Bluebottle：發動攻擊非洲法語系國家銀行行動的駭客組織

2023 年 1 月 5 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

利用全新的攻擊策略、技術及程序 (TTPs) 延續先前記錄的行動。

Bluebottle 是一個專門鎖定金融機構發動目標式攻擊的網絡犯罪組織，它延續對法語系國家的銀行發動攻擊。該組織廣泛使用就地取材、兩用工具和商品化的惡意軟體，在此行動中並沒有部署自定義的惡意軟體。

博通的軟體部門賽門鐵克觀察到的行動似乎是 Group-IB 自 2022 年 11 月起記錄的報告中行動的延續。Group-IB 記錄的行動時間跨越 2019 年中至 2021 年，它表示在那個時期，這個名為 OPERA1ER 的駭客組織在 30 次目標式攻擊中至少竊取 1100 萬美元。

Group-IB 記錄的行動與賽門鐵克看到的活動在攻擊策略、技術及程序 (Tactics、Techniques、and Procedures，TTPs) 方面的相似之處包括：

- 活動中看到兩個相同網域：personnel[.]bdm-sa[.]fr
- 使用一些相同的工具：Ngrok、PsExec、RDPWrap、Revealer Keylogger、Cobalt Strike Beacon
- 在兩組活動中均未發現自定義惡意軟體
- 鎖定對象遍及非洲法語系國家
- 兩組活動的特徵還使用特定行業和特定地區的網域名稱

雖然這似乎是 Group-IB 所記錄的行動延續，但賽門鐵克近來看到的行動時間，至少從 2022 年 7 月持續到 2022 年 9 月，儘管其中一些行動可能早在 2022 年 5 月就開始，最近的攻擊也採用如下較新的一些 TTPs，包括：

- 一些跡象顯示攻擊者可能使用 ISO 檔作為初始感染媒介
- 在攻擊的初始階段使用商品化惡意軟體 GuLoader
- 跡象顯示攻擊者採用了濫用內核驅動程式 (kernel drivers) 來停用安全防護軟體

攻擊鏈

最初的感染媒介未知，但在受害網路上所發現最早的惡意檔案具有以徵才招聘為主題的法語檔名。這些可能促使了誘餌的作用。在某些情況下，惡意軟體的命名是為了誘騙使用戶認為它是一個 PDF 檔，例如：

- *fiche de poste.exe ("job description")*
- *fiche de candidature.exe ("application form")*
- *fiche de candidature.pdf.exe ("application form")*

這些檔案很可能是透過魚叉式網路釣魚電子郵件發送給受害者，這與 Group-IB 為 OPERA1ER 行動記錄的初始感染媒介一致。

儘管賽門鐵克研究人員觀察到大部分行動始於 2022 年 7 月，但至少有一名受害者早在 2022 年 5 月中旬就在其網路上發現類似的命名主題的竊密程式。在這種情況下，惡意軟體開始以包含可執行 SCR檔的 ZIP 檔形式。

- *fiche de candidature(1).zip (ZIP 壓縮檔)*
- *fiche de candidature.scr (SCR 可執行檔)*

該檔案是一個較舊、可能是商品化的惡意軟體。很難確定它何時被用於針對這些組織。但是，它與 OPERA1ER 在 2021 年報告的感染媒介一致。

然而，7 月份以徵才招聘為主題的惡意軟體在某些路徑中被觀察到，顯示為 CD-ROM。這可能表示插入真正的光碟，但也可能是惡意 ISO 檔被傳送給受害者並掛載。 ISO 檔是一種壓縮檔，其中包含可在光碟上找到的相同資料副本或圖片。在 2022 年的其他行動中，惡意 ISO 檔已被用於初始感染媒介，包括在以傳播勒索軟體為最終目標的行動中與 Bumblebee 載入程序一起使用。如果 Bluebottle 和 OPERA1ER 攻擊者確實是同一個，這意味著他們在 2022 年 5 月至 2022 年 7 月之間交換感染技術。在 Group-IB 記錄的行動中沒有看到 ISO 檔。

在許多情況下，傳遞給受害者的徵才招聘為主題的惡意軟體是名稱為 GuLoader 的商品化啟動程式。 GuLoader 是一個基於 shellcode 的下載程式，具有反分析功能。除了惡意檔案外，啟動程式還會部署一些合法的二進位檔作為其惡意攻擊行動的誘餌。 GuLoader 以自解壓 NSIS 可執行檔的形式傳播給受害者。這個 NSIS 腳本解密並將混淆的 shellcode 注入另一個程序。在 7 月行動中最常觀察到的程序是 ieinstal.exe，即 IE 瀏覽器附加元件安裝程式的程序，但也包括 aspnet_regbrowsers.exe，即 ASP.NET 瀏覽器註冊工具。

IE 瀏覽器附加元件安裝程式的程序可能被利用從 hxxp://178.73.192[.]15/ca1.exe 等網址下載惡意 .NET 下載程式。發現多個 .NET 下載程式濫用檔案傳輸服務 transfer[.]sh 下載 .RTF 副檔名的檔案。此有效籌載未知，但下載程序主要在將其作為 .NET DLL 掛載。

在部署 GuLoader 和 .NET 啟動程式 (loaders) 之後，在受害者網路上發現其他各種的入侵後利用工具。其中包括公開可用的 Netwire 遠端存取木馬 (RAT) 和開放原始碼的 Quasar 遠端存取木馬 (RAT)。攻擊者還使用商業入侵後利用工具 Cobalt Strike Beacon。Bluebottle 使用的 Cobalt Strike Beacon 變種採用 API hammering (錘擊技術) 來規避安全軟體偵測。

使用具簽章的驅動程式來終止處理程序

攻擊者還部署一組惡意軟體，其目的可能是停用受害網路上的安全軟體。該惡意軟體由兩個元件組成，一個是從第三方檔案讀取程序列表的 DLL 控制項 ，另一個是具簽章的“helper”驅動程式是由第一個驅動程式控制並用於終止清單中的處理程序。

攻擊者使用 Windows 服務控制 (sc.exe) 來啟動驅動程式：

sc create fgt binPath= %TEMP%fgt.sys type= kernel
sc start fgt

2022 年 8 月，賽門鐵克偵測到到相同的驅動程式疑似被用於針對加拿大一家非營利組織的勒索軟體攻擊行動的前置作業。在受害者網路上發現的另一個工具是 Infostealer.Eamfo，這是一個與 Cuba、Noberus 和 Lockbit 勒索軟體攻擊有關的駭客工具。

同一支驅動程式似乎也被多個組織用於類似目的。Mandiant 記錄一個名為 UNC3944 以獲取財務利益為動機的駭客組織，它使用相同驅動程式來停用安全防護軟體。它將此驅動程式稱為 POORTRY，將使用它的惡意軟體稱為 STONESTOP。而 Mandiant 當時確實指出，“POORTRY 出現在不同的駭客組織中，並且與可購得或在不同組織間免費共享的惡意軟體一致。”

Sophos 也記錄 Cuba 勒索軟體營運商使用名為 BURNTCIGAR 的啟動程式載入具簽章的驅動程式以停用防護軟體的實例。啟動程式的動作類似於此活動中看到的惡意 DLL。

其他供應商向微軟回報這些驅動程式，該公司暫停開發者帳戶並增加防護措施來解決這些問題。

Bluebottle 在最近這項行動中短期目標似乎部分是持續性和憑證盜竊。攻擊者使用憑證盜竊技術和工具，例如：修改 WDigest 設定和部署 Mimikatz，以及一個開放原始碼的偽造登錄畫面鍵盤側錄器。

關於橫向移動，攻擊者部署用於網域信任列舉的滲透測試工具 SharpHound，並使用 PsExec 在受害組織中執行其他的檔案。

關於持續性，有證據顯示攻擊者使用“net localgroup /add”指令新增帳號。他們還部署一個開放原始碼 RDPWrap 腳本，用來在受害系統上啟用多個 RDP 通訊。此腳本也修改註冊表並在防火牆上開啟通訊埠 3389 以允許 RDP 流量通過。有跡象顯示，該行動可能是“實際操作鍵盤”行動，而不是自動化行動。雖然我們看不到攻擊者進行哪些進一步的動作，但受害者以及與 Group-IB 記錄的行動的交叉跡像都顯示該行動可能是出於獲取財務利益為動機。

受害者

在賽門鐵克所偵測到到的活動中，三個非洲國家的三個不同的金融機構遭到入侵，這三個機構的的多台電腦都遭受到感染。

其中之一受感染機構網路的活動如下：

第一次活動出現在 2022 年 7 月中旬，當時在受感染的系統上發現以徵才招聘為主題的惡意軟體。部署一個下載程式，檢測到 Sharphound hacktool 並部署一個名為 fakelogonscreen 的工具。

在網路遭到初始入侵後大約三週，攻擊者被發現使用命令提示字元和 PsExec 進行橫向移動。在攻擊這一點上，攻擊者似乎“實際操作鍵盤”。攻擊者出於多種目的使用各種兩用工具和就地取材工具，包括：

- Quser 用來用戶搜索
- Ping 用於檢查網際網網連接
- Ngrokngrok 是一個反向代理，透過在公共的端點和本地運行的Web 服務器之間建立一個安全的通道。
- net localgroup /add 用來新增帳號
- Fortinet VPN 用戶端--可能用於存取的備用通道
- Xcopy 複製 RDP 包裹（Wrapper）檔
- netsh 在防火牆中開啟 3389 通訊埠
- 檔名為 Autoupdatebat 的“自動化RDP 包裹（Wrapper）檔安裝和更新程式”工具可在系統上啟用多個 RDP 通訊
- SC privs 修改 SSH 代理權限--這可能是為了密鑰盜竊或安裝另一個通道而一再遭篡改

使用的惡意工具包括：

- GuLoader
- Mimikatz
- Revealer Keylogger
- Backdoor.Cobalt
- Netwire RAT
- The malicious DLL and driver for killing processes

該網路上還部署多個其他未知的檔案。最後一次活動是在 2022 年 9 月，但 Ngrok 通道工具一直保留在網路上，直到 2022 年 11 月。

一些相同的工具也部署在其他受害者身上，GuLoader 在所有三名受害者身上都可以看到。將所有三名受害者的活動關聯起來的其他活動包括：

- 相同的 .NET 下載程式
- 使用了惡意驅動程式
- 至少有一個相同的 transfer[.]sh 網址

結論

雖然賽門鐵克無法確認 Bluebottle 是否成功地將我們看到的行動獲取實質的收益，但根據 Group-IB 的記錄，該組織在 2019 年至 2021 年期間成功地將其活動帶來錢潮，顯示該組織在過去得到很大的金錢收益。

其行動的實質效益意味著 Bluebottle 食髓知味，不太可能放棄相關活動。它似乎非常關注非洲法語系國家，因此這些國家的金融機構應對本部落格中列入的活動保持高度警惕。攻擊者似乎是講法語，因此也不能排除他們將這種行動擴展到其他地區法語系國家的可能性。

文章中提及的工具詞彙表

- **Cobalt Strike**：一種現成的工具，可用於執行指令、注入其他程序、提升當前程序或模擬其他程序，以及上傳和下載檔案。表面上具有作為滲透測試工具的合法用途，但總是被歹徒所利用。
- **GuLoader**：一個基於 shellcode 的下載程式，具有反分析功能。除了惡意檔案外，啟動程式還會部署一些合法的二進位檔作為其惡意活動的誘餌。
- **Mimikatz**：常見的免費工具，能夠變更權限，匯出安全憑證以及根據組態以明碼形式恢復Windows密碼。
- **Netsh**：Windows 命令列工具，允許使用者配置和顯示各種網路通訊伺服器角色和元件的狀態。
- **Netwire RAT**：一種遠端存取木馬，能夠竊取密碼、鍵盤側錄，並包括遠端控制功能。
- **Ngrok**：一種通道工具，允許用戶開啟安全通道，讓他們立即開啟對遠端系統的存取，而無需接觸任何網路設置或打開路由器上的任何通訊埠。
- **Ping**：一種線上免費提供的工具，允許使用者確定網路上的特定位置是否有回應。
- **PsExec**：用於在其他系統上執行程序的Microsoft Sysinternals工具。該工具主要由攻擊者用於在受害者網路上橫向移動。
- **Quasar RAT**：一種遠端存取木馬，主要針對Windows系統，讓使用者透過網路遠端控制其他電腦。
- **Quser**：顯示有關遠端桌面會話主機伺服器上的使用者通訊的資訊。可以使用此命令來確定特定使用者是否登錄到特定的遠端桌面會話主機伺服器。
- **RDPWrap**：啟用遠端桌面主機支援和 RDP 工作階段的開放原始碼工具。
- **Revealer Keylogger** (鍵盤側錄程式)：免費工具，記錄輸入到電腦中的所有內容。
- **SharpHound**：可以在網域控制器和加入網域的Windows系統中收集資料。

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)

檔案雜湊值 (SHA256)

117c66c0aa3f7a5208b3872806d481fd8d682950573c2a7acaf7c7c7945fe10d — ZIP檔
c56c915cd0bc528bdb21d6037917d2e4cde18b2ef27a4b74a0420a5f205869e6 — 竊密程式
91b3546dde60776ae3ed84fdf4f6b5fba7d39620f0a6307280265cde3a33206b — .NET 下載程式
9c4c9fa4d8935df811cae0ce067de54ffdb5cfb4f99b4bc36c5aa2a1ac6f9c8f — .NET 下載程式
1f6be4c29dfb50f924377444e5ca579d3020985a357533fc052226f0091febf6 — .NET 下載程式
d5b8009dcb50aac8a889e24f038a52fe09721d142a3f1eaa74ac37fff45e9ba2 — .NET 下載程式
ae4ff662c959cf24df621a2c0b934ed1fa1c26a270a180f695cd5295579afbbd — .NET 下載程式
0612ef9d2239edeab05f421e3188e2cfcadacbaeafbc9b8e35e778f7234aaa3b — .NET 下載程式
4acd4335ca43783ff52c0ccbb7e757ea14fb261c33d08268e85ed0ac34e0abec — .NET 下載程式
47718762dc043f84fb641b1e0a8c65401160cc2e558fd38c14d5d35a114b93cb — .NET 下載程式
a539961f80feb689546a2e334b03aed81252a04fae032e2d28ed9a7000b3afff — .NET 下載程式
07ca6122fde46d48f71bcde356d5eeb89040e4a6e83441968a9dade98dc36fe5 — .NET 載入器
938f50cb2e2d670497209e8cef5bf1042f752b6bf76d1547d68040b5a27f618b — .NET 載入器
a257eeebba15afecf76b89a379e066e5ed79a2bb9da349c1fdb5a24316abc753 — GuLoader
f276c6a25d6b865c6202978f1d409e8b74e063263eab517f249cf6d3ad3fae4a — GuLoader
3d0fd0444a9e295135ecfdc8c87ddc6dcdff63969c745e0218469332aef18dfe — GuLoader
ac98e6bf6d16904355b1c706bc2b79761a8b09044da40f2c8bce35142ef8bcc8 — GuLoader
ca75b0864d8308efe94eb0822de55eb7f5cfd482d2190100dfd00d433ee790a0 — GuLoader
088110b0ee3588a4822049cf60fff31c67323a9b5993eae3104cc9737a47ce0c — GuLoader
b4adbb5d017d6452c2e1700584261cd3170ee5a14ac658424945f15177494ba1 — GuLoader
818284e7ea0a4bd64ba0eda664f51877ed8c6d35bf052898559dbf4ad8030968 — GuLoader
fa6ca0a168f3400a00dc43f1be07296f4111d7ad9b275809217a9269dd613ae8 — GuLoader
d5b3b1304739986298ba9b7c3ff8b40b3740233d6bb02437ce61a20ee87468bc — GuLoader
8495a328fdd4afd33c3336e964802018d44c1dda15b804560743d6276e926218 — GuLoader
ce2ea1807d984e1392599d05f7ab742bae4f20f8ef80c5a514fbdeede2ff7e55 — Quasar RAT
e933ec0f52cbc60b92134d48b08661b1af25c7d93ff5041fc704559b45bd85b8 — Netwire RAT
6db5e2bb146b11182f29d03b036af4e195044f0ef7a8f7c4429f5d4201756b8f — Cobalt Strike

f4fba2181668f766fdfbd1362420a53ac0b987f999c95baf5dbe235fd3bad4b8 — Cobalt Strike

ec2146655e2c04bf87b8db754dd2e92b8c48c4df47b64a9adc1252efd8618e62 — 假的登錄畫面

e5633d656dea530a62f5ad2792f253e74453712be34d2eadfb49190f7a9ee10b — 用於註冊 Helper Driver 的惡意 DLL

0440ef40c46fdd2b5d86e7feef8577a8591de862cfd7928cdbcc8f47b8fa3ffc — 具簽章的 Helper 驅動程式

5090f311b37309767fb41fa9839d2770ab382326f38bab8c976b83ec727e6796 — Sharphound

5e245281f4924c139dd90c581fc79105ea19980baa68eeccf5bf36ae613399b9 — PsExec

31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc — Mimikatz4

網路指標

hxxp://files[.]ddrive[.]online:444/load

hxxp://85.239.34[.]152/download/XWO_UnBkJ213.bin

hxxps://transmissive-basin[.]000webhostapp[.]com

hxxps://udapte[.]adesy[.]in

banqueislamik[.]ddrive[.]online

hxxps://transfer[.]sh/get/mKwvWI/NHmZJu.rtf

hxxps://transfer[.]sh/get/RTPlqa/oISxUP.rtf

hxxp://files[.]ddrive[.]online:4448/a

hxxp://banqueislamik[.]ddrive[.]online:4448/ZPjH

hxxp://46.246.86[.]12/ca3.exe

hxxp://178.73.192[.]15/ca1.exe

personnel[.]bdm-sa[.]fr

185.225.73[.]165

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。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

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，以及基於比原廠更孰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