保安資訊--本周(2021/09/03)
賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠的首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業與經驗，來創造賽門鐵克解決方案的最大效益，落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的一些努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您知道自己已受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 **保安資訊有限公司** | 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。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處

賽門鐵克的入侵預防系統(IPS)是業界一流的深層封包檢測技術引擎，可保護包括財富500 強企業和消費者在內的數億個端點(桌機/筆電/伺服主機)。

在過去的 7 天內，SEP 的網路層保護引擎(IPS) 在 130 萬個受保護端點上總共阻止了2.078 億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：

- 在31萬1,000台端點上，阻止了9,480萬次嘗試掃描Web服務器的漏洞。
- 在58萬4,600台端點上，阻止了4,960萬次嘗試利用的Windows作業系統漏洞的攻擊。
- 在9萬9,200台Windows伺服主機上，阻止了2,290萬次攻擊。
- 在25萬9,800端點上，阻止了1,920萬次嘗試掃描伺服器漏洞。
- 在12.78萬台端點上，阻止了840萬次嘗試掃描在CMS漏洞。
- 在16萬台端點上，阻止了480萬次嘗試利用的應用程式漏洞。
- 在36萬4,700台端點上，阻止了710萬次試圖將用戶重定向到攻擊者控制的網站的攻擊。
- 在6,600台端點上，阻止了430萬次加密貨幣挖礦攻擊。
- 在64,700台端點上，阻止了450萬次向惡意軟體C&C連線的嘗試。
- 在11,500台端點上，阻止了38萬5,400次加密勒索嘗試。

強烈建議用戶在桌機/筆電/伺服主機上啟用 IPS (不要只把 SEP/SES 當成一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲的最快最有效的協助。

2021/09/03

好工具拿來做壞事又一樁！常用的滲透測試工具--Metasploit，也被用於加密貨幣挖掘攻擊活動

多年來常使用於滲透測試及反派團隊(Red Team)演練的 Metasploit 滲透測試平台。但也被網路犯罪分子用作其攻擊鏈的一部分。 最近有報導稱，某組織使用流行的測試框架 Metasploit 及其後門模組 (Meterpreter) 部署加密貨幣挖礦。

賽門鐵克已於第一時間提供有效的保護功能，並以下述的命名及對應的防護機制來提供具體說明。

檔案型(基於病毒定義檔)防護：

- Meterpreter
- Trojan.Gen.MBT

2021/09/02

最近觀察到的惡意垃圾郵件活動，會派送被稱為：MassLogger訊息盜取器(infostealer)，正在瞄準攻擊目標

MassLogger 是一種透過地下論壇分發的廉價且易於獲得的訊息盜取器(infostealer)。最近在 8 月觀察到的惡意垃圾郵件活動，似乎很有可能是發動目標攻擊初期的釣餌派送。

惡意垃圾郵件活動，利用看似合法的商業通信，以緊急訂單或緊急事件誘騙受害者開啟包含在 zip 中的附加惡意可執行檔。

賽門鐵克已於第一時間提供有效的保護功能，並以下述的命名及對應的防護機制來提供具體說明。

檔案型(基於病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan Horse

郵件安全防護機制：

不管是地端自建(SMG/SMSEX)的郵件過濾/安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

2021/08/30

*地球巴庫(Earth Baku)進階持續威脅(APT)集團採用全新的載入器及後門程式

最近浮出水面的攻擊成為了頭條新聞，新的惡意軟體工具已作為*地球巴庫(Earth Baku)攻擊活動的一部分。Earth Baku 是一個進階持續威脅 (APT) 組織，也被稱為 APT41。這些攻擊主要針對太平洋地區的組織。這些工具包括 StealthMutant 和 StealthVector，它們既是shellcode載入器也是後門 ScrambleCross。相比之前滲透目標網路被發現時，該惡意軟體目前設計的更容易自定義，並使用更複雜的規避技術。

賽門鐵克已於第一時間提供有效的保護功能，並以下述的命名及對應的防護機制來提供具體說明：

檔案型(基於病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

基於網頁防護(如果您有使用WSS-地端或雲端網頁分類/過濾/安全服務)：

被發現的惡意IP及網域名稱已於第一時間收錄於不安全分類列表中。

2021/08/27

勒索軟體Hive鎖定醫療機構、缺乏相關因應措施的企業而來

賽門鐵克安全回應中心獲悉最近美國聯邦調查局(FBI)於本月中發布了緊急警報(Flash Alert)，警告有關 Hive 勒索軟體的活動。Hive 早在今年6月份就被發現，並從那時起針對各種企業和醫療保健行業發動攻擊。根據警示，Hive 採用網路釣魚電子郵件以及對受害者網路中有漏洞的 RDP 存取進行散播。這種勒索軟體背後的入侵者利用「雙重敲詐手段」，不僅盜竊機密資料，並威脅受害者在贖金要求得不到滿足時，將這些資料公諸於世。

賽門鐵克已於第一時間提供有效的保護功能，並以下述的命名及對應的防護機制來提供具體說明：

檔案型(基於病毒定義檔)防護：

- Downloader
- Heur.AdvML.B
- Ransom.Hive
- Trojan Horse
- Trojan.Gen.MBT
- Behavior-based
- SONAR.RansomHive!g1
- SONAR.RansomHive!g2

網路層(IPS)防護：

- Attack: Ransom.Gen Activity 29

2021/08/26

在最新的攻擊活動中觀察到的「Karma」勒索軟體

最近，我們知道了被稱爲「Karma」的勒索軟體變種的惡意活動正在流行。惡意軟體加密受害者的檔案，並在檔案中新增.karma副檔名。KARMA-ENCYPTED.txt 贖金說明被放在受害者電腦上的各種目錄中。威脅者建議受害者透過贖金通知單上記載的電子郵件地址與他們聯繫。他們還威脅說，如果不滿足贖金要求，將公開泄露機密資料。

賽門鐵克已於第一時間提供有效的保護功能，並以下述的命名及對應的防護機制來提供具體說明：

檔案型(基於病毒定義檔)防護：

- Heur.AdvML.C
- Heur.AdvML.M
- Ransom.Gen
- Trojan Horse
- WS,Malware.1

基於行為偵測技術(Snoar)的防護：

- SONAR.RansomKarma!g1
- SONAR.Ransomware!g12