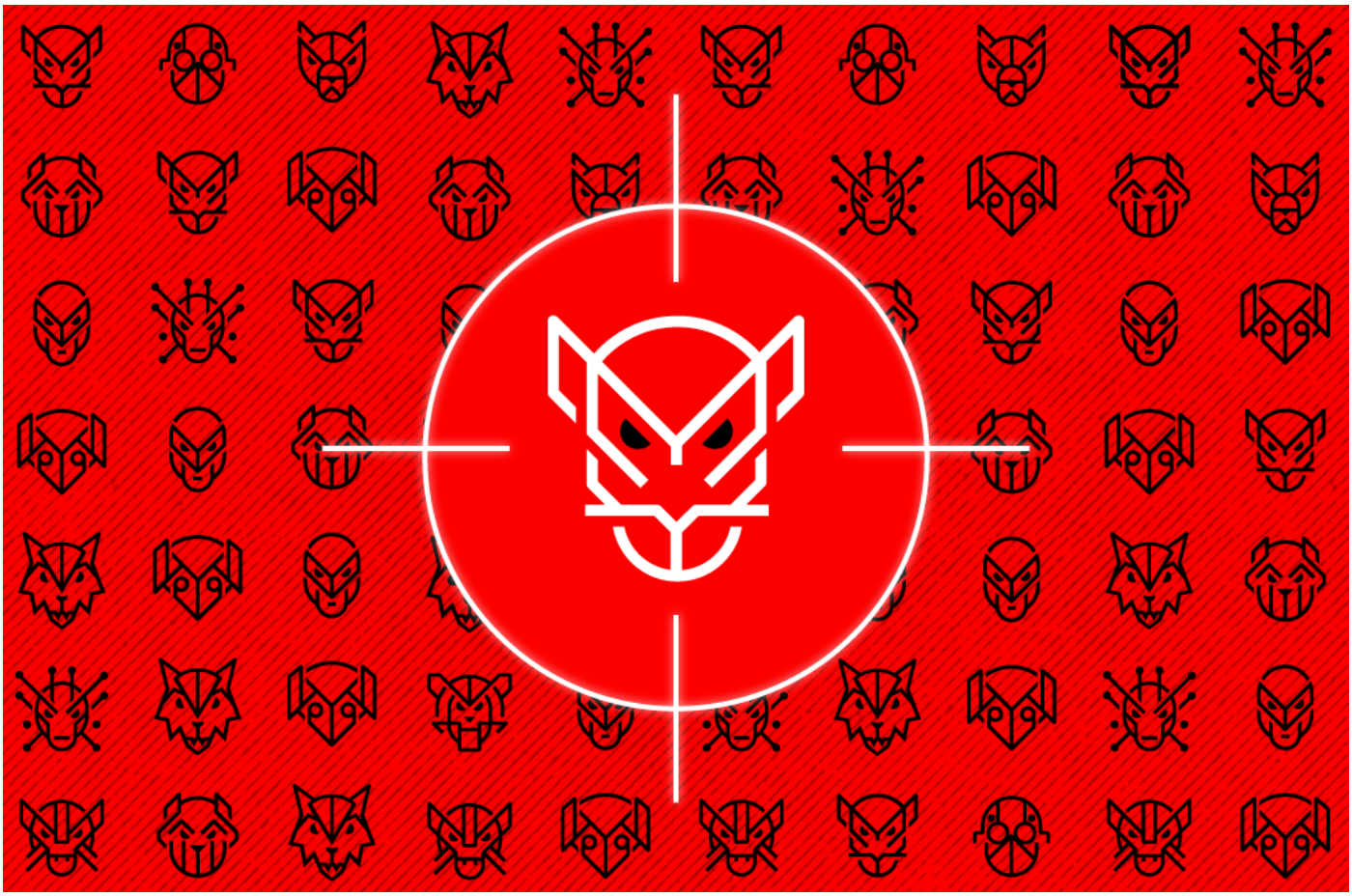
IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations

Counter Adversary Operations ⋮⋮ 11/9/2023



CrowdStrike Counter Adversary Operations has been investigating a series of cyberattacks and strategic web compromise (SWC) operations targeting organizations in the transportation, logistics and technology sectors that occurred in October 2023. Based on a detailed examination of the malicious tooling used in these attacks, along with additional reporting and industry reports, CrowdStrike Intelligence attributes this activity to the IMPERIAL KITTEN adversary.

Tune in to today's episode of the Adversary Universe podcast, "*Iran's Rise from Nascent Threat Actor to Global Adversary****" and learn about the history of cyber threat activity linked to Iran.***

CrowdStrike Intelligence collection has identified that contemporary IMPERIAL KITTEN intrusion chains leverage the following tactics, techniques and procedures:

- Use of public scanning tools, one-day exploits, SQL injection and stolen VPN credentials for initial access
- Use of scanning tools, PAExec and credential theft for lateral movement
- Data exfiltration by leveraging custom and open source malware to target Middle Eastern entities

CrowdStrike Intelligence analyzed several malware samples associated with IMPERIAL KITTEN activity, including:

- IMAPLoader, which uses email for command and control (C2)
- A similar sample named StandardKeyboard
- A malware sample that uses Discord for C2
- A Python generic reverse shell delivered via a macro-enabled Excel sheet

This next-stage tooling indicates IMPERIAL KITTEN continues to use email-based C2 mechanisms, similar to those used in their *Liderc* malware family.

Inside IMPERIAL KITTEN's Activity

IMPERIAL KITTEN is an Iran-nexus adversary with a suspected connection to the Islamic Revolutionary Guard Corps (IRGC). The adversary, active since at least 2017, likely fulfills Iranian strategic intelligence requirements associated with IRGC operations. Its activity is characterized by its use of social engineering, particularly job recruitment-themed content, to deliver custom .NET-based implants. Historically, IMPERIAL KITTEN has targeted industries including defense, technology, telecommunications, maritime, energy, and consulting and professional services.

Between early 2022 and 2023, CrowdStrike Intelligence observed IMPERIAL KITTEN conduct SWC operations with a focus on targeting organizations in the transportation, logistics and technology sectors. In a SWC, the adversary attempts to compromise victims based on their shared interest by luring them to an adversary-controlled website.

To date, the following adversary-controlled domains have served as redirect locations from compromised (primarily Israeli) websites, as well as locations where information collected to profile visitor systems is sent:

- `cdn.jguery[.]org`
- `cdn-analytics[.]co`
- `jquery-cdn.online`
- `jquery-stack.online`
- `cdnpakage[.]com`
- `fastanalizer[.]live`
- `fastanalytics[.]live`
- `hotjar[.]info`
- `jquery-code-download[.]online`
- `analytics-service[.]cloud`
- `analytics-service[.]online`
- `prostatistics[.]live`

Early 2022 SWC domains used the Matomo analytics service[1] to profile users who visited the compromised Israeli websites. Later iterations of SWC domains use a custom script to profile the visitor by collecting their browser information and IP address, which is then sent to a hardcoded domain. Previously reported activity targeted organizations in the Israeli maritime, transportation and technology sectors.

Industry and CrowdStrike Intelligence collection reporting have described a malware family tracked as *IMAPLoader,* which is the final payload of the SWC operations. An analysis of IMPERIAL KITTEN's

campaigns, including the use of *IMAPLoader* and additional malware families, is below.

Initial Access

Industry reporting indicates in some instances, the adversary directly serves malware to victims from the SWC.[2] Consistent with prior CrowdStrike reporting on credential stealers from 2021, there is some evidence that IMPERIAL KITTEN targets organizations, such as upstream IT service providers, in order to identify and gain access to targets that are of primary interest for data exfiltration.

There is also evidence indicating their initial access vectors consist of:

- Use of public one-day exploits
- Use of stolen credentials to access VPN appliances
- SQL injection
- Use of publicly available scanning tools, such as nmap
- Use of phishing to deliver malicious documents

All assessments around initial access methods not previously documented in connection with IMPERIAL KITTEN activity carry low confidence based on uncorroborated single-source reporting.

Phishing

IMPERIAL KITTEN's phishing operations reportedly include the use of malicious Microsoft Excel documents. While the sample mentioned in October 2023 industry reporting is not publicly available, CrowdStrike Intelligence acquired a similar version of the delivery document.

The lure is a macro-enabled Excel sheet, likely created in late 2023 (SHA256 hash: `b588058e831d3a8a6c5983b30fc8d8aa5a711b5dfe9a7e816fe0307567073aed`).

Once the victim opens the file and enables macros, the document extracts the files `runable.bat`, `tool.bat`, and `cln.tmp`, and a copy of the Python 3.11 interpreter to the system's `%temp%` directory. The batch files create persistence via the registry Run key named `StandardPS2Key`, and run the main Python payload SHA256 hash: `cc7120942edde86e480a961fceff66783e71958684ad1307ffbe0e97070fd4fd` in 20-second intervals.

The Python payload is a simple reverse shell that connects to a hardcoded IP address on TCP port 6443. The shell sends a predefined challenge GUID (`3d7105f6-7ca1-4557-b48e-6b4c70ee55a6`) and expects the C2 to respond with a separate GUID (`fdee81e1-b00f-4a73-ae48-4a0ee5dee49a`) for authentication. The malware then reads commands in a loop, executes them and returns the result. The analyzed version supports the following commands:

- `cd` (change working directory)
- `run` (start subprocess with command)
- `set timer to` (change beacon interval)

The analyzed sample was configured with `x.x.x.x` as the C2 server. This is not valid and will result in an error — it is likely the result of a test build or third-party modification.

Lateral Movement

There is information to suggest IMPERIAL KITTEN achieves lateral movement through the use of PAExec (the open-source PsExec alternative) and NetScan, and uses ProcDump to dump the LSASS process memory for credential harvesting. Lastly, IMPERIAL KITTEN likely deploys custom malware or open source tooling, such as MeshAgent,[3] for data exfiltration. These assessments are made with low confidence as they rely on single, uncorroborated source reporting.

Adversary Tooling

IMPERIAL KITTEN operations reportedly leverage multiple tools, including custom implants; *IMAPLoader* and *StandardKeyboard*, which both use email for C2; and a remote access tool (RAT), which uses Discord for C2.

IMAPLoader is a malware family distributed as a dynamic link library (DLL) to be loaded via AppDomainManager injection.[4] It uses email for C2 and is configured via static email addresses embedded in the malware. Typographical errors in embedded folder names and log messages indicate the author is likely not a native English speaker. While timestamps are not available in most samples, the oldest version was first observed in the wild on September 1, 2022.

Table 1 gives an overview of the available samples and configured C2 email addresses. All of them share the same functionality, although the last sample (SHA256 hash: `32c40964f75c3e7b81596d421b5cefd0ac328e01370d0721d7bfac86a2e98827`) differs in naming of the IMAP folders and has only one configured C2 address, indicating it is possibly a development version.

The malware disguises itself as `StreamingUX Updater` and persists through a scheduled task of that name. It connects to `imap.yandex[.]com` over TLS and uses the built-in .NET IMAP library to create two folders for C2, prefixed with a randomly generated UUID (including a typographical error):

- `<UUID>-Recive`
- `<UUID>-Send`

IMAPLoader uses attachments in email messages to receive tasking and send replies. It hardcodes creation and modification dates of the attachment to 2018-12-05 and 2019-04-05, respectively.

Hash SHA256	C2 Email
`989373f2d295ba1b8750fee7cdc54820aa0cb42321cec269271f0020fa5ea006`	`leviblum@yandex[.]com`
`fa54988c11aa1109ff64a2ab7a7e0eeec8e4635e96f6c30950f4fbdcd2bba336`	`brodyheywood@yandex[.]com` `justin.w0od@yandex[.]com`
`5c945a2be61f1f86da618a6225bc9d84f05f2c836b8432415ff5cc13534cfe2e`	`n0ah.harrison@yandex[.]com` `giorgosgreen@yandex[.]com`
`87ccd1c15adc9ba952a07cd89295e0411b72cd4653b168f9b3f26c7a88d19b91`	`oliv.morris@yandex[.]com` `harri5on.patricia@yandex[.]com`
`32c40964f75c3e7b81596d421b5cefd0ac328e01370d0721d7bfac86a2e98827`	`d3nisharris@yandex[.]com` `hardi.lorel@yandex[.]com`

Table 1. IMAPLoader samples and C2 email addresses

Industry reporting also noted IMPERIAL KITTEN deploys a malware family named *`StandardKeyboard`*,[5] which shares similarities with the *IMAPLoader* malware family. *StandardKeyboard* also uses email for C2 communication, and the malicious code uses the same open source .NET library for communicating with IMAP

servers.[6] Unlike *IMAPLoader*, this malware persists on the infected machine as a Windows Service named `Keyboard Service`, created by the malicious .NET executable WindowsServiceLive.exe (SHA256 hash: `d3677394cb45b0eb7a7f563d2032088a8a10e12048ad74bae5fd9482f0aead01`). *StandardKeyboard*'s main purpose is to execute Base64-encoded commands received in the email body. The results will be sent to the following email addresses:

- `itdep[@]update-platform-check[.]online`
- `office[@]update-platform-check[.]online`

The email subject contains the MAC address of the infected machine prepended by "From: ". The body of the email contains Base64-encoded information listed in Figure 1, followed by the string `Sender: <MAC Address>`.

```
***Order: <command>
***Time: <unused integer value>
***Response: <command output>
***Exit: <command exit code>
***At: <attachment>
```

Figure 1. Data sent to the C2 after command execution

Before initiating the email communication with the C2, *StandardKeyboard* verifies the availability of internet connection by contacting Google DNS using ICMP and sending the string `hi there`.

Finally, CrowdStrike Intelligence collection identified another related malware family, posing as a CV creator that uses a company in the logistics sector as a lure (SHA256 hash: `1605b2aa6a911debf26b58fd3fa467766e215751377d4f746189566067dd5929`). The malware is heavily obfuscated and drops an embedded payload after multiple stages of decryption and deobfuscation. It establishes persistence through a scheduled task named `Windows\System\System`.

The final stage (SHA256 hash: `3bba5e32f142ed1c2f9d763765e9395db5e42afe8d0a4a372f1f429118b71446`) uses Discord for C2 and is most likely related to a phishing campaign observed in March 2022. It contains a rare prefix in its PDB path field of the PE header, which, aside from this sample, is only present in samples of *IMAPLoader* in CrowdStrike holdings.

Assessment

CrowdStrike Intelligence attributes the above activity, including the use of SWC and *IMAPLoader* and related malware families, to the IMPERIAL KITTEN adversary. This assessment, made with moderate confidence, is based on:

- The continued use of previously reported SWC infrastructure
- The continued use of email-based C2 and Yandex email addresses for C2
- Overlaps between *IMAPLoader* and the industry-reported *SUGARDUMP* malware family that targeted Israel-based transportation sector organizations in 2022[7]
- Continued focus on targeting Israeli organizations in the transportation, maritime and technology sectors, which is consistent with the adversary's target scope

- Use of job-themed decoy and lure content used in their malware operations

CrowdStrike Intelligence attributes the described initial access and post-exploitation methods to IMPERIAL KITTEN with low confidence. This assessment carries low confidence as it is based on single-source reporting that has not been corroborated.

MITRE ATT&CK

Tactic	Technique	Observable
Reconnaissance	T1590.005 – Gather Victim Network Information: IP Addresses	*IMAPLoader* beacons the victims public IP address obtained via a web service
Resource Development	T1584.006 – Compromise Infrastructure: Web Services	IMPERIAL KITTEN SWC is mostly based on compromised websites
Initial Access	T1189 – Drive-by Compromise	IMPERIAL KITTEN distributes malware through SWC
Execution	T1059.003 – Command and Scripting Interpreter: Windows Command Shell	*IMAPLoader* collects system information via cmd.exe scripts
	T1059.005 – Command and Scripting Interpreter: Visual Basic	IMPERIAL KITTEN installs Python backconnect shell via malicious visual basic scripts in Excel documents
	T1059.006 – Command and Scripting Interpreter: Python	Malicious Excel documents drop Python-based backconnect shell
Persistence	T1037.005 – Boot or Logon Initialization Scripts: Startup Items	*IMAPLoader* persists through the registry Run key
Defense Evasion	T1055 – Process Injection	*IMAPLoader* executes via AppDomainManager injection
	T1140 – Deobfuscate/Decode Files or Information	*IMAPLoader* and *SUGARRUSH* obfuscate C2 addresses via integer arrays
Discovery	T1518.001 – Software Discovery: Security Software Discovery	*IMAPLoader* enumerates installed antivirus software
Collection	T1005 – Data from Local System	*IMAPLoader* beacons local system configuration and username to C2
Command and Control	T1071.003 – Application Layer Protocol: Mail Protocols	*IMAPLoader*, *StandardKeyboard* and *SUGARRUSH* utilize email for C2
	T1095 – Non-Application Layer Protocol	The Python-based backconnect shell relies on raw sockets for communication
Exfiltration	T1041 – Exfiltration Over C2 Channel	All malware in this report exfiltrate data directly over the C2 protocol

Table 2. Mapping to the MITRE ATT&CK® framework

Appendix: IMPERIAL KITTEN Infrastructure

Virtual private server VPS infrastructure recently associated with IMPERIAL KITTEN tooling is included in Table 3. CrowdStrike Intelligence currently attributes this infrastructure to IMPERIAL KITTEN with low confidence based on the aforementioned reporting.

Domain	IP Address	Internet Service Provider
NA	`146[.]185.219.220`	G-Core Labs S.A.
NA	`193[.]182.144.12`	Interhost Communication Solutions Ltd.
NA	`194[.]62.42.98`	Stark Industries Solutions Ltd.

NA	64[.]176.165.70	AS-CHOOPA
NA	95[.]164.61.253	Stark Industries Solutions Ltd.
NA	95[.]164.61.254	Stark Industries Solutions Ltd.
NA	45[.]32.181.118	AS-CHOOPA
NA	193[.]182.144.120	Interhost Communication Solutions Ltd.
NA	64[.]176.164.117	AS-CHOOPA
NA	45[.]155.37.140	SHOCK-1
NA	192[.]71.27.150	Interhost Communication Solutions Ltd.
NA	185[.]212.149.35	Oy Crea Nova Hosting Solution Ltd.
NA	51[.]81.165.110	OVH SAS
NA	82[.]166.160.20	Cellcom Fixed Line Communication L.P.
NA	192[.]52.166.71	ASN-QUADRANET-GLOBAL
NA	162[.]252.175.48	M247 Europe SRL
NA	45[.]93.82.109	LLC Baxet
NA	77[.]91.74.230	Stark Industries Solutions Ltd.
NA	77[.]91.74.21	Stark Industries Solutions Ltd.
NA	195[.]20.17.14	CLOUD LEASE Ltd.
NA	185[.]253.72.206	O.M.C. Computers & Communications Ltd.
NA	185[.]220.206.251	O.M.C. Computers & Communications Ltd.
NA	185[.]241.4.7	O.M.C. Computers & Communications Ltd.
NA	195[.]20.17.198	CLOUD LEASE Ltd.
NA	45[.]93.93.198	O.M.C. Computers & Communications Ltd.
NA	83[.]229.81.175	O.M.C. Computers & Communications Ltd.
NA	146[.]185.219.97	G-Core Labs S.A.
NA	193[.]182.144.175	Interhost Communication Solutions Ltd.
NA	103[.]105.49.108	VMHaus Limited
NA	185[.]105.0.84	G-Core Labs S.A.
NA	45[.]81.226.38	Zomro B.V.
NA	149[.]248.54.40	AS-CHOOPA
NA	194[.]62.42.243	Stark Industries Solutions Ltd.
NA	94[.]131.114.32	Stark Industries Solutions Ltd.
NA	45[.]8.146.37	Stark Industries Solutions Ltd.
NA	45[.]155.37.105	SHOCK-1
NA	163[.]182.144.239	NATURALWIRELESS
NA	64[.]176.172.26	AS-CHOOPA
NA	77[.]91.94.151	Clouvider Limited
NA	95[.]164.18.234	Stark Industries Solutions Ltd.
NA	74[.]119.192.252	Stark Industries Solutions Ltd.
NA	82[.]166.160.26	Cellcom Fixed Line Communication L.P.
NA	64[.]176.165.229	AS-CHOOPA
NA	193[.]182.144.52	Interhost Communication Solutions Ltd.
NA	64[.]176.171.141	AS-CHOOPA
blackcrocodile[.]online	217.195.153[.]114	Shock Hosting
updatenewnet[.]com	**Prev:** 45.155.37.105	Edis Gmbh
link.mymana[.]ir	193.182.144[.]52	Edis Gmbh
NA	193.182.144[.]239	Edis Gmbh
NA	64.176.165[.]229	Choopa
NA	64.176.171[.]141	Choopa

NA	64.176.165[.]70	Choopa
NA	95.164.61[.]253	Stark Industries Solutions Ltd.
NA	95.164.61[.]254	Stark Industries Solutions Ltd.

Table 3. IMPERIAL KITTEN infrastructure

Footnotes

1. https://github.com/matomo-org/matomo
2. https[:]//www.pwc[.]com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html
3. https[:]//github[.]com/Ylianst/MeshAgent
4. https[:]//pentestlaboratories[.]com/2020/05/26/appdomainmanager-injection-and-detection/
5. https[:]//www.pwc[.]com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html
6. https[:]//github[.]com/smiley22/S22.Imap
7. https://www.mandiant[.]com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping