Imperial Kitten Group Deploys Novel Malware Families

Original report published on: November 09, 2023[1]

Executive Summary

CrowdStrike released an article on Imperial Kitten (also known as Yellow Liderc, Tortoiseshell, TA456, and Crimson Sandstorm), a cyber threat actor that has been conducting strategic web compromise (SWC) operations and cyberattacks against organisations in the transportation, logistics and technology sectors in October 2023.

IMPERIAL KITTEN is believed to be connected to the Islamic Revolutionary Guard Corps (IRGC) and likely serves Iranian strategic intelligence interests related to IRGC operations. Imperial Kitten's activity is characterised by its use of social engineering, especially job recruitment-themed content, to deliver custom .NET-based implants.

The threat actor has historically targeted industries such as defence, technology, telecommunications, maritime, energy, and consulting and professional services.

Background

Imperial Kitten uses social engineering (such as use of job-themed decoy and lure content), public scanning tools, one-day exploits, SQL injection, stolen Virtual Private Network (VPN) credentials, and custom and/or open-source malware to gain initial access, lateral movement, and data exfiltration.

The threat actor uses several malware families, including custom implants; IMAPLoader and StandardKeyboard, which both use email for command and control (C2) communication; and a remote access tool (RAT), which uses Discord messenger for C2 communication.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Implement and enforce strong password policies and multi-factor authentication (MFA)
- Ensure timely patching and updating of systems and applications to mitigate the risk of exploitation through known vulnerabilities.
- Regularly monitor the attack surface and examine any unusual activities that could signal the lateral movement of a threat actor or the presence of malware.
- Validate before adding malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).
- Closely monitor inbound and outbound network traffic for suspicious communications or data transmissions

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise[1]

SHA256 Hash	Description
b588058e831d3a8a6c5983b30fc8d8aa5a711b5dfe9a7e816fe0307567073aed	Macro-enabled Excel
cc7120942edde86e480a961fceff66783e71958684ad1307ffbe0e97070fd4fd	Python payload
32c40964f75c3e7b81596d421b5cefd0ac328e01370d0721d7bfac86a2e98827	IMAPLoader
989373f2d295ba1b8750fee7cdc54820aa0cb42321cec269271f0020fa5ea006	IMAPLoader
fa54988c11aa1109ff64a2ab7a7e0eeec8e4635e96f6c30950f4fbdcd2bba336	IMAPLoader
5c945a2be61f1f86da618a6225bc9d84f05f2c836b8432415ff5cc13534cfe2e	IMAPLoader
87ccd1c15adc9ba952a07cd89295e0411b72cd4653b168f9b3f26c7a88d19b91	IMAPLoader
d3677394cb45b0eb7a7f563d2032088a8a10e12048ad74bae5fd9482f0aead01	WindowsServiceLive.exe
1605b2aa6a911debf26b58fd3fa467766e215751377d4f746189566067dd5929	Pose as CV Creator
3bba5e32f142ed1c2f9d763765e9395db5e42afe8d0a4a372f1f429118b71446	Uses Discord for C2

Domain	Description
blackcrocodile[.]online	Malicious Domain
updatenewnet[.]com	Malicious Domain
link[.]mymana[.]ir	Malicious Domain
cdn[.]jguery[.]org	Malicious Domain
cdn-analytics[.]co	Malicious Domain
jquery-cdn.online	Malicious Domain
jquery-stack.online	Malicious Domain
cdnpakage[.]com	Malicious Domain
fastanalizer[.]live	Malicious Domain
fastanalytics[.]live	Malicious Domain
hotjar[.]info	Malicious Domain
jquery-code-download[.]online	Malicious Domain

analytics-service[.]cloud	Malicious Domain
analytics-service[.]online	Malicious Domain
prostatistics[.]live	Malicious Domain

IP Address	**Description**
146[.]185[.]219[.]220	Malicious IP
193[.]182[.]144[.]12	Malicious IP
194[.]62[.]42[.]98	Malicious IP
64[.]176[.]165[.]70	Malicious IP
95[.]164[.]61[.]253	Malicious IP
95[.]164[.]61[.]254	Malicious IP
45[.]32[.]181[.]118	Malicious IP
193[.]182[.]144[.]120	Malicious IP
64[.]176[.]164[.]117	Malicious IP
45[.]155[.]37[.]140	Malicious IP
192[.]71[.]27[.]150	Malicious IP
185[.]212[.]149[.]35	Malicious IP
51[.]81[.]165[.]110	Malicious IP
82[.]166[.]160[.]20	Malicious IP
192[.]52[.]166[.]71	Malicious IP
162[.]252[.]175[.]48	Malicious IP
45[.]93[.]82[.]109	Malicious IP
77[.]91[.]74[.]230	Malicious IP
77[.]91[.]74[.]21	Malicious IP
195[.]20[.]17[.]14	Malicious IP
185[.]253[.]72[.]206	Malicious IP
185[.]220[.]206[.]251	Malicious IP

185[.]241[.]4[.]7	Malicious IP
195[.]20[.]17[.]198	Malicious IP
45[.]93[.]93[.]198	Malicious IP
83[.]229[.]81[.]175	Malicious IP
146[.]185[.]219[.]97	Malicious IP
193[.]182[.]144[.]175	Malicious IP
103[.]105[.]49[.]108	Malicious IP
185[.]105[.]0[.]84	Malicious IP
45[.]81[.]226[.]38	Malicious IP
149[.]248[.]54[.]40	Malicious IP
194[.]62[.]42[.]243	Malicious IP
94[.]131[.]114[.]32	Malicious IP
45[.]8[.]146[.]37	Malicious IP
45[.]155[.]37[.]105	Malicious IP
163[.]182[.]144[.]239	Malicious IP
64[.]176[.]172[.]26	Malicious IP
77[.]91[.]94[.]151	Malicious IP
95[.]164[.]18[.]234	Malicious IP
74[.]119[.]192[.]252	Malicious IP
82[.]166[.]160[.]26	Malicious IP
64[.]176[.]165[.]229	Malicious IP
193[.]182[.]144[.]52	Malicious IP
64[.]176[.]171[.]141	Malicious IP
217[.]195[.]153[.]114	Malicious IP
45[.]155[.]37[.]105	Malicious IP
193[.]182[.]144[.]52	Malicious IP

193[.]182[.]144[.]239	Malicious IP
64[.]176[.]165[.]229	Malicious IP
64[.]176[.]171[.]141	Malicious IP
64[.]176[.]165[.]70	Malicious IP
95[.]164[.]61[.]253	Malicious IP
95[.]164[.]61[.]254	Malicious IP

Email	**Description**
harri5on.patricia[@]yandex[.]com	C2 Email Account
d3nisharris[@]yandex[.]com	C2 Email Account
hardi.lorel[@]yandex[.]com	C2 Email Account
itdep[@]update-platform-check[.]online	C2 Email Account
office[@]update-platform-check[.]online	C2 Email Account

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	T1590.005	Gather Victim Network Information: IP Addresses
Resource Development	T1584.006	Compromise Infrastructure: Web Services
Initial Access	T1189	Drive-by Compromise
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.005	Command and Scripting Interpreter: Visual Basic
	T1059.006	Command and Scripting Interpreter: Python
Persistence	T1037.005	Boot or Logon Initialisation Scripts: Startup Items
Defence Evasion	T1055	Process Injection
	T1140	Deobfuscate/Decode Files or Information
Discovery	T1518.001	Software Discovery: Security Software Discovery
Collection	T1005	Data from Local System
Command and Control	T1071.003	Application Layer Protocol: Mail Protocols

	T1095	Non-Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

References

1. ^ “IMPERIAL KITTEN Deploys Novel Malware Families”