Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

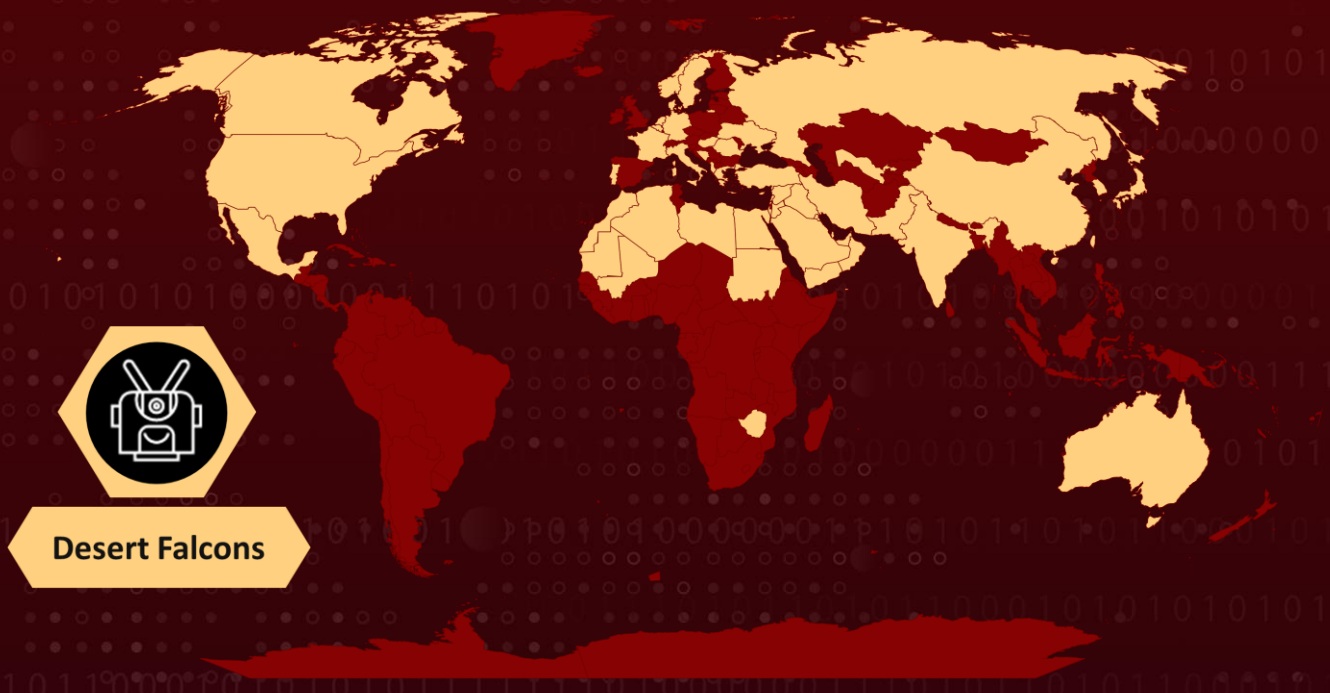
Desert Falcon Strikes with an Upgraded Arsenal

Date of Publication	Admiralty code	TA Number
April 11, 2023	A1	TA2023179

Summary

First Appearance: 2011
Actor Name: Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)
Target Industries: Government, Media, Financial, Research Institutions, Education, Activists, Political Leaders, Energy Firms, Physical Security Companies, Critical infrastructure, Defense, Transportation, Utilities, Aerospace, Think Tanks
Target Region: Akrotiri and Dhekelia, Albania, Algeria, Australia, Bahrain, Belgium, Bosnia and Herzegovina, Canada, China, Cyprus, Denmark, Egypt, France, Germany, Greece, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kuwait, Lebanon, Libya, Mali, Mauritania, Mexico, Morocco, Netherland, Netherlands, Norway, Oman, Pakistan, Palestine, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Korea, Sudan, Sweden, Syria, Taiwan, Turkey, UAE, Ukraine, USA, Uzbekistan, Yemen, Zimbabwe.
Malware: Micropsia backdoor and Arid Gopher info-stealer malware

Actor Map



Actor Details

#1

Starting in 2011, the cyber-espionage group known as Desert Falcon, which also goes by the aliases APT-C-23 and Mantis, began conducting its operations. The group's initial infections were reported in 2013, and it has since been known to target organizations located in Israel as well as numerous firms across various Middle Eastern countries.

#2

During their most recent attacks, the group employed enhanced versions of their custom Arid Gopher and Micropsia backdoors to gain access to their targets, followed by an extensive theft of credentials and exfiltration of stolen data. The primary function of Micropsia appears to be running secondary payloads for the Desert Falcon, and it is executed via WMI.

#4

The exact method of initial infection for this campaign is currently unknown. However, it is noteworthy that Desert Falcon has previously utilized tactics such as spear-phishing emails and the creation of fake social media profiles to entice their targets into installing malware on their devices.

#5

In one instance of this campaign, the group distributed three different versions of the same toolset across three groups of PCs within a targeted organization, possibly as a precautionary measure. Following this, Micropsia was deployed and executed, successfully establishing contact with a command and control (C&C) server.

#6

To execute and conceal their campaigns, Desert Falcon is known to utilize a collection of custom-built malware tools such as ViperRat, FrozenCell (aka VolatileVenom), and Micropsia can operate across Windows, Android, and iOS platforms. Arid Gopher, a variant of Micropsia malware, is coded in the Go programming language and was first identified in March 2022. The group's transition to Go is not unexpected, as it allows their malware to evade detection.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)	Gaza **MOTIVE** Information theft and espionage	Akrotiri and Dhekelia, Albania, Algeria, Australia, Bahrain, Belgium, Bosnia and Herzegovina, Canada, China, Cyprus, Denmark, Egypt, France, Germany, Greece, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kuwait, Lebanon, Libya, Mali, Mauritania, Mexico, Morocco, Netherland, Netherlands, Norway, Oman, Pakistan, Palestine, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Korea, Sudan, Sweden, Syria, Taiwan, Turkey, UAE, Ukraine, USA, Uzbekistan, Yemen, Zimbabwe.	Government, Media, Financial, Research Institutions, Education, Activists, Political Leaders, Energy Firms, Physical Security Companies, Critical infrastructure, Defense, Transportation, Utilities, Aerospace, Think Tanks

Recommendations

To avoid falling victim to cyber attacks, businesses must remain vigilant and take necessary precautions. While routine education and awareness training are important, it is crucial to also consider factors such as MFA fatigue and web browser hygiene. Additionally, it is important to always verify the authenticity of email attachments and avoid opening untrusted links. By implementing these measures, businesses can better protect themselves against potential threats.

It is recommended to take precautions against the shellcode deployed by Desert Falcon, which uses a 32-bit stager to download another stage from a command-and-control (C&C) server via a basic TCP-based protocol. The specific C&C server IP address and port number used by the attackers are 104.194.222[.]50 port 4444. Measures should be taken to block traffic to this IP address and port and monitor network traffic for any attempts to communicate with it.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1190 Exploit Public-Facing Application	T1566 Phishing
T1059 Command and Scripting Interpreter	T1053 Scheduled Task/Job	T1204 User Execution	T1047 Windows Management Instrumentation
T1543 Create or Modify System Process	T1574 Hijack Execution Flow	T1548 Abuse Elevation Control Mechanism	T1055 Process Injection
T1564 Hide Artifacts	T1562 Impair Defenses	T1070 Indicator Removal	T1036 Masquerading
T1212 Exploitation for Credential Access	T1056 Input Capture	T1083 File and Directory Discovery	T1046 Network Service Discovery
T1057 Process Discovery	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1001 Data Obfuscation
T1105 Ingress Tool Transfer	T1571 Non-Standard Port	T1047 Windows Management Instrumentation	T1566.002 Spearphishing Link

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	4840214a7c4089c18b655bd8a19d38252af21d7dd048591f0af12954232b267f,4a25ca8c827e6d84079d61bd6eba563136837a0e9774fd73610f60b67dca6c02,624705483de465ff358ffed8939231e402b0f024794cf3ded9c9fc771b7d3689,7ae97402ec6d973f6fb0743b47a24254aaa94978806d968455d919ee979c6bb4,8d1c7d1de4cb42aa5dee3c98c3ac637aebfb0d6220d406145e6dc459a4c741b2,b6a71ca21bb5f400ff3346aa5c42ad2faea4ab3f067a4111fd9085d8472c53e3,bb6fd3f9401ef3d0cc5195c7114764c20a6356c63790b0ced2baceb8b0bdac51,bc9a4df856a8abde9e06c5d65d3bf34a4fba7b9907e32fb1c04d419cca4b4ff9,d420b123859f5d902cb51cce992083370bbd9deca8fa106322af1547d94ce842

TYPE	VALUE
SHA256	0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311,3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529,82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4,85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097,cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341,f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8,21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8,58331695280fc94b3e7d31a52c6a567a4508dc7be6bdc200f23f5f1c72a3f724,5af853164cc444f380a083ed528404495f30d2336ebe0f2d58970449688db39e,0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038,1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa,211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d,d10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798,5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61f1db8793ee4,f38ad4aa79b1b448c4b70e65aecc58d3f3c7eea54feb46bdb5d10fb92d880203,c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b,f98bc2ccac647b93f7f7654738ce52c13ab477bf0fa981a5bf5b712b97482dfb,411086a626151dc511ab799106cfa95b1104f4010fe7aec50b9ca81d6a64d299,5ea6bdae7b867b994511d9c648090068a6f50cb768f90e62f79cd8745f53874d,6a0686323df1969e947c6537bb404074360f27b56901fa2bac97ae62c399e061,11b81288e5ed3541498a4f0fd20424ed1d9bd1e4fae5e6b8988df364e8c02c4e,1b62730d836ba612c3f56fa8c3b0b5a282379869d34e841f4dca411dce465ff6,220eba0feb946272023c384c8609e9242e5692923f85f348b05d0ec354e7ac3c
URLs	hxxp[:]//5.182.39[.]44/esuzmwmrtajj/cmsnvbyawttf/mkxnhqwdywbu
Domains	jumpstartmail[.]com paydayloansnew[.]com picture-world[.]info rnacgroup[.]com salimafia[.]net seomoi[.]net soft-utils[.]com chloe-boreman[.]com criston-cole[.]com
IPV4:PORT	104.194.222[.]50:4444

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks

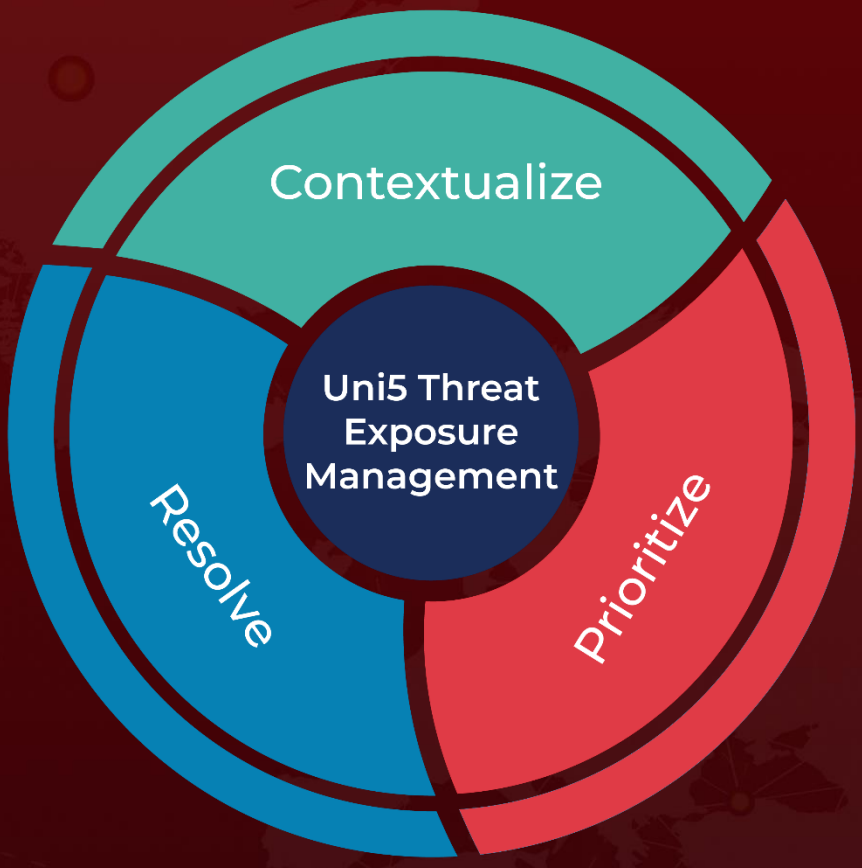
https://blog.talosintelligence.com/arid-viper-targets-palestine/

https://securelist.com/the-desert-falcons-targeted-attacks/68817/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 11, 2023 • 8:19 AM

More at www.hivepro.com