巴西近 100 個組織成為銀行木馬的目標

2021 年 10 月 26 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

最近的行動顯示，這種活動對拉丁美洲的組織和個人來說是一個持續的威脅。

自 2021 年 8 月下旬以來，巴西多達 100 個組織成為銀行木馬的目標，最近的活動發生在 10 月初。

該行動似乎是 2020 年 ESET 研究人員所發佈的活動之延續。攻擊者似乎沒有因身分曝光而收斂，賽門鐵克（現為全球最大網通晶片公司--博通--BroadCom 的 ESD 企業安全部門）在最近的攻擊中發現了大量全新的入侵指標（IOC）。

賽門鐵克的威脅獵人團隊於 2021 年 9 月 30 日在客戶環境中發現可疑行動時，首次意識到這最新活動。我們的雲分析技術檢測到此初始可疑活動，進一步調查發現有人試圖將名為 mpr.dll 的可疑檔下載到客戶的環境中。Msiexec.exe 試圖從可疑的網址下載檔案。進一步分析顯示，下載了五個檔案，其中四個檔案具有簽章，似乎是合法的 DLL 檔，但名為 mpr.dll 的檔則無簽章，對於單一個 DLL 檔案佔有 588 MB 的容量來說，大到有點可疑。賽門鐵克研究人員得出結論，這是一個「拉丁美洲銀行木馬」，因為在本次行動中與ESET在 2020 年發佈對拉丁美洲銀行木馬的研究中看到相似的特徵和檔名。

我們的分析師進一步調查顯示，自 2021 年 8 月下旬以來，類似的活動一直針對多個不同的組織。事實上，多達 98 個組織可能成為類似活動的目標，所有受影響的組織都位於巴西。

這項活動所針對的行業包括資訊技術 (IT)、專業服務、製造業、金融服務和政府組織。

什麼是「拉丁美洲銀行木馬」？

銀行木馬是一種惡意軟體，被設計成可以竊取受害者的網路銀行資訊，讓惡意行動者可以存取受害者的銀行帳戶。一旦入侵電腦，惡意軟體通常藉由監視受害者正在存取的網站並將其與預定的清單進行比較。如果受害者瀏覽銀行網站，特洛伊木馬通常會在合法頁面上彈出假的登錄視窗，以試圖獲取受害者的銀行憑證。這些彈跳視窗通常模仿特定銀行的合法登錄頁面，並且很有說服力。

雖然曾經是網路犯罪領域最大威脅之一，但銀行木馬的鋒芒最近在世界許多地方已被勒索軟體取代。特別是在拉丁美洲，它們仍然主導著許多網路犯罪活動。

在其 2020 年報告中，ESET 確定有 11 個銀行特洛伊木馬集團在拉丁美洲活動，並且這些集團相互合作。之所以得出這個結論，是因為在拉丁美洲部署銀行木馬的網路犯罪分子，使用了許多共用戰術(手法)、技術和過程(程序) (TTP)。

最近活動的攻擊鏈

我們沒有觀察到此行動中最初的感染媒介是什麼，但它可能是利用垃圾郵件行動或惡意廣告傳播的惡意網址，這通常是拉丁美洲銀行特洛伊木馬行動的第一步。然後，受害者被連往到以下惡意網址：

- hxxps://centreldaconsulta[.]com/
- hxxps://www.centralcfconsulta[.]net/
- hxxps://centralcfconsulta[.]net/index3.php?api=vFUMIfUzGz2QdjxTFKAMyTlh
- hxxps://centralcfconsulta.net/
- hxxps://www.centralcfconsulta[.]net/index3.php?api=r0ubnHRxDycEy5uFPViNA55Y3t
- hxxps://www.centralcfconsulta[.]net/index3.php?api=4DQSbdp3hLqPRGTbOGtl7jCD9FKNViKXmKd9Lv
- hxxps://centreldaconsulta[.]com/index3.php?api=nJsdr1J3h0fsG18sRAVQt6JjVW
- hxxps://centreldaconsulta[.]com/index3.php?api=ThMyMCAQEOLIC9nO
- hxxps://www.centralcfconsulta[.]net/index3.php?api=wen1eIFCeUh0jAS3mWIDUhSLt3sXMQ

然後受害者被重導到 Amazon Web Services (AWS) 網址，攻擊者似乎濫用該網址作為命令和控制 (C&C) 伺服器，包含 Microsoft 軟體安裝程式 (MSI) 檔案的 ZIP 壓縮檔會從 AWS 環境中下載。

ESET 報告稱，在拉丁美洲部署銀行木馬的大多數集團已於 2019 年開始使用 MSI 檔作為初始下載。MSI 檔案可用於安裝、移除和更新在 Windows 系統上執行的應用程式。

如果受害者點擊兩下下載的壓縮檔內的MSI檔，它將執行 msiexec.exe，然後連接到第二台 C&C 伺服器以下載另一個包含有效籌載 (mpr.dll 的 ZIP 檔以及其他合法的可攜式執行檔 (PE))。觀察到 msiexec.exe 存取的網址包括：

- hxxp://13.36.240[.]208/ando998.002
- hxxp://13.36.240[.]208/msftq.doge
- hxxp://15.237.60[.]133/esperanca.lig2
- hxxp://15.237.60[.]133/esperanca.liga
- hxxp://52.47.163[.]237/microsft.crts
- hxxp://52.47.163[.]237/nanananao.uooo
- hxxp://15.237.27[.]77/carindodone.ways

該 ZIP 壓縮檔包含了重新命名的合法 Oracle 應用程式--VBoxTray.exe。這是利用 DLL 搜尋順序劫持來載入有效籌載 (mpr.dll) 而執行的。DLL 搜尋順序劫持利用 Windows 處理 DLL 的方式，允許攻擊者將惡意代碼載入到合法程序中。mpr.dll 檔也大於 100 MB，以規避向安全服務提交(後送給安全軟體判讀)，安全服務往往不會處理超過該大小的檔案。在 ESET 報告中詳述的銀行木馬活動中觀察到了這兩個檔以及完全相同的處理程序 (Process)。

然後為重新命名的 VBoxTray.exe 建立持久性以便始終通過 Windows 註冊表或 Windows Management Instrumentation (WMI) 將 mpr.dll 做側載。這是拉丁美洲銀行木馬攻擊鏈中使用的另一種常用技術。

對此活動保持警戒

此活動背後的攻擊者為逃避檢測而採取的各種步驟（例如：使用大檔作為有效籌載，使其不會被安全軟體掃描，以及利用合法處理程序 (Process) 和應用程式進行惡意目的）表明，此攻擊活動背後的人是相當老練精明、複雜的參與者。受此活動影響的組織數量也顯示，可能有大量人員負責此活動--並且可能有多個團體支援此活動。正如 ESET 所說，這可能是許多團體以合作的方式行事，在拉丁美洲營運的各種銀行木馬攻擊團體所採取的方法。

雖然勒索軟體目前主導了網路犯罪相關領域的大部分聲量，但重要的是要記住，它並不是唯一的威脅。銀行特洛伊木馬有可能成為個人和組織代價高昂的問題，因此人們，特別是那些位於拉丁美洲的人，在這種活動似乎特別流行的地方，需要對這種威脅保持警戒。

簡單的步驟（例如：確保您在所有金融帳戶上啟用了多重身份驗證）可以幫助減輕此類威脅的影響。

保護／緩解措施

賽門鐵克已經於第一時間提供多種有效保護。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.Bancos

有關最新的防護更新，請訪問賽門鐵克防護公告。

感染指標 (IOC:Indicators of Compromise)

IOC	說 明
ad6116abb88fd0383cf6f5a9f66a6ad8dda2be06bdc02a0fc071584689b69055	ZIP
0ee61e700ce0c71afe9bb2c8d7c253b560ddf535c3fd1f633b67e27f68731963	ZIP
35bbbe15471d45d7abb9300576eaee8f2f4d68d469b2cfc816342847e8f91db2	ZIP
cf7417c7dcaa27add45bfbba9984f40e0d11c24030a2036c44bd8591a54b4f8f	ZIP
dee81a0164862d8be16e42177be61d78e82c8e903cbae3686c170b7a81e41f24	ZIP
e0c2ce9a2f7ae075e2fee6960af3c69c45fc41ce101499e5697599389a35cb85	ZIP
ff8897e5fff9f76bf8d84d478d476f5a9278cbe0a355781224b69c0a28ab4540	ZIP
b0c1c6ee59144ae7fbed50a4da8abf8a04510759699076728f2ccfa45ac6fa37	ZIP
0cb4baaaad8751fe293739ddd874437b5b3c6e4ad72747bb9327db6cc74317a8	ZIP
1f6bc4e5c07c3c74764581f1b35c401a5857228a15948402a9bde765d6d58cb3	ZIP
2b85c92db126e93658f2e74da11b3a0ca8001a4f33f293b0e796d952c8d543d9	MSI
52c8236da569e448127dd0735943ae8ad16428e026883c78aae6b0853efc7ece	MSI
7cf033b0d80e07c2b5b0675c8aa09a3b3108135b9b2e1d053d52f19964eebc7d	MSI

IOC	說 明
8240909d109da9fd2969ff56bf64a8d75de256539dc825c0c5739b7dc57d5eb5	MSI
8cf0b8b993bba3b1aa3b4b7980d9d784b048dd45c47699a0e04121dd89f2152e	MSI
9aeb864a3e587bee375c20eb953750c62ecd58d8f7c1feb2212d3d027c74232f	MSI
b2c317529c7f95db85867bce6085878ed8db7bdb89f6283708b4261f73808b95	MSI
cd66d3f21ec3d4751df942e057e4cad548922f02a9d2253e402b5f7d878b3a39	MSI
cfe570c69f1794e9c6c950761f6f2cc1b553d53c82563982850ef8cb77442b35	MSI
d5bb070c69c88f3e8de09d17c77dd57bad9adde8c03d625f4497d3a4bcc8892e	MSI
feb86261d3d6551d92fc1e5554f22a1e9aeece4b5ed5737587580613b6a1d55d	mpr.dll
e118e0898e000e10c26376d73f5571e2b185c2c4789ed9b5d36bce166dc1dd17	mpr.dll
5ee4719fc1be0238875ad3d79260d09677bf110b4add8057d767e34b5a3d716d	mpr.dll
2081f9406af8936ff0c638df9191da763848bea0aae328c54f8e18419d9cd0df	mpr.dll
86bb40de9a98c277d29a677b1c1a54f88741ebe9418e7354ec65519102703fb9	mpr.dll
160500920795f38338d2fa12be80fb7a52d804c3d843626832a42c93bd4d28ee	mpr.dll
61c0e242c7a959dd673a4abded8a47ab02b919319666d9e81f9ac213a08fc90e	mpr.dll
993017c033afb58545d0f5d76288d54bf008cfbc10e19794a152adf3b59f5fbf	mpr.dll
c01cf8ad6e85743ed687e131b53b90e8cee72d20b50f7faebd7ac793df1d1c1d	mpr.dll
2bb4f701a97222d52af5623dba6cd61cae37527a2dd866fe246bbb2f55bdceb4	mpr.dll
5516bfffad1229f65bee736bec6f121abcddab8b5f673d98836e9d68c67c8194	mpr.dll
939cdcfdd19b78ad35d1cad2af8baf31413d180639bb0022eb0796c82fcc64ef	mpr.dll
5e54d306f17f39b78ccc79cc19c12b0ff3ba1ea4e0785b58f9ff55e8b5578a07	mpr.dll
a1e414d88df22263827233fc65fc8e4114ded43b8d14bd1c09956d834eba525e	mpr.dll
hxxps://centreldaconsulta[.]com/	URL
hxxps://www.centralcfconsulta[.]net/	URL
hxxps://centralcfconsulta[.]net/index3.php?api=vFUMIfUzGz2QdjxTFKAMyTlh	URL
hxxps://centralcfconsulta[.]net/	URL
hxxps://www.centralcfconsulta[.]net/index3.php?api=r0ubnHRxDycEy5uFPViNA55Y3t	URL
hxxps://www.centralcfconsulta[.]net/index3.php?api=4DQSbdp3hLqPRGTbOGtl7jCD9FKNViKXmKd9Lv	URL
hxxps://centreldaconsulta[.]com/index3.php?api=nJsdr1J3h0fsG18sRAVQt6JjVW	URL
hxxps://centreldaconsulta[.]com/index3.php?api=ThMyMCAQEOLIC9nO	URL
hxxps://www.centralcfconsulta[.]net/index3.php?api=wen1eIFCeUh0jAS3mWIDUhSLt3sXMQ	URL
hxxp://13.36.240[.]208/ando998.002	URL
hxxp://13.36.240[.]208/msftq.doge	URL
hxxp://15.237.60[.]133/esperanca.lig2	URL
hxxp://15.237.60[.]133/esperanca.liga	URL
hxxp://52.47.163[.]237/microsft.crts	URL
hxxp://52.47.163[.]237/nanananao.uooo	URL
hxxp://15.237.27[.]77/carindodone.ways	URL

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/banking-trojan-latam-brazil
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。2021/10

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