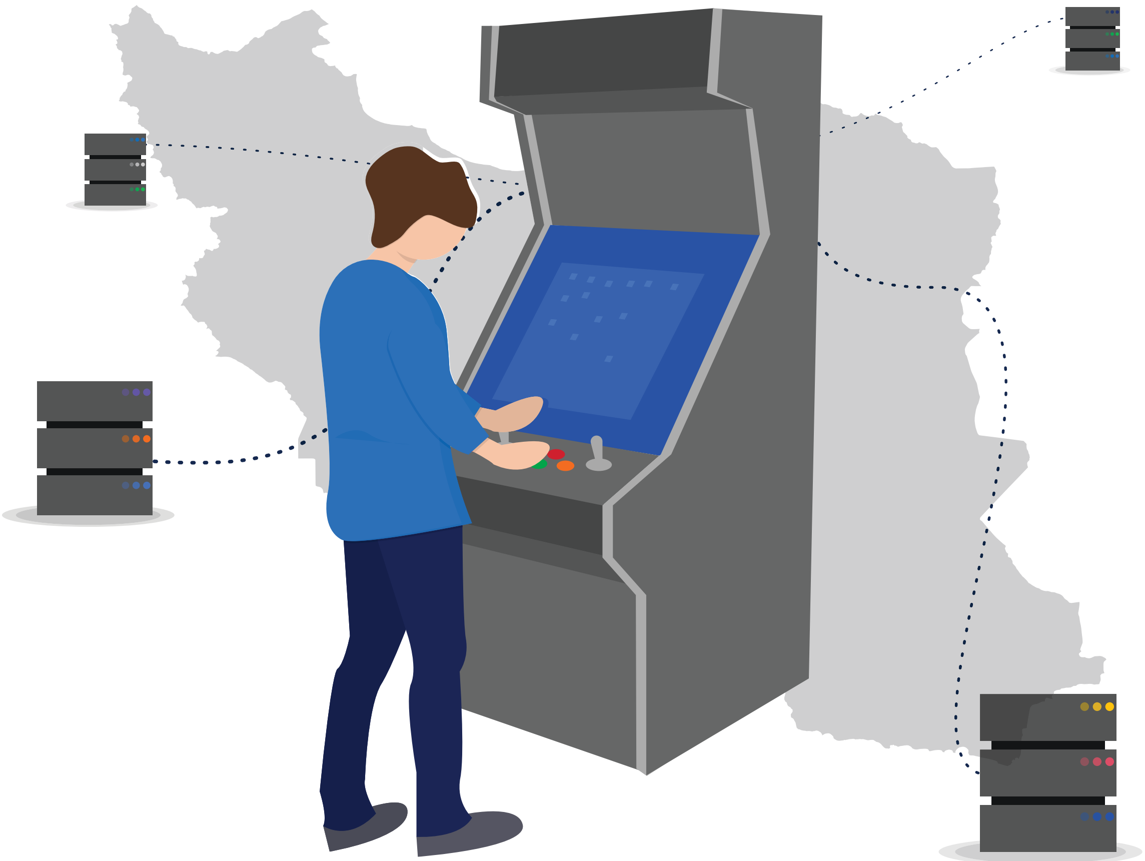
Recorded Future

CYBER THREAT ANALYSIS

Operation Gamework:

Infrastructure Overlaps Found Between BlueAlpha and Iranian APTs

By Insikt Group®



CTA-2019-1212

Earlier this year, Recorded Future's Insikt Group published research titled "Iranian Threat Actor Amasses Large Infrastructure Network to Target Saudi Organizations," which analyzed the network infrastructure of suspected Iranian state-sponsored CNO threat actors. We continued to monitor the activity until late July 2019 using proprietary techniques including Recorded Future network traffic analysis and Recorded Future domain analysis.

Data sources included the Recorded Future® Platform, Farsight Security's DNSDB, ReversingLabs, VirusTotal, Shodan, and common OSINT tools.

The target audience for this research includes security practitioners and threat intelligence professionals who exhibit an interest in Russian and Iranian nation-state computer network operational activity.

Executive Summary

Over the course of 2019, there were several documented instances of Russian threat actor groups hijacking Iranian group infrastructure, most recently with the U.K. National Cyber Security Center (NCSC) and U.S. National Security Agency (NSA) jointly releasing an advisory outlining how the Russian-attributed threat group Turla had co-opted two Iranian malware families, likely without Iranian knowledge.

In our analysis, we uncovered evidence of an overlap in operational infrastructure between a threat actor Insikt Group tracks as BlueAlpha and suspected Iranian nation-state activity. There is a strong overlap between BlueAlpha and Gamaredon Group malware and infrastructure TTPs; therefore, we assess with moderate confidence that BlueAlpha is a Russian state-sponsored threat actor. Notably, the Security Service of Ukraine (SBU) has attributed the Gamaredon Group to the FSB 16th and 18th divisions.

Further, we found more overlaps between infrastructure associated with several well-documented Iranian threat actor groups, including APT33 (Elfin), APT35 (Charming Kitten), and MUDDYWATER. Both APT33 and APT35 are believed to be operating in line with strategic priorities set by the Iranian Revolutionary Guard Corps (IRGC); the organizational attribution for MUDDYWATER is less clear at this stage. For ease of comprehension, we will refer to the clustering of APT33, APT35, and MUDDYWATER infrastructure as the "Iran-nexus" in this report. Please note that we do not assess, at this stage, that these groups are a single homogenous Iranian threat actor, but rather that they all have notable overlapping TTPs.

Key Judgments

We continue to discover infrastructure overlaps among several Iranian threat actor groups. When coupled with our prior research on the tiered approach to the Iranian cyber operational administration, we assess that distinctions between these threat actor groups continue to blur, which leads us to consider the following hypotheses, which are not mutually exclusive:

- Some form of organizational overlap is placed over the management of operational resources between Iranian groups.
- The overlaps indicate that the groups are closely aligned, share resources, and are possibly all working for the same organization, which we assess is likely to be the IRGC for the APT33, APT35, and MUDDYWATER nexus.
- The infrastructure overlaps point to a potential misclassification of Iranian threat actor groups, or suggest that the groups have evolved such that previous classifications may be inadequate.

In two separate instances, we identified unique domain characteristics that linked a domain spoofing the Saudi International Petrochemical Company and used by the Iran-nexus threat actor group to the operational infrastructure of the suspected-Russian state-sponsored threat actor BlueAlpha. We have high confidence in the association of these domains and the operational activity associated with them to BlueAlpha in 2019, which points to the following potential hypotheses:

- BlueAlpha mimicked the TTPs of the Iran-nexus groups. We assess that this is a likely scenario given the two (1, 2) very notable recent examples of FSB-affiliated threat actors hijacking Iranian APT infrastructure.
- BlueAlpha commandeered old Iran-nexus group infrastructure. Insikt Group assesses that this is also a likely scenario, given that other FSB-affiliated threat actors such as Turla have demonstrated an effective ability to use false flags.

- Iran-nexus group mimicked Gamaredon Group TTPs. Insikt Group assesses this to be an unlikely scenario, because it would require a very high degree of technical and operational preparedness and would be a high-risk maneuver by the Iran-nexus group in order to target Ukrainian interests.
- An operational collaboration exists between the Iran-nexus group and BlueAlpha. While collaboration on training and sharing of techniques is plausible, actual operational infrastructure sharing would require non-trivial deconfliction efforts to ensure targeted operations were effective. We assess this to be an unlikely scenario.

Outlook

On October 21, the U.K. National Cyber Security Center (NCSC) and U.S. National Security Agency (NSA) jointly released an advisory outlining how the Russian-attributed threat group Turla had co-opted two Iranian tools, likely without Iranian knowledge. NCSC and NSA were able to make the distinction between the Iranian activity using these tools and the Turla activity on the basis of three factors:

1. Administration of infrastructure from either Turla or Iranian-associated IP addresses
2. Turla group scanned for Iranian-associated backdoors
3. Turla compromised Iranian infrastructure by deploying their own implants

Turla has been attributed by Estonian intelligence services and the Czech government to the Russian Federal Security Service (FSB). The Security Services of Ukraine as well as threat intelligence researchers have also attributed Gamaredon Group to the FSB.

In our research, we observed significant overlapping operational infrastructure between Iranian groups APT33, APT35, and MUDDYWATER. We assess with moderate confidence that all three groups are likely tied to the IRGC and the continued blurring of TTPs between the three groups is likely to continue to inhibit clustering of IRGC-originated threat activity.

We also uncovered significant overlaps between the operational infrastructure for the Iran-nexus group and the Gamaredon Group. The number of overlapping domains indicate our observations are a key departure from previously reported Gamaredon activity. This departure was the apparent Middle Eastern targeting, as Gamaredon have typically targeted Ukrainian interests in the past. For that reason, we opted for the BlueAlpha designator for the suspected Russia state-sponsored threat actor. We assess BlueAlpha and Gamaredon Group are closely aligned groups with similar TTPs and are both likely tied to Russia’s FSB. Insikt Group assesses that Russian state-sponsored groups will continue to conduct cyber operations that use techniques such as false flags or leverage vulnerable operational infrastructure of other threat actors in order to obfuscate activity and hinder attribution efforts.