Cyber-Threat Newsletter – 16 Feb 16

(b)(3) 10 USC ⊥ 424

Patches & Updates of the Week:

(U) Adobe's February security update fixes holes in Flash, Photoshop, and more
Adobe has released new versions to address security issues reported in products like Adobe Flash, Adobe Photoshop CC, Adobe Bridge CC, Adobe Connect, and Adobe Experience Manager. The most patched product was, as usual, Adobe's Flash Player, which received 22 security updates, all with a critical severity rating. Most updates (14) resolved memory corruption vulnerabilities that allowed attackers to execute code on the victim's machine and take control of the user's PC. Additionally, Adobe also fixed six use-after-free vulnerabilities, a heap buffer overflow vulnerability, and another type confusion vulnerability, all of which also led to remote code execution. Windows and Mac users should update their Flash Player to version 20.0.0.306 (released earlier today) while Linux users should update to the latest version, which is 11.2.202.569. The same security patches have also been integrated with the AIR runtime, which was updated to version 20.0.0.260. The surprise entry on Adobe's February security bulletin is Photoshop, which received, alongside Adobe Bridge, three security patches to fix memory corruption vulnerabilities that could lead to code execution. The most recent versions of Adobe Photoshop CC considered safe are now 16.1.2 (2015.1.2) and 15.2.4 (2014.2.4) while the safest Adobe Bridge CC version is now 6.2. Adobe also released version 9.5.2 of Adobe Connect, its video conferencing software, which patched three security issues and also added a feature to protect against CSRF (Cross-Site Request Forgery) attacks. Last on Adobe's list was the Adobe Experience Manager (formerly known as CQ5 or Communique5), a Java-based CMS that the company bought in 2010. This package received four security hotfixes for versions 6.1.0, 6.0.0, and 5.6.1, which now protect its owners against a Java deserialization issue, a CSRF bug, an information disclosure problem, and a URL filter bypass vulnerability. (Softpedia 10Feb16)

(U) Microsoft Patch Tuesday fixes 13 flaws in release covering Windows, Edge and IE
Microsoft has issued its latest Patch Tuesday release, fixing 13 flaws covering key products including Windows, the Edge browser and, of course, Internet Explorer. This month's package is not as bad as the one before it when there were a lot of serious vulnerabilities to deal with, but it still contains enough patches to be of note to IT teams, especially the four 'critical' fixes. Microsoft noted that all versions of Windows are affected by some of the flaws, and urged users of Windows Vista and later, including Windows 10, to get patching immediately. The highest priority item is MS16-022, which contains fixes for 22 vulnerabilities for Adobe Flash, all of them rated as 'critical' and capable of handing the attacker complete control over the target machine. A large chunk of the Microsoft fixes provide protection against remote code execution (RCE) threats. One of these applies to Windows Journal, which has interested Craig Young, a security researcher at Tripwire. "Today marks the 12th RCE bug Microsoft is patching in Windows Journal in just 10 months. This is particularly interesting because Windows Journal vulnerabilities were basically unheard of before 2015," he said. "While the increased scrutiny of Windows Journal may be an indication of Microsoft's successes in the tablet space, it is important to remember that the flaw is not limited to tablets. "In fact every piece of software installed on a computer adds to the potential attack surface even if that software is not frequently used. (v3.co.uk 10Feb16)

(U) Google issues Chrome update to fix Windows, Mac, and Linux bugs
Google issued a Chrome update to address Windows, Mac, and Linux vulnerabilities that, if exploited, would allow remote attackers to take control of affected systems. The updated Chrome version (48.0.2564.109) addressed six vulnerabilities, including flaws that allowed same-origin bypass in Chrome extensions (CVE-2016-1622), DOM same-origin bypass (CVE-2016-1623), Buffer overflow in Brotli (CVE-2016-1624), a Chrome Instant Navigation bypass (CVE-2016-1625), a PDFium out-of-bounds read (CVE-2016-1626), and updates based on Google's ongoing internal audits and other initiatives (CVE-2016-1627). The bugs were discovered by Mariusz Mlynski, lukezli, Jann Horn, and an anonymous security researcher working with HP's Zero Day Initiative. Google also announced it will no longer allow Flash display ads on AdWords or DoubleClick Digital Marketing campaigns, starting 30 June. The search giant's continues its efforts to move off Flash to HTML5. Flash display ads will no longer be accepted on Google Display Network or DoubleClick, starting 2 January 2017. (scmagazine.com 10Feb16)

(U) Oracle issues an emergency patch to Java for Windows
Security problems are not new to Java, though it is, admittedly, not the only platform that suffers from these problems. Now Oracle has acknowledged a new hole and it is bad enough to issue an out of cycle emergency patch. The security flaw, CVE-2016-0603, requires the user to access a malicious website and accept the download of Java version 6, 7 or 8 in order to become infected. However, for those who fall for it, the attack will allow for a total compromise of the system. "Because the exposure exists only during the installation process, users need not upgrade existing Java installations to address the vulnerability. However, Java users who have downloaded any old version of Java prior to 6u113, 7u97 or 8u73, should discard these old downloads and replace them with 6u113, 7u97 or 8u73 or later", writes Eric Maurice of Oracle. (BetaNews 08Feb16)

Threats & Vulnerabilities of the Week:

(U) New, improved DMA Locker ransomware patches decryption flaw
The creators of the DMA Locker ransomware released an updated version that now includes a patch to fix a flaw that left earlier iterations easily decryptable. The ransomware's third version now includes an RSA key and key validation, a researcher called Hasherezade said in a Tuesday Malwarebytes blog post. "This time the key necessary to decrypt files must be supplied not as a text, but as RSA key file," the researcher explained. "The author of this malware, despite appearing inexperienced in programming, seems to be very determined to gradually improve the quality of the product," said Hasherezade wrote. In addition to addressing the decryption flaw, coding in the previous versions was so shoddy that the malware would sometimes crash a computer before the victim received a ransom demand. It is unclear if that problem persists in the latest iteration of DMA Locker. (scmagazine.com 10Feb16)

(U) Vulnerabilities in Trane thermostats heat up IoT safety concerns
Talos yesterday disclosed a trio of dangerous Internet of Things (IoT) vulnerabilities that were discovered and subsequently patched in smart thermostats manufactured by HVAC company Trane. Researchers from Talos, an offshoot of Cisco Systems, first discovered flaws in the connected thermostat -- sold under the brand new ComfortLink II -- in April 2014. Trane patched two of the bugs in April 2015 and fixed the third vulnerability as of 27 January 2016. The vulnerabilities could have allowed bad actors to remotely access and operate the thermostats, as well as trigger arbitrary code to use the device as conduit for local network and external network attacks, Talos said in a blog post. The research group also recommended that ComfortLink II owners update their firmware immediately, as it was unclear if Trane had "effectively communicated the necessity of installing these updates to their customers." "While IoT devices such as smart thermostats, home lighting and security systems bring an added level of convenience into our lives, these vulnerabilities highlight the dangers of insecure development practices," Talos cautioned. (scmagazine.com 10Feb16)

(U) Poseidon hacker group behind long-running extortion scheme
Kaspersky Lab has linked a single group to a long-known campaign of cyberattacks that appears to be aimed at extorting corporate victims. The Poseidon Group may have been active since 2001, according to an analysis of malware samples. The group's tools have been designed to function on systems set to English and Portuguese. Victims are usually sent spear-phishing emails and malware hidden inside office documents. Once on a network, the hackers explore its topology in order to eventually steal intellectual property and commercial information. But the most interesting facet of Poseidon is that it doesn't just steal data. "The information exfiltrated is then leveraged by a company front to blackmail victim companies into contracting the Poseidon Group as a security firm," Kaspersky wrote. Even if a company is blackmailed into using Poseidon's alleged services, the group tries to maintain its malware on the affected company's system. Kaspersky didn't provide a lot of detail about the ruse, but said that at least 35 companies have been affected in industries such as banking, government, telecommunications, manufacturing and energy, besides media and public relations firms. Kaspersky said it has reached out to companies that appear to have been infected and shared indicators of compromise, or technical information that points to an attack. (IDG News Service 10Feb16)

(U) Hearthstone gamers who download cheats may be cursed with malware
Evoking the old axiom "cheaters never prosper," Symantec yesterday warned online gamers of new Windows-based malware schemes victimizing fans of the strategy card game Hearthstone: Heroes of Warcraft. According to the company's Security Response blog, hackers behind these cyberthreats are preying on dishonest players who seek out third-party cheat apps to improve their rankings and build their weapons caches. A title of video game developer Blizzard Entertainment, Hearthstone is a free spin-off to the wildly popular World of Warcraft franchise, reportedly boasting more than 40 million registered accounts as of November 2015. With such a large pool of potential victims, Hearthstone is a tantalizing target for hackers looking to cash in by uploading malicious gaming applications to online distribution sites. Once an infected file is downloaded by a gamer, the hidden malware can steal Bitcoin funds or install backdoors for remote access to users' PCs. Val Saengphaibul, senior security researcher at Symantec, told SCMagazine.com that many of these booby-trapped apps "piggyback off of a known Hearthstone app name and try to socially engineer the cheater to download" the similarly-named fraudulent file. Symantec detailed two separately discovered cyberthreats in its blog post. The first, detected on 2 February 2016, is the newly discovered malware Trojan.Coinbitclip, which poses as a "gold and dust" hacking tool. In Hearthstone, gold and dust are units of currency. The player thinks downloading the file will help him to accrue extra gold and dust at no cost, but in truth the trojan robs the gamer of his very-real Bitcoin currency. "Because Bitcoin addresses are long and include random characters, many users who mine Bitcoins use a clipboard to facilitate the process. Trojan.Coinbitclip hijacks the user's clipboard and replaces the user's Bitcoin address with one from its own list -- this is how the malware steals someone's Bitcoin," Symantec explains in its blog. The second threat is the four-year-old trojan Backdoor. Breut, which as of December 2015 was now posing as an add-on deck-tracking application for Hearthstone. Deck trackers provide players with insight into which cards they haven't drawn yet. "This threat is capable of opening a back door, recording from the webcam, logging key strokes and stealing passwords," the company's blog post warned. Symantec also warned that many video game bots -- tools that allow your computer to play and earn rewards for you while you tend to other matters -- are also often riddled with malware, though there was no specific example in the blog post. Symantec recommended that gamers arm their devices with a strong, updated antivirus program. But the safest course of action is not to download any third-party game apps at all, lest the cheaters get cheated themselves. (scmagazine.com 10Feb16)

(U) Java-based Trojan was used to attack over 400,000 systems
A cross-platform remote access Trojan that's being openly sold as a service to all types of attackers, from opportunistic cybercriminals to cyberespionage groups, has been used to attack more than 400,000 systems over the past three years. The RAT (Remote Access Tool/Trojan), which depending on the variant is known as Adwind, AlienSpy, Frutas, Unrecom, Sockrat, jRat or JSocket, is evidence of how successful the malware-as-a-service model can be for malware creators. Adwind is written in Java, so it can run on any OS that has a Java runtime installed including Windows, Mac OS X, Linux and Android. The Trojan has been continuously developed since at least 2012 and is being sold out in the open via a public website. Like most Trojans, Adwind can be used to remotely control infected computers; to steal files, key strokes and saved passwords; to record audio and video through the computer's webcam and microphone and more. Because it has a modular architecture, users can also install plug-ins that extend its functionality. The Adwind author, who researchers from Kaspersky Lab believe to be a Spanish-speaking individual, is selling access to the RAT on a subscription-based model, with prices ranging from $25 for 15 days to $300 a year. The buyers get technical support, obfuscation services to evade antivirus detection, virtual private network accounts and free scans with multiple antivirus engines to ensure that their sample is not detected when deployed. The latest incarnation of Adwind was launched in June 2015 under the name JSocket and is still being sold. "In 2015, Russia was the most attacked country, with UAE and Turkey again near the top, along with the USA, Turkey and Germany," the Kaspersky researchers said in a blog post. They estimated that by the end of 2015 there were around 1,800 Adwind/JSocket users, putting the developer's annual revenue at over $200,000. The large number of users makes it hard to build an attacker profile. The RAT could be used by anyone from low-level scammers to cyberspies and private individuals looking to monitor their partners or spouses. One possible method to prevent its installation is to change the default application for handling JAR files to something like Notepad. This will prevent the code's execution and will just result in a notepad window with gibberish text in it. Unfortunately that's not possible in most business environments, as Java is still a major programming language for business applications. (IDG News Service 09Feb16)

(U) Skype targeted by T9000 backdoor Trojan
Palo Alto Networks researchers spotted a new, more complex backdoor trojan that is targeting Skype users and which can identify and evade the security software found on the victim's computer. Palo Alto's Josh Grunzweig and Jen Miller-Osborn, part of the company's Unit 42 research team, dubbed the backdoor T9000 as it is a newer variant of the T5000 backdoor. The researchers noted in a blog post that the T9000's primary function is to gather information on the victim by capturing encrypted data, take screenshots of specific applications One way the T9000 differs from other backdoor trojans is by being more complicated, using a multi-stage installation program and it has a list of 24 security software products that it checks for during installation enabling the malware to avoid detection. "The author of this backdoor has gone to great lengths to avoid being detected and to evade the scrutiny of the malware analysis community," the researchers wrote in the blog. The primary target for the T9000 has been large organizations, Grunzweig and Osborn said. One reason for this could be the heavy adoption of Skype among businesses that see the face-to-face video software as a useful tool, said Tim Erlin, Tripwire's director of security and risk strategy. "Users may think of Skype as a valuable channel for exchanging information, but that user value translates into profit for cyber attackers," he said to SCMagazine.com in an email Monday. Those Skyping with an infected computer may also find themselves being viewed from afar as the researchers found the trojan periodically snaps images during video calls and just to cover all its bases T9000 also hijacks audio calls storing them as .wav files. When decrypted, we can see that the malware periodically takes images of the video calls. Audio calls are stored as .wav files. (scmagazine.com 08Feb16)

(U) Vulnerabilities allow delivery of malware through web page fonts
A researcher discovered vulnerabilities in the Graphite font processing library (also called Libgraphite) that affects many applications, including Firefox, OpenOffice, Thunderbird, Pale Moon, WorldPad and many Linux distributions. The flaws would allow hackers to take recent attacks that infect web users through malware-infected web pages to the next level. One of the vulnerabilities (CVE-2016-1521) allows attackers to deliver malicious code to web users who visit a web page that contains Graphite-enabled fonts. "Since Mozilla Firefox 11 and later versions directly support Graphite, the attacker could easily compromise a server and then serve the specially crafted font when the user renders a page from the server (since Graphite supports both local and server-based fonts)," stated Cisco in a corporate blog post. The other vulnerabilities involve a heap data buffer overflow (CVE-2016-1522) and vulnerabilities that allow DDoS attacks (CVE-2016-1523 and CVE-2016-1526). The flaws were discovered by Yves Younan, a researcher in Cisco's Talos Group. (scmagazine.com 08Feb16)

Incidents of Interest:

(U) Identity thieves obtain 100,000 electronic filing PINs from IRS system
The Internal Revenue Service was the target of an attack that used stolen social security numbers and other taxpayer data to obtain PINs that can be used to file tax returns electronically. The attack occurred in January and targeted an IRS Web application that taxpayers use to obtain their so-called Electronic Filing (E-file) PINs. The app requires taxpayer information such as name, Social Security number, date of birth and full address. Attackers attempted to obtain E-file PINs corresponding to 464,000 unique SSNs using an automated bot, and did so successfully for 101,000 SSNs before the IRS blocked it. The personal taxpayer data used during the attack was not obtained from the IRS, but was stolen elsewhere, the agency said in a statement. The IRS is notifying affected taxpayers via mail and will monitor their accounts to protect them from tax-related identity theft. While the IRS said that externally acquired taxpayer data was used, the agency did suffer a security breach last year that allowed attackers to gain information such as Social Security information, date of birth and street address for over 300,000 taxpayers. (IDG News Service 10Feb16)

(U) Russian hackers used malware to manipulate the Dollar/Ruble exchange rate
Russian-language hackers have managed to break into Russian regional bank Energobank, infect its systems, and gain unsanctioned access to its trading system terminals, which allowed them to manipulate the Dollar/Ruble exchange rate. "The criminals made purchases and sales of US dollars in the Dollar/Ruble exchange program on behalf of a bank using malware. The attack itself lasted only 14 minutes, however, it managed to cause a high volatility in the exchange rate of between 55/62 (Buy/Sell) rubles per 1 dollar instead of the 60-62 stable range," Russian security company Group-IB shared in a recently published whitepaper. "To conduct the attack criminals used the Corkow malware, also known as Metel, containing specific modules designed to conduct thefts from trading systems (..) Corkow provided remote access to the ITS-Broker system terminal by 'Platforma soft' Ltd., which enabled the fraud to be committed." The attack happened in February 2015, but the preparation for it lasted much longer. During this period, the Corkow Trojan was functional and constantly updated itself to avoid detection by antivirus software installed at the bank." The incident lead to an investigation by the Russian central bank, and Energobank also called in Group-IB's researchers to investigate. "As a result of the attack, the compromised bank which terminal was used for intrusion, suffered a huge financial and reputational damage, since many players on the market didn't trust the hacking theory of the incident and tended to believe that a simple mistake had occurred," noted Group-IB's researchers, who were called in by Energobank to investigate the incident. "Experts say that many companies that were trading at the time of the attack and successfully made profit while the attackers are believed to have received no money from the operation. This evidence leads us to believe that these hacker actions could be a test of the ability to influence the market and capitalize on future attacks." It seems likely that the attack was perpetrated by the Metel cyber-criminal group, whose exploits half a year later have resulted in a successful attack involving the compromise of an unnamed bank and automation of the rollback capability of ATM transactions, and the criminals making off with hundreds of millions of rubles. To execute the attack, they used the aforementioned Corkow Trojan and, once again, the Niteris exploit pack to perpetrate the initial drive-by download of the malware. "Various hacker groups demonstrate increased interest towards trading and brokerage systems and their clients, which is evidenced by the specific modifications in malware they use," the researchers commented. "Hackers target primarily companies in Russia and CIS countries, though it is noticed that the amount of attacks targeting the USA has increased 5 times since 2011." For an in-depth overview of this group's actions and technical details about the malware they used, check out the whitepaper. (net-security.org 09Feb16)

(U) Pro-Palestine hacktivist makes good on threat, posts data on FBI and DHS personnel
Following through on his threat, the hacker responsible for breaching the Department of Justice's (DOJ) web portal has publicly posted stolen data corresponding to roughly 20,000 employees of the FBI and 9,000 from the Department of Homeland Security (DHS). Using the data dump as a means to express support for Palestine, the hacktivist on Sunday tweeted a link to a CryptoBin page containing a list of DHS personnel's names, job titles, private emails, phone numbers and more. Then yesterday the perpetrator struck again, using the same m.o. to publish the FBI's personnel data. The hacker wrote: "Long Live Palestine, Long Live Gaza" above the data dump and also included a #FreePalestine hashtag. At this point, neither CryptoBin page is available. In a statement to SCMagazine.com by DHS spokesperson S.Y. Lee, DHS said, "We are looking into the reports of purported disclosure of DHS employee contact information. We take these reports very seriously; however there is no indication at this time that there is any breach of sensitive or personally identifiable information." Even so, the data breach is new blemish on the federal government's already spotty IT security record -- especially with the 2015 hack of the US Office of Personnel Management fresh in people's minds. Considering that the hacktivist gained access to government systems through a combination of phishing and social engineering, Tim Erlin, director of IT security and risk strategy at cybersecurity solution company Tripwire, told SCMagazine.com that moving forward, the federal government should "couple [employee] training with technology controls that prevent individuals from taking unauthorized action even when they're convinced that they should". (scmagazine.com 09Feb16)

OGA

(U) Hacker steals and posts personal details on 9,000 DHS employees
A hacker posted the names, phone numbers, and other details about 9,000 Department of Homeland Security employees and says he will post 20,000 similar records about FBI workers. He claims to have records that include military emails and credit card numbers, according to a published report. Motherboard writer Joseph Cox writes that Sunday he received the stolen personal data, some of which came from a single Department of Justice computer hacked using a compromised email account and social engineering. Cox wrote he checked out the accuracy of the personal information by calling up some of the numbers at random, and in many cases reached voicemail of the persons named or they picked up the phone themselves. The hacker told Cox that after he compromised the email account of a Department of Justice employee, he tried but failed to log into a DoJ Web portal, then social-engineered an employee into giving him credentials. The hacker downloaded 200GB of data from the machine and had access to 1TB, but "couldn't take all of" it, the story says. (Network World 08Feb16)

OGA

Items of Interest

(U) Obama administration plans new high-level cyber official
The Obama administration is creating a new high-level federal official to coordinate cybersecurity across civilian agencies and to work with military and intelligence counterparts, as part of its 2017 budget proposal announced Tuesday. The $19-billion increase in cybersecurity funding across all government agencies -- up more than 35 percent from last year -- is entitled the "Cybersecurity National Action Plan" and is an effort touted by the White House as the "capstone" of seven years of often faltering attempts to build a cohesive, broad federal cybersecurity response. Measures include more cybersecurity training for the private sector, emphasizing multi-factor authentication on tax data and government benefits and efforts to reduce the use of Social Security numbers as identifiers. The tasking of a single high-level official with tracking down cyber intruders in federal government networks establishes a position long in place at companies in the private sector. The lack of such a government role has been especially notable after hackers stole the personal information of 21 million Americans, whose information was housed at the Office of Personnel Management. The budget notes that US Cyber Command is building a Cyber Mission Force of 133 teams assembled from 6,200 military, civilian and contractors from across military and defense agencies. The president also proposed a $3.1 billion effort to modernize the often antiquated federal technical infrastructure and networks, replacing legacy systems that frequently serve as critical gaps in cybersecurity. While many of the proposals such as the new cybersecurity official can be done through existing appropriations or executive authorities, the modernization effort will require congressional approval, said Michael Daniel, special assistant to the president and cybersecurity coordinator. The White House expects broad support for what has not been a partisan issue. The budget includes more cybersecurity advisors, a roughly fourfold increase in civilian cyber defense teams at the US Department of Homeland Security, charged with security for the .gov domain, to 48. The Department of Homeland Security plans to expand its EINSTEIN system, which was created to detect and block cyberattacks on federal agencies. The president signed an executive order Tuesday creating a permanent Federal Privacy Council, which will bring together privacy officials from across government to help with implementing comprehensive federal privacy guidelines. The president is also establishing a Commission on Enhancing National Cybersecurity that would involve congressional and private sector leaders who will be tasked with making recommendations in government cybersecurity for the next decade. (AP 09Feb16)

(U) Chinese cyberspies pivot to Russia in wake of Obama-Xi Pact

Cyber espionage attacks by Chinese advanced persistent threat groups against Russian targets have increased by 300 percent in the past two months, according to a top security expert with Kaspersky Lab. Costin Raiu, director of the global research and analysis team at Kaspersky Lab, says his firm's researchers witnessed a dramatic drop in Chinese-speaking APTs going after US and UK organizations' intellectual property in September after President Obama and Chinese president Xi Jinping came to a historic agreement not to conduct cyber spying attacks for economic gain. Kaspersky Lab refrains from confirming the actual actors behind advanced groups such as nation-states, so it refers to these attackers as "Chinese-speaking" cyber espionage groups. Raiu said the cyber espionage groups appear to have shifted their focus to Russia and other former Soviet countries as new sources of intellectual property for economic gain in the wake of the Obama-Xi pact. Kaspersky's Raiu said his company has seen activity from Mirage, a Chinese-speaking APT group that traditionally has targeted ministries of foreign affairs, waging attacks in Russia. "Now they are super-active in Russia," he said, with interests in military espionage, for example. But there have been "several" APT groups seen targeting Russian victims, he said. Kurt Baumgartner, principal security researcher at Kaspersky Lab, says the increased activity targets "a geopolitical profile." Industries that support those geopolitical interests and structure are also under attack, he said. CrowdStrike also has seen more Chinese attacks on Russia -- from a specific Chinese APT group called Hammer Panda against Russian Federation nations. But it's also still seeing China-based attacks on US companies. (Dark Reading 09Feb16)

(U) Algorithm developed to predict future botnet attacks

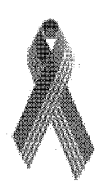
Six botnets have been discovered and traced back to their perpetrators by an algorithm produced by researchers at Israel's Ben-Gurion University (BGU) of the Negev. The scientists who built the formula say it will allow law enforcement to trace administrators responsible for future attacks. The key to the work is analyzing data produced by previous attacks, the cybersecurity researchers say. The new algorithm first identifies the botnet and then allows it to be traced, according to the scientists at Deutsche Telekom Innovation Labs at BGU. The team had access to a wealth of honeypot data collected by one of the largest telcos in the world, Deutsche Telekom. Through machine learning and analysis of that honeypot data, "they built a breakthrough program that identifies the botnet by finding similar attack patterns," BGU claims. A honeypot is a way of baiting the botnet and then collecting intelligence about it. It was that data the team had access to. Once you've identified the botnet and its source, you can go after the administrators, the scientists think. The team reckons they found six botnets. But not only that, they think that they can now tell if an attack came from a genuine person or from a robot. And they say that they can "predict future attacks," BGU says. "This is the first time such a comprehensive study has been carried out and returned with unique findings," Dudu Mimran, CTO of Deutsche Telekom Innovation Labs at BGU, said in the article. The team made their announcement at Israel Defence's CyberTech 2016 event. (Network World 08Feb16)

(U) Internet Archive sets up a malware museum

The Internet Archive (archive.org) has now added a special section that provides a historical look at how malware started out and has evolved over time. Archive.org is the same service where you can find the highly useful Wayback Machine that lets users navigate older versions of some of the Internet's domains, and see how they have evolved over time. Curated by Mikko Hypponen, Chief Research Officer at F-Secure, the Malware Museum project aims to document the first attempts at infecting user computers and damaging their network. The project lists only viruses from the '80s and '90s and has only 79 entries, but it's growing with each new day. All entries are DOS viruses, and they're running inside the DOSBox game emulator. To prevent any damage, Mr. Hypponen removed most of the destructive capabilities these viruses had, and users can also safely download them on their computer and take a look at their internal make-up. (Softpedia 08Feb16)

(b)(3) 10 USC ⊥ 424

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



(b)(3) 10 USC ⊥ 424