NATION-STATE CYBERATTACKS

Threat Brief: Iranian-Linked Cyber Operations

6 min read

By: Unit 42
Published: 9 January, 2020 at 6:00 PM PST
Categories: High Profile Threats , Nation-State Cyberattacks
Tags: Advanced Persistent Threat , APT34 , Cobalt Gypsy , DarkHydrus , Elfin , Evasive Serpens , Helix Kitten , Magic hound , MuddyWater , Newscaster , OilRig , Refined Kitten , Shamoon , Shamoon 2 , Shamoon 3 , Static Kitten

This post is also available in: 日本語 (Japanese)

Executive Summary

With elevated tensions in the Middle East region, there is significant attention being paid to the potential for cyber attacks emanating from Iran. The following threat brief contains a summary of historical campaigns that are associated with Iranian activity and does not expose any new threat or attack that has occurred since the events of January 3rd, 2020.

Since 2010, it is thought that Iran has been highly active in cyber operations campaigns throughout the world. A number of groups and campaigns have been named and published on by the private sector, but direct attribution to the nation-state of Iran is still largely lacking in many of these instances. Most attribution published by the private sector has relied on tactical evidence surrounding targeting and possible motivations. It is important to keep this in mind, while at the same time understanding that without additional evidence, the current attribution set is accepted industry-wide as fact. Unit 42 has not gathered evidence to specifically attribute any of the accepted groups as originating from Iran, but also has not observed any evidence to counter any publicly made claims.

Overview of Iran-Linked Campaigns: Some of the currently active groups or campaigns publicly attributed by the industry as originating from Iran are:

- OilRig (AKA APT34/Helix Kitten)
- MagicHound (AKA APT35/Newscaster/Cobalt Gypsy)
- APT33 (AKA Refined Kitten/Elfin)

- DarkHydrus
- Shamoon
- MuddyWater (AKA Static Kitten)

There appear to be two distinct motivators for these groups, espionage and destruction. The majority of observed attack campaigns have been espionage related, with the associated groups appearing to seek continued access into a target organization or access to sensitive data. A smaller number of highly focused destructive attacks have been observed over time, beginning with the original Shamoon attack in 2012, with additional iterations years after, and more recently with StoneDrill and ZeroCleare.

Overall, cyber attacks thought to be originating from Iran have been persistent and ongoing for the last decade. The target radius for these groups have spanned across the globe, across all major industries. Although perceived retaliatory actions may occur in the near future, even those actions are most likely in conjunction with ongoing attack campaigns and operations.

Iranian TTPs: Behaviorally, several tactics and techniques have been observed across multiple groups and campaigns over time. The following is a list of commonly observed tactics and techniques along with their associated ATT&CK IDs:

- Phishing (**T1193** and **T1192**)
- Credential harvesting (**T1078**, **T1003**, **T1503**, **T1081**, **T1214**)
- DNS Tunneling (**T1071**)
- DNS Hijacking (**T1326**)
- EldoS RawDisk driver (**T1485**, **T1488**, **T1487**, **S0364**)
- Malicious macros (**T1204**)
- Weaponized Excel and Word documents (**T1204**, **T1221**, **T1173**)
- Script based backdoors (**T1064**, **T1027**)
- Webshell deployment (**T1108**, **T1133**, **T1190**, **T1027**)
- Domain masquerading (**T1328**)
- Scheduled tasks (**T1053**)
- Use of Mimikatz (**T1003**, **T1207**, **T1098**, **T1081**, **S0002**)
- Exploitation of enterprise VPN Software (**T1133**, **T1210**)

General Mitigations: With this knowledge of common behaviors, some mitigations recommendations are:

- Increase education and awareness against phishing attacks in your organization via exercises and informational resources
- Enable or implement multi-factor authentication on public facing systems, or more preferably, across the entire organization
- Enable or implement credential theft detection features in network security devices
- Enable or implement anomalous DNS behavior detection/prevention capability
- Blacklist EldoS RawDisk driver, unless absolutely required for business purposes
- Review security policies for macro documents and restrict execution where possible
- Review security policies for script file execution on endpoints and restrict where possible
- Review all public facing network applications and deploy up-to-date patches
- Enable or implement domain or URL categorization features in network security devices
- Scan endpoints for new or unknown scheduled tasks
- Implement detection and prevention logic for behaviors associated with Mimikatz
- Patch remotely exposed software for known vulnerabilities as soon as possible

Palo Alto Networks' Customer Mitigations: Palo Alto Networks customers should adopt best practices and evaluate their security posture to protect against the threats outlined in this document as well as other threats that may impact their network and users.

- **Best Practice Resources**
- **Best Practice Assessment**
- **Security Lifecycle Review**

Group Details

OilRig (AKA APT34/Helix Kitten)

https://attack.mitre.org/groups/G0049/

OilRig is a threat group Unit 42 named and discovered in May 2016. Since then, we have extensively researched their campaigns and operations. This threat group is extremely persistent and relies heavily on spear-phishing as their initial attack vector, but has also been associated with other more sophisticated attacks such credential harvesting campaigns and DNS hijacking. In their spear-phishing attacks, OilRig preferred macro-enabled Microsoft Office (Word and Excel) documents to install their custom payloads that came in the form of portable executables (PE), PowerShell and VBScripts. OilRig's custom payloads frequently used DNS tunneling as a command and control (C2) channel.

Once gaining access to an end point, actors would use credential dumping tools, such as Mimikatz to gather credentials to legitimate accounts to then move laterally to other systems on the network. When presented with a webserver, OilRig would install a webshell as another ingress point to maintain access to the network.

References

https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/

https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/

https://unit42.paloaltonetworks.com/unit42-analyzing-oilrigs-ops-tempo-testing-weaponization-delivery/

https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

https://unit42.paloaltonetworks.com/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/

https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

https://unit42.paloaltonetworks.com/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

https://unit42.paloaltonetworks.com/unit42-oilrig-performs-tests-twoface-webshell/

https://unit42.paloaltonetworks.com/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/

https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/

https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/

https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/

https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

Magic Hound (AKA APT35/Newscaster/Cobalt Gypsy)

https://attack.mitre.org/groups/G0059/

The Magic Hound campaign targeted energy, government, and technology organizations with spear-phishing emails as a delivery mechanism. These emails delivered macro-enabled Microsoft Office documents and PE files within attachments. The documents and executables attached to emails would install a variety of tools from portable PE files, .NET Framework PE files, Meterpreter, IRC bots, an open sourced Meterpreter module called Magic Unicorn, and an open sourced Python RAT called Pupy.

The custom tools used in the Magic Hound campaign provided connections to other threat groups, such as the IRC Bot which was very similar to the Parastoo tool associated with the NEWSCASTER threat group. Also, a Magic Hound C2 server was also used as a C2 server for a tool called MPKBot that had been associated with the Rocket Kitten threat group.

References

https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/

APT33 (AKA Refined Kitten/Elfin)

https://attack.mitre.org/groups/G0064/

APT33 is a threat group thought to have strong interest in the aeronautics and energy sectors. They use spear-phishing attacks with a domain masquerading technique to make the links in their emails appear legitimate. They are known to use custom tools in conjunction with well-known publicly available backdoors that are sold in various hacking forums. A recent report uncovered this threat group's attack infrastructure, which leveraged commercial VPN providers in addition to compromised systems to use as proxies to further mask their origins. This activity exemplified how this adversary group and other related groups will attack organizations outside of their mission objective to augment their own capabilities to complete their task.

References

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/

DarkHydrus

https://attack.mitre.org/groups/G0079/

The DarkHydrus threat group has targeted government entities and educational institutions with spear-phishing attacks and credential harvesting campaigns. DarkHydrus is a more sophisticated group when compared to others operating in the region, as their toolset and TTPs show a higher skill level. DarkHydrus has used custom tools in addition to publicly available red-teaming tools such as Phishery. They have also been observed using Google Drive for their C2 channel.

References

https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

https://unit42.paloaltonetworks.com/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/

https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/

Shamoon

The original Shamoon attack was launched in 2012 and targeted two specific organizations in the energy sector with the goal of rendering their respective computer systems inoperable by wiping their disks. The attack package included a commercially available driver to execute the wiping tasks and also included a worming component which allowed the package to spread within a target organization in an automated manner. The 2012 incident was one of the first large scale targeted destructive attacks that had been publicly shared. Since the original 2012 attack, two other instances of Shamoon have been discovered, in 2016 as well as 2018. In each instance, the primary capabilities and functionality remained largely the same.

References

https://securelist.com/shamoon-the-wiper-copycats-at-work/57854/

https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/

https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/

https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/

https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

https://unit42.paloaltonetworks.com/shamoon-3-modified-open-source-wiper-contains-verse-from-the-quran/

MuddyWater (AKA Static Kitten)

MuddyWater is a group that emerged in 2017 and was initially thought to be part of the financially motivated criminal group commonly referred to as FIN7 due to the use of an open source tool that was used by both sets of activity. Additional investigation revealed no other similarities in either tools or tactics, thus concluding that the MuddyWater activity was likely operated by a separate actor. This group generally used spear-phishing with macro-enabled Office documents to deliver their payloads, which were either embedded directly in the macro, or hosted on a first stage C2 server. These C2 servers were observed to be either third party file hosting sites or code sharing repositories such as GitHub. A significant portion of MuddyWater's toolset consisted of open sourced red-teaming tools such as Invoke-Obfuscation, Lazagne, Mimikatz, etc.

References

https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

https://securelist.com/muddywater/88059/

https://www.clearskysec.com/muddywater2/

https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/

Conclusion

Assuming the highlighted groups are indeed Iranian in origin, their activity has been well documented and the various groups often times use very similar tactics and techniques to execute their attacks, such as the heavy use of spear-phishing and credential harvesting. This activity has been persistent for the last decade, and it should be expected to continue or increase with recent geopolitical events. However, across all of these groups as well as others that were not

highlighted, another consistent theme has been the abuse of poorly implemented IT and security policies. Enabling Multi-Factor Authentication (MFA) throughout an organization, properly segmenting networks, limited macro-enabled documents, and disallowing network activity to unknown domains are examples of relatively simple policies that could have assisted in the neutralization of these adversary groups' malicious actions.

Indicators

Unit 42 has consolidated the IOCs of the referenced groups in this report and stored them in our GitHub repository. This dataset should not be considered comprehensive of all potential Iran-linked cyber operations, and may be subject to change without notice.

Link to IOCs on GitHub

Back to top

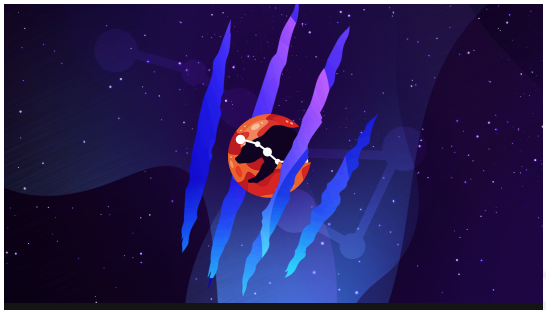
TAGS

Advanced Persistent Threat | APT34 | Cobalt Gypsy | DarkHydrus | Elfin | Evasive Serpens | Helix Kitten | Magic hound | MuddyWater | Newscaster | OilRig | Refined Kitten | Shamoon | Shamoon 2 | Shamoon 3 | Static Kitten

Threat Research Center

Next: Wireshark Tutorial: Examining Ursnif Infections

Related Nation-State Cyberattacks Resources



THREAT ACTOR GROUPS

Fighting Ursa Luring Targets With Car for Sale

Advanced Persistent Threat | APT28 | Fancy Bear

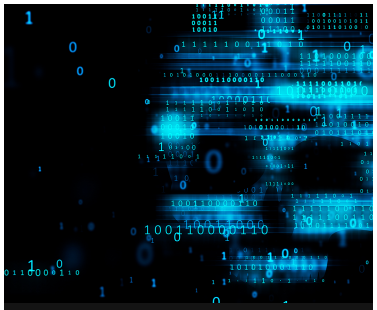
Read now →

THREAT ACTOR GROUPS

Threat Actor Groups Tracked by Palo Alto Networks Unit 42

Academic Serpens | Agent Serpens | Agonizing Serpens

Read now →



THREAT RESEARCH

Operation Diplomatic Specter: An Chinese Cyberespionage Campa Rare Tool Set to Target Governm

Advanced Persistent Threat | Bac | China