UNCLASSIFIED



Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

August 15th, 2014

This document was prepared by The Institute for National Security Studies (INSS) – Israel and The Cyber Security Forum Initiative (CSFI) – USA to create better cyber situational awareness (Cyber SA) of the nature and scope of threats and hazards to national security worldwide in the domains of cyberspace and open source intelligence. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities, and follow-on measures. This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted. These materials, including copyrighted materials, are intended for "fair use" as permitted under Title 17, Section 107 of the United States Code ("The Copyright Law"). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner. Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: dcoi@inss.org.il.

CSFI and the INSS would like to thank the Cyber Intelligence Analysts who worked on collecting and summarizing this report.

ISRAEL

US warns of consequences against cyber-attacks towards Israel

In an interview on CBS News, the United State House Intelligence Committee Chairman Mike Rogers disclosed that some states are behind the DDoS cyber-attacks targeted towards Israel. Rogers warned this could lead to further destabilization in the region and added, "What consequences that might have are still not known." In correlation to Rogers' response, an article published in Forbes by INSS researchers claimed the attacks not only came from state sponsored groups like Syrian Electronic Army (SEA) but also possibly from terror groups who have infiltrated hacktivist groups like Anonymous. While this time the attacks caused minimal damage on the cyber realm, they had significant effect on the actual battlefield. As Colonel N., Head of the IDF cyber defense unit, revealed since the beginning of Operation Protective Edge, there are more and more attempts to hack and disrupt the IDF system. "The ability of the IDF to work effectively and shortly on the battlefield depends on advanced technology… We want that the technological capabilities will be the base for success, and this is why we block any attempt to hurt those capabilities, which are necessary factor in IDF effectiveness in the battlefield."

Cyber-attacks against Israel up by 500% due to Iran-linked botnet

Arbor Network's ASERT team published an in-depth report depicting an increase in distributed denial of service (DDoS) attacks against Israel, which went from an average of 30 attacks per day in June to 150 attacks per day in July - a 500% increase. The attacks also lasted longer in July with an average duration of 1 hour and 40 minutes, compared to just 20 minutes in June.

USA

Former Anonymous member once more behind foreign cyber attacks

Former Anonymous member and eventual double agent, Hector Xavier Monsegur aka Sabu, was part of cyber-attacks on the Turkish government by using his own cyber group and Turkish hacktivists, RedHack. Sabu instructed via FBI orders that all Turkish websites would be through RedHack. Court documents show all documents stolen during this campaign were filed with the FBI, including confidential emails, databases, and login credentials. This is not the first time Sabu has been behind cyber-attacks against foreign countries; he was previously linked to cyber-attacks against Iran, Syria, and Pakistan leading many to speculate he was gaining intelligence.

US contractor target of computer breach

The largest US contractor in background checks and security clearances, USIS, has been the victim of phishing attempts on an unmarked number of employees. The company declared the attack "has all the markings of a state-sponsored attack." The FBI launched an investigation into the attack as some DHS personal information was affected. Additionally, the US Computer Emergency Readiness Team (US-CERT) has begun conducting an investigation, which will include forensic analysis. The US Congress also voiced their disapproval of the breach, as USIS was recently granted $190 million for DHS's immigration system and has been facing a lawsuit against a whistleblower. USIS is the same contractor who provided security clearances for Edward Snowden and the Navy Yard shooter.

RUSSIA

The biggest Russian cyber crime

A Russian criminal ring amassed the largest known collection of stolen Internet credentials, Hold Security, a security firm from Wisconsin, confirmed. Stolen information included 1.2 billion username and password combinations, and more than 500 million email addresses were exposed. The offense includes confidential material gathered from 420,000 websites, including household names and small Internet sites. “Hackers did not just target US companies, they targeted any website they could get, ranging from Fortune 500 companies to very small websites,” said Alex Holden, the founder and chief information security officer of Hold Security. Websites inside Russia had also been hacked, and Mr. Holden said he saw no connection between the hackers and the Russian government.

ARAB COUNTRIES

Hamas’ cyber hacks linked to psychological warfare

Hamas has invested in hacking different Israeli websites during its current operations. Domino’s Pizza Israel's Facebook page had been hacked with different posts mentioning that Hamas’ would unleash thousands of rockets together, directed at Israel. In addition, they managed to send mass text messages to Israeli cell phones, claiming to be from the Israel Security Agency reporting on bogus attacks and injuries happening within Israel. Noit stopping there, Hamas has attempted hacking Twitter and satellite broadcasts by surging the psychological warfare. Most of the attacks have attempted to slow down Internet providers in Israel or involve phishing.

Iraqi conflict breeds cyber-war between factions

As part of the current conflict happening in Iraq, differing sides began using hackers in order to gather intelligence as well as using social media to gain supporters. The different parties are local groups using malware for targeted intelligence on each other. One malware program, called Njrat, was used to create networks of machines they could control remotely. Once machines were infected with the Njrat malware, attackers began stealing files or using a computer's camera or microphone to monitor what was going on surrounding it.

CHINA and APAC

Taiwan accuses China of launching cyber-attacks

Taiwan has accused China of launching frequent cyber-attacks against the state. Taiwan’s Science and Technology Minister, Simon Chang, stated: “The Chinese cyberwar units have been engaging with Taiwan units almost every day… Many of the attacks were aimed at stealing relevant information for use in negotiations with Taiwan.” Even though Taiwan has their own cyber units within the military, Chang insisted it was no match for Chinese numbers or technological capabilities.

Sri Lanka and Thailand holding Cyber Security Conferences 2014

The second annual EC-Council Cyber Security Summit was held at Cinnamon Lakeside, Sri-Lanka. Cyber Security Summit 2014 was co-organized by CICRA Consultancies Ltd and the Daily FT. IT professionals and senior officials from the corporate and government sectors participated on the Cyber Security Summit. On the side, Thailand

organized the Cyber Defense Initiative Conference (CDIC) 2014; the conference was organized to encourage cooperation between government agencies, private sector, and international agencies. They held training sessions on how to increase computers' data security and how to protect it. CDIC 2014 was organized under the heading "The Next Generation of Cybersecurity Intelligence: Protecting our nation against cyber threats." In terms of cyber defense, Sri Lanka and Thailand are not the most powerful countries in the region; however, they have begun developing their cyber security industry to face several cyber-attacks but need serious development to reach the level of China, South Korea, and Japan.

EUROPE

France in middle of vast cyber espionage operation

According to a report by Kaspersky Lab, France is at the center of cyber espionage with Epic Turla, which was launched in 2012 and continued into July 2014. The campaign infected hundreds of computers in several government institutions, including the Ministries of Interior, Commerce, Foreign Affairs, Defense, Education, Secret Services, and Embassies from 45 countries. At the beginning, the cyber espionage operation exploited two zero-day vulnerabilities, including Escalation of Privileges in Windows XP and Windows Server 2003 and an exploit in Adobe Reader. The report also explains that social engineering techniques have been used along with waterhole strategies, allowing the attacker to infect a frequently visited site. Information discovered during the investigation into Epic Turla revealed the origin of the attack, showing they were compiled on a system using Russian language. Russia, alongside China, has become more and more active in cyber espionage. Despite the creation of a cyber-defense, reserve, and the development of its national cyber security policy, France must pay more attention to malware and social engineering activities running on its national computer systems and networks. The campaign was not only targeted to France, but the virus was also identified in the United States, Iran, and Russia.

Vodafone gained cyber security accreditation by the UK government

The UK Vodafone telecom company has become the first national telecom company awarded a cyber-security accreditation by the UK government. Indeed the company received the Cyber Plus Essential Accreditation. According to the UK government, the Vodafone internal IT system scored 100% when auditors tested it. The company declared: "We want our customers to be assured that when they do business with us we are doing everything possible to protect their data, our critical system and business operations." This accreditation arrived only a few months after Vodafone explained that phone conversations are no longer private and secure because of governmental agencies often listening into phone calls by requesting direct connections with network equipment. In fact, it is paradoxical that on one side, the government delivers cyber security accreditation to prove the security quality offered by telecom operators and on the other side, they have full access to any phone calls and violate user privacy.

Schoolchildren to be trained in cyber warfare

A new cyber security program, "Cyber-Centurion" targets to UK teens, is offering the children an opportunity to challenge themselves and increase their cyber skills. The participants are given an effected computer image, and within a certain time limit, they need to restore the image from the bugs and malfunctions. The program is adapted from the US Air Force, "Cyber Patriot" program, which includes 1,500 international teams from the East Asian hemisphere. The purpose of the "Cyber-Centurion" program is to enable children with a passion in the cyber field, as well as provide them an in depth look into the cyber world and enhance UK's cyber security.

UK Campaign raises cyber-attack awareness

Britain's National Crime Agency began a new project in the effort to secure private computers and their users in the UK. Accordingly, more than 40% of adults in the UK have not installed security updates or security programs. The result is an unsecured cyber space surrounding the British public. Officials claim every computer not properly secured is a potential cause for danger to the user and his surroundings. The program calls upon the public to be "cyber streetwise," and too understand the threats in order to take the necessary steps to protect their personal identity.