The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

12 February 2014

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

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

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, Sandia Labs

February 11, Softpedia – (International) **New POS malware JackPOS targets companies in Canada, Brazil, India and Spain.** Researchers at IntelCrawler identified a new piece of point-of-sale (POS) malware dubbed JackPOS that has been spotted in attacks on POS systems in several countries over the past 3 weeks. The malware is disguised as the Java Update Scheduler in drive-by attacks and has affected POS systems in the U.S. and several other countries. Source: http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml

February 11, The Register – (International) **MtGox takes heat as reasons for Bitcoin FAIL surface.** Bitcoin exchange site MtGox reported that it continued to suspend transactions to third-party accounts after detecting suspicious transactions in its network that could involve attackers abusing a transaction malleability issue to receive payments twice. Source:http://www.theregister.co.uk/2014/02/11/mtgox_takes_heat_as_bitcoin_transactions_remain_on_hold/

February 11, Softpedia – (International) **Malicious versions of Flappy Bird game send SMSs to premium rate numbers.** Trend Micro researchers spotted several rogue versions of the recently-discontinued Flappy Bird game for Android that are designed to send SMS messages to premium rate numbers. Source: http://news.softpedia.com/news/Malicious-Versions-of-Flappy-Bird-Game-Send-SMSs-to-Premium-Rate-Numbers-425977.shtml

February 10, Threatpost – (International) **New 'Mask' APT campaign called most sophisticated yet.** Researchers at Kaspersky Lab identified a sophisticated advanced persistent threat (APT) campaign targeting government offices, embassies, and energy companies in several countries for over 5 years dubbed Careto/Mask. The campaign appears to be operated by Spanish-speakers and utilizes at least one zero-day vulnerability, with versions of its malware for Windows, OS X, and Linux systems. Source: http://threatpost.com/new-mask-apt-campaign-called-most-sophisticated-yet/104148

U.S. to offer companies broad standards to improve cybersecurity
Digital Journal, 12 Feb 2014: The U.S. government is expected on Wednesday to release the final version of voluntary standards meant to help U.S. companies in nationally critical industries better protect themselves against cyber attacks. Criticized in earlier drafts for being too vague and toothless, the so-called cybersecurity framework attempts to turn a vast amount of industry input into guidelines designed for 16 different sectors whose disruption could be devastating to the country. Exactly one year after President Barack Obama issued an executive order directing a Commerce Department agency to compile voluntary minimum standards, the National Institute of Standards and Technology, or NIST, is due to issue guidelines, which companies have no obligation to adopt. Drafters of the framework had to allay concerns by many in the private sector that their voluntary standards could someday become regulations. The threat of restrictive rules has helped stall progress on passing a cybersecurity law in Congress. The framework, drafted by the non-regulatory NIST in consultation with thousands of industry experts, offers broad benchmarks for companies to measure the effectiveness of their cyber defenses. "The federal government has an overriding interest to protect critical

infrastructure," said Norma Krayem, a former official at the Transportation, State and Commerce departments who now works with infrastructure companies as a senior policy adviser at law firm Patton Boggs. "But they don't own or control it, and at the moment, the cyber framework is the means to work collaboratively with critical infrastructure to address (cybersecurity) concerns." Cybersecurity experts warn that relentless efforts to hack into U.S. banks and financial institutions, the power grid and other critical infrastructure, paired with instances of disruptive attacks abroad, pose a national security threat. The issue recently became a household topic after hackers stole about 40 million credit and debit card records and 70 million other records with personal customer data from the third-largest U.S. retailer, Target Corp. Many experts have expressed alarm about the lack of awareness or reluctance among some companies' leadership to spend more money on cyber defenses. The framework could force the issue into more executive suites, analysts say. "At a minimum, it's going to force this conversation up the food chain, out of the CEO office into the boardroom," said Tom Kellermann, a former member of Obama's Commission on Cyber Security and software company executive now with professional services firm Alvarez & Marsal. But it is unclear whether the private sector, always concerned about liabilities attached to any standards, would widely adopt the voluntary framework. The Departments of Homeland Security, Commerce and Treasury are reviewing potential incentives for adoption. It is also unclear how effective the framework will prove in practice. "At that high level, they got it right. ... Further down, it gets murky really fast," said Andrew Ginter, vice president of industrial security at Waterfall Security Solutions, whose clients include power plants and water-treatment facilities. "The NIST framework never uses the word 'firewall.' It's that abstract," he said, referring to a common standard component of network security. According to earlier drafts, the framework offers sweeping categories such as "access control" or "data security" to evaluate how effectively a company identifies and protects network assets, and detects, responds to and recovers from breaches, on a one-to-four-tier scale for implementation. The categories then break into slightly narrower areas, such as keeping inventories of used software platforms and applications, ensuring that top executives know roles and responsibilities, and setting information security policies. The voluntary standards are meant to complement and fill the gaps left by existing regulations that apply to some of the sectors, such as energy and financial services. To read more click **HERE**

As crimeware evolves, phishing attacks increase

Heise Security, 12 Feb 2014: The number of phishing campaigns increased by more than 20 percent in the third quarter of 2013, with crimeware attacks evolving and proliferating, according to the APWG. The total number of unique phishing websites observed rose to 143,353 in Q3, up from Q2's 119,101. The increase is generally attributable to rising numbers of attacks against money-transfer and retail/e-commerce websites. During the same period, there was an 8 percent decline in the number of brands targeted by phishers, as the number of brands targeted fell from an all-time high of 441 in April 2013 to 379 in September 2013. "In the 3rd quarter of 2013, we also saw a change in the phishing themes used by malware authors. An emphasis on social media-themed subjects, such as 'Invitation to connect on LinkedIn', was used to entice users who would be used to seeing such subjects," said APWG contributor Carl Leonard of Websense Security Labs. APWG member PandaLabs cataloged nearly 10 million new crimeware samples from July to September, and PandaLabs observed that the number of new malware samples in circulation in the first nine months of 2013 was larger than the total for all of 2012. More than 59 percent of computers in China appeared to be infected with malware or spyware, a record high for any country. The complete report is available **here**. To read more click **HERE**

Exposing the profitability of private data

Heise Security, 12 February 2014: Security breaches, cyber criminals, and organized attacks made it nearly impossible to keep personal and financial data private, according to Trend Micro. This annual report provides an insight into the vulnerabilities of today's technology that is rapidly becoming interconnected and "smart." "Last year encompassed major security breaches, increased malware, and mobile threats that impacted people from all walks of life around the world," said Raimund Genes, CTO, Trend Micro. "Now more than ever, consumers and corporations alike must be diligent in understanding their vulnerabilities, and what should be done from a security perspective to better protect

personal data and guard against compromised privacy. While this report details the threat landscape of 2013, more importantly it explains how these threats will continue to evolve and what should be done to mitigate the negative impact." Report highlights include:

- Financial threats: As online banking malware that directly target victims' finances intensified globally this year, prolific ransomware increased and evolved into Cryptolocker throughout the year.
- Mobile threats: There was a sizable increase in both volume and sophistication of mobile threats, as PC-based threats transitioned to mobile platforms. By the end of 2013, we saw a total of 1.4 million malicious and high-risk Android apps being identified. And Apple users are not immune. 2013 saw an increase in phishing attacks specifically targeting Apple users as criminals recognize the potential revenue from this install base.
- Personal privacy: Through social networking and "personal cloud" accounts, personal privacy became a recurring issue. Aggressive phishing attacks riding on the release of popular products such as PS4 and Xbox One emerged to compromise personal information.
- Infrastructure attacks: High-profile incidents of infrastructure being targeted by cyber-attacks became a reality in South Korea, demonstrating how critical operations can be impacted on a broad scale.
- Unsupported software: 2013 saw increased awareness regarding unsupported versions of Java and Windows XP, which will present widespread security challenges as patches and upgrades cease when support for XP ends April 2014.

To read more click **HERE**

Europe seeks expanded role in running the Internet

Fox News, 12 Feb 2014: European authorities are calling for changes to how the Internet is regulated, following a series of revelations about the U.S. National Security Agency's surveillance practices. The revelations about efforts from U.S. spy agencies to tap into the very backbone of the Internet have shaken worldwide faith in online privacy, leading Europe's multinational governing body the European Commission to suggest that the world revisit how the Web is maintained. 'The next two years will be critical in redrawing the global map of Internet governance.' - European Commission vice-president Neelie Kroes "The next two years will be critical in redrawing the global map of Internet governance," Commission Vice-President Neelie Kroes said in a statement. "Europe must contribute to a credible way forward for global Internet governance. Europe must play a strong role in defining what the net of the future looks like." The Internet was invented in the United States and is currently run by a non-governmental organization called the Internet Corporation for Assigned Names and Numbers (ICANN), established in 1998 and headquartered in Los Angeles. Now the EC is seeking "a clear timeline for the globalization of ICANN" and commitments to transparency and security. The EC push is the latest effort to wrest control of the Internet from ICANN and the United States, a movement spearheaded by the United Nations through a body known as the International Telecommunications Union. A global outcry followed revelations in 2012 that the ITU sought to regulate the Internet, which U.S. representatives feared could have led to content censorship. Kroes said the EC isn't in favor of regulation from the UN agency. "We are rejecting a United Nations or governmental take-over of Internet governance. We want geographic balance, not government control. We want a timeline to globalize ICANN governance. And we want to make sure everyone has a voice in the debate," she said. Nigel Hickson, a vice president at ICANN, said the American agency hopes to maintain its governance approach, which enables private companies, technical experts and the public to advise the agency. "ICANN is pleased that the European Commission in this important communication is emphasizing the need to sustain the multi-stakeholder approach to governing the Internet. It is an approach that is defined by global inclusivity, where voices from business, government and independent Internet users are welcome," Hickson said in an email. "We are looking forward to working together with all relevant global parties … to create policy solutions aimed at keeping the Internet open and unified, which is vital for the growth of national economies." Tuesday was labeled a global day of protest against online

surveillance, with over 5,000 websites joining in a protest called The Day We Fight Back. Participants were asked to post banners of support and encouraging people to contact their representatives in Congress to get behind the USA Freedom Act, legislation proposed by Rep. Jim Sensenbrenner (R-Wis.) and Sen. Patrick Leahy (D-Vt.). The bill would put curbs on the NSA's domestic surveillance practices, particularly on the use of the massive database of U.S. communications it has been building. To read more click **HERE**