Iranian Actor “Group5” Targeting Syrian Opposition

By SecurityWeek News

Published: 2016-08-04 · Archived: 2026-04-05 18:11:22 UTC

A threat actor using Iranian-language tools, Iranian hosting companies, operating from the Iranian IP space at times was observed targeting the Syrian opposition in an elaborately staged malware operation, Citizen Lab researchers reveal.

The operation was first noticed in late 2015, when a member of the Syrian opposition flagged a suspicious email containing a PowerPoint slideshow, which led researchers to a watering hole website with malicious programs, malicious PowerPoint files, and Android malware.

The threat actor was targeting Windows and Android devices of well-connected individuals in the Syrian opposition, researchers discovered. They called the actor **Group5**, because it targets Syrian opposition after regime-linked malware groups, the Syrian Electronic Army, ISIS (also known as the Islamic State or ISIL), and a group linked to Lebanon did the same in the past.

To conduct its attacks, the group uses social engineering, as it “borrows opposition text and slogans for e-mail messages and watering holes,” Citizen Lab researchers say. The group’s technical quality, however, is low, and researchers suggest that they identified the actor early in its lifecycle, before it could launch a full campaign using the malware it staged and prepared.

The group is believed to be state-sponsored, at least in some form, though it’s yet unclear which state is behind it. However, Citizen Lab researchers reveal that Group5 is likely a new entrant in Syria, and that there is “only circumstantial evidence pointing to an Iranian nexus.” Yet, the group’s activity shows that Syrian opposition is facing continuing information security risks.

The investigation was triggered by a suspicious email received in early October 2015 by Noura Al-Ameer, a well-connected Syrian opposition political figure, which was sent from the same IP address that hosted the command and control (C&C) server the malware inside it was connecting to.

The email was sent from an address on *assadcrimes[.] info*, a website found to be distributing other malicious files, including a . ppsx and a .exe. The PPSX documents, for example, were found to be leveraging the CVE-2014-4114 vulnerability to drop and execute malicious code, but also to execute OLE objects using animation actions within a PowerPoint slideshow.

Researchers also discovered that the group was employing two commonly available Remote Access Trojans (RATs): njRat and NanoCore RAT for its nefarious operations. The binaries were delivered hidden under several layers of obfuscation to reduce the possibility of detection by antivirus software.

The two malware variants were used to collect data from the compromised machines, to keep an eye on the victim's screen, or capture passwords and keystrokes. They were also used to remotely delete files and even to spy on the computer user via the microphone or webcam.

In addition to these malicious applications for Windows, the *assadcrimes[.]info* website also contained a decoy Flash Player update page that linked to a piece of Android malware called DroidJack. The Trojan, which evolved from a piece of malware called SandroRAT, was recently used in a global attack, hidden inside a fake Pokémon GO application.

The Trojan was created to capture messages, contacts, photos and other data from the infected Android device, as well as to remotely activate the phone camera and microphone, without notifying the victim. The use of this malware isn't surprising, researchers say: "It is common for Syrians to share Android APK files outside the Google Play Store, as Google Play Services are not available within Syria."

Because the *assadcrimes[.]info* operators left a folder containing the website logs public, researchers were able to identify the IP addresses used by Group5 while developing the site, though they couldn't conclusively identify victims' IPs. During the site's early development in the first half of October, it was accessed hourly from an Iranian IP block. The operators also accessed the site from the malware's C&C server, Citizen Lab says.

"These links provide evidence for an Iranian nexus, and suggest that the operator may have been taking steps to conceal their true origin IP. However, these steps were not well executed, which enabled us to track Group5 as they continued to access the site," researchers reveal. According to them, however, the threat actor appears to have abandoned the site after New Year, following a flurry of activity in October 2015.

According to researchers, there is also the possibility that a known group was behind all this operation and that a key piece that was missing from the puzzle prevented the investigators from making the correct associations, although the tools used to obfuscate the RATs link the group to known threat actors (Mr. Tekide) and tools (the PAC Crypt tool).

“We cannot conclude with certainty that Group5 is Iran-based, although the confluence of information outlined above provides a circumstantial case. The IP addresses observed during early stages of development of the Assadcrimes website, as well as the Iranian hosting provider and the Persian language mailer, all speak to a level of Iranian presence. The additional apparent involvement of an Iranian malware developer with ties to a known Iranian cyber actor, whether his involvement was unwitting or intentional, only strengthens the Iranian connection,” researchers say.

Related: India-Linked Threat Actor Targets Military, Political Entities Worldwide

Related: Hacktivists Leak 43GB of Data From Syrian Government

---