UNCLASSIFIED



Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

September 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

Israeli cyber security: a growing market

Two new reports, one from "Themarker" and "The Time" and a second from "Pitchbook Data," had marked a big win for Israeli cyber. The first shows the Israeli cyber industry had doubled itself in the last three years. The second shows that about 90 Israeli companies are due to make 10 million dollars or more in 2014, fifteen of them with expected revenue of more than 100 million dollars.

The Israeli start-up Cybertinel uncovers extensive computer espionage network hitting over 300 sensitive organizations in Germany, Austria, and Switzerland

The Israeli cyber security firm Cybertinel, which focuses on protecting networks against APT and zero-day attacks, had uncovered a 14 year long cyber espionage campaign. The hackers, which were identified as Germans, had used a Trojan horse to penetrate more than 300 companies in Germany, Austria, and Switzerland. After the hackers accessed the target networks, they transferred data to an external domain. The "security platform automatically uncovers sophisticated cyber-attacks and provides immediate countermeasures," as stated on the Cybertinel site.

The hacktivist Anonghost group attacked Israel under banner of #OpIsraelReborn campaign

On the twelfth of September, the pro-Palestinian hacktivist group Anonghost launched a cyber-attack against Israel as part of its #OpIsraelReborn campaign. The group hacked and defaced the official website of Israel – Russia – Ukraine & CIS Chambers of Commerce and Industry. The Israeli website was defaced with a song and a message in support of Palestine. Anonghost routinely attacks Israeli websites, especially the government. The group is well-known for its website defacement speciality in order to broadcast their messages against the state of Israel and in support to Palestinian people.

USA

US Army Cyber Command launching new Cyber Protection Brigade

On the fifth of September at Fort Gordon in Georgia, the US Army launched its new Cyber Protection Brigade, which is going to be led by Col. Donald Bray. The Lt. Gen. Edward Cardon, commanding general of the US Army Cyber Command recently declared, "This new Army brigade represents a deeper Army investment in its cyberspace capabilities." The Cyber Protection Brigade will be divided in Cyber Protection Teams, including a mix of soldiers and civilians. The brigade will include 20 of these teams, each one with about 39 people. According to information released from the US Cyber Command, the teams will conduct defensive cyberspace operations in support of joint and Army missions. Moreover, these new teams will be trained to a common joint standard. It was the biggest change in the US Cyber Command since Michael Rogers was appointed head of the US Cyber Command and the NSA.

RUSSIA

Russian hackers hacked nearly 5 million Gmail user accounts

Along with 4.93 million Gmail accounts, more than 1 million Russian account credentials of Yandex and Mail.Ru were leaked. Neither Google, Yandex, nor Mail.Ru services have made any statements yet, but all three recourses immediately recommended its users to change their passwords and use the two-step verification system for their accounts. It seems that 60% of the accounts were active during the attack. At the moment, there is no further information about the technique employed or the motivation of the attack.

CHINA AND APAC

China performs large scale cyber espionage operations

The security company FireEeye has recently highlighted the industrial scale of China's cyber espionage. The investigation conducted by the American company revealed that two spying groups that use the same hacking tools and techniques despite the fact that they are miles away from each other and having different targets. The company explained that the first group is the Guangdong Province-based Moafee attack group, which targets the US and other countries' governments' defense industry and military organisations. The second is the Jiangsu Province-based DragonOK, which targets Asian high-tech and manufacturing companies. According to a report made by the company, both groups are using several overlapping tools, techniques, procedures, backdoors, and remote administration tools to infiltrate and stay on the targeted networks. FireEye added that "they deploy several methods to hide their activities, including checking for the number of core processors attaching password-protected documents and providing a password in the email contents; and sending large files padded with unnecessary null bites to evade network and host-based AV engines that can't scan larger files."

EUROPE

NATO strengthen its cyber security policy and cooperation

On the fifth of September. NATO members from 60 countries met at the International NATO summit in Wales to discuss the strengthening of NATO cyber security policy and cooperation. According to the Times, officials from NATO's cyber-defence unit have been meeting with the UK electronic spying agency GCHQ and other agencies since July to share intelligence and prepare for this summit. NATO's members agreed on strengthening the international cyber-security policy and the international cooperation between nations by updating the 2011 cyber-security policy. In this new version, NATO's leaders are expected to recognise that there is no distinction between physical attacks and cyber-attacks against the organisation. Indeed according to the NATO article, 5 member states will have to help any other member state targeted by an armed attack, including a cyber-attack, in the new NATO cyber-defence policy. According to Jamie Shea, NATO deputy assistant secretary general for emerging security challenges, "The new cyber-policy has already been endorsed by NATO's 28 member countries, and I have no doubt the heads of state and government will do the same." However, not all aspects of this new cyber-security policy have been unveiled

for security reasons. This new policy recognises that certain cyber-attacks could potentially have the same level of disruption as conventional warfare. This new cyber security policy highlights the fact that today's cyber-weapons developed by states or cyber terrorist groups will be officially considered as weapons of war, just as traditional weapons.

UK government launching free online cyber security course

The UK Government decided to offer a free online cyber security course. According to the government, this initiative is aiming to provide IT knowledge to everyone in order to train new specialists, improve the skills of current cyber security experts, and make "vibrant, resilient, and more secure cyberspace." The government is collaborating with the Massive Open Online Course (MOOC), and the content of the course has been developed by the Open University including network security, cryptography, malware, threat landscape, and ways to reduce cyber risks. The course will be available on FutureLearn.com. This website usually hosts free online courses for UK and overseas universities. According to the government, the course would be available 4 times a year over the next 36 months. After the civil cyber security competition launched by the UK Ministry of Defense last month to protect their systems, the UK is now showing its strong desire to strengthen its national cyber security by involving its people and make cyber defense a national issue. UK seems to adopt a strategy that aims to make every citizen aware of the importance of a good cyber security to protect the nation.

AFRICA

Tanzania: Cyber-crime talks for Arusha

Cyber Defence EastAfrica 2014 conference with a theme "Fight Against Financial and Data Privacy Crime in East Africa" is being held nowadays in Arusha (September 16-19). During the sessions, it was revealed that Tanzania have so far lost nearly $10 billion through cyber related fraud crimes, involving mostly card skimming and ATM pumping electronic thefts. Other issues to be discussed or presented in the Arusha conference would be the current cybercrime situation, challenges, opportunities, the way forward, the status of cyber laws in Tanzania and East Africa, computer security incidents, navigating through cyber security landscape, legal aspects of digital forensics, industrial espionage, and the 20 critical security controls governance issues.

Cybercrime a key issue in new ISS - UNIDIR collaboration

The Institute for Security Studies (ISS) and the United Nations Institute for Disarmament Research (UNIDIR) will be collaborating to tackle emerging threats in Africa, including cybercrime and cybersecurity. The initiative comes at a time when the threat of cybercrime in Africa, particularly via mobile and web-based technology, is on the rise.