資財三乙 108AB0723 詹佩庭

Kaseya 駭客攻擊事件

事件簡述：

Kaseya 是一家為管理服務商（MSP）和 IT 公司提供 IT 管理軟體的公司，Kaseya 在 7 月 2 日坦承遭到駭客入侵，駭客成功入侵其就地部署的 Kaseya VSA 軟體，並向 Kaseya VSA 客戶發動勒索軟體攻擊，根據 Kaseya 的估計，只有不到 60 家 Kaseya VSA 客戶直接遭到波及，牽連了接近 1,500 家的下游廠商。雖然 Kaseya 宣稱 VSA SaaS 並未受到影響，但為了以防萬一也將 VSA SaaS 一併下線。

Kaseya 安全漏洞：

以下為荷蘭漏洞揭露協會（Dutch Institute for Vulnerability Disclosure，DIVD）公佈相關漏洞的編號與摘要，但不包含漏洞細節。

- DCVE-2021-30116 憑證外洩漏洞
- CVE-2021-30117 資料隱碼漏洞
- CVE-2021-30118 遠端程式攻擊漏洞
- CVE-2021-30119 跨站指令碼漏洞
- CVE-2021-30120 雙因素認證繞過漏洞。
- CVE-2021-30121 本地文件包含漏洞
- CVE-2021-30201 XML 外部實體注入漏洞

駭客攻擊手法：

VSA 軟體通常用來向客戶推送軟體更新，這次被武器化來推送惡意 PowerShell 腳本，然後將 REvil 勒索病毒載入客戶系統。重要的是要注意，非 Kaseya 客戶也可能因為服務商而遭受到影響。

攻擊 Kaseya VSA 的 Sodinokibi/REvil 勒索病毒（偵測為 Ransom.Win32.SODINOKIBI.YABGC）會停用某些服務並終止正常軟體（如瀏覽器和生產力工具）相關的程序。具體來說，它會終止下列程序：

- agntsvc
- dbeng50
- dbsnmp
- encsvc
- excel
- firefox
- infopath
- isqlplussvc
- msaccess
- mspub
- mydesktopqos
- mydesktopservice
- ocautoupds
- ocomm
- ocssd
- onenote
- oracle
- outlook
- powerpnt
- sqbcoreservice
- sql
- steam
- synctime
- tbirdconfig
- thebat
- thunderbird
- visio
- winword
- wordpad
- xfssvcco

Sodinokibi 偵測到作業系統語系為下列任何一種語言，則會自行終止：

- Arabic – Syria
- Armenian Eastern
- Azeri Cyrillic
- Azeri Latin
- Belarusian
- Georgian
- Kazakh
- Kyrgyz Cyrillic
- Romanian – Moldova
- Russian
- Russian – Moldova
- Syriac
- Tajik
- Tatar
- Turkmen
- Ukranian
- Uzbek Cyrillic
- Uzbek Latin

***REvil 勒索病毒被認為是 GandCrab 的後繼任，以針對高知名受害者和採用雙重勒索策略迫使受害者支付贖金而聞名。**

安全建議：

因為勒索病毒可能具備多重進入點和加密功能，所以企業必須擁有良好的備份策略和多層次安全防護來保衛其網路並保護其關鍵業務資料：

- 電子郵件和網頁防護技術能夠封鎖垃圾郵件和惡意連結來防止勒索病毒進入你的網路。
- 伺服器防護技術能夠保護伺服器抵禦漏洞攻擊。
- 網路防護技術能夠防止勒索病毒從伺服器散播到端點或在端點間散播來保護你的網路。
- 端點防護技術可以防止勒索病毒執行來保護端點系統。