保安資訊--本周(台灣時間2023/06/16)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 75 萬 6,200 台受保護端點上總共阻止了 9,020 萬次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2023/06/11)**

- 在**15萬3,800**台端點上，阻止了**3,950**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬8,800**台端點上，阻止了**1,950**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬1,200**台**Windows**伺服主機上，阻止了**1,320**萬次攻擊。
- 在**8萬4,000**台端點上，阻止了**250**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,700**台端點上，阻止了**84萬5,600**次嘗試掃描在**CMS**漏洞。
- 在**6萬5,400**台端點上，阻止了**140**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**630**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4萬3,000**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**16萬1,900**台端點上，阻止了**900**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,100**台端點上，阻止了**9萬6,000**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。

2023/06/15
Skuld惡意竊密軟體

Skuld 是最近發現由 Golang 程式語言所撰寫的惡意竊密軟體。Skuld 目標是搜集系統資訊、受害者的機密檔案、加密貨幣、Discord 權杖、暫存在各種網頁瀏覽器中的 Cookie、瀏覽紀錄、表單資料……等資訊。該惡意軟體會執行各種防監聽 (anti-debugging) 和虛擬環境偵測……等規避檢測伎倆。也會透過 Discord webhook 或經由將壓縮檔上傳到 Gofile 存儲服務來滲出被盜的資料。

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

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.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。

2023/06/15
以ChatGPT為幌子的Android手機惡意軟體

威脅行為者不斷建立以 ChatGPT 為幌子的誘餌，以傳播偽裝成目前非常流行的 AI 聊天機器人的惡意軟體。正在傳播的惡意軟體包括兩種類型，一種是偽裝成“SuperGPT”APP 的 Meterpreter 木馬，另一種是自稱為“ChatGPT”的木馬，它向泰國的高資費門號發送誘餌內容簡訊。高資費門號比撥打普通電話號碼的費用更高，而且最終可能會所費不貲。

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
- WS.Malware.1
- WS.Malware.2

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
- AppRisk:Generisk

2023/06/15

Shuckworm駭客間諜組織持續發動對烏克蘭的網路攻擊行動

Shuckworm 駭客間諜組織持續對烏克蘭發動多起網路攻擊行動，最近的目標包括安全部門、軍隊和政府組織。Shuckworm（又名 Gamaredon、Armageddon）是一個與俄羅斯有聯繫的駭客組織，自 2014 年首次出現以來，其行動幾乎完全集中在烏克蘭。烏克蘭官員公開表示，該駭客組織代表俄羅斯聯邦安全局 (FSB) 開展活動。眾所周知，Shuckworm 使用網路釣魚電子郵件作為初始感染媒介，然後繼續將其他後門程式和酬載等感染鏈工具下載到目標電腦上。

在我們部落格文章集中有更詳細的內容可供參考：Shuckworm：剖析俄羅斯駭客針對烏克蘭發動的無情網路攻擊行動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen12
- Downloader
- ISB.Downloader!gen281
- ISB.Downloader!gen490
- ISB.Heuristic!gen5
- Scr.Malcode!gen
- Trojan Horse
- W97M.Downloader

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。

2023/06/14

TONEDROP--Earth Preta駭客集團的新型惡意程式植入器(Dropper)軟體

在真實網路情境上發現一種名為 TONEDROP 的新型惡意程式植入器 (Dropper)，歸因於 Earth Preta (又名 Mustang Panda) 這個進階持續性威脅 (APT) 組織。惡意程式植入器 (Dropper) 用於傳送來自 TONEINS 和 TONESHELL 惡意軟體家族的惡意軟體酬載。該網路攻擊行動針對亞太地區 (APAC)、西亞和歐洲等不同地區的許多國家／地區。在他們的攻擊中，攻擊者利用偽裝成 Google Drive 的下載站點來提供初始有效籌載。

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(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：

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

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/06/14

RecordBreaker惡意竊密程式偽裝成.NET更新檔傳播

眾所周知，RecordBreaker 惡意軟體是 Raccoon 惡意竊密程式的後繼強化版本。該惡意軟體於去年首次出現，並持續在真實網路情境流竄。最新的 RecordBreaker 散布行動將初始下載程式偽裝成 Microsoft .NET Framework 更新套件。該惡意軟體執行各種防監聽 (anti-debugging) 和沙箱檢測等規避檢測伎倆。如果在虛擬環境中運行，它只會從官方 Microsoft 入口網站下載合法的 .NET 更新安裝檔，然後自行終止。在 VM 環境之外，RecordBreaker 有效負載將從惡意 C&C 伺服器獲取。惡意竊密程式一旦執行，便具有從遭駭電腦中竊取機敏資訊的能力功能。

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：

- AGR.Terminate!g2

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.B
- Heur.AdvML.B!100
- 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：

- Web Attack: Webpulse Bad Reputation Domain Request

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。

2023/06/12

Excel 帳單陷阱的社交工程網路攻擊：星際檔案系統(IPFS) 網路釣魚行動針對土耳其的產業

星際檔案系統 (IPFS) 網路釣魚持續在全球氾濫，賽門鐵克最近發現到一個攻擊行動，攻擊者針對大中型土耳其產業以及在當地設有辦事處的跨國公司。分析多個受害者的脈絡後發現，這些攻擊背後的參與者主要針對保險、能源和製造業（包括汽車、布料、化學品等）的公司。惡意電子郵件（主題：Fatura ödeme kopyası）試圖用假帳單引誘受害者。點擊惡意網址後，用戶將被重定向到代管在 IPFS 上的釣魚網頁版面，該頁面幾可亂真地偽裝成 Excel 文件，提示他們輸入電子郵件密碼以獲得完全存取權限。

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。

2023/06/12

Censored勒索軟體

賽門鐵克發現一種名為“Censored”的勒索軟體正在傳播，其目標是消費者和小型企業的個別電腦。它會向受害者索價 200 美元等值的比特幣作為贖金。目前，該勒索軟體似乎並未橫向傳播。它應該屬於 Chaos 勒索軟體的後繼變種，因為還看不出跟其勒索軟體家族有任何相似之處或相關聯。

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：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

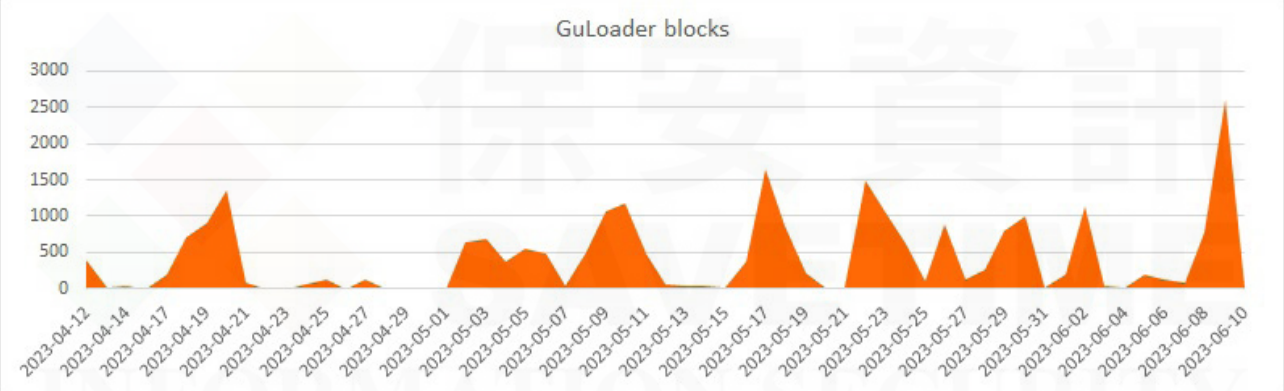
2023/06/12

防護亮點：再次檢視GuLoader進階下載器

~ 防護亮點 ~

我們在今年 3 月發布一份關於 GuLoader 的防護亮點公告，在上週五觀察到活動激增後，這是一個簡短的追蹤，以確認它仍舊嘗試做不法行為，並且仍然成功的被 Symantec 防護產品主動攔截。

回顧一下，GuLoader 是一種基於 shellcode 的進階下載器，它使用各種反分析技巧來試圖逃避檢測並使逆向工程更加困難，其目標是提供一系列惡意軟體，包括但不限於勒索軟體、竊密程式、銀行木馬、遠端存取木馬 (RAT) 和代理 (proxy)。GuLoader 主要透過各種不同主旨的垃圾郵件進行傳播，包括帶有其他惡意軟體連結的版本，或者在某些情況下直接包含嵌入式腳本的附件，該腳本會試圖在使用者系統上構建 PowerShell 腳本並執行它。最終的有效籌載也各不相同，但 FormBook、Agent Tesla、NanoCore 和 Netwire 是最常見。



賽門鐵克為 GuLoader 提供多個零時差防保護。以下是目前的前 10 名：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Exp.CVE-2017-11882!g7
- Packed.NSISPacker!g14
- Scr.Malcode!gen19
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

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於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。

欲深入瞭解更多有關於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。

2023/06/12

發現DoubleFinger惡意程式載入器被用於傳播加密貨幣偷竊程式的攻擊行動中

最近在傳播加密貨幣偷竊程式的攻擊行動中發現被稱為 DoubleFinger 的惡意程式載入器。載入步驟最初是透過夾帶惡意 .pif 附件的垃圾郵件發送。一旦受害者執行該檔案，就會啟動初始攻擊階段。該攻擊行動的最終有效籌載是一種被稱為 GreetingGhoul 的加密貨幣偷竊程式。還發現一些利用 DoubleFinger 相關網路攻擊行動提供不同的有效籌載--Remcos，這是一種被各種威脅參與者使用的商業遠端存取木馬 (RAT)。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

2023/06/12

SpectralViper後門程式

在最近針對越南企業的網路攻擊行動中發現到 SpectralViper 後門程式。該後門極為隱密，並具有檔案上傳／下載、命令執行以及檔案／目錄以及操縱權杖等功能。最近傳播 SpectralViper 的行動，還在整個感染鏈中利用額外的惡意程式載入器和 PowerShell 惡意軟體，DonutLoader、P8Loader 和 PowerSeal 等惡意軟體也都曾經出現過。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- 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。

2023/06/11

STRRAT：觀察到全球活動

STRRAT 並不是一種新的威脅，它已經存在一段時間，並且仍然被世界各地的駭客組織與個人積極使用，以發動本地型、全球性、有針對性及亂槍打鳥的隨機攻擊行動。在最近的一個例子中，賽門鐵克發現到一名駭客對一家知名的德國跨國製藥和生物技術公司進行域名仿冒，以進行魚叉式網路釣魚行動。電子郵件主旨是“CONFIRM VERBAL GERMANY ORDER (JUNE)”，它針對歐洲、中東、亞洲、拉丁美洲和北美的各個行業。該行動採用典型“Quote”誘餌和包含惡意 Java 腳本檔案（STRRAT 惡意軟體）的 .cab 附件，主要在對受感染的系統執行遠端存取和控制。

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：

- ISB.Dropper!gen12

2023/06/11

電子郵件憑證(帳密)盜竊：對巴西組織的持續威脅

巴西的網路犯罪持續增加，網路釣魚是最主要的威脅之一。賽門鐵克每天都會發現到針對巴西組織和在當地設有分支機構的外國公司的多起攻擊行動。在最近的一個範例中，一名攻擊者一直在瘋狂犯罪，試圖透過惡意電子郵件竊取電子郵件憑證（帳密）。 這些電子郵件的主旨是：「Aviso: Confirme sua conta de email para não ser suspensa!」，攻擊者主要在欺騙受害者相信他

們的電子郵件帳號有被暫停的風險。為避免這種情況，系統會提示他們登錄網路釣魚頁面。如果誘騙成功，攻擊者可以在地下市場上出售被盜的存取權限、進行身份盜用、發起複雜的魚叉式網路釣魚攻擊、發動商業電子郵件詐騙 (BEC)，甚至從其他系統竊取敏感資料。

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。

2023/06/09

Darkrace勒索軟體

Darkrace 是一種全新的勒索軟體，表現出與 Lockbit 惡意軟體變種的某些相似之處，並且可能源於被洩露 Lockbit 3.0 的程式碼。Darkrace 加密被害者檔案並為其附加隨機副檔名。該惡意軟體能夠從目標電腦上刪除陰影副本，並在加密完成後清除所有可執行惡意檔案。留在電腦上的勒索說明檔案內含受害者可透過電子郵件聯絡攻擊者的說明，以及指向威脅攻擊者營運的洩密網站的連結網址。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransom!gen109
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g189
- SONAR.SuspLaunch!g193

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.B

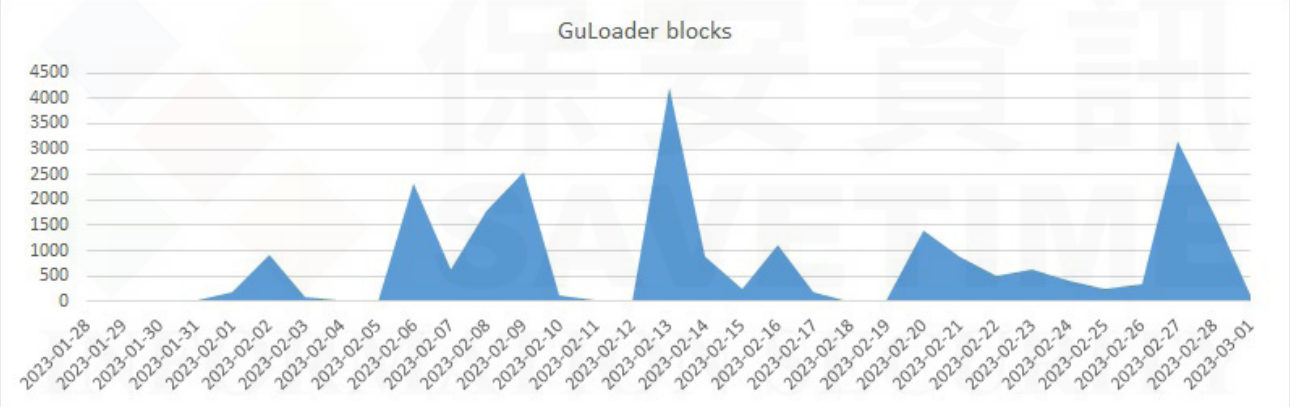
2023/03/06

防護亮點：第一時間成功攔截～GuLoader隱藏在眾目睽睽之下的先進惡意軟體下載程式

～防護亮點～

GuLoader 是一種進階型的 shellcode (利用軟體漏洞讓 CPU 執行特定程序的機械碼)，GuLoader利用多種對抗分析的方式來增加反向工程的難度，使得它更難被偵測到。它的終極目標是傳遞一系列的惡意軟體，包含勒索軟體 (ransomware)、偷取敏感資訊的惡意軟體 (infostealers)、偷取金融資訊的惡意軟體 (banking Trojans)、遠端存取木馬 (RAT)、代理程式 (Proxy) 等。賽門鐵克威脅獵手團隊最近在一篇名為「Bluebottle：發動攻擊非洲法語系國家銀行行動的駭客組織」(Bluebottle campaign targeting banks in French-speaking African countries) 的網誌中介紹關於 GuLoader 的初階攻擊方式。

我們經常觀察到 GuLoader 是透過垃圾郵件的方式來散佈包含多種版本的 ISO 檔案，這些 ISO 檔中嵌入了 VBE 腳本，而 VBE 腳本再建立另一個 Powershell 腳本並執行它。



有多種 *GuLoader* 被偵測到，此處僅顯示 *Scr.Malcode!gen36*

雖然 GuLoader 不是什麼新的惡意軟體，但有趣的是作者為了不被偵測到而採取的措施。上面提到的 ISO/VBE 攻擊大致流程是……一開始一個經過代碼混淆的 Powershell 腳本去 Google Drive 下載並取出 GuLoader shellcode(使用 base64 編碼格式)，然後藉由 Windows API (CallWindowProcA) 將 shellcode 解碼 (base64)。從這裡開始 GuLoader 的作者就已進行避免偵測或延緩分析的措施。這些公告並不打算過於強調細節或技術性資訊，因此我們將儘量簡化說明。

GuLoader的反偵測技巧

- 反防毒軟體 #1：GuLoader 首先試圖防止作業系統從與 GuLoader 相關的 shellcode 區塊生成可執行檔，這是一個非常古老的技巧。
- 反除錯 #1：GuLoader 透過 Windows API 設置一個向量例外狀況處理常式(VEH)，並將代碼執行流指向到受管理的異常處理程序，該程序會嘗試捕捉由 EXCEPTION_SINGLE_STEP(TrapFlag) 引起的異常。 TrapFlag 允許處理器在單步模式下運行，可以操縱它以防止追踪。
- 反除錯 #2：反硬體間斷點和反軟體間斷點。硬體和軟體的間斷點是指在除錯時的暫停事件。GuLoader 會檢查這些事件並試圖防止它們。

- 反虛擬機 #1：記憶體分頁掃描。GuLoader 使用 NtQueryVirtualMemory API 掃描整個記憶體和處理程序，檢查是否有任何虛擬機 (VM) 或除錯工具相關的字串。
- 防禦逃避 #1：Heaven's Gate 是一種在 2000 年代中期為了相容性目的而使用的一種方法，允許在 32 位元程序中執行 64 位元程式碼。GuLoader shellcode 使用 Heaven's Gate 執行一個 64 位元程式碼中介(stub)使其不被注意。
- 反虛擬機 #2：GuLoader 檢查是否存在與 QEMU(VM) 模擬器相關的文件，例如：C:\Program Files\Qemu-ga\qemu-ga.exe 和 C:\Program Files\qga\qga.exe。
- 反除錯 #3：GuLoader 對 DbgBreakPoint 和 DbgUiRemoteBreakin 進行修補，來避免除錯器將其加入主機的執行程序當中。
- 防禦逃避 #2：移除 NTDLL32 中的 Hooks(用來插入自定義程式碼或函數)。GuLoader shellcode 掃描 NTDLL 中的 SYSCALL 狀態模式，提取 SYSCALL 編號並將函數代碼恢復到原始狀態。
- 反沙箱 #1：列舉視窗。GuLoader 呼叫 EnumWindows API 來計算在受害者機器上運行的上層視窗(無論可見與否)。如果數量低於 12，則 shellcode 終止。
- 反除錯 #4：ThreadHideFromDebugger。一種常見的反除錯技術，利用 NtSetInformationThread API 來有效的將執行緒標記為對除錯器不可見。
- 反沙箱 #2：GuLoader 使用各種 API 來列舉 Windows 驅動程式、已安裝的軟體和服務，並將它們的雜湊值與預先儲存的雜湊值進行比較。
- 反除錯 #5：ProcessDebugPort。Guloader 呼叫 NtQueryInformationProcess 來檢測是否有除錯器附加到它的處理程序中。

在多次嘗試隱藏之後，GuLoader shellcode 使用執行程序掏空技術 (Process Hollowing) 將自己注入到另一個執行程序當中，執行程序掏空技術是一種代碼注入技術，可以將記憶體中合法執行程序的可執行區段替換(或附加)為惡意代碼。

最後，在經過一連串的反偵測技巧 (在我們的案例中顯然是不成功的) 之後，GuLoader 將下載最終有效負載。在這個特定的案例中，有效負載是臭名昭張的 Agent Tesla。

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的**零時差**攻擊，能通過以下方式識別 GuLoader：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen36

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於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。

欲深入瞭解更多有關於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。