Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**17 September 2020**

PIN Number
**20200917-001**

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **the Internet Crime Complaint Center (IC3)**.

Local Field Offices:
**www.fbi.gov/contact-us/field-office**

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrator's guard against the persistent malicious actions of cyber actors. This product was coordinated with DHS-CISA.

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

## IRGC-Associated Cyber Operations Against US Company Networks

**Summary**
The FBI is sharing information about a group of Iran-based cyber actors recently indicted for conducting malicious cyber operations to obtain access to US-based networks and steal information. The Iranian nationals indicted are Said Pourkarim Arabi, a member of Iran's Islamic Revolutionary Guard Corps (IRGC), Mohammad Reza Espargham, and Mohammad Bayati, both associates of Arabi. Since at least 2015, the actors conducted malicious cyber activity against US-based and foreign organizations and companies involved in aerospace or satellite technology and international government organizations in the United States, the United Kingdom, Singapore, Australia, and Israel.

The FBI is providing an overview of the group's tactics, techniques, and procedures, as well as indicators of compromise, to aid potential targets in the identification of malicious activity.

# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**Details**

The FBI has observed Iran-based cyber actors conducting multi-phased cyber operations targeted against companies in the United States. The FBI advises these cyber actors can achieve substantial unauthorized access to US company networks through harvesting of personally identifying information, use of fraudulent identities, social engineering, and off-the-shelf malicious tools. These operations have led to significant financial losses, with the actors accessing sensitive business information, intellectual property, and vendor information.

The FBI has observed these actors beginning their operations by identifying employees connected to the US aerospace and satellite industry. The FBI judges the malicious cyber actors obtained personal details needed to impersonate employees via openly available sources, such as professional development and networking Web sites. The actors create fraudulent social media accounts impersonating those individuals. The actors then use information about those employees for other purposes related to their operations, such as registering email and PayPal accounts and fraudulently purchasing domains and hacking tools.

The FBI has observed the actors create and send customized spear-phishing emails purporting to be from the individuals whose identities they had stolen. The emails would entice recipients to take action – usually clicking on a malicious link, which would download malware being downloaded onto the victim's computer and enable unauthorized access to victim networks. In one instance, the actors were observed hosting malicious code on a file-sharing service registered in the name of a US company employee, and including links to that malicious code in spear-phishing emails. One of the actors was observed using a fraudulent domain to host malware, then sending a link to the malware via spear phishing.

The FBI observed these actors conducting follow-on activities to expand and maintain their unauthorized access, such as creating additional backdoors and escalating privileges. The actors were observed using the below tools to exploit victims.

| Tool | Description |
|---|---|
| Metasploit Framework | An open source pen-testing framework sometimes used by attackers to exploit vulnerable systems and gain remote access. Metasploit contains a catalog of prewritten modules and payloads that make its usage by attackers very simple. |
| Mimikatz | A post-exploitation tool that dumps passwords from memory, as well as hashes, PINS, and Kerberos tickets. |
| NanoCore RAT | Remote Access Trojan that allows a user to remotely access and control computers. Also used to record user credentials and conduct surveillance using infected computers. |
| OCRA shell-code stagers | Used to execute intrusions once malicious code is active on a running system. |
| Python Backdoor | Open source backdoor written in the Python programming language. Additional way to control a victim's computer. |

The FBI advises that the below indicators of compromise are historical in nature, but may be used to identify historical targeting efforts.

| Indicator | Context |
|---|---|
| tleanalyser[.]com | May be included in spear-phishing messages as a provided link |
| theanalyser@gmail[.]com | May be included in spear-phishing messages as contact email |
| reseller.apples@gmail[.]com | Sending account for spear-phishing emails |
| noreply@theanalyser[.]com | From: line on spear-phishing messages |
| idc-team[.]net | May be identified in malware |
| 109.236.81[.]86 | Used in 2017 intrusion activity |
| 91.210.107[.]120 | Used in 2017 intrusion activity |

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**Example spear-phishing email using a link to a file-sharing service account hosting malware:**

**From:** [redacted]@[redacted]
**Sent:** Saturday, September 17, 2016 10:35 AM
**To:** [redacted]@[redacted]
**Subject:** [redacted] parallel image processing project

Hello,
I'm Dr. [redacted]
I am currently a [redacted] at the [redacted] specializing in geomorphology, glaciology, and geographic information technologies.Im working on a project about remote sensing and developed an application in parallel image processing for that reason I need a huge satelite image resource for testing my application. is it possible for you to Prepare it for me or test my attached application and send me feedback.
external application link
link to download
cheers.
--
Dr. [redacted]
Associate Professor [redacted]

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**Example spear-phishing email using an actor-registered and controlled domain hosting malware:**

**From:** noreply@tleanalyser.com
**To:** [redacted]@[redacted].com>, [redacted]
**Sent:** Monday, 12 June, 2017 15:40:55
**Subject:** [redacted] Satellite Tracking Software

Hello dear

After months of hard work, we are delighted to officially announce the launch of our new and ultimate software for tracking satellite.
Our goal with this new software is to provide our visitors an easier way to track their desired satellite and also to allow the visitor the ability to conduct not only neighborhood searches but new developments and building specific searches. The new software is interactive and gives better access to conduct TLE and Map searches. Our current and prospective clients will find useful information about our services and recent production numbers on the homepage.

You can download our ultimate software from the link below:

http://www.tleanalyser.com/download.php

Kind regards
[redacted] Software Department
Contact Email: tleanalyser@gmail. com

**Recommendations**

- Ensure anti-virus and anti-malware software is enabled and signature definitions are updated regularly in a timely manner. Well-maintained anti-virus software may prevent use of commonly deployed attacker tools that are delivered via spear phishing.

- Adopt threat reputation services at the network device, operating system, application, and email service levels. Reputation services can be used to detect or prevent low-reputation email addresses, files, URLs, and IP addresses used in spear-phishing attacks.

- Deploy application control software to limit which applications and executable code can be run by users. Email attachments, and files downloaded via links in emails, often contain executable code. Application control software limits users so they can only execute applications and code allowed by the organization, rendering malicious executables delivered via spear phishing unable to execute.

- Limit the use of administrator privileges. Users who browse the internet, use email, and execute code with administrator privileges make spear phishing much more effective by enabling attackers to move laterally across a network, gain additional accesses, and access highly sensitive information.

- Be suspicious of unsolicited contact via email or social media from any individual you do not know personally.

- Be suspicious of unsolicited or unexpected email or social media messages enticing recipients to open an attached or hosted file.

# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**Reporting Notice**

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts may be identified at www.fbi.gov/contact-us/field-office. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

**Administrative Note**

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

## Your Feedback Regarding this Product is Critical

**Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey**