

I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona

 proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

July 23, 2021



Blog

Threat Insight

I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona

July 28, 2021 JOSHUA MILLER, MICHAEL RAGGI, & CRISTA GIERING

Key Takeaways

- TA456, an Iranian-state aligned actor, spent years masquerading as the persona “Marcella Flores” in an attempt to infect the machine of an employee of an aerospace defense contractor with malware.
- The malware, dubbed by Proofpoint as LEMPO, was designed to establish persistence, perform reconnaissance, and exfiltrate sensitive information.
- TA456 actively targets smaller subsidiaries and contractors in support of efforts to compromise larger defense contractors using a supply chain compromise.
- While targeting defense contractors is not new for TA456, this campaign uniquely establishes the group as one of the most determined Iranian-aligned threat actors tracked by Proofpoint because of its significant use of social engineering, cross platform communication, and general persistence.

Overview

Proofpoint researchers have identified a years-long social engineering and targeted malware campaign by the Iranian-state aligned threat actor TA456. Using the social media persona “Marcella Flores,” TA456 built a relationship across corporate and personal communication platforms with an employee of a small subsidiary of an aerospace defense contractor. In early June 2021, the threat actor attempted to capitalize on this relationship by sending the target malware via an ongoing email communication chain. Designed to

conduct reconnaissance on the target's machine, the macro-laden document contained personalized content and demonstrated the importance TA456 placed on the target. Once the malware, which is an updated version of Lidere that Proofpoint has dubbed LEMPO, establishes persistence, it can perform reconnaissance on the infected machine, save the reconnaissance details to the host, exfiltrate sensitive information to an actor-controlled email account via SMTPS, and then cover its tracks by deleting that day's host artifacts.

This campaign exemplifies the persistent nature of certain state aligned threats and the human engagement they are willing to conduct in support of espionage operations. In mid-July, Facebook disrupted a network of similar personas they attributed to Tortoiseshell. LEMPO, the malware, whose delivery Proofpoint disrupted, along with the network of personas, are attributed to TA456. This actor is believed to be loosely aligned with the Islamic Revolutionary Guard Corps (IRGC) via association with the Iranian company Mahak Rayan Afraz (MRA), according to Facebook's analysis.

Threat Actor Highlights: TA456

Aliases: Tortoiseshell, Imperial Kitten

Attribution: Iran

Primary Mitre TTPs: T1048: Exfiltration Over Alternative Defense, Protocol, T1566.002: Phishing: Spearphishing Link, T1592: Gather Victim Host Information

Industries Typically Targeted:
IT, Government

Campaign Breakdown

Proofpoint data shows that over at least eight months, "Marcella (Marcy) Flores" sent TA456's target benign email messages, photographs, and a video to establish her veracity and build rapport with the intended victim. At one time, TA456 attempted to send a benign, but flirtatious video via a OneDrive URL. In early June, a TA456 actor self-identified as "Marcy" sent another OneDrive link, this time masquerading as a diet survey (Figure 1).

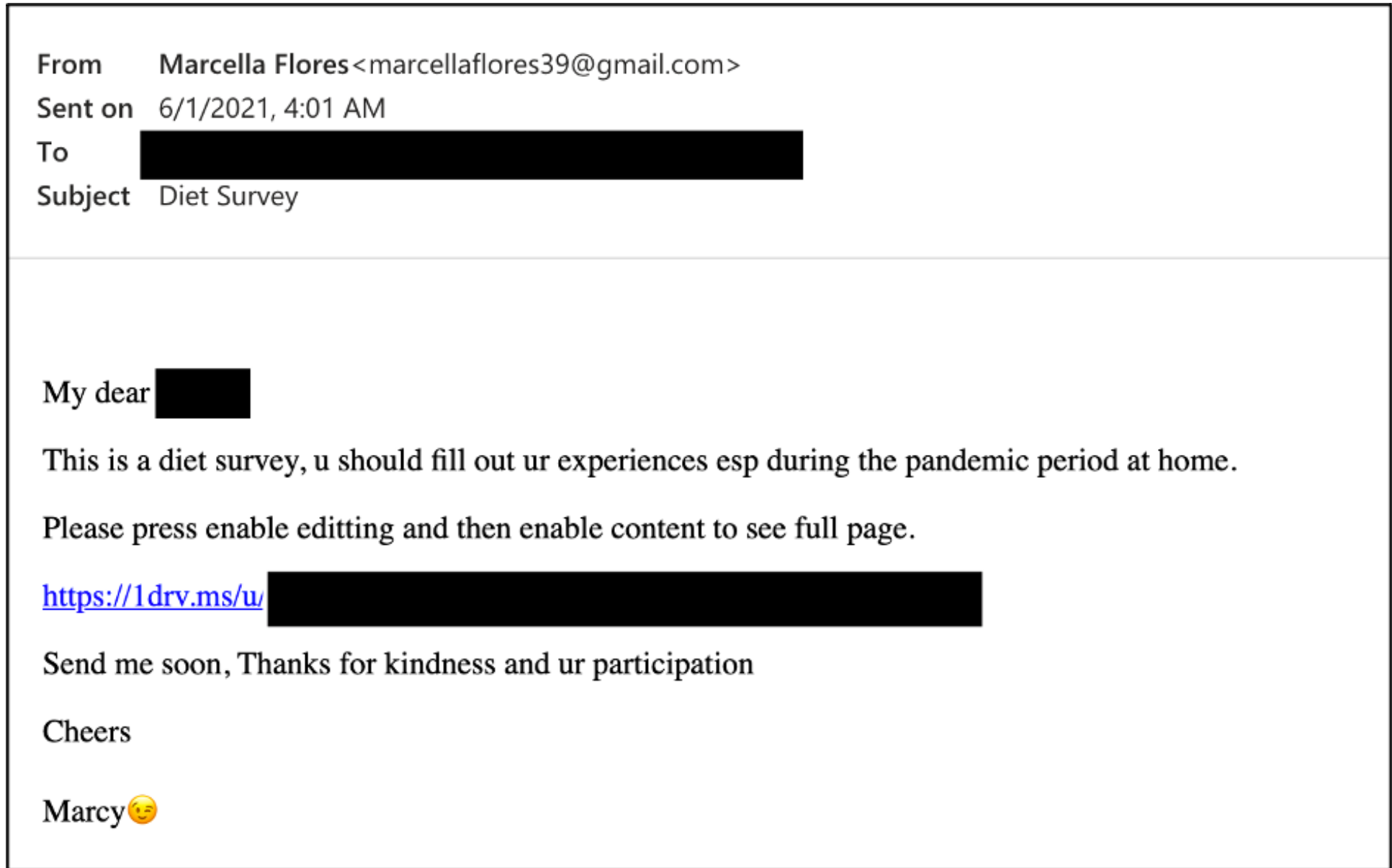


Figure 1. The diet survey email sent to the target.

The OneDrive URL delivered a .rar file (dfddbdo9ccea598c4841f1abbc927f1c661d85d4bd9bcbo81f7c811212d8a64a) containing a .xlsm (Figure 2) (612bdfb4f6eaf920a7a41fa06de8d99f6ecf6ad147374efa6eb1d5aff91df558). Using previous conversation topics with the target, the .xlsm purported to be pandemic diet assistance and requested that the user enable content to access the privacy protected portions of the file. If the content is enabled, the macro will create and hide the directory \Appdata\Perflog and then write LEMPO, a very simple but ingenious plaintext stealer comprised of Visual Basic Script (VBS), to that directory (Schedule.vbs 1534f95f49ddf2ada38561705f901e5938470c1678d6a81fof4177ba7412ef5b). After authoring the VBS, the Excel macro will add a registry key (HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Schedule /t REG_SZ /d C:\Users\[redacted_username]\AppData\Perflog\Schedule.vbs /f) to ensure LEMPO is run upon user login.

Diet in pandemic - Microsoft Excel

	A	B	C	D	E	F	G
1	Food habits	Your response					
2	For privacy issues, this file is utterly confidential and anonymuos. Therefore you are asked to click on "Enable Content" to have access throughout file.						
3	Eat plenty of fresh vegetables, legumes and fruits						
4	Eat plenty of cereals, preferably wholegrain, such as breads, rice, pasta and noodles						
5	Include lean meat, fish, poultry and/or alternatives						
6	Include milks, yoghurts, cheeses and/or alternatives						
7	Batch cook large quantities of food to freeze						

Ready | 100% | 9:14 AM 6/1/2021

Figure 2. The diet survey .xlsm file.

The macro in the Excel document also contains code to connect via HTTP POST to showip[.]net. The response, along with the results of "net use" and "netstat -nao" are stored in a hidden sheet within the .xlsm, reminiscent of the technique described in Facebook's July 15th announcement. Proofpoint analysts assess this may indicate code partially remaining from an earlier iteration of the tool that came before LEMPO or a desire for redundancy in TA456's reconnaissance tooling.

LEMPO

The LEMPO reconnaissance tool is a Visual Basic Script dropped by an Excel macro. Leveraging built-in Windows commands it enumerates the host in a variety of ways, records the collected data and then exfiltrates the intelligence to an actor-controlled email account using Microsoft's Collaboration Data Objects (CDO). CDO, previously known as OLE Messaging or Active Messaging, is an application programming interface included with Microsoft Windows and Microsoft Exchange Server products. While most of this analysis is based off the sample blocked by Proofpoint (1534f95f49ddf2ada38561705f901e5938470c1678d6a81f0f4177ba7412ef5b) in June 2021, we also identified a similar sample (da65aa439e90d21b2cf53afef6491e7dcda19dd1bbec50329d53f3d977ee089) uploaded to a public malware repository with an upload date of June 2020.

Reconnaissance

LEMPO collects the following information and records it to %temp%\Logs.txt

- Date and time
- Computer and usernames
- System information via WMIC os, sysaccount, environment, and computer system commands
- Antivirus products located in the "SecurityCenter2" path
- Drives
- Tasklist
- Software and version
- Net users and user details

Following the connectivity check, detailed in the following section, LEMPO writes the following to %temp%\Logs.txt

- Firewall rules
- List of running processes via Powershell Get-Process
- IP config
- Domain hosts, users, computers, and local groups
- Trusted domains
- Network shares
- Arp cache
- Tracert
- External IP (via showip.net)
- Connections (netstat -nao)

Connectivity

Prior to the network focused reconnaissance, LEMPO checks connectivity by reaching out to Yandex, Google, Yahoo, Github, Mailchimp, Mega, Arxiv (an online academic repository specializing in electrical engineering and scientific research), and Twitter using ping and curl (Figure 3). The June 2020 version of LEMPO includes only a connectivity check to ford[.]com.

```
Date and Time ----- >%temp%\Logs.txt && date /t>%temp%\Logs.txt && time /t>%temp%\Logs.txt"
PC and User Names ----- >%temp%\Logs.txt && whoami>%temp%\Logs.txt"
System Information os----- >%temp%\Logs.txt && wmic os get /value >%temp%\Logs.txt"
System Information SYSACCOUNT----- >%temp%\Logs.txt && wmic SYSACCOUNT get>%temp%\Logs.txt"
System Information ENVIRONMENT----- >%temp%\Logs.txt && wmic ENVIRONMENT get>%temp%\Logs.txt"
System Information computersystem----- >%temp%\Logs.txt && wmic computersystem get>%temp%\Logs.txt"
Antivirus ----- >%temp%\Logs.txt && WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
Drives ----- >%temp%\Logs.txt && wmic volume get caption, label, capacity, freespace /all>%temp%\Logs.txt"
Tasks List ----- >%temp%\Logs.txt && tasklist /v>%temp%\Logs.txt"
- Software ----- >%temp%\Logs.txt && wmic product get name,version>%temp%\Logs.txt"
- Net Users ----- >%temp%\Logs.txt && net user>%temp%\Logs.txt"
- User Details ----- >%temp%\Logs.txt && net user %username%>%temp%\Logs.txt"
- Ping Status ----- >%temp%\Logs.txt && ping www.yandex.com -n 1 >%temp%\Logs.txt"
- Ping Status google----- >%temp%\Logs.txt && ping www.google.com -n 1 >%temp%\Logs.txt"
- Ping Status yahoo----- >%temp%\Logs.txt && ping www.yahoo.com -n 1 >%temp%\Logs.txt"
- Ping Status github----- >%temp%\Logs.txt && ping www.github.com -n 1 >%temp%\Logs.txt"
- Ping Status mailchimp----- >%temp%\Logs.txt && ping www.mailchimp.com -n 1 >%temp%\Logs.txt"
- curl Status google----- >%temp%\Logs.txt && curl https://www.google.com/ >%temp%\Logs.txt"
- curl Status mega----- >%temp%\Logs.txt && curl https://mega.io/ >%temp%\Logs.txt"
- curl Status arxiv----- >%temp%\Logs.txt && curl https://arxiv.org/ >%temp%\Logs.txt"
- curl Status twitter----- >%temp%\Logs.txt && curl https://twitter.com/?lang=en >%temp%\Logs.txt"
- firewall_rule ----- >%temp%\Logs.txt && netsh advfirewall firewall show rule name=all>%temp%\Logs.txt"
- powershell checker----- >%temp%\Logs.txt && powershell.exe gps>%temp%\Logs.txt"
- IP Config ----- >%temp%\Logs.txt && ipconfig /all>%temp%\Logs.txt"
- Hosts of Domain ----- >%temp%\Logs.txt && net view /domain>%temp%\Logs.txt"
- Users of Domain ----- >%temp%\Logs.txt && net user /domain>%temp%\Logs.txt"
- Computers of Domain ----- >%temp%\Logs.txt && net computer /domain>%temp%\Logs.txt"
- Groups of Domain ----- >%temp%\Logs.txt && net group /domain>%temp%\Logs.txt"
- Local Groups of Domain ----- >%temp%\Logs.txt && net localgroup /domain>%temp%\Logs.txt"
- Trusted Domains ----- >%temp%\Logs.txt && nltest /trusted_domains>%temp%\Logs.txt"
- Network Shares ----- >%temp%\Logs.txt && net share>%temp%\Logs.txt"
- Arp ----- >%temp%\Logs.txt && arp d && arp -a>%temp%\Logs.txt"
- Trace Route ----- >%temp%\Logs.txt && tracert -d -w 1 8.8.8.8 >%temp%\Logs.txt"
- Valid IP ----- >%temp%\Logs.txt && curl showip.net>%temp%\Logs.txt"
- Connections Status ----- >%temp%\Logs.txt && netstat -nao>%temp%\Logs.txt"
- Dir Perflog ----- >%temp%\Logs.txt && dir /s %userprofile%\AppData\Perflog>%temp%\Logs.txt"
- Check Reg Key ----- >%temp%\Logs.txt && reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Detection>%temp%\Logs.txt"
- Passwords ----- >%temp%\Logs.txt && findstr /spin /c:user /c:pass /c:vpn %userprofile%\desktop\*.txt>%temp%\Logs.txt && findstr /spin /c:us
- Users Directory List ----- >%temp%\Logs.txt"
```


Figure 3.

After finishing that additional recon, LEMPO moves Logs.txt from %temp% to \Perflog. LEMPO then checks to ensure the Registry Key previously mentioned has been added and then uses the findstr command to identify files containing “user,” “pass,” and “vpn.” The findstr command returns any matching lines which could collect usernames and passwords from the computer. Logs.txt is then compressed into Logs.zip

Exfiltration

LEMPO uses hardcoded credentials with Microsoft’s CDO to exfiltrate the information over SMTPS on port 465. In the June 2021 version of LEMPO, TA456 uses the same Yahoo email address to send and receive the exfiltrated information. In the 2020 version of LEMPO, TA456 sent from a Yandex account to a Tutanota email account. Notably, the Yandex email within the 2020 version of the LEMPO implant masqueraded as large technology company focused on supporting the energy industry. After exfiltrating the information, LEMPO sleeps for 30 seconds and then deletes both Logs.txt and Logs.zip.

There’s Something About Marcy

“Marcella (Marcy) Flores” was conversing with the targeted aerospace employee since at least November 2020 and was friends with them on social media since at least 2019. Besides the Gmail account used for attempted malware delivery, Marcella maintained a now suspended Facebook profile.



Marcella Flores

Cuando suena la melodía, los pasos se mueven, el corazón canta y el espíritu comienza a bailar

Friends Photos Videos

About

Work



Aerobics Instructor at The Harbour Health Club Liverpool

June 2, 2013 - Present · Liverpool

In the heart of Liverpool city centre, The Harbour Health Club Liverpool offers customer with everything you would want from a health club. In the gym you will find a variety of cardiovascular machines including treadmills, bikes, steppers, cross trainers and rowers. I be glad to visit u soon.

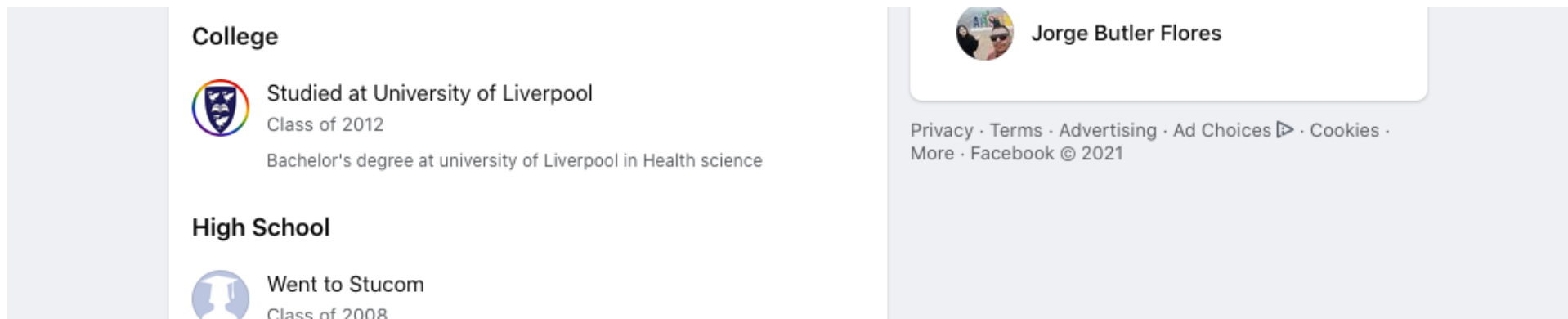
Others Named Marcella Flores

See More


Others With a Similar Name




Azi Flores




College

 Studied at University of Liverpool
Class of 2012
Bachelor's degree at university of Liverpool in Health science

High School

 Went to Stucom
Class of 2008

 **Jorge Butler Flores**


[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#)  · [Cookies](#) · [More](#) · Facebook © 2021

Figure 4.

Open-source research indicates “Marcella” interacted with TA456’s target on social media starting in late 2019. The earliest publicly available Facebook profile photo of “Marcella” was uploaded on May 30, 2018. Proofpoint’s analysis indicates the profile bears strong similarities to fictitious profiles previously used by Iranian APTs to socially engineer targets of intelligence value. The “Marcella” profile appeared to be friends with multiple individuals who publicly identify as defense contractor employees and who are geographically dispersed from “Marcella’s” alleged location in Liverpool, UK. On July 15, 2021, Facebook announced they had disrupted a network of Facebook and Instagram personas, including “Marcella’s,” they attributed to the Iranian-aligned actor.

Targets

TA456 routinely conducts reconnaissance campaigns disguised as news related spam that target individuals employed by aerospace defense contractors. The targeting of U.S. defense contractors, particularly those supporting contracts in the Middle East, is consistent with historical Iranian cyber activity. Additionally, Proofpoint has observed TA456 targeting individuals employed at multiple subcontractors and subsidiaries of larger defense companies. This is possibly an effort to target the primary contractor via less secure downstream component suppliers that share a network environment. Open-source research indicated the individual targeted by “Marcella” in this campaign works as a supply chain manager. This is consistent with TA456’s TTP of targeting business and information technology-related individuals within their target organization.

Attribution

Proofpoint attributes this campaign to TA456, an Iranian-aligned adversary focused on espionage efforts against defense industrial base employees and contractors, particularly those supporting efforts in the Middle East. TA456 overlaps with activity tracked as Tortoiseshell, and Imperial Kitten. On July 15, 2021, Facebook attributed a portion of Tortoiseshell's activity to Mahak Rayan Afraz (MRA), an Iranian IT company with ties to the IRGC. Based on previous malware analysis and historical open-source research, Proofpoint concurs with this attribution.

Additionally, LEMPO shares multiple similarities with Tortoiseshell's Liderc, including extensive machine reconnaissance, exfiltration via email, hardcoded email addresses with similar formatting, and overall pattern of targeting companies and individuals aligned with the American defense industrial base.

Outlook

TA456 demonstrated a significant operational investment by cultivating a relationship with a target's employee over years in order to deploy LEMPO to conduct reconnaissance into a highly secured target environment within the defense industrial base. Facebook's announcement demonstrated TA456 had established an extensive network of these personas dedicated to enabling cyberespionage operations. While Proofpoint did not observe the delivery of any remote access trojans or command and control channels like TA456's Syskit, the information potentially gathered by LEMPO could be operationalized in a variety of ways. These include the utilization of stolen VPN credentials, exploitation of vulnerabilities in the identified software, or the customization of more advanced malware delivered from "Marcella."

TA456's dedication to significant social engineering engagement, benign reconnaissance of targets prior to deploying malware, and their cross platform kill chain establish TA456 to be one of the most resourceful Iranian-aligned threats tracked by Proofpoint. The "Marcella Flores" persona is likely not the only one in use by TA456, making it important for those working within or tangentially to the defense industrial base to be vigilant when engaging with unknown individuals regardless of whether it is via work or personal accounts.

Subscribe to the Proofpoint Blog