



Homeland
Security

TEFT GREEN

AUGUST 2016

THE
WASP

CYBERSECURITY SITUATIONAL AWARENESS



THE WASP

CYBERSECURITY SITUATIONAL AWARENESS

TOP: GREEN


AUGUST 2016

CONTENTS



NCCIC Metrics

- 4** NCCIC Cyber Analytics Report
- 5** NCCIC Reported Federal Incidents




NCCIC Cyber HIGHLIGHTS

- 6** Featured Article
 - » Security Software Flaws Lead to Growing Concerns over Broader Industry Challenges
- 9** Current Activity
 - » U.S. Democratic National Committee (DNC) Cyber Intrusion
 - » Let's Not Forget About the Classics
- 13** Emerging Technology
 - » Fansmitter Malware
 - » Exploiting Wearable Devices
 - » Contactless Infusion X5



NCCIC PARTNER SPOTLIGHT

- 17** Office of Cyber and Infrastructure Analysis
 - » Seaport Operations and Possible Consequences from Malicious Cyber Activity



NCCIC PUBLICATIONS

- | | |
|--|---|
| <ul style="list-style-type: none">21 US-CERT Products<ul style="list-style-type: none">» Analysis Reports» Indicator Bulletins» Malware Analysis Reports» Malware Initial Findings Reports» Security Bulletins» Security Publications» Technical Alerts | <ul style="list-style-type: none">22 ICS-CERT Products<ul style="list-style-type: none">» ICS-CERT Monitor» Industrial Control System Advisories/Alerts |
|--|---|



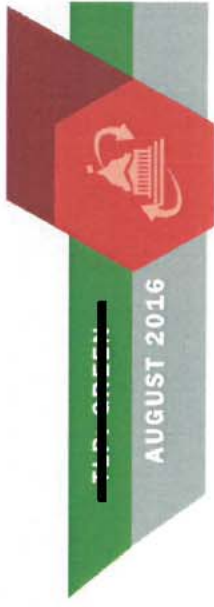
THE WASP

CYBERSECURITY SITUATIONAL AWARENESS

AUGUST 2016

DISCLAIMER: This product is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this report or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

NCCIC Metrics



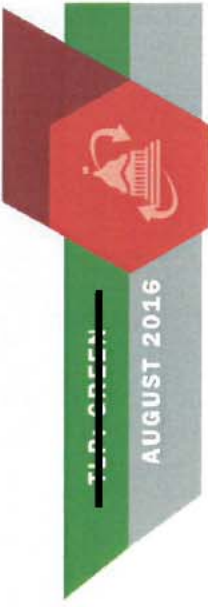
NCCIC Cyber Analytics Report

- 1 NCCIC Totals
- 2 NCCIC Monthly Cyber Analytics Report by Branch

*Monthly numbers reported are totals from previous month

1		2	
July 2016	FY15	July 2016	FY16 YTD
<p>Total Incident Reports from Federal, Critical Infrastructure Organizations, and International Partners</p>		<p>(b) (7)(E)</p>	
<p>Vulnerabilities Detected Through Scans and Assessments</p>		<p>(b) (7)(E)</p>	
<p>Security Alerts, Bulletins, and Other Products</p>		<p>(b) (7)(E)</p>	
Reporting Organizations	Measure Description	July 2016	FY16 YTD
US-CERT	Indicators Shared - ECS	(b) (7)(E)	(b) (7)(E)
ICS-CERT	Cyber Security Evaluation Tool (CSET) Downloaded and Distributed	(b) (7)(E)	(b) (7)(E)
	ICS-CERT Products Developed for Critical Infrastructure Asset Owners	(b) (7)(E)	(b) (7)(E)
	New Critical Infrastructure Incident Response Tickets	(b) (7)(E)	(b) (7)(E)
	Newly Opened Vulnerability Tickets Affecting ICS	(b) (7)(E)	(b) (7)(E)
NCC	Communications Incident Reports from Federal, Critical Infrastructure Organizations	(b) (7)(E)	(b) (7)(E)
Operations & Integration	Situational Awareness and Vulnerability Products Produced	(b) (7)(E)	(b) (7)(E)
MS-ISAC	Vulnerabilities Detected	(b) (7)(E)	(b) (7)(E)
	Vulnerabilities Mitigated	(b) (7)(E)	(b) (7)(E)
	Incident Reports	(b) (7)(E)	(b) (7)(E)

NCCIC Metrics



Monthly Reported Federal Incidents



- 1 By Category
- 2 By Percent Difference
- 3 By Category & Sub Category

3

Category	Sub Category	June 2016	July 2016
01 - Unauthorized Access	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
02 - Denial of Service (DoS)			
03 - Malicious Code			
04 - Improper Usage			
05 - Scans/Probes/Attempted Access			
06 - Investigation			

1

(b) (7)(E)

2

(b) (7)(E)



JUNE 2016
JULY 2016

Cyber Highlights

FEATURED ARTICLE: SECURITY SOFTWARE FLAWS LEAD TO GROWING CONCERNS OVER BROADER INDUSTRY CHALLENGES

In late June 2016, Google security researcher Tavis Ormandy and the Project Zero security team reminded the cybersecurity community of its ever-expanding attack surface with revelations of critical vulnerabilities he discovered in Symantec and Norton antivirus security software product lines.¹ That miscreants could potentially leverage the same security software designed to protect our personal computers, mobile devices, as well as our Nation's critical information networks and systems to aid in their attacks against them is alarming. While Ormandy admits that some of the flaws he discovered were basic and should have been caught by the company in the code development and review phase of production, others were much more serious.² It should be noted that the most critical vulnerabilities discovered were proof-of-concept exploits, and at the time of this report Symantec was unaware of exploitation of or adverse impacts to customer networks or systems.³

Technical Details

One of the most critical vulnerabilities uncovered in the Ormandy-led Project

Zero reports include a serious flaw in the "Decomposer" of Symantec's antivirus scan engine.⁴ The decomposer is a major component in their security software product line and is responsible for unpacking archive file formats such as ZIP and RAR.⁵ Ormandy discovered that the company likely based their RAR decompression on an outdated version of the open-source unrar code by RAR Labs released in January 2012.⁶ Ormandy also verified that exploitation of multiple publicly known vulnerabilities could result in wormable remote code execution as NT AUTHORITY\SYSTEM on Windows and root on Linux and Mac rendering the following products critically vulnerable: Norton Antivirus (All Versions, All Platforms), Symantec Endpoint Protection (All Versions, All Platforms), Symantec Scan Engine (All Platforms), Symantec Email Security (All Platforms), Symantec Protection Engine (All Platforms), Symantec Protection for SharePoint Servers, etc.^{7,8} One of the major discoveries from the Project Zero reports were Symantec's use of the kernel to host their decomposer, which led to, in certain cases on Windows, vulnerable code execution resulting in remote kernel memory corruption.^{9,10}

The kernel is the central module of an operating system usually loaded into a protected area of memory to prevent it from being overwritten by programs or other parts of the operating system and is typically responsible for memory, process and task, and disk management.¹¹

Impact

These recently discovered critical vulnerabilities impact the entire Symantec and Norton security software product lines and provide an avenue for hackers to gain remote code execution on Windows and root access to Linux and Mac operating systems.^{12,13} Furthermore, some of the reported vulnerabilities require no user interaction and are network-aware, potentially resulting in the creation of computer worms.¹⁴ Symantec rated its Linux, Mac, and UNIX platform unpacking vulnerability a 9.1/10 severity score in the Common Vulnerability Scoring System and mentioned in its advisory that, "the most common symptom of a successful attack would result in an immediate system crash, also known as Blue Screen of Death."¹⁵

With over \$6.5 billion in reported net revenue last fiscal year, ranking fifth and sixth in antivirus vendor (7.1 percent) and antivirus product (3.6 percent) market share respectively, the use of Symantec's business and personal consumer security products is widespread across the federal, state, local, tribal, and territorial, private sector, and international cybersecurity enterprise.^{16,17} Furthermore, although some automated patching from Symantec has been pushed to many customers to address the critical vulnerabilities exposed in the Project Zero reports, not all customers are capable of receiving automated patching to their systems, which means a significant amount of machines are likely still at risk.¹⁸

Industry Challenges and Implications

Tavis Ormandy and Google's Project Zero team are no strangers to



proof-of-concept exploitation of security software products. Over the past year, the team has exposed flaws in security software for high-profile antivirus vendors such as Avast, AVG Technologies, Comodo, Eset, FireEye, Intel Security, Kaspersky Lab, McAfee, Trend Micro, and others, leaving many cybersecurity experts and business and personal consumers concerned about the broader implications to the industry as a whole.^{19,20} Many of the flaws uncovered in previous research included vulnerabilities that would have allowed attackers to remotely execute malicious code on systems, abusing the functionality of the security software to gain higher privileges on those systems and to defeat the anti-exploitation defenses of third-party applications.²¹ Security software including antivirus protection, intrusion detection and prevention systems, and firewalls, due to their trusted code status and high levels of privilege granted on critical systems, provide ideal targets for hackers seeking opportunities to compromise entire enterprises.²² Nonetheless, while many security researchers are concerned that software manufacturers lack rigorous and consistent quality assurance and control processes, few security firms have focused efforts on identifying and addressing vulnerabilities in these products.

There has been speculation from the cybersecurity community regarding the security software industry's persistent challenges in developing secure code for its antivirus products. While some experts believe the issues lie in the industry's ability to recruit and retain software designers that understand secure development or its use of riskier programming language (i.e., C and C++) in developing security software, others believe that its continued reliance on outdated legacy code in its antivirus

products is to blame.²³ These problems are exacerbated by an ever-increasing attack surface due to antivirus programs' need to inspect large amount of data and information from a variety of sources (e.g., email, network shares, local file systems, USB attached storage devices); the large number of antivirus components that implement layered protection (i.e., drivers for intercepting network traffic, plug-ins that interact and integrate with browsers and email clients, graphical user interfaces, and subsystems that perform signature-, behavior- and cloud-based scanning and more); and users' tendency to grant antivirus programs with the highest possible levels of privilege on their systems and networks.²⁴

Industry Outlook

Targeting antivirus software or exploiting vulnerabilities in the software to evade detection is no new phenomenon. There is much evidence to suggest that foreign intelligence services and other advanced persistent threat groups have targeted antivirus products for years. For example, over at least a five-year period between 2009 and 2014, a sophisticated cyberespionage campaign, Careto (a.k.a. "The Mask"), used multi-platform malware to compromise the computers of hundreds of government and private organizations in over 30 countries.²⁵ During the operation, among other tactics, techniques, and procedures (TTPs), the hacker group exploited a vulnerability in older versions of Kaspersky's antivirus products (patched in 2008) to avoid discovery on critical networks and systems across the globe.²⁶ Moreover, previous reporting has cited cases where nation-state actors have subverted security measures and antivirus protection to compromise and reprogram certain hard drive brands

to ensure the malware remained undetected by security software.²⁷ These and many other similar campaigns launched over the past decade have made it clear that security software is an area of opportunity for hackers that should not be overlooked and could reap significant reward.

As a whole, the security software industry continues to fight against the notion that their products tend to either make companies more vulnerable or do not justify the time and money spent. Over the past few years, security experts have become more vocal in their criticism of antivirus protection and have concluded that most hackers who target their organizations typically utilize new TTPs that avoid antivirus detection altogether.²⁸ Complicating matters, free websites such as Virus Total allow hackers to test their attack methods against the most popular malware scanning engines prior to launch. However, some experts believe that antivirus vendors have improved their product offerings over the last few years, delivering new features beyond basic malware protection making the investment in endpoint protection platform (EPP) worthwhile.

Endpoint protection platform generally comprises a collection of products to include anti-malware, anti-spyware, personal firewalls, host-based intrusion prevention, and port and device control.²⁹

Yet, over the past few years, the enterprise EPP market has suffered from virtually flat revenues even as

the number of reported seat licenses sold has increased, indicating a slight decline in the license revenue per seat.³⁰ Due to organizations' growing focus on and commitment to next generation cybersecurity solutions, this trend is likely to continue over the next few years.³¹

Mitigation Options and Best Practices

NCCIC encourages users and network administrators to patch Symantec or Norton antivirus products immediately. While there has been no evidence of exploitation, the ease of attack, widespread nature of the products, and severity of the exploit may make this vulnerability a popular target.³² According to Symantec, any user that utilizes Symantec or Norton antivirus products who have not taken steps to mitigate risk from the recently discovered vulnerabilities should:³³

- Restrict access to administrative or management systems to authorized privileged users.
- Restrict remote access, if required, to trusted/authorized systems only.
- Run under the principle of least privilege where possible to limit the impact of potential exploit.
- Keep all operating systems and applications current with vendor patches.
- Follow a multi-layered approach to security. At a minimum, run both firewall and anti-malware applications to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network- and host-based intrusion detection systems to monitor network traffic for signs of anomalous

or suspicious activity. This may aid in the detection of attacks or malicious activity related to the exploitation of latent vulnerabilities.

Most experts agree that antivirus alone cannot address enterprise security and should be used as one approach in a multi-layered cybersecurity strategy. The following are general best practices and recommendations that organizations should consider implementing in addition to antivirus protection:

- Organizations should implement a multi-layered strategy that combines traditional antivirus software with intelligence sharing, next generation protection tools, security services, training for IT professionals, and routine security assessments applied to applications, hardware, and software.³⁴
- The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) recommends applying application whitelisting in a phased approach to only allow pre-approved programs and services to run.³⁵
 - » NIST encourages organizations to perform risk assessments prior to implementing this technique to determine whether full deployment is feasible and beneficial to their unique environments.
 - » NIST advises that application whitelisting requires a dedicated staff in the same way antivirus and intrusion detection technology does, so resource constraints should be considered.



Cyber Highlights

CURRENT ACTIVITY: U.S. DEMOCRATIC NATIONAL COMMITTEE (DNC) CYBER INTRUSION

Created during the Democratic National Convention in 1848, the DNC is the oldest continuing party committee and is responsible for governing the Democratic Party, coordinating and planning its presidential nominating convention, and promoting the Party's platform.¹ Governed by its Charter and Bylaws, the DNC comprises chairs and vice-chairs of each state Democratic Party Committee and over 200 members elected by Democrats in all 50 states and territories.²

In late April, CrowdStrike, a cybersecurity firm that analyzes threats to network security and specializes in cyber threat intelligence, was contacted by the DNC to investigate its party's networks for malicious cyber activity.³ As a result of its investigation, the company publically released a comprehensive report in mid-June that revealed evidence of two separate data breaches into DNC networks they believe to be the work of two sophisticated Russian intelligence affiliated hacker groups, Fancy Bear (also known as Sofacy and APT 28) and Cozy Bear (also known as Cozy Duke and APT 29), all names designated by commercial security firms.⁴ According to CrowdStrike, Fancy Bear and Cozy Bear have previously infiltrated unclassified networks for the White House, State Department, and U.S. Joint Chiefs of Staff, as well as businesses across

the Aerospace, Defense, Energy, Extractive, Financial Insurance, Legal, Manufacturing, Media, Think Tanks, Pharmaceutical, Research, and Technology industries, and other U.S. and foreign government entities and other military and defense ministry-centric organizations.⁵

CrowdStrike revealed that Cozy Bear's intrusion of DNC networks occurred in summer 2015, while Fancy Bear breached DNC networks sometime in April 2016. The intrusion provided the hacker groups with sensitive information, including an entire database of opposition research on GOP presidential candidate Donald Trump, all DNC emails and chat messages, and a number of DNC voicemail messages.^{6,7} Weeks after the DNC discovery, the Democratic Congressional Campaign Committee (DCCC)—the official campaign arm of the Democrats in the House of Representatives—revealed that its networks had been compromised in what appeared to be a sophisticated cyber threat campaign similar to the DNC breach. U.S. security firms, ThreatConnect and Fidelis, teamed up to investigate the compromise and ultimately concluded that Fancy Bear was likely the responsible party.⁸ This assessment was supported by German intelligence, which indicated that the servers used to register four associated suspicious domains were the same ones used in the DNC breach that resolved to a Fancy Bear command and control (C2) IP address.⁹ Finally, both compromises included the use of the exact same fictitious registrant email addresses used to register faux domains.¹⁰

Immediately following the DNC revelations and CrowdStrike's public attribution of Russian government involvement, cyber actor(s) by the

moniker "Guccifer 2.0" leaked a series of DNC documents to the public, claimed to have been exfiltrated from DNC servers.¹¹ A number of U.S. private cybersecurity and intelligence firms have released moderate to high-confidence assessments indicating the "Guccifer 2.0" leaks are part of a Russian disinformation campaign to offer the Kremlin plausible deniability.^{12,13,14}

Tactics, Techniques, and Procedures

According to a number of cybersecurity experts, many of the tactics, techniques, and procedures (TTPs) used in the DNC compromise are strikingly similar to past network intrusions and malicious activity associated with Russian intelligence operations. Multiple private security firms and experts have corroborated evidence of Russian involvement, including the use of malware and methods identical to those used in other previous attacks attributed to the Fancy Bear and Cozy Bear. One example is the use of an SSL certificate and command-and-control address hardcoded into the DNC malware used in a 2015 hack of the German Parliament that German security officials attributed to Russian military intelligence. Fancy Bear has also been linked publicly to France TV5 Monde TV station breach and the German Bundestag breach last year.^{15,16,17}

In their detailed DNC assessment, CrowdStrike, having monitored both Fancy Bear and Cozy Bear activity prior to this incident, revealed some of the most common TTPs used by each group in previous attacks:

- Leveraging of a wide range of sophisticated implants as well as malware



for Linux, OSX, IOS, Android, and Windows phones.¹⁸

- Domain registration that closely resembles the domains of legitimate organizations to lure victims into its established phishing sites on those domains to steal victims' credentials.¹⁹
- Reliance on broadly targeted spearphishing campaigns that include malicious web links to droppers that, once activated on a system, deliver sophisticated, highly configurable, and customizable remote access tools (RATs) that evade detection and give the hackers control of the machines.²⁰

Although both groups are believed to have compromised the DNC network, no collaboration between the two actors was discovered during the CrowdStrike investigation. This phenomenon is not uncommon, as according to the European Council on Foreign Relations, the relationship between Russia's domestic and military intelligence agencies is highly adversarial at best.^{21,22}

Cyber Highlights

CURRENT ACTIVITY: LET'S NOT FORGET ABOUT THE CLASSICS

Ransomware is a hot topic within the cybersecurity community and the fastest growing malware threat today.²³ In 2016, more than 50 new variants of ransomware have already been identified, more than was seen in 2014 and 2015 combined.²⁴ Regardless of the success and prevalence of ransomware, it is good to remember that cyber criminals still use other varieties of malware that have been around for years, like banking trojans, in order to make a profit.

Banking trojans consist of malware designed to target banking services and typically rely on email spam campaigns, social engineering, downloader malware, and drive-by download attacks via exploit kits to steal financial information of bank customers and businesses for profit.²⁵ Once installed, the malware waits for users to access their online banking websites to steal banking credentials through screen captures, keylogging, or man-in-the-middle attacks. Even though financial credentials are the primary target for the malware, banking trojans can steal other information and credentials to compromise other accounts or more systems.²⁶

Threat Analysis

Symantec reporting indicates that banking trojans have been in decline for the past few years, likely due to takedown efforts of law enforcement against

criminal groups and their botnets, as well as cyber criminal's transition to ransomware and other money making schemes.²⁷ Figure 1 shows a significant drop in the number of systems detected by Symantec that were compromised by banking trojans. The decline in numbers could be misleading; malicious cyber actors may simply be getting better at surreptitiously accessing targets that give the best success in defrauding accounts.²⁸

Even with this decline, banking malware remains a threat to individual customers and the financial industry worldwide. Recent reporting has seen an increase in malware campaigns targeting multiple countries. This can

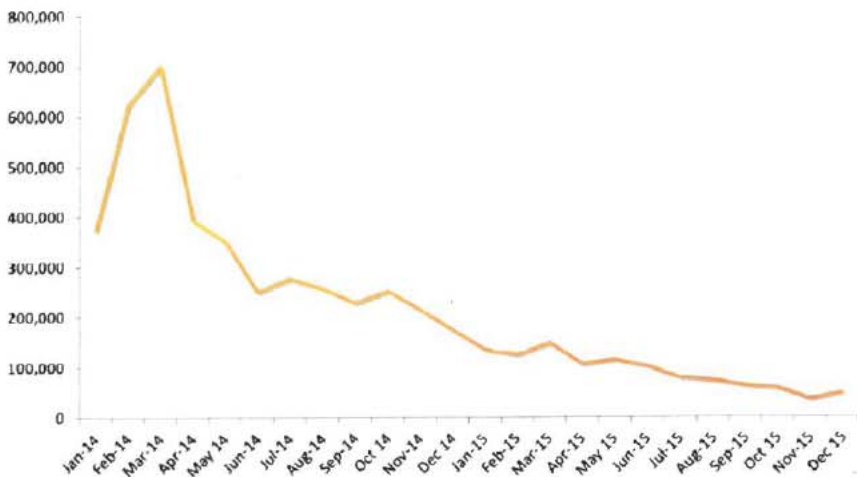


Figure 1 - Computers Compromised with Banking Trojans, 2014-2015²⁹

be indicative of an increase in the sophistication and organization of cyber criminal groups, since changes in target geography require significantly more effort than simple changes to malware configuration files.³⁰ Malware authors also continually work to improve the efficiency and capability of their software to expand victim targeting, improve obfuscation, and maximize profit. Some recent reports include:

- Security firm Proofpoint detected a surge of banking Trojans targeting Canadian businesses and citizens, that while not uncommon, the volume and diversity of the campaigns indicated a notable rise. Six different malware variants were observed, to include Dridex, Zeus, Kronos, Gootkit, Ursnif and Vawtrak. It was noted that all the campaigns observed used unsolicited spam email as the distribution method.³¹ The spam messages used macros, packager shell objects, and web links to deliver malicious payloads to users.³²

- IBM X-Force researchers reported that operators of the GozNym banking malware were testing out redirection attacks on four of the largest banks in the United States, with a focus on business banking services.³³ GozNym is a hybrid of both the Nymaim and Gozi ISFB malware. The Nymaim malware source code provides stealth and persistence, while the Gozi ISFB code adds the banking Trojan's capabilities to

facilitate fraud via infected Internet browsers.³⁴ GozNym uses redirection attacks to hijack malware-infected users to a website that looks exactly like their bank's site and has them log into their account in a completely unprotected environment. The bank's website is not being compromised in any way and the fake sites are perfect replicas, hosted on servers the cyber criminals control. According to attack volume data reported by IBM, the malware is quickly becoming a top global player, ranking fifth in the cybercrime arena for 2016, as of June 2016.³⁵

- Researchers at Sophos Group recently reported that the Vawtrak banking trojan (aka Snifula) is slowly but surely becoming a serious threat.³⁶ They are calling the latest iteration Version 2 (v2), stating that the malware has acquired the capability to target even more users, introduced a modular architecture, and has better obfuscation. These new capabilities use encryption and changes in parameter functions to hinder data analysis by cybersecurity professionals.³⁷ Vawtrak v2 targets customers of banks and financial companies in the US, the UK, Ireland, the Czech Republic, Canada, Japan, Romania and Israel. Apart from financial institutions, the malware can also inject websites of some online retail companies, telecoms, and social media companies.

Recommended Best Practices

One way to reduce the threat of banking trojans is to adopt better security practices for online banking. Online banking involves certain risks. If using online banking to conduct financial transactions, consumers need to be aware of the risks and take precautions to minimize them. The following practices can help consumers avoid common security problems associated with banking trojans and online banking:³⁸

- Protect your computer
 - » Install anti-virus, firewall, anti-spyware, and anti-malware programs on your computer and keep them up to date using automatic updates. The same applies to operating systems and Web browsers. Also use Web content filters to block ads that may contain drive-by downloads.³⁹
- Verify email correspondence from bank
 - » Do not reply to any email requests for security information, warnings of an account suspension, opportunities to make easy money, or overseas requests for financial assistance. Also, links found in these suspicious emails should not be clicked. Forward phishing emails to spam@uce.gov, and to the company, bank, or organization impersonated in the email.

- Do not access your account from public locations
 - » Avoid situations where personal information can be intercepted, retrieved, or viewed by unauthorized individuals. Conduct online bank transactions in locations that are not subject to public monitoring and avoid using any computer that other people can freely access; it is possible for your account information to be stored in the web browser's temporary memory.
- Check your account balance regularly
 - » Timing is a factor in your response to unauthorized electronic fund transactions. If you receive a paper account balance, make sure that you reconcile it with your online balance.
- If your account is compromised, take swift action
 - » File a report with the following organizations:
- Associated bank
- Local police
- Federal Trade Commission – www.ftc.gov
- Internet Crime Complaint Center – www.ic3.gov
- The three major credit bureaus (Equifax, Experian, and TransUnion)

Cyber Highlights

EMERGING TECHNOLOGY:

When it comes to developing new methods, ideas, or products affecting cyberspace, innovation isn't limited to researchers, software engineers, or cybersecurity professionals. Malicious cyber actors continually look for new ways to gain unauthorized access to networks and systems, install malicious software to do harm or for profit, or exfiltrate data for personal, political, or economical gain. The following examples are of emerging technology, concepts, or techniques being developed by the cybersecurity community or cyber malicious actors that could be of interest to the NCCIC and our partners.

FANSMITTER MALWARE

Researchers from the Ben-Gurion University in Israel have reportedly discovered a method to steal data from a computer by hijacking the cooling fans contained within and manipulating the sounds they create. The malware, dubbed Fansmitter, targets air-gapped systems by controlling the speed of the internal fans, altering the audio waves generated and using those audio waves as a covert communication channel to send data to another device.¹ Exfiltrating data from air-gapped systems via covert communication channels is not a new concept. There have been several different techniques reported over the years that can allegedly exploit air-gapped systems:

- In 2015, Cyber Security Labs demonstrated a proof-of-concept attack that leveraged a computer's heat emissions and a computer's built-in thermal sensors to transfer data between systems. While reportedly successful, there are significant limitations. The attack only transfers 8 bits of data per hour and the systems have to be within 40 centimeters of each other.²
- In 2014, Cyber Security Labs researchers developed a proof-of-concept technique called AirHopper that uses radio signals to covertly send data from an infected computer to a receiving mobile phone. The malware uses a computer's video card to generate radio signals that transmit modulated data that is received and decoded by the FM radio receiver built into mobile phones.³ The same researchers later introduced GSMem, malware that is based on the AirHopper concept, but uses cellular frequencies sent over multi-channel memory buses.⁴
- In 2013, German researchers investigated the feasibility of BadBIOS, malware that allegedly used high-frequency transmissions to jump air-gapped systems. While they were unable to corroborate the existence of BadBIOS, they were able to show that high-frequency networking was possible using a network stack based on a communication system originally

Air-gapped computers are systems that typically store sensitive or confidential information and are physically isolated from the Internet or other less secure networks.

designed for underwater communication.⁵

What makes Fansmitter unique is that its method of attack can exfiltrate data acoustically, even when audio hardware and speakers have been disabled or removed. Most computers use fans to move air through the chassis and to keep electronic components, like the main CPU and graphics card cool. The sound produced by these fans is the result of rotating blades forcing air past static vanes. The number of blades and their rate of rotation determine the frequency of the sound produced. If the rotation rate changes, the frequency of the sound changes.⁶

Technical Details

Fansmitter's attack model enables a covert out-of-band communication channel between a transmitter and receiver, both of which have to first be compromised in the preliminary attack phase. In the researcher's scenario, a personal computer was used as the transmitter and a mobile smartphone acts as the receiver. Researchers were able to demonstrate the effective transmission of encryption keys and passwords with a bit rate of up to 900 bits/hour. The information was transmitted using a special protocol that divides the data into packets made up of a preamble and a payload. The preamble consists of the signal 1010, which the listening device (receiver) can use for calibration. This is followed by a payload of 12 bits that encodes the data to be transmitted, which can then be picked up by a listening device within 8 meters of the transmitter.⁷ Figure 1 shows the acoustic signal received by a mobile phone from multiple distances.

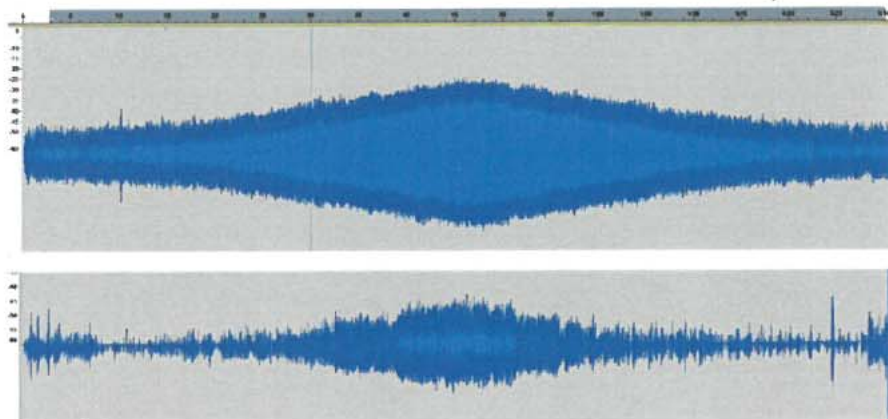


Figure 1 – The acoustic signal of a CPU fan, as received by a mobile phone from one meter distance (upper figure) and four meters (lower figure)

Conclusion

Successful execution of this type of attack takes a high degree of coordination, as it is reliant on both the transmitting and receiving devices to be initially compromised and be in fairly close proximity (8 meters or less) to one another, but it is still a possible attack vector. The Fansmitter research team believes that the technique can also be used to leak data from different types of IT equipment, embedded systems, and Internet of Things devices that have no audio hardware, but contain fans of various types and sizes.⁸ Potential countermeasures include generating enough background noise that acoustic transmissions are impossible, replacing fans with specialized quiet ones or using a water cooling system, or keeping sensitive computers in restricted areas where mobile phones and other recording devices are banned.⁹

EXPLOITING WEARABLE DEVICES

As networked, wearable devices—Fitbits, Jawbones, Samsung Gears, and Apple Watches—become more enmeshed in our daily lifestyle, the threat to the personal data these devices can collect, both knowingly and unknowingly, rises exponentially. Computer scientists from the Stevens Institute of Technology and Binghamton University recently performed a study that suggests that many smartwatches and fitness trackers can be exploited and leveraged to steal PIN codes, like those used in automated teller machines (ATMs).¹⁰ The researchers created a computer algorithm, named Backward PIN-Sequence Inference, that can guess a password or PIN with about an 80 percent success rate on the first attempt, and over 90 percent within three attempts.¹¹ The algorithm predicts the PIN codes using motion data collected by the wearable device's accelerometer, gyroscope, or magnetometer. Attackers can get this information either by infecting the wearable device with malware or intercepting the Bluetooth connection

linking the device to another device, like a smartphone. This poses a new and potentially serious security flaw in the “what you know” authentication mechanism of key-based security systems.

Technical Details

The research team provided 20 participants with three different wearable devices, and instructed them to make approximately 5,000 sample PIN entries on keypads or laptop keyboards. Using a nearby wireless sniffer, the team captured Bluetooth Low Energy data packets transmitted by sensors in the wearable devices to a paired smartphone. Sensor data was then extracted from the Bluetooth packets and used for the subsequent attack.¹²

The attack technique consists of two primary components, (1) the development of millimeter-level distance estimation and direction derivation schemes that capture fine-grained hand movements from sensor data, and (2) the implementation of the Backward PIN-Sequence Inference algorithm that exploits the key entering sequence.¹³ The first estimates the distance and direction of hand movements between consecutive keystrokes, and the second combines those estimates to infer the entire key entry sequence of the targeted user based on the spatial and temporal constraints between key entries. An interesting point is that the algorithm determines the PIN sequence in a reversed manner, beginning with the “Enter” key. This makes sense, since many key-based security systems require the user to hit “Enter” as the final significant hand motion after entering a code.¹⁴

Conclusion

According to the Stevens research team, this is the first technique that reveals personal PINs by exploiting information from wearable devices without the need for contextual or relevant information.¹⁵ The research is still new but the team's findings are indicative of the need for better understanding of the security vulnerabilities inherent in wearable

devices. Countermeasures are still being investigated, but one initial suggestion by the team is to inject "noise" into sensor data so it cannot be used to derive fine-grained hand movements, but still allows for fitness and other movement tracking. Better encryption between the wearable device and the paired device (smartphone, tablet, etc.) is also recommended.

CONTACTLESS INFUSION X5

A criminal group going by the name, The CC Buddies, is selling a device on the Dark Web that they claim is capable of copying data from contactless debit cards if held as close as eight centimeters away from the victim's card. The group claims its device can copy up to 15 contactless cards per second and was selling the device, as well as associated cables and software, for 1.2 bitcoins (approximately \$825) at the time of the referenced article.¹⁶ Figure 2 shows a screen capture of the CC Buddies website on the Dark Web.

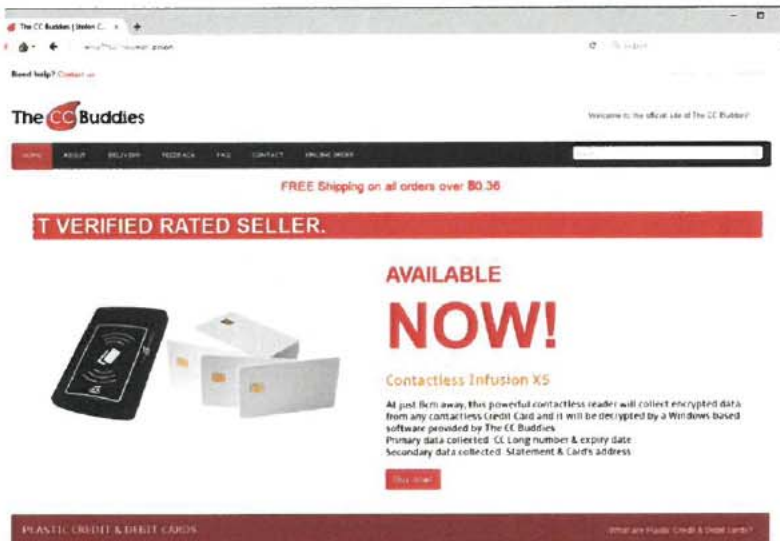


Figure 2 – Screen Capture of CC Buddies Website on the Dark Web

Technical Details

Contactless cards have embedded computer chips that use RFID (radio-frequency identification) technology for wireless data transfer capability and EMV chip technology, which is becoming the global standard for inter-operation between chip-based credit and debit cards and associated payment systems (e.g., EMV capable point-of-sale terminals and ATMs).¹⁷ This technology is slowly replacing payment cards using magnetic stripes, as it is presumed to be more secure and will reduce counterfeit fraud rates.¹⁸

EMV stands for the names of the original developers of EMV chip technology: Europay, MasterCard, and Visa.

The Contactless Infusion X5 allegedly copies the credit card number and expiration date from the chip of the victim's card and encrypts the data. If additional information is stored on the victim's RFID-capable chip, the XC5 is able to copy that information as well and store it internally, until the malicious actor connects the device to a computer and downloads the data.¹⁹

CC Buddies also claim the X5 is capable of detecting and reading any bank card at 1024kpbs (kilobits per second) within a distance of eight centimeters. The device is purported to have a built-in 5V battery with 10 hours of battery life and the ability to read any card that operates at 13.56MHz (megahertz), however, it can currently only decrypt bank cards.²⁰

Conclusion

Per online security news website, TechWorm, the Contactless Infusion X5 is believed to be the first RFID scanning tool that specifically targets contactless cards.²¹ If CC Buddies' claims for the Contactless Infusion X5 are valid, the device could potentially hack hundreds of contactless cards in a short period of time, especially in crowded areas like subways, malls, or concert venues. However, advertisement of the device's capability may be a scam by thieves trying to make money off of other gullible thieves. Additional research found at least one report calling the CC Buddies fraudsters and providing evidence that the X5 is really just a contactless reader produced by Advanced Card Systems Holdings Limited (ACS) that sells for only \$59.²² Figure 3 shows the ACR1281U-C2 Contactless Reader, offered by ACS. The device appears very similar to the X5.



Figure 3 – Screen Capture of ACR1281U-C2 Contactless Reader Offered by ACS



NCCIC Partner Spotlight

OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

SEAPORT OPERATIONS AND POSSIBLE CONSEQUENCES FROM MALICIOUS CYBER ACTIVITY

In the United States and its territories, approximately 3,200 cargo and passenger handling facilities are located within 360 commercial ports. Of these, about 150 are deep-water seaports administered by 126 public seaport agencies.^{1,2} The primary role of seaports is to facilitate the movement of trade to both foreign and domestic markets. Seaports are critical facilities in the export and import of raw and finished goods and in the movement of goods across the United States. According to a 2015 study completed for the American Association of Port Authorities, seaports in the United States had a total economic value in 2014 of \$4.56 trillion. Of this, \$124.45 billion was direct business revenue, and \$4.3 trillion was the economic value created by the movement of cargo through seaports.³ Seaports in the United States are dependent on the Energy, Communications, Information Technology (IT), and Transportation Systems Sectors for daily operations.

Ports and vessels use many information systems and communications technologies for various functions such as navigation, communication, equipment operation, cargo movement and tracking, business operations, and security.⁴ A cyber-attack by malicious actors on networks at a port or aboard a ship can result in lost cargo, port delays, disruptions, and physical and environmental damage, depending on the systems affected. The impact to port operations, which could last for days or weeks, would depend upon the damage done to the port's networks and facilities. Examples of malicious actors gaining access to terminal operating systems and cargo databases include hackers recruited by an organized crime group to breach IT systems used to control the movement and location of containers at the Port of Antwerp, Belgium, between 2011 and 2013. Hackers first gained access to the network by sending malware to port staffs' accounts. After the initial breach was discovered

and mitigated, miscreants physically broke into port premises and attached hardware key-logging devices onto computers. The group hid narcotics among legitimate cargo, and gained unauthorized access to IT systems, which gave them the location and security details of containers, so they could send in drivers to steal the cargo before the legitimate owner arrived.^{5,6} In 2012, crime syndicates penetrated the cargo systems used by Australian Customs and Border Protection, allowing them to determine if authorities were suspicious of their shipping containers.^{7,8}

Seaport cyber vulnerabilities, if unaddressed, could pose a significant risk in port facilities and aboard vessels within the Maritime Subsector. Potential vulnerabilities include limited cybersecurity training and preparedness, errors in software, inadequately protected commercial off-the-shelf technologies and legacy systems, network connectivity and interdependencies, software similarities, foreign dependencies, GPS jamming or spoofing, and insider threats.

A lack of emphasis on cybersecurity training and preparedness for personnel at ports and aboard vessels can also increase cyber vulnerabilities because reduced awareness by personnel increases the potential for malicious activities and limits best practice guidelines.

Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) and distributed control systems, are used throughout the Maritime Subsector, including in operations such as loading, unloading, and transportation of bulk and containerized cargo (See Figure 1 and 2). Modern ICS often use commercial off-the-shelf technologies that are network-based and connected to other systems. In addition, the growing integration of legacy SCADA systems into modernized networks presents new targets for malicious actors. Furthermore, the increased use of common operating systems such as Windows and Linux in seaport-based ICS, mobile devices, and the use of wireless networks increase the number of potential entry points into a network for malicious actors.

Vessels also can be vulnerable to a malicious actor who may want to shut them down by either taking control of certain onboard ICS or damaging them directly. These activities could prevent the departure of vessels from the port and significantly delay terminal operations. If disabled while underway, the vessel could block shipping channels or present a hazard

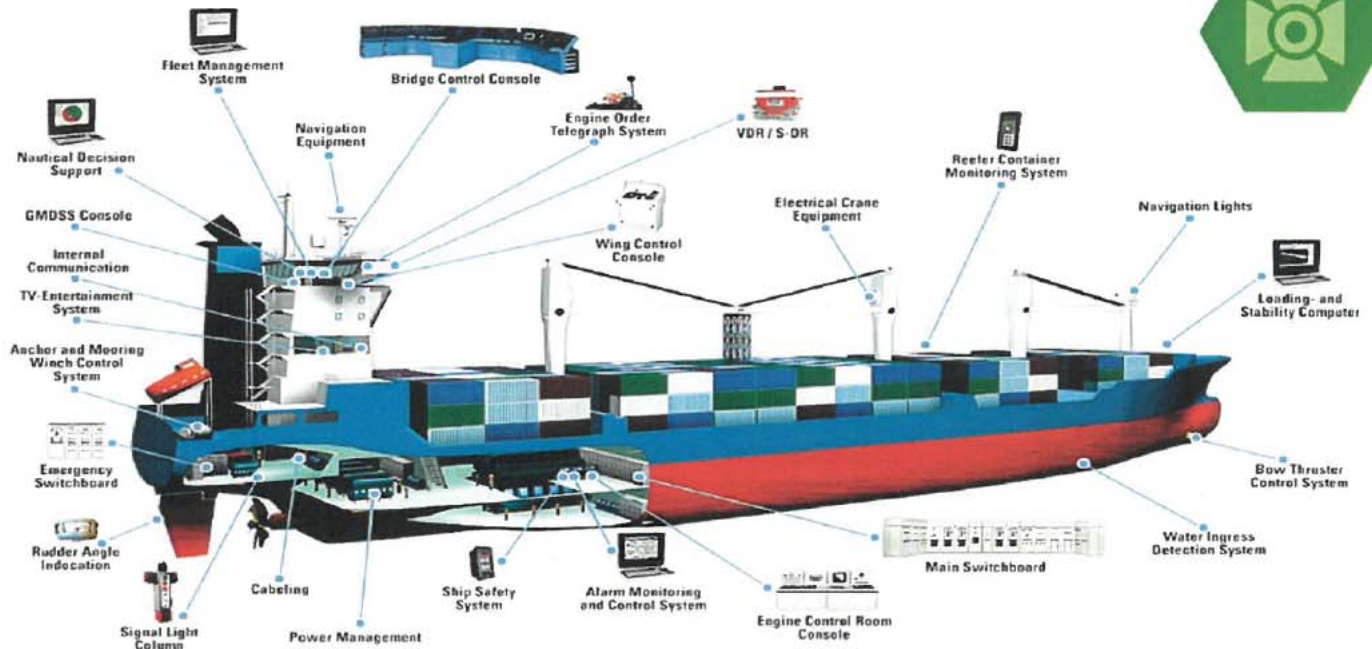


Figure 1 - Illustration of Shipboard ICS



Figure 2 - Illustration of Shore-based ICS



to navigation. The potential for malicious actors to manipulate the engine and ICS functions also poses a significant risk to include initiating fires, explosions, or potential manipulation of the vessel speed, causing it to run aground or collide with other vessels.

Software vulnerabilities can have a significant negative impact on maritime operations. Malicious actors could exploit software flaws to gain unauthorized access to maritime networks. Many ports, ships, terminals, and shipping companies across the world use common systems and software. Therefore, exploitation of associated vulnerabilities during the manufacturing process could result in widespread consequences from malicious cyber activity to compromise of port networks.

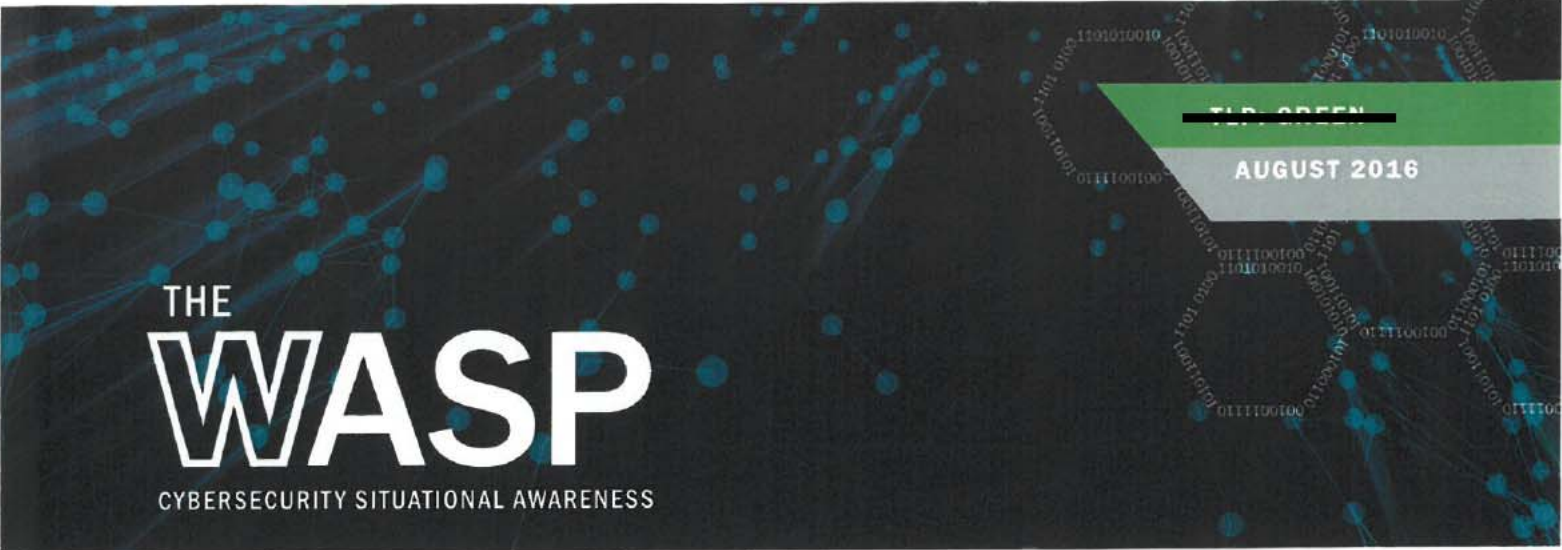
Another important support element of port and shipping operations is the Global Positioning System (GPS). GPS jamming or spoofing can significantly affect the movement of a ship in instances where the vessel is not under the physical control of the crew and visual navigation aids are not closely monitored. In addition, some equipment within ports, such as automated gantry cranes, also relies on GPS to operate effectively. A disruption in the GPS dependent service—whether through equipment manipulation or the intentional or unintentional blocking of GPS signals—can effectively deny the usage of this equipment and disrupt port operations until GPS capability is restored.

As with all critical infrastructures, “Insider Threats” have always been of concern. The National Infrastructure Advisory Council defines insider threat to critical infrastructure as “one or more individuals with the access and/or insider knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, or facilities with intent to cause harm.”⁹ Intent to do harm is also not required for insider threats to exist; possible careless and poorly trained individuals could represent a significant vulnerability in the operation of maritime networks.¹⁰ These individuals can allow malicious actors into sensitive systems through several methods: executing malware sent through emails (phishing attack), accessing websites that infect the computer with malware (watering hole attack), or manipulating them into providing sensitive information (social engineering).

Unless organizations responsible for maritime security worldwide address cyber vulnerabilities, they will continue to pose a significant risk to port facilities and aboard vessels within the Maritime Subsector. Several mitigation measures can increase the security and resiliency of ports, such as setting up maritime cybersecurity standards, sharing information across the sector, conducting routine vulnerability assessments, using best practices, mitigating insider threats, and developing contingency plans for cyber-attacks.

INFORMATION ABOUT THIS SUMMARY AND THE OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

This article is a summary of an Office of Cyber and Infrastructure Analysis’ (OCIA) Cyber Infrastructure Security and Resilience Note that examined the potential for malicious actors to use cyber capabilities to disrupt operations at U.S. commercial seaports and the impact major disruptions would have on other critical infrastructure sectors. The Department of Homeland Security Office of Cyber and Infrastructure Analysis (OCIA) mission is to support efforts to protect the Nation’s critical infrastructure through an integrated analytical approach evaluating the potential consequences of disruption from physical or cyber threats and incidents.



THE WASP

CYBERSECURITY SITUATIONAL AWARENESS

POINT OF CONTACT

Please take a few minutes to complete the survey at the end of this product. For all inquiries pertaining to this product or to contribute to the NCCIC Partner Spotlight, please contact NCCIC Customer Service at NCCICCustomerService@hq.dhs.gov or 1-888-282-0870.

CAN I SHARE THIS PRODUCT?

- Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- If you would like to share this product outside your organization, please contact NCCIC Customer Service to obtain permission.
- If other partner organizations and stakeholders would like to subscribe to NCCIC Fusion Analysis Cell products, please contact NCCIC Customer Service.

NCCIC Publications

US-CERT Products

Analysis Reports:

(b) (7)(E)

Indicator Bulletins:

(b) (7)(E)

Malware Analysis Reports:

(b) (7)(E)

Malware Initial Findings Reports:

(b) (7)(E)

NCCIC Publications

US-CERT Products

Security Bulletins:

SB16-186 – Vulnerability Summary for the Week of June 27, 2016	(TLP: WHITE)
SB16-193 – Vulnerability Bulletin for the Week of July 4, 2016	(TLP: WHITE)
SB16-200 – Vulnerability Summary for the Week of July 11, 2016	(TLP: WHITE)
SB16-207 – Vulnerability Summary for the Week of July 18, 2016	(TLP: WHITE)

Security Publications:

Ransomware	(TLP: WHITE)
------------	--------------

Technical Alerts:

TA16-187A – Symantec and Norton Security Products Contain Critical Vulnerabilities	(TLP: WHITE)
TA16-091A: Ransomware and Recent Variants	(TLP: WHITE)

ICS-CERT Products

ICS-CERT Monitor:

May-June 2016

Industrial Control System Advisories/Alerts:

ICSA-16-182-01 Eaton ELCSOFT Programming Software Memory Vulnerabilities	(TLP: WHITE)
ICSA-16-182-02 Siemens SICAM PAS Multiple Vulnerabilities	(TLP: WHITE)
ICS-Alert-16-182-01 Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities	(TLP: WHITE)
ICSA-16-187-01 – Rexroth Bosch BLADEControl-WebVIS Vulnerabilities	(TLP: WHITE)
ICSA-16-140-02A – Siemens SIPROTEC Information Disclosure Vulnerabilities	(TLP: WHITE)
ICSA-16-189-01 WECON LeviStudio Buffer Overflow Vulnerabilities	(TLP: WHITE)
ICSA-16-189-02 Moxa Device Server Web Console Authorization Bypass Vulnerability	(TLP: WHITE)
ICSA-16-194-01 Tollgrade Smart Grid EMS Lighthouse Vulnerabilities	(TLP: WHITE)
ICSA-16-194-02 GE Proficy HMI SCADA CIMPLICITY Privilege Management Vulnerability	(TLP: WHITE)
ICSA-16-196-01 Schneider Electric Pelco Digital Sentry Video Management System Vulnerability	(TLP: WHITE)
ICSA-16-196-02 Moxa MGate Authentication Bypass Vulnerability	(TLP: WHITE)
ICSA-16-196-03 Schneider Electric SoMachine HVAC Unsafe ActiveX Control Vulnerability	(TLP: WHITE)
ICSMA-16-196-01 Philips Xper-IM Connect Vulnerabilities	(TLP: WHITE)

This list contains products TLP: GREEN and lower

NCCIC Publications

ICS-CERT Products

Industrial Control System Advisories/Alerts:

ICSA-16-173-01A Advantech WebAccess ActiveX Vulnerabilities	(TLP: WHITE)
ICSA-16-103-01B Siemens Industrial Products glibc Library Vulnerability	(TLP: WHITE)
ICSA-16-208-01 Siemens SIMATIC WinCC, PCS 7, and WinCC Runtime Professional Vulnerabilities	(TLP: WHITE)
ICSA-16-208-02 Siemens SIMATIC NET PC-Software Denial of Service Vulnerability	(TLP: WHITE)
ICSA-16-208-03 Siemens SINEMA Remote Connect Server Cross-site Scripting Vulnerability	(TLP: WHITE)
ICSA-16-173-03 Rockwell Automation FactoryTalk EnergyMetrix Vulnerabilities	(TLP: WHITE)

This list contains products TLP: GREEN and lower

The Watch & Warning Analytic Synopsis Product (WASP) provides cybersecurity situational awareness to NCCIC partners and stakeholders and informs cyber risk management policies and decision. This product is produced by the NCCIC Fusion Analysis Cell. For more information about NCCIC, please visit: <https://www.dhs.gov/national-cybersecurity-andcommunications-integration-center>



Cyber Highlights

Featured Article: SECURITY SOFTWARE FLAWS LEAD TO GROWING CONCERNS OVER BROADER INDUSTRY CHALLENGES

¹ Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," June 30, 2016, accessed July 8, 2016, <https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/>.

² Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," June 30, 2016, accessed July 8, 2016, <https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/>.

³ Symantec, "Security Advisories Relating to Symantec Products – Symantec Messaging Gateway Multiple Security Issues (SYM16-005)," April 18, 2016, accessed July 11, 2016, https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&msgid=20160418_00.

⁴ Tavis Ormandy, "Symantec Antivirus Multiple Remote Memory Corruption Unpacking RAR CVE-2016-2207," April 28, 2016, accessed June 8, 2016, <https://bugs.chromium.org/p/project-zero/issues/detail?id=810>.

⁵ Tavis Ormandy, "Symantec Antivirus Multiple Remote Memory Corruption Unpacking RAR CVE-2016-2207," April 28, 2016, accessed June 8, 2016, <https://bugs.chromium.org/p/project-zero/issues/detail?id=810>.

⁶ Tavis Ormandy, "Symantec Antivirus Multiple Remote Memory Corruption Unpacking RAR CVE-2016-2207," April 28, 2016, accessed June 8, 2016, <https://bugs.chromium.org/p/project-zero/issues/detail?id=810>.

⁷ Tavis Ormandy, "Symantec Antivirus Multiple Remote Memory Corruption Unpacking RAR CVE-2016-2207," April 28, 2016, accessed June 8, 2016, <https://bugs.chromium.org/p/project-zero/issues/detail?id=810>.

⁸ Tavis Ormandy, "How to Compromise the Enterprise Endpoint," June 28, 2016, accessed July 8, 2016, <http://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html>.

⁹ Tavis Ormandy, "How to Compromise the Enterprise Endpoint," June 28, 2016, accessed July 8, 2016, <http://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html>.

¹⁰ Tom Brant, "Experts: Symantec Security Flaw is as Bad as it Gets," June 30, 2016, accessed July 8, 2016, <http://in.pcmag.com/software/104796/news/experts-symantec-security-flaw-is-as-bad-as-it-gets>.

[experts-symantec-security-flaw-is-as-bad-as-it-gets](http://in.pcmag.com/software/104796/news/experts-symantec-security-flaw-is-as-bad-as-it-gets).

¹¹ Vangie Beal, "Term: Kernel," 2016, accessed June 8, 2016, <http://www.webopedia.com/TERM/K/kernel.html>.

¹² Tavis Ormandy, "How to Compromise the Enterprise Endpoint," June 28, 2016, accessed July 8, 2016, <http://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html>.

¹³ Tom Brant, "Experts: Symantec Security Flaw is as Bad as it Gets," June 30, 2016, accessed July 8, 2016, <http://in.pcmag.com/software/104796/news/experts-symantec-security-flaw-is-as-bad-as-it-gets>.

¹⁴ US-CERT, "Symantec and Norton Security Products Contain Critical Vulnerabilities – Alert (TA16-187A)," July 5, 2016, accessed July 11, 2016, <https://www.us-cert.gov/ncas/alerts/TA16-187A>.

¹⁵ Symantec, "Security Advisories Relating to Symantec Products – Symantec Messaging Gateway Multiple Security Issues (SYM16-005)," April 18, 2016, accessed July 11, 2016, https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&msgid=20160418_00.

¹⁶ Symantec, "2015 Annual Report," 2015, accessed July 11, 2016, http://s1.q4cdn.com/585930769/files/doc_financials/2015Report/SyMC-2015-Annual-Report-Bookmarked-FINAL.pdf.

¹⁷ OPSWAT, "Market Share Analysis of Antivirus & Compromised Devices," January 2015, accessed July 11, 2016, <https://www.opswat.com/resources/reports/antivirus-and-compromised-device-january-2015>.

¹⁸ Symantec, "Security Advisories Relating to Symantec Products – Symantec Messaging Gateway Multiple Security Issues (SYM16-005)," April 18, 2016, accessed July 11, 2016, https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&msgid=20160418_00.

¹⁹ Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," June 30, 2016, accessed July 8, 2016, <https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/>.

²⁰ Lucian Constantin, "Antivirus Software Could Make Your Company More Vulnerable," January 8, 2016, accessed July 15, 2016, <http://www.cio.com/article/3020324/antivirus-software-could-make-your-company-more-vulnerable.html>.

²¹ Lucian Constantin, "Antivirus Software Could Make Your Company More Vulnerable," January 8, 2016, accessed July 15, 2016, <http://www.cio.com/article/3020324/antivirus-software-could-make-your-company-more-vulnerable.html>.

[ware-could-make-your-company-more-vulnerable.html](http://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/).

²² Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," June 30, 2016, accessed July 15, 2016, <https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/>.

²³ Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," June 30, 2016, accessed July 15, 2016, <https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/>.

²⁴ Lucian Constantin, "Antivirus Software Could Make Your Company More Vulnerable," January 8, 2016, accessed July 26, 2016, <http://www.cio.com/article/3020324/antivirus-software-could-make-your-company-more-vulnerable.html>.

²⁵ Kaspersky Lab, "Unveiling 'Careto' – The Masked APT (TLP: Green)," February 2014, accessed July 26, 2016, http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthetmask_v1.0.pdf.

²⁶ Kaspersky Lab, "Unveiling 'Careto' – The Masked APT (TLP: Green)," February 2014, accessed July 26, 2016, http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthetmask_v1.0.pdf.

²⁷ Kelly Jackson Higgins, "What You Need to Know about Nation-State Hacked Hard Drives," March 2, 2015, accessed July 26, 2016, <http://www.darkreading.com/attacks-breaches/what-you-need-to-know-about-nation-state-hacked-hard-drives/d/d-id/1319296>.

²⁸ Robert McMillan, "Is Antivirus Software a Waste of Money?" March 2, 2012, accessed July 27, 2016, <http://www.wired.com/2012/03/antivirus/>.

²⁹ AVS, "Gartner Magic Quadrant for Endpoint Protection Platforms," January 17, 2014, accessed July 27, 2016, <http://blogs.antisvirus-sales.ca/en/blog/gartner-magic-quadrant-for-endpoint-protection-platforms/>.

³⁰ AVS, "Gartner Magic Quadrant for Endpoint Protection Platforms," January 17, 2014, accessed July 27, 2016, <http://blogs.antisvirus-sales.ca/en/blog/gartner-magic-quadrant-for-endpoint-protection-platforms/>.

³¹ Rebecca Greenfield, "Antivirus is Dead. Meet the Next Generation of Anti-Hacker Tools," May 6, 2014, accessed July 27, 2016, <http://www.fastcompany.com/3030075/whos-next-antivirus-is-dead-meet-the-next-generation-of-anti-hacker-tools>.

³² US-CERT, "Symantec and Norton Security Products Contain Critical Vulnerabilities – Alert



(TA16-187A),” July 5, 2016, accessed July 11, 2016, <https://www.us-cert.gov/ncas/alerts/TA16-187A>.

³² Symantec, “Security Advisories Relating to Symantec Products – Symantec Messaging Gateway Multiple Security Issues (SYM16-005),” April 18, 2016, accessed July 11, 2016, https://www.symantec.com/security_response/securityupdates/detail.jsp?Fid=security_advisory&pid=security_advisory&year=&suid=20160418_00.

³³ Lucian Constantin, “Antivirus Software Could Make Your Company More Vulnerable,” January 8, 2016, accessed July 26, 2016, <http://www.cio.com/article/3020324/antivirus-software-could-make-your-company-more-vulnerable.html>.

³⁴ National Institute of Standards and Technology, NIST Special Publication 800-167, Guide to Application Whitelisting, October 2015, accessed July 28, 2016, <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-167.pdf>.

Cyber Highlights

Current Activity:

U.S. DEMOCRATIC NATIONAL COMMITTEE (DNC) CYBER INTRUSION,

LET'S NOT FORGET ABOUT THE CLASSICS

¹ DNC Services Corporation, “About Party Organization: The Democratic National Committee,” 2016, accessed July 29, 2016, <https://www.democrats.org/about/our-party/party-organization>.

² DNC Services Corporation, “About Party Organization: The Democratic National Committee,” 2016, accessed July 29, 2016, <https://www.democrats.org/about/our-party/party-organization>.

³ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

⁴ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

⁵ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

⁶ Ellen Nakashima, “Russian Government Hackers Penetrated DNC, Stole Opposition

Research on Trump,” June 14, 2016, accessed July 29, 2016, https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html.

⁷ Harper Neidig, “WikiLeaks Release Includes Hacked DNC Voicemails,” July 27, 2016, accessed July 29, 2016, <http://thehill.com/blogs/blog-briefing-room/news/289541-wikileaks-releases-hacked-dnc-voicemails>.

⁸ ThreatConnect, “Fancy Bear has an (IT) Itch that They Can't Scratch,” July 29, 2016, accessed August 4, 2016, <https://www.threatconnect.com/fancy-bear-it-itch-they-cant-scratch/>.

⁹ ThreatConnect, “Fancy Bear has an (IT) Itch that They Can't Scratch,” July 29, 2016, accessed August 4, 2016, <https://www.threatconnect.com/fancy-bear-it-itch-they-cant-scratch/>.

¹⁰ ThreatConnect, “Fancy Bear has an (IT) Itch that They Can't Scratch,” July 29, 2016, accessed August 4, 2016, <https://www.threatconnect.com/fancy-bear-it-itch-they-cant-scratch/>.

¹¹ Trusted third-party reporting, “Guccifer 2.0 Leak of DNC Documents Most Likely Part of Russian Disinformation Campaign,” June 17, 2016, accessed July 29, 2016.

¹² Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

¹³ Trusted third-party reporting, “Guccifer 2.0 Leak of DNC Documents Most Likely Part of Russian Disinformation Campaign,” June 17, 2016, accessed July 29, 2016.

¹⁴ David E. Sanger and Eric Schmitt, “Spy Agency Consensus Grows That Russia Hacked DNC,” July 26, 2016, accessed July 29, 2016, http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html?_r=0.

¹⁵ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

¹⁶ The Telegraph, “Russian Hackers Accused of Attacks on Bundestag and French TV Broadcaster,” June 11, 2015, accessed August 1, 2016, <http://www.telegraph.co.uk/news/worldnews/europe/germany/11666815/Russian-hackers-accused-of-Bundestag-attack.html>.

¹⁷ Joseph Menn and Leigh Thomas, “France Probes Russian Lead in TV5Monde Hacking: Sources,” June 10, 2015, accessed August 1, 2016, <http://www.reuters.com/article/us-france-russia-cybercrime-idUSKBN00>

Q2GG20150610.

¹⁸ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

¹⁹ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

²⁰ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

²¹ Dmitri Alperovitch, “Bears in the Midst: Intrusion into Democratic National Committee,” June 15, 2016, accessed July 29, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

²² Mark Galeotti, “Putin's Hydra: Inside Russia's Intelligence Services,” May 11, 2016, accessed August 1, 2016, http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services.

²³ DHS Interagency Report, “How to Protect Your Networks from Ransomware”, accessed 11 July 2016

²⁴ Trend Micro, “Ransomware 101: What, How, and Why”, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works>, accessed 11 July 2016

²⁵ Secure Works, “Banking Botnets: The Battle Continues”, <https://www.secureworks.com/research/banking-botnets-the-battle-continues>, accessed 18 July 2016

²⁶ Secure Works, “Banking Botnets: The Battle Continues”, <https://www.secureworks.com/research/banking-botnets-the-battle-continues>, accessed 18 July 2016

²⁷ Symantec, “Financial Threats 2015”, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/financial-threats-2015.pdf, accessed 11 July 2016

²⁸ Dark Reading, “Symantec: Financial Trojans Declined by 73% in 2015”, <http://www.darkreading.com/vulnerabilities--threats/symantec-financial-trojans-declined-by-73-in-2015/d/d-id/1324923>, accessed 18 July 2016

²⁹ Ibid

³⁰ IBM, “IBM X-Force Threat Intelligence Report



2016". <http://www-01.ibm.com/commori/ssi/cgi-bin/ssi/alias?htmlifid=WGL03114USEN>, accessed 11 July 2016

¹¹ IB Times, "Banking Trojans on the Rise in Canada – Dridex, Kronos, and Zeus Among Those Detected", <http://www.ibtimes.co.uk/banking-trojans-rise-canada-dridex-kronos-zeus-among-those-detected-1568941>, accessed 11 July 2016

¹² Proofpoint, "Banking Trojans Go Loonie for Toonies: Dridex, Vawtrak, and Others Increase Focus on Canada", <https://www.proofpoint.com/us/threat-insight/post/banking-trojans-dridex-vawtrak-others-increase-focus-on-canada>, accessed 12 July 2016

¹³ Security Intelligence, "GozNym: Living in America", <https://securityintelligence.com/goznym-launches-redirection-in-the-united-states/>, accessed 12 July 2016

¹⁴ Security Intelligence, "Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim", <https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/>, accessed 12 July 2016

¹⁵ Security Intelligence, "GozNym: Living in America", <https://securityintelligence.com/goznym-launches-redirection-in-the-united-states/>, accessed 12 July 2016

¹⁶ Help Net Security, "Vawtrak Banking Shifts to New Targets", <https://www.helpnetsecurity.com/2016/06/14/vawtrak-banking-trojan-shifts-new-targets/>, accessed 11 July 2016

¹⁷ Sophos, "Vawtrak v2", <https://www.sophos.com/en-us/medialibrary/PDFs/technical/20/papers/sophos-vawtrak-v2-sahin-wyke.pdf?la=en>, accessed 11 July 2016

¹⁸ US-CERT, "Banking Securely Online", https://www.us-cert.gov/sites/default/files/publications/Banking_Securely_Online07102006.pdf, accessed 18 July 2016

¹⁹ Tom's Guide, "What is a Banking Trojan", <http://www.tomsguide.com/us/banking-trojan-definition,news-18457.html>, accessed 18 July 2016

Cyber Highlights

EMERGING TECHNOLOGY:

²⁰ CSO Online, "Researchers Steal Data From a PC by Controlling the Noise From the Fans", <http://www.csoonline.com/article/3088323/security/researchers-steal-data-from-a-pc-by-controlling-the-noise-from-the-fans.html>, accessed 13 July 2016

²¹ Wired, "Stealing Data From Computers Using Heat", <https://www.wired.com/2015/03/stealing-data-computers-using-heat/>, accessed 27 July 2016

²² Wired, "How Attackers Can Use Radio Signals and Mobile Phones to Steal Protected Data", <https://www.wired.com/2014/11/airhopper-hack/>, accessed 27 July 2016

²³ Wired, "Researchers Hack Air-Gapped Computer with Simple Cell Phone", <https://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/>, accessed 27 July 2016

²⁴ Ars Technica, "Scientist-Developed Malware Prototype Covertly Jumps Air Gaps Using Inaudible Sound", <http://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound/>, accessed 27 July 2016

²⁵ Technology Review, "How Fansmitter Malware Steals Data From Air-gapped Computers", <https://www.technologyreview.com/s/601816/how-fansmitter-malware-steals-data-from-air-gapped-computers/>, accessed 28 July 2016

²⁶ Cornell University Library, "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers", <https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf>, accessed 13 July 2016

²⁷ Ibid

²⁸ Ibid

²⁹ Stevens Institute of Technology, "Friend or Foe? Your Wearable Devices Reveal Your Personal PIN", <https://www.stevens.edu/sites/stevens.edu/files/ChenWearablesPaper.pdf>, accessed 28 July 2016

³⁰ The Hacker News, "Hackers Can Steal Your ATM PIN From Your Smartwatch or Fitness Tracker", <http://thehackernews.com/2016/07/hacking-smartwatch-atm.html>, accessed 28 July 2016

³¹ Phys.org, "Your Smartwatch is Giving Away Your ATM PIN", <http://phys.org/news/2016-07-smartwatch-atm-pin.html>, accessed 28 July 2016

³² Stevens Institute of Technology, "Friend or Foe? Your Wearable Devices Reveal Your Personal PIN", <https://www.stevens.edu/sites/stevens.edu/files/ChenWearablesPaper.pdf>, accessed 28 July 2016

³³ Ibid

³⁴ Science Daily, "Your Smartwatch is Giving Away Your ATM PIN", <https://www.sciencedaily.com/releases/2016/07/160706131951.htm>, accessed 28 July 2016

³⁵ Softpedia, "New Device Sold on the Dark Web Can Clone Up to 15 Contactless Cards Per Second", <http://news.softpedia.com/news/new-device-sold-on-the-dark-web-can-clone-up-to-15-contactless-cards-per-second-505200.shtml>, accessed 28 July 2016

³⁶ Datacard Edge, "EMV vs NFC Technology: Setting the Record Straight", <http://datacardedge.com/articles/emv-vs-nfc-technology-setting-the-record-straight/>, accessed 28 July 2016

³⁷ CreditCards.com, "8 FAQs About EMV Credit Cards", <http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php>, accessed 28 July 2016

³⁸ Softpedia, "New Device Sold on the Dark Web Can Clone Up to 15 Contactless Cards Per Second", <http://news.softpedia.com/news/new-device-sold-on-the-dark-web-can-clone-up-to-15-contactless-cards-per-second-505200.shtml>, accessed 28 July 2016

³⁹ Ibid

⁴⁰ TechWorm, "\$710 Tool Can Sniff Contactless Card Details From 8cm Away and Clone Them", <http://www.techworm.net/2016/06/710-tool-can-sniff-contactless-card-details-8cm-away-clone.html>, accessed 28 July 2016

⁴¹ Malwr Posts, "Debunking Scam!! Contactless Infusion X5", <https://malwrpost.wordpress.com/2016/06/17/debunking-scam-contactless-infusion-x5/>, accessed 28 July 2016

NCCIC Partner Spotlight

Office of Cyber and Infrastructure Analysis

SEAPORT OPERATIONS AND POSSIBLE CONSEQUENCES FROM MALICIOUS CYBER ACTIVITY

⁴² American Association of Port Authorities, "U.S. Public Port Facts", www.aapa-ports.org/industry/content.cfm?ItemNumber=1032, accessed 25 June 2015.

⁴³ A seaport is a harbor at or accessible to the seacoast that accommodates seagoing vessels. A deep draft harbor is one that is constructed to a depth of more than 45 feet. For definition of deep draft, see U.S. Code, Title 33, § 2241, www.gpo.gov/fdsys/pkg/USCODE-2010-title33/pdf/USCODE-2010-title33-chap36-subchap11-sec2241.pdf, accessed 16 July 2015.

⁴⁴ American Association of Port Authorities, "Glossary of Maritime Terms", www.aapa-ports.org/industry/content.cfm?ItemNumber=1077, accessed 14 September 2015.

⁴⁵ Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663828.pdf, accessed 14 September 2015.



⁶ Bateman, Tom, "Police warning after drug traffickers' cyber-attack," BBC, October 16, 2013, www.bbc.com/news/world-europe-24539417, accessed 8 September 2015.

⁷ Robertson, Jordan and Michael Riley, "The Mob's IT Department," Bloomberg Businessweek, July 7, 2015, www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/, accessed 8 September 2015.

⁸ Cyberkeel, "Maritime Cyber-Risks," October 15, 2014, www.cyberkeel.com/images/pdf-files/Whitepaper.pdf, accessed 8 September 2015.

⁹ Kochetkova, "Maritime industry is easy meat for cyber criminals," Kaspersky Labs, May 22, 2015, <https://blog.kaspersky.com/maritime-cyber-security/8796/>, accessed 8 September 2015.

¹⁰ Noonan, Thomas and Edmund Archuleta, "The Insider Threat to Critical Infrastructures," National Infrastructure Advisory Council, April 8, 2008, www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, accessed 15 September 2015.

¹¹ Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663826.pdf, accessed 14 September 2015.

UNCLASSIFIED



Homeland Security

National Protection and Programs Directorate

NPPD Customer Feedback Survey

Product Title:

1. Please select the partner type that best describes your organization.

2. Overall, how satisfied are you with the usefulness of this product?

- Very Satisfied
- Somewhat Satisfied
- Neither Satisfied Nor Dissatisfied
- Somewhat Dissatisfied
- Very Dissatisfied

3. How did you use this product in support of your mission?

- Integrated into one of my own organization's information or analytic products
- Used contents to improve my own organization's security or resiliency efforts or plans
If so, which efforts?
- Shared contents with government partners
If so, which partners?
- Shared contents with private sector partners
If so, which partners?
- Other (please specify)

4. Please rank this product's relevance to your mission. (Please portion mark comments.)

- Critical
- Very Important
- Somewhat Important
- Not Important
- N/A

5. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Timeliness of product or support	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Relevance to your information needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. How could this product or service be improved to increase its value to your mission? (Please portion mark comments.)

To help us understand more about your organization so we can better tailor future products, please provide (OPTIONAL):

Name:	<input type="text"/>	Position:	<input type="text"/>
Organization:	<input type="text"/>	State:	<input type="text" value="Select One"/>
Contact Number:	<input type="text"/>	Email:	<input type="text"/>

SUBMIT FORM

[Privacy Act Statement](#)
[Paperwork Reduction Act Compliance Statement](#)

UNCLASSIFIED