap malware) This abuse is often part of a "shell escape" or other actions to bypass an execution environment with restricted permissions. Alternatively, adversaries

may choose to find and target vulnerable binaries with the setuid or setgid bits already enabled (i.e. [File and Directory Discovery](https://attack.mitre.org/techniques/T1083)). The setuid and setguid bits are indicated with an "s" instead of an "x" when viewing a file's attributes via `ls -l`. The `find` command can also be used to search for such files. For example, `find / -perm +4000 2>/dev/null` can be used to find files with setuid set and `find / -perm +2000 2>/dev/null` may be used for setgid. Binaries that have these bits set may then be abused by adversaries.(Citation: GTFOBins Suid)

Name

Active Scanning

ID

T1595

Description

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction. Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.(Citation: Botnet Scan)(Citation: OWASP Fingerprinting) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections

that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Sector

Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Url

Value
http://38.6.173.11/xmrigCC-3.4.0-linux-generic-static-amd64.tar.gz

IPv4-Addr

Value
103.159.133.23
193.29.13.179
195.80.148.18
38.6.173.11

StixFile

Value
fdfbfc07248c3359d9f1f536a406d4268f01ed63a856bd6cef9dccb3cf4f2376
ef7c24494224a7f0c528edf7b27c942d18933d0fc775222dd5fffd8b6256736b
b26458a0b60f4af597433fb7eff7b949ca96e59330f4e4bb85005e8bbcfa4f59
8d7c5ab5b2cf475a0d94c2c7d82e1bbd8b506c9c80d5c991763ba6f61f1558b0
710a9d2653c8bd3689e451778dab9daec0de4c4c75f900788ccf23ef254b122a
29bd4fa1fcf4e28816c59f9f6a248bedd7b9867a88350618115efb0ca867d736

External References

- https://www.rapid7.com/blog/post/2024/02/15/rce-to-sliver-ir-tales-from-the-field/
- https://otx.alienvault.com/pulse/65cf4b438c3b886f23ead1b9