Yellow Liderc ships its scripts and delivers IMAPLoader malware

By PricewaterhouseCoopers

Archived: 2026-04-05 16:17:29 UTC

Author: PwC Threat Intelligence

Executive summary

Since 2019, PwC has tracked an Iran-based threat actor we refer to as Yellow Liderc (a.k.a. Imperial Kitten, Tortoiseshell, TA456, Crimson Sandstorm). As reported in our previous Year in Retrospect publications,[1,2,3] this threat actor remains an active and persistent threat to many industries and countries, including the maritime, shipping and logistics sectors within the Mediterranean; nuclear, aerospace and defence industries in the US and Europe; and IT managed service providers in the Middle East.

In this blog we will cover a recently-observed sample of malware linked to Yellow Liderc that has been used alongside strategic web compromises. The following are the key points of our analysis:

- Between 2022 and 2023, the threat actor has conducted strategic web compromises to embed JavaScript which fingerprints website visitors and captures victim user location, device information, and time of visits. Targeting of these attacks have focused primarily on the maritime, shipping and logistics sectors, with some victims being served follow-on malware which we have named IMAPLoader.
- IMAPLoader is a .NET malware that has the ability to fingerprint victim systems using native Windows utilities and acts as a downloader for further payloads. It uses email as a C2 channel and is able to execute payloads extracted from email attachments and is executed via new service deployments.
- We have previously observed Yellow Liderc developing .NET malware which uses similar email-based C2 channels and hard-coded commands to gain information about the victim’s environment; however, IMAPLoader is executed via an injection technique known as 'AppDomain Manager Injection', a technique we have not observed Yellow Liderc using before.
- Additional analysis shows widespread phishing activity that have been conducted concurrently to the threat actor's strategic web compromises. This activity is used to deliver a malicious Excel file that drops a basic Python backdoor.

Introduction

Yellow Liderc is an Iran-based threat actor that has been active since at least 2018. As previously reported in our 2020 Year in Retrospect publication, Yellow Liderc is an Islamic Revolutionary Guard Corp. (IRGC) aligned threat actor, which focuses on targeting Aviation, Automotive, Aerospace and Defense, Logistics, Maritime and Information Technology organisations. Geographically, the threat actor focuses on targeting organsiations

throughout the Middle East, Europe, both North and South America and parts of South Asia. In 2021, open source reporting documented alleged connections between the threat actor and the IRGC,[4] which also aligns with our previous reporting.[5]

Yellow Liderc is known for a variety of tactics and techniques, including phishing, social engineering and strategic web compromises. The threat actor uses both custom and off-the-shelf malware including PowerShell backdoors and infostealers in order to gather information about victim systems. The threat actor has previously used macro enabled documents that drop a VBS script, commonly referred to as LEMPO, which establishes persistence, performs reconnaissance, and exfiltrates sensitive information. The threat actor often favours exfiltration of sensitive information to an actor-controlled email account via SMTPS or IMAP, and has been observed using both dedicated mailboxes and third party services for their email accounts.[7][8]

Strategic Web Compromises

Since 2022 Yellow Liderc has frequently compromised legitimate websites and inserted malicious JavaScript,[9,10,11] often referred to as a watering hole attack or strategic web compromise. The JavaScript is used by the threat actor to fingerprint website visitors by capturing user location, device, time of visits, etc. The script enables the actor to infect specific user systems, matching a target fingerprint, with malware and gain access to the organisation's network.

This activity has heavily focused on the maritime, shipping and logistics sectors within the Mediterranean. Previous open source reporting has described some of this specific targeting by the threat actor.[12,13] PwC has observed the following domains being actively used by Yellow Liderc throughout 2022 and 2023 in various watering hole attacks:

- ztransportorganizationil[.]xyz
- cdnpakage[.]com
- hotjar[.]info
- fastanalizer[.]live
- fastanalytics[.]live

In some attacks, the threat actor would serve malware to their targets upon visiting the infected websites because their fingerprints apparently indicated they could be a high value target. PwC observed a new sample of malware used in those later stages, which we have named IMAPLoader. We assess that IMAPLoader is a replacement to a Python-based IMAP implant the actor used in late 2021 and early 2022.[14] The overall functionality is similar to past malware leveraged by the threat actor, but IMAPLoader uses a new injection technique not previously seen with Yellow Liderc, and is detailed below.

IMAPLoader

The following sample is a DLL written in .NET and acts as a downloader, leveraging email communication as a means of command and control (C2) communication.

Filename	StreamingUX.dll
SHA-256	989373f2d295ba1b8750fee7cdc54820aa0cb42321cec269271f0020fa5ea006
File type	Win32 DLL
File size	175,104 bytes
Created	2022-12-18 12:27:50

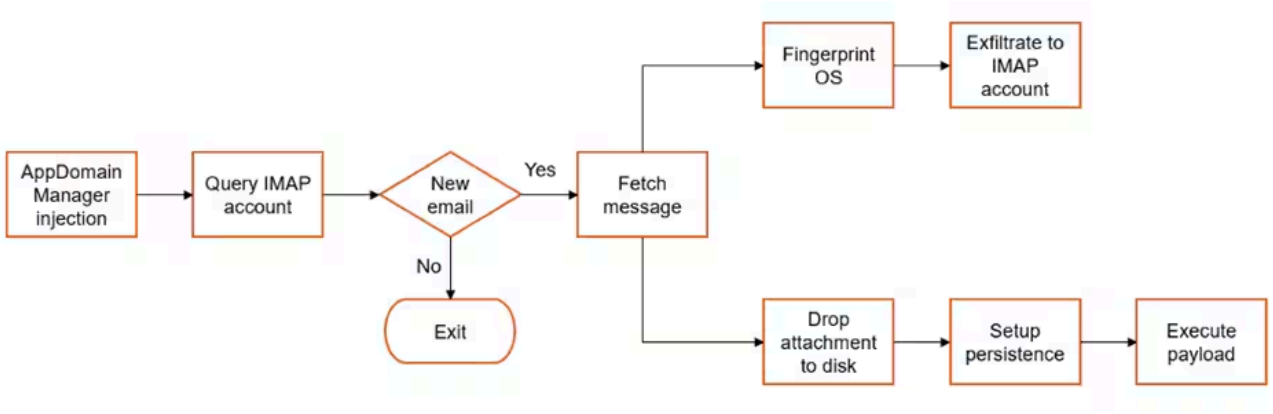

Figure 1 – Overview of IMAPLoader's functionality

In order to run, IMAPLoader uses an injection technique known as 'AppDomain Manager Injection',[15] which was first publicly disclosed in a proof of concept in 2020. The injection forces a Microsoft .NET application to load a specially crafted .NET assembly (IMAPLoader in this case). Upon execution, IMAPLoader extracts the full path to itself, and makes the Windows Console Window that is created when the application is started hidden from view. This is achieved by directly importing the Windows DLLs kernel32.dll and user32.dll and calling the GetConsoleWindow and ShowWindow APIs respectively.

The malware then queries the IMAP accounts (email addresses) hardcoded in the DLL which are both decimal encoded. These include two email addresses and passwords, which once decoded, show Yandex email addresses, a common email provider used by this threat actor:

- leviblum[@]yandex.com; and
- brodyheywood[@]yandex.com.

The malware then runs a WMI query to determine the operating system version, followed by scheduling tasks depending on the version identified. One of those tasks is to check for specific mailbox folders in a folder misspelled by the threat actor. Messages in the "Recive" folder are likely to contain further payloads as

attachments. IMAPLoader proceeds to compile a list of unseen messages in this folder and prepare for attachment extraction via the hard coded Yandex email addresses.

Depending on which Yandex account successfully logged in to, a new object imapClient3 is created which can interact with the remote email. By calling WMI class Win32_ComputerSystemProduct, IMAPLoader extracts the system UUID strings. This is later converted into a SHA-256 hash value and the first 21 characters (converted to uppercase) are used as an identifier in any further communication with the IMAP account. This likely indicates the Yandex accounts are intended for use across multiple victims, in contrast to their previous Python-based IMAP implant.

The briefly mentioned extraction of attachments uses the Ux.Attachment method to return a dictionary object, where the first entry is the name of the attachment (stored as a string), and the second entry stores the raw attached file as a byte object. The attachment is subsequently stored in the same location on disk as IMAPLoader. We also observed in the code that there is a persistence mechanism via Ux.EditTask. This method ensures persistence on the system for the new retrieved payload, which we assess is likely to be a PE executable file. The method is used to edit the Windows task (previously created by IMAPLoader as StreamingUX Updater [version number]) by updating the path to point to the new payload.

In the last chain of actions, the new payload is executed, by calling the ProcessStartInfo class. Finally, a new thread is created in the context of IMAPLoader which is used to fingerprint the system and exfiltrate collected content by sending an email to the same IMAP account used to retrieve the payload. While we have previously observed the threat actor developing .NET malware which uses similar email-based C2 channels and hard-coded commands to gain information about the victim's environment, IMAPLoader is executed via the 'AppDomain Manager Injection' technique, a technique we have not observed Yellow Liderc using before, which shows an evolution of this threat actors tools and techniques.

An early version of IMAPLoader

We detected another sample from September 2022 which we assess is an earlier version of IMAPLoader:

Filename	saveImapMessage.exe
SHA-256	32c40964f75c3e7b81596d421b5cefd0ac328e01370d0721d7bfac86a2e98827
File type	Win32 EXE
File size	170,496 bytes
Created	2101-11-11 01:04:26

PDB path	F:\vsp\saveImapMessage\saveImapMessage\obj\Debug\saveImapMessage.pdb

Although saveImapMessage.exe is an EXE file rather than a DLL, this shares a similar .NET file structure. It also contains the same functionality as our original sample (StreamingUX.dll) which in this case is located in a namespace called ‘downloader’. We also found a .NET DLL named JobTitle.dll which shares a partial PDB path with saveImapMessage.exe (F:\\vsp\) and drops a version of IMAPLoader to the victim’s system.

The infection chain for IMAPLoader is composed of three stages, using a decoy Excel document and legitimate Microsoft application for injection as seen in Figure 3.

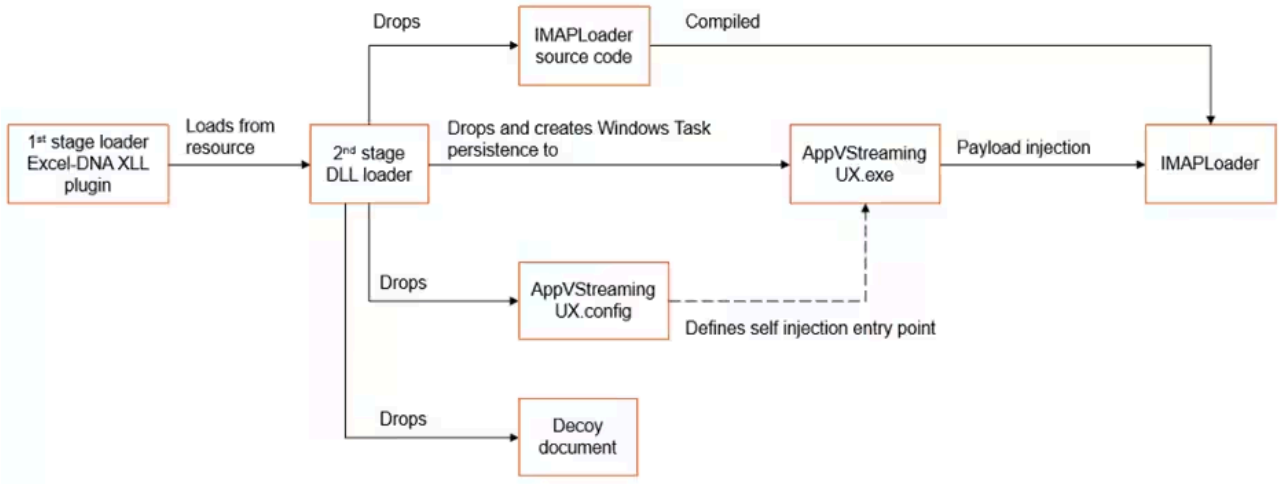

Figure 3 - Infection chain to deliver and execute IMAPLoader

Stage 1

The first stage is distributed as an Excel-DNA XLL plugin,[17] an open source library that enables .NET integration into Microsoft Excel files. One of its resources is called JOBTITLE which stores the 2nd stage component of the multi-part infection chain.

Stage 2

As soon as JobTitle.dll is executed, it writes a C# source code file named source.cs to disk. This is subsequently compiled into a .NET DLL file called sign.dll, a version of IMAPLoader, by leveraging the native C# compiler tool csc.exe.

Three additional files extracted by JobTitle.dll from its resources are also written to disk: a benign Microsoft Excel document, a modified Microsoft Windows application and an associated configuration file.

- The decoy document used by the threat actor to avoid raising victim suspicion during the execution chain;
- A configuration file used to trigger the injection of the IMAPLoader component into AppVStreamingUX.exe by leveraging the AppDomain Manager Injection technique previously mentioned;

and,

- AppVStreamingUX.exe appears to be a legitimate Microsoft Windows app that has been modified by the threat actor as the compilation timestamp is set to a future date. A new Windows Task called MicrosoftEdgeCrashFixsTaskMachineUA, is created and configured to load AppVStreamingUX.exe, which leads to the process self injection and the execution of the sign.dll binary, the third and last stage of the infection chain.

Stage 3

The last DLL has the same functionality as discussed in the earlier StreamingUX.dll IMAPLoader analysis. The email addresses used for C2 communication also match our earlier analysis indicating the threat actor has likely reused its infrastructure for different victims. As per the previous sample, host fingerprinting is performed at every new payload execution, by creating a new process and executing cmd.exe with the same parameters as before.

Additional phishing activity

Pivoting on the strategic web compromise infrastructure shows links to infrastructure we assess is likely used by Yellow Liderc in their phishing operations. For example, both ztransportorganizationil[.]xyz and officemicrosoftsign[.]com shared a resolution at IP 138.124.183[.]100. Many similar domains can be identified from additional pivots made on this threat actor's infrastructure that have been active since at least 2022, such as the one shown in Figure 4.

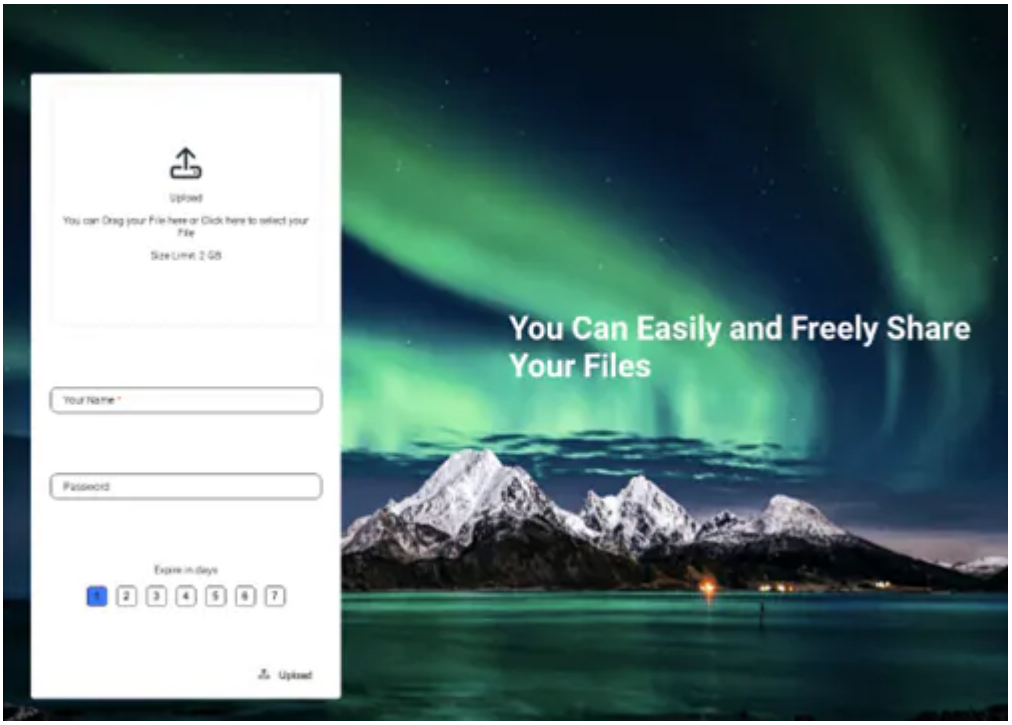

Figure 4 – Phishing page hosted on cheapfortest[.]store

All of this assessed phishing activity is likely aimed at a wider target audience, rather than solely focused on the maritime or shipping sectors within the Mediterranean. Some of the domains are generically themed around

Microsoft accounts which can be used against a wide variety of targets, while other domains are specifically aimed at the travel and hospitality sectors within Europe.

In some cases, the threat actor is likely credential harvesting based on observations of the phishing pages being served. For example, Figure 5 below, shows a generic Microsoft login page that Yellow Liderc is using to trick targets into entering their credentials. It is assessed that the likely delivery method of this and similar domains described throughout are sent via spear phishing emails.

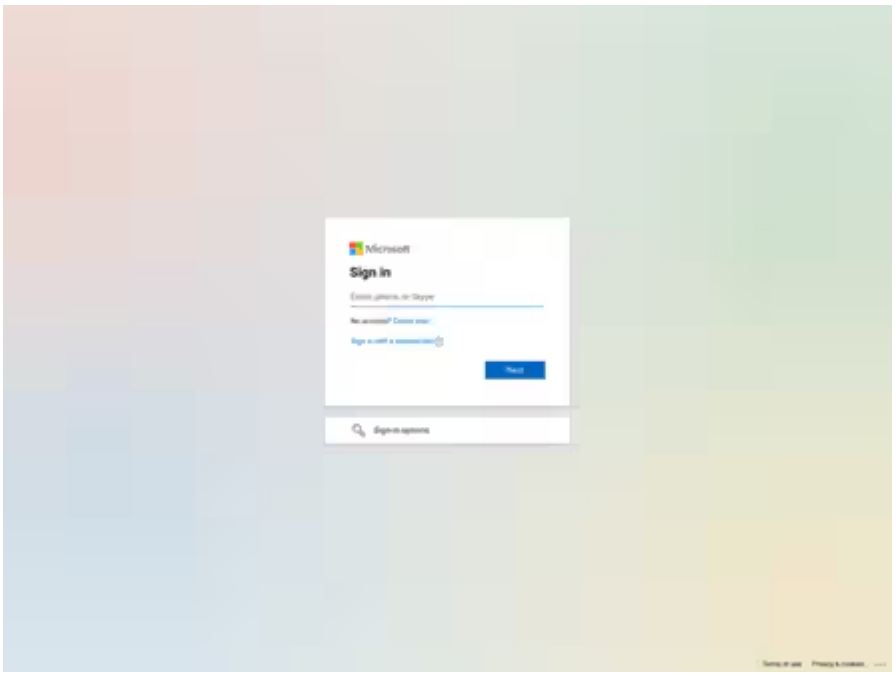

Figure 5 – Phishing page hosted on loginlive[.]formsmicrosoftoffice[.]com[.]oauth2[.]live

In other cases, malware is served to targets upon visiting the phishing website. For example, the threat actor served a macro-enabled Excel document that drops a VBScript. The use of macro-enabled documents that drop VBScripts is very similar to past Yellow Liderc activity which we have reported on privately,[18] alongside open source reporting.[19]

Filename	income_statement1.xlsm
SHA-256	1a996d98ab897bbc3a0249ea43afaf841b31396be7cbe61b443a58d1c9aab071
File type	XLSM
File size	3,122,078 bytes

Created	2011-05-30

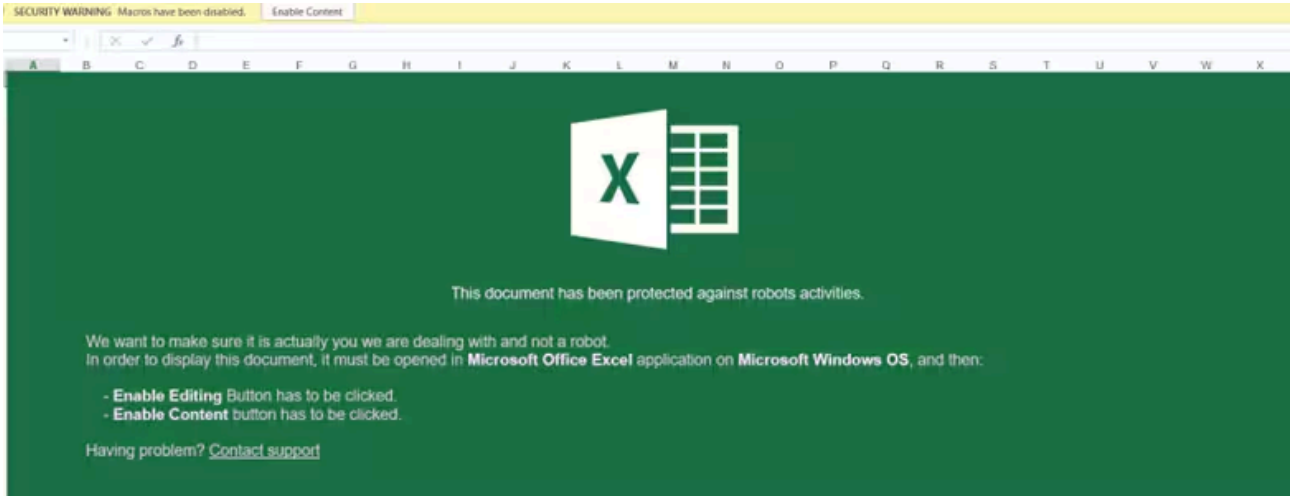

Figure 6 – Macro-enabled document served visiting phishing websites

Upon opening, the macro-enabled Excel document contains a custom message requesting the user to enable macros. Once enabled, the user is presented with a decoy document. The macro itself writes several files to disk including a chain of scripts that set up a registry run key for persistence, a Python payload, and a local copy of Python 3.11.

Filename	cln.tmp
SHA-256	cc7120942edde86e480a961fceff66783e71958684ad1307ffbe0e97070fd4fd
File type	TMP
File size	4,384 bytes

Conclusion

Yellow Liderc is a highly persistent threat that remains active in targeting organisations with the described strategic compromise tactics and phishing activity. Analysis of IMAPLoader shows an evolution of the threat actor's tools which will likely continue to evolve, as the threat actor stays focused on targeting a variety of sectors and regions which align with its strategic interests.

Overview of TTPs

PwC recommends searching historical logs and configuring alerting for the indicators or detection content provided in this report. If any of these indicators are discovered, or detection content generates alerts, we recommend organisations investigate their origin and conduct forensic analysis. If there are no significant findings, we recommend blocking the provided malicious indicators.

More detailed information on each of the techniques used in this report, along with detection and mitigations, can be found on the following MITRE pages:

Tactic	**Technique**	**ID**	**Procedure**
Resource Development	Establish Accounts: Email Accounts	T1585.002	The threat actor uses Yandex accounts for its C2 communication.
Resource Development	Develop Capabilities: Malware	T1587.001	We assess IMAPLoader is a bespoke .NET malware developed by the threat actor.
Resource Development	Compromise Infrastructure	T1584	The threat actor compromises legitimate websites to host malicious files and scripts.
Reconnaissance	Gather Victim Host Information	T1592	The threat actor fingerprints website visitors by capturing user location, device, and time of visits.
Initial Access	Drive-by Compromise	T1189	The threat actor compromises a legitimate website and injects some form of malicious code such as JavaScript.
Execution	Command and Scripting Interpreter: JavaScript	T1059.007	The threat actor uses JavaScript to execute fingerprint users or download and executing script files.

Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	IMAPLoader issue commands to discover system, network and user information via cmd.exe.
Execution	User Execution: Malicious File	T1204.002	The macro-enabled document requires a user to open and interact with the file to execute the payload.
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005	Scheduled tasks are used to maintain persistence for payloads.
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	The macro writes several files to disk including a script that establishes persistence with reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v StandardPS2Key /d %temp%\hed.vbs /f.
Defense Evasion	Masquerading: Masquerade Task or Service	T1036.004	Task name and author mimics legitimate Microsoft Windows services.
Defense Evasion	Process Injection: Dynamic-link Library Injection	T1055.001	An injection technique called AppDomain Manager Injection is used to load IMAPLoader.
Discovery	System Information	T1082	WMI commands are used to obtain OS version.

	Discovery		
Discovery	System Network Configuration Discovery	T1016	Basic network information is obtained through ipconfig command.
Discovery	System Owner/User Discovery	T1033	Basic user information is obtained through whoami command.
Discovery	File and Directory Discovery	T1083	Directory listings are run using dir command.
Command and Control	Application Layer Protocol: Mail Protocols	T1071.003	The threat actor uses IMAP protocols to communicate via email C2.
Exfiltration	Exfiltration Over C2 Channel	T1041	IMAPLoader exfiltrates the results of system, network and user commands to the C2.

Indicators of Compromise

Malware Indicators

Indicator	**Type**
989373f2d295ba1b8750fee7cdc54820aa0cb42321cec269271f0020fa5ea006	SHA-256
32c40964f75c3e7b81596d421b5cefd0ac328e01370d0721d7bfac86a2e98827	SHA-256

3e3effa0388f362e891ccf6f9169f9fb9627698bea5fefa57084353603502886	SHA-256
528f4d63c5abcfd137569e2dda49b5730432fb189ef2263cd6e7222cbb6ccb75	SHA-256
91526246682b47e5f4e396130f2ff93943fbdcaf742262345fb35ae950f1d2b2	SHA-256
26881615e121584b8814916d2f0228de97439cf6b654fca58b2228ff893fcfbc	SHA-256
92687d1f47244d3a1d7b02fbccf389b9819fd7cc3a31036ae30c2d4d88a3f266	SHA-256
9fcb7dea92ad0fe5fa6d6a5a5bd47caea5d3bc44aee247a001fcefdc56500111	SHA-256
7bf2aaf5f82ba5ed834b6ee270e4a7326a191985ea6cc27bdaba17816d1f2ca9	SHA-256
d3677394cb45b0eb7a7f563d2032088a8a10e12048ad74bae5fd9482f0aead01	SHA-256
ebf2ec38ed0c4cd05aaae1bdb4af862294d8bd874f7830c42f6905e94de239cf	SHA-256
0ec131ca6fae3272025774731374620 86b3ce3130896fd8d8db69247ac720f04	SHA-256
87ccd1c15adc9ba952a07cd89295e0411b72cd4653b168f9b3f26c7a88d19b91	SHA-256
cc7120942edde86e480a961fceff66783e71958684ad1307ffbe0e97070fd4fd	SHA-256
1a996d98ab897bbc3a0249ea43afaf841b31396be7cbe61b443a58d1c9aab071	SHA-256
c43ae2eaa8b134861f4539b205bf97b4e6b3b857	SHA-1
35be50f7f7f47abe64e555cae3088f40b7b3ebbe	SHA-1

a20e34f575dc2816088d8a6ae0dc9940bd229e95	SHA-1
065a43ffd414f62efd779af4bfb5b9e9290bb3f2	SHA-1
48e30cd34178be36d7cfea2479361dd8280e726d	SHA-1
124d3cc91135766d4f93a5527bd323e1c23a3e2a	SHA-1
01b4ed3e7d026f9b9038e93bb3313602256aaf2f	SHA-1
5ceff2dbf7091c3906003bf5b77fd08deb71317e	SHA-1
8d2a0b8b94a1a0fc1d357737d06809b8aac93165	SHA-1
1860938bb192344df34b2ade9d804c91681d767d	SHA-1
64c06102653cd94b67417160b1ec61f240cd4d78	SHA-1
afa40f62a1df6a3949f46a61055be043cf9ff55d	SHA-1
ed7e2cd95b442a290478ae750794f0c346de8e73	SHA-1
0a3ec309299058c12a579c04d110001b77c311c5	SHA-1
97d132f248bc95ea2810a816574756f6	MD5
e78142f546f2972117db1d8403d556be	MD5
88ed93f824fbc5c73f7b47bf9d32b8e7	MD5

ee2de347c90c21e0e6917223c32ac61b	MD5
cb97310e5ca5ebc6a12358e97219487a	MD5
6bfb2b02992de48a0242a7ff03623205	MD5
6d02207c9ce1b3967077065c40eb1bb1	MD5
d009734407d38aac5735d182b0fffc86	MD5
366623939b90fdf277b43f457ac7b2ed	MD5
0df7bda8bfbb5828ca09fff7e70b34b8	MD5
50516ccade993979b18d7896ff17c3c9	MD5
d9d153b162a8edab7841e9747a086e2c	MD5
a6b68493ace6398f95fc5720b1a16526	MD5
20507d265a7495cc1e4ade1e8639666e	MD5
StreamingUX.dll	Filename
saveImapMessage.exe	Filename
JobTitle.dll	Filename
sign.dll	Filename

StandardKeyboard.exe	Filename
WindowsServiceLive.exe	Filename
income_statement1.xlsm	Filename
cln.tmp	Filename
leviblum[@]yandex.com	Email address
brodyheywood[@]yandex.com	Email address
hardi.lorel[@]yandex.com	Email address

Network Indicators

Indicator	**Type**
criticimfreedom[.]site	Domain
megamodel[.]studio	Domain
instructables[.]live	Domain
instructables[.]service	Domain
outlookmicrosoftonline[.]com	Domain
nirsoft[.]app	Domain

nirsoft[.]ink	Domain
mentalfloss[.]live	Domain
myfridgefood[.]live	Domain
transportorganizationil[.]shop	Domain
metatransfer[.]online	Domain
msofficesign[.]com	Domain
fastanalytics[.]live	Domain
prostatistics[.]live	Domain
fastanalizer[.]live	Domain
cdnpakage[.]com	Domain
europetourtravels[.]world	Domain
europetourtravels[.]link	Domain
oauth2[.]online	Domain
oauth2[.]live	Domain
loginlive[.]formsmicrosoftoffice[.]com[.]oauth2[.]live	Domain

login[.]microsoftonilne[.]com[.]oauth2[.]online	Domain
192.254.71[.]7	IPv4
192.71.27[.]20	IPv4
193.182.144[.]68	IPv4
192.71.27[.]170	IPv4
195.20.17[.]237	IPv4
162.252.175[.]142	IPv4
64.46.102[.]11	IPv4
167.88.166[.]26	IPv4
188.227.58[.]158	IPv4
216.108.231[.]123	IPv4
79.132.128[.]169	IPv4
45.155.249[.]180	IPv4
45.133.16[.]108	IPv4
38.60.136[.]253	IPv4

45.138.27[.]3	IPv4
195.238.126[.]132	IPv4
94.131.114[.]48	IPv4
192.71.27[.]30	IPv4
193.182.144[.]185	IPv4
83.229.73[.]203	IPv4
77.91.74[.]5	IPv4
178.23.190[.]74	IPv4
94.131.114[.]23	IPv4
216.108.237[.]80	IPv4
104.238.156[.]70	IPv4
212.29.215[.]67	IPv4
212.150.236[.]253	IPv4
170.130.55[.]55	IPv4

1 PwC Cyber Threats 2020: A Year in Retrospect

2 PwC Cyber Threats 2022: A Year in Retrospect

3 PwC Cyber Threats 2022: A Year in Retrospect

4 https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/

5 CTO-TIB-20210211-02A - Caught in a .NET

6 https://www.proofpoint.com/uk/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

7 CTO-TIB-20210211-02A - Caught in a .NET

8 CTO-TIB-20220628-02A - Three varieties of Liderc

9 CTO-TIB-20221208-01A - Yellow Liderc ships its scripts

10 CTO-QRT-20230815-01A - Yellow Lidercs recent script activity

11 CTO-QRT-20230418-01A - Yellow Liderc strikes again

12 https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping

13 https://www.clearskysec.com/fata-morgana/

14 CTO-TIB-20220628-02A - Three varieties of Liderc

15 ‘AppDomain Manager Injection: New Techniques For Red Teams’, Rapid7, https://www.rapid7.com/blog/post/2023/05/05/appdomain-manager-injection-new-techniques-for-red-teams/ (5th May 2023)

16 GitHub, ‘netbiosX/GhostLoader’, https://github.com/netbiosX/Ghostloader

17 Excel-DNA, ‘Excel-DNA’, https://excel-dna.net/

18 CTO-TIB-20210730-01A - Eat, Sleep, Liderc, Repeat

19 https://www.proofpoint.com/uk/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

---