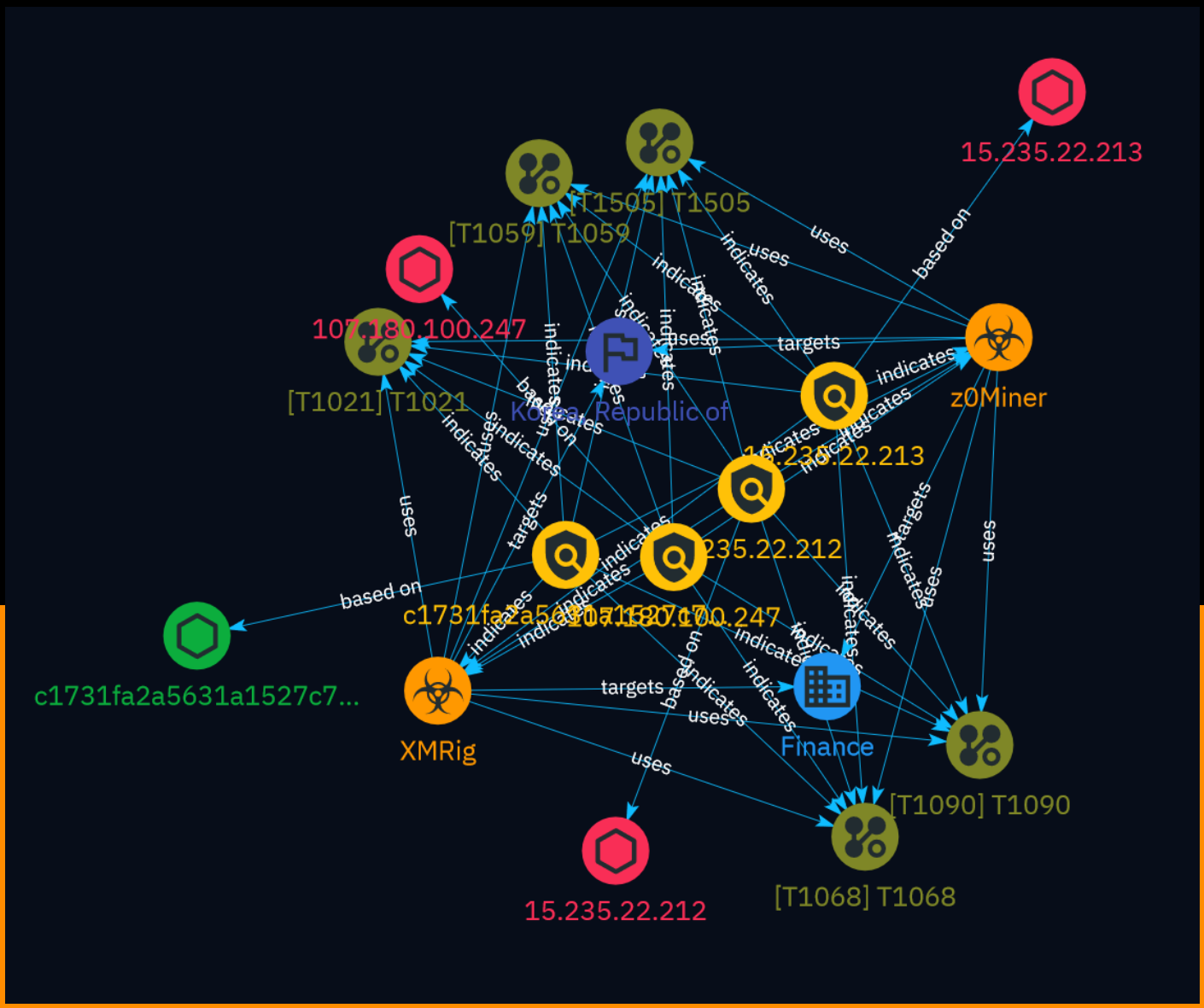
Mar 08 2024

NETMANAGEIT

# Intelligence Report

# z0Miner Exploits Korean Web Servers to Attack WebLogic Server



# Table of contents

## Overview


- Description 4
- Confidence 4
- Content 5


## Entities


- Indicator 6
- Malware 9
- Attack-Pattern 10
- Country 14
- Sector 15


## Observables


- IPv4-Addr 16
- StixFile 17

# External References


- External References 18

# Overview

## Description

AhnLab Security intelligence Center (ASEC) has discovered numerous instances of threat actors attacking vulnerable Korean servers. This post examines a recent case in which the 'z0Miner' threat actor targeted Korean WebLogic servers. The actor has a history of distributing miners against vulnerable servers and is known for exploiting WebLogic server vulnerabilities.

## Confidence

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

100 / 100

# Content

N/A

# Indicator

**Name**

15.235.22.213

**Description**

- **Zip Code:** N/A - **ISP:** OVH SAS - **ASN:** 16276 - **Organization:** OVH SAS - **Is Crawler:** False - **Timezone:** America/Toronto - **Mobile:** False - **Host:** ip213.ip-15-235-22.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:** CA - **Region:** Quebec - **City:** Terrebonne - **Latitude:** 45.70000076 - **Longitude:** -73.7519989

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '15.235.22.213']

**Name**

c1731fa2a5631a1527c77494eb353340ba57868902215f151147410353bbd0e6

**Description**

SHA256 of 98e167e7c2999cbea30cc9342e944a4c

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'c1731fa2a5631a1527c77494eb353340ba57868902215f151147410353bbd0e6']

**Name**

15.235.22.212

**Description**

- **Zip Code:** N/A - **ISP:** OVH SAS - **ASN:** 16276 - **Organization:** OVH SAS - **Is Crawler:** False - **Timezone:** America/Toronto - **Mobile:** False - **Host:** ip212.ip-15-235-22.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:** CA - **Region:** Quebec - **City:** Terrebonne - **Latitude:** 45.70000076 - **Longitude:** -73.7519989

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '15.235.22.212']

**Name**

107.180.100.247

## Description

- **Zip Code:** N/A - **ISP:** GoDaddy.com, LLC - **ASN:** 400754 - **Organization:** Go-daddy-com-llc - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 247.100.180.107.host.secureserver.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:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.0469017 - **Longitude:** -77.49030304

## Pattern Type

stix

## Pattern

[ipv4-addr:value = '107.180.100.247']

# Malware

| Name |
| --- |
| z0Miner |

| Name |
| --- |
| XMRig |

# Attack-Pattern

| Name |
| --- |
| T1505 |
| **ID** |
| T1505 |
| **Description** |
| Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW) |
| **Name** |
| T1068 |
| **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**

T1059

**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**

T1090

**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**

T1021

**ID**

T1021

## Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

# Country

| Name |
| --- |
| Korea, Republic of |

# Sector

| Name |
| --- |
| Finance |
| **Description** |
| Public and private entities involved in the allocation of assets and liabilities over space and time. |

# IPv4-Addr

| Value |
| --- |
| 15.235.22.213 |
| 15.235.22.212 |
| 107.180.100.247 |

# StixFile

| Value |
| --- |
| c1731fa2a5631a1527c77494eb353340ba57868902215f151147410353bbd0e6 |

# External References

- https://asec.ahnlab.com/en/62564/
- https://otx.alienvault.com/pulse/65eb43b73126f426dbb1e92b