保安資訊--本周(台灣時間2023/07/07)
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 69 萬 3,100 台受保護端點上總共阻止了 8,550 萬次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2023/07/03)**

- 在**14萬1,500**台端點上，阻止了**3,710**萬次嘗試掃描**Web**服務器的漏洞。
- 在**23萬9,400**台端點上，阻止了**1,680**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬2,100**台**Windows**伺服主機上，阻止了**1,330**萬次攻擊。
- 在**9萬3,800**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬6,400**台端點上，阻止了**92萬3,100**次嘗試掃描在**CMS**漏洞。
- 在**6萬9,900**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**22萬1,700**台端點上，阻止了**530**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3,500**台端點上，阻止了**180**萬次加密貨幣挖礦攻擊。
- 在**14萬3,900**台端點上，阻止了**910**萬次向惡意軟體**C&C**連線的嘗試。
- 在**1,800**台端點上，阻止了**7萬1,800**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。

2023/07/06

德國、奧地利和瑞士正遭受Warzone 遠端存取特洛伊木馬(RAT)的威脅

Warzone (又稱AveMaria) 是一個遠端存取特洛伊木馬 (RAT)，在威脅領域出現已經有一段時間了。雖然它的流行程度沒有其他 RAT 和惡意竊密程式高，但多年來一直保持穩定的態勢。賽門鐵克經常發現在世界各地與 Warzone 有關的網路攻擊行動。

在最近的一個例子中，發現一個全新的攻擊行動，主要針對德國、奧地利、瑞士的組織以及與當地有聯繫的國際機構。這些惡意郵件聲稱是付款收據 (主旨：Überprüfen Sie den Zahlungsbeleg)，包含一個內含 Warzone RAT 的 .ARJ 壓縮檔附件。

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：

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn34

2023/07/06

一個正在嶄露頭角的勒索軟體家族：Underground Team(*地下團隊)

勒索軟體的命名有一種規則是以贖金支付說明的內容來命名，Underground Team 算是這種命名方式的勒索軟體的全新家族。該贖金支付說明似乎是針對已鎖定的目標，包括可以描述受害者的具體細節，該集團甚至在贖金支付說明中提供關於網路和資訊安全的細節或建議。當然，在最好的情況下，來自這樣的駭客集團的任何東西都應該極其謹慎以對。該勒索軟體一旦加密後不會改變檔案名稱或副檔名，但會在系統中的幾個地方置放勒索軟體贖金支付說明。

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：

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

2023/07/05

Wagner(*瓦格納)勒索軟體

瓦格納傭兵叛變的幾天後，人們發現到一個名為『瓦格納』的勒索軟體開始在俄羅斯到處傳播。當成功執行時，這個勒索軟體會在被加密檔上附加一個 .wagner 的副檔名，並將瓦格納的標誌設置為桌面背景圖案，並在遭駭人的電腦上留下一個勒索贖金支付說明檔案（Wagner.txt）。該勒索軟體是Chaos索軟體的另一個變種。

該贖金支付說明沒有提供任何解密指示或需支付贖金金額。幕後的藏鏡人猜測是受瓦格納的意識形態感招，要執行瓦格納針對俄羅斯軍方領導人的任務。該說明還包括一個可能與瓦格納的招募工作有關的聯繫號碼，以及一個 Telegram 連絡人。

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.SuspLaunch!g193

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/07/05

面對釣魚郵件與釣魚簡訊：PayPay 用戶遭受空前的網路攻擊行動

PayPay 是日本廣受歡迎的行動支付服務商，也是軟銀公司和雅虎日本公司的合資公司，它於 2018 年 10 月推出，提供使用智慧型手機的用戶進行方便和安全的無現金交易服務。

這項服務允許使用者將他們的銀行帳戶、信用卡或其他支付方式串連到該應用程式。然後，他們可以透過掃描店家的二維碼 (OR Code) 或輸入商戶的電話號碼來進行支付。該應用程式還提供一個『PayPay紅利』系統，使用者可以賺取和兌換紅利用於日後的消費扣抵。

多年來，這項服務在日本非常普及，使其成為網路犯罪分子高度覬覦的目標。最近幾個月，PayPay 網路釣魚行動有所增加，歹徒向日本消費者和企業發送多封電子郵件或簡訊。如果用戶被成功引誘，他們將被重定向到精心設計的假冒 PayPay 網站，以詐騙他們的帳號與密碼。

以下是近期釣魚信件的主旨欄內容示例：

- 【重要】PayPay銀行からのお知らせ
- PayPayお客様のアカウント認証に関するお知らせ

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：

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)。

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。

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。

2023/07/04

喬裝成由巴基斯坦國家災害管理局(NDMA)發送的電子郵件釣魚行動

使用微軟電子郵件帳號的用戶非常多，所以歹徒發動微軟電子郵件的帳號與密碼的網路釣魚行動不勝枚舉，而且每天都在伺機行動。歹徒採用各種社交工程伎倆以及網路釣魚工具。最近，有歹徒喬裝成巴基斯坦國家災害管理局 (NDMA) 發送釣魚信件，用假發票和和環球銀行金融電信協會 (SWIFT) 支付系統轉帳來引誘受害者。如果有人成功地落入圈套，被惡意郵件、HTML 或 PDF 等附件所欺騙並點擊網址，他們將被重導向到另一個釣魚頁面，要求他們使用微軟的電子郵件憑證登錄。在這次攻擊行動，歹徒主要針對的是全球的金融和能源公司。

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：

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)。

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。

2023/07/04

Neo_Net駭客組織，持續瞄準西班牙和智利的銀行，還有揮軍其他國家的跡象

根據最近的報導，一個被稱為 Neo_Net 的駭客組織自 2021 年以來就持續在發動網路犯罪行動，他們的目標是西班牙和智利的銀行客戶。他們還被觀察到正在向世界各地的其他銀行蔓延。Neo_Net 採用各種伎倆，包括透過 Ankarex（一個網路釣魚即服務的平臺）進行網路釣魚，建立虛假的網站，以及散佈惡意的手機 APP，所有這些都被用來進行金融網路釣魚活動。

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：

- AdLibrary:Generisk
- AppRisk:Generisk

2023/07/04

老而彌堅～Linux平台上的Rekoobe後門程式不時推出新功能

Rekoobe 後門程式屬於一個相對老牌的惡意軟體家族，它不時地以全新的變種重出江湖。Rekoobe 是源於開放原始碼所撰寫的 Tiny Shell 後門程式，已知主要針對 Linux 伺服器。該惡意軟體的功能包括下載任意的有效籌載，運行目標主機對攻擊者主機發起連線的 reverse shell，從攻擊者操控的 C&C 伺服器接收和執行命令，以及從遭駭入的電腦中竊取資料。該惡意軟體與被稱為 APT-31 的威脅組織有廣泛的關連，但其他駭客組織過去可能也已經在利用它。

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：

- Backdoor.Trojan
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.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。

2023/07/04

SmugX網路攻擊行動，採用HTML挾帶伎倆

SmugX 是一個全新發現的針對歐洲的大使館和外交部的網路攻擊行動。該行動顯示出與以前歸屬於 Mustang Panda 和 Red Delta 駭客組織的行動有一定程度的重疊。SmugX 採用 HTML 挾帶伎倆 (HTML smuggling)，將惡意的有效籌載隱藏在 HTML 檔案中。在感染鏈的後半段，攻擊者還利用 JavaScript、.msi 檔案和側載的 .dll 檔。該行動的最終有效籌載是 PlugX 惡意軟體，這是一個眾所周知的遠端存取木馬 (RAT)，至少自 2008 年以來就被各種高階駭客組織所採用。

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：

- Backdoor.Roboform
- JS.Downloader
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- 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。

2023/07/04

macOS平台上出現全新的RustBucket惡意軟體變種

在真實網路情境中發現，macOS 平台上的 RustBucket 惡意軟體的全新變種。該惡意軟體在2023 年 5 月初首次被報導，它的營運被歸屬於 BlueNoroff 駭客集團（也與北韓的 Lazarus 高階駭客集團有關）。該惡意軟體似乎在不斷發展，在最近的攻擊行動中，它能夠透過利用 LaunchAgents 在 MacOS 上常駐。在造駭入的系統上發現，該惡意軟體可協助駭客收集已安裝的應用程式、正在運行的程序及其狀態、當前的時間戳記等資訊，然後將收集到的資料滲出到駭客所操控的 C&C 伺服器。

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：

- OSX.Trojan.Gen
- 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)：

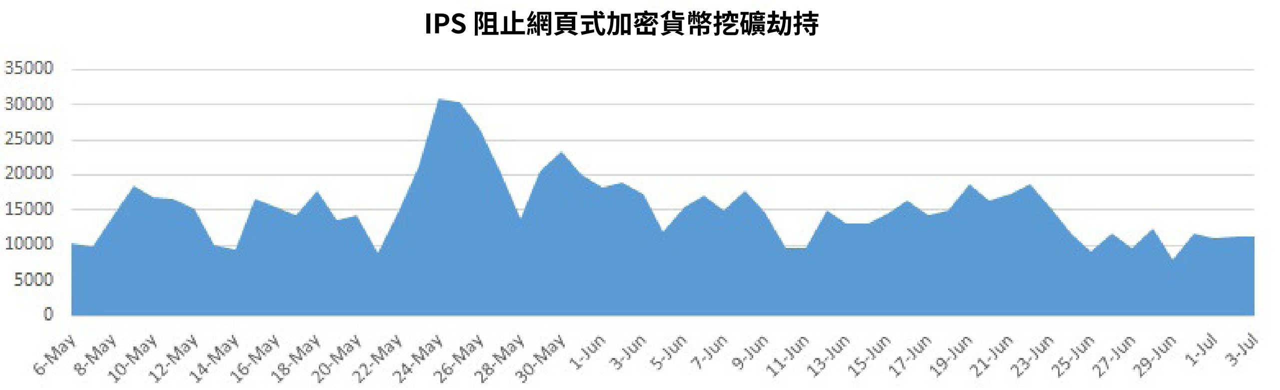
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/07/03

防護亮點：加密貨幣挖礦劫持

~ 防護亮點 ~

透過瀏覽器也可以進行加密貨幣挖礦，它是在瀏覽器核心，運行腳本語言。這種方法與更常見的加密貨幣開採程式的方法不同，後者需要下載和運行一個專用的挖礦程式。如果網頁中被注入了一個加密貨幣挖礦腳本，那麼只要瀏覽該網頁的用戶處於瀏覽狀態，他們電腦上的運算效能就會被暗中用來挖掘加密貨幣。一些網站可能改絃易轍以加密貨幣挖礦取代廣告來增加營利，只要告訴客戶在瀏覽該網站時，他們的 CPU 效能將被用於挖掘加密貨幣，這就可以。然而，一些網站在客戶不知情或不同意的情況下，暗中利用瀏覽網站的電腦或手機／筆電等行動裝置的運算資源來挖掘加密貨幣。這被稱為加密貨幣挖礦劫持。賽門鐵克每天都會阻止成千上萬的此類攻擊。



典型的藉由瀏覽器的挖礦劫持場景中，攻擊者駭入一個網站，並在網站中注入幾行 JavaScript 的惡意程式。這個被注入的惡意程式碼會讓瀏覽該網站的電腦為駭客挖掘加密貨幣 (挖礦)。門羅幣 (Monero) 就是一個可藉由瀏覽器來挖礦的典型案例，該加密貨幣使用RandomX 演算法，這是一種適用於某些 PoW 區塊鏈的演算法。從過往的案例來看，加密劫持要麼利用基於 JavaScript 的加密劫持服務，例如：2017 年引起軒然大波的 Coinhive，要麼依靠遭駭的外掛程式或惡意的瀏覽器擴充功能來提供惡意的 JavaScript。

與勒索軟體等威脅不同，勒索軟體會立即中斷受害者對其設備的存取，而加密貨幣挖礦劫持可以在受害者意識到發生什麼之前，在其設備上悄悄進行很長時間的運算效能盜用。即使是完全安裝最新修補程式的設備也可以透過基於流覽器的挖礦成為受害目標。這種加密貨幣挖礦劫持的主要影響與電腦效能有關。潛在的影響包括設備性能變慢，電池過熱，設備變得無法使用，以及在雲端運行的企業因用電量增加而導致成本增加，這些企業是根據 CPU 的使用量來收費的。此外，客戶和商譽的損失也是對網站所有者和企業的潛在影響。

一些加密劫持的案例包括：

- 2023年2月，針對 Kubernetes Cluster 進行 Dero 挖礦的加密劫持行動。
- RapperBot DDoS 惡意軟體將加密劫持作為新的收入來源。
- 暴露在網際網路上的 Linux 和物聯網（IoT）設備在暴力攻擊中被劫持，這是最近觀察到的加密劫持行動的一部分。

賽門鐵克的入侵預防系統（IPS）技術透過使用多種檢測來阻止相關的惡意網路活動，保護客戶免受基於流覽器的加密劫持，其已識別方式如下：

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: JSCoinminer Download*
- Web Attack: JSCoinminer Website*

*星號代表多個類似名稱的檢測，例如：Web Attack: JSCoinminer Download 1、Web Attack: JSCoinminer Download 2……等等。

欲瞭解更多有關於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。

2023/07/03

Atlas(*阿特拉斯)剪貼簿竊密器(Clipper)

Atlas 是一種剪貼簿竊密器 (Clipper) 惡意軟體，主要透過將受害者的加密錢包地址與攻擊者的加密錢包地址交換來劫持加密貨幣交易。Atlas 剪貼簿竊密器 (Clipper) 利用 Telegram 來進行 C&C 通訊。該惡意軟體還具有監視和終止選定系統程序的功能，例如：與惡意軟體偵測或監聽 (debugging) 等相關的程序。

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.SuspBeh!gen667

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.2
- WS.Reputation.1

基於機器學習的防禦技術：

- 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 564

2023/06/30

Manic Menagerie 2.0網路攻擊行動

Manic Menagerie 2.0 是一項針對歐盟和美國的網站代管業者和 IT 供應商之長期網路惡意攻擊行動。雖然該行動的初始時間可以追溯至 2020 年，但該駭客組織最近的活動發生在 2023 年 4 月，這證明該攻擊行動仍在繼續。Manic Menagerie 2.0 行動的目的是將 Web shell 和加密貨幣挖礦程式部署到受感染的伺服器上。注入的 web shells 可能為攻擊者提供進一步侵入的立足點，而數位貨幣挖礦程式則允許利用受感染的伺服器從中牟利。據觀察，攻擊者還利用各種自定義和兩用工具，例如：PCHunter、GoIIS、GodPotato、PetitPotam 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!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Rotpotato!g1
- Linux.Coinminer
- Trojan Horse
- Trojan.Coinbitminer
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

- Trojan.Malscript
- WS.Malware.1

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。

2023/06/30

ThirdEye(*第三隻眼)竊密程式

有報導稱在已經飽和的威脅環境中，出現一種全新的竊密程式，稱為 ThirdEye (*第三隻眼)。ThirdEye 仍在不斷發展，該惡意軟體的最新版本具有收集有關磁碟詳細資訊、卷冊資訊、已安裝的應用程式、正在運行的程序等資訊功能。然後擷取的資訊將被轉發送到攻擊者所操控的 C&C 伺服器。

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：

- Linux.Lightaidra
- Trojan Horse
- 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。