November 16, 2021 • 6 min read

Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021

Microsoft Threat Intelligence Center (MSTIC)

Over the past year, the Microsoft Threat Intelligence Center (MSTIC) has observed a gradual evolution of the tools, techniques, and procedures employed by malicious network operators based in Iran. At CyberWarCon 2021, MSTIC analysts presented their analysis of these trends in Iranian nation state actor activity during a session titled "*The Iranian evolution: Observed changes in Iranian malicious network operations*". This blog is intended to summarize the content of that research and the topics covered in their presentation and demonstrate MSTIC's ongoing efforts to track these actors and protect customers from the related threats.

MSTIC consistently tracks threat actor activity, including the groups discussed in this blog, and works across Microsoft Security products and services to build detections into our products that improve customer protections. We are sharing this blog today so that others in the community can also be aware of the latest techniques we have observed being used by Iranian actors.

As with any observed nation-state actor activity, Microsoft has directly notified customers that have been targeted or compromised, providing them with the information they need

to help secure their accounts. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing MSTIC to track it as a unique set of information until we reach a high confidence about the origin or identity of the actor behind the activity. Once it meets the criteria, a DEV is converted to a named actor.

Three notable trends in Iranian nation-state operators have emerged:

- They are increasingly utilizing ransomware to either collect funds or disrupt their targets.
- They are more patient and persistent while engaging with their targets.
- While Iranian operators are more patient and persistent with their social engineering campaigns, they continue to employ aggressive brute force attacks on their targets.

Ransomware

Since September 2020, MSTIC has observed six Iranian threat groups deploying ransomware to achieve their strategic objectives. These ransomware deployments were launched in waves every six to eight weeks on average.

Figure 1: Timeline of ransomware attacks by Iranian threat actors

In one observed campaign, PHOSPHORUS targeted the Fortinet FortiOS SSL VPN and unpatched on-premises Exchange Servers globally with the intent of deploying ransomware on vulnerable networks. A recent blog post by the DFIR Report describes a similar intrusion in which actors leveraged vulnerabilities in on-premise Exchange Servers to compromise a victim environment and encrypt systems via BitLocker. MSTIC also attributes this activity to PHOSPHORUS. PHOSPHORUS operators conducted widespread scanning and ransomed targeted systems through a five-step process: Scan, Exploit, Review, Stage, Ransom.

Scan

In the early part of 2021, PHOSPHORUS actors scanned millions of IPs on the internet for Fortinet FortiOS SSL VPN that were vulnerable to CVE-2018-13379. This vulnerability allowed the attackers to collect clear-text credentials from the sessions file on vulnerable Fortinet VPN appliances. The actors collected credentials from over 900 Fortinet VPN servers in the United States, Europe, and Israel so far this year. In the last half of 2021,

PHOSPHORUS shifted to scanning for unpatched on-premises Exchange Servers vulnerable to ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065).

Exploit

When they identified vulnerable servers, PHOSPHORUS sought to gain persistence on the target systems. In some instances, the actors downloaded a Plink runner named *MicrosoftOutLookUpdater.exe*. This file would beacon periodically to their C2 servers via SSH, allowing the actors to issue further commands. Later, the actors would download a custom implant via a Base64-encoded PowerShell command. This implant established persistence on the victim system by modifying startup registry keys and ultimately functioned as a loader to download additional tools.

Review

After gaining persistence, PHOSPHORUS actors triaged hundreds of victims to determine which of them were fitting for actions on objectives. On select victims, operators created local administrator accounts with a with a username of "help" and password of "_AS_@1394" via the commands below. On occasion, actors dumped LSASS to acquire credentials to be used later for lateral movement.

```
net user help _AS_@1394 /add
net localgroup administrators help /add
net localgroup "Remote Desktop Users" help /add
```

Stage and Ransom

Finally, MSTIC observed PHOSPHORUS employing BitLocker to encrypt data and ransom victims at several targeted organizations. BitLocker is a full volume encryption feature meant to be used for legitimate purposes. After compromising the initial server (through

vulnerable VPN or Exchange Server), the actors moved laterally to a different system on the victim network to gain access to higher value resources. From there, they deployed a script to encrypt the drives on multiple systems. Victims were instructed to reach out to a specific Telegram page to pay for the decryption key.


Screenshot of ransom message

Patience and persistence

MSTIC has observed PHOSPHORUS threat actors employing social engineering to build rapport with their victims before targeting them. These operations likely required significant investment in the operator's time and resources to refine and execute. This trend indicates PHOSPHORUS is either moving away from or expanding on their past tactics of sending unsolicited links and attachments in spear-phishing email campaigns to attempt credential theft.

PHOSHORUS – Patient and persistent

PHOSPHORUS sends "interview requests" to target individuals through emails that contain tracking links to confirm whether the user has opened the file. Once a response is received from the target user, PHOSPHORUS attackers send a link to a benign list of interview questions hosted on a cloud service provider. The attackers continue with several back-and-forth conversations discussing the questions with the target user before finally sending a meeting invite with a link masquerading as a Google Meeting.

Once the meeting invite is sent, the attackers continuously reach out to the target user, asking them to test the Google Meeting link. The attackers contact the targeted user multiple times per day, continuously pestering them to click the link. The attackers even go so far as to offer to call the target user to walk them through clicking the link. The attackers are more than willing to troubleshoot any issues the user has signing into the fake Google Meeting link, which leads to a credential harvesting page.

MSTIC has observed PHOSPHORUS operators become very aggressive in their emails after the initial lure is sent, to the point where they are almost demanding a response from the targeted user.

CURIUM – In it for the long run

CURIUM is another Iranian threat actor group that has shown a great deal of patience when targeting users. Instead of phishing emails, CURIUM actors leverage a network of fictitious social media accounts to build trust with targets and deliver malware.

These attackers have followed the following playbook:

- Masquerade as an attractive woman on social media
- Establish a connection via social media with a target user via LinkedIn, Facebook, etc.
- Chat with the target daily
- Send benign videos of the woman to the target to prime them to lower their guard
- Send malicious files to the target similar the benign files previously sent
- Request that the target user open the malicious document
- Exfiltrate data from the victim machine

The process above can take multiple months from the initial connection to the delivery of the malicious document. The attackers build a relationship with target users over time by having constant and continuous communications which allows them to build trust and confidence with the target. In many of the cases we have observed, the targets genuinely believed that they were making a human connection and not interacting with a threat actor operating from Iran.

By exercising patience, building relationships, and pestering targets continuously once a relationship has been formed, Iranian threat actors have had more success in

compromising their targets.

Brute force

In 2021, MSTIC observed DEV-0343 aggressively targeting Office 365 tenants via an ongoing campaign of password spray attacks. DEV-0343 is a threat actor MSTIC assesses to be likely operating in support of Iranian interests. MSTIC has blogged about DEV-0343 activity previously.

Analysis of Office 365 logs suggests that DEV-0343 is using a red team tool like o365spray to conduct these attacks.

Targeting in this DEV-0343 activity has been observed across defense companies that support United States, European Union, and Israeli government partners producing military-grade radars, drone technology, satellite systems, and emergency response communication systems. Further activity has targeted customers in geographic information systems (GIS), spatial analytics, regional ports of entry in the Persian Gulf, and several maritime and cargo transportation companies with a business focus in the Middle East.

As we discussed in our previous blog, DEV-0343 operators' 'pattern of life' is consistent with the working schedule of actors based in Iran. DEV-0343 operator activity peaked Sunday through Thursday between 04:00:00 and 16:00:00 UTC.

Figure 2: DEV-0343 observed operating hours in UTC

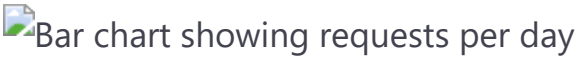

Figure 3: DEV-0343 observed actor requests per day

Known DEV-0343 operators have also been observed targeting the same account on the same tenant being targeted by other known Iranian operators. For example, EUROPIUM

operators attempted to access a specific account on June 12, 2021 and ultimately gained access to this account on June 13, 2021. DEV-0343 was then observed targeting this same account within minutes of EUROPIUM operators gaining access to it the same day. MSTIC assesses that these observed overlapping activities suggest a coordination between different Iranian actors pursuing common objectives.

Closing thoughts: Increasingly capable threat actors

As Iranian operators have adapted both their strategic goals and tradecraft, over time they have evolved into more competent threat actors capable of conducting a full spectrum of operations including:

- Information operations
- Disruption and destruction
- Support to physical operations

Specifically, Iranian operators have proven themselves to be both willing and able to:

- Deploy ransomware
- Deploy disk wipers
- Deploy mobile malware
- Conduct phishing attacks
- Conduct password spray attacks
- Conduct mass exploitation attacks
- Conduct supply chain attacks
- Cloak C2 communications behind legitimate cloud services

MSTIC thanks CyberWarCon 2021 for the opportunity to present this research to the broader security community. Microsoft will continue to monitor all this activity by Iranian actors and implement protections for our customers.