Campaign Report

Infection chain analysis

(1) Downloaded Trojan

The XMI download file (detected by Trend Micro as Trojan.Linux.MALXMR.USNELH820) is a Bash script, shown in Figure 2, that moves laterally to other hosts in the same container network using information from */.ssh/known_hosts*.

(2) Persistence & Dropper

The commands shown in Figure 3 download and execute the XMI Bash script and a Python script named "d.py" (Trojan.Python.MALXMR.D).

(3) Coinminer

We detect the cryptocurrency-mining payload, whose download script is shown in Figure 8, as Coinminer.Linux.MALXMR.UWELD. Interestingly, the cryptocurrency wallet used by the threat actors is the same one used in campaigns that exploited vulnerabilities such as CVE-2019-3396, a Confluence vulnerability, and CVE-2017-5638, an Apache Struts vulnerability. According to a report by Tencent Security, the 8220 mining group, a criminal gang based in China, is behind the campaign that exploited CVE-2017-5638.

(4) DDoS bot

In addition, the attack drops another payload in the form of a DDoS bot (Backdoor.Linux.KAITEN.AMV) as shown in Figure 9.

News Report

Intelligence | Internet of Things | Laws and regulations | Malware | Mobile | Terrorism | ICS-SCADA | EXTENDED COOKIE POLICY

A new variant of the AESDDoS bot is exploiting a recent vulnerability in the Atlassian collaborative software Confluence.

Cite and state events from another report

Security experts at Trend Micro have spotted a new variant of AESDDoS botnet that is exploiting a recently discovered vulnerability in the Atlassian collaborative software Confluence.

The flaw exploited in the attacks, tracked as CVE-2019-3396, is a server-side template injection vulnerability that resides in the Widget Connector macro in Confluence Server.

Threat actors leverage the vulnerability to install denial of service (DDoS) malware and crypto-currency miners, and to remotely execute code.

"In our analysis, we saw that an attacker was able to exploit CVE-2019-3396 to infect machines with the AESDDoS botnet malware." reads the analysis published by Trend Micro. "A shell command was remotely executed to download and execute a malicious shell script (Trojan.SH.LODEX.J), which in turn downloaded another shell script (Trojan.SH.DOGOLOAD.J) that finally installed the AESDDoS botnet malware on the affected system."