關於 Kaseya 勒索軟體供應鏈攻擊：您所應該知道的事

針對用於向數百個組織提供 REvil 勒索軟件的 MSP 軟體的供應鏈攻擊

威脅獵手團隊
賽門鐵克

2021年7月5日*更新：我們的部落格已更新，提供了有關勒索軟體如何執行的更多詳細信息以及其他保護訊息。*

在涉及Kaseya VSA軟體和使用它的多個託管服務提供商(MSP)的供應鏈攻擊中，數百個組織成為REvil（又名Sodinokibi）勒索軟體的目標。昨天（7月3日星期五）爆出攻擊的消息，促使Kaseya公司建議其VSA客戶關閉他們的VSA伺服器以防止他們受到損害。這次攻擊的時間又恰逢美國7月4日的假期週末，所以有許多組織可能人員不足。

賽門鐵克客戶是否受到保護？

是的，Symantec Endpoint產品會主動阻止用於在這一波攻擊中傳輸勒索軟體負載的工具。

有多少個組織受到影響？

據Kaseya稱，只有很少部分客戶受到影響，“目前估計全球不到40家”。但是，這些組織中的每一個都可能是擁有多個客戶的MSP供應商。目前的報告顯示有數百名受害者。

在此攻擊期間，REvil 是如何傳送到電腦的？

雖然用於破壞Kaseya VSA伺服器端的漏洞尚未完全披露，目前已知，攻擊者向Kaseya VSA客戶端傳送了一個惡意批次指令碼和一個名為 agent.crt的ASCII PEM。下載器偽裝在ASCII PEM檔案中，該檔案嘗試禁用Microsoft Defender後，再使用certutil進行解碼。它下載並利用了兩個資源，一個是舊的但合法的Windows Defender(MsMpEng.exe)拷貝版本，另一個則為自定義惡意載入程序。下載器將這兩個檔案寫入磁碟並執行 MsMpEng.exe，然後執行載入並匯出自定義的mpsvc.dll。

攻擊的動機是什麼？

REvil攻擊通常是出於金錢動機。然而，有一些跡象表明，這些攻擊可能是出於政治動機的破壞。有些例子表明攻擊者在選擇目標時似乎有政治動機。

在這次攻擊中，有些惡意程式的某些字串提到了喬・拜登總統、前總統唐納德・川普和Black Lives Matter。攻擊者要求45,000美元的贖金，這也有可能是對美國第45任總統川普的另一次相關。

此外，REvil的 Tor支付網站在撰寫本文時已關閉，這意味著受害者將無法支付贖金。該組織是否遇到技術困難，或者是否從未打算收取贖金尚不清楚。

什麼是 REvil/Sodinokibi ？

REvil（檢測為Ransom.Sodinokibi）是一個勒索軟體家族，由賽門鐵克稱為Leafroller的網路犯罪組織開發。勒索軟體用於有針對性的攻擊，攻擊者試圖對受害者網路上的所有電腦進行加密，以期勒索大筆贖金。眾所周知，該組織會在加密之前竊取受害者資料，並威脅除非支付贖金不然就公布該些資料，。

Leafroller是營運中最成熟和最多產的目標勒索軟體組織之一。在開發REvil之前，該組織與一個名為Gandcrab較老的勒索軟體家族有關。目前已知，Leafroller經營勒索軟體即服務，將其工具套裝出售給稱為附屬公司的合作者，以獲取他們勒索的贖金。

防護／緩解

已運行Symantec Endpoint產品的電腦上會檢測並阻止與這些攻擊相關的工具。

檔案防護的特徵碼：

- Downloader
- Heur.AdvML.C
- Packed.Generic.618
- Ransom.Sodinokibi
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於網路的防護：

- Ransom.Gen Activity 29
- Audit: Ransom.Gen Activity 55

各項入侵指標

d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e - Dropper

df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e - Dropper

dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f - Dropper

aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7 - Dropper

66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8 - Dropper

81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471 - Dropper

1fe9b489c25bb23b04d9996e8107671edee69bd6f6def2fe7ece38a0fb35f98e - Dropper

8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd - Sodinokibi

e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2 - Sodinokibi

d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20 - Sodinokibi

d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f - Sodinokibi

cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6 - Sodinokibi

0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402 - Sodinokibi

8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f - Sodinokibi

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址:https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/kaseya-ransomware-supply-chain
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2021/07

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有IT Team的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的IT Team，經由常態性的教育訓練、精簡的快速手冊以及標準SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入Symantec解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保安資訊：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588