Iran and Russia blamed for state-sponsored espionage

web.archive.org/web/20161020180305/http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/

Steve Gold

January 22, 2014

January 22, 2014

Security analyst says that a cyber warfare arms agreement is inevitable

Iran and Russia blamed for state-sponsored espionage

A U.S. research group has identified no less than five state-sponsored espionage groups, including actors from China, Iran and Russia.

According to CrowdStrike's annual analysis of security threats, these espionage groups include:

Deadeye Jackal: commonly known as the Syrian Electronic Army (SEA)

***Emissary Panda**:* a China-based actor that targets foreign embassies to collect data on government, defence, and technology sectors

***Energetic Bear**:* a Russian group that collects intelligence on the energy industry

***Magic Kitten**:* an established group of cyber attackers based in Iran, who carried on several campaigns in 2013, including a series of attacks targeting political dissidents and those supporting Iranian political opposition

***Numbered Panda**:* a group of China-based attackers, who conducted a number of spear phishing attacks in 2013

Dmitri Alperovitch, CrowdStrike's CTO, says that the report seeks to explain the motivation and intent behind cyber warfare attacks originating from China, Iran, Russia and Syria, and focuses on what's most important – namely the adversary - rather than just the exploits they create.

This is, he explained, a major step in fighting cyber security threats on a new battleground - identifying and defending against human adversaries, rather than simply trying to block malicious code.

The research firm's report says that Strategic Web Compromise (SWC) attacks have become a favourite attack vector of targeted attack groups originating from China and Russia, while the *Numbered Panda* group from China has been carrying out G20-themed spear phishing.

The Iran-based actor known as *Magic Kitten*, meanwhile, was spotted targeting pro-democratic activists as a precursor to the May 2013 Iranian elections, whilst the Russian *Energetic Bear* group was very active against Western energy sector targets.

Emissary Panda, which CrowdStrike defines as a Chinese nexus intrusion group, has been targeting foreign embassies to deliver malware in a SWC campaign.

The report highlights the Russians as being involved in the same type of state-sponsored attacks identified by Mandiant in its 2013 report on Chinese state-sponsored attack vectors.

"A recent investigation into the activity of a Russian-speaking adversary identified an actor whose services may have been acquired for specific operations on behalf of a nation-state customer," reads the analysis.

"This adversary has been involved in targeted activity for nearly a decade, but malware analysis showed significant similarities to known cybercrime activity utilising Sheldor and ZeuS malware."

"The combination of criminal and targeted activity suggests an adversary that conducts malicious activity on its own accord, possibly as part of a continuing criminal enterprise, and also at the direction of a government entity," it adds.

The report adds that the motivations of private entities that conduct operations in support of a nation-state may vary, but in certain circumstances, "it may be that a government will turn a blind eye to criminal activity if an actor will use its skills to further the state's interests."

In other attacks, CrowdStrike says that it may well be that the private entity is a company that sells its expertise and resources to its government, or to the governments of other countries.

"Another motivation could be more nationalistic - possibly like the case of *Deadeye Jackal*, where a private group lends its services to the state out of a feeling of patriotism," the report concludes.

Commenting on the analysis of the state-sponsored attacks, leading analyst Sarb Sembhi, a Director of Consulting with Incoming Thought, told *SCMagazineUK.com* that there are some assumptions that have to be made about state-level attacks, and one of these is that the attacks are very real and have been taking place for many years.

"If you look at the G20 nations, my observations suggest that if any of these countries are not involved in cyber warfare, then I would be very surprised," he said, adding that, whilst we have yet to reach the stage where a single piece of malware has same damage potential as a nuclear bomb, it is only a matter of time before that breakthrough is made.

At that point, says Sembhi - who is a leading light at ISACA, the not-for-profit IT security association - there will have to be a multi-country agreement on the control of cyber warfare, just as there has been with nuclear weapons.

"Nation states will have to agree on a set of rules in which they work out what can and cannot be done with state-sponsored malware and its like," he said.