DomainTools

THREAT BRIEF

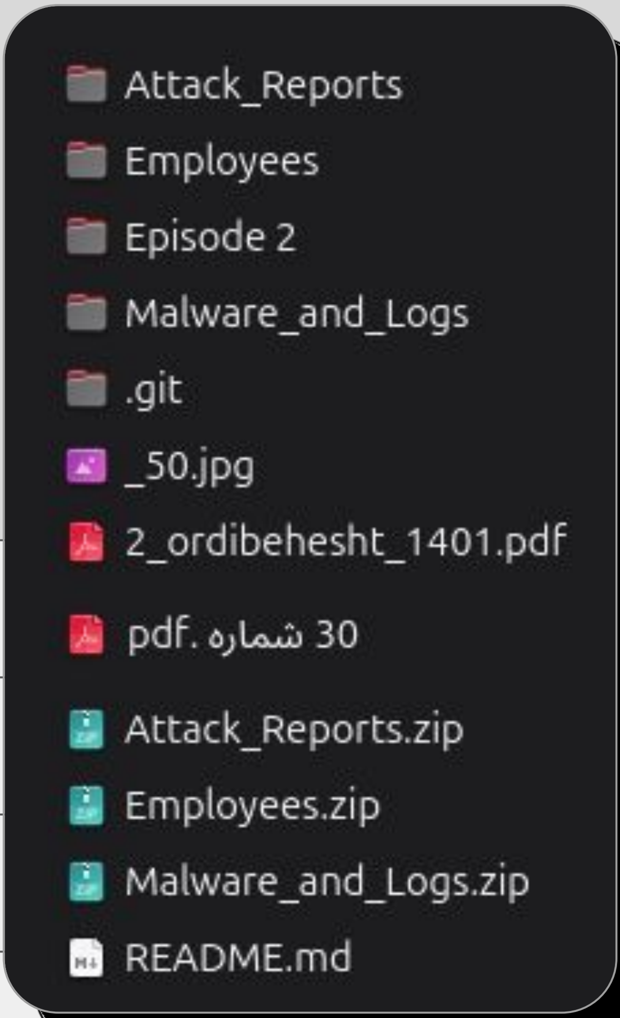
Inside APT 35:

The Operational Profile and Administrative Backbone of an Iranian Cyber Operator

DomainTools

Background

In October, 2025, internal documents from APT 35 (also referenced as “Charming Kitten”) were leaked on github. The documents revealed APT 35/Charming Kitten to be a bureaucratized intelligence collection apparatus with structured tasking, measurable outputs, supervisory oversight, and specialized teams with a focus on systematic access, sustained collection, and exploitable intelligence yields.



```
Attack_Reports
Employees
Episode 2
Malware_and_Logs
.git
_50.jpg
2_ordibehesht_1401.pdf
pdf. شماره 30
Attack_Reports.zip
Employees.zip
Malware_and_Logs.zip
README.md
```

DomainTools

Operational Profile

NAME:

APT 35, Charming Kitten, PHOSPHORUS (Microsoft), TA453 (Proofpoint), or APT 42 (Mandiant/Google)

MOTIVE:

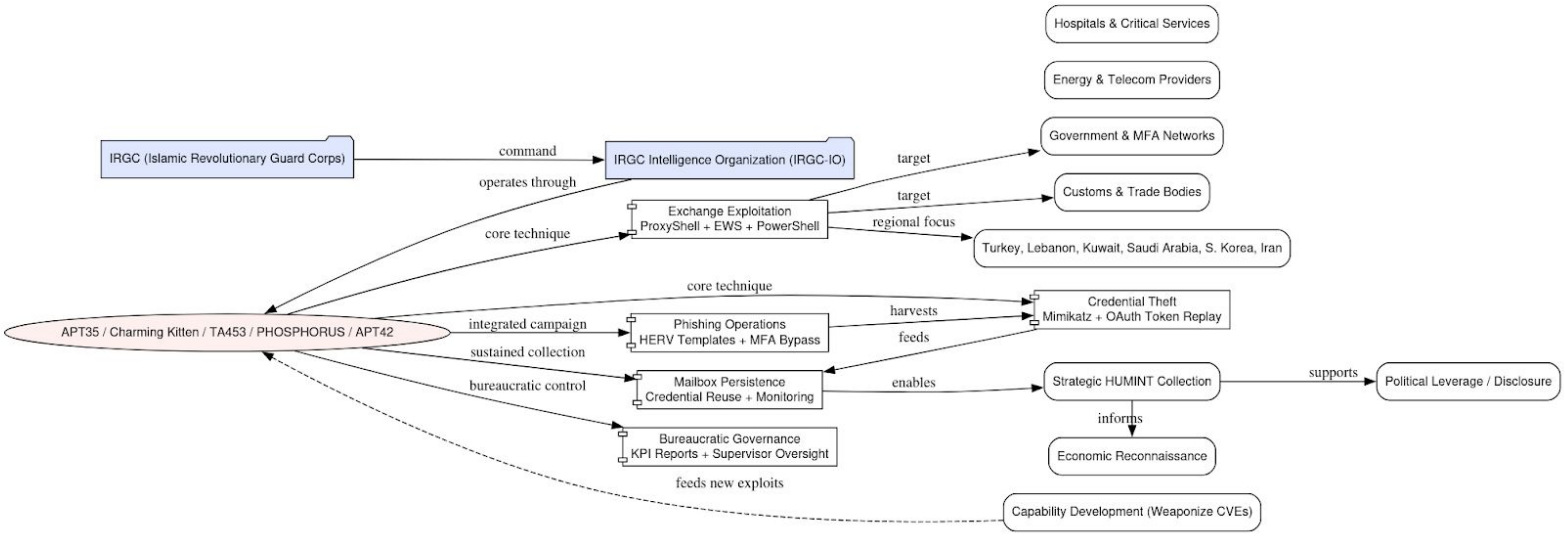
State-sponsored espionage, operating under the supervision of the Islamic Revolutionary Guard Corps Intelligence Organization

SIGNATURE:

Weaponized Exchange and Ivanti exploits leveraging ProxyShell chains, EWS enumeration, and PowerShell automation for Global Address List (GAL) and mailbox extraction.

TARGETS LEAKED:

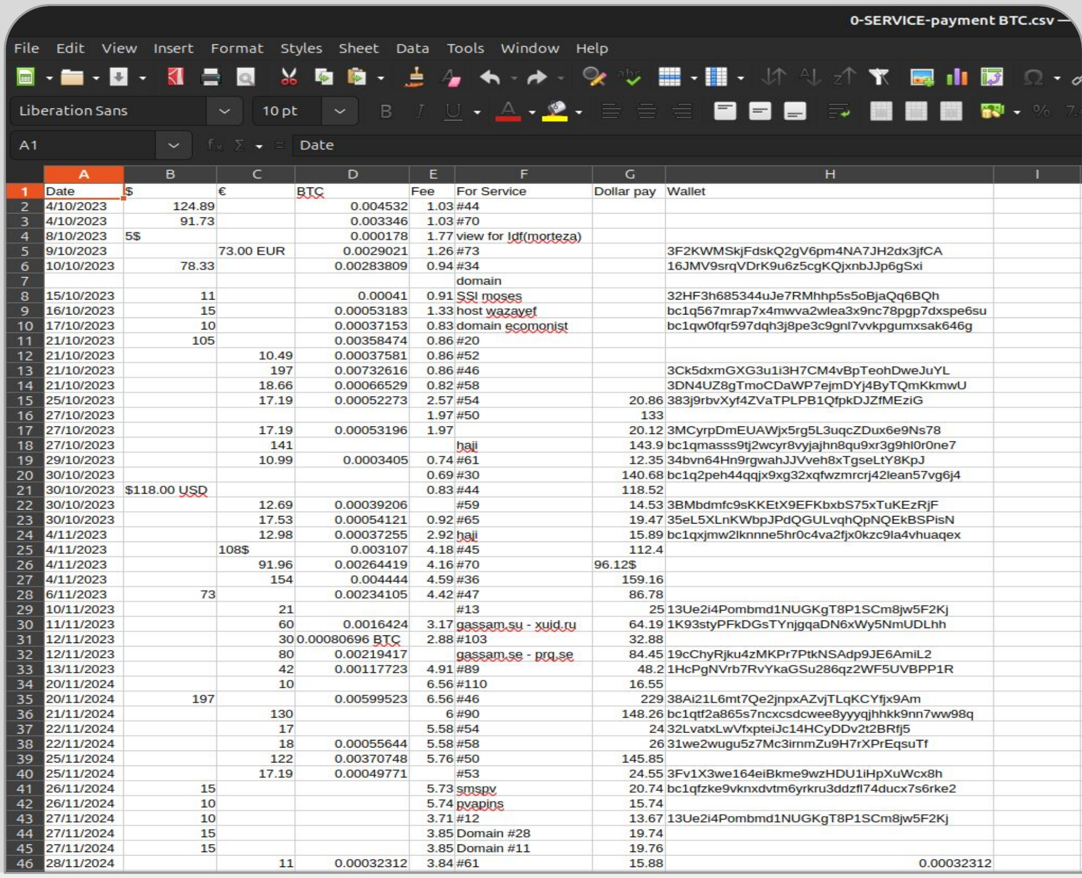
- *Türkiye* – Türk Telekom (212.175.168.58);
- *Saudi Arabia* – Nour Communication Co. Ltd (212.12.178.178);
- *Kuwait* – Fast Communication Company Ltd (83.96.77.227);
- *South Korea* – IRT-KRNIC-KR (1.235.222.140);
- *Türkiye/Jordan Campaign Overlap* – “Campaign Jordan (کمپین جردن)”;
- *Singapore* RIPE hosted relay (128.199.237.132);
- *Iran (Domestic)* – Pishgaman Tejarat Sayar DSL Network (109.125.132.66)


Hospitals & Critical Services
Energy & Telecom Providers
IRGC (Islamic Revolutionary Guard Corps)
command
IRGC Intelligence Organization (IRGC-IO)
target
Government & MFA Networks
operates through
target
Customs & Trade Bodies
Exchange Exploitation
ProxyShell + EWS + PowerShell
regional focus
core technique
Turkey, Lebanon, Kuwait, Saudi Arabia, S. Korea, Iran
core technique
Credential Theft
Mimikatz + OAuth Token Replay
harvests
APT35 / Charming Kitten / TA453 / PHOSPHORUS / APT42
integrated campaign
Phishing Operations
HERV Templates + MFA Bypass
feeds
sustained collection
Mailbox Persistence
Credential Reuse + Monitoring
enables
Strategic HUMINT Collection
supports
Political Leverage / Disclosure
bureaucratic control
informs
Bureaucratic Governance
KPI Reports + Supervisor Oversight
Economic Reconnaissance
feeds new exploits
Capability Development (Weaponize CVEs)

Financial Operations

Sanctions Evasion: Iran’s cyber apparatus, including APT 35, functions via a parallel digital micro-smuggling economy, utilizing tiny, repeatable crypto payments via a crypto gate small enough to slip under compliance radars.

Procurement Method: Cryptocurrency payments are funneled into a limited number of merchant endpoints, while the ledger documents the dispersed operational footprint, domains, virtual servers, and service nodes. Leaked files tied VPS payments paid through Cryptomus, routed through resellers in Cyprus, the Netherlands, and Central Europe, to specific operational artifacts like domains and services in use.



	A	B	C	D	E	F	G	H	I
1	Date	$	€	BTC	Fee	For Service	Dollar pay	Wallet	
2	4/10/2023	124.89		0.004532	1.03	#44			
3	4/10/2023	91.73		0.003346	1.03	#70			
4	8/10/2023	5$		0.000178	1.77	view for Idf(morteza)			
5	9/10/2023		73.00 EUR	0.0029021	1.26	#73		3F2KWMSkjFdskQ2gV6pm4NA7JH2dx3jfCA	
6	10/10/2023	78.33		0.00283809	0.94	#34		16JMV9srqVDrK9u6z5cgKQjxnbJJp6gSxi	
7						domain			
8	15/10/2023	11		0.00041	0.91	SSl moses		32HF3h685344uJe7RMhhp5s5oBjaQq6BQh	
9	16/10/2023	15		0.00053183	1.33	host wazayef		bc1q567mrap7x4mwva2wlea3x9nc78pgp7dxspe6su	
10	17/10/2023	10		0.00037153	0.83	domain ecomonist		bc1qw0fqr597dqh3j8pe3c9gnl7vvkpgumxsak646g	
11	21/10/2023	105		0.00358474	0.86	#20			
12	21/10/2023		10.49	0.00037581	0.86	#52			
13	21/10/2023		197	0.00732616	0.86	#46		3Ck5dxmGXG3u1i3H7CM4vBpTeohDweJuYL	
14	21/10/2023		18.66	0.00066529	0.82	#58		3DN4UZ8gTmoCDaWP7ejmDYj4ByTQmKkmwU	
15	25/10/2023		17.19	0.00052273	2.57	#54	20.86	383j9rbvXyf4ZVaTPLPB1QfpkDJZfMEziG	
16	27/10/2023				1.97	#50	133		
17	27/10/2023		17.19	0.00053196	1.97		20.12	3MCyrpDmEUAWjx5rg5L3uqcZDux6e9Ns78	
18	27/10/2023		141			haji	143.9	bc1qmasss9tj2wcyr8vyjajhn8qu9xr3g9hl0r0ne7	
19	29/10/2023		10.99	0.0003405	0.74	#61	12.35	34bvn64Hn9rgwahJJVveh8xTgseLtY8KpJ	
20	30/10/2023				0.69	#30	140.68	bc1q2peh44qqjx9xg32xqfwzmrcrj42lean57vg6j4	
21	30/10/2023	$118.00 USD			0.83	#44	118.52		
22	30/10/2023		12.69	0.00039206		#59	14.53	3BMbdmfc9sKKEtX9EFKbxbS75xTuKEzRjF	
23	30/10/2023		17.53	0.00054121	0.92	#65	19.47	35eL5XLnKWbpJPdQGULvqhQpNQEkBSPisN	
24	4/11/2023		12.98	0.00037255	2.92	haji	15.89	bc1qxjmw2lknnne5hr0c4va2fjx0kzc9la4vhuaqex	
25	4/11/2023		108$	0.003107	4.18	#45	112.4		
26	4/11/2023		91.96	0.00264419	4.16	#70	96.12$		
27	4/11/2023		154	0.004444	4.59	#36	159.16		
28	6/11/2023	73		0.00234105	4.42	#47	86.78		
29	10/11/2023		21			#13	25	13Ue2i4Pombmd1NUGKgT8P1SCm8jw5F2Kj	
30	11/11/2023		60	0.0016424	3.17	gassam.su - xuid.ru	64.19	1K93styPFkDGsTYnjgqaDN6xWy5NmUDLhh	
31	12/11/2023		30	0.00080696 BTC	2.88	#103	32.88		
32	12/11/2023		80	0.00219417		gassam.se - prq.se	84.45	19cChyRjku4zMKPr7PtkNSAdp9JE6AmiL2	
33	13/11/2023		42	0.00117723	4.91	#89	48.2	1HcPgNVrb7RvYkaGSu286qz2WF5UVBPP1R	
34	20/11/2024		10		6.56	#110	16.55		
35	20/11/2024	197		0.00599523	6.56	#46	229	38Ai21L6mt7Qe2jnpxAZvjTLqKCYfjx9Am	
36	21/11/2024		130		6	#90	148.26	bc1qtf2a865s7ncxcsdcwee8yyyqjhhkk9nn7ww98q	
37	22/11/2024		17		5.58	#54	24	32LvatxLwVfxpteiJc14HCyDDv2t2BRfj5	
38	22/11/2024		18	0.00055644	5.58	#58	26	31we2wugu5z7Mc3irnmZu9H7rXPrEqsuTf	
39	25/11/2024		122	0.00370748	5.76	#50	145.85		
40	25/11/2024		17.19	0.00049771		#53	24.55	3Fv1X3we164eiBkme9wzHDU1iHpXuWcx8h	
41	26/11/2024	15			5.73	smspv	20.74	bc1qfzke9vknxdvtm6yrkru3ddzfl74ducx7s6rke2	
42	26/11/2024	10			5.74	pvapins	15.74		
43	27/11/2024	10			3.71	#12	13.67	13Ue2i4Pombmd1NUGKgT8P1SCm8jw5F2Kj	
44	27/11/2024	15			3.85	Domain #28	19.74		
45	27/11/2024	15			3.85	Domain #11	19.76		
46	28/11/2024		11	0.00032312	3.84	#61	15.88	0.00032312	

Domain and Infrastructure Footprints

DOMAIN INFRASTRUCTURE:

The domain ecosystem uncovered in the dump reflects the familiar operational grammar of Iranian threat actors: disposable brands, thematic cover identities, and parallel infrastructure branches tailored to function, mission, and deniability. Operators distribute their presence across loosely coupled domains that mimic recruitment agencies, talent portals, religious fronts, job boards, and generic operational shells. The result is an environment where each hostname appears mundane in isolation.

MOSES STAFF CONNECTION:

The leaked files, including registered domain names, revealed the same administrative infrastructure supporting APT 35 also supported the hacktivist brand, Moses Staff. The same ProtonMail accounts and registrars supporting APT 35's domains also supported Moses Staff's domains, and Moses Staff first recorded activity aligns with entries in the financial ledgers.

DOMAIN CLUSTERS:

Moses Staff	moses-staff[.]io, moses-staff[.]to, and moses-staff[.]se
Internal-Use Operational Infrastructure	tecret.com, cavinet[.]org, kanplus[.]org, termite[.]nu, and dreamy-jobs[.]com.
Employment-themed social engineering	wazayif-halima[.]org, israel-talent[.]com, and israel-talent[.]xyz
Earlier Iranian influence operations - grassroots civic activism	bbmovements[.]com

The Role of DNS Intelligence

Examining the APT 35-linked domains in DomainTools opens up a multitude of investigative next steps. In addition to viewing each domain's predictive Risk Score (with the cluster having an average score of **68**), guided pivots reveal new connected infrastructure such as email addresses, name servers, ISPs, mail servers, and more.

For example, DomainTools connects the operational domain termite[.]nu to the Bulgarian ISP **S3 Company Ltd**. This ISP connects to 91 other domains which have a significantly high average Risk Score of **87** - an incredibly strong indicator of malicious intent.

S3 Company Ltd. Domains

DOMAIN NAME	FIRST SEEN	RISK SCORE
iranianwar[.]com	January 12, 2026	100
psdvault[.]cx	April 16, 2025	97
ecupanda[.]com	February 24, 2025	99
egvnsavzxphu[.]com	February 15, 2025	96
technologyonepro[.]com	February 11, 2025	97
payments-stage-ecu[.]com	January 19, 2025	99