[redacted]

[redacted] Cyber-Threat Newsletter – 12 Oct 16

(b)(3) 10 USC ⊥ 424

Patches & Updates of the Week:

(U) Google Chrome update corrects use-after-free vulnerability

(U) Google last week announced the impending rollout of Chrome version 53.0.2785.143, which includes three security fixes for the Windows, Mac and Linux operating systems. According to US-CERT, a remote attacker could exploit one of these vulnerabilities in order to take control of an affected system. According to Google's Chrome Releases blog post page, the latest update addresses a high-severity use-after-free vulnerability -- officially designated CVE-2016-5177 -- that was found in the open-source V8 JavaScript Engine by an anonymous external researcher who was awarded a $5,000 bug bounty. Google's own internal security audits and fuzz testing also resulted in additional fixes, the company reported. (scmagazine.com, 03Oct16)

Threats & Vulnerabilities of the Week:

(U) New insulin pump flaws highlight security risks from medical devices

(U) Medical device manufacturer Animas, a subsidiary of Johnson & Johnson, is warning diabetic patients who use its OneTouch Ping insulin pumps about security issues that could allow hackers to deliver unauthorized doses of insulin. The vulnerabilities were discovered by Jay Radcliffe, a security researcher at Rapid7 who is a Type I diabetic and user of the pump. The flaws primarily stem from a lack of encryption in the communication between the device's two parts: the insulin pump itself and the meter-remote that monitors blood sugar levels and remotely tells the pump how much insulin to administer. The pump and the meter use a proprietary wireless management protocol through radio frequency communications that are not encrypted. This exposes the system to several attacks. First, passive attackers can snoop on the traffic and read the blood glucose results and insulin dosage data. Then, they can trivially spoof the meter to the pump because the key used to pair the two devices is transmitted in clear text. "This vulnerability can be used to remotely dispense insulin and potentially cause the patient to have a hypoglycemic reaction," the Rapid7 researchers said in a blog post. A third issue is that the pump lacks protection against so-called relay attacks, where a legitimate command is intercepted and then is played back by the attacker at a later time. This allows attackers to perform an insulin bolus without special knowledge, the researchers said. While the meter-remote is advertised to work from up to 10 meters away, it is technically possible to launch spoofing attacks from much greater distances with more powerful radio transmission gear like that used by ham radio hobbyists. Animas has published a security notice on its website with recommendations and will also send letters to customers. (IDG News Service, 04Oct16)

(U) Multilingual ransomware Polyglot talks good game, but can't match CTB-Locker

(U) A recently discovered ransomware trojan known as Polyglot tries very hard to imitate the menacing cryptor CTB-Locker, but ultimately falls short in its encryption strength and can be defeated, according to Kaspersky Lab. Polyglot is so named because it supports five different languages, allowing victims to switch translations by clicking on flags representing the native tongues of U.S., Russia, Italy, Spain and Ukraine. According to a Kaspersky blog post published today, Polyglot is distributed via spam emails containing a link to a malicious RAR archive that carries the cryptor's executable code. Following encryption, the malware delivers a ransom note via desktop wallpaper that, strangely enough, displays an image unique to each individual victim. The malware demands payment in bitcoins, granting the victim only 96 hours to respond before files are permanently encrypted. First appearing in late August, Polyglot has quite a few elements in common with CTB-Locker, including "the graphical interface window, language switch, the sequence of actions for requesting the encryption key, the payment page [and] the desktop wallpapers," Kaspersky reported. Moreover, Polyglot's visual appearance is strikingly similar to CTB-Locker and its ransom message and instructions are literally lifted from its predecessor. Just as CTB-Locker compresses victims' files with Zlib, Polyglot packs file content into a ZIP archive. In both cases, the compressed content is then encrypted with AES-256. "This technique seems noteworthy, because we don't often see ransomware that packs the data before encryption. Most trojans just encrypt the original file content," said Sinitsyn. The two malicious trojans also use the same algorithms to create encryption keys, allow victims to decrypt five files for free, and communicate with a command-and-control server located on the Tor network. Despite these parallels, a Kaspersky Lab analysis has revealed that Polyglot was developed separately from CTB-Locker, with markedly different program architectures and virtually no coding shared between them. Sinitsyn, along with fellow blog post authors and analysts Anton Ivanov and Orkhan Mamedov, has theorized that perhaps Polyglot's creators want to trick victims and researchers into thinking the trojan actually is CTB-Locker, leaving no hope that the files can be salvaged without paying up. But they can, because unlike CTB-Locker, Polyglot contains several fatal mistakes that allow victims to decrypt their files without paying the bitcoin ransom. For starters, the ransomware generates symmetric encryption keys based on a randomly generated array of characters; however, the strength of the random sequence generation procedure is surprisingly weak. In fact, reported Kaspersky, it takes mere minutes on a standard PC to conduct a thorough search of the entire set of possible keys for an encrypted file. Even though there is a password-protected ZIP archive below this layer of encryption, this feature is also flawed because the archive key length is only four bytes, and those bytes are borrowed from a unique ID assigned to the computer by the operating system, known as MachinGUID. "Furthermore, a slightly modified MachineGUID string is displayed in the requirements text displayed to the victim; this means that if we know the positions in which the four characters of the ZIP archive password are located, we can easily unpack the archive," reads the blog post. (scmagazine.com, 03Oct16)

(U) Linux Mirai Trojan causing mayhem with DDoS attacks
(U) Linux.Mirai has been found to be carrying out DDoS attacks. The malicious program first appeared in May 2016, detected by Doctor Web after being added to its virus database under the name Linux.DDoS.87. The Trojan can work with the SPARC, ARM, MIPS, SH-4, M68K architectures and Intel x86 computers. Linux.DDoS.87 searches the memory for the processes of other Trojans and terminates them once it has been launched on an infected computer. The Trojan creates a file named .shinigami in its folder and verifies its presence from time to time to avoid terminating itself. Then it attempts to connect to its command and control server for more instructions. When directed to do so by cyber-criminals, the Trojan can launch UDP flood, UDP flood over GRE, DNS flood, TCP flood (several types), and HTTP flood DDoS attacks. To help prevent this, Doctor Web researchers recommend that after booting up, users run a full scan of all disk partitions. (scmagazine.com, 30Sep16)

(U) New record-breaking DDoS reportedly delivered by >145k hacked cameras
(U) Last week, security news site KrebsOnSecurity went dark for more than 24 hours following what was believed to be a record 620 gigabit-per-second denial of service attack brought on by an ensemble of routers, security cameras, or other so-called Internet of Things devices. Now, there's word of a similar attack on a French Web host that peaked at a staggering 1.1 terabits per second, more than 60 percent bigger. The attacks were first reported on 19 September by Octave Klaba, the founder and CTO of OVH. The first one reached 1.1 Tbps while a follow-on was 901 Gbps. Then, last Friday, he reported more attacks that were in the same almost incomprehensible range. He said the distributed denial-of-service (DDoS) attacks were delivered through a collection of hacked Internet-connected cameras and digital video recorders. With each one having the ability to bombard targets with 1 Mbps to 30 Mbps, he estimated the botnet had a capacity of 1.5 Tbps. On Monday, Klaba reported that more than 6,800 new cameras had joined the botnet and said further that over the previous 48 hours the hosting service was subjected to dozens of attacks, some ranging from 100 Gbps to 800 Gbps. On Wednesday, he said more than 15,000 new devices had participated in attacks over the past 48 hours. Prior to last week, the biggest DDoS attack Akamai had mitigated was one in June that peaked at 363 Gbps. Security experts have been warning for years that Internet-connected devices posed a potential threat. In early 2015, the threat was finally confirmed with evidence showing that DDoSes that disrupted Sony's PlayStation Network and Microsoft's Xbox Live were largely powered by home routers that had been hacked and corralled into a powerful botnet. In June, researchers at security firm Sucuri uncovered a botnet of 25,000 closed-circuit TVs bombarding a brick-and-mortar jewelry store. It's not easy for most people to know if their routers, DVRs, and other Internet-connected devices are infected. Depending on the type of attack they're carrying out, devices may show no sign they're taking part in a crippling DDoS. The most important things end users can do is to change all default passwords, or better yet, to never connect the devices to the Internet in the first place. Of course, a connectionless router or modem won't be of any use, but often closed circuit TV cameras work just fine without a connection. With no easy remedy for the growing epidemic of infected devices, people should be prepared for attacks that have the ability to disrupt ever bigger swaths of the Internet. (ars technical, 28Sep16)

(U) IPv4 server hacked in 12 minutes while IPv6 server remained untouched
(U) A small experiment carried out by Sucuri's CTO, Daniel Cid, shows the security advantages IPv6 has over IPv4, but also the dangers of using factory default or common user-password combinations to secure online servers. Cid carried out his experiment at the start of the month when he set up ten servers and left their SSH ports open to external connections. He ran five servers on IPv4-only addresses, while the other five ran only on IPv6 addresses. Both servers had their root password set to "password," a big no-no on live production environments. According to Cid, the first IPv4 server fell after only 12 minutes, with the other four servers getting hacked after a few more minutes. It took the hacker 20 seconds to brute-force the SSH root account. On the other hand, Cid says that after a week, nobody even bothered to scan any of the IPv6 servers, at least once, let alone hack them. "What we can draw from this is that the obscurity of IPv6 helps to minimize the noise of attacks," Cid says. "Most likely, this is because it is more difficult to map the range of IPv6 addresses (2^128) than it is with the range of IPv4 addresses (2^32)." Additionally, there are so-called scan lists of IPv4 addresses available online, which include the IP ranges of several well-known hosting providers, which also aid attackers in hacking IPv4 servers. But things didn't end there. Before Cid had any time to disable and scrap the compromised IPv4 servers, the attacker had already downloaded the Linux/XOR.DDoS malware and was busy launching attacks against a Chinese website. Digital Ocean detected the massive 800+ Mbps SYN packet flood originating from the five hacked servers, and intervened to shut down the servers. (Softpedia, 28Sep16)

Incidents of Interest:

(U) Hackers finding little interest for their stolen NSA hacking tools
(U) The hackers who are auctioning off cyberweapons allegedly stolen from the National Security Agency are growing annoyed and want cash. The ShadowBrokers' sale of the stolen tools has so far generated little interest, and over the weekend, the hackers complained in a message posted online, using broken English. "TheShadowBrokers is not being interested in fame. TheShadowBrokers is selling to be making money," the hackers said. As of Monday, their auction only had one substantial bid at 1.5 bitcoins, or $918. Many of the other bids were valued at less than $1. Although anyone can participate, the hackers haven't said when they'll accept the final bid. The hackers hoped to receive 1 million bitcoins, or $611 million, in exchange for leaking all they stole for free to the public. The unusual conditions have led some security researchers to suspect the auction is a publicity stunt. But the ShadowBrokers claim in their latest posting that the auction is real, despite "sounding crazy." "Expert peoples are saying Equation Group Firewall Tool Kit worth $1 million," the group said. "TheShadowBrokers is wanting that $1 million." They made the auction public to draw in the most bidders and never expected a bid of 1 million bitcoins, they added. "Anticipate end (to the auction) when reasonable sum raised and bidding stops," the hackers added. Although the ShadowBrokers are offering no guarantees, they did claim they have many more hacking tools that can target other platforms such as Windows, Linux and mobile devices. The tools up for auction will target one of these platforms and include ways to hack a system remotely and remain a persistent threat, they said. "Value estimated in millions of euros/dollars," the group added. It's unclear if the tools are really from the NSA. But the hackers claim to have stolen them from the Equation Group, an elite cyberespionage team suspected to work for the US government. The hackers are hoping that victims and adversaries of the Equation Group will eventually bid on the auction. But the ShadowBrokers appear to be growing impatient. Their posting was also riddled with expletives. (IDG News Service 03Oct16)

OGA

[redacted]

(U) FBI reports more attempts to hack voter registration system

(U) The US Federal Bureau of Investigation has found more attempts to hack the voter registration systems of states, ahead of national elections. The agency had reportedly found evidence in August that foreign hackers had breached state election databases in Illinois and Arizona, but it appears that there have been other attempts as well, besides frequent scanning activities, which the FBI describes as preludes for possible hacking attempts. "There have been a variety of scanning activities, which is a preamble for potential intrusion activities, as well as some attempted intrusions at voter registration databases beyond those we knew about in July and August," FBI Director James Comey told the House Judiciary Committee on Wednesday. Comey said that the systems that could be at risk were the voter registration systems that are connected to the Internet. The vote system in the US, in contrast, is hard to hack into "because it's so clunky and dispersed," he added. He advised states to get the best information they can get from the Department of Homeland Security and ensure their systems are tight as there is "no doubt that some bad actors have been poking around." The US government is not sure whether Russia, which is said to have interfered in US elections since the 1960s, aims to influence the outcome of the election or try to sow seeds of doubt about the sanctity of the process, Director of National Intelligence James R. Clapper recently told The Washington Post in an interview. Clapper said that "there's a tradition in Russia of interfering with elections, their own and others." To ensure that hackers don't get to the electoral system, the DHS is working with state election officials on best practices on security, especially where there is any dependence on the Internet, Clapper said. So far 18 states have requested the assistance of the DHS, said Secretary Jeh Johnson, in testimony this week before a Senate committee. (IDG News Service 28Sep16)

(U) Cyber firm challenges Yahoo claim hack was state-sponsored

(U) A cyber security company on Wednesday asserted that the hack of 500 million account credentials from Yahoo was the work of an Eastern European criminal gang, adding another layer of intrigue to a murky investigation into the unprecedented data heist. Arizona-based InfoArmor issued a report whose conclusion challenged Yahoo's position that a nation-state actor orchestrated the heist, disclosed last week by the internet company. InfoArmor, which provides companies with protection against employee identify theft, said the hacked trove of user data was later sold to at least three clients, including one state-sponsored group. Reuters was unable to verify the report's findings. Yahoo declined comment. The Federal Bureau of Investigation, which is investigating the hack, did not return a call seeking comment. A US government source familiar with the Yahoo investigation said there was no hard evidence yet on whether the hack was state-sponsored. Attribution for cyber attacks is widely considered difficult in both the intelligence and research communities. The task is made especially challenging by the fact that criminal hackers sometimes provide information to government intelligence agencies or offer their services for hire, making it hard to know who the ultimate mastermind of a hack might be. InfoArmor concluded the Yahoo hackers were criminal after reviewing a small sample of compromised accounts, Andrew Komarov, the firm's chief intelligence officer, said in an interview. The hackers, dubbed Group E, have a track record of selling stolen personal data on the dark web, and have been previously linked to breaches at LinkedIn, Tumblr and MySpace, Komarov said. (Reuters 28Sep16)

Items of Interest

(U) Cloud providers not expanding security as fast as customers adopt cloud

(U) Information security professionals trust the cloud even less now than they did last year, despite efforts by cloud-service providers to tighten security, according to the SANS Institute. Sixty-two percent of respondents said they are concerned that unauthorized outsiders could access data stored on public cloud services, compared to just 40 percent last year. In 2015, 33 percent of respondents said they lacked the tools and low-level access to usage data that would allow them to identify a data breach or do forensic analyses that would make incident response effective; 56 percent made the same complaint this year. InfoSec professionals seem to have accepted the ongoing migration to the cloud as inevitable, however, and are doing what they can to secure sensitive data and applications in the public cloud. "InfoSec professionals recognize the flexibility and cost-effectiveness of the cloud as clearly as anyone else, but they are still concerned that the lack of tools and visibility makes it more difficult to secure data in the cloud," according to SANS analyst and survey author Dave Shackleford. "Many are working in tandem with business unit managers to find new technologies and policy approaches to reduce that risk -- which is a big reason more companies feel comfortable storing employee and customer data in the cloud." Overall, 48 percent of respondents' organizations store employee data in the cloud, and 24 percent store customer financial data there. In addition, 27 percent use cloud-based email and messaging and 17 percent use collaboration or document management services in the public cloud. Shackleford continues, "Cloud providers do offer more security tools for their own platforms, and some have expanded support of industry standard security frameworks and reporting methods to increase visibility and integration with customers' existing security tools." For InfoSec professionals, however, the greatest challenges are still the limited ability to access data controls built into cloud platforms, integration with existing tools and the slow progress toward APIs or services to bridge the gap between internal and external security. "By this time next year we hope to see a lot more support for third-party solutions, better access for forensic analysis, and more openness about the security controls and processes cloud providers use," Shackleford says. "Cloud providers are improving, but they're not moving fast enough to address the needs of enterprises that continue to migrate sensitive data into the public cloud". (helpnetsecurity.com 04Oct16)

(U) Air Force cybersecurity campaign takes off
(U) Air Force CIO Lt. Gen. William Bender released a memo announcing a yearlong Cyber Secure campaign to address cybersecurity throughout the service. "In 2016, it is no longer adequate to have just National Cybersecurity Awareness Month," the memo states. "Going forward, we must position cyber at the forefront of our thinking, planning and operations to successfully support the five core missions" of the Air Force. Due to the interconnected nature of the expanding internet of things, "our devices, aircraft and systems are more vulnerable to exploitable attack vectors," Bender wrote. "Every time you log onto a system, click on a link, download a file or plug one device into another, we risk exposing our systems to exploitation." He added that any device that communicates with other computer systems and most modern military equipment "in some way is part of cyberspace." Bender also announced that he was establishing the chief information security office based on a recommendation from the chief of staff of the Air Force. "Industry leaders have been utilizing this approach to cybersecurity for several years, and it is time we had an enterprise strategy to protect and operate in cyberspace," Bender wrote, adding that Air Force members are the most powerful tool to augment cybersecurity. (fcw.com 04Oct16)

(U) General says US soldiers need better cyber training
(U) The US Army must begin training its soldiers to endure and then continue to fight after suffering a cyberattack on the battlefield. Gen. Gustave "Gus" Perna, commander of Army Materiel Command, said during the annual meeting of the Association the US Army, said soldiers will have to learn how to deal with a cyberattack and continue their mission, according to Military.com. Perna is fearful that unless steps are taken to procure the proper equipment and the soldiers trained in its use American forces could be at a disadvantage when in combat. "We must be able to understand what can happen to our systems through a cyberattack, and what is the enemy's capability and how do we counter that," Perna said, reported Military.com. (scmagazine.com 04Oct16)

(U) IBM Security partnership promises to patch critical vulnerabilities 'in seconds'
(U) An expanded partnership between endpoint security platform Carbon Black and IBM Security could help businesses patch vulnerabilities faster, the pair announced on Tuesday. According to a spokesperson, the new offering will be able to "prevent 85 percent of enterprise-level hacks." The press release announcing the expanded partnership said that the solution will be able to patch critical security vulnerabilities "in seconds." The two companies originally partnered up back in February 2016, when IBM announced that its X-Force Incident Response Services would use Carbon Black's Enterprise Response product in its operations. They also announced then that IBM's QRadar and BigFix would integrate with core Carbon Black products as well. Tuesday's announcement builds on that original integration, while also declaring that IBM will resell Carbon Black directly to its customers as well. According to the press release, the new offering "correlates Carbon Black's endpoint activity data with public Common Vulnerabilities and Exposures (CVE) databases to deliver a prioritized list of actively exploited vulnerabilities tailored to each organization." The problem with most enterprise security, the press release states, is that businesses tend to patch broadly due to poor visibility, and may miss a serious attack vector. The new collaborative effort between the firms seeks to increase transparency and point out which endpoint vulnerabilities need to be prioritized. Carbon Black endpoint data will be "funneled" into IBM BigFix, the press release said which is the key piece to allowing security professionals to act more quickly and make those patches in "seconds." According to the press release, it is "the only solution on the market that combines continuous and centrally recorded endpoint data with the ability to enforce policies on devices enterprise-wide to solve the pervasive patch-management problem security teams are facing. (techrepublic.com 04Oct16)

(U) Standards group releases guidelines on cyber information sharing
(U) The non-governmental Information Sharing and Analysis Organization Standards Organization has released an initial set of guidelines to promote private-sector cybersecurity information sharing. ISAOs are the non-critical infrastructure version of Information Sharing and Analysis Centers, and were established under Executive Order 13691. That directive, issued in February 2015, states: "Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis." Though voluntary, EO 13691 does call for the Department of Homeland Security to "strongly encourage the development and formation of [ISAOs]." According to executive order, "ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities." They can also be public sector, private sector or a mix, and can be either for-profit or nonprofit entities. ISAOs are designed to complement DHS' existing information sharing programs. The National Cybersecurity and Communications Integration Center is tasked with coordinating with ISAOs that wish to voluntarily share information. The ISAO SO brought together members of industry, government and academia who spent months preparing the initial guidelines. The four resulting documents, the organization said, are designed to be informational and not prescriptive. They generally pose questions for prospective ISAO members to consider before forming an ISAO. "The purpose of these efforts is ultimately to improve the ability of organizations to, as outlined in the EO, 'detect, investigate, prevent, and respond to cyber threats' while protecting the privacy and civil liberties of citizens," the guidelines state. In addition to focusing on the structure, mission and membership of ISAOs, the guidelines also stress the importance of developing trust mechanisms to encourage effective information sharing. "An ISAO can only function when a certain level of trust exists between its members, between the members and the ISAO, and between the ISAO and its partners," states the guidelines. The larger question is trust between ISAOs and DHS. So far, efforts by the department to encourage the sharing of cyber threat and breach data with the government have met with a lukewarm response by private entities. The guidelines issued by ISAO represent another evolutionary step in what has been a long process of trying to develop information sharing systems and mechanisms. And, the ISAO SO stressed that establishing an ISAO is an iterative process. "The guidelines presented in this document are intended to assist in this process by raising the most critical strategic and operational factors for consideration," the guidelines state. "ISAOs are encouraged to periodically reevaluate these guidelines as they evolve. (fcw.com 30Sep16)

(U) Curtain closes on Ransomware Encryptor RaaS, but with master key

(U) Those victims targeted over the past year by the ransomware as a service (RaaS) named Encryptor RaaS may be at a loss to ever recover their encrypted files, according to a report from Trend Micro. That is owing to the fact that after operating for a year the service has shuttered. That's the good news, Trend Micro researchers said. The bad news, however, is the developers behind the malware have taken with them into oblivion the master key. The one that would allow those victimized by the RaaS to recover their files. The ransomware, first detected in July 2015, at the time seemed to be set to rival such competitors as Tox and ORX Locker, arriving with multiplatform capabilities, customization options and an appealing price that was said to make it a good entry point for miscreants attracted to the dark side. In fact, the install was so easy, Trend Micro said, that all a client needed to do was set up a Bitcoin Wallet ID. Downloaded from the Tor network, buyers of the ransomware were required to shell out five percent of revenue rather than the 40 percent required by rival service Cerber, for example. Researchers at Trend Micro detected as late as March 2016 that the developers of the ransomware were still actively tweaking its capabilities to render it undetectable, including signing the ransomware with legitimate certificates and employing counter-AV services and crypters. With its infrastructure hidden away on the Tor network, to market the ransomware the developer went so far as to offer a file-signing service for his clients, promising stolen Authenticodes that allowed him to sign Encryptor RaaS samples at no cost. "Four months after, however, the service abruptly closed up shop," the researchers wrote. The fall may have been the result of detection after a C&C server was exposed and its systems detected on a valid cloud service. After a few sputters and attempts to relaunch, it was shut down completely. As of early April 2016, the Trend Micro researchers observed the affiliate chat forum exploding with animosity between the developer and clients dissatisfied with the shutdown. The curtain closed on 5 July 2016, with the developer, who goes by the handle "jeiphoos," alerting victims that they can no longer recover their files, as he deleted the master key, Trend Micro reported. (scmagazine.com 29Sep16)

(U) Energy sector addressing cybersecurity threats

(U) An international organization said Thursday a group of energy companies joined it in forming an industry body to tackle cybersecurity threats. "We see that cyber-security incidents are increasing with attempted attacks on a daily basis," Rune Waerstad, an engineer at Royal Dutch Shell, said in a statement. "By collaborating with others in the industry, we can ensure that we end up with one globally applicable regulation that is suitable for the oil and gas sector." The industry's certification body DNV GL estimates cybercrimes costs the energy and utilities sector about $12.8 million each year in lost business and equipment damage. For those focused on operations offshore, the group said a layer of confidence is needed as cybercrime evolves as a bigger and more complex threat to the industry. So far, eight companies from Shell to Norwegian major Statoil teamed up to for an industry partnership to address the emerging threat. A report on the cost of cybercrime by HP Enterprise Security found energy and utility companies suffered a greater financial loss than the financial sector. DNV GL said the scope of the joint industry partnership was to offer guidelines to tackle the emerging threat. The industry body is already working alongside French supermajor Total to address risk management at its operations off the coast of Norway. "Dealing with cyber-security challenges has become a key focus area for the oil and gas sector," DNV GL consultant Pal Borre Kristoffersen said. "Attacks are becoming increasingly costly and harder for companies to recover from". (UPI 29Sep16)

[redacted]

OGA

[redacted]

(b)(3) 10 USC ⊥ 424

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

[redacted]

(b)(3) 10 USC ⊥ 424