Analysis of Active Kthmimu Mining Trojans

Time: May 27, 2022 Source: Antiy CERT

1 Overview

Since March 2022, Antiy CERT has successively captured attack samples of the Kthmimu mining Trojan, which is mainly spread through the Log4j 2 vulnerability. Since the exposure of the Log4j 2 vulnerability, the Trojan has been active in mining activities. At the same time, it has spread malicious scripts to both Windows and Linux platforms, and downloaded the Monero mining program for mining.

The mining Trojan uses a PowerShell script to download and execute the Monero open source mining program XMRig on the Windows platform. In addition, the script also has the functions of creating scheduled task persistence, judging that the system user contains key strings, and creating scheduled tasks. On the Linux platform, the Trojan uses a shell script to download mining programs, and the script also clears competing mining programs, downloads other scripts, and creates scheduled tasks.

It has been verified that the Windows and Linux versions of the Antiy Zhijia Terminal Defense System (IEP) can effectively detect and kill the mining Trojan.

2. ATT&CK mapping map corresponding to the event

The attacker launched a mining Trojan on the target system, and the ATT&CK mapping map corresponding to this attack event is shown in the following figure.

Figure 2-1 ATT&CK mapping map corresponding to events

The technical points used by attackers are shown in the following table:

Table 2-1 ATT&CK technical behavior description table corresponding to events

ATT&CK Stage / Category	specific behavior	Notes
reconnaissance	Active scan	Scan for log4j 2 vulnerabilities
initial visit	Leverage public-facing applications	Leverage public-facing applications such as Java
implement	Utilize command and script interpreters	Using PowerShell and Shell Scripting
	利用Windows管理规范（WMI）	删除现有WMI类的实例
持久化	利用计划任务/工作	设置计划任务
防御规避	混淆文件或信息	使用Base64进行混淆
发现	发现系统所有者/用户	判断系统用户名
	发现进程	发现竞品进程
影响	资源劫持	利用系统CPU资源

3.攻击流程和传播途径

3.1 攻击流程

Kthmimu挖矿木马在Windows平台中使用名为“lr.ps1”的PowerShell脚本执行主要功能，具体功能为下载挖矿程序和配置文件，删除现有Windows Management Instrumentation (WMI)类的实例，判断系统用户名中是否包含“SYSTEM”字符串，如果包含，使用PowerShell命令下载字符串，执行后续指令。如果不包含“SYSTEM”字符串，创建名为“log4”的计划任务，每隔5分钟重复一次。结束竞品进程程序，下载开源门罗币挖矿程序XMRig和配置文件并执行。在Linux平台中使用名为“lr.sh”的Shell脚本执行主要功能，具体功能为下载并执行挖矿程序、结束竞品挖矿程序和创建计划任务等。

图3-1 攻击流程

3.2 传播途径

攻击者使用Log4j 2漏洞进行传播攻击脚本，以下是Windows和Linux双平台Log4j 2漏洞利用代码。

图3-2 下载lr.ps1

图3-3 下载lr.sh

3.3 攻击事件样本整理

根据攻击事件对样本进行梳理得到如下信息：

表3-1 攻击事件样本整理

样本下载地址	详细说明
hxxp[:]//14.55.65.217:8080/a/x.exe	Windows门罗币挖矿程序
hxxp[:]//14.55.65.217:8080/a/lr.ps1	Windows恶意PowerShell
hxxp[:]//14.55.65.217:8080/a/config.json	门罗币挖矿配置文件
hxxp[:]//14.55.65.217:8080/a/x.rar	Linux门罗币挖矿程序
hxxp[:]//14.55.65.217:8080/a/lr.sh	Linux恶意Shell
hxxp[:]//14.55.65.217:8080/a/apache.sh	Linux恶意Shell

表3-2 挖矿脚本中的矿池地址和钱包地址

矿池地址	钱包地址
91.121.140.167:80	45tdM15BthJWCKScmdxF9nGKfnZJpV8jK3ZmBDUofM5fdzoXURTrb9QQeCwiNXHyvibVFqtxeWwx57FnCqL4Z3y4S4G2tTy
pool.supportxmr.com:80	

根据矿池地址记录，目前，该钱包现在平均算力约170KH/s。

图3-4 挖矿算力

4.防护建议

针对非法挖矿，安天建议企业采取如下防护措施：

1.安装终端防护：安装反病毒软件，针对不同平台建议安装安天智甲终端防御系统Windows/Linux版本；

2. Strengthen SSH password strength: Avoid weak passwords. It is recommended to use 16-bit or longer passwords, including combinations of uppercase and lowercase letters, numbers and symbols, and avoid using the same password for multiple servers;

3. Update patches in a timely manner: It is recommended to enable the automatic update function to install system patches, and vulnerable parts such as servers, databases, and middleware should update system patches in time;

4. Update third-party application patches in time: It is recommended to update third-party application patches such as Tomcat, WebLogic, JBoss, Redis, Hadoop and Apache Struts in a timely manner;

5. Enable logs: enable key log collection functions (security logs, system logs, error logs, access logs, transfer logs, and cookie logs) to provide a basis for tracking security events;

6. Host reinforcement: Penetration testing and security reinforcement of the system;

7. Deploy Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and traceability of malicious code. Antiy Ocean Exploration Threat Detection System (PTD) takes network traffic as the detection and analysis object, can accurately detect the known massive malicious code and network attack activities, and effectively discover network suspicious behaviors, assets and various unknown threats;

8. Antiy service: If you are attacked by malware, it is recommended to isolate the attacked host in time, and protect the site and wait for the security engineer to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.

It has been verified that both Windows and Linux versions of Antiy Zhijia Terminal Defense System (IEP) can effectively detect and kill the mining program.

Figure 4-1 Effective protection of Antiy Zhijia for Windows

Figure 4-2 Antiy Zhijia Linux version effectively scans and kills

5. Sample Analysis

5.1 Analysis of Windows samples

5.1.1 lr.ps1

Table 5-1 Script files

virus name	Trojan/Win32.Ymacco
original file name	lr.ps1
MD5	701EDFC11EE90B8A0D106B6FD98F5B42
File size	2.84KB (2,904 bytes)
interpreted language	PowerShell
VT首次上传时间	2022-03-06 02:22:32
VT检测结果	12/59

删除现有Windows Management Instrumentation (WMI)类的实例，判断系统用户名中是否包含“SYSTEM”字符串，如果包含，使用PowerShell命令下载字符串，执行后续指令。

图5-1 删除WMI类的实例

如果不包含“SYSTEM”字符串，创建名为“log4”的计划任务，每隔5分钟重复一次。结束竞品进程程序，下载开源门罗币挖矿程序XMRig和配置文件并执行。

图5-2 下载挖矿程序

5.2 Linux样本分析

5.2.1 lr.sh

表5-2 脚本文件

病毒名称	Trojan[Downloader]/Shell.Agent
原始文件名	lr.sh
MD5	E06704BCBED0CE2D7CADE20FA1D8A7B6
文件大小	2.09KB(2,138字节)
解释语言	Shell
VT首次上传时间	2022-03-05 22:26:41
VT检测结果	20/58

结束竞品挖矿进程。

图5-3 结束竞品挖矿程序

创建计划任务，查询重要目录下的挖矿关键字符串等信息，如果则强制结束相关进程。

图5-4 创建计划任务

下载挖矿程序和配置文件以及脚本文件并执行，最后删除脚本文件。

图5-5 下载挖矿程序和配置文件

5.2.2 apache.sh

结束竞品程序，独占系统资源。

图5-6 结束竞品进程

6.IoCs

IoCs
3EDCDE37DCECB1B5A70B727EA36521DE
701EDFC11EE90B8A0D106B6FD98F5B42

BF9CC5DF6A9FF24395BD10631369ACBF

D6E55C081CCABD81E5DE99ABFE9597F4

135276572F4C6A8B10BD31342997B458

E06704BCBED0CE2D7CADE20FA1D8A7B6

639825B85E02E6B9DFFCA50EE4DE9B6B

56BB7858F60C026DF6D48C32099EA2E7

14.55.65.217

14.55.65.199

91.121.140.167

pool.supportxmr.com:80

hxxp[:]//14.55.65.217:8080/a/x.exe

hxxp[:]//14.55.65.217:8080/a/lr.ps1

hxxp[:]//14.55.65.217:8080/a/config.json

hxxp[:]//14.55.65.217:8080/a/lrr.txt

hxxp[:]//14.55.65.217:8080/a/x.rar

hxxp[:]//14.55.65.217:8080/a/lr.sh

hxxp[:]//14.55.65.217:8080/a/apache.sh