保安資訊--本周(台灣時間2023/10/13)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 66 萬 7,200 台受保護端點上總共阻止了 8,530 萬次攻擊。這些攻擊中有 88.2% 在感染階段前就被有效阻止：**(2023/10/09)**

- 在**13萬9,000**台端點上，阻止了**3,680萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**20萬4,300**台端點上，阻止了**1,510萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬6,300**台**Windows**伺服主機上，阻止了**1,530萬**次攻擊。
- 在**8萬6,700**台端點上，阻止了**290萬**次嘗試掃描伺服器漏洞。
- 在**1萬5,100**台端點上，阻止了**120萬**次嘗試掃描在**CMS**漏洞。
- 在**6萬6,900**台端點上，阻止了**150萬**次嘗試利用的應用程式漏洞。
- 在**25萬3,800**台端點上，阻止了**490萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3,000**台端點上，阻止了**200萬**次加密貨幣挖礦攻擊。
- 在**12萬3,400**台端點上，阻止了**820萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**830**台端點上，阻止了**6萬1,600**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。

2023/10/12

ToddyCat進階持續威脅(APT)駭客集團鎖定亞洲的政府機構和電信公司

據報道，一項被稱為「Stayin' Alive」的全新網路攻擊行動以鎖定亞洲的政府機構和電信公司為目標。使用的工具組和利用的基礎設施顯示與名為 ToddyCat 的進階持續威脅 (APT) 駭客集團有特定的關聯。據了解，該駭客集團曾針對知名亞洲組織發動類似的攻擊。這起「Stayin' Alive」行動，使用一組獨特的下載器和惡意後門程式，稱為 CurLog、CurLu 和 CurKeep。初始攻擊鏈是以魚叉式網路釣魚電子郵件伎倆得逞，後續被植入的有效籌載可以對受感染的端點執行偵察並向攻擊者控制的 C&C 伺服器回報。

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- 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.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!200
- Heur.AdvML.C

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

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。

2023/10/12

Lambda(*拉姆達)勒索軟體

Lambda (又稱 LambdaCrypter) 是最近發現在真實網路情境傳播的普通勒索軟體。該惡意軟體會加密使用者檔案並在被加密後的檔案冠上 .Lambda 副檔名。成功加密後，惡意軟體會以名為「LAMBDA_README.txt」的 .txt 文字檔投放勒索及贖金支付說明。攻擊者建議受害者瀏覽勒索信中提到的洋蔥加密網站，以獲取有關如何恢復加密檔案的進一步說明。

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(SONAR)的防護：

- SONAR.Ransomware!g38
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Lambda
- Trojan Horse
- Trojan.Gen.MBT
- 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：

- Attack: Ransom.Gen Activity 46
- System Infected: Trojan.Backdoor Activity 568
- System Infected: Trojan.Backdoor Activity 634

2023/10/11

老狗新把戲～LostTrust勒索軟體

LostTrust 是最近發現的勒索軟體，據信是 MetaEncryptor 惡意軟體改名後的重出江湖。該惡意軟體背後的攻擊者透過公共洩漏網站，公布受害者被攻擊的詳細資訊。LostTrust 勒索軟體會對使用者檔案進行加密，並冠上 .losttrustencoded 的副檔名。勒索與贖金支付說明是透過名為 !LostTrustEncoded.txt 的 .txt 檔案傳遞，該檔案被放置在受感染端點上的每個加密資料夾中。該惡意軟體還具有停用目標電腦上的各種程序和服務以及刪除卷影副本的功能。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomPlay!gen1
- SONAR.SuspLaunch!g190

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2023/10/11

小心！Bing的人工智慧聊天機器人被惡意廣告濫用

一些威脅者利用惡意廣告（惡意付費廣告）試圖引誘受害者下載並執行某些惡意軟體，這已經不是什麼新鮮事了。不過，現在惡意廣告可以從單純的網頁搜尋延伸到 Bing 的人工智慧 (AI) 聊天機器人，因為廣告會被注入聊天機器人對話中，這可能會讓用戶對廣告產生更強的信任感。在這種情況下，廣告是對知名搜尋引擎的虛假模仿，將毫無戒心的受害者引導到一個帶有合法工具相似頁面的錯別字／搶註域名的很相似網站。

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：

- ISB.Heuristic!gen37
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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。

2023/10/11

CVE-2023-42793 TeamCity驗證繞過漏洞被勒索軟體集團開採利用

CVE-2023-42793 是最近揭露的 JetBrains TeamCity CI／CD（持續整合和部署）伺服器中的一個驗證繞過漏洞（CVSS 評分：9.8 嚴重）。如果開採利用該漏洞，未經身份驗證的攻擊者可能會透過 HTTP(S) 存取 TeamCity 伺服器，並導致對易受攻擊的伺服器進行管理控制或進一步的遠端程式碼執行 (RCE) 攻擊。據報道，該漏洞已被各種勒索軟體犯罪集團廣泛開採利用，原廠已在產品版本 2023.05.4 中發布修補程式來解決該問題。

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：

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：

- Web Attack: TeamCity Authentication Bypass CVE-2023-42793

2023/10/11

主流IP分享器／WIFI AP都被鎖定～物聯網惡意程式：Mirai後續新變種已擴大其開採利用物聯網漏洞的範圍

被稱為 IZ1H9 的物聯網惡意程式：Mirai後續新變種已擴大其開採利用物聯網漏洞的範圍。該惡意軟體目前擴大針對各種設備，包括 D-Link 和 Netis 路由器、Sunhillo SureLine、Geutebruck IP 攝影機、Zyxel 設備、TP-Link Archer、Korenix Jetwave 無線 AP、TOTOLINK 路由器等。感染 IZ1H9 後，遭入侵的裝置將成為殭屍網路的一部分，允許攻擊者完全遠端控制，並可用於發動 DDoS 攻擊。該惡意軟體還包含一個資料區間 (Data Section)，其中包含用於暴力攻擊的出廠預先定義登入帳號與密碼。

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：

- Linux.Mirai
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1

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)：

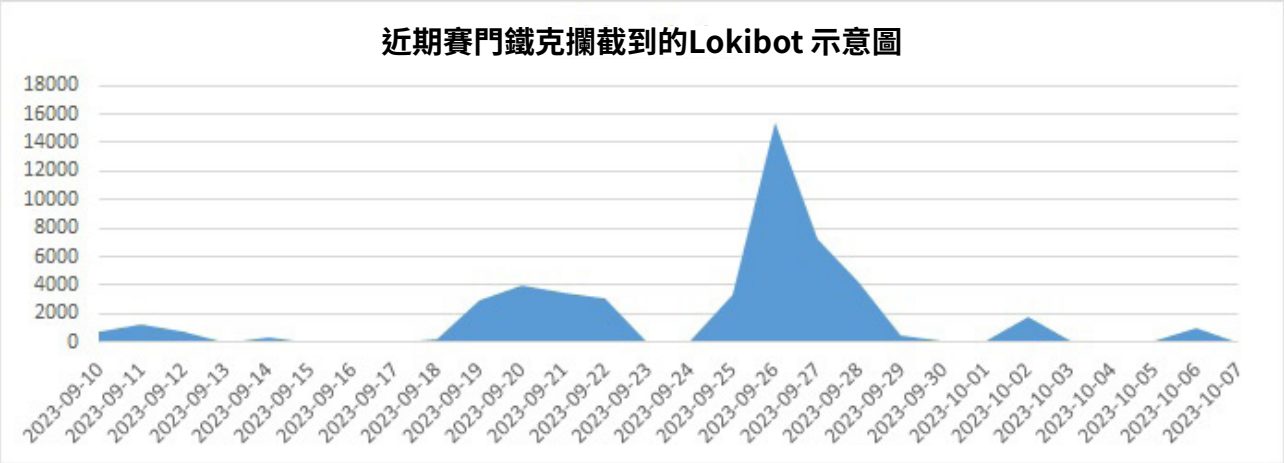
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/10/10

防護亮點：Lokibot仍然是一個危險

Lokibot 竊密程式的歷史可以追溯到 2015 年左右，至今仍然非常活躍，它透過持續發動一連串的垃圾郵件行動進行傳播，通常利用電子郵件中附加的惡意 PDF、RTF 和 Office 文件作為感染媒介，並使用報價、運輸、銀行、SWIFT、發票和支付相關的社交工程主旨，Lokibot 試圖從數百個應用程式中竊取憑證，包括瀏覽器、FTP 用戶端、電子郵件用戶端、SSH 用戶端、加密貨幣錢包和密碼管理軟體，並可能使用幾種不同的打包方法進行混淆，但最終在執行主要有效籌載之前會將其自身解壓縮到記憶體中，這通常是安全產品會攔截它的地方。

賽門鐵克最近觀察到新的攻擊行動中出現各種主旨的電子郵件，包括報價、付款確認、新合約、採購訂單等。



像往常一樣，電子郵件包含一個附件，可以是壓縮檔案（rar、gz 等）或 Microsoft Office 文件。不論是哪種狀況下，實際的 Lokibot 有效籌載的可執行檔都可以寄生在附件檔裡面。以下範例顯示一封附件包含 .gz 檔案的電子郵件--這是使用 gzip 壓縮技術壓縮的檔案。

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Lokibot
- Infostealer.Lokibot!12
- Infostealer.Lokibot!16

- Infostealer.Lokibot!22
- Infostealer.Lokibot!34
- Infostealer.Lokibot!43
- Infostealer.Lokibot!gm
- Scr.Malcode!gen59
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34
- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Exp.CVE-2017-11882!g5
- Exp.CVE-2017-11882!g6
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Web.Reputation.1
- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1
- SONAR.SuspBeh!gen667

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: Bad Reputation Process Request 4

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)。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。

2023/10/10

台灣用戶請注意：Grayling進階持續威脅(APT)駭客組織，鎖定台灣多個機構組織

Broadcom 旗下的企業安全部門：賽門鐵克的威脅獵手團隊觀察到一個前所未見的進階持續威脅 (APT) 駭客組織的行跡，並且採用自訂惡意軟體。該組織被稱為 Grayling，使用 DLL 側載技術來濫用惡意軟體進行情報收集。鎖定目標包括台灣製造業、IT 和生物醫學領域的許多組織。

對受害機器的初始存取，似乎透過利用脆弱的透通方式，在網際網路的公眾服務之基礎設施來實現。一旦在內網建立立足點，後續的活動包括部署各種有效酬載，例如：NetSky、Cobalt Strike……等。進一步觀察到的活動包括提權、網路掃描和搭配惡意程式下載器的使用。

歡迎參閱我們的部落格中文章，有更詳細的內容：前所未見的駭客組織鎖定多個台灣組織為攻擊目標

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Rozena!gen3
- Pwdump
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2023/10/09

Android 平台上的全新銀行金融木馬：GoldDigger

GoldDigger 是安卓平台上的的全新銀行金融木馬惡意軟體。最近在針對越南地區的安卓手機用戶的攻擊行動中觀察到這種惡意軟體。GoldDigger 會在受感染的裝置上濫用輔助服務，以竊取個人資料、簡訊內容、2FA 認證碼、銀行憑證／帳密以及加密貨幣應用程式和錢包中的資料……等。除此之外，該惡意軟體還具有鍵盤側錄和遠端存取功能。

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：

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.Malapp
- 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。

2023/10/09

中國間諜行動瞄準亞洲半導體產業

一項全新的間諜活動利用 Cobalt Strike 惡意軟體針對台灣、新加坡和香港的半導體公司。該間諜行動與多個中國 APT 駭客組織有聯繫。

根據最近的研究，攻擊者正在使用提及台積電 (TSMC) 的誘餌來發動攻擊。這些誘餌會導致後續的 Hyperbro 載入程式，該程式使用簽署的 CyberArk 二進位檔案透過 DLL 測載進行載入。然後使用 Hyperbro 在記憶體中執行 Cobalt Strike Beacon。

DLL 側載是一種眾所周知的技術，攻擊者將惡意 DLL 放置在預期可以找到合法 DLL 的目錄中。然後，攻擊者自己運行合法應用程式（在大多數情況下是自己安裝的）。再合法應用程式載入並執行有效的惡意籌載。

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Meterpreter
- Packed.Generic.347
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!400
- Heur.AdvML.A!500

- Heur.AdvML.A!300
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2023/10/08

以色列--哈馬斯衝突，興起「網域搶註」(typo-squatting)潮

10月7日至8日週末，以色列發生重大事件，起因於巴勒斯坦最大的激進伊斯蘭組織：哈馬斯發起的重大衝突。在過去的兩天裡，賽門鐵克觀察到 170 多個新註冊的網域名稱，這些域名似乎與捐贈、政治和衝突相關資訊有關，有些人將衝突稱為戰爭。雖然並非所有觀察到的網域都是惡意或可疑，但賽門鐵克標記可疑網域並繼續監控惡意活動。

在重大事件期間，尤其是那些引起廣泛關注的事件（例如：戰爭和其他危機）期間，網路（惡意）活動通常會激增，人們搜尋與事件相關的資訊。網路犯罪分子透過申請註冊拼字錯誤的網域來魚目混珠。這些網域的名稱與合法網站或活動類似，但包含輕微的記錯或打錯的網域名稱。當使用者在搜尋活動資訊時輸入錯誤或拼寫錯誤時，他們可能最終會造訪這些惡意網站，而不是預期中的網站。

這種伎倆允許網路犯罪分子從事各種邪惡活動，例如：傳播錯誤訊息、進行網路釣魚攻擊、捐贈詐騙或散佈惡意軟體。由於情緒高漲和獲取最新資訊的緊迫感，用戶在這段時間可能更容易受到傷害。

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。

2023/10/06

未知名的APT駭客組織，濫用DinodasRAT遠端存取後門程式，攻擊圭亞那政府機構

根據最近發布的一份報告，觀察到一個未知名的威脅組織針對圭亞那的某個政府機構發動前所未有的後門程式攻擊。報告中將這個攻擊行動稱為「*水雉行動」（Operation Jacana），所採用的遠端存取後門程式被稱為 DinodasRAT，其允許攻擊者在受感染的機器上執行多種操作。該操作包括但不限於檔案和作業系統的操弄、資料外洩、啟動反向 shell……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(SONAR)的防護：

- SONAR.TCP!gen6

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
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。

保安資訊 SAVETIME INFORMATION SECURITY