Iranian targeting of IT sector on the rise

microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/

November 18, 2021

Iranian threat actors are increasing attacks against IT services companies as a way to access their customers' networks. This activity is notable because targeting third parties has the potential to exploit more sensitive organizations by taking advantage of trust and access in a supply chain. Microsoft has observed multiple Iranian threat actors targeting the IT services sector in attacks that aim to steal sign-in credentials belonging to downstream customer networks to enable further attacks. The Microsoft Threat Intelligence Center (MSTIC) and Digital Security Unit (DSU) assess this is part of a broader espionage objective to compromise organizations of interest to the Iranian regime.

Until July 2021, Microsoft had observed relatively little history of Iranian actors attacking Indian targets. As India and other nations rise as major IT services hubs, more nation state actors follow the supply chain to target these providers' public and private sector customers around the world matching nation state interests.

To date this year, Microsoft has issued more than 1,600 notifications to over 40 IT companies in response to Iranian targeting, compared to 48 notifications in 2020, making this a significant increase from years past (Figure 1). The focus of several Iranian threat groups on the IT sector particularly spiked in the last six months – roughly 10-13% of our notifications were related to Iranian threat activity in the last six months, compared to two and a half percent in the six months prior (Figure 2).

Most of the targeting is focused on IT services companies based in India, as well as several companies based in Israel and United Arab Emirates. Although different in technique from other recent supply chain attacks, these attacks represent another example of how nation state actors are increasingly targeting supply chains as indirect vectors to achieve their objectives.

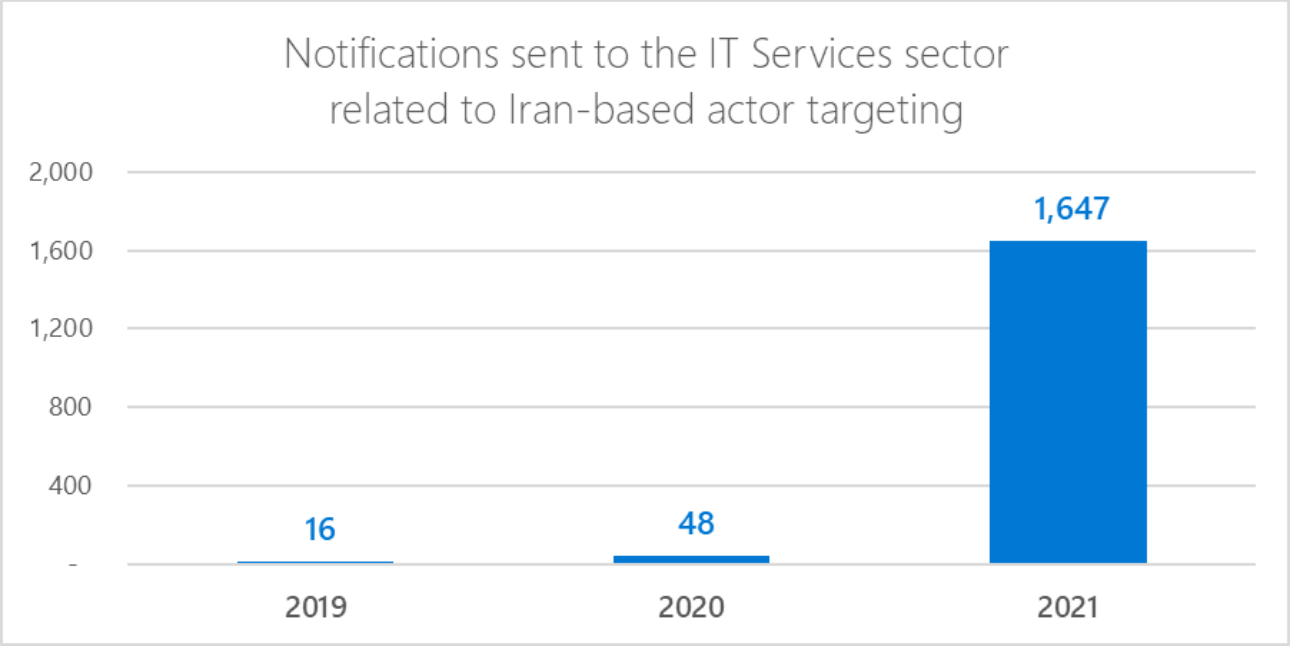

Figure 1: Number of notifications sent to IT Services related to Iran-based actor targeting

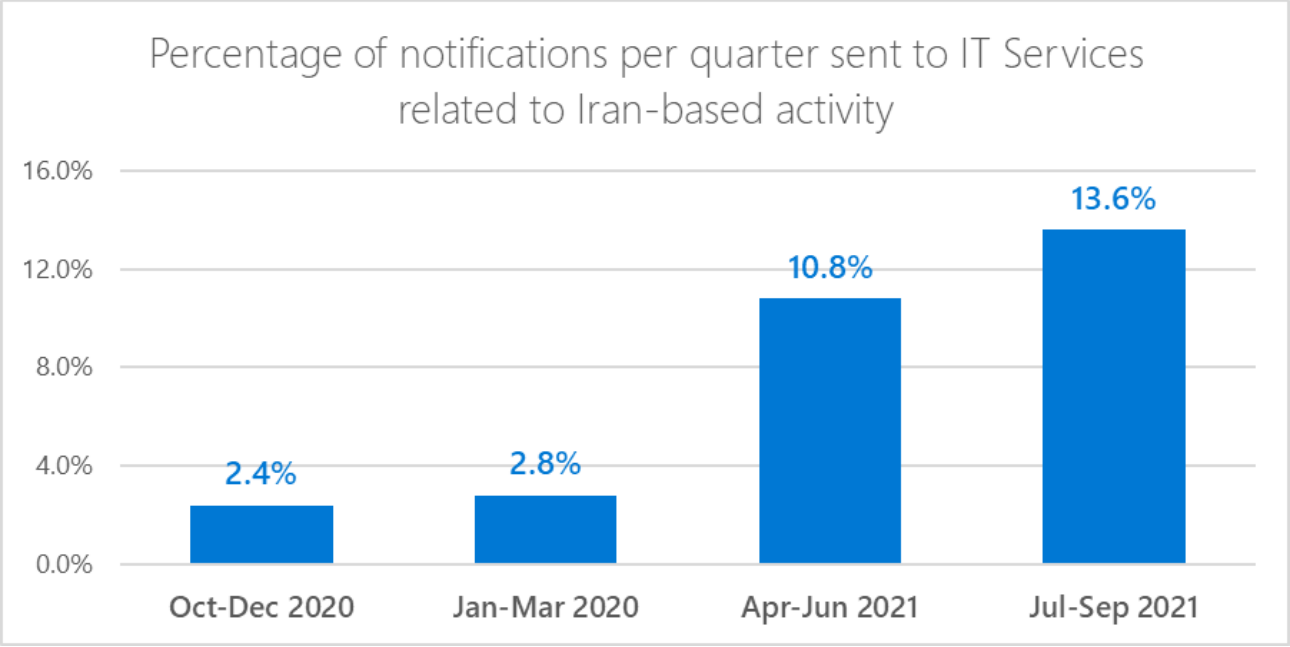

Figure 2: Percentage of notifications per quarter sent to IT Services NSNs related to Iran-based activity

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 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.

Observed activity

In July 2021, a group that MSTIC tracks as DEV-0228 and assesses as based in Iran compromised a single Israel-based IT company that provides business management software. Based on MSTIC's assessment, DEV-0228 used access to that IT company to extend their attacks and compromise downstream customers in the defense, energy, and legal sectors in Israel. In September, we detected a separate Iranian group, DEV-0056, compromising email accounts at a Bahrain-based IT integration company that works on IT integration with Bahrain Government clients, who were likely DEV-0056's ultimate target. DEV-0056 also compromised various accounts at a partially government-owned organization in the Middle East that provide information and communications technology to the defense and transportation sectors, which are targets of interest to the Iranian regime. DEV-0056 maintained persistence at the IT integration organization through at least October.

MSTIC detected a significant increase in these and other Iranian groups targeting IT companies based in India beginning in mid-August. From mid-August to late September, we issued 1,788 nation state notifications (NSNs) across Iranian actors to enterprise customers in India, roughly 80% of which were to IT companies, an exponential rise from the 10 notifications we issued the previous three years in response to previous Iranian targeting. Iranian cyber actors have rarely targeted India, and the lack of pressing geopolitical issues that would have prompted such a shift suggests that this targeting is for indirect access to subsidiaries and clients outside India.

Credential theft leads to downstream compromise

DEV-0228 dumped credentials from the on-premises network of an IT provider based in Israel in early July. Over the next two months, the group compromised at least a dozen other organizations, several of which have strong public relations with the compromised IT company. MSTIC assesses at least four (4) of those victims were compromised using the acquired credentials and access from the IT company in the July and August attacks. Here are two such examples:

> DEV-0228 operators compromised the on-premises network of a law firm in Israel in August through an account managed by the IT provider via PAExec (a custom version of the Windows Sysinternals tool PsExec).

```
Pa.exe  \\###.##.#.## -u {user name}\{domain name} -p "********" -s cmd.exe
```

> DEV-0228 operators also compromised a defense company in Israel by signing into an email account provisioned for the same IT provider on the victim's Office 365 tenant. The attackers likely obtained those credentials from the initial compromise of the IT provider in July.

Custom implant to establish persistence

DEV-0228 operators used a custom implant to establish persistence on victim hosts and then dumped LSASS. The implant is a custom remote access Trojan (RAT) that uses Dropbox as a command and control (C2) channel and is disguised as *RuntimeBroker.exe* or *svchost.exe*.

Operators staged their tools in a *C:\Windows\TAPI* directory on the victim hosts:

- C:\Windows\TAPI\lsa.exe
- C:\Windows\TAPI\pa.exe
- C:\Windows\TAPI\pc.exe (procdump)
- C:\Windows\TAPI\Rar.exe

Microsoft will continue to monitor DEV-0228 and DEV-0056 activity and implement protections for our customers. The current detections, advanced detections, and IOCs in place across our security products are detailed below.

Indicators of compromise (IOCs)

Type	Indicator
svchost.exe	2a1044e9e6e87a032f80c6d9ea6ae61bbbb053c0a21b186ecb3b812b49eb03b7
svchost.exe	9ab7e99ed84f94a7b6409b87e56dc6e1143b05034a5e4455e8c555dbbcd0d2dd
lsa.exe	43109fbe8b752f7a9076eaafa417d9ae5c6e827cd5374b866672263fdebd5ec3
wdmsvc.exe	18a072ccfab239e140d8f682e2874e8ff19d94311fc8bb9564043d3e0deda54b
Pa.exe (PAExec.exe)	ab50d8d707b97712178a92bbac74ccc2a5699eb41c17aa77f713ff3e568dcedb

Recommended defenses

The following guidance can mitigate the techniques described in the threat activity:

- Enable multi-factor authentication to mitigate compromised credentials.
  - For Office 365 users, see multi-factor authentication support.
  - For Consumer and Personal email accounts, see how to use two-step verification.
- Use passwordless solutions like Microsoft Authenticator to secure accounts.
- Review and enforce recommended Exchange Online access policies.
  Block ActiveSync clients from bypassing Conditional Access policies.
- Block all incoming traffic from anonymizing services where possible.
- Turn on the following attack surface reduction rule to block or audit activity associated with this threat:
  Block credential stealing from the Windows local security authority subsystem (lsass.exe)

Detections

Microsoft 365 Defender

Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- Backdoor:MSIL/ShellClient.A
- Backdoor:MSIL/ShellClient.A!dll
- Trojan:MSIL/Mimikatz.BA!MTB

Endpoint detection and response (EDR)

Alerts with the following titles in the security center can indicate threat activity on the network:

- DEV-0228 actor activity
- DEV-0056 actor activity

The following alerts might indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity, but they are listed here for reference:

- Suspicious connection to remote service
- Possible command-and-control activity
- Suspicious access to LSASS service
- Sensitive credential memory read

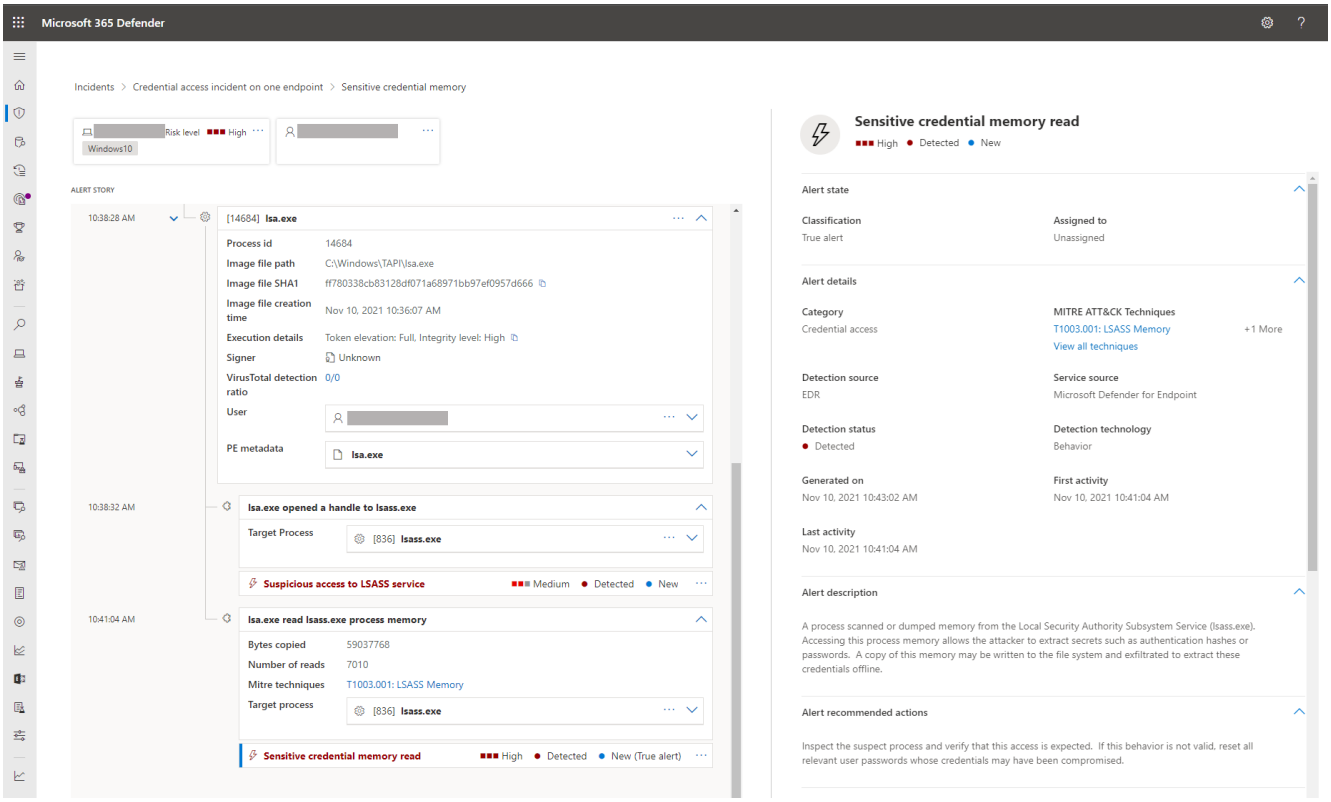

Figure 3: Microsoft 365 Defender alert showing credential dumping activity

Microsoft 365 Defender correlates related alerts into consolidated incidents to help customers determine with confidence if observed alerts are related to this activity. Customers using the Microsoft 365 Defender portal can view, investigate, and respond to incidents that include any detections related to the activity described in this blog.

Advanced hunting queries

Microsoft Sentinel

The indicators of compromise (IoCs) included in this blog post can be used by Microsoft Sentinel customers for detection purposes using the queries detailed below.

Command Line Activity November 2021

This hunting query looks for process command line activity related to observed activity. The query uses additional data from Microsoft Defender for Endpoint to generate a risk score associated with each result. Hosts with higher risk events should be investigated first.

https://github.com/azure/azure-sentinel/blob/master/Hunting%20Queries/MultipleDataSources/Dev-0056CommandLineActivityNovember2021.yaml

FilePath/Hashes query November 2021

This hunting query looks for file paths/hashes related to observed activity as detailed in this blog.

https://github.com/Azure/Azure-Sentinel/tree/master/Detections/MultipleDataSources/Dev-0228FilePathHashesNovember2021.yaml

In addition to these queries, there are equivalent queries that use the Advanced SIEM Information Model (ASIM) to look for the same activity.

https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries/ASimProcess/imProcess_Dev-0056CommandLineActivityNovember2021-ASIM.yaml

https://github.com/Azure/Azure-Sentinel/tree/master/Detections/ASimFileEvent/imFileEvent_Dev-0228FilePathHashesNovember2021-ASIM.yaml

Microsoft 365 Defender

To locate malicious activity related to the activity described in this blog, customers can run the following queries in Microsoft 365 Defender or Microsoft Defender for Endpoint.

Identify use of PAExec in your environment

Look for *PAExec.exe* process executions in your environment. Run query.

```
DeviceProcessEvents
| where FileName =~ "paexec.exe" or ProcessVersionInfoOriginalFileName =~ "paexec.exe"
| where not(ProcessCommandLine has_any("program files", "-service"))
```

Identify files created in the Windows\Tapi directory

Look for files created in the Windows\Tapi directory. Run query.

```
DeviceFileEvents
| where FolderPath has @"C:\Windows\TAPI"
```

Suspicious PowerShell commands

Look for suspicious PowerShell process execution. Run query.

```
DeviceProcessEvents
| where ProcessCommandLine has_any("/q /c color f7&", "Net.We$()bClient",
"$b,15,$b.Length-15") or
(ProcessCommandLine has "FromBase64String" and ProcessCommandLine has_all("-nop",
"iex", "(iex"))
```