Second Iranian State-Sponsored Ransomware "Project Signal" Emerges

flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/

April 30, 2021

Blogs

Blog

A Second Iranian State-Sponsored Ransomware Operation “Project Signal” Emerges

Flashpoint has validated recently leaked documents that indicate Iran’s Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company called “Emen Net Pasargard” (ENP) (aka “Imannet Pasargad,” “Iliant Gostar Iranian,” “Eeleyanet Gostar Iraniyan”). These three documents were originally leaked between March 19 and April 1, 2021, by the Iranian dissident group “Lab Dookhtegan,” famous for providing highly reputable intelligence on Iranian state-sponsored cyber programs.

Leaked Documents Confirm Second Iranian State-Sponsored Ransomware Operation

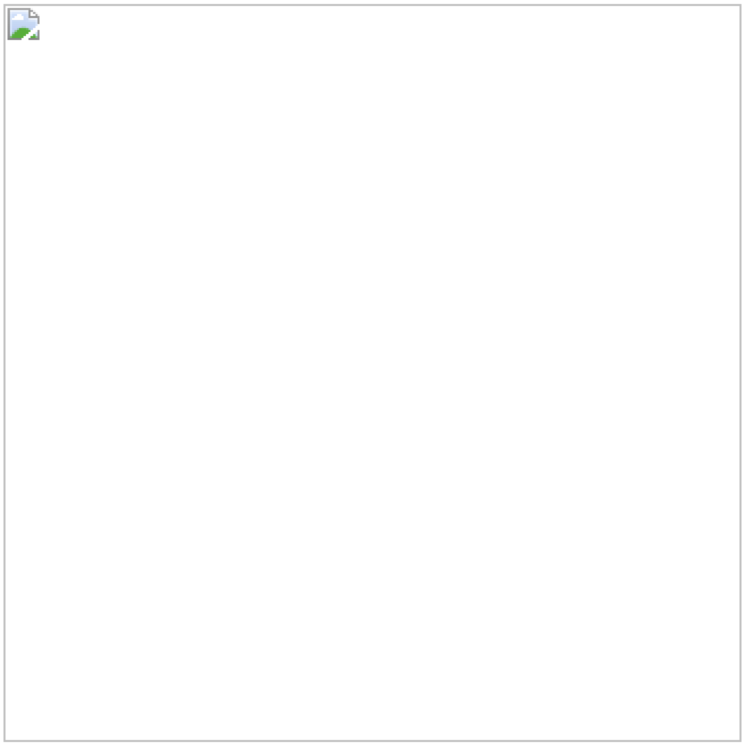
Flashpoint has validated recently leaked documents that indicate Iran’s Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company called “Emen Net Pasargard” (ENP) (aka “Imannet Pasargad,” “Iliant Gostar Iranian,” “Eeleyanet Gostar Iraniyan”). These three documents were originally leaked between March 19 and April 1, 2021, by the Iranian dissident group “Lab Dookhtegan,” famous for providing highly reputable intelligence on Iranian state-sponsored cyber programs.

Documents Shed Light on “Project Signal” Ransomware Operations

ENP’s ransomware project dubbed “Project Signal” began sometime between late July 2020 and early September 2020, when ENP’s internal research organization the “Studies Center” began investigating unspecified target websites with the goal of “preparing for operations.” A leaked internal ENP spreadsheet showed that during this time, the group was researching three to four websites per day and that at the time the spreadsheet was written around twenty sites had been reviewed and analyzed by the Studies Center.

Project Signal was also referenced in another spreadsheet showing that the project had been assigned to ENP’s “Cyber Directorate,” responsible for carrying out ENP’s offensive cyber operations. The transfer of the Signal project from the Studies Center to the Cyber Directorate demonstrated that the ransomware project had progressed from the research and planning phase to the operational phase. In the spreadsheet, the word “ransom” was listed as the goal for the Signal project and the project was slated to take place between October 18 to 21, 2020, with a listed completion date of October 21, 2020.

Figure 1: Copy of Project Signal’s Leaked Ransomware Workflow



Conclusive Proof of ENP Involvement in Project Signal Ransomware

The newly leaked documents reveal that ENP had launched a ransomware operation in late October 2020. According to Lab Dookhtegan, ENP operates on behalf of Iran's intelligence services providing cyber capabilities and support to Iran's Islamic Revolutionary Guard Corps (IRGC), the IRGC Quds Force (IRGC-QF), and Iran's Ministry of Intelligence and Security (MOIS). The documents also act as further evidence of prior Lab Dookhtegan allegations that ENP is closely affiliated with an unspecified IRGC cyber unit, both operating out of the same building and certain ENP employees holding dual positions and, in fact, primarily serving this IRGC cyber unit.

ENP's Close Ties to Iranian State and the IRGC Beyond Question

In another undated ENP document leaked by Lab Dookhtegan, details of Project Signal outlined the intricate operational processes, workflows, and best practices to successfully conducting this ransomware campaign. Based on this information, Flashpoint assesses with a high degree of confidence that ENP was involved in Project Signal ransomware operations, and was almost certainly acting on behalf of the Iranian state and the IRGC.

Learn more about **Flashpoint Threat Readiness and Response** offerings and how Flashpoint prepares and actively supports organizations to respond to any ransomware attack.

Financial Motivations: Real or More Subterfuge?

The ransomware workflow for Project Signal included steps that suggest financial gain were at least part of the group's motivations. The first indication is that the workflow includes steps for receiving Bitcoin payments from ransomware victims. Second, decryption steps were also included, with a "thumbs up" symbol placed next to the word "decryption." Based on these two factors—that ENP was likely accepting victim Bitcoin payments and following through to decrypt victim accounts upon payment—it appears that, at least on the surface, ENP's Project Signal ransomware operation was financially motivated.

On the other hand, there's an alternative, equally-plausible explanation in which the appearance of financial motivation was the group's intention for incorporating these financial payment steps with goal being to mimic the tactics, techniques, and procedures (TTPs) of other financially-motivated cybercriminal ransomware groups. Particularly in this instance, with the Project Signal ransomware operation conducted by a well-organized, Iranian state-sponsored group, the inclusion of cryptocurrency payment and decryption steps as further subterfuge techniques are arguably more conceivable than an Iranian state-sponsored group seeking relatively negligible financial returns.

Iran’s Track Record of Financial Motivation Misdirection Further Suggests Subterfuge in Play

Iran has a history of attempting to use cybercriminal TTPs to blend in with non-state-sponsored malicious cyber activity to avoid attribution and maintain plausible deniability. It’s largely assumed that Iran has been behind multiple destructive and disruptive attacks in recent years; most notably the 2012 Shamoon attacks against Saudi Aramco and the 2012 Operational Ababil DDoS attacks against US financial institutions.

Other Iranian APT groups use similar techniques to blend in with the cybercriminal threat landscape. For example, APT33 is known to use publicly available remote access trojans (RATs) like Nanocore to blend in with normal cybercriminal activity and avoid the attribution which typically comes from the implementation of custom malware.

Timing with Iranian “Pay2Key” Ransomware May Not Be Coincidence

The timing of ENP’s Project Signal also coincided with the Iranian ransomware campaign, “Pay2Key,” that began exclusively targeting Israeli companies across a broad array of verticals in December 2020. Similarly to ENP’s Project Signal, Pay2Key includes financially motivated characteristics in its operational workflow. As of April 30, 2021 at the time of publishing this blog post, Flashpoint is aware of six Israeli firms that had leaked internal documents due to Pay2Key ransomware. However, it’s been reported that Pay2Key has infected at least eighty Israeli companies with their ransomware.

As is true for ENP’s Project Signal, if Pay2Key is sponsored by Iran, it’s possible the appearance of financial motivation could have been an obfuscation technique designed to mimic a cybercriminal group. At this point in time, Flashpoint can neither confirm any attributes of Project Signal targets nor if there is any link between ENP’s Project Signal and Pay2Key.

—-

**May 2, 2021, 9:56 PM EDT: Flashpoint removed extraneous references to MuddyWater and Operation Quicksand.*

Learn More About Flashpoint Ransomware Readiness Response

Request a demo today and see firsthand how Flashpoint’s Threat Readiness and Response offerings ensure your entire team is prepped and able to respond to any ransomware attack. And when equipped with Flashpoint Intelligence Platform and our dedicated, prebuilt ransomware dashboards, you move a step ahead of ransomware attacks and the cybercriminal groups who use them.