勒索軟體組織使用新型客製化資料收集工具

2023 年 4 月 19 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

該工具允許攻擊者取得通常會被作業系統鎖定的資料

Play 勒索軟體組織正在使用兩種新的客製化工具，它可以羅列受攻擊網路上所有使用者和電腦，並從通常會被作業系統鎖定的磁碟區陰影複製服務 (VSS) 中複製檔案。

Grixba

Symantec 的研究人員發現的第一個工具是 Grixba(Infostealer.Grixba)，它是一個網路掃描工具，用於列出網域中的所有使用者和電腦。(賽門鐵克已於 2019 年第四季正式合併為博通 (BoradCom) 的軟體事業部的企業安全部門

攻擊者使用基於 .NET 的竊密程式，藉由 WMI、WinRM、遠端註冊表和遠端服務來羅列出電腦中的軟體和服務。惡意軟體檢查安全防護軟體和備份軟體、遠端管理工具和其他程式是否存在，並將收集到的資訊保存在 CSV 檔中，然後壓縮成 ZIP 檔案，以便攻擊者進行手動滲透。

Play 勒索軟體組織利用 Costura 開發 Grixba 程式，Costura 是一個流行的 .NET 開發工具，用於將應用程式所依賴的多個項目 (DLL檔) 併入一個執行檔中。這種方式消除程式及其依賴項目需要分別部署的需求，使分享和部署應用程式更加容易。Costura 將一個 costura.commandline.dll 檔嵌入應用程式中，讓 Grixba 使用它來解析指令。

Symantec 對 Grixba 樣本進行分析，發現了以下幫助訊息和功能：

幫助訊息

```
Type type -h for help
GRB_NET  1.1.2.0
Copyright Zabbix 2022ERROR(8):
  Required option 'm, mode' is missing.
  Required option 'i, input' is missing.

-m, --mode            Required. GRB mode. scan/scanall/clr. scan -
network scanner. scanall - grab all.  clr - event logs cleaner.
-i, --input           Required. Input: f/r/s. f - file, r - range, s
- subnet, d - domain.
-d, --data            File.txt/127.0.0.1-127.0.0.255/127.0.0.1-24
-u, --username        Username for scanning
-p, --password        Password for scanning
-h, --help            (Default: ) Show help and usage.
-t, --threads         (Default: 150) Threads count. Max is 200.
Default 150.
-w, --wait            (Default: 5000) Wait time in ms. 1000 = 1s
-r, --remote_start    (Default: 0) Start remote services
-k, --domain_name     (Default: ) Domain name for Users and
Computers gathering. if not set will be used domain of current user.
--help                Display this help screen.
--version             Display version information.
```

圖1. Grixba 惡意軟體顯示的幫助訊息

掃描模式

掃描模式透過 WMI、WinRM、遠端註冊表和遠端服務來羅列軟體和服務。

用檢查以下 (幾乎檢查所有品牌的防毒軟體) 安全防護軟體是否存在：

- Defence
- Defender
- Endpoint
- AntiVirus
- BitDefender
- Kaspersky
- Norton
- Avast
- WebRoo
- AVG
- ESET
- Malware
- Defender
- Sophos
- Trend
- Symantec Endpoint Protection
- Security
- McAfee
- TotalAV
- pcprotect
- scanguard
- Crowdstrike
- Harmony
- SentinelOne
- MVISION
- WithSecure
- WatchGuard
- FireEye
- FSecure
- Carbon Black
- Heimdal
- HitmanPro
- VIPRE
- Anti-Virus
- DeepArmor
- Morphisec
- Dr.Web

它也會檢查以下的備份軟體 (幾乎檢查所有主流備份軟體) 是否存在：

- Veeam
- Backup
- Recovery
- Synology
- C2
- Cloud
- Dropbox
- Acronis
- Cobian
- EaseUS
- Paragon
- IDrive

接著檢查以下遠端管理工具是否存在：

- VNC
- Remote
- AnyDesk
- TeamViewer
- NinjaOne
- Zoho
- Atera
- ConnectWise
- RemotePC
- GoTo Resolve
- GoToAssist
- Splashtop SOS
- BeyondTrust
- Remote Desktop Manager
- Getscreen
- Action1
- Webex
- Atlassian
- Surfly
- Electric
- Pulseway
- Kaseya VSA
- XMReality
- SightCall
- DameWare
- ScreenMeet
- Viewabo
- ShowMyPC
- Iperius
- Radmin
- Remote Utilities
- RemoteToPC

最後，它檢查以下應用程式是否存在：

- Hitachi Storage Navigator Modular
- .NET
- Office
- Adobe
- Word
- Excel
- Java
- Office
- Learning
- DirectX
- PowerPoint

該惡意軟體隨後將所蒐集到的資訊存成 CSV 檔，並使用 WinRAR 將它們壓縮成一個名為 export.zip 的檔案。

Grixba 壓縮的 CSV 檔案清單：

- alive.csv
- wm.csv
- soft.csv
- all_soft.csv
- mount.csv
- users.csv
- remote_svc.csv
- cached_RDP.csv

掃描模式

掃描模式與 Scanall 模式類似，但會掃描更廣泛的程式。

清除模式

清除模式會從本地和遠端電腦中刪除日誌。它還會查找以下的登錄值：

SYSTEM\\CurrentControlSet\\services\\eventlog

SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\WINEVT\\Channels

使用 "EvtOpenLog" 和 "EvtClearLog" API 來刪除日誌，並從 Windows 的事件追蹤機制 "Microsoft-Windows-WMI-Activity" 刪除 WMI 活動日誌。

VSS 複製工具

最近，Play 勒索軟體組織還使用另一個基於 .NET 的可執行程式，也是使用 Costura 工具開發的。

Costura 將 AlphaVSS 類別庫嵌入可執行檔中。 AlphaVSS是 .NET 框架的一個類別庫，提供一個高階界面與 VSS 進行互動。該類別庫通過提供一組可控制的 API，使 .NET 程式更容易與 VSS 進行交流。開發人員可以使用這些 API 來生成、管理和刪除陰影複本，以及存取有關現有陰影複本的資訊，例如：檔案大小和狀態。

Play 勒索軟體組織新開發的工具使用 AlphaVSS 從 VSS 快照中複製檔案。該工具羅列 VSS 快照中的檔案和資料夾，並將它們複製到目標目錄中。讓攻擊者在加密之前從受感染的電腦上的 VSS 卷冊中複製檔案。這使得攻擊者可以複製通常會被作業系統鎖定的檔案。

Play 勒索軟體背景資訊

Play 勒索軟體 (也稱為 PlayCrypt)，根據 Symantec 追踪發現是由 Balloonfly 組織所開發，並於 2022 年 6 月推出，之後發起多次著名的攻擊。如同現在大多數的勒索軟體一樣，Play 執行雙重勒索攻擊，也就是在加密之前就從受害者網路中洩露資料。雖然勒索軟體組織最初針對的是拉丁美洲的組織，特別是巴西，但很快就擴大其目標。

Play 組織以針對 Microsoft Exchange 漏洞 (CVE-2022-41080、CVE-2022-41082) 以及其他漏洞來獲得遠端程式碼執行 (RCE) 並滲透受害者網路而聞名。該組織還是最早開始使用間歇性加密的勒索軟體組織之一，這種技術可以更快地加密受害者的系統。這種手法包括僅加密目標檔案中的部分內容，這仍會使資料無法恢復。

Play 組織還引人注目的是，它似乎不是作為勒索軟體即服務 (RaaS) 而運做，而 Balloonfly 組織似乎既進行勒索攻擊又開發勒索軟體。

客製化工具的使用率正在上升

越來越多的勒索軟體組織使用客製化工具來進行攻擊。這可能包含許多原因，例如：使攻擊更有效率並減少滯留時間。客製化工具可以針對特定目標環境進行定制，使勒索軟體組織可以更快速、更有效率的進行攻擊。使用專有工具還可以使勒索軟體操作者更容易操作及控制。如果一個工具廣泛的被使用，它可能會被其他攻擊者進行逆向工程或更改，可能造成削弱初始攻擊的效果。藉由保持其工具的專有性和獨特性，勒索軟體組織可以維持其競爭優勢並最大化其利潤。

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)

如果入侵指標 (IOC) 是惡意的且我們可以取得該檔案，Symantec Endpoint 產品將檢測並封鎖該檔案。

SHA256

762bb8a7209da29afb89f7941ae1c00a04cf45a144c6c5dddcfa78ff0d941539 – Play ransomware
86e4e23f9686b129bfb2f452acb16a4c0fda73cf2bf5e93751dcf58860c6598c – SystemBC malware
f706bae95a232402488d17016ecc11ebe24a8b6cb9f10ad0fa5cbac0f174d2e7 – SystemBC malware
c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71193c – Infostealer.Grixba
453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb – Infostealer.Grixba
f71476f9adec70acc47a911a0cd1d6fea1f85469aa16f5873dd3ffd5146ccd6b – Infostealer.Grixba
a8a7fdbbc688029c0d97bf836da9ece926a85e78986d0e1ebd9b3467b3a72258 – NetScan
5ef9844903e8d596ac03cc000b69bbbe45249eea02d9678b38c07f49e4c1ec46 – NetScan
f81bd2ac937ed9e254e8b3b003cc35e010800cbbce4d760f5013ff911f01d4f9 – VSS copying tool
367d47ad48822caeedf73ce9f26a3a92db6f9f2eb18ee6d650806959b6d7d0a2 – WinRAR
6f95f7f53b3b6537aeb7c5f0025dbca5e88e6131b7453cfb4ee4d1f11eeaebfc – WinSCP
1409e010675bf4a40db0a845b60db3aae5b302834e80adeec884aebc55eccbf7 – PsExec

惡意連線

137.220[.]49.66 – SystemBC C&C
justiceukraine.com – SystemBC C&C

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy
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。2023/4

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。

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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。