CENAA

NEWSLETTER 9-11 2015

CENAA

Anonymous and ISIS

Source: Wikimedia

ISIS hacker who passed U.S. military data to terrorists was arrested in Malaysia. It is a Kosovo citizen and he have handed the hacked information over to Junaid Hussain who was killed in a US drone strike.

ISIS affiliates and supporters started #AmericaUnderHacks campaign to‘celebrate‘ 9/11 terrorist attacks. It looks like that the hashtag have been overtaken by users trolling ISIS. ISIS is also running service to assist jihadists to use encrypted communications and other things. NBCreports defined it as a 24-hour ISIS Help Desk. It should help its soldiers spread its message worldwide, launch more attacks on foreign soil and recruit followers. Combating Terrorism Center at West Poin’s military academy uncovered an ISIS security manul and other related documents from ISIS forums, social accounts and chat rooms. The original guide was written by a Kuwaiti security firm Cyberkov.

After the Paris attakcs in November, Anonymous has declared total war against the Islamic State. They announced the beginning of #OpParis campaign to hunt down ISIS’s social media channels and online supporters. The Indian hackers have joined Anonymous in the cyber war against ISIS. They are helping identifying ISIS websites, Twitter and Facebook accounts. Users around the world have united to troll ISIS fighters as rubber ducks. Anonymous has employed a similar trick of trolling ISIS.

Anonymous delivered its promise and has taken down the main messaging forum used by ISIS. They want to make it difficult for the group to communicate between them. Anonymous had also taken down over 20,000 Twitter accounts linked to the militant group. On the other hand Twitter says that Anonymous‘ list of alleged ISIS accounts is higly inaccurate and that many of the “taken down“ accounts do not belong to ISIS. The attacks on ISIS come even from Anonymous affiliated team called GhostSec, which takes down hidden ISIS website on dark web and replaces it with an advert of Viagra. The most recent claims diclosed that the GhostSec caught and interrupted messages sent between the ISIS group members, and then forwarded those messages to the international law enforcement agency. The analysis reveals that the jihadists of Islamic State are choosing to transfer their web properties to US-hosted websites to protect their operations against hacking attempts because U.S. laws prohibits hacking.

Anonymous was also able to trace the location of ISIS hack group called CyberCaliphate and found that they are operating from a single IP address in Kuwait. They said that CyberCaliphate fakes most of its hack attacks and release publicly available information claimed to be stolen or they take credit for hack attacks done by other groups.

ISIS responded to Anonymous declaration of “total war“ by calling the hacker group “idiots“ and offering guidance to its online followers to prevent cyberattacks. For example, they warned followers to avoid talking on Telegram and to change Internet protocol addresses continually. Telegram have already shut down 78 ISIS channels. This popular end-to-end encrypted messaging app has been used by ISIS since October, when Telegram introduced Secret Chat feature and after the Anonymous declared war against ISIS.

Hacker group named Islamic state cyber Army have warned Iran to stop war on the Islamic State otherwise they will publish sensitive and classified inforamtion of Iranian Government. This group has also unveiled a list of US military and security officials. It is not the first time they published such list. The claim that it is a response to Anonymous attacks on twitter accounts and forum of ISIS members.

The US government has started arresting people who are showing support for ISIS on social media. This has raised questions on freedom of expression and the First Amendment in the US.

The ISIS is trying to hack US electrical power companies but they are terrible at it. UK is facing similar threats. According to UK Chancellor Osborne, ISIS terrorists are trying to launch deadly cyber-attacks on the country’s important national infrastructure. On one hand ISIS has had very limited success to date but on the other hand they managed to hacke top british ministers in sophisticated espionage operation. This claim comes from british GCHQ.

Vulnerabilities

Source: Computing

Researchers at iTrust at the Singapore Universtity developed a project to demonstrate how hackers can gain access to corporate network by using a smartphone-equipped drone to hack your printer.

FBI infected seized servers, that were used to host abusive content, with spyware. They exploited the vulnerability in Tor by using a Flash plugin to reveal the identity.

Even the antivirus is not secure. Security researchers discovered Zero-day vulnerabilities in Kaspersky and FireEye.

Hacking tools itself have become relatively easy to use, and you don‘t need to be a pro-level hacker. A company named Gleg collects, resells and researches SCADA zero-days. The exploit cost $8,100 and you need a Canvas license, which has a price of $3,000 for 10 users. The research is not focused to control SCADA systems, but to write exploits for vulnerabilities for the Canvas framework. They sell the sool only privately and not to governments. According to a new report published by the Chatham House, civil nuclear facilities worldwide are targets for cyber attacks, and the nuclear industry is falling behind other industries when facing cyber security.

The director of one of Europe's top aviation agencies warned that hackers could infiltrate critical systems in an airplane on the ground. It took the expert five minutes to crack Aircraft Communications Addressing and Reporting System and a couple of days to access the aircraft control system on the ground. The pilots could receive a false messages that could affect their decision making.

US military forces

DARPA wants to protect critical infrastructure from cyber attacks. They launched a new program called Rapid Attack Detection, Isolation and Characterization, and want to make develop innovative technologies that can quickly detect and respond to cyber attacks on critical infrastructures in the US, and especially those vital to the Department of Defense's missions.

US Navy is developing cyber protection system, named RHIMES, to enhance cyber security and to protect the Naval's shipboard electrical and mechanical control systems from cyber attacks. Because of fears of hacking, the US Naval Academy has returned to using celestial navigation for all new recruits, and teaching them the use sextants.

Upcoming U.S. Cyber Command project for $460 million will outsource to industry all command mission support activities, including "cyber joint munitions" assessments and "cyber fires" planning. Computer code capable of killing adversaries is expected to be developed and deployed if necessary. U.S. Congress also ordered U.S. Cyber Command to carry out simulated "war games" against Russia, along with Iran, China and North Korea.

Source: Wikimedia

Russian computer programmers were helping to write computer software for sensitive U.S. military communications systems by a long time Army contractor. The Army contractor said the software they wrote had made it possible to infect the Pentagon's systems with viruses.

Trend Micro has uncovered a cyber espionage campaign called the Operation Iron Tiger. Chinese hackers carried it out on U.S. Defense Contractors.

U.S. Air Force has unveiled its special aircraft named EC-130H Compass Call that is capable to hack targeted enemy networks wirelessly and directly from the aircraft. It uses noise-jamming feature. It can jam enemy's communication networks and perform cyber attacks on the ground-based military networks.

US politics

Some of the world's largest tech firms have come together to issue a public protest against controversial US cybersecurity bill (CISA). Critics say it does not adequately protect users' privacy. The tech firms approved the goal of the legislation, but could not support it in its current form. Even the Department of Homeland Security doesn't want the power it would get under CISA. They argued for example that the bill could sweep away important privacy protections. Despite that Senate passed CISA with privacy flaws unfixed.

Source: Wired

According to America's intelligence chiefs the next attack they worry them involve direct manipulation of data, changing perceptions of what is real and what is not. Big cyber attacks that have been disclosed so far in 2015 involved the theft of data.

Another problem is direct attacks on critical infrastructure. In Greater San Francisco unknown suspects cut backbone fiber optic Internet cables. This appears to be the fourteenth attack on the critical communications infrastructure.

James Clapper, director of national intelligence, is skeptical about US-China cyber deal and that Chinese cyber attacks will diminish. As we write in the China section below, Clapper appears to be right, because the report says that the attacks continues even after the deal has been signed.

The CIA pulled officers from Beijing after major hacks into Office of Personnel Management. The theft can be characterized as political espionage. The Chinese could have compared those records with the list of embassy personnel and who was not on the list could be a CIA officer.

Hillary Clinton says that the US needs the help of Silicon Valley to defeat ISIS. Stopping the spread of ISIS online is one critical step toward defeating them on the ground.

CENAA

NEWSLETTER 9-11 2015

CENAA

US Regulator declared Bitcoin a commodity. U.S. Commodity Future Trading Commission has added Bitcoins and other virtual currencies to the commodity basket.

According to a review of federal records obtained by USA TODAY, U.S. Department of Energy computer systems have been successfully compromised more than 150 times between 2010 and 2014. Over a 48-month period ending in October 2014, a total of 1,131 cyberattacks have been reported.

European region

Source: Wikimedia

After the U.S. it's the UK that has signed with China a truce on industrial hacking and cyber theft. It is a similar deal. Another country is Germany. Together with China they are working to create an agreement that would eliminate economic cyber attacks between them. Germany's interest may be primarily focused on addressing the issue of brand piracy from Chinese factories.

UK will also boost its cyber security defences, including a new £165 million Defence and Cyber Innovation Fund, which is similar in its intent to DARPA. It will provide funding to startups who are creating cutting-edge technology, but it is dwarfed in its scope by DARPA. UK is raising spending on special forces, cybersecurity and intelligence agencies. Announcements were made in response to the Islamic State attack in Paris. Chancellor Osborne said that Britain would spend £1.9 billion up to 2020 countering cyber attacks as well as developing an offensive capability to counter criminals, rogue states, terrorists and others. The government's total cyber spending will be more than £3.2 billion. Osborne also announced creation of a National Cyber Center. But he said that the decision to ramp up cyber defence funding had been taken before bloodshed in Paris and that intelligence agencies are building elite cyber offensive forces, which will be run jointly between GCHQ and the Defence Ministry and will target criminal gangs, militant groups, individual hackers and hostile powers, using a "full spectrum" of actions. The National Crime Agency and GCHQ have also formed a new unit called Joint Operations Cell. It will monitor child pornography on the dark web, but primarily it should increase ability to identify and stop serious criminals.

MI5 has been secretly collecting UK phone data for over 10 years, and the revelation came after Theresa May outlined a new bill regulating online surveillance by authorities. According to BBC report MI5 recorded just the fact contact was made. According to Nick Clegg only 'tiny handful' of ministers knew of mass surveillance.

UK government has announced a new Draft Investigatory Powers Bill. It should ban companies such as Apple from offering end-to-end encryption. On the other hand the government itself recognises the benefit of strong encryption for its own purposes.

Recently the former British defence secretary Des Browne warned that the Trident nuclear weapons system could be vulnerable to cyber-attack. He is seeking assurance from Prime Minister that they will be secured from hostile persistent threat actors, such as China and Russia.

UK police has arrested fourth hacker responsible for hack of British telecoms giant TalkTalk. The attack may have taken place due to SQL injection attack and revealed personal information of 4 Million customers. Vodafone has been also hacked by the cyber criminals, which view nearly 2000 customer accounts. This information might be used in future attacks. High-profile data breaches took place against T-Mobile, Patreon and Scottrade. For example in T-Mobile's case, attack potentially exposed details of 15 Million people, including data about military I.D., home addresses etc.

The European Court of Justice has ruled against the transatlantic Safe Harbor agreement. Large tech firms are likely to feel the impact of the decision immediately, because they must abide data privacy regulations in each of the member states. The only other option is the creation of data centers based within Europe, so that the date would stay in Europe. Microsoft will host data in Germany, but the reason is to evade US spying and has anything to do with Safe Harbor agreement. Access to data will be controlled by a T-Systems, a subsidiary of Deutsche Telekom. German parliament on the other hand has approved data retention. The new law is requiring telecommunications operators and ISPs to share customer data with the police. This is despite the two previous laws having been ruled unconstitutional. Following revelations of electronic mass surveillance, the European Parliament says that EU citizens' rights are still in danger. The members decided to call on EU member states to drop any criminal charges against Edward Snowden, grant him protection etc.

The European Union plans to ban bitcoin and any form of anonymous payment online to curb terrorism funding. This is a completely different approach then the one we see in US, which made bitcoin a legal commodity.

The Germany's foreign intelligence agency BND is expanding its Internet surveillance capabilities. Netzpolitik published its secret 300 million Euro investment program "Strategische Initiative Technik". Civil society and members of Parliament criticise the agency's new powers and demand an end to the program.

Ukraine establishes cyber policy. The Ukrainian Minister of the Interior Avakov announced to set up a new department for the prevention and prosecution of cybercrime. It is done as a part of a larger police reform.

NATO

Tunisia and NATO is planning to boost the cooperation in security and defence, and one of the included priorities is cyber defence. NATO is also bolstering its cyber defence cooperation with Czech Republic. It is the first Ally to sign a new Memorandum of Understanding on cyber defence cooperation.

NATO plans to grow its cyber partnership with industry, and they wont to build on the growing alignment of cyber defence between its 28 nations and the alliance.

At NATO's next summit in Warsaw 2016, cyber security will be a major topic. It faces a struggle on collective cyber-defence doctrines, because there are for example collective differences in the definition of a serious cyber attack.

Source: DefenceTalk

Estonia hosted the largest annual cyber defence exercise "Cyber Coalition 2015" with around 600 cyber defenders. It was a 5-day training event in which Allies and partners defended their networks from a series of complex security challenges.

Belgium has joined the NATO Cooperative Cyber Defence Centre of Excellence as a Sponsoring Nation. Currently 17 nations (with Belgium) have signed on as Sponsoring Nation.

On the other hand, Sweden seeks to join NATO's Strategic Communications Centre of Excellence, which leads development of cyber defence, counter information warfare and counter-disinformation strategies and was opened in Riga in January 2015. Other NATO members in the Nordic-Baltic region are also showing an interest in joining StratCom.

China

Source: Reuters

In September US and China reached historic agreement on economic espionage, where they agreed not to conduct or support cyber espionage and intellectual property theft, including trade secrets or other confidential business information for the purposes of commercial gain. But a report from October showed that China is still hacking US companies. Latest Snowden documents also revealed that Chinese were behind F-35 hack, as was expected before.

A joint report published by ThreatConnect and Defense Group Inc., connects PLA unit 78020, a state sponsored hacking team that intelligence to advance China's interests in the South China Sea, to the Naikon advanced persistent threat group. According to FireEye hackers have made the region of Southeast Asia one of the most targeted in the world amid heightened regional tensions (disputes over territorial waters).

On the international level, Wang Qun, director-general of the Arms Control Department of the Chinese Foreign Ministry, said that it is necessary to bring about an international code of conduct on cyberspace. During the first December should start high-level cyber crime talks between US and China with potentially establishing acceptable norms for cyber espionage.

Russia

Russia's Internet regulator has recently said that Twitter must store local user's data in the country. A new Federal Law No. 242-FZ came into force in September, and it requires all foreign businesses that handle the personal data of Russian citizens to keep them on servers located in Russia. Most Russian language websites are hosted offshore and it will send shockwaves through global markets. There are no big data players native to Russia. But Russia's Rosenergoatom recently started the construction of a massive data center and will be powered by existing nuclear power station. They previously approached Google and Facebook to offer space on the upcoming campus, in order to comply with the new law.

A Russian-speaking spy gang known as Turla was hijacking the satellite IP addresses of legitimate users and was using them to steal data from other infected machines and hides their command server. Kaspersky Lab has found evidence that the group have been using the technique since at least 2007.

U.S. is worried about Russian submarines and spy ships, which are aggressively operating near vital undersea cables. Among some American military and intelligence officials it raises concerns that the Russians might be planning to attack those lines in times of tension or conflict. Pentagon planners worries most that Russia appear to be looking for vulnerabilities at much greater depths, where the breaks are hard to find and repair, and they cannot monitor the cables.

Russian hacking team "Operation Pawn Storm" attempted to hack Dutch Safety Boards servers to find information about MH17 report, but the attacks have not been successful according to the Dutch Safety Board. The report from F-Secure details "The Duke" malware family and its connections to Russia. Seven years a cyber-espionage group has been operating out of Russia and behest of the Russian government. It targeted think tanks, governments, and other organizations.

But the Russian military is also under attacks. Their members have been receiving well-crafted phishing emails. Attackers use Chinese-language tools and Chinese command-and-control installations. It can be China, but someone can be trying to cast the blame on them.

Source: HackRead

After the Turkish air force planes took down a Russian fighter jet near the Syrian border, the Turkish hacktivist group took down the official website of Russian Central Bank.

Rest of the World

Source: SC Magazine

The G20 countries agree that hacking industrial targets for profit isn't right. They agreed to abstain from hacking for commercial gain. It is not a legally binding agreement, but it gives justification if the countries want to react to future acts.

Japan's NEC Corporation will boost Indonesian cyber security by developing its capabilities. It will design a "security operation center". Next country from the area is Thailand. Royal Thai Armed Forces plans to establish a cyber warfare unit and becoming the latest military in Southeast Asia with intention to invest in digital network security. The unit will represent all three armed forces

Australia's new data retention law comes into effect, and from now telecommunications companies will keep large amounts of metadata for two years. It was implemented against organized terrorist and criminals. They will collect data about: whom you called, missed numbers, duration of calls, device date and more. Australia has been also a target of cyber spying. According to The Australian, Chinese and Russian hackers attempted to steal top secret futuristic submarine plans being built for Australian Navy. Hackings have been aimed at the submarine builders in Japan, France and Germany, which are bidding for $20 billion contract.

After exploit in car vulnerabilities, the Canadian military, the Department of National Defence and government is searching for a contractor who can find vulnerabilities in their vehicle, and exploit them in order to gain access to the vehicle.

Egypt's military arrested 150 terrorists through "Telegram" after monitoring the coordination processes between them in Telegram chat site. Terrorist group Ansar Beit al-Maqdis announced this and warned all his followers not to enter on the application again.

Iranian Government has blocked Telegram messaging services. According founder of Telegram Iranian ministry of ICT demanded that Telegram provided them with spying and censorship tools, but Telegram will not help them. Dell released an analysis of tracking a suspected Iran-based threat group (Threat Grop-2889) and uncovered a network of fake LinkedIn profiles. They assess that the purpose of this group is to target potential victims through social engineering. European authorities have taken down a cyber espionage campaign they believed to be linked to Iran's Revolutionary Guard. It was a coordinated action. Researchers from U.S.-Israeli security firm Check Point Software have discovered the inner workings of this cyber espionage campaign and had informed national computer security response teams in Germany, Britain and the Netherlands. They released a report, which details how they burrowed inside the hacker group's database. Finally, the new Facebook's alert system has helped the US State Department officials that they were tipped off about an Iranian hacking campaign.