保安資訊--本周(台灣時間2022/11/11)賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠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知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並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，確保您已知道自己受到最佳的保護。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(以下皆為美國時間)

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)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 87 萬 9,400 台受保護端點上總共阻止了1.186億次攻擊。這些攻擊中有 87% 在感染階段前就被有效阻止：**(2022/11/08)**

- 在**13萬3,200**台端點上，阻止了**5,010**萬次嘗試掃描**Web**服務器的漏洞。
- 在**31萬3,800**台端點上，阻止了**2,270**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬7,700**台**Windows**伺服主機上，阻止了**2,010**萬次攻擊。
- 在**8萬1,200**端點上，阻止了**350**萬次嘗試掃描伺服器漏洞。
- 在**3萬900**台端點上，阻止了**150**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬9,600**台端點上，阻止了**210**萬次嘗試利用的應用程式漏洞。
- 在**31萬7,700**台端點上，阻止了**790**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3,100**台端點上，阻止了**101**萬次加密貨幣挖礦攻擊。
- 在**4萬5,900**台端點上，阻止了**500**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,300**台端點上，阻止了**14萬9,300**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得最快最有效的協助。

2022/11/10

Earth Longzhi進階持續威脅組織(APT)，利用自定義載入程式將Cobalt Strike部署到企業

據報導，Earth Longzhi 進階持續威脅組織(APT)（已知是 APT41 的一個分支組織）利用自定義版本的載入程式來部署 Cobalt Strike 有效籌載。至少自 2020 年以來，該組織在各種攻擊行動過程中一直針對烏克蘭、台灣、馬來西亞、泰國和菲律賓的企業。根據正在發動中的攻擊行動研判，攻擊者一直在部署不同版本的 Cobalt Strike 載入程式和其他一些定制型的駭客工具。一些已被發現的載入程式包含 CroxLoader、Symatic Loader、BigpipeLoader 和 OutLoader。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!g226
- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm1
- Hacktool.Mimikatz
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- Heur.AdvML.C

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)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/11/10

惡意程式與時俱進～利用星際檔案系統(IPFS)網路的惡意軟體家族：Agent Tesla 和 Hannabi Grabber

星際檔案系統 (IPFS) 是一個分散式的點對點超媒體傳輸協議，目的是要建立分散式共用檔案的網路協定。最近觀察到，IPFS 網路越來越被各種威脅者濫用，目的是代管和傳遞惡意軟體。在最近利用 IPFS 的攻擊行動中看到的兩個不同的惡意軟體家族是 Agent Tesla 和 Hannabi Grabber。觀察到的攻擊行動傾向於使用指向 IPFS 網路上代管的有效籌載的網路釣魚鏈接或透過惡意垃圾郵件傳播的惡意軟體載入程式，這些惡意軟體載入程式從 IPFS 網路內的存儲空間下載有效籌載。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Downloader!gen8
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

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)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/11/09

重磅回歸～IceXLoader 惡意軟體以新變種回歸

IceXLoader 是用 Nim 程式語言撰寫的下載器(惡意軟體的一種)，最初於 2022 年 6 月被發現。它通常用於攻擊鏈的第二或第三階段，以下載和部署額外的惡意軟體籌載。根據最近一份報告，在真實網路環境發現一個新的 IceXLoader 3.3.3 版本。除了下載有效籌載外，IceXLoader 還建立持久性並收集有關受感染主機的各種系統參數，包括作業系統版本、IP 地址和硬體資訊等。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen66
- SONAR.SuspDataRun
- SONAR.SuspDrop!gen1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

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)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/11/09

鎖定特定語系的～Yashma-Chaos 勒索軟體新變種

Yashma 是一種 Chaos 勒索軟體變種，於 2022 年 5 月左右首次出現。根據最近的報導，最新版本的 Yashma 最近已經在真實網路環境傳播。眾所周知，Yashma 二進製檔案是透過在今年初在幾個地下論壇上洩露的 Chaos 勒索軟體產生器產出。Yashma 包含在執行前檢查受感染機器的作業系統語系的功能。如果該語系在攻擊者預先設定的排外(不攻擊)名單中，則惡意軟體將在執行此檢查時中止執行。Yashma 能夠刪除受感染端點上的本地備份和陰影複製 (shadow copies)。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen625
- SONAR.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/11/09

Dagon Locker 勒索軟體

Dagon Locker 勒索軟體，其程式碼與 MountLocker 和 Quantum 勒索軟體有很強的相似性。該惡意軟體以勒索軟體即服務的形式出售。Dagon 能夠在進行檔案加密之前終止系統程序和服務。檔案被加密後會被附加 “.dagoned” 的副檔名。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.Ransomware!g3
- SONAR.Ransomware!g7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Quantum
- Trojan.Gen.2
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

2022/11/08

安卓行動平台遠端存取木馬(RAT) 用於攻擊印度國防人員

Spymax 遠端存取木馬(RAT) 的種變最近被用於攻擊印度國防人員。Spymax 遠端存取木馬(RAT)程式碼是公開的，因此獲得多個駭客集團和個人青睞。國防人員被透過 WhatsApp 社交軟體 的促銷信引誘，然後被誘騙安裝假冒的 PDF 閱讀器應用程式(APP)。隨後，該惡意應用程式(APP)將獲得對該裝置的存取權，得以收集和洩漏機敏資訊，足以危及國家安全。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Android.Reputation.1
- Android.Reputation.2

2022/11/08

HardBit 勒索軟體

在過去的幾週裡，另一個名為 HardBit 的勒索軟體集團一直以鎖定非個人的組織單位為目標。該威脅者沒有在贖金說明中標註贖金金額，而是提示受害者透過電子郵件或 Tox 聊天軟體與他們聯繫。與許多其他勒索軟體威脅一樣，他們只接受比特幣作為付款方式。此時，經典的雙重勒索策略（洩露或出售被盜檔案）似乎沒有被採用，如果受害者不付款，它們會鍥而不捨地一再攻擊。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Scr.Malcode!gdn32

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/08

他山之石可以攻錯，手機金融服務請小心～多個手機行動惡意軟體家族針對印度的銀行用戶

據報導，最近有一大波利用簡訊(SMS)夾帶網頁鏈接的網路釣魚攻擊行動，針對印度的銀行用戶。這些攻擊會散播各種行動惡意軟體家族，包括 Elibomi、FakeReward、AxBanker、IcRAT 和 IcSpy。策動該威脅行動的威脅者假冒與印度幾家知名銀行的官方網站極為相似的網路釣魚網站。被散播的的惡意軟體酬載具有收集和外洩用戶資訊，包括銀行憑證和信用卡資訊等。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AdLibrary:Generisk
- Android.Reputation.2
- AppRisk:Generisk

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)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/11/08

RanHassan（又名 DcDcrypt）勒索軟體

RanHassan 也稱為 DcDcrypt 是另一種常見的勒索軟體家族。已知該惡意軟體於 2022 年 5 月左右首次被發現，目標是印度和各種阿拉伯語系國家的用戶。RanHassan 是用 C# 撰寫，檔案被加密後會被附加“. Enc”的副檔名。該惡意軟體的功能很陽春，沒有刪除備份／卷影副本或在受感染機器上建立任何持久性的功能。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/07

Lunar Reborn(*月球重生)竊密程式

Lunar Reborn 是另一個最近被廣為宣傳的竊密程式。賽門鐵克已經觀察到可能由多個駭客組織和個人進行的測試和惡意下載活動。該惡意軟體很簡單，並且具有常見的竊密程式功能（對 Growtopia 和 Roblox 有興趣），包括以下內容：

- 從常見的 Chromium 和 Gecko 類的瀏覽器中竊取密碼、cookie、瀏覽記錄、信用卡、自動填寫(autofills)機制的帳密等
- 竊取 Growtopia 帳戶
- 竊取 Roblox cookies(*餅乾)
- 竊取 Discord 權杖
- 竊取加密錢包
- 自我刪除

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.ProcHijack!gen8
- SONAR.SuspBeh!gen633

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/11/07

看不到與以色列有關聯～Exodus(*出埃及記)竊密程式

過去幾週，賽門鐵克觀察到與Exodus(*出埃及記)竊密程式相關的測試活動。該竊密程式最近已在用於軟體開發和版本控制的知名 Internet 託管服務上分享。Exodus 與其他最近的竊密程式非常相似，其中一些主要功能包括：

- 竊取已知的網路瀏覽器、VPN 和 FTP 密碼
- 搜尋文件和擷取螢幕畫面
- 針對加密貨幣錢包的剪貼簿竊密攻擊
- 收集系統訊息
- 鍵盤側錄
- 竊取 Steam、Uplay、Battle.Net、Minecraft 會話訊息
- 劫持 Telegram 和 Discord 帳戶

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/07

依客戶需求提升功能～BlueFox (*藍狐狸)竊密程式不時有新版本釋出

一種被稱為 BlueFox 竊密程式的最新版本正在地下論壇上做廣告。此竊密程式歸屬於Distamx駭客集團所有，以惡意軟體即服務 (Malware-as-a-Service) 的營運方式銷售。該惡意軟體會根據用戶要求和回應與互動來持續優化版本。

BlueFox Stealer 最早是在 2021 年 12 月的俄語系的地下論壇中首次出現。

新變種針對所有受歡迎的網路瀏覽器，並針對資訊和憑證盜竊以及已知的螢幕擷取和系統指紋辨識技術。它針對幾乎所有桌面加密貨幣錢包。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.Dropper!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/07

老神在在～CLOP 勒索軟體，禍害頻傳

CLOP 勒索軟體並非新的勒索軟體，事實上它至少從 2019 年就已經存在。從那以後的幾年裡，人們不斷看到它透過魚叉式網路釣魚、易受攻擊的脆弱伺服主機、RDP 暴力攻擊等多種感染媒介來針對各種規模的組織。這種威脅幕後的威脅者正在使用雙重勒索戰術，威脅如果不支付贖金，就會出售或洩露被盜的加密文件。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/07

樹大招風～網路攻擊者濫用知名軟體品牌傳播RomCom遠端存取木馬(RAT)

就在上個月，RomCom 遠端存取木馬 (RAT) 已被用於針對烏克蘭軍事基礎設施的目標式攻擊。根據最新報導，該惡意軟體幕後的威脅者也一直在濫用已知軟體品牌進行 RAT 散佈。惡意軟體植入程序被偽裝成 KeePass Password Manager、SolarWinds NPM 和 Veeam Backup and Recovery 軟體等的安裝程式。攻擊者一直在利用虛假網站和誤植網域名稱來散佈這些安裝程式。烏克蘭似乎仍然是攻擊者的主要目標，但相信英語系國家也可能是次要目標。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

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)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/11/07

尾隨在網路銀行用戶背後的-手機簡訊(SMS)竊取惡意程式

據報導，在最近的一波攻擊中，安卓平台上的手機簡訊(SMS)竊取惡意程式正鎖定印度網路銀行的客戶。惡意的安裝包 .apk 透過網路釣魚的網址(URL) 傳播，並偽裝成 HDFC 銀行應用程式來兌換積點或折扣優惠券。該惡意軟體會竊取信用卡訊息和用戶的個人詳細訊息，包括電話號碼和電子郵件地址。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AdLibrary:Generisk
- Android.Reputation.2

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)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/11/07

模組化夠靈活，老牌遠端存取木馬(RAT)：Orcus，在真實網路環境依舊活躍

Orcus 是一支眾所周知的老牌遠端存取木馬 (RAT)，最早是在 2016 年發現，並且它仍然繼續在各種真實網路環境大量被散佈。該惡意軟體具有典型的 RAT 功能，包括遠端管理、鍵盤側錄、憑證盜竊、遠端程式碼執行等等。眾所周知，Orcus 透過魚叉式網路釣魚或透過瀏覽網頁時的順道下載 (drive-by-download) 攻擊方式來傳播的。由於其模組化架構，惡意軟體可以透過客製化或下載外掛程式來進行功能強化。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen57
- SONAR.SuspBeh!gen609
- SONAR.SuspBeh!gen625
- SONAR.TCP!gen1
- SONAR.UACBypass!gen9

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Sorcurat
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Trojan.Backdoor Activity 634

2022/11/03

又是勒索軟體～Warlock Dark Army(*術士黑暗軍隊)勒索軟體

最近在網路威脅生態中發現一個名為 Warlock Dark Army 的勒索軟體威脅者。被該勒索軟體加密後，他們要求 0.1473799 比特幣的贖金來解密。與知名度更高的攻擊者不同的是，它們似乎不會在環境中橫向擴散，並且很可能透過瀏覽網頁時的順道下載 (drive-by-download) 攻擊方式來傳播或 RDP 暴力攻擊作為感染媒介。截至目前為止，使用了基於 Chaos 勒索軟體的勒索軟體變種，該集團的活躍度已經比較低。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen616
- SONAR.SuspBeh!gen625
- SONAR.SuspTempRun
- SONAR.SuspTempRun2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.CryptoTorLocker

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C