THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

13 November 2014

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

Stuxnet worm entered Iran's nuclear facilities through hacked suppliers

Engadget, 13 Nov 2014: You may have heard the common story of how Stuxnet spread: the United States and Israel reportedly developed the worm in the mid-2000s to mess with Iran's nuclear program by damaging equipment, and first unleashed it on Iran's Natanz nuclear facility through infected USB drives. It got out of control, however, and escaped into the wild (that is, the internet) sometime later. Relatively straightforward, right? Well, you'll have to toss that version of events aside -- a new book, Countdown to Zero Day, explains that this digital assault played out very differently. Researchers now know that the sabotage-oriented code first attacked five component vendors that are key to Iran's nuclear program, including one that makes the centrifuges Stuxnet was targeting. These companies were unwitting Trojan horses, security firm Kaspersky Lab says. Once the malware hit their systems, it was just a matter of time before someone brought compromised data into the Natanz plant (where there's no direct internet access) and sparked chaos. As you might suspect, there's also evidence that these first breaches didn't originate from USB drives. Researchers saw that Stuxnet's creators compiled the first known worm mere hours before it reached one of the affected companies; unless there was someone on the ground waiting to sneak a drive inside one of these firms, that code reached the internet before it hit Natanz. To read more click **HERE**

November 11, KWWL 7 Waterloo – (Iowa) **Parking data breach at Eastern Iowa Airport.** The Eastern Iowa Airport in Cedar Rapids revealed November 11 a data breach that may have compromised the information of an unknown amount of customers who used credit or debit cards at the airport's public parking facilities between September 29 and October 29, after discovering that a server was being mined for data. Authorities isolated the server and continue to investigate the extent of the incident. Source: http://www.kwwl.com/story/27359520/2014/11/11/parking-data-breach-at-the-eastern-iowa-airport

November 10, KTLA 5 Los Angeles – (California) **55 laptops stolen from library on UCLA campus; police ask for help finding burglar.** The University of California Police Department is searching for a suspect who stole 55 laptops worth $33,000 from the Charles E. Young Research Library on the University of California, Los Angeles campus November 8. Source: http://ktla.com/2014/11/10/55-laptops-stolen-from-library-on-ucla-campus-police-ask-for-help-finding-burglar/

November 12, Softpedia – (International) **18-year-old remotely exploitable vulnerability in Windows patched by Microsoft.** Microsoft released a patch November 11 for a data manipulation vulnerability that has existed in Windows operating systems starting with Windows 95. Researchers with IBM's X-Force discovered and reported the vulnerability in May, which could have been used by attackers to gain control of affected systems for the last 18 years. Source: http://news.softpedia.com/news/18-year-Old-Remotely-Expoitable-Vulnerabililty-in-Windows-Patched-By-Microsoft-464769.shtml

November 12, Help Net Security – (International) **Microsoft patches Windows, IE, Word, SharePoint and IIS.** Microsoft released its monthly Patch Tuesday round of updates for its products, which includes 14 bulletins including one patching a zero-day vulnerability in the Windows OLE packager for Windows Vista and newer Windows operating systems. Source: http://www.net-security.org/secworld.php?id=17627

November 12, Softpedia – (International) **18 critical vulnerabilities patched in Flash Player 15.0.0.223.** Adobe released a new version of its Flash Player software, closing 18 critical security issues, 15 of which could allow an attacker to execute arbitrary code. Source: http://news.softpedia.com/news/18-Critical-Vulnerabilities-Patched-in-Flash-Player-15-0-0-223-464731.shtml

November 12, Network World – (International) **Google DoubleClick down, leaving sites ad-free.** The Google DoubleClick for Publishers service experienced an outage November 12, preventing ads from being displayed on several Web sites. Google stated that the company was working to resolve the issue. Source: http://www.networkworld.com/article/2846816/business-continuity/google-doubleclick-down-leaving-sites-ad-free.html

November 12, Softpedia – (International) **Air-gapped systems targeted by Sednit espionage group.** Researchers with ESET stated that the Sednit espionage group (also known as APT28 or Sofacy) have employed a tool known as Win32/USBStealer since at least 2005 that can exfiltrate data from air gapped systems. The tool is added to a compromised system connected to the Internet and then plants the tool on any removable storage device, collects information on the air gapped system, and then transmits it back to the attackers whenever the storage device is next connected to an Internet-connected system. Source: http://news.softpedia.com/news/Air-Gapped-Systems-Targeted-by-Sednit-Espionage-Group-464734.shtml

November 11, Softpedia – (International) **Uroburos espionage group is still active, relies on new remote access trojan.** G Data researchers found that the Uroburos espionage group (also known as Turla or Snake) remains active and is using two similar versions of a new remote access trojan (RAT) known as ComRAT that includes increased obfuscation and anti-analysis capabilities. Source: http://news.softpedia.com/news/Uroburos-Espionage-Group-Is-Still-Active-Reles-on-New-Remote-Access-Trojan-464694.shtml

November 10, Securityweek – (International) **SQL injection vulnerability patched in IP.Board forum software.** Invision Power Services released patches for its IP.Board forum software November 9, closing a SQL injection vulnerability several hours after its discovery on versions 3.3.x and 3.4.x. Source: http://www.securityweek.com/sql-injection-vulnerability-patched-ipboard-forum-software

November 10, Securityweek – (International) **iOS security issue allows attackers to swap good apps for bad ones: FireEye.** Researchers with FireEye identified a new attack dubbed a Masque Attack that can allow attackers to replace a legitimate iOS app with a malicious one if both applications use the same bundle identifier. Victims targeted by the attack must be lured into installing the malicious app which can then be replaced by the malicious app on jailbroken and non-jailbroken iOS devices. Source: http://www.securityweek.com/ios-security-issue-allows-attackers-swap-good-apps-bad-ones-fireeye

November 11, Softpedia – (International) **Hacker steals payment data from One Love Organics website.** One Love Organics notified consumers October 30 that the online beauty product company’s server was compromised and the personal information, including payment card data, of customers who made purchases between August 24 and October 15 may have been breached. A representative reported that an attacker leveraged a vulnerability in the Web site’s shopping cart feature to perform and SQL injection, and that the vulnerability has since been closed. Source: http://news.softpedia.com/news/Hacker-Steals-Payment-Data-from-One-Love-Organics-Website-464725.shtml

NOAA says four of its websites breached by Chinese hackers

Fox, 13 Nov 2014: Hackers from China were able to breach government computer systems at the agency that oversees the National Weather Service, according to the chairman of a Congressional subcommittee that oversees the National Oceanic and Atmospheric Agency's budget. NOAA confirmed the hacking Wednesday, saying in a statement that four of its websites were "compromised by an Internet-sourced attack" in recent weeks. NOAA spokesman Scott Smullen declined comment on the source of the intrusion, however. NOAA operates a network of weather satellites and websites that distribute crucial information to public and private organizations, including forecasts for airlines and other transportation companies. In the statement, Smullen said the agency's staff "detected the attacks and incident response began immediately." While Smullen declined to provide more detail, U.S. Rep. Frank Wolf, R-Virginia, told The Associated Press that NOAA officials told him the attack originated in China. He accused the agency of keeping quiet about the attacks until reporters from the Washington Post began asking about the maintenance. "I think they didn't want to say anything because they were embarrassed," he said of agency officials. Wolf chairs a House Appropriations subcommittee that oversees the NOAA budget. Word of the NOAA attack comes two days after the U.S. Postal Service disclosed that hackers were responsible for a data breach which compromised information from some of its customers and employees. Officials have not publicly discussed the source of that attack, but the Washington Post reported that Chinese hackers are also suspected in that episode. To read more click HERE

'Guccifer,' Bush family hacker, speaks out: 'What I did was right'

Fox, 13 Nov 2014: The hacker known as Guccifer, whose exploits brought the world such images as George W. Bush's self-portrait in the shower, doesn't regret his actions: "OK, I broke the law, but seven years in a maximum-security prison? I am not a murderer or a thief," he tells the New York Times, which notes that two of his cellmates in a Romanian prison are convicted killers. "What I did was right, of course." He justifies it, the paper reports, with a lengthy statement on how the Illuminati run the world, the 9/11 attacks were a conspiracy, and a nuclear attack on Chicago is planned for next year. But a Romanian prosecutor doesn't see politics behind the hacking, which he says targeted "no Illuminati, just famous and beautiful girls." Guccifer—or Marcel-Lehel Lazar of Romania—didn't need particularly high-tech methods to break into accounts of the Bush family, Colin Powell, and other well-known people, the Times reports. The Smoking Gun offers a comprehensive list of his victims, who range from entertainers like Steve Martin to Titanic investigator Robert Ballard. The unemployed 43-year-old did it all with a "clunky" desktop computer and his phone, guessing at answers to users' security questions. In January, Guccifer feared that authorities were onto him, so he destroyed his hard drive with an ax. But pieces he left behind were used as evidence against him. To read more click HERE

ISPs are removing encryption from customers' emails

Heise Security, 13 Nov 2014: A number of ISPs in the US and Thailand have recently been spotted actively removing encryption from their customers' data sent to email servers, the Electronic Frontier Foundation warned on Monday. The ISPs are doing it by removing from the customers' data the STARTTLS flag, which is used by email servers to request encryption when talking to another server or client. "By stripping out this flag, these ISPs prevent the email servers from successfully encrypting their conversation, and by default the servers will proceed to send email unencrypted," explained EFF technologist Jacob Hoffman-Andrews. "This type of STARTTLS stripping attack has mostly gone unnoticed because it tends to be applied to residential networks, where it is uncommon to run an email server." Unlike PGP and S/MIME, STARTTLS does not provide end-to-end encryption, but just server-to-server. Nevertheless, it has some advantages over the former:

- It protects metadata (subjet lines, TO, FROM, CC and BCC fields)
- Users don't have to do anything for it to function
- An email server with STARTTLS can provide Forward Secrecy for emails.

Combining all these technologies together - and it can be done - provides more security. Unfortunately, as we see now happening, the STARTTLS flag is easy to spot (it's not encrypted) and interfere with. "It is important that ISPs immediately stop this unauthorized removal of their customers' security measures," says Hoffman-Andrews. "ISPs act as trusted gateways to the global Internet and it is a violation of that trust to intercept or modify client traffic, regardless of what protocol their customers are using. It is a double violation when such modification disables security measures their customers use to protect themselves." He also shared that the EFF is working on improving STARTTLS with STARTTLS Everywhere, a tool that will require encryption for servers that are already known to support it. To read more click HERE

73% of organizations say BYOD increases security risks

Heise Security, 12 Nov 2014:
Findings from a Kensington survey on the security risks created by BYOD policies in the enterprise show that 73 percent believe that BYOD represents greater security risks for their organization, and yet 59 percent still approve the use of personal devices for business usage. The survey found that across multiple B2B vertical industries – including Education, Healthcare, Financial Services, Retail and Manufacturing – CEOs, CIOs, CSO, and IT professionals are significantly concerned with how BYOD is impacting the security of their enterprise environments. To address these concerns a number of physical security measures are being leveraged with varying adoption and as many as 55 percent report that they are considering further investments in this security area. Physical security measures in use by survey respondents included:

- 64 percent use employee training and guidelines
- 61 percent use anti-malware and encryption
- 55 percent have employed compliance and governance policies
- 48 percent use data loss prevention and authentication solutions

"With the rapid rise in the use of mobile devices and laptops, organizations need to become vigilant in their ability to protect those devices from the risk of theft or loss that may put critical business and personal data in the wrong hands," said Judy Barker, Global Product Marketing Manager, Kensington. "With the BYOD onslaught, this risk is even more critical. By employing simple and secure device locking mechanisms organizations can easily safeguard their data, their brand and their reputation, with the immediacy they need to avert this threat." To read more click HERE

Brazilian, Chinese govt sites host the most phishing pages

Heise Security, 7 Nov 2014: Occasionally, cyber crooks compromise websites administered by governments and make them host phishing pages. But how often does that happen? Cyvveillance researchers have analyzed a year’s worth of phishing URLs they have collected - a little over 72,000 unique domain names - to find that answer, and have found that 195 distinct phishing attacks were hosted on government-administered servers. Sites belonging to Brazilian and Chinese governments were most successfully targeted, followed by those administered by Colombian, Turkish, and Nepalese governments. "The data suggest that countries whose economies are growing quickly may have a harder time securing their infrastructure online than more established economic powers," the researchers noted. "For example, with China’s breakneck pace of growth it should be no surprise that there are government servers stood up without optimal security in place. A hallmark of emerging markets is a lack of skilled or technical labor." They also pointed out that this type of attack is usually not perpetrated by state-sponsored attackers, but by common cyber crooks. To read more click HERE

What attackers do after bypassing perimeter defenses

Heise Security, 6 Nov 2014: Vectra Networks collected data over five months from more than 100,000 hosts within sample organizations to gain a deeper understanding of breaches that inevitably bypass perimeter defenses, and what attackers do once inside networks. They found that more than 11,000 hosts experienced one or multiple cyber-attacks that made it through perimeter defenses. Of these attacked hosts, 10 percent had detections for two or more attack phases – such as botnet monetization, command and control, reconnaissance, lateral movement and exfiltration. Overall, 15 percent of hosts in the participating organizations experienced a targeted attack. Once the attackers established a stronghold, they performed reconnaissance via internal port scans, lateral movement using brute force attacks, remote control of the attack with command and control communication, and exfiltration through hidden tunnels. Oliver Tavakoli, CTO of Vectra Networks, said: "Cyber attacks are increasingly sophisticated, highly organized, and successful despite $60 billion invested in cyber security annually worldwide. All of the attack phases detected in this report are ones that evaded organizations' perimeter and endpoint security systems. Additional key findings of the study include:

- Eighty-five percent of attacks experienced by the sample organizations were opportunistic attacks. Two percent of the hosts experiencing an opportunistic attack were being used to spread botnet malware to other computers within the organization.
- Fifteen percent of attacks experienced by the sample organizations were targeted attacks. Two percent of these hosts under targeted attack were breached to the exfiltration stage, where the attacker was preparing to steal data.
- Seven percent of hosts had both botnet and exfiltration detections, which indicates possible theft of credentials for use in a subsequent targeted attack against the sample organization or other organizations.

To read more click HERE

Smartphones Owned at Mobile Pwn2Own Hacking Competition

Softpedia, 13 Nov 2014: Security protections for iPhone 5S, Samsung Galaxy S5, Nexus 5 and Amazon Fire Phone came undone in the first day of the Mobile Pwn2Own hacking competition at PacSec security conference in Tokyo. The contest is currently at its third reiteration and attracted sponsorship from Google and Blackberry. In most of the cases, the attack vector used by the hackers to take control of the phones was the Near Field Communication (NFC) technology, which is available in the latest models of smartphones from prominent vendors. During the competition, the hackers relied on NFC to trigger a deserialization issue in code specific to Samsung, which led to the compromise of a Galaxy S5; this was achieved by Team MBSD from Japan. Another successful attempt to own the same type of device, also through NFC, belonged to Jon Butler of South Africa's MWR InfoSecurity, who took advantage of a logical error. This is specific to Samsung Galaxy S5 devices. Google-supported Nexus 5 from LG was the second smartphone to fall victim to an NFC attack. Initiated by Adam Laurie from the UK's Aperture Labs, the compromise consisted of an exploit stemming from two security vulnerabilities that forced pairing two devices through Bluetooth. However, the main event was the compromise of the iPhone 5S, an action that made use of two bugs to create a full sandbox escape in Safari mobile web browser. The feat was achieved by lokihardt@ASRT. MWR InfoSecurity managed to compromise another mobile phone, this time Amazon's Fire Phone. It was a three-man effort that combined a total of three bugs aimed at the device's web browser; this successful hack ended the first day of the competition. Organized by the HP's Zero-Day Initiative (ZDI), this year's Mobile Pwn2Own is sponsored by Google and BlackBerry with prizes amounting to $425,000 / €341,500. All vulnerabilities exploited during the competition are zero-days, and any details relating to them and the exploit techniques used are provided only to the vendors, via responsible disclosure, and HP ZDI. The conclusion of the first day of contest are easy to draw: despite all security claims, smartphones are vulnerable. The targets were Samsung Galaxy S5, LG Nexus 5, iPhone 5S and Amazon Fire Phone, and all of them have been compromised, either through code specific to the manufacturer or through the technology they integrate. On Thursday, the second and last day of this year’s competition, the final two participants take aim at Windows Phone (Nico Joly) and the Android operating system (Jüri Aedla). To read more click HERE

DDoS Attacks Cost $40,000 per Hour on Average

Softpedia, 13 Nov 2014: A report seeking to measure the impact of distributed denial-of-service (DDoS) attacks on affected organizations reveals that the average cost per hour of such an assault is $40,000 / €32,180, with half of the surveyed companies recording losses of $500,000 / €402,000 during an incident. The study was conducted by Incapsula, a company providing protection solutions against DDoS attacks, on 270 organizations in the US and Canada, from different industry sectors. The number of employees for each of them varies from 250 to 10,000. Financial losses are not tied only to mitigating the incident As per the information from the surveyed entities, 49% of the recorded DDoS attacks lasted between six to 24 hours. These are the cases where cost estimation is averaged at $40,000 / €32,180 for every hour of the attack. 15% of the respondents declared costs in excess of $100,000 / €80,500 per hour. Incidents extending over the period of several days and even more than one week have also been reported. According to Incapsula, the first half of the year saw a 350% increase in large-scale volumetric DDoS incidents, which are also getting more powerful and last longer. These are intended to exhaust the available network bandwidth, resulting in disruption of services. The losses associated with DDoS attacks are not assessed strictly from the event mitigation standpoint and include the overall impact on the company. “Costs are not limited to the IT group; they also have a large impact on units such as security and risk management, customer service, and sales. “Additionally, most respondents who had been targeted experienced a variety of non-financial costs. 87% experienced at least one non-financial consequence, such as loss of customer trust, loss of intellectual property,” the report states. In a little more than half of the cases surveyed, hardware and software had to be replaced, which also incurs expenses. As it was expected, the IT division is the most affected from a financial point of view, followed by customer sales and the security/risk management unit. Most companies do not use dedicated anti-DDoS technology Getting the company back to the normal state of business is also an aspect that has to be taken into consideration because, in most of the cases, recovering from a DDoS attack can take months and sometimes even years, assessing the entire extent of the damage not being possible in all instances. What is certain is the fact that these incidents have a long-term effect. As far as managing the incident is concerned, many of the respondents lacked the necessary plans and solutions for defending against DDoS attacks, some still relying on web application or network firewalls. However, 43% of them stated that their organization used a dedicated solution for combating the DDoS threat. To read more click HERE

US Coast Guard Contractor Pleads Guilty to Stealing Personal Info

SoftPedia, 13 Nov 2014: Taking a computer in for repairs can result in exposing private information about the owner, as cases where repairmen harvest such data are not rare. An individual in Connecticut facing such an accusation pleaded guilty before a federal court in Hartford. Identified as Larry Mathews, 34, of Pawcatuck, the individual stands accused of “computer intrusion in furtherance of a tortious invasion of privacy;” translated into plain English, this means that he was copying personal data from machines he was servicing (these included both computer systems and other electronic devices). This happened on more than 250 occasions. The ransacking took place in 2008, when Mathews had a computer repair business and was also engaged as a civilian contractor for the US Coast Guard, working as a computer technician, the court records say. According to News8, the details copied by Mathews included names and passwords, as well as private multimedia content, some of it explicit in nature, recorded by the owners of the computers. Had he not shared the stolen data with a third party, the perpetrator would have never been caught. He was reported to the police in 2013. Considering that credentials were involved, these could have been put up for sale on underground forums, or he could have taken advantage of them himself through money extortion schemes. However, it is unclear if the culprit tried to monetize the stolen data or if he broke into the online accounts. Mathews waived his right for indictment and pleaded guilty. He is scheduled to receive his sentence on February 4, 2015, facing five years of jail time at most and a fine of up to $250,000 / €200,000. It is unlikely that he will receive the maximum punishment though, especially if no financial gains have been proven as a result of his actions. Users should know that even if the device is broken, most of the times the data stored on it is not damaged and can be extracted without any trouble. To eliminate any risk of personal information falling into the wrong hands, it is recommended to remove the storage device from the gadget before taking it to repairs or selling it. If this cannot be done, creating a backup and encrypting the data should be considered; if the repairs require overwriting the files, the backup can be restored. Wiping the storage unit has proven not to be a good way to maintain privacy because the files can still be recovered with the use of special software that is publicly available and free. As such, if encryption is applied, even if the data is recovered, it would still be protected. To read more click HERE

Weak Password Opens the Computer of FBI's Most Wanted Hacker

Softpedia, 13 Nov 2014: Jeremy Hammond, 29, the hacker with a key role in breaking into the computer systems of Stratfor security intelligence company back in 2011, thinks that the weak password guarding access to his encrypted laptop permitted authorities to find incriminating evidence about his activities. Hammond is currently in custody at Manchester Federal Prison in Kentucky, as a result of Hector Monsegur's cooperation with the FBI. Monsegur, a hacker himself, was known online as Sabu and coordinated the activity of the LulzSec outfit; after getting caught by the authorities he turned informant and helped them catch other hackers. Top priority during the raid: closing the laptop lid Known online under the alias Anarchaos, Hammond was arrested (currently serving a 10-year sentence) at his home in 2012 for the Stratfor incident, which resulted in the leak of massive amounts of confidential information consisting of emails between the company and its clients. Additional data spilled online included credit card information, which had been stored in plain text, from a client list which had Northrop Grumann, the Marine Corps and Time Warner Cable on it. The US Department of Homeland Security and the Defense Department were also Stratfor clients at the time. According to a profile from the Associated Press, at the time of the arrest, the 29-year-old was chatting with some friends in the kitchen of his apartment in Chicago when the front door was kicked in and a flash bang was thrown. Although everyone else's reaction was to hit the floor, Hammond had other concerns, such as protecting access to his computer. His response to the flash bang was to dart to the bedroom and close the lid of the laptop, which would trigger the encryption of all the data on the storage device. In encrypted state, information on the hard drive could be accessed only by providing the security password. This could be obtained through cracking, but it would take too long to complete in the case of strong countersigns. The cat is not to blame However, Hammond's was a weak password that could have been cracked in no time, based on a dictionary containing words related to his life and interests. "My password was really weak," he said. His string of choice for protecting data on the laptop was "Chewie 123." This was the name of his cat followed by the most ubiquitous numbers found in passwords. The hacker is to be released in 2020. A password cracking algorithm would try out this combination in the first attempts to produce a match for the countersign's hash. Passwords need to be as strong as possible in order to avoid cracking them with automated tools. Cybercriminals have built large dictionaries for this purpose and sometimes rely on powerful cloud computing to reveal the string of characters corresponding to stolen hashes. Of course, this would work only if salt is not applied. To read more click HERE

Stream from Insecure Surveillance Cameras Available to Anyone

Softpedia, 12 Nov 2014: Video streams from an impressive number of surveillance cameras from around the world is publicly available on a website, not because they've been hacked, but because their owners failed to protect access with a password. Poorly protected equipment is bound to become the object of scrutiny of third-party individuals, at one point. In this case, the administrators of insecam.com have built a system that automatically scours the web in search of cameras and DVR systems that have the default username and password pair (admin:admin, admin:12345) to protect them from unauthorized access. Important to note is that webcams integrated into personal computers or USB-connected ones are not taken into consideration. But even so, plenty of people use them for monitoring personal perimeters such as the inside or the outside of a residence. It appears that the administrators want to raise awareness of the importance of applying a personal password to keep the stream private, otherwise anyone can search the Internet and find the default credentials for accessing the stream captured by the device. Armed with this information, burglars can easily look online for the IP address of the device, tap into the video feed and record the daily routine of the victim. Not only this, but they already know where the cameras are. In the FAQ section of the site it is clearly stated that the availability of the streams is not the result of a hack attempt, but simply of using publicly available and free online tools to find them. Google is one way to start, but other engines, such as Shodan, specifically designed for finding Internet-facing hardware components based on several criteria, can also be used. "Owners of these cameras use default password by unknown reason. There are a lot of ways to search such cameras in internet using Google, search software or specialised search sites," an entry in the FAQ reads. Tens of thousands of cameras are listed on insecam.com, and more are constantly added. Their owners can request taking down the feed, but the only way their privacy is respected is to apply a different password than the one set by the manufacturer or vendor of the equipment. At the moment of writing, at the top of the list with insecure IP cams are the United States (11,046), Republic of Korea (6,536), China (4,770), Mexico (3,359) and France (3,285). Italy and the United Kingdom are next, with 2,870 and 2,421 insecure cameras, respectively. A rough total is estimated at 73,000. To read more click HERE