THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

15 September 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

September 11, Help Net Security – (International) **Chinese attack groups operate in parallel in cyber espionage campaigns: FireEye.** Researchers with FireEye discovered two cyberespionage campaigns originating in two regions of China that appear to share several commonalities including using the same custom backdoors and remote access trojans (RATs). One campaign dubbed Moafee targets various military, government, and defense industry entities while the second known as DragonOK targets high-tech and manufacturing companies in Taiwan and Japan. Source: http://www.securityweek.com/chinese-attack-groups-operate-parallel-cyber-espionage-campaigns-fireeye

September 11, Help Net Security – (International) **Researchers find malicious extension in Chrome Web Store.** Trend Micro researchers identified several malicious extensions inside the Chrome Web Store, including one spread via a Facebook scam campaign that allows attackers to post statuses, send messages, and take other actions using a victim's Facebook account. Source: http://www.net-security.org/malware_news.php?id=2863

Cybersecurity expert sees rising threat from 'adversaries'
Herald-Mail Media, 11 Sep 2014: A noticeable spike in cybersecurity threats has been seen in recent years, evidenced by reports of identity theft, data breaches and phishing scams often reported in the media. "It's hard to quantify it, but there is a huge increase in adversaries," Kelley Dempsey, senior information security specialist at the National Institute of Standards and Technology, told about 25 local business professionals Wednesday morning during a monthly Eggs & Issues breakfast hosted by the Hagerstown-Washington County Chamber of Commerce. "If you look at firewall statistics, there are constantly people banging against firewalls trying to get in," she said. "Anyone who's running a firewall and looking at their logs, they can see — it doesn't matter how large or small the business is, they're trying to find any information they can find." Dempsey spent about an hour highlighting numerous threats to data security for small businesses, as well as some simple steps to take to safeguard information of customers. The thing that has changed dramatically in the cybersecurity realm is that hackers today need little to no expertise in information technology to gain access to personal information, according to Dempsey. "The tools have gotten easier to get, so whereas 10, 15 years ago, you had to be a computer scientist ... and now everything is just available on the Internet," she said. "Anyone who wants to be an adversary can just go out and start downloading malware programs and find ways to get in" to business or personal information systems. The goal of many hackers is to gain access to a business's data system, where thousands of customers' personal information is stored, and then resell that information to others online. Examples of that type of activity include Target and Home Depot data breaches, which compromised the credit card information of millions of customers, Dempsey said. Threats to personal information are just as real. The recent flood of nude photographs online of dozens of female celebrities, including actress Jennifer Lawrence and model Kate Upton, might have been the result of a targeted phishing email scam, according to some media reports. The easiest thing for the public and small businesses to do is back up their data, use strong passwords with at least 12 characters and "don't click on crazy links," Dempsey said. "That's probably the most important," she said, referring to the phishing links that often appear in unsolicited emails or social-media postings. John Berry, a manager with Global

Data Consultants and a chamber board member, said after the presentation that backup protection is the most important step all small businesses must take. "Backup protection is so crucial because it allows you to have a reset button," he said. "Without that data to be able to restore to a compromised system, you truly have nowhere to turn." "You're always vulnerable to threats," Berry said. "It's kind of like the alarm sign in your front yard — you just want to make them go to the next house. Ultimately, if you do just some of the basic self-checks, common-sense logical steps that can try and safeguard you or make it that much more difficult ... you're probably better off." To read more click HERE

Comcast Is Threatening To Cut Off Customers Who Use Tor Web Browser

Business Insider, 15 Sep 2014: Multiple users of anonymous web browser Tor have reported that Comcast has threatened to cut off their internet service unless they stop using the legal software. According to a report on Deepdotweb, Comcast customer representatives have branded Tor "illegal" and told customers that using it is against the company's policies. Tor is a type of web browser that, in theory, makes all your internet activity private. The software routes traffic through a series of other connected internet users, making it difficult for governments and private companies to monitor your internet usage. Up to 1.2 million people use the browser, which became especially popular after Edward Snowden leaked information showing that the NSA was eavesdropping on ordinary citizens. Prior to that, Tor had been popular among people transacting business on Silk Road, the online market for drugs and hitmen. The problem is that downloading or using Tor itself isn't illegal. Plenty of people might have legitimate reasons to want to surf the web in private, without letting others know what they were looking at. But Tor has been pretty popular with criminals. Comcast has reportedly begun telling users that it is an "illegal service." One Comcast representative, identified only as Kelly, warned a customer over his use of Tor software, DeepDotWeb reports: Users who try to use anonymity, or cover themselves up on the internet, are usually doing things that aren't so-to-speak legal. We have the right to terminate, fine, or suspend your account at any time due to you violating the rules. Do you have any other questions? Thank you for contacting Comcast, have a great day. Comcast customers, speaking to Deepdotweb, claimed that Comcast repeatedly asked them which sites they were accessing using Tor. In a statement to Deepdotweb, Comcast defended its actions, seemingly asserting that it needs to be able to monitor internet traffic in case they receive a court order. To read more click HERE

Study: 15 Million Devices Infected With Mobile Malware

Dark Reading, 9 Sep 2014: Fifteen million mobile devices are infected with malware, and most of those run Android, according to a new report by Alcatel-Lucent's Kindsight Security Labs. Researchers found that "increasingly applications are spying on device owners, stealing their personal information and pirating their data minutes, causing bill shock." Mobile spyware, in particular, is on the rise. Four of the 10 top threats are spyware, including SMSTracker, which allows the attacker to remotely track and monitor all calls, SMS/MMS messages, GPS locations, and browser histories of an Android device. Mobile infections increased by 17 percent in the first half of 2014, raising the overall infection rate to 0.65 percent. About sixty percent of the infected devices are Android smartphones. About 40 percent are Windows PCs connecting through mobile networks. Windows Mobile, iPhones, Blackberrys, and Symbian devices combine for less than 1 percent. To read more click HERE

WH Official: Cyber Coverage Will Be a Basic Insurance Policy By 2020

NextGOV, 8 Sep 2014: By 2020, private firms will be buying cybersecurity insurance when they sign up for product liability coverage and other basic policies, a top White House cyber official said Monday. There isn't a market for cyber insurance yet — not for lack of interest, but because of the lack of data on the odds companies will be breached and the true costs of those hacks. Now, that kind of information is starting to become more transparent, what with major retailers, banks and other companies reporting breaches daily and industries finally taking inventory of their security postures. Within six years, "we're going to be well on our way to everyone having cyber insurance as just a basic set of insurance, just like property insurance," said Ari Schwartz, director for cybersecurity on the White House National Security

Council, during a Sept. 8 panel discussion at the Nextgov Prime conference. Some businesses are clamoring for coverage, but cannot obtain the type of policies they need. A Bipartisan Policy Center report on power grid cybersecurity published in February recommended the government initially guarantee coverage. "A federal backstop would increase carriers' willingness to offer cyber insurance and lower the cost of doing so," said the co-authors, who included retired Gen. Michael Hayden, former CIA and National Security Agency director. Schwartz, however, said the marketplace is "really growing quite a bit" today without government intervention. However, the demand for such services still outstrips the supply. For example, retail giant Target reportedly couldn't find an adequate policy for cyber losses after hackers raided the big box store's payment system last year. At the time, Target pieced together $100 million in coverage, along with a $10 million deductible, which, according to The New York Times, will barely take care of an anticipated $1 billion in losses. Target attempted to obtain more insurance, but at least one carrier rejected the retailer. "The insurance companies couldn't sell it to them because they didn't have the actuarial data to be able to figure out what the costs should be and how it should work," Schwartz said. "Part of that issue is getting the information that we need in this space." Industries now are also beginning to collect the necessary data from victims and potential victims in a way that protects their identities, he said. For example, there is the "Electricity Subsector Cybersecurity Capability Maturity Model," a 92-page yardstick that delineates both the levels of protection organizations should maintain and judges how they stack up against those benchmarks. Conversations among the White House, the departments of Energy and Homeland Security and power companies led to the development of the maturity model. "We've seen a lot of different industries start to build maturity models for cybersecurity," Schwartz said. The model used by the electricity sector is being used by most large companies in the industry, he noted. Oil and natural gas firms, as well as telecommunications companies, are following suit with their own gauges, Schwartz added. "You have different industries now building these and the insurance companies are looking at what those industries are doing and are able to provide insurance much more easily for those sectors that have maturity models," he said. "That's a really positive sign." To read more click HERE

In China, Cybercrime Underground Activity Doubled In 2013

DarkReading, 3 Sep 2014: Forget intelligence gathering. Financially motivated cybercrime is booming behind the Great Wall.China has become infamous for politically motivated intelligence gathering, but new research from Trend Micro shows that a financially motivated, politically independent cybercrime underground is alive and growing behind the Great Wall, as well. The new report shows that Chinese cybercrime underground activity doubled between 2012 and 2013. According to Trend Micro CSO Tom Kellermann, it has likely tripled since then. Further, Kellermann says, these criminals are not just targeting victims in other countries. The targets include "the bourgeois, nouveau-riche Chinese elite who have profited from capitalism" in a country with a dwindling middle class. The Chinese government "has been focused externally... on information dominance and espionage," Kellermann says. The technological skills cultivated by the country's leaders are coming back to hurt them in the form of new cybercriminals "who are not beholden to the regime. They believe money is God and believe that crime has evolved with technology." Other recent Trend Micro research shows that the Chinese underground is largely focused on mobile device/services attacks -- Android-based products in particular -- and charges customers a premium for that work. The most sought mobile crime products and services are SMS spamming, premium service numbers, and SMS servers. SMS spamming is relatively inexpensive, ranging from $50 for 5,000 text messages ro $460 for 100,000 messages. Premium service numbers -- used to subscribe mobile users to unwanted services and charge them a fee for it -- run from $2,500 per year to $36,000 per year. SMS servers -- radio frequency hardware that forces nearby phones to disconnect from legitimate base stations and connect to the attacker's SMS server instead -- cost $7,400. The reasons for the higher price tags, says Kellermann, are that mobile attacks require more creative code and can offer bigger payoffs. For one thing, mobile payments are more popular in Southeast Asia than they are in the United States, which makes mobile devices more attractive. "I'd pay more" for mobile attacks, "because I can hack your life," he says. "If the [mobile] device is an extension of yourself, then I can hack you." In comparison, the most popular nonmobile attack tools are quite affordable. DDoS toolkits can be rented for $81 per month. RAT "licenses" range from $97 to $258 per year, depending on the software. Even the new DNS attack services cost only $323. The attack products and services appear to be sophisticated and professional. However, the methods the criminal marketplace uses to communicate are not. The communication tool of choice is QQ groups, a feature of the QQ instant messaging app. Unlike most organized criminals in Eastern Europe, who often rigorously vet customers before working with them, these Chinese groups make themselves quite available to the general public. A simple search of QQ groups turns up results like the "China DDoS and Hacking Service Group." Download the full report here. To read more click HERE