[redacted] Cyber-Threat Newsletter – 01 Feb 16

Patches & Updates of the Week:

(U) Lenovo blunder means '12345678' used as password for default file sharing app
Lenovo has been forced to release urgent software fixes after a number of embarrassing flaws were uncovered in its products, including one that left a hard-coded password set to '12345678' by default. Researchers at Core Security posted an advisory that listed four vulnerabilities in Lenovo's ShareIT function that could result in man-in-the-middle attacks, information leaks and the bypassing of encryption. ShareIT is a free Lenovo application that lets users share files and folders between computers, smartphones, and tablets. The flaws affect ShareIT for Android 3.0.18 and Windows 2.5.1.1. Other products and versions may also be affected, but they were not tested. Core Security revealed that the problems were reported to Lenovo in October, and the fixes were finally rolled out on 25 January. (v3.co.uk, 27Jan16)

(U) Intel fixes security bug to prevent attackers from hijacking the driver update process
Intel has released version 2.4 of the Intel Driver Update Utility, fixing a critical security flaw (CVE-2016-1493) that enabled attackers to intercept driver updates and serve malware instead. The Intel Driver Update Utility is a desktop application which Intel users can install and automate the driver update process. The utility works by scanning a user's PC, detecting all Intel devices, checking to see if there's a newer version for the devices' drivers, and then downloading, installing, and updating the older drivers. What security researchers from CoreSecurity discovered is that this utility was using HTTP to contact Intel's download servers. The attacker could serve up malware instead of the proper Intel drivers, and the Intel Driver Update Utility would automatically download the files and automatically launch them into execution, all with system-level privileges, which a driver update utility usually requests from users when it's installed. Affected Intel Driver Update Utility versions are 2.0, 2.1, 2.2, and 2.3. To be on the safer side of this bug, download and replace your older versions with v2.4. (Softpedia, 21Jan16)

Threats & Vulnerabilities of the Week:

(U) Beware of Facebook "Security System Page" scams


Facebook users have lately become targets of phishers who are not satisfied with stealing the users' login information, but they want their security questions and payment card information as well. These crooks are trying to make the targets believe their Facebook account has been reported by other users and will be disabled in they don't "verify" it by entering their login credentials: Once they do this, they are asked to "upgrade" their credit card information: The colour and font scheme used for these pages usually reminds of Facebook's, but a look at the page's URL should make clear to everyone that this page has nothing to do with the popular social network. Unfortunately, there are people who panic and forget to look for such things, or simply don't know what to look for in order to spot a fake, and this is why security outfits often report on these scams -- to educate users. A slew of these fake "security pages" have been taken down recently, but new ones are sure to pop up soon (if they haven't already). As long as there are people that fall for these schemes, they will continue to crop up. (net-security.org, 27Jan16)

(U) Versatile Linux backdoor acts as downloader, spyware
Another Linux Trojan has been discovered by researchers, and this one is pretty versatile: it opens a backdoor into the infected device, can download and run additional malicious files, and can spy on users by logging keystrokes and making screenshots. Dr. Web researchers dubbed it Xunpes, and it consists of two components: a generic dropper and the actual backdoor, which gets saved into the /tmp/.ltmp/ folder after the dropper is launched. "Once launched, the backdoor written in C decrypts the configuration file using the key that is hard-coded in its body. Its configuration parameters include a list of C&C servers and proxy servers' addresses and other information necessary for the correct operation of the malicious program. After that, the Trojan establishes connection to the server and waits for commands from cybercriminals," the researchers explained. The Trojan can be made to execute over 40 commands sent by the attacker. Among these are to get a decryption of future commands from the server, remove itself, download files and execute them, terminate the backdoor, create, open, copy, rename, delete files and folders, run bash commands, generate KeyPressed and ButtonRelease events, take screenshots and log keystrokes and send it all to the C&C server, and much more. It's interesting to note that the dropper also displays a curious login box, asking the user to enter their login and password. (net-security.org, 25Jan16)

(U) Web reconnaissance attack infects 3,500 websites
Alarms are ringing in Symantec's offices, as its research team has discovered a massive Web injection campaign that's currently infecting Web servers around the Internet. According to telemetry data received from Symantec security products, the company's staff has identified a common pattern in the source code of many websites. Since the beginning of the year, unknown attackers have started adding the same piece of JavaScript code to multiple websites that should not be connected in any way. Symantec estimates this number to be around 3,500, with over 75 percent hosted in the US, and the rest in India, the UK, Italy, Japan, France, Canada, Russia, Brazil, and Australia. Most of the infected websites belong to private businesses, educational institutes, and government websites. The unauthorized code added at the top of the websites is not malicious, but Symantec says it's collecting private data on visitors, like user IP, page title, page URL, URL referral, Flash version, user language settings, and screen resolution. The most simple explanation is that attackers are currently in the attack's early stage where they're collecting data on website visitors, which they will later use to select the appropriate attack type for each infected site's visitors base. It would be extremely easy for attackers to replace the current unauthorized code with something more malicious that redirects users to an exploit kit, and from there, deliver banking trojans, adware or ransomware. (Softpedia, 22Jan16)

(U) "Deliberately hidden" backdoor found on US government's comms system

Researchers from Austrian infosec outfit SEC Consult have unearthed what they dubbed a "deliberately hidden backdoor account" in NX-1200, a network controller appliance for conference rooms manufactured by AMX, which is used by governmental and military bodies (even the US White House), educational and healthcare institutions, hotels and conference centers all over the US. Subsequent research showed that other 30+ solutions by AMX also contain the backdoor. According to the researchers, they discovered a function that sets up a subtle administrative user account named BlackWidow to the internal user database: "This account can be used to log on to the web interface as well as SSH. Functions to retrieve a list of all users in the database were found to deliberately hide this user. Further, using this backdoor account grants additional features on the remote-client, such as a facility to capture packets on the network interface which not even an administrator account can perform," they explained in the advisory. After they contacted AMX and shared their finding, the company shipped a fix for the backdoor after seven months. Unfortunately, as the researchers found, the fix removed the BlackWidow backdoor account and created another one named "1MB@tMaN," with the exact same capabilities. After failing to get in touch with the company again (to point out the "no-fix" fix), the researchers decided to go public with their discovery (but did not share the password for the backdoor account). AMX did get in touch with the company on Wednesday, and informed them that they released firmware updates for the affected products. "Removed debugging account to prevent security vulnerability," the notes accompanying the update say. SEC Consult has yet to check the update to see that the issue is satisfactorily fixed. In the meantime, the AMX spokesman had this to say by way of an explanation: "First, 'Black widow' was an internal name for a legacy diagnostic and maintenance login for customer support of technical issues. Commonly used in legacy systems, it was not 'hidden' as suggested, nor did it provide access to customer information. While such a login is useful for diagnostics and maintenance, during our routine security review in the summer of 2015, we determined that it would be prudent to eliminate this feature as part of a comprehensive software update. We informed our customers and the update was deployed in December 2015. '1MB@tMaN' was an entirely different internal feature that allowed internal system devices to communicate. It was not an external login nor was it accessible from outside of the product. The '1MB@tMaN' internal system device capability also was not related to nor a replacement for the 'Black Widow' diagnostic login. The only connection was the fact that our software update that eliminated 'Black Widow' also provided an update to the '1MB@tMaN' internal capability that eliminated this name. In terms of the names, these were light hearted internal project names that our programmers used with no intended meaning. We take security very seriously and are continuously testing our own systems and capabilities and developing more sophisticated updates." (net-security.org, 22Jan16)

(U) Fake Facebook emails deliver malware masquerading as audio message

A new spam campaign is targeting Facebook users. It uses the same approach as the recent one aimed at WhatsApp users, and Comodo researchers believe that the authors of both campaigns are likely the same. The fake emails are made to look like an official communication from the popular social network, and their goal is to make the victims believe they have received a voice message: As in the previous WhatsApp campaign, the subjects of the emails contain a set of random characters (e.g. "An audio announcement has been delivered! Lucqmc", "You got a vocal memo! Fcqw"). "These are most likely being used to bypass antispam products rather than identify the user," the researchers posited. The attachment that the recipients are urged to download and open contains a malicious executable -- a variant of the Nivdort information-stealing Trojan. Once run, the malware will automatically replicate itself into "C:\" directory and add a Windows Registry entry that will allow it to run automatically after each restart or shutdown of the machine. It also attempts to prevent users from accessing websites of AV vendors (by modifying the Windows Hosts file) and attempts to disable Firewall notifications from the Windows Security Center (with another Windows Registry modification), which may make it difficult to spot and remove. "In this age of cyberattacks, being exposed to phishing is a destiny for every company, well-known or not. It may not be the most groundbreaking attack method cybercriminals use -- but there's no denying that they're becoming more clever when crafting their messages," noted Fatih Orhan, Director of Technology for Comodo and the Comodo Threat Research Lab. "More frequently, they're using 'too good to be true' promises and action-oriented language in the subject lines to entice recipients to open the emails, click the links or attachments and spread the malware". (net-security.org, 21Jan16)

(U) Nest, other IoT devices, sends user info in the clear

Researchers at Princeton University's Center for Information Technology Policy (CITP) found security vulnerabilities in many of the most popular IoT devices that they looked at, including Google's Nest Thermostat. Ph.D. student Sarthak Grover and CITP fellow Roya Ensafi found that most of the devices leak user information. Nest was found to leak the zip code of the weather station that users enter when configuring the device, unencrypted over the Internet. In most cases, the information leaked by the Nest thermostat is the same as the zip code of the device owner. As CITP acting director Nick Feamster asked in a CITP blog post, "When would a user ever enter a zip code other than that of their home, where the thermostat was located?" At a presentation at the Federal Trade Commission (FTC) PrivacyCon conference, Grover warned that IoT devices can leak sensitive information, including whether device owners are at home and the activities of the device owners. "The devices inside the home send all of the information to the cloud," he said during his talk. "In fact, if you have two devices in the home and they want to talk to each other, currently they will talk to the cloud and the information will get back to the home." Many other IoT devices were found to leak even more sensitive information than Nest's thermostat. The research team also examined the Belkin WeMo Switch, Ubi Smart Speaker, Sharx Security Camera, PixStar Digital Photoframe, and Smartthings hub. PixStar's Digital Photoframe, for example, a digital photo display that loads pictures from users' Facebook accounts, sends all information unencrypted, or in the clear. (scmagazine.com, 21Jan16)

(U) Authorized Symantec reseller scams users into buying security software
Malwarebytes researchers have discovered a new tech support scam that, unlike most, is being perpetrated by an active member of the Symantec Partner Program. Users are being tricked into visiting a web page sporting a fake warning imitating those shown by Symantec's Norton AV, and urged to contact tech support via a "support toll free helpline": Calling the offered phone number will get the victims in touch with a "support technician" that first instructs them to visit a website that will allow him to gain remote control of the computer, and will then open and show them the Windows EventViewer. "Sadly, Microsoft's central log and error reporting tool can all too easily be leveraged thanks to those yellow and red warnings, which the majority of the time are perfectly normal. Of course, for a scammer it's the perfect way of claiming those are infections or viruses," says Malwarebytes' Jerome Segura. The technician has also other tricks up his sleeve to "prove" that the computer is infected, and ultimately offers the victims to install the Norton AV solution and fix the problem for $199, or an even more extensive service for an additional $50 more: All in all this is a typical tech support scam, and the only thing that makes it stand out is the fact that it seems to be perpetrated by a company that is a current Symantec business partner that's authorized to sell the company's products, including maintenance services and support. "It is a sad state of affairs when tech support scammers are not ashamed of using lies to sell their products and services but also double cross their partners, thereby inflicting brand and reputation damage," Segura pointed out.,The company -- Silurian Tech Support, Inc. -- has been reported to Symantec, and its website has been taken down shortly after. (net-security.org, 21Jan16)

(U) Threat group uses dating sites to build a botnet of vulnerable home routers
At least five dating websites may be involved in an attack scenario that is spreading a worm to site visitors, infecting their home router and adding it to a botnet. The worm is a variant of TheMoon, which was first discovered in February 2014, and works by taking advantages of weaknesses in the HNAP (Home Network Administration Protocol) protocol. Attackers are using one-night stand dating sites to spread the worm. On each malicious website, the infection occurs via a two-step phase launched via a malicious iframe embedded on the page. This worm prevents users from using some of the router's inbound ports, and it also opens outbound ports through which it spreads to other routers. Neither in 2014 nor in late 2015, when Damballa researchers came across this threat, did the worm have a C&C infrastructure behind it. This means the botnet is currently only in its incipient or testing stages, spreading to affected devices, in an attempt to build a larger infrastructure, which may be useful later down the road. This theory is also validated by the fact that, towards the end of the year, the worm's second-stage iframe URL was disabled, and the ELF binary removed from the download servers. "There are different scenarios on how the criminals could bring their victims to visit an affected website via malvertising, exploit kits or phishing email. The criminals moved from scanning IP ranges for potential vulnerable home routers to embedding the attack on a website," Damballa's Loucif Kharouni explains. "It feels like this conversion to a web-based attack is new and under construction." Damballa reports that the new TheMoon worm sample is not currently detected by any antivirus maker. The security vendor also tracked down the owner of the malicious dating site used to spread the worm and found out that he's also the man behind four other dating sites of the same nature. The company does not believe him to be the actual criminal behind this new botnet and thinks his identity was stolen and used illegally to register the domains. In 2014, security researchers discovered that most of the vulnerable devices were various models of Linksys DLink home routers. (Softpedia, 21Jan16)

(U) Old, unpatched flaws exploited to achieve control of Windows systems, networks
Foxglove Security researcher Stephen Breen has demonstrated that you don't need to exploit a 0-day or even a recently discovered vulnerability to gain the highest level of privilege available on a Windows machine (Windows 7, 8, 10, Server 2008, Server 2012). "This is important because many organizations unfortunately rely on Windows account privileges to protect their corporate network," Breen explained. "Often it is the case that once an attacker is able to gain high privileged access to ANY workstation or server on a Windows network, they can use this access to gain "lateral movement" and compromise other hosts on the same domain." He achieved it by concatenating exploits for three known vulnerabilities, some of which were discovered as far back as 2000, but were never fixed because a fix would break backward Windows compatibility. "The exploit consists of 3 main parts, all of which are somewhat configurable through command-line switches. Each part corresponds to an already well known attack that has been in use for years," the researcher explains and adds that part of the attack code they used was "shamelessly borrowed" from a previous PoC exploit published by Google Project Zero. The three steps of the attack are as follows: 1)NBNS spoofing (NBNS is a broadcast UDP protocol for name resolution commonly used in Windows environments) 2)Setting up a fake WPAD (Web Proxy Auto-Discovery Protocol) proxy server 3)NTLM relay attack. The researcher admits that the exploit will not work always and on all Windows versions the same way. "It is also a bit flaky sometimes, due to the quirks in how Windows handles proxy settings and the WPAD file," he noted. "Often when the exploit doesn't work, it is required to leave it running and wait. When Windows already has a cached entry for WPAD, or is allowing direct internet access because no WPAD was found, it could take 30-60 minutes for it to refresh the WPAD file. It is necessary to leave the exploit running and try to trigger it again later, after this time has elapsed." Breen says that enabling "Extended Protection for Authentication" in Windows should stop NTLM relay attacks (the last stage of the attack). (net-security.org, 21Jan16)

Incidents of Interest:

(U) Israel's power grid hit with ransomware
Speaking at the Cybertech 2016 Conference, Israel's Minister of Infrastructure, Energy and Water, Yuval Steinitz, told the crowd that the country's power grid was the target of a cyberattack that took place this past Monday, 25 January. "The virus was already identified and the right software was already prepared to neutralize it. We had to paralyze many of the computers of the Israeli Electricity Authority," said Mr. Steinitz, quoted by The Times of Israel. While Mr. Steinitz made it look like a targeted cyber-espionage campaign that involved spyware and other malicious trojans, Israeli tech site ynet (Google Translate link) got to the bottom of the incident and discovered it was only a ransomware infection. The chances are that the people behind it were only after the money and did not specifically target Israel's electrical grid in any way or form. Ransomware can't impact Israel's power grid enough to bring it down because it does not have the capabilities to do so. Most ransomware will at best lock down a computer by encrypting sensitive files. At government institutions, most of the data is backed up anyway, and in a power supply company, sensitive ICS/SCADA equipment can be decoupled from infected computers if necessary and controlled through another PC. (Softpedia, 27Jan16)

(U) Hackers may have wider access to Ukrainian industrial facilities

Hackers were able to attack four sections of Ukraine's power grid with malware late last year because of basic security lapses and they could take down other industrial facilities at any time, a consultant to government investigators said. Three power cuts reported in separate areas of western and central Ukraine in late December were the first known electrical outages caused by cyber attacks, causing consternation among businesses and officials around the world. The consultant, Oleh Sych, told Reuters a fourth Ukrainian energy company had been affected by a lesser attack in October, but declined to name it. He also said a similar type of malware had been identified by the Ukrainian anti-virus software company Zillya! where he works as far back as July, making it impossible to know how many other systems were at risk. "This is the scariest thing -- we're living on a powder keg. We don't know where else has been compromised. We can protect everything, we can teach administrators never to open emails, but the system is already infected," he said. Ukraine has also been targeted in other cyber attacks, which included hacking into the system of Ukraine's biggest airport and TV news channels. Security services and the military blamed the attacks on Russia, an allegation dismissed by the Kremlin as evidence of Ukraine's tendency to accuse Russia of "all mortal sins". Sych, who said he could not reveal all the details of the probe, said there was no conclusive evidence that the attacks originated in Russia. One of the emails was sent from the server of a German university, another from the United States, he said. He said the hackers had sent the emails in question to workers at the affected power distribution companies with infected Word or Excel files that were meant to look like official correspondence from the energy ministry. They contained topics that would have been recognizable to the workers and were not sent out en masse but targeted certain individuals instead. One of the emails was about regional electricity production levels, he said. "It was all very simple and stupid," Sych said, adding that the hackers totally wiped the data of some of the computers in one of the firms. Details of the impact of the attacks have been sketchy, but one is reported to have affected 80,000 customers for two hours. The three named companies declined to comment on Sych's remarks. (Reuters, 27Jan16)

(U) Ransomware author blackmails security researcher who refuses to give in

The author of the Magic ransomware strain has agreed to release all decryption keys for free, if Utku Sen, a Turkish security researcher, takes down his Hidden Tear open-source ransomware project from GitHub. Utku Sen has become really famous in the infosec community as of late, after he released the source code of two ransomware strains as open source projects on GitHub. The first project he created was named Hidden Tear, and malware operators used it to create the Cryptear.B ransomware family. Unfortunately for the malware operators, the ransomware's encryption contained an encryption flaw, left intentionally by Utku in its source code, which allowed him and other security researchers to help victims decrypt their locked files without paying the ransom. The second project was the EDA2 ransomware, which didn't contain an encryption backdoor, but came with a fully-working C&C server admin panel, which contained a backdoor account. This second project was used for the Magic ransomware family. The problem is that the operator of this ransomware campaign decided to host the C&C server admin panel on a free hosting provider's infrastructure. Once the hosting provider discovered what the malware operator was up to, it shut down and deleted his account, inadvertently deleting the database with all the encryption keys. Utku Sen publicly apologized for this incident, and then removed the EDA2 ransomware project from GitHub, but with no doubt, the project is still shared via underground forums and black markets. As it turns out, the Magic ransomware author had a backup of some of the encryption keys, before the hosting provider deleted his account. Impressed by the story of a user who lost pictures of his newborn son, the Magic ransomware's author decided to release this user's encryption key for free. The ransomware's operator then had a sudden change of heart and decided that he'd release all encryption keys for free, without requiring Bitcoin payments, if Utku Sen would take down the Hidden Tear project and also pay him 3 Bitcoin (around $1,200 / €1,100). After further negotiations from Bleeping Computer's Lawrence Abrams, the Magic ransomware author cut down his demands, and only asked for Utku Sen to remove the Hidden Tear GitHub repo. (Softpedia, 26Jan16)

(U) Biggest DDoS attack yet

Arbor Networks' 11th Annual Worldwide Infrastructure Security Report reveals that, for the first time in history, a company reported a DDoS attack that surpassed the 500 Gbps mark, something that was almost unbelievable only a few years back. The report, which included responses from 354 industry professionals, showed that DDoS attacks, in general, grew in intensity, and besides the single 500 Gbps attack, companies also reported incidents that reached peak values of 450 Gbps, 425 Gbps, and also 337 Gbps. Furthermore, 20 percent of the respondents also admitted they saw attacks of over 50 Gbps peak value while another quarter reported on peak attacks that reached over 100 Gbps, values much greater than in the past years. Two-thirds of the total DDoS attacks targeted end customers while the other third of attacks were aimed at the ISP itself, and inadvertently affected its customers as well. In addition, 33 percent of all respondents said they were affected by DDoS attacks launched against cloud services. This figure went up from 29 percent last year and 19 percent two years ago, showing a greater dependency on online services and especially their "online" status. Additionally, 44 percent of all respondents also said they saw more than 21 DDoS attacks in a single month while 9 percent also claimed they saw DDoS attacks carried out via IPv6 infrastructure for the first time. Most of these attacks were attributed to "criminals demonstrating attack capabilities" while in second and third place came "online gaming-related" and "criminal extortion attempts." Besides DDoS attacks, the Arbor Networks 11th Annual Worldwide Infrastructure Security Report includes information on other security threats affecting companies around the world. The report is available for free online. (Softpedia, 27Jan16)

OGA

Items of Interest

(U) Flash is expected to be dead in two years
According to the 2016 global media format report published by Encoding.com, Flash only made up six percent of mobile and web video in 2015, down from 21 percent in 2014. The company believes Flash will be completely gone within the next two years. So what's replacing it? Right now, H.264 is still the leading video codec, making up 72 percent of online videos. But H.264 isn't new, it's been around for 13 years, and the next generation of codecs are starting to pick up steam. WebM -- which is royalty-free -- is on pace to be the next big video codec, with 12 percent of the market and the leading HTML5 video delivery system for Chrome and Firefox. H.265 or HEVC, the format The International Telecommunications Union (ITU) anointed as the successor to H.264 is growing, but only makes up 6 percent of the market, half of WebM's reach. The lack of growth is likely due to the fact that companies using the codec must pay royalty fees to the patent owners, unlike its competitor WebM. But with the ability to reproduce content at half the bitrate as H.264 and with support from Netflix who uses it for 4K streaming and Apple's FaceTime (on newer devices), the expectation is H.265 will become a mainstream codec right along with WebM. (The Verge, 27Jan16)

(U) Internet search engine snoops on webcams around the world
It's now possible to snoop on webcams around the world after a search engine launched a new service for the Internet of Things (IoT), that lets users watch online images recorded in real time. Shodan, a search engine for the Internet of Things, allows users to snoop on screenshots of anything filmed by a webcam from cash register cameras to babies sleeping in a cot. Shodan randomly searches the Internet on the lookout for Internet Service Providers (ISP) with open ports. Once it discovers a vulnerable webcam, it files the ISP address, camera details and takes screenshot. Users of the Shodan search engine can type in specific terms to see images from insecure webcams. Dan Tentler, a security researcher told Ars Technica UK that the ability to see screenshots from webcams is "all over the place, practically everything you can think of." Ars Technica then carried out a search using Shodan which "turned up some alarming results" including a baby sleeping in Canada, a man in a bathroom and a random kitchen in Spain. Dan Tentler told Ars Technica that there are millions of insecure webcams and that number will continue to grow as the webcams become even more popular and drop in price. Many webcams are available for $20. Tentler said: "The consumers are saying 'we're not supposed to know anything about this stuff [cybersecurity],'. The vendors don't want to lift a finger to help users because it costs them money." An expert in software programming and hacking who wanted to remain anonymous told Sputnik that "These devices [IoT] are usually hackable with ease." Shodan's new webcam snooping service has opened up the world of vulnerable webcams of pictures that probably should be private for anyone who uses it and for just $49, users can pay to view images running in real time -- as long as the IoT remains insecure. (Sputnik, 26Jan16)

(U) US agencies have 2 weeks to report if they were affected by the Juniper backdoor
The US House Oversight and Government Reform Committee has sent out 24 letters, calling various US government agencies to report on the status of Juniper network equipment and if they were affected by the ScreenOS backdoor vulnerability. Just before Christmas, Juniper announced it discovered unauthorized code in its ScreenOS operating system, used for its firewall networking equipment. Juniper released patches to fix these issues, but taking into account that very few network administrators patch their systems right away, many companies may probably still be running vulnerable versions of ScreenOS. In letters sent out to various US agencies, the US Senate is now trying to find out who did their job and who's still lagging behind. All US agencies have until 4 February 2016, to report on the status of their ScreenOS patching operations so that the US Government can understand the actual extent of the damage these vulnerabilities cause (d) in its infrastructure. The agencies that received these letters are: NASA, US Department of Defense, US Department of State, US Department of Labor, US Department of Education, US Department of Energy, US Department of Commerce, US Department of Agriculture, US Department of Transportation, US Department of Health and Human Services, US Department of Treasury, US Department of the Interior, US Department of Veteran Affairs, US Department of Housing and Urban Development, US Social Security Administration, US Office of Personnel Management, US Environmental Protection Agency, US Nuclear Regulatory Commission, US General Services Administration, US Agency for International Development, US Small Business Administration, US Securities and Exchange Commission, Consumer Financial Protection Bureau, and National Science Foundation. (Softpedia, 26Jan16)

(U) Engineers build cyber security testbed to help protect the power grid
It's easy to think of the electrical grid as the power plants, the high voltage lines, the transmission towers, the substations and all the low-voltage distribution lines that bring power to our homes and businesses. An attack on that grid would involve getting out and cutting lines or dropping towers. But there's another, less visible piece to the grid -- all the computers and communication networks that make it work. Attackers can go after the cyber grid, too. "From an attack standpoint, that's the cheapest form of attack with the lowest chance of being caught," said Doug Jacobson, a University Professor of Electrical and Computer Engineering at Iowa State University. "It's asymmetrical warfare at its best. A single individual can cause enormous damage. To minimize the threat of that kind of attack, Jacobson and Manimaran Govindarasu, Iowa State's Ross Martin Mehl and Marylyne Munas Mehl Computer Engineering Professor, are leading studies of grid cyber security while also training industry professionals and educating students to protect the nation's critical infrastructure. A major part of their project is developing a high-fidelity, open-access testbed to help secure the power grid. They call it "PowerCyber" and it's designed to do vulnerability analysis, risk assessment, attack-defense evaluations and other tests. PowerCyber integrates all of those elements -- including actual relay equipment and other hardware -- then adds sophisticated models of the grid system and virtual Internet technology. That Internet technology is based on ISEAGE (pronounced "ice age," the Internet-Scale Event and Attack Generation Environment), a controlled, simulated Internet for cyber security studies. Jacobson developed the technology at Iowa State with support from the US Department of Justice. "We can use this testbed to run attacks and see the consequences on the power system," Govindarasu said. "If it's a blackout, how do we mitigate that? We can also prepare for these attacks and for our defenses." The PowerCyber testbed is being developed with support from the National Science Foundation and the US Department of Homeland Security. The US Department of Energy is also supporting other Iowa State projects related to the cyber defense of the country's power grid infrastructure. So far, the testbed has been used in industry training and graduate courses. It has also been used as a resource for researchers in industry, at other universities and at national laboratories. (technology.org, 25Jan16)

(U) White House turns to Pentagon in US background checks shake-up
The US government will set up a new agency to do background checks on employees and contractors, the White House said on Friday, after a massive breach of US government files exposed the personal data of millions of people last year. As a part of a sweeping overhaul, the Obama administration said it will establish a National Background Investigations Bureau. It will replace the Office of Personnel Management's (OPM) Federal Investigative Services (FIS), which currently conducts each year more than 2 million background investigations for scores of federal agencies. The move, a stiff rebuke for FIS and OPM, comes after last year's disclosure that a hack of OPM computers exposed the names, addresses, Social Security numbers and other sensitive information of roughly 22 million current and former federal employees and contractors, as well as applicants for federal jobs and individuals listed on background check forms. Unlike FIS, the new agency's information systems will be handled by the Defense Department, making it even more central to Washington's effort to bolster its cyber defenses against constant intrusion attempts by hackers and foreign nationals. The White House gave no timeline for implementing the changes, but said some would begin this year. It will seek $95 million more in its upcoming fiscal 2017 budget for information technology development, according to a White House fact sheet. A transition team will develop a plan to migrate existing functions from FIS while continuing to provide investigative services, the US Director of National Intelligence James Clapper wrote in a blog on the OPM website. (Reuters, 22Jan16)

(U) US Air Force cyberspace weapon achieves operational status
The US Air Force Intranet Control Weapon System has achieved full operational status, becoming the first cyberspace weapon system to do so. The AFINC weapon system is designed to control the flow of all external and inter-base traffic through centrally managed gateways. The system is comprised of 16 Gateway Suites and two Integrated Management Suites, and is operated by 26 Network Operations Squadrons. The weapon system was built to enhance the US Air Force's cybersecurity capabilities, which Air Force officials say is increasingly important. The system replaces and consolidates over 100 regionally managed Air Force network entry points into 16 centrally managed access points in an effort to speed up defensive actions. It serves over one million Air Force users around the world. The AFINC weapon system was designated as a weapon system by the Air Force Chief of Staff in March 2013 before achieving Initial Operational Capability in May 2014. (UPI, 21Jan16)

(U) DHS to showcase cybersecurity research
The Department of Homeland Security funds a variety of cybersecurity research through academia, small businesses, industry and government and national labs. On 17-19 February, DHS will showcase some of the results of that funding. The 2016 Cyber Security Division R&D Showcase and Technical Workshop, held in Washington DC, will highlight the status of the latest cybersecurity research, enable collaboration among the researchers and government agencies and connect the technologies to transition partners. The showcase will feature 10 innovative technology solutions from the Cyber Security Division's portfolio that have potential for commercialization. The workshop portion will feature over 70 presentations, highlighting the work of Cyber Security Division's principal investigators. Events are open to both public and private sector cybersecurity professionals. (Government Computer News, 20Jan16)

(U//~~FOUO~~) US critical infrastructure sector saw 20-percent rise in cyber incidents in FY 2015
(U//~~FOUO~~) US critical infrastructure systems experienced a 20-percent increase in attempted cyber security breaches in FY 2015, according to a 19 January US press article citing an end-of-year DHS report. The DHS Industrial Control Systems Cyber security Emergency Response Team (ICS-CERT) responded to 295 cyber security incidents involving critical infrastructure, compared to 245 in FY 2014. A significant number of incidents were enabled by "insufficiently architected networks," according to the report. Energy—last year's most commonly targeted sector—experienced a 42-percent decline in breach attempts, while the critical manufacturing sector experienced an overall increase in attacks, primarily widespread spear-phishing campaigns. In FY 2014, there were only 42 "relatively easy to execute and demonstrably effective" spear-phishing incidents, compared to 109 in FY 2015. (fcw.com, 19Jan16)

(b)(3) 10 USC ⊥ 424

Note: This is not original product but is consolidated from various sources.

(b)(3) 10 USC ⊥ 424