保安資訊--本周(台灣時間2023/03/24)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 81 萬 6,300 台受保護端點上總共阻止了 1 億 210 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/03/20)**

- 在**15萬9,900**台端點上，阻止了**4,360**萬次嘗試掃描**Web**服務器的漏洞。
- 在**29萬2,100**台端點上，阻止了**2,140**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬7,400**台**Windows**伺服主機上，阻止了**1,620**萬次攻擊。
- 在**8萬5,600**台端點上，阻止了**280**萬次嘗試掃描伺服器漏洞。
- 在**2萬100**台端點上，阻止了**120**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬8,900**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**27萬5,600**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**9,600**台端點上，阻止了**230**萬次加密貨幣挖礦攻擊。
- 在**15萬900**台端點上，阻止了**1,170**萬次向惡意軟體**C&C**連線的嘗試。

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。

2023/03/23

新駭客集團也來參一腳～利用PowerMagic後門和CommonMagic惡意軟體框架

根據最新一份報告，一個前所未見的威脅攻擊者一直針對位於頓內次克（Donetsk）、盧甘斯克（Luhansk）和克里米亞（Crimea）地區的組織進行攻擊。攻擊者一直利用名為 CommonMagic 的全新模組化惡意軟體框架以及 PowerMagic 後門。感染鏈涵蓋從 .zip 壓縮檔中得出的 .lnk 檔，再去呼叫或下載包含已加密的效籌載二進位碼檔案和 .vbs 腳本的 .msi 安裝檔。植入的惡意軟體會嘗試收集資料、允許攻擊者從受感染的端點收集螢幕截圖也是常見的功能。

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.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen89
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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。

2023/03/23

DotRunpeX 惡意注入程式，廣受不同惡意軟體家族採用

DotRunpeX 惡意注入程式最近被發現涉入多個網路攻擊行動，這些攻擊行動傳播各種惡意軟體家族的有效籌載。DotRunpeX 主要透過惡意附件、Google Ads 濫用或透過偽裝成各種應用程式下載入口網站傳播。這個基於 .NET 的惡意注入程式受到自定義版本 KoiVM 虛擬器的保護，它利用一種稱為 Process Hollowing 的程式碼注入技術。在最近的攻擊行動中藉助 DotRunpeX 傳播的一些有效籌載惡意軟體家族包括：AgentTesla、Formbook、PrivateLoader、RecordBreaker、Redline Stealer、Vidar Stealer 等等。

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：

- AGR.Terminate!g2
- SONAR.ProcHijack!g51
- 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.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

2023/03/22

Mystic多功能竊密程式

Mystic 竊密程式是另一種普通的竊密程式，它一直在威脅領域四處遊蕩，但遠沒有同家族中的其他惡意軟體那麼普遍。偶爾會檢測到命令和控制服務器 (C&C)，Mystic 竊密程式的登錄頁面會顯示兩個對角對齊的紫色和綠色圓圈。近期活動的幕後黑手正在透過瀏覽網頁常見的“偷渡式”下載伎倆傳播它。以下是它的資訊收集功能：

- 電腦資訊（名稱、用戶名稱、guid等）
- 網頁瀏覽器自動填寫表格和歷史記錄
- 來自各個 APP 位置（例如：Bitcoin、DashCore、Exodus、Guarda、Electrum、MyMonero 等）的加密貨幣錢包相關資料或檔案。

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 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：

- Infostealer
- Suspicious: Reputation

基於機器學習的防禦技術：

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

2023/03/22

微軟最新CVE-2023-24880 Windows SmartScreen漏洞，已被Magniber勒索軟體大量濫用

CVE-2023-24880 是最近披露的 Windows SmartScreen 漏洞，該漏洞被攻擊者用來建立可執行檔以繞過 Windows 中 Web 的安全標記 (MOTW)防護 。攻擊者正在利用錯誤驗證碼簽章的 .MSI 檔案，這會導致 SmartScreen 錯誤，進而繞過向最終用戶顯示安全警告。據報導，該漏洞在傳播 Magniber 勒索軟體的惡意攻擊行動中被大量濫用。

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：

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：

- Exp.CVE-2023-24880
- JS.Downloader
- Ransom.Magniber
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/03/22

Mispadu銀行木馬針對拉丁美洲國家

Mispadu（又名 Ursa）是一種銀行木馬，最初於 2019 年被發現，以拉丁美洲用戶為目標。根據最近一份報告，一項利用 Mispadu 的全新攻擊行動於 2022 年 8 月左右開始，目前仍在進行中。該活動試圖竊取銀行憑證，但也鎖定儲存在 Outlook 和 Chrome 應用程式中的憑證作為目標。該惡意軟體主要透過垃圾郵件或惡意廣告傳播。已知攻擊者還會入侵知名的合法網站並將其用於惡意軟體傳播。

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.SuspLoad!gen2
- SONAR.SuspPE!gen32

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

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

2023/03/22

HookSpoofer竊密程式

HookSpoofer 是一支全新的竊密程式，源於 StormKitty 竊密程式的開放源始碼。已知該惡意軟體經由與假冒軟體大補帖捆綁在一起來進行傳播。HookSpoofer 的功能包括鍵盤側錄、資料裁剪、經由 VPN 應用程式和網頁瀏覽器竊取資料、螢幕截圖、竊取加密貨幣錢包等。竊取的資訊透過 Telegram 機器人發送給攻擊者。

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.NPE
- WS.Malware.1

基於機器學習的防禦技術：

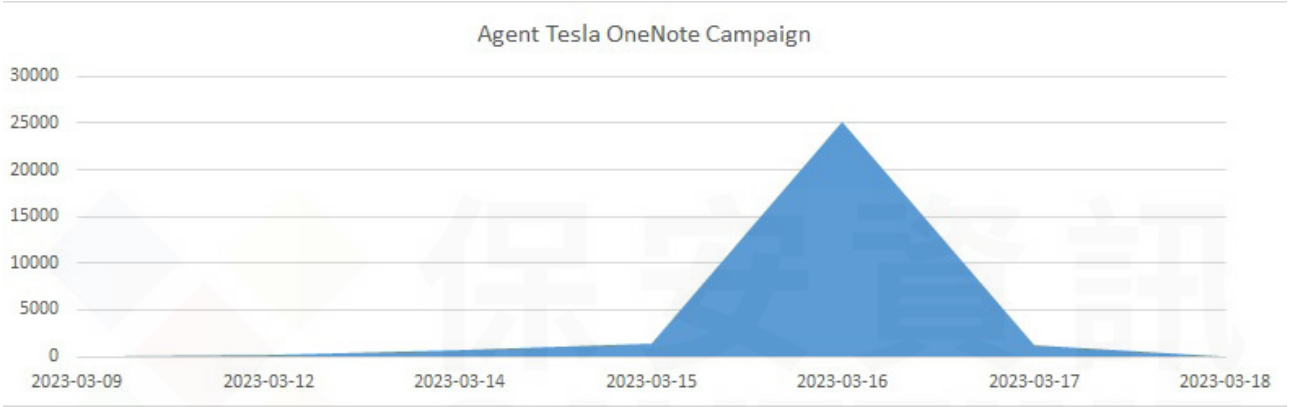
- Heur.AdvML.A

2023/03/20

防護亮點：Agent Tesla的OneNote活動

～防護亮點～

我們長期關注並且已經多次發布有關 **Agent Tesla** 的訊息，因為它是一個非常普遍的竊密程式，因此值得警惕。仍然主要透過惡意電子郵件進行傳送，通常帶有普通的社交主旨，主旨包含帳單、報價、運輸、SWIFT 等，並且仍然試圖從受害裝置竊取機密訊息，包括儲存在瀏覽器，電子郵件和 VPN 用戶端中的密碼。正如之前報導，它還包含遠端存取功能，入侵可能讓其他的有效負載被植入到受感染的主機上。



這個最新的攻擊行動使用幾個主旨，包括“德意志銀行…”、“付款建議…”、“訂單…”，並使用以下攻擊鏈，這次使用 OneNote 筆記本檔作為惡意附件：

Email --> .onepkg --> OneNote --> PowerShell --> Agent Tesla

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 **零時差**防護技術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.MalOneNote!gen1

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。

2023/03/20

Winter Vivern--進階持續性攻擊(APT)駭客組織針對政府組織發動的網路釣魚攻擊行動

Winter Vivern 進階持續性攻擊 (APT) 駭客組織是一個鮮為人知的親俄組織。該組織一直在使用已知的攻擊媒介，例如：模仿政府網站作為釣魚網站來傳播他們的惡意酬載檔案，進而使他們能夠獲得對系統未授權的存取並透過與 C&C 伺服器建立連接來發起網路攻擊。

該APT 組織過去的目標是印度、梵蒂岡、斯洛伐克以及最近的波蘭和烏克蘭的政府組織。

在最近觀察到的活動中，該組織將其惡意軟體偽裝成存放在模仿政府網站假的防毒軟體掃描程式，透過魚叉式網路釣魚電子郵件作為政府發送通知訊息給特定對象。

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)。

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.MSOffice!g7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.MalMacro!gen3
- Trojan.Gen.2
- Trojan Horse
- Trojan.Mdropper
- 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。

2023/03/20

漏洞不補永遠存在～四年前被揭露的Progress Telerik UI開發軟體漏洞，持續讓多個駭客組織對政府機構發動網路攻擊

根據最新的美國國土安全部網路安全暨基礎設施安全局 (CISA) 公告，多個駭客組織在最近針對政府機構的攻擊中，利用一個已經被揭露四年的老牌 Progress Telerik UI 開發軟體遠端程式碼執行漏洞 (CVE-2019-18935)。某一些活動歸因於稱為 XE Group 的駭客組織。 這個駭客組織一直在利用偽裝成 PNG 檔案的惡意 DLL檔，並濫用 w3wp.exe（IIS 執行程式）等合法程序在受感染的 IIS 伺服器上執行這些 DLL。該惡意軟體可能會列出系統檔案和目錄，連接到攻擊者控制的

C&C 伺服器並下載額外的有效籌載。在某些情況下，攻擊者還會在受感染的系統上植入 ASPX webshell。webshells 可以作為被感染伺服器的列表、目錄瀏覽、檔案下載和命令執行的窗口。

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!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Hacktool.Webshell
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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

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
- Web Attack: Telerik UI CVE-2019-18935
- Web Attack: Telerik UI CVE-2019-18935 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。

2023/03/20

Hinata分散式阻斷服務(DDoS)殭屍網路

Hinata 或 HinataBot 是新發現用 Golang 程式語言撰寫的分散式阻斷服務 (DDoS) 殭屍網路。在感染鏈中，惡意軟體利用弱憑證和一些舊的 Hadoop YARN、Realtek (CVE-2014-8361) 和華為 (CVE-2017-17215) 漏洞。根據當下情境不同，HinataBot 可能會利用各種通訊協定發動 DDoS 攻擊，包括 HTTP、UDP、TCP 和 ICMP。

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.Lightaidra
- Trojan Horse
- WS.Malware.2

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: Huawei Router RCE CVE-2017-17215
- Web Attack: Realtek SDK RCE CVE-2014-8361

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。

2023/03/20

冰火(*IceFire)勒索軟體現在也針對Linux

在最近針對全球媒體和娛樂組織的攻擊中，發現 IceFire 勒索軟體的 Linux 版本。攻擊者一直在利用 IBM Aspera Faspex (一種集中式檔案傳輸 Web 應用程式) 中的漏洞 (CVE-2022-47986) 來傳播惡意軟體。IceFire 會排除對預設的系統相關目錄和檔案進行加密，以防止系統不穩定而讓受害者提早發現。該惡意軟體會將 .iFire 副檔名新增到被加密的檔案，並將勒索熟金支付說明放到所有存在被加密檔案的目錄。

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.NPE
- WS.Malware.1

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: IBM Aspera Faspex RCE CVE-2022-47986

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。

2023/03/19

Keyzetsu加密貨幣的剪貼簿竊密程式(Clipper)

Keyzetsu 是多如過江之鯽的加密貨幣之剪貼簿竊密程式 (Clipper) 新成員，已在威脅領域闖出名號，目前透過 Evernote 等非法盜拷的軟體、Realtek 等驅動程式安裝檔以及 Google update 等軟體更新程式進行傳播。當這種惡意軟體成功感染設備並劫持受害者的錢包時，它能夠透過 Telegram 機器人和 Telegram 的 API 通知其作者--這是當今竊密程式中相當普遍的技術。

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!gen633

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/03/19

Chaos勒索軟體變種，這次潛伏在惡意VPN安裝程式

惡意軟體威脅者經常將他們的惡意軟體偽裝成 VPN 安裝程式，因為 VPN 越來越受歡迎，而且許多人都在尋求保護其線上隱私和安全的方法。

賽門鐵克觀察到 Chaos 勒索軟體變種背後的駭客組織或個體戶，鎖定在有風險的地方搜索 VPN 安裝程式、資安認知薄弱的消費者和企業用戶。偽裝成 VPN 安裝程式的勒索軟體會在加密檔案後新增 .locked 副檔名，並投放典型 Chaos 勒索軟體贖金支付說明。受害者被要求支付價值 1,500 美元的比特幣來解密檔案。此攻擊行動沒有採用雙重勒索伎倆。

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.SuspDrop!gen1

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

2023/03/19

簡訊釣魚詐騙行動：網路犯罪分子瞄準印度拉米(Rummy)紙牌遊戲玩家

幾百年來，博弈一直是許多文化的一部分，讓人興奮且著迷的中獎吸引著人們。然而，只要有錢，尤其是沉溺於金錢，犯罪往往就會隨之而來。多年來，博弈助長無數網路犯罪欺詐、網路釣魚和惡意軟體行動。

賽門鐵克最近觀察到與博弈相關的簡訊詐騙攻擊行動是鎖定印度熱門的拉米紙牌遊戲，一種在 2 到 6 個玩家之間玩，每個玩家發13張牌的紙牌來形成：群組及順組的兩種牌組。最先將手上的牌出完的人獲勝。

如果用戶落入簡訊圈套，誤以為他們的 Rummy 帳戶有 98,305 印度盧比匯入（相當於撰寫本文時的 1,191 美元），他們將被重定向到一個欺詐性的線上信用卡網站並提示輸入他們的姓名、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。

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已於第一時間收錄於不安全分類列表中。

2023/03/17

語音網路釣魚在韓國仍然占主導地位

韓國行動用戶仍然是語音網路釣魚的目標，並且觀察到最近的一次行動，受害者被誘騙落入偽裝成知名金融機構以較低的貸款利率所吸引而安裝歹徒設計的惡意 APP。根據報告，他們隨後被誘騙提供他們的財務詳細訊息，例如：銀行帳號和信用卡資訊。

在語音網路釣魚中，惡意軟體操作員會冒充權威人士並聯絡被害者，例如：銀行員工要求提供個人資訊、信用卡和銀行帳戶詳細資訊，以獲取實質獎勵。語音網路釣魚於 2006 年在南非首次被報導，此後網路釣魚造成的損失呈滾雪球式增長。

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。

- 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。