Iranian “Dream Job” campaign

Ver 1.1
11/24

TLP: Clear www.clearskysec.com

Contents

Iranian Dream Job campaign

Executive Summary

ClearSky Cyber Security has uncovered the infrastructure of an Iranian campaign targeting the aerospace industry by distributing the SnailResin malware via a scheme of a “dream job” offering, AKA the Iranian “Dream Job” campaign.

“Dream Job” is a campaign in which the adversary manipulates the targets by offering them a "dream job", mainly to employees in aerospace, aviation, and defense.

Clear Sky Security uncovered[1] in August 2020 the first "Dream Job" campaign, run by North Korean Lazarus Group.

https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

We attribute the current "Dream Job" campaign to TA455, a subgroup of the Iranian threat actor "Charming Kitten". In the campaign, we discovered a file containing the SnailResin malware. Both SlugResin and SnailResin were attributed by Microsoft to a subgroup of charming kitten (also known as APT35 and Smoke Sandstorm[1]). Our investigation revealed that the malware is downloaded from a domain that impersonates a job recruiting website (recurring theme for the adversary), through which the recruiter's LinkedIn profile is revealed. The adversary appears to be using the same profile as in previous attacks.

Malware files were detected as Kimsuky/Lazarus APT groups by antivirus engines in a few cases instead of Charming Kitten.

We found significant similarities between the North Korean Lazarus APT Group and Charming Kitten attacks. There are several similarities between these two threat actors, including the use of the "Dream Job" luring campaign, the attack technique, and the use of several malware files to deploy malware through DLL Side Loading attacks.

The following conclusions can be drawn as a result:

- Charming Kitten impersonated the North Korean campaign to conceal their activities.

[1] security.microsoft.com/intel-explorer/articles/39a136d2?tid=ba71bfaa-87f8-4029-af04-f4eb1aa171f2

- North Korea shared with Iran their attack methods and tools, hence similarity in attack scenario and detection.

Iran's "Dream Job" campaign has been active since at least September 2023, constantly changing its infrastructure and malware. Mandiant published an article in February 2024 about "suspected Iranian espionage activity targeting the Middle East aerospace, aviation, and defense industries, especially in Israel and the United Arab Emirates (UAE), as well as possibly Turkey, India, and Albania.[2]

LinkedIn profiles of the "recruiters" identified in the current campaign are "newer versions" of those previously reported by Mandiant.

One profile we discovered was associated with a fake company called "Careers 2 Find" which previously worked for "1st Employer", a fake recruiting website highlighted by Mandiant in February.

TA455, also known as Smoke Sandstorm, BOHRIUM and Yellow Dev13, is a subgroup of Iranian threat actor **Charming Kitten** (**APT35**). TA455 targets organizations in Israel using double attack scenarios (two scenarios in one attack, one malicious and one for camouflage), DLL search order hijacking and masquerading as recruiters for companies, to target company employees with spear-phishing.

Charming Kitten also known as APT35, is an Iranian Advanced Persistent Threat (APT) group active in targeting various sectors for many years, especially focusing on governmental and military sectors. Charming Kitten frequently uses multi-stage infection chains designed to steal sensitive data and facilitate remote access for further exploitation.

In recent campaigns, Charming Kitten has leveraged social engineering tactics, primarily through phishing, to lure victims. This group is reportedly leveraging high-level obfuscation and custom malicious code to evade detection while delivering these payloads. Their methods align closely with command-and-control operations, which allow them to manage and exfiltrate data from compromised networks effectively. Charming Kitten’s focus in 2024 has intensified in Eastern Europe and Israel, likely influenced by the ongoing geopolitical tensions surrounding Iran’s alliances and interests, particularly against entities perceived as oppositional to Iranian geopolitical aims.

[2] cloud.google.com/blog/topics/threat-intelligence/suspected-iranian-unc1549-targets-israel-middle-east/

The group's technical sophistication is moderate to high, using both established RATs and complex, custom-built malware.

The group's infrastructure and campaign characteristics bear resemblance to previous Iranian state-backed campaigns but have adapted to bypass current security measures, with significant use of evasive techniques to ensure persistence within targeted networks. This ongoing threat has led cybersecurity firms to increase monitoring and mitigation efforts, specifically in sectors most affected by Charming Kitten's activities, such as governmental, military, and critical infrastructure organizations.

Techniques Employed by TA455 for Evading Detection

1. **Impersonating Other Threat Actors**: TA455 intentionally attempts to mislead investigators by mimicking the tactics and tools of other threat actors, specifically the North Korean Lazarus group. This includes utilizing similar "Dream Job" lures, attack techniques, and even malware files that overlap with those used by Lazarus in DLL side-loading attacks. This deliberate misattribution aims to create confusion and hinder accurate attribution efforts.

2. **Leveraging Legitimate Services:** To conceal their infrastructure and C2 communications, TA455 hides within the traffic of legitimate online services like Cloudflare, GitHub and Microsoft Azure cloud. Using Cloudflare for their malicious domains like "careers2find[.]com" helps to mask the true server location and ownership, making it harder to track their operations. Similarly, they exploit GitHub to host encoded C2 server information, retrieving it through seemingly innocuous accounts like "msdnedgesupport". This blending with legitimate traffic allows them to maintain a low profile and avoid raising red flags for security systems.

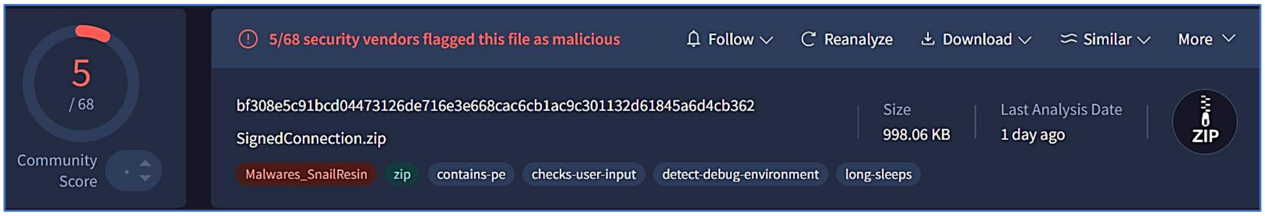
3. **Multi-Stage Infection Process:** TA455 uses a carefully designed multi-stage infection process to increase their chances of success while minimizing detection. The initial spearphishing emails likely contain malicious attachments disguised as job-related documents, which are further concealed within ZIP files containing a mix of legitimate and malicious files. This layered approach aims to bypass security scans and trick victims into executing the malware. Once executed, the malware performs various actions in stages, like checking the victim's IP address and retrieving C2 server information from compromised GitHub accounts, making it harder to detect and analyze the full scope of the attack.

4. **Exploiting Trust and Professional Networks:** By leveraging LinkedIn, a platform inherently built on trust and professional connections, TA455 seeks to gain credibility and avoid raising suspicion. Their use of fake recruiter profiles associated with fabricated companies further strengthens the deception and makes it more likely for victims to engage with their malicious links and attachments. This exploitation of a trusted platform allows them to bypass traditional security measures that might flag suspicious emails or websites.
5. **Constant Evolution of Infrastructure and Malware:** TA455 continuously modifies its infrastructure and malware, making it harder for security researchers and tools to keep up. Their constant adaptation, evidenced by changing domains, IP addresses, and malware variants, forces defenders to constantly update their defenses and makes it challenging to establish consistent detection patterns.
6. **Low Antivirus Detection Rates:** The malicious ZIP file used in the campaign was only flagged as malicious by five antivirus engines, with a primary misattribution to the North Korean Kimsuky group. This low detection rate highlights their ability to craft malware that evades traditional signature-based detection methods. This could be achieved through various techniques like obfuscation, encryption, or the use of one-day exploits.
7. **High-Level Obfuscation and Custom Code:** TA455's use of advanced obfuscation techniques and custom-built malware, designed specifically to evade detection. By employing sophisticated methods to conceal their malicious code, they can bypass security tools that rely on identifying known malware signatures or behaviors. This demonstrates a moderate to high level of technical sophistication and a commitment to staying ahead of security defenses
8. **Target Specificity**: The "Dream Job" campaign consistently targets the aerospace, aviation, and defense industries. This suggests a strategic interest in acquiring sensitive information and potentially disrupting operations within these critical sectors. The focus on these industries aligns with Iran's geopolitical interests and its history of cyber espionage activities targeting entities perceived as adversaries.
9. **Persistence and Evolution**: the Iranian "Dream Job" campaign has been active since at least September 2023, indicating a persistent effort by TA455. The constant changes in infrastructure and malware demonstrate their adaptability and commitment to staying ahead of security measures. This highlights the need for ongoing vigilance and proactive defense strategies.

Technical Analysis

Main malicious file in the campaign - SignedConnection[.]zip

On October 29th, 2024, a registered user from the US uploaded the ZIP file, followed by an unregistered user from the US. There are five engines that flag the file as malicious, with the main attribution to North Korean Kimsuky (a recurring misattribution in adversary attacks).



5/68 security vendors flagged this file as malicious

bf308e5c91bcd04473126de716e3e668cac6cb1ac9c301132d61845a6d4cb362

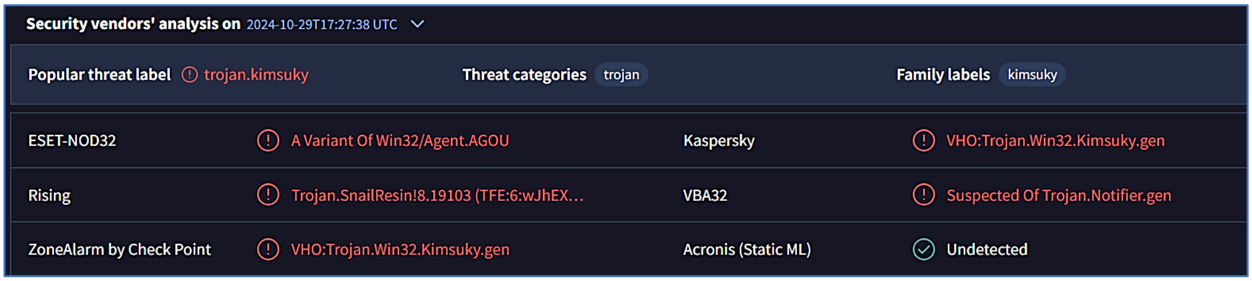
SignedConnection.zip

Malwares_SnailResin · zip · contains-pe · checks-user-input · detect-debug-environment · long-sleeps

Size: 998.06 KB

Last Analysis Date: 1 day ago

File name: SignedConnection[.]zip
File type: ZIP
Md5: bb4c8f42cc624c628e4b98bd43f29fa6
Sha1: 3a0b3426f4a2f85e0c82b2804aab7f5d5bb63fb7
Sha256: bf308e5c91bcd04473126de716e3e668cac6cb1ac9c301132d61845a6d4cb362



Security vendors' analysis on 2024-10-29T17:27:38 UTC

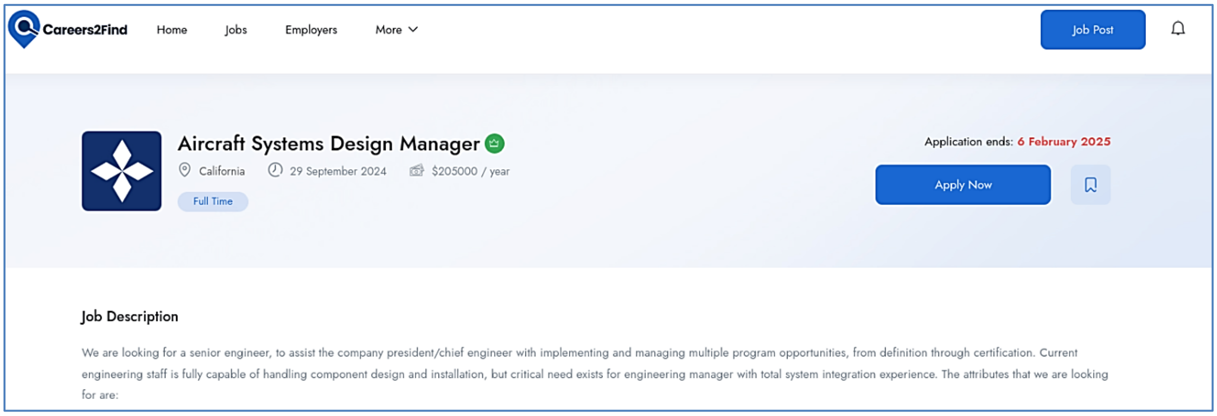
Popular threat label trojan.kimsuky · **Threat categories** trojan · **Family labels** kimsuky

ESET-NOD32	A Variant Of Win32/Agent.AGOU	Kaspersky	VHO:Trojan.Win32.Kimsuky.gen
Rising	Trojan.SnailResin!8.19103 (TFE:6:wJhEX...	VBA32	Suspected Of Trojan.Notifier.gen
ZoneAlarm by Check Point	VHO:Trojan.Win32.Kimsuky.gen	Acronis (Static ML)	Undetected

The ZIP file is downloaded ITW from the domain: **careers2find[.]com.**

The Domain **careers2find[.]com** was created four months ago, hiding it's real IP under Cloudflare service.

A job offer in the aerospace industry was found on the Iranian threat actor's "recruitment" site. In the past, this sector has been targeted by the actor.



Aircraft Systems Design Manager

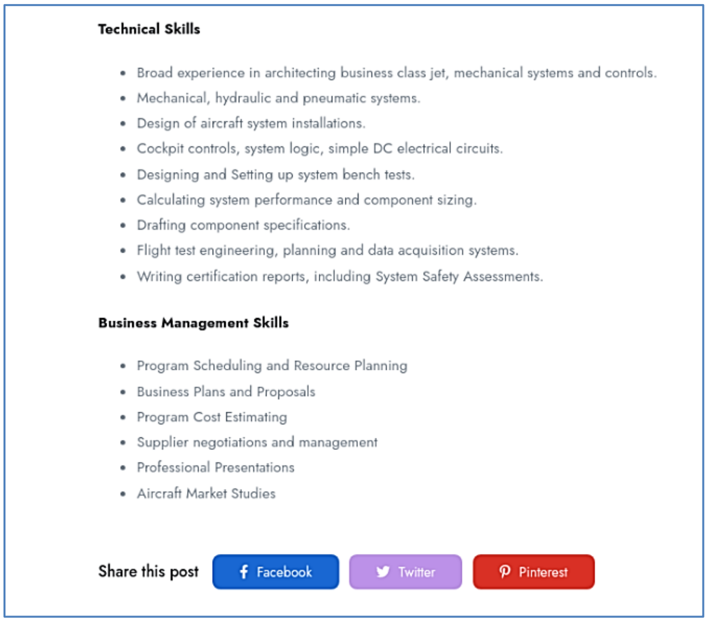
California · 29 September 2024 · $205000 / year

Full Time

Application ends: 6 February 2025

Job Description

We are looking for a senior engineer, to assist the company president/chief engineer with implementing and managing multiple program opportunities, from definition through certification. Current engineering staff is fully capable of handling component design and installation, but critical need exists for engineering manager with total system integration experience. The attributes that we are looking for are:



Technical Skills

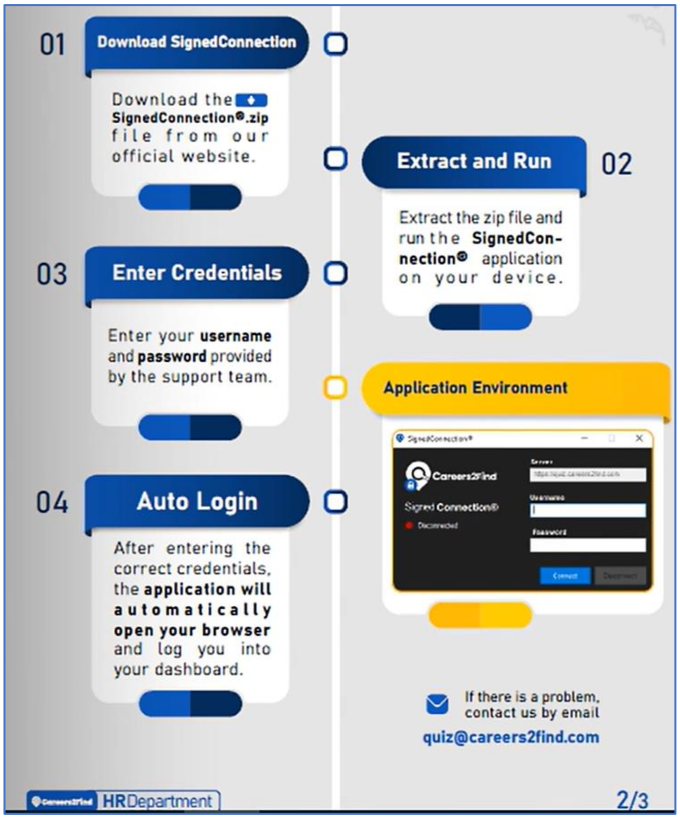
- Broad experience in architecting business class jet, mechanical systems and controls.
- Mechanical, hydraulic and pneumatic systems.
- Design of aircraft system installations.
- Cockpit controls, system logic, simple DC electrical circuits.
- Designing and Setting up system bench tests.
- Calculating system performance and component sizing.
- Drafting component specifications.
- Flight test engineering, planning and data acquisition systems.
- Writing certification reports, including System Safety Assessments.

Business Management Skills

- Program Scheduling and Resource Planning
- Business Plans and Proposals
- Program Cost Estimating
- Supplier negotiations and management
- Professional Presentations
- Aircraft Market Studies

From the campaign's website, a job posting for the aerospace industry.

A PDF instruction file (see image below) is also downloaded from the same website **careers2find[.]com** with instructions on how to "safely" access the website. It is designed to ensure infection.



01 **Download SignedConnection**

Download the SignedConnection®.zip file from our official website.

02 **Extract and Run**

Extract the zip file and run the **SignedConnection®** application on your device.

03 **Enter Credentials**

Enter your **username** and **password** provided by the support team.

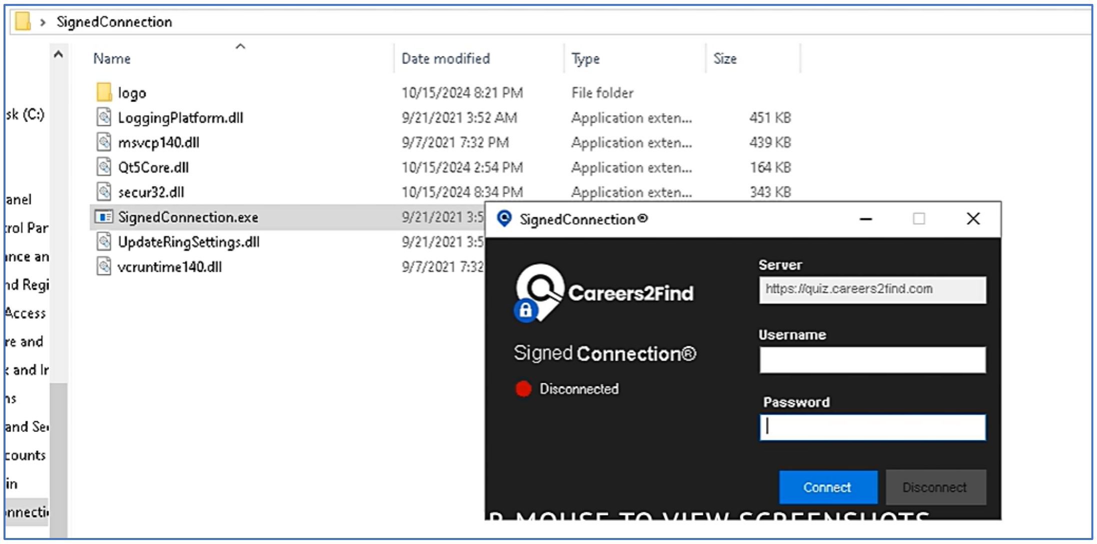
Application Environment

04 **Auto Login**

After entering the correct credentials, the **application will automatically open your browser** and log you into your dashboard.

If there is a problem, contact us by email **quiz@careers2find.com**

Several files, including legitimate ones, are included in the downloaded ZIP file. Clicking the highlighted EXE file displays the following GUI:



Name	Date modified	Type	Size
logo	10/15/2024 8:21 PM	File folder	
LoggingPlatform.dll	9/21/2021 3:52 AM	Application exten...	451 KB
msvcp140.dll	9/7/2021 7:32 PM	Application exten...	439 KB
Qt5Core.dll	10/15/2024 2:54 PM	Application exten...	164 KB
secur32.dll	10/15/2024 8:34 PM	Application exten...	343 KB
SignedConnection.exe	9/21/2021 3:5		
UpdateRingSettings.dll	9/21/2021 3:5		
vcruntime140.dll	9/7/2021 7:32		

SignedConnection®

Careers2Find

Signed Connection®

● Disconnected

Server: https://quiz.careers2find.com

Username:

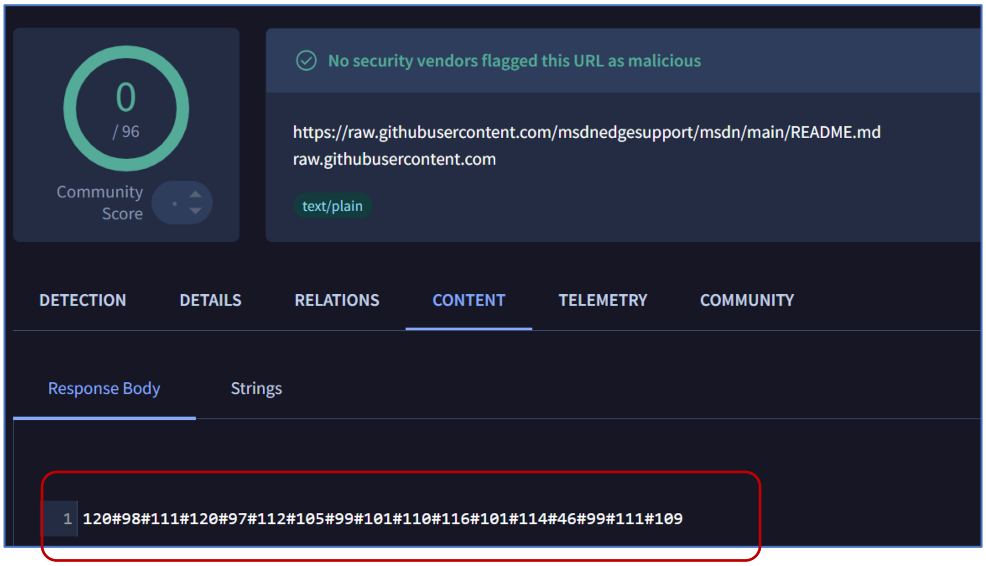
Password:

Most of the ZIP files were added to it on October 15th, 2024.

The following actions occur when the EXE file is executed:

- The malicious file secur32[.]dll is loaded by DLL side loading (there is a legitimate file with the same name, but the one in question is malicious).
- The IP address of the victim computer is checked by the website api[.]ipify[.]org.
- Accessing the GitHub account msdnedgesupport to download information: [https://]raw.ghubusercontent.com/msdnedgesupport/msdn/main/README.html

Downloaded information is ASCII encoded and looks like this:



No security vendors flagged this URL as malicious

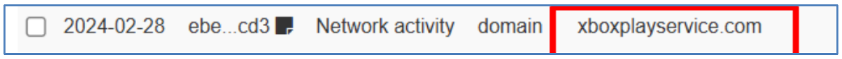
https://raw.githubusercontent.com/msdnedgesupport/msdn/main/README.md
raw.githubusercontent.com

```
120#98#111#120#97#112#105#99#101#110#116#101#114#46#99#111#109
```

After deleting the # characters and converting the numbers to characters using ASCII table, the C2 server address is revealed: xboxapicenter[.]com.

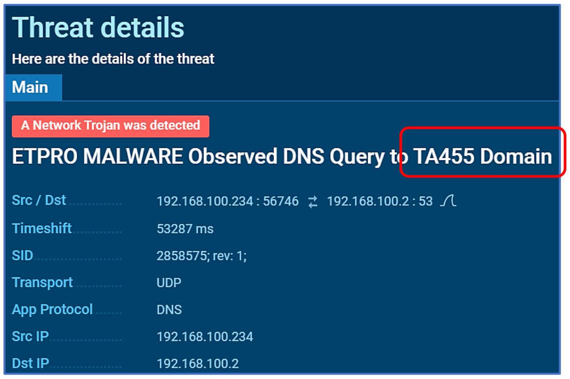
This domain resolves to "Stark Industries” IP address: 89.221.225[.]249.

The actor previously used a fake XBOX domain:



□ 2024-02-28	ebe...cd3	Network activity	domain	xboxplayservice.com

During execution simulation, Proofpoint EDR identified the domain xboxapicenter[.]com as belonging to threat actor TA455.



Threat details

Here are the details of the threat

Main

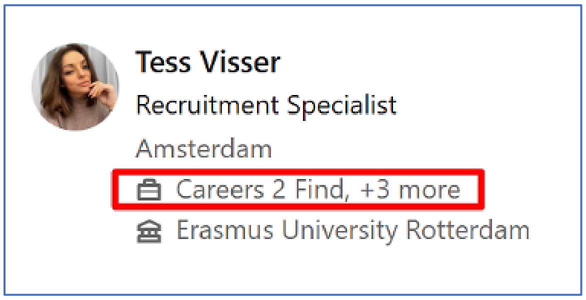
A Network Trojan was detected

ETPRO MALWARE Observed DNS Query to TA455 Domain

Src / Dst	192.168.100.234 : 56746 ⇄ 192.168.100.2 : 53
Timeshift	53287 ms
SID	2858575; rev: 1;
Transport	UDP
App Protocol	DNS
Src IP	192.168.100.234
Dst IP	192.168.100.2

Revealing the "recruiters" fake identities

Recent searches on Careers2Find revealed a LinkedIn profile that had served as a threat actor's recruiter in the past; however, the domain was only created four months ago.



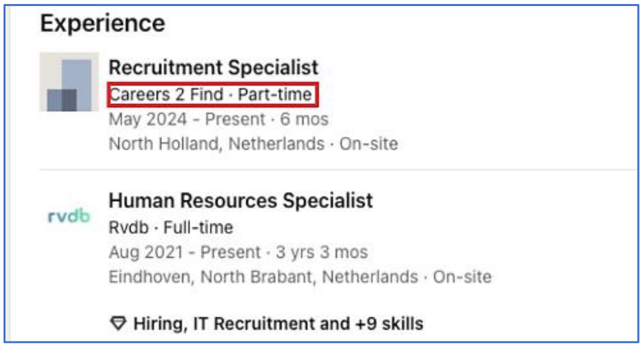
Tess Visser

Recruitment Specialist

Amsterdam

Careers 2 Find, +3 more

Erasmus University Rotterdam

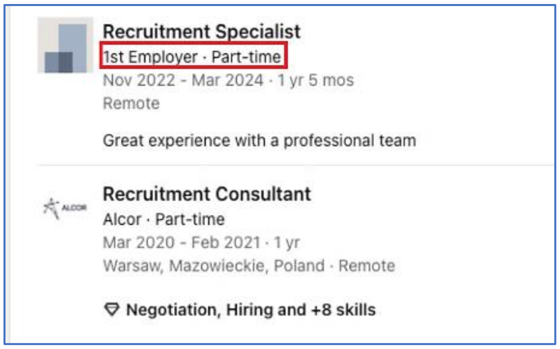


Experience

Recruitment Specialist
Careers 2 Find · Part-time
May 2024 - Present · 6 mos
North Holland, Netherlands · On-site

Human Resources Specialist
Rvdb · Full-time
Aug 2021 - Present · 3 yrs 3 mos
Eindhoven, North Brabant, Netherlands · On-site

Hiring, IT Recruitment and +9 skills



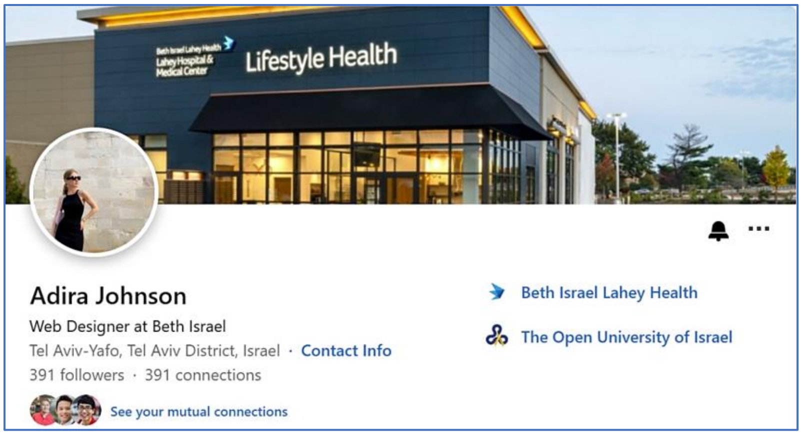
Recruitment Specialist
1st Employer · Part-time
Nov 2022 - Mar 2024 · 1 yr 5 mos
Remote

Great experience with a professional team

Recruitment Consultant
Alcor · Part-time
Mar 2020 - Feb 2021 · 1 yr
Warsaw, Mazowieckie, Poland · Remote

Negotiation, Hiring and +8 skills

The following profiles were also detected claiming to be recruiters for this company:



Adira Johnson

Web Designer at Beth Israel

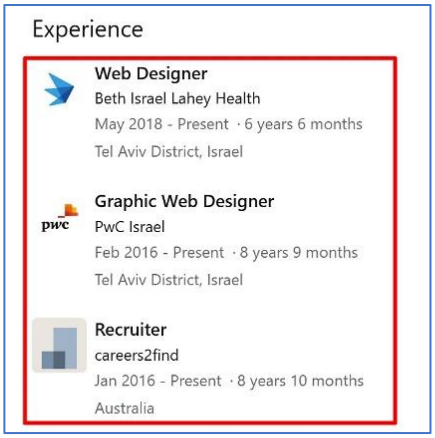
Tel Aviv-Yafo, Tel Aviv District, Israel · Contact Info

391 followers · 391 connections

See your mutual connections

Beth Israel Lahey Health

The Open University of Israel

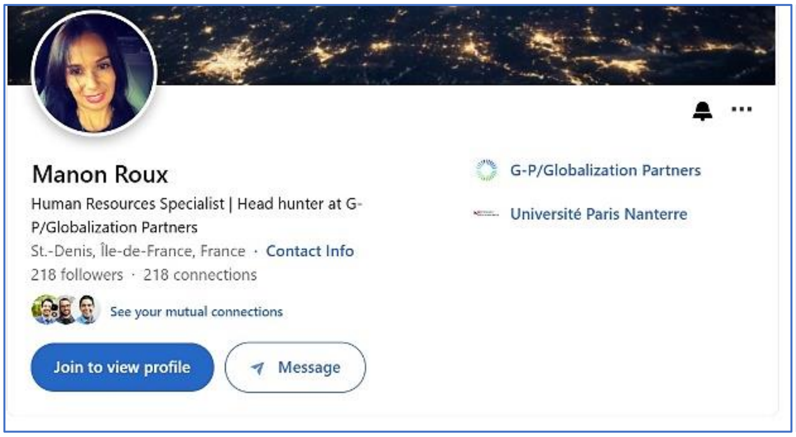


Experience

Web Designer
Beth Israel Lahey Health
May 2018 - Present · 6 years 6 months
Tel Aviv District, Israel

Graphic Web Designer
PwC Israel
Feb 2016 - Present · 8 years 9 months
Tel Aviv District, Israel

Recruiter
careers2find
Jan 2016 - Present · 8 years 10 months
Australia



Manon Roux

Human Resources Specialist | Head hunter at G-P/Globalization Partners

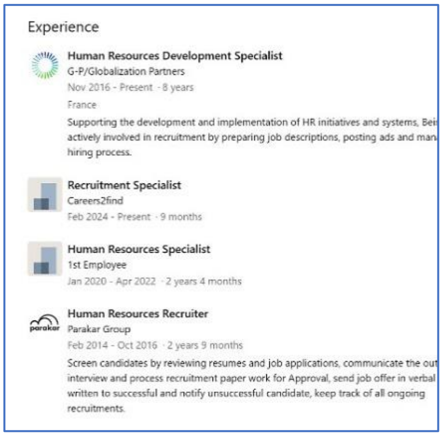
St.-Denis, Île-de-France, France · Contact Info

218 followers · 218 connections

See your mutual connections

G-P/Globalization Partners

Université Paris Nanterre



Experience

Human Resources Development Specialist
G-P/Globalization Partners
Nov 2016 - Present · 8 years
France
Supporting the development and implementation of HR initiatives and systems, Bei
actively involved in recruitment by preparing job descriptions, posting ads and man
hiring process.

Recruitment Specialist
Careers2find
Feb 2024 - Present · 9 months

Human Resources Specialist
1st Employee
Jan 2020 - Apr 2022 · 2 years 4 months

Human Resources Recruiter
Parakar Group
Feb 2014 - Oct 2016 · 2 years 9 months
Screen candidates by reviewing resumes and job applications, communicate the out
interview and process recruitment paper work for Approval, send job offer in verbal
written to successful and notify unsuccessful candidate, keep track of all ongoing
recruitments.

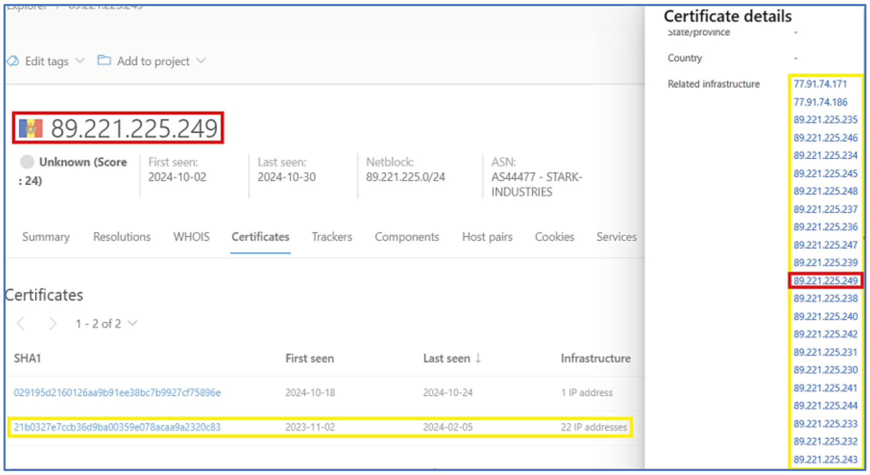
Infrastructure analysis

Examining the digital certificates linked to IP address 89[.]221.225.249, resolved by domain xboxapicenter[.]com, yielded a second certificate linked to 20 more IP addresses of the same range: 89[.]221.225.0/24, as well as two other IP addresses from the range 77[.]91.74.0/24 (from the same AS).

Although the certificate was issued before the C2 server domain was established, it was also linked to the above IP address. The addresses associated with this certificate are consecutive within the range. This certificate is associated with additional addresses attributed to an Iranian adversary with low confidence according to ClearSky.

Certificate details:

Common name:
Subject: localhost
Issuer: localhost
SHA1: 21b0327e7ccb36d9ba00359e078acaa9a2320c83
Serial number: 84540175500579177624119799943918273904002380806



89.221.225.249

Unknown (Score : 24) | First seen: 2024-10-02 | Last seen: 2024-10-30 | Netblock: 89.221.225.0/24 | ASN: AS44477 - STARK-INDUSTRIES

Certificates

1 - 2 of 2

SHA1	First seen	Last seen ↓	Infrastructure
029195d2160126aa9b91ee38bc7b9927cf75896e	2024-10-18	2024-10-24	1 IP address
21b0327e7ccb36d9ba00359e078acaa9a2320c83	2023-11-02	2024-02-05	22 IP addresses

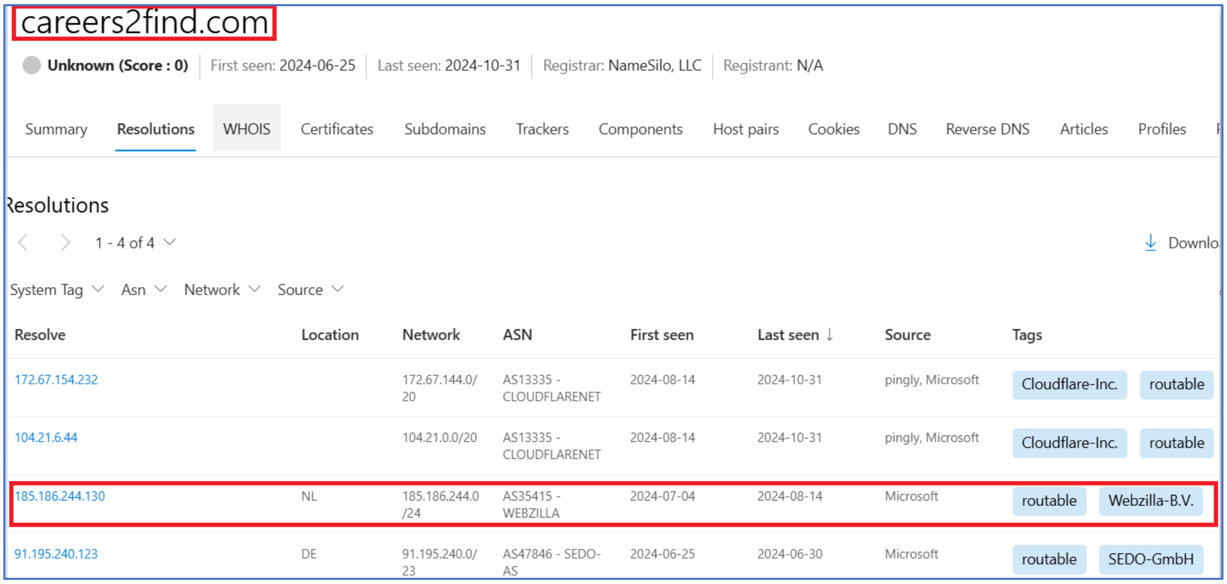
Certificate details

State/province	-
Country	-
Related infrastructure	77.91.74.171 77.91.74.186 89.221.225.235 89.221.225.246 89.221.225.234 89.221.225.245 89.221.225.248 89.221.225.237 89.221.225.236 89.221.225.247 89.221.225.239 89.221.225.249 89.221.225.238 89.221.225.240 89.221.225.242 89.221.225.231 89.221.225.230 89.221.225.241 89.221.225.244 89.221.225.233 89.221.225.232 89.221.225.243

Domain careers2find[.]com, attributed to the threat actor, resolved to a unique IP address of an ASN rarely used by Iranian threat actors prior to its resolution to Cloudflare IP addresses:

IP	AS \ ASN	Registrant
185[.]186.244.130	Webzilla B.V. \ 35415	Hostry Inc. and Inxy

As this is a unique IP address resolved to by a domain attributed to the threat actor prior to its transfer to Cloudflare service, ClearSky attributes it to the threat actor with high confidence.



careers2find.com

Unknown (Score : 0) | First seen: 2024-06-25 | Last seen: 2024-10-31 | Registrar: NameSilo, LLC | Registrant: N/A

Resolutions

1 - 4 of 4

Resolve	Location	Network	ASN	First seen	Last seen ↓	Source	Tags
172.67.154.232		172.67.144.0/20	AS13335 - CLOUDFLARENET	2024-08-14	2024-10-31	pingly, Microsoft	Cloudflare-Inc. routable
104.21.6.44		104.21.0.0/20	AS13335 - CLOUDFLARENET	2024-08-14	2024-10-31	pingly, Microsoft	Cloudflare-Inc. routable
185.186.244.130	NL	185.186.244.0/24	AS35415 - WEBZILLA	2024-07-04	2024-08-14	Microsoft	routable Webzilla-B.V.
91.195.240.123	DE	91.195.240.0/23	AS47846 - SEDO-AS	2024-06-25	2024-06-30	Microsoft	routable SEDO-GmbH

TTPs used by TA455 in the Iranian "Dream Job" Campaign

TTP	Description	Insights	MITRE ATT&CK
Initial Access	Spearphishing via LinkedIn	TA455 leverages the trust and professional networking nature of LinkedIn to approach targets with seemingly legitimate job offers. This method increases the likelihood of victims opening malicious attachments or clicking on links leading to compromised websites.	T1566.001: Spearphishing Attachment. T1566.002: Spearphishing Link
Execution	DLL Side-Loading	By utilizing DLL side-loading, TA455 exploits the Windows operating system's DLL search order to load a malicious DLL instead of the legitimate one. This technique allows them to execute malicious code within the context of a trusted process, making it harder to detect.	T1574.002: DLL Side-Loading
Discovery	IP Address Discovery	Determining the victim's IP address is crucial for the attackers to assess the target's location and potentially tailor their attacks based on geographic region or organizational affiliation. TA455 utilizes the website api[.]ipify[.]org for this purpose.	T1592: Gather Victim Host Information

Command and Control	The use of GitHub for hosting the C2 domain.	TA455 employs GitHub as a covert communication channel for their C&C infrastructure. By encoding the C&C server address within seemingly innocuous files on a GitHub repository, they can retrieve it while blending in with legitimate users, making detection more difficult.	T1102.001: Web Service: Dead Drop Resolver: GitHub
Defense Evasion	Impersonation of Other Threat Actors	TA455 deliberately mimics tactics and tools associated with North Korean Lazarus APT Group, creating intentional misattribution in an attempt to deflect blame and complicate investigations. The frequent detection of their malware as Kimsuky further reinforces this tactic. In the attack, legitimate file names are used as the malicious payload to facilitate DLL Side Loading.	T1036.005: Masquerading: Match Legitimate Name or Location
Defense Evasion	Obfuscation and Evasive Code	TA455 incorporates advanced obfuscation techniques and utilizes custom malicious code to evade detection by traditional security solutions. This includes multi-stage infection chains and reliance on legitimate services like Cloudflare to mask their infrastructure.	T1027: Obfuscated Files or Information
Collection	Exfiltration over C2 Channel	TA455 uses its established C2 channel, facilitated through GitHub and encoded communication, to exfiltrate collected data from compromised systems.	T1041: Exfiltration Over C2 Channel

Indicators Of Compromise:

Files (SHA-1):
2a29ba7302024ec1255811abec2a532136d12fef
3a0b3426f4a2f85e0c82b2804aab7f5d5bb63fb7
1acd34fb6de5c645e03ded9875046979be7893c4
2e7fc6d63ce16075a3fe3584e03be24a9bc220e1
aa5fcea406edd406bd6e0a23e83beebe2b3582d1
c52beb64f7450fce923d15efaa1e5be4c0e43d2b

Network:
careers2find.com
xboxapicenter.com
hxxps[://]raw[.]githubusercontent[.]com/msdnedgesupport
hxxps[://]github[.]com/msdnedgesupport
185[.]186[.]244[.]130
89[.]221[.]225[.]249
77[.]91[.]74[.]171 (low probability)
77[.]91[.]74[.]186 (low probability)
89[.]221[.]225[.]235 (low probability)
89[.]221[.]225[.]246 (low probability)
89[.]221[.]225[.]245 (low probability)
89[.]221[.]225[.]234 (low probability)
89[.]221[.]225[.]248 (low probability)
89[.]221[.]225[.]237 (low probability)
89[.]221[.]225[.]236 (low probability)
89[.]221[.]225[.]247 (low probability)
89[.]221[.]225[.]239 (low probability)
89[.]221[.]225[.]238 (low probability)

89[.]221[.]225[.]240 (low probability)
89[.]221[.]225[.]242 (low probability)
89[.]221[.]225[.]231 (low probability)
89[.]221[.]225[.]230 (low probability)
89[.]221[.]225[.]241 (low probability)
89[.]221[.]225[.]244 (low probability)
89[.]221[.]225[.]233 (low probability)
89[.]221[.]225[.]232 (low probability)
89[.]221[.]225[.]243 (low probability)