

Abstract

ClearSky discovered a new malware associated with the Iranian SiameseKitten (Lyceum) group with medium-high confidence.

The file is downloaded from a domain registered on June 6th, and it communicates with a previously unknown command and control server whose IP address is adjacent to that of the domain. This indicates an attacker-controlled at least two IP's on the same range.

The downloaded file is a reverse shell that impersonates an Adobe update. The group has previously used this method¹

The reverse shell is dropped by a parent file signed with a fake Microsoft certificate, along with a lure PDF document and an executable designed to establish persistence.

There seems to be a shared use of fake Microsoft certificates by a variety of Iranian groups, as Phosphorus was previously observed using the same method².

Additionally, the lure PDF document relates to drone attacks conducted in Iran, resembling a similar document previously employed by SiameseKitten³.



The attack scenario

¹ research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage

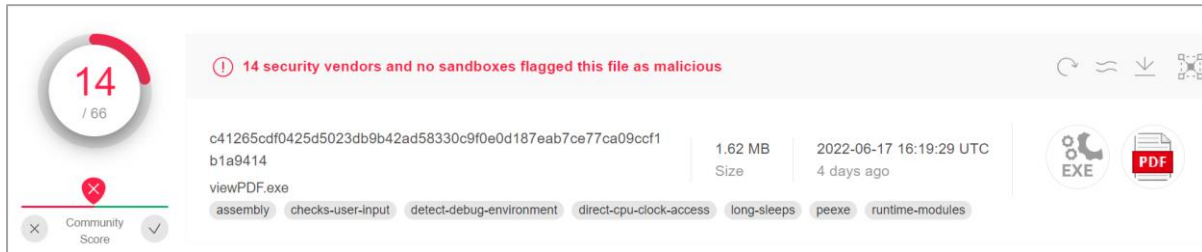
² deepinstinct.com/blog/iranian-threat-actor-continues-to-develop-mass-exploitation-tools

³ MD5 - 13814a190f61b36aff24d6aa1de56fe2 (File name: ir_drones.docm)

TTPs

Reverse Shell File

The reverse shell file's details are as follows:



File Name: viewPDF[.]exe

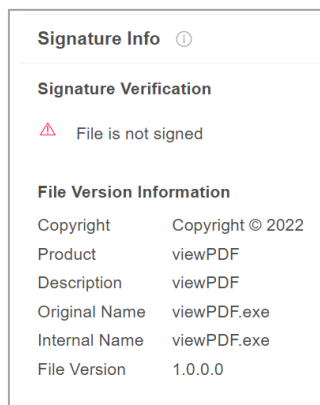
File Type: Win32 EXE

MD5: 7b4c70526b499e4d7f3d77a47235a67c

SHA-1: 8dbc4d59ba9f5c9b6b49cc9fbdbf8eef8cbdf972

SHA-256: c41265cdf0425d5023db9b42ad58330c9f0e0d187eab7ce77ca09ccf1b1a9414

The file appears to be an Adobe PDF document, using the company's icon and listing it in its details. An attempt was made by the attackers to avoid detection by registering the file as created on 29.06.2044



Following is the encrypted information relayed to the C&C server:

Network stream

89.39.149.18: 6500 VM: 64433

RAW data flow between two hosts

1 of 3 Hide all View HEX Text Highlight chars

00000000	23 31 7C 5A 6D 51 7A 4F 44 4A 69 4E 32 4E 69 4F	#1 ZmQzODJiN2NiO
00000010	57 49 34 4D 54 56 69 4E 6A 45 79 4E 47 56 6D 4D	WI4MTViNjEyNGVmM
00000020	7A 42 6C 59 54 55 31 4E 7A 64 68 5A 44 6C 38 4D	zB1YTU1NzdhdZD18M
00000030	48 78 44 4F 6C 78 56 63 32 56 79 63 31 78 68 5A	HxD01xVc2Vyc1xhZ
00000040	47 31 70 62 6C 78 42 63 48 42 45 59 58 52 68 58	G1pb1xBcHBEYXRhX
00000050	45 78 76 59 32 46 73 58 46 52 6C 62 58 42 63 64	ExvY2FsXFR1bXBcd
00000060	6D 56 79 59 6E 4D 75 5A 58 68 6C 23	mVyYnMuZXhl#

↓ Recv: 15 b Timeshift: 21813 ms Download

00000000 32 30 30 30 30 30 7C 59 58 56 30 62 77 3D 3D 200000|YXV0bw==

↑ Send: 169 b Timeshift: 21846 ms Download Hide

00000000	23 32 30 30 30 30 7C 61 75 74 6F 7C 31 23 23	#200000 auto 1#
00000010	32 31 30 30 30 30 7C 61 75 74 6F 7C 54 57 6C 6A	210000 auto TW1j
00000020	63 6D 39 7A 62 32 5A 30 49 46 64 70 62 6D 52 76	cm9zb2Z0IFdpbmRv
00000030	64 33 4D 67 57 31 5A 6C 63 6E 4E 70 62 32 34 67	d3MgW1Z1cnNpb24g
00000040	4D 54 41 75 4D 43 34 78 4E 6A 49 35 4F 53 34 30	MTAuMC4xNjI0S40
00000050	4D 7A 46 64 44 51 6F 6F 59 79 68 67 4D 6A 41 78	MzFdDQooYykgMjAx
00000060	4E 79 42 4E 61 57 4E 79 62 33 4E 76 5A 6E 51 67	NyBNaWNybnNvZnQg
00000070	51 32 39 79 63 47 39 79 59 58 52 70 62 32 34 75	Q29ycG9yYXRpb24u
00000080	49 45 46 73 62 43 42 79 61 57 64 6F 64 48 4D 67	IEFsbCByaWdodHMg
00000090	63 6D 56 7A 5A 58 4A 32 5A 57 51 75 44 51 6F 4E	cmVzZXJ2ZWQudQoN
000000a0	43 6B 4D 36 58 44 34 3D 23	CkM6XD4=#

After decrypting from base64, the following information is displayed:

Input
length: 106
lines: 1

|ZmQzODJiN2NiOWI4MTViNjEyNGVmMzB1YTU1NzdhdZD18MHxD01xVc2Vyc1xhZG1pb1xBcHBEYXRhXExvY2FsXFR1bXBcdmVyYnMuZXhl#

Output
time: 1ms
length: 78
lines: 1

fd382b7cb9b815b6124ef30ea5577ad9|0|C:\Users\admin\AppData\Local\Temp\verbs.exe

Input

start: 139 length: 139
end: 139 lines: 1
length: 0

TWlJcm9zb2Z0IFdpbmRvd3MgW1Z1cnNpb24gMTAuMC4xNjI5OS40MzFdDQooYykgMjAxNyBNawNyb3NvZnQgQ29ycG9yYXRpb24uIEFsbCByaWdodHMgcmVzZXJ2ZWQuDQoNckM6XD4

Output

start: 105 time: 0ms
end: 104 length: 104
length: -1 lines: 4

```

Microsoft Windows [Version 10.0.16299.431]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\>

```

It looks like a reverse shell waiting for instructions from the attacker, downloaded after the parent file is executed.

Parent File

The parent file's details are the following:

24

/ 66

24 security vendors and 1 sandbox flagged this file as malicious

8883bbd14017d0946aefd2c6fbc7b2c9b0b6b2439f96125bf4ae1c3d314a03c7

5.66 MB
Size

2022-06-18 08:07:38 UTC
3 days ago

C:\Users\JITech\Desktop\new malware samples extracted\8883bbd14017d0946aefd2c6fbc7b2c9b0b6b2439f96125bf4ae1c3d314a03c7.exe

64bits assembly direct-cpu-clock-access invalid-signature overlay peexe runtime-modules signed

File Name: irdrones1.exe, viewPDF.scr

File Type: Win32 EXE

MD5: 29b6b195cf0671901b75b7d2ac6814f6

SHA-1: 6745f60a8bf6a960d2617e6387f6748e03e13f7a

SHA-256: 8883bbd14017d0946aefd2c6fbc7b2c9b0b6b2439f96125bf4ae1c3d314a03c7

The file was initially submitted on June 6th, uploaded from the United Arab Emirates. Its creation date is registered as 25.06.2020, but the certificate shows 08.06.2022 as the signing date. This also aligns with common detection avoidance methods:

Signature Verification

⚠ A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

File Version Information

Date signed 2022-06-08 09:40:00 UTC

Signers

- Microsoft

Name	Microsoft
Status	The certificate or certificate chain is based on an untrusted root.
Issuer	Microsoft
Valid From	12:40 PM 06/08/2022
Valid To	12:40 PM 06/08/2023
Valid Usage	All
Algorithm	sha256RSA
Thumbprint	04C2D4C31313628066DC29C37AA4240765C3FA15
Serial Number	48 F9 4D ED B5 4C A0 22 B6 D8 30 41 46 57 B4 EC 57 B1 E9 9A

Its serial number cannot be verified, as it does not exist, indicating that it was faked to avoid detection. Checking URLs related to the file shows that it was downloaded from the following domain:

hxxp[:]//planet-informer[.]me/pdf/?id=1026&pid=316

8883bbd14017d0946aefd2c6fbc7b2c9b0b6b2439f96125bf4ae1c3d314a03c7

Help

DETECTION

DETAILS

RELATIONS

BEHAVIOR

CONTENT

SUBMISSIONS

ITW Urls ⓘ

Scanned

2022-06-16

Detections

0 / 95

Status

200

URL

http://planet-informer.me/pdf/?id=1026&pid=316

ITW Domains ⓘ

Domain

planet-informer.me

Detections

0 / 93

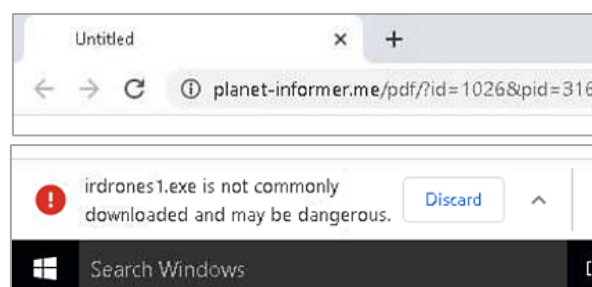
Created

2022-06-02

Registrar

NAMECHEAP INC







The link is active, and the file is functional at the time of writing this report:



The website's IP address is 89[.]39[.]149[.]19:

HTTP Requests	40	Connections	9	DNS Requests	9	Threats	1	Filter by IP or domain
Timeshift	Status	Rep	Domain	IP				
1036 ms	Responded	✖	accounts.google.com	172.217.23.109				
1041 ms	Responded	⚠	planet-informer.me	89.39.149.19				

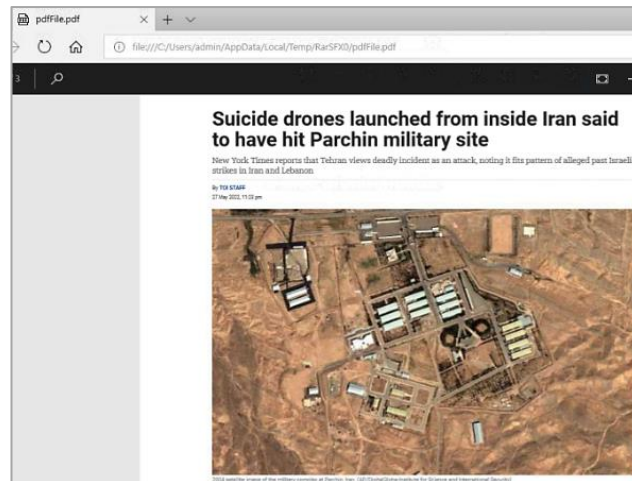
Once the file is downloaded, a C&C server with an adjacent IP address is contacted, 89[.]39[.]149[.]18 using port 6500:

HTTP Requests		53	Connections		25	DNS Requests		14	Threats		1	Filter by PID, domain, name or ip		PCAP
Contacts		Time	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN			
	309.08 s	TCP	✓	-	-			142.250.185.142	443	safebrowsing...	Google Inc.			
	362.31 s	TCP	?	-	-			89.39.149.18	6500	-	Data Room, Inc			

Both addresses belong to the same AS, and the same registry:

89.39.149.18	89.39.149.19
“ ip: "89.39.149.18",	“ ip: "89.39.149.19",
“ hostname: "breh.straetegy.com",	“ hostname: "znsjdg.preaue.com",
“ city: "Bucharest",	“ city: "Bucharest",
“ region: "București",	“ region: "București",
“ country: "RO",	“ country: "RO",
“ loc: "44.4323,26.1063",	“ loc: "44.4323,26.1063",
“ org: "AS19624 Data Room, Inc",	“ org: "AS19624 Data Room, Inc",
“ postal: "050011",	“ postal: "050011",
“ timezone: "Europe/Bucharest",	“ timezone: "Europe/Bucharest",

As shown in the following screenshots, the PDF File (.pdf) lure document used in this attack compares to the lure document used during a previously observed attack from March 2022:



Lure document used during the current attack



Lure document from March 2022

The parent file also downloads verbs.exe, an executable designed to establish persistence using the infected machine's Startup folder:

Timeshift	PID	Process name	Filename	Content
123.48 s	5516	cmd.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\verbs.exe	55.5 Kb executable

Indicators:

Type	Value
md5	29b6b195cf0671901b75b7d2ac6814f6
sha1	6745f60a8bf6a960d2617e6387f6748e03e13f7a
sha256	8883bbd14017d0946aefd2c6fbc7b2c9b0b6b2439f96125bf4ae1c3d314a03c7
md5	77d5ef3b26138baabf52fd14a0625298
sha1	ee2e63037f4a7717da62bb0c2c54b1f618d9df42
sha256	50e643e06c1fd6b334668439c1fb734c9d42707f80af2edbc0e5541513546fe

md5	b10a50cb12b82bde90124aad3f48180d
sha1	2bafc1d8f996b0f26cb70beafd00d5a0482c96bb
sha256	6d051c8954c7dab8b82f79779c0c630b95a9b8ad80a49658a55e0dfe6e5aba9f
md5	7b4c70526b499e4d7f3d77a47235a67c
sha1	8dbc4d59ba9f5c9b6b49cc9fbdbf8eef8cbdf972
sha256	c41265cdf0425d5023db9b42ad58330c9f0e0d187eab7ce77ca09ccf1b1a9414
domain	planet-informer.me
ip-dst	89.39.149[.]18
ip-dst	89.39.149[.]19

Mitre attack patterns:

Boot or Logon Autostart Execution - T1547

Command-Line Interface - T1059

ClearSky Cyber Security Intelligence Report



Ahead of the Threat Curve

2022 (C)All rights reserved to ClearSky Security Ltd.

TLP: WHITE - Subject to standard copyright rules, information may be distributed freely, without restriction.