THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

4 November 2014

October 31, Softpedia – (International) **Upatre malware dropper sent to Bitstamp exchange users.** Researchers with ThreatTrack identified an email campaign targeting users of the Bitstamp digital currency exchange that uses sophisticated social engineering to attempt to trick users into opening an attachment containing the Upatre malware dropper. The dropper then adds the Dyre (also known as Dyreza) banking malware to compromised systems. Source: http://news.softpedia.com/news/Upatre-Malware-Dropper-Sent-to-Bitstamp-Exchange-Users-463703.shtml

November 1, Meade County Times-Tribune; Rapid City Journal – (South Dakota) **Meade School District dealing with information breach.** South Dakota's Meade School District discovered a computer breach October 30 caused by an internal computer error that made hundreds of Social Security numbers of former students available online by allowing access to the district's transcript server. Authorities worked to determine the origin of the breach and correct the issue. Source: http://rapidcityjournal.com/news/meade-school-district-dealing-with-information-breach/article_270ad32f-f63c-5f66-8331-391ec0d6b2a8.html

November 3, The Register – (International) **VMware: Yep, ESXi bug plays 'finders keepers' with data backups.** VMware confirmed an issue reported by users of its ESXi 4.x and ESXi 5 hypervisor where virtual machines with Changed Block Tracking (CBT) enabled and that have been increased in size by more than 128GB show an inaccurate list of allocated virtual machine disk sectors, which could cause backed-up data to be unrecoverable. VMware recommended that users disable and then re-enable CBT and stated that the company is working on a permanent solution. Source: http://www.theregister.co.uk/2014/11/03/vmware_data_gobbling_bug/

November 3, SC Magazine – (International) **Researchers notice uptick in 'Poweliks' trojan infections.** Symantec researchers observed an increase in reported Poweliks trojan infections, with the malware delivered by spam emails, exploit kits, and a spam campaign that impersonates the U.S. Postal Service and Canadian Post. Source: http://www.scmagazine.com/researchers-notice-uptick-in-poweliks-trojan-infections/article/380746/

October 31, Securityweek – (International) **New RAT hijacks COM objects for persistence, stealthiness.** Researchers at G DATA Software's SecurityLabs identified a new remote access trojan (RAT) dubbed COMpfun that hijacks legitimate Component Object Model (COM) objects to evade detection by security software. The RAT is capable of executing code, logging keystrokes, downloading or uploading files, and other tasks. Source: http://www.securityweek.com/new-rat-hijacks-com-objects-persistence-stealthiness

FBI investigating 'Cryptowall' malware

The Examiner, 3 Nov 2014: The U.S. Bureau of Investigations (FBI) is reportedly investigating a computer virus called Cryptowall that has infected over 800,000 computers worldwide since February. Nearly one third of computers affected by the malicious virus are in the United States. According to an ABC News report on Monday, cyber-criminals or hackers employ Cryptowall malware to kidnap victims computer files and essentially hold them hostage. If victims want the computer

files back, they must pay a ransom – in bitcoins, the untraceable currency as mysterious to victims as Cryptowall itself. To date, CryptoWall victims have paid more than $1 million to the hackers to regain access to their kidnapped information. In June, the New York Times reported on Cryptowall, warning that ransom-ware similar to Cryptolocker was quickly spreading. Cryptolocker infected 300,000 computers before the FBI and international law enforcement were able to take it down. Cryptowall file-encrypting ransomware was first identified in April, 2014. A cyber threat researcher for SophosLabs, Anand Ajjan said both CryptoWall and CryptoDefense have the same code, and the only difference is the name. However, CryptoWall's encryption can't be reversed without the key. Previous ransomware attacks used social engineering in spam to trick you into downloading the malware. The more sophisticated CryptoWall can access your computer files just by visiting a website that is rigged up with an exploit kit. Since a public and private key combination is needed to decrypt files, it is impossible to recover affected files but the Windows system restore feature can restore your computer to the last saved restore point before the Cryptowall virus. In Windows Vista and Windows 7, the feature is called 'Previous Versions." The Durham, New Hampshire Police department's entire computer system was wiped out on June 5, when an officer received what appeared to be a legitimate message from a known contact. The officer clicked a link in the email and unknowingly downloaded the CryptoWall malware. In June, 2012, the U.S. Department of Homeland Security issued a warning to American businesses about a computer virus dubbed the "Flame," a sophisticated data-stealing worm responsible for a cyber attack on Iran's oil industry. Cyber security experts said "the Flame" had the same code as the Stuxnet virus, which was responsible for destroying several centrifuges used for Iran's nuclear enrichment program in 2010. The "Flame" was active for up to two years before it was identified by security experts. In addition to continuous breaches of security at U.S. businesses including retailers and banks, repeated cyber attacks on U.S. government and military websites, including the Department of Defense, Department of Justice, FBI and other law enforcement agencies has sparked a sense of urgency by cyber security officials to address threats to U.S. computer networks. In December, 2012, former National Security Agency (NSA) director, John "Mike" McConnell said United States officials have been repeatedly warned about the threat of potential cyber attacks that could have a tremendous negative impact on the country. In November 2011, then Chairman of the Joint Chiefs of Staff, General Martin Dempsey spoke of constant breaches to U.S. cyber-security at a forum in London. Dempsey said "we're under constant attack every day." To read more click **HERE**

25,000 employees' private records compromised and millions of dollars lost

The Salt Lake Tribune, 4 Nov 2014: A cyberattack similar to previous hacking intrusions from China penetrated computer networks for months at USIS, the government's leading security clearance contractor, before the company noticed, officials and others familiar with an FBI investigation and related official inquiries said. The breach, first revealed by the company and government agencies in August, compromised the private records of at least 25,000 employees at the Homeland Security Department (DHS) and cost the company hundreds of millions of dollars in lost government contracts. In addition to trying to identify the perpetrators and evaluate the scale of the stolen material, the government inquiries have prompted concerns about why computer detection alarms inside the company failed to quickly notice the hackers and whether federal agencies that hired the company should have monitored its practices more closely. A computer forensics analysis by consultants hired by the company's lawyers defended USIS' handling of the breach, noting it was the firm that reported the incident. The analysis said government agencies regularly reviewed and approved the firm's early warning system. In the analysis, submitted to federal officials in September and obtained by the AP, the consultants criticized the government's decision in August to indefinitely halt the firm's background investigations. USIS reported the cyberattack to federal authorities on June 5, more than two months before acknowledging it publicly. The attack had hallmarks similar to past intrusions by Chinese hackers, according to people familiar with the investigation. In March, hackers traced to China were reported to have penetrated computers at the Office of Personnel Management, the federal agency that oversees most background investigations of government workers and has contracted extensively with USIS. The possibility that national security background investigations are vulnerable to cyber-espionage could undermine the integrity of the

verification system used to review more than 5 million government workers and contract employees. "The information gathered in the security clearance process is a treasure chest for cyber-hackers. If the contractors and the agencies that hire them can't safeguard their material, the whole system becomes unreliable," said Alan Paller, head of SANS, a cybersecurity training school, and former co-chairman of DHS' task force on cyber-skills. The Office of Personnel Management and the Department of Homeland Security indefinitely halted all USIS work on background investigations in August. OPM, which paid the company $320 million for investigative and support services in 2013, later decided not to renew its background check contracts with the firm. The move prompted USIS to lay off its entire force of 2,500 investigators. Last month, the federal Government Accounting Office ruled that Homeland Security should re-evaluate a $200 million support contract award to USIS. The GAO advised the department to consider shifting the contract to FCi Federal, a rival firm. To read more click **HERE**

Fileless Poweliks Malware Distributed through Spam and Exploit Kits

Softpedia, 4 Nov 2014: The amount of reports involving Poweliks Trojan has been growing lately as the cybercriminals behind the threat appeal to different distribution methods, spam being the most prevalent at the moment. Poweliks is not a regular piece of malware because it resides in the memory of the system and stores absolutely no file on the disk, making it more difficult to detect. After compromising the computer, the malware creates registry entries with commands that verify for the presence of PowerShell or .NET Framework and for executing the payload. Security researchers at Symantec have observed that the Trojan has been delivered through spam emails lately, purporting to be sent by the Canadian Post or the US Postal Service. The lure consists in details about a missed package delivery. Poweliks is not a new form of malware as it was documented by researchers at German security vendor G Data at the end of July. Furthermore, the Trojan was spotted to be delivered by Angler Exploit Kit by French vulnerability researcher Kafeine; he saw the payload being delivered to unsuspecting users since September. However, unlike the discovery made by G Data, the sample found by Kafeine did not achieve persistency and would be eliminated at the next computer restart because no registry entries were created to allow the malware to start with the operating system. To read more click **HERE**

NIST Guide to Cyber Threat Information Sharing is open for comments

Heise Security, 30 Oct 2014: NIST has announced the public comment release of Draft Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing. The purpose of this publication is to assist organizations in establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle. The publication explores the benefits and challenges of coordination and sharing, presents the strengths and weaknesses of various information sharing architectures, clarifies the importance of trust, and introduces specific data handling considerations. The goal of the publication is to provide guidance that improves the efficiency and effectiveness of defensive cyber operations and incident response activities, by introducing safe and effective information sharing practices, examining the value of standard data formats and transport protocols to foster greater interoperability, and providing guidance on the planning, implementation, and maintenance of information sharing programs. NIST is asking the public to comment on the draft by November 28, 2014. They are to be sent to sp800-150comments(at)nist.gov. To read more click **HERE**

Extracting data from air-gapped computers via mobile phones

SoftPedia, 4 Nov 2014: A group of researchers from the Department of Information Systems Engineering at Ben-Gurion University in Israel have demonstrated and detailed a technique that can allow attackers to exfiltrate data from an "air-gapped" computer. More often than not, computers housing sensitive data - whether it belongs to the government, a business, or any other type of organization - are kept off the Internet and internal networks and have their Bluetooth feature switched off in order to prevent attackers easily reaching and compromising them and the information they hold. Often, even those individuals that are allowed to access or simply be in the vicinity of these computers are prohibited of having a mobile phone with them, which is usually left in a locker somewhere on the premises, but not very near to the

place where these computers are located. Still, this security procedure can be violated, by accident or on purpose, and mobile phones might be brought close enough to be used in an attack. The researchers dubbed their technique "AirHopper." The premise for making it work is that the attacker has already compromised the computer containing the sensitive data, and is now looking for a way to exfiltrate it in without anyone noticing. "While it is known that software can intentionally create radio emissions from a video display unit, this is the first time that mobile phones are considered in an attack model as the intended receivers of maliciously crafted radio signals," they explained in their paper. They proved that a mobile phone with an FM radio receiver - whether it belongs to the attacker or to an individual working in the organization, oblivious that his phone has been compromised - can be used to extract the data by collecting the radio signals emanating from the compromised computer. Their research proved that textual and binary data can be exfiltrated from physically isolated computer to mobile phones at a distance of 1-7 meters- The transfer of the data is relatively slow - 13-60 Bps - but still fast enough to extract things like passwords. There are ways to prevent this type of attack. "Countermeasures of the technical kind include physical insulation, software-based reduction of information-bearing emission, and early encryption of signals. Procedural countermeasures include official practices and standards, along with legal or organizational sanctions," the researchers noted. To read more click **HERE**

OS X Yosemite sports serious privilege escalation bug

Softpedia, 4 Nov 2014: A Swedish researcher has unearthed a serious bug that affects the newest version of OS X - version 10.10, or Yosemite - and which could allow attackers to gain complete control of the target's Mac machine. It's a privilege escalation bug he dubbed Rootpipe, but declined to explain why, as the explanation could reveal details that would help attackers find it and create an exploit. The existence of the flaw has been indirectly confirmed by Apple when they asked the researcher to delay publishing details about it until January 2015, after a fix for the bug is released and pushed out to users. TrueSec researcher Emil Kvarnhammar says he found the flaw while preparing for two security events at which he wanted to demonstrate one. As not many POC for OS X bugs are published and most affect older versions of the OS, he thought he would try to find one himself. He admits that he was surprised that he found one after only a few days of binary analysis. "I started looking at the admin operations and found a way to create a shell with root privileges," he told Magnus Aschan. "Normally there are 'sudo' password requirements, which work as a barrier, so the admin cant gain root access without entering the correct password. However, Rootpipe circumvents this." The flaw is present in OS X versions 10.8, 10.9 and 10.10 (Beta 6), and TrueSec released a demo of the exploit: Users can protect themselves by setting up a new account without administrative permissions and use that one until a patch for the flaw is released, says Kvarnhammar, and adds that it's a good idea to for them to use Apple's FileVault hard drive encryption tool. To read more click **HERE**

Risky file sharing practices can cause data loss and compliance violations

Softpedia, 4 Nov 2014: Organizational leadership is failing to respond to the escalating risk of ungoverned file sharing practices among their employees, and that employees routinely breach IT policies and place company data in jeopardy, according to the Ponemon Institute. "Data leakage and loss from negligent file sharing is now just as significant a risk as data theft," noted Larry Ponemon, chairman of the Ponemon Institute. "While most companies take steps to protect themselves from hacking and other malicious activities, these same organizations are entirely unprepared to guard against risky and ungoverned file sharing using consumer-grade applications like Dropbox." The research found that file sharing poses a major threat to enterprise security, and that senior managers at organizations are having difficulty setting and enforcing effective policies to safeguard against data leakage. Many organizations are vulnerable to both data loss and non-compliance due to cloud file sharing and improper file sharing practices – and it starts from the top down. Further, it is clear that the enterprise IT department has lost control of user application decision-making, as well as of company data.

More than 1,000 IT security professionals from the United States, United Kingdom, and Germany were surveyed. Key findings from the report include:

- Almost half (49 percent) of respondents believe their company lacks clear visibility into employees' use of file sharing/file sync and share applications.
- Half of respondents (51 percent) aren't convinced their organizations have the ability to manage and control user access to sensitive documents and how they are shared.
- The majority of organizations have policies governing the use of file sharing, but policies are not being communicated to employees effectively.
- Only 54 percent of respondents say their IT department is involved in the adoption of new technologies for end users, including cloud-based services.
- More sobering, approximately 61 percent of respondents confessed that they have "often or frequently" done the following:
- Accidentally forwarded files or documents to individuals not authorized to see them.
- Used their personal file-sharing/file sync-and-share apps in the workplace.
- Shared files through unencrypted email.
- Failed to delete confidential documents or files as required by policies.

Ponemon's research concludes that these file-sharing issues are making enterprises extremely vulnerable to data loss and compliance violations. This vulnerability is heightened for regulated industries like financial services, where the risks and repercussions of data loss are more severe. The research also showed that employees are acting badly when it comes to data sharing and collaboration, routinely violating IT policy in order to get things done faster. Survey respondents indicated a lack of senior-level accountability in their organizations for developing and implementing file-sharing policies. Of senior level respondents, 44% did not believe they had the ability to manage and control user access to sensitive documents and how they are shared. Among respondents who do have that ability, their confidence in asserting it was mixed. To read more click **HERE**

Cybersecurity priorities shift to insider threats

Federal Times, 3 Nov 2014 A survey of government IT professionals finds that training to prevent cyber security threats is an investment priority for more than 60 percent of federal civilian and defense/military organizations. (Fort Meade Alliance) A survey of federal IT managers in both the civilian and defense sectors showed a shift in cybersecurity concerns from outside actors to insider threats and a focus on the need to educate employees. The survey — commissioned by the Fort Meade Alliance and conducted by Market Connections, Inc. — posed five questions to 200 federal IT decision-makers about the biggest challenges and opportunities they saw in the cybersecurity realm. While intentional leaks like the information released by former intelligence contractor Edward Snowden put the focus on malicious internal threats, IT managers expressed more concern with issues surrounding misuse and accidental data leakage. Not following proper cyber hygiene policies ("misuse") was the No. 1 security concern among IT decision-makers, with 52 percent characterizing it as a "prolific" threat. Accidental leaks (i.e., copying the wrong person on an email) was fifth on the list, with 39 percent of respondents claiming it is an issue. Phishing, malware and spam tactics were second (49 percent), third (47 percent) and fourth (42 percent), respectively, among the most "prolific cyber threats plaguing" agencies. Data breaches and cyber espionage were further down the list, at 33 percent and 15 percent, respectively. Conversely, a 2012 survey found that only 40 percent were wary of misuse as a security issue at that time, while 25 percent were concerned with cyber espionage and 59 percent with malware attacks. Respondents ranked new security systems as the No. 1 investment opportunity in the coming year (66 percent), with employee training (61 percent) and implementation of new policies (57 percent) close behind. While 61 percent of those surveyed named training as an investment priority, this was significantly higher among IT managers on the defense side. Some 71 percent of respondents in the defense sector cited end-user training as a priority, compared to 55 percent among civilian agencies. To read more click **HERE**

Persistent cyberattacks of U.S. companies on the rise

Washington Times, 3 Nov 2014: Economic cyberwarfare is on the rise as cyberattacks on U.S. companies are increasing in both frequency and severity. And costs are mounting. Much like a computer virus compares to an infectious virus in humans, there is a battle between treating the symptoms versus treating the disease when it comes to funding; along with a sheer lack of knowledge and concern by some. Companies must do more to increase their resiliency from attack, and fight to stay ahead in cybersecurity. Over the last year, cyberattacks have compromised financial and personal data — both corporate and consumer — maintained by big-name companies such as Target, Home Depot, J.P. Morgan Chase, eBay, Apple, Yahoo!, UPS, P.F. Chang's and Dairy Queen. Malware, such as the Backoff malware, has infected more than 1,000 U.S. businesses. According to FBI Director James Comey, "There are two kinds of big companies in the United States. There are those who've been hacked and those who don't know they've been hacked." Corporations are both the leading source of new technology and the backbone of growth through innovation. It is imperative that they continue to play a leading role in cybersecurity. By sharing information and working cooperatively with each other, government entities and international partners, U.S. companies can help mitigate cyberthreats. Congress and the administration must help to create an environment where cyberthreats are taken seriously and corporations willing to help can share security-enhancing information risk-free. Companies who find themselves early targets of such attacks can help others using similar systems to prepare for and repel such attacks by sharing the knowledge they have gained in the course of identifying and dealing with the assault. Rule makers must be wary of saddling companies with overbearing cybersecurity regulation, as this can be counterproductive. Just before convening last week's Third Annual Cybersecurity Summit, the U.S. Chamber of Commerce penned a letter to the U.S. Securities and Exchange Commission warning that increased regulation would damage the relationship between U.S. businesses and government and their ability to counter persistent attacks. Cyberthreats extend beyond national boundaries, and so must cybersecurity cooperation. According to a PwC survey, global IT security incidents grew 48 percent, to 42.8 million, in 2014. The recent attack on J.P. Morgan reportedly originated in Russia. The attacked that compromised 4.5 million patient records at Community Health Services is thought to have come from China. Recent reports by network security company FireEye and cyber analytic company Novetta tell of the very real threat from two sophisticated cybergroups: Russia's APT28 and China's Axiom. The costs associated with cyberthreats vary widely, but they are significant at any level. From intellectual-property theft to denial-of-service attacks, the cost of cybercrime in the U.S. can vary from $1.6 million to $60 million per company, and is growing every year. Meanwhile, the global cost of cybercrime is estimated as high as $575 billion in 2013. Yet, there is no 100 percent security against loss. Cyberinsurance is becoming an important tool for businesses to mitigate losses from the increasing number of breaches and attacks by sophisticated, state-sponsored aggressors. Cyberrisks have become pandemic. They threaten all of us on a daily basis, whether we are aware of it or not. By promoting information sharing, cybersecurity insurance, and collaboration in combatting cyber crime, Congress and the administration can help create an environment for improved commercial cybersecurity. Cybercriminals will only continue to expand their activities. Cooperative, voluntary partnerships are the most nimble, effective means of fighting back. To read more click **HERE**