# The Beacon

Florida Fusion Center #19-022 | Cyber and Critical Infrastructure Report | January 2019, Issue #18

## Summary

**Mining in Plain Sight: Browser-Based Cryptojacking -** What happens when someone steals your processor power to mine cryptocurrencies for themselves? Learn how to protect your computer from cryptojacking.

**I Always Feel Like Somebody's Watching Me -** Are you the only one watching your cameras? Unsecured devices can be a way for bad actors to spy; find out how to protect yourself and your privacy.

**Weak Links: Supply Chain Compromises -** We're all aware of the threat that hacking poses, but what about physical exploitation of hardware at the point of manufacture? We examine recent reports of tampering with server motherboards.

**Internal Revenue ~~Scams~~ Service -** It's time to file your taxes and time for scammers to try and steal your returns. Learn how to spot these traps before you fall victim.

**Business Email, Compromised -** A look at the growing problem of hackers infiltrating an organization's email server and using social engineering tactics to steal resources.

**Nyet So Fast! U.S. Response to Russia's Cyber Activities -** As nation-state actors appear in news headlines for their exploits in the cyber world, we take a look at Russian activity.

## Contents



## About *The Beacon*

*The Beacon* is the Florida Fusion Center's cyber and critical infrastructure publication, produced by the Florida Infrastructure Protection Center (FIPC). Designed to highlight information of interest, *The Beacon* features events and trends that occur in Florida or specifically affect Florida.

The Florida Infrastructure Protection Center was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters.

**Contact the FIPC**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us

# Editor's Corner

## A Look Back on 2018

Last year was a busy year for the cyber world. The 2018 elections kept many law enforcement and cyber experts busy, but just because the elections are over, doesn't mean it's time to relax. Many agencies are already drawing up security plans for the 2020 elections! While election security might keep many cyber experts busy, here are some other things to think about in 2019.

When you hear 'artificial intelligence' (A.I.), you may think of robots or super computers, but A.I. exists in more forms than just cyborgs. Also known as machine learning, artificial intelligence in cybersecurity is the concept that software can learn to detect threats and evolve to meet challenges. Machine learning can help detect problems and intrusions before a human would, but it has some downsides; namely, A.I. might miss (and therefore learn to miss) malware.[1] As more cybersecurity firms turn toward using machine learning, bad actors have shown interest in both thwarting A.I. by deciphering their algorithms, and using A.I. to probe networks for vulnerabilities. It's feasible that we could see attacks on networks become more automated; by that same token, we may see security improve by utilizing the same technology to detect vulnerabilities.

Critical infrastructure cyber security remains a high priority. Last year, we saw certain nation-state actors probe U.S. electrical grids looking for holes,[2] with each attack having varying levels of success. (Read more about nation-state activity in Nyet So Fast!) Ransomware made for a useful tool in attacking various targets around the U.S., including hospitals and even the City of Atlanta.[3] It is plausible to expect that ransomware campaigns could continue to target critical infrastructure and public offices, and as such, these sectors should invest time and resources into making sure their systems are compliant with the latest security updates.

Privacy will always have a spot in the light, especially as governments and private companies alike try to balance information collection with a user's rights. The European Union's General Data Protection Regulation (GDPR) was implemented in May 2018, and made sweeping changes to data protection policy, not just in Europe but globally. The disparate laws in different countries (and even between some U.S. states) have caused issues for companies navigating data retention. There has been some talk in the U.S. about implementing similar measures at the federal level, and we expect to see more headway into this topic over the coming year.[4]

This year may lack the headline-grabbing action of an election, but there is no shortage of issues to keep our attention.

[1] https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/
[2] https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html
[3] https://www.bbc.com/news/technology-46381033
[4] http://fortune.com/2018/11/29/federal-data-privacy-law/

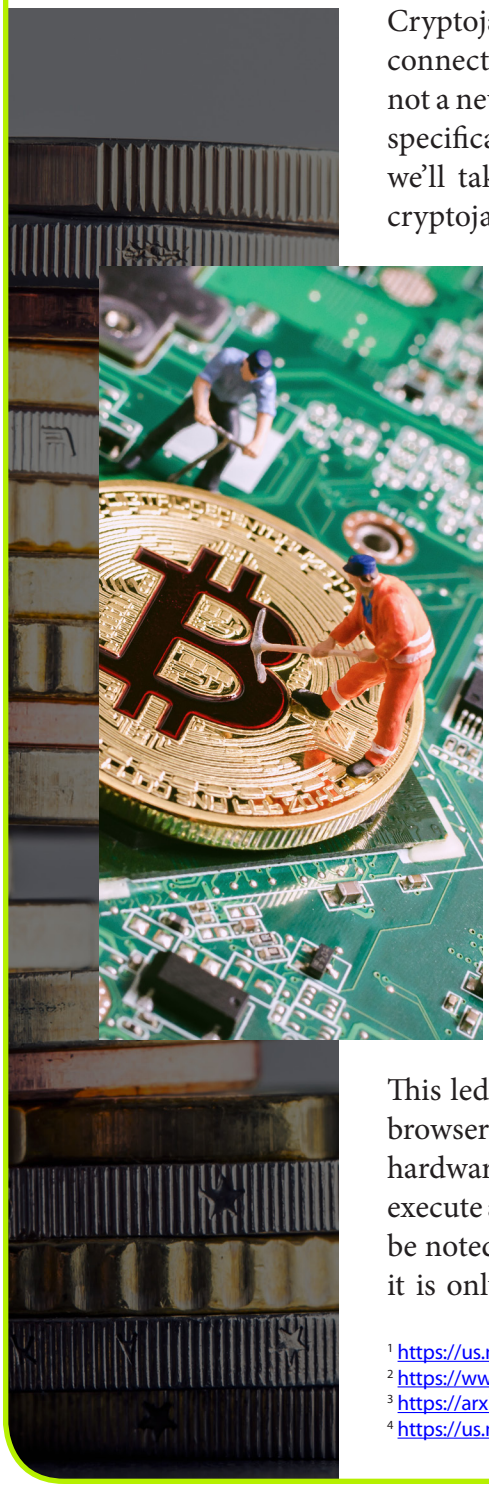


Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

**Contact us:**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us

# Cyber Threats

## Mining in Plain Sight: Browser-Based Cryptojacking



Cryptojacking, the unauthorized use of a computer, tablet, mobile phone, or connected home device by cybercriminals to mine for cryptocurrency,[1] is not a new process. However, there has been a recent uptick in cryptojacking; specifically the process of browser-based cryptojacking.[2] In this article, we'll take a look at how this process differs from previous iterations of cryptojacking and factors contributing to its rise in use.

### How does cryptojacking work?

Essentially, cryptojacking is the process of a bad actor compromising a machine they don't own and using it to mine cryptocurrency. As currencies like Bitcoin rose in value, it became more resource intensive to mine. In an effort to avoid a massive electric bill and the cost of mining hardware, cybercriminals will engage in cryptojacking. This is comparable to outsourcing the labor of cryptomining; the problem is the laborers often didn't sign up for the work.[3] Early versions of cryptojacking entailed bad actors targeting a victim's computing power via the machine's hardware. Cybercriminals used basic fraud tactics, such as social engineering and phishing, to infect victim machines with malware and turn them into mining machines.[4] At one point, a victim might not have noticed that their machine was running cryptomining scripts in the background; now, however, currencies like Bitcoin have reached a point where an average computer will exhibit noticeable strain, even shut down, if infected with this type of malware. This made the process easier for victims to notice, driving bad actors to develop newer, "gentler" methods of cryptojacking.

This led to browser-based cryptojacking. Compared to previous iterations, browser-based cryptojacking targets a victim's browser rather than their hardware. Cybercriminals will inject malicious script on a website that will execute and run mining scripts when a victim visits the infected site. It should be noted that running mining scripts on a browser is not illegal on its own; it is only when a website's visitors are not informed that their computing

[1] https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html
[2] https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency
[3] https://arxiv.org/pdf/1808.00811.pdf
[4] https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html



Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

**Contact us:**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us

power is being used to mine cryptocurrency that it becomes a crime. This process is less taxing on the average computer, and is therefore, harder to detect.

**Why is browser-based cryptojacking surging?**

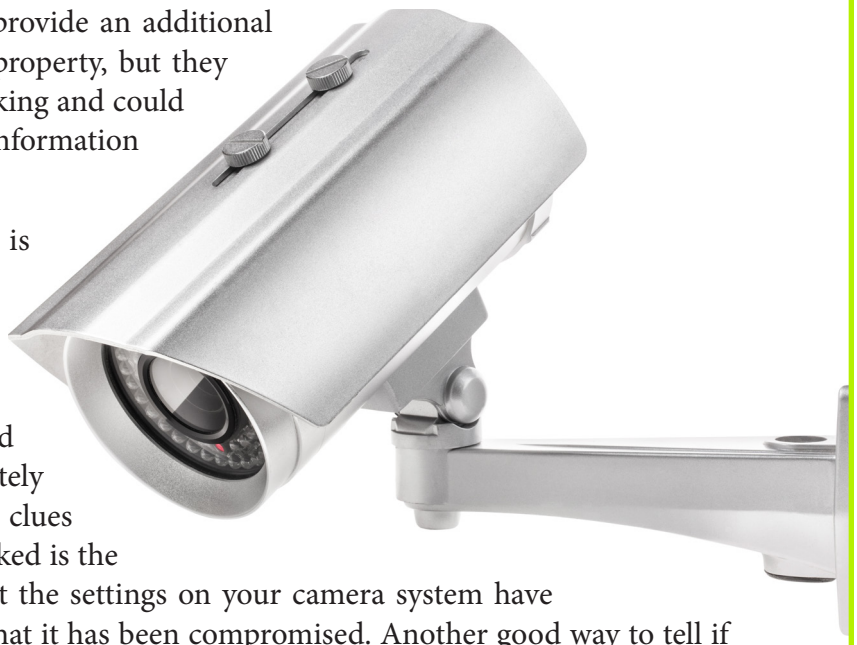
The springboard for browser-based cryptojacking appears to have been the launching of Coinhive, a browser-based mining service that mines for the cryptocurrency Monero.[5] Coinhive was originally pitched as a method for website owners to "earn an income without running intrusive or annoying advertisements," on their websites.[6] The code has since emerged as one of the top malware threats tracked by multiple security firms.[7] While Monero isn't as highly valued as Bitcoin, the heightened anonymity it offers, as well as the potential capability of exchanging it for another currency, makes it appealing to cybercriminals.[8] As previously stated, the process is gentle enough on an average computer that it is difficult to detect, and it is easy to implement, setting the stage for a highly lucrative setup. This method involves using smaller amounts of computing power from a larger number of victims, rather than a larger amount of computing power from a smaller number of victims. Malicious advertising techniques that have been seen in the past, such as the "pop under" technique in which ads load underneath a browser window in an effort to remain hidden, are also being used in cryptojacking, and will likely continue to be seen along with other malware propagation and evasion techniques.[9]

**What can I do to avoid getting cryptojacked?**

A machine running cryptomining scripts may exhibit symptoms of running slowly, an unusually high amount of processing power usage, or overheating. If you notice your machine is acting sluggish, it might be a good idea to dig a bit deeper to see if anything unwanted is running without your consent. There are web extensions available that can block some mining scripts, available under different names on various browsers, as well as extensions that will block anything that uses JavaScript. Using strong anti-virus software is also encouraged to help detect unsecured websites that may be running cryptojacking scripts as you browse the web. It is also advisable for users to keep their software up-to-date and patched to limit the spread of cryptojacking attacks.[10]

[5] https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/
[6] Ibid.
[7] Ibid.
[8] https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency
[9] Ibid.
[10] https://blog.avast.com/protect-yourself-from-cryptojacking

# I Always Feel Like Somebody's Watching Me



Security cameras are a good way to provide an additional layer of protection to your home or property, but they are vulnerable to new methods of hacking and could be providing would-be thieves with information they could later use against you.

Hacking a home security system is surprisingly easy and can be done with basic technology and instructions found online.[1] Luckily, there are several ways to improve the security of your home camera system that would make it harder for criminals to remotely gain access. Recognition of suspicious clues that your camera system has been hacked is the first line of defense. If you notice that the settings on your camera system have been changed, this is a possible sign that it has been compromised. Another good way to tell if your camera is being accessed remotely is if there is an extreme spike in the data flow on your local internet network. If you notice any of these suspicious signs, or you would like to take proactive steps to prevent your camera falling victim, you can take action to attempt to make your cameras more secure. There are several ways you can achieve this goal:

- Always use secure passwords that would be hard for a hacker to guess. Never keep the default password that comes with your device.
- If you buy a used security system, remember to change the password. Make it complex and completely different from what it was before.
- Limit the number of devices used to access the feed from the camera. This makes it easier to figure out if you have been hacked when looking at the camera's logs to see which devices have accessed the feed.
- Never use public Wi-Fi to access your security cameras as these networks are NOT secure.
- Regularly upgrade the system's firmware so that your system has the most current security software installed.
- Use a wired system, when possible; when not possible, make sure to use WPA2 wireless connections to ensure the highest degree of security available.
- Unplug your USB desktop webcam when not in use. For computers with integrated webcams (such as laptops), consider covering it with tape when not using it. This won't stop someone from hacking it, but they can't see anything if they do.

[1] https://www.ifsecglobal.com/cyber-security/how-to-hack-a-security-camera/

If you do notice that your camera system has been hacked you should update the firmware on the system, change the password, and contact the security company immediately to see if there is a fix for the issue as soon as possible.[2]

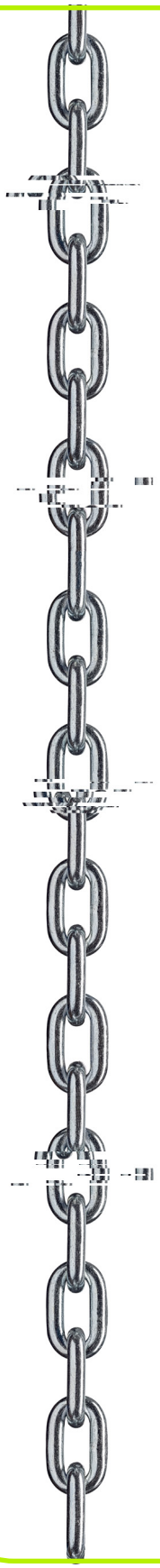
So what's the worst that could happen if your cameras get hacked? Most often these camera systems (and other Internet of Things devices) are used as components of a botnet to either direct debilitating amounts of traffic to sites or to mine cryptocurrency. While this might not sound like anything pressing to the average user, having your device compromised in this manner can mean losing access to it, slow connection speeds, or even irreparable damage to the device. More insidiously, a hacker could potentially watch the feed from a compromised camera.[3] External security cameras may not seem like an invasion of privacy, but many people with nanny cams that point into their homes may want to consider the risks. Compromised cameras pose a considerable threat to privacy and cybersecurity, and serve as another reason to make sure you have strong passwords.

[2] https://www.protectamerica.com/home-security-blog/tech-tips/can-security-cameras-be-hacked_15498
[3] https://www.usatoday.com/story/tech/columnist/saltzman/2018/03/01/has-someone-hacked-your-webcam-heres-how-stop-cyber-snoopers/377676002/

## Weak Links: Supply Chain Compromises

The risks of supply chain compromise have been a hot topic of discussion in the tech world over the last several months. In October 2018, Bloomberg released a controversial report claiming to have discovered compromises in both hardware and software of the tech industry's biggest companies. These compromises were reported to have first been identified in 2015, and potentially allow suspected Chinese hackers to infiltrate and possibly infect machines with malware.[1] In what the report detailed as a two-pronged approach, the bad actors infiltrated web portals that deliver firmware updates remotely to devices as well as compromised actual hardware by installing malicious computer chips onto motherboards bound for U.S. consumers. Bloomberg's report has yet to be confirmed by U.S. government sources, and tech giants, such as

[1] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to infiltrate-america-s-top-companies



Apple and Amazon, countered the report immediately, stating that they have found no evidence that their network infrastructure was breached.[2,3] Further, a third-party audit of Supermicro (a hardware component company) found no physical alterations to motherboards, and network logs showed no suspicious transmissions.[4]

Regardless of the results of these reports, supply chain compromise represents a substantial risk in the cybersecurity world. Imagine taking a server out of its packaging and it already being compromised by a sneaky addition to its motherboard; or downloading the latest security patch directly from the manufacturer only to find out that the update also contained malicious software. Both of these scenarios are hard to predict and even harder to detect. Such an invasion of critical components could not only lead to the loss of intellectual property, but the erosion of consumer confidence and trust.

The methods of compromise identified as targets would be difficult to combat; firmware portals (usually presented as some type of proprietary client) are highly trusted files that control the most basic of hardware functions, such as communication to and between servers. Tampering with hardware components, including small chips or motherboards, could be virtually impossible to detect. Compromises to these products could pose a risk to thousands of other private and government entities, not to mention certain critical sectors such as banking and healthcare.

Unfortunately, there are no easy solutions beyond good security posture on the cyber-front and rigorous inspection and testing of components once they arrive from the manufacturer. The vast majority of the components in question are made in China.[5] Moving hardware production from China to someplace local may increase security, but also increases cost prohibitively.[6] The Pentagon has taken steps recently to restrict certain Chinese technology companies from being used by federal government personnel for official purposes, due to suspected security risks posed by the devices. Recently, the U.S. Department of Commerce instituted a 7-year export restriction toward another Chinese tech company, essentially banning U.S. companies from selling components to them.[7]

It is likely that we have not heard the last of this phenomenon. Regardless of whether the open-source media articles hold reliable information, there seems to be some anxiety surrounding the security of technology supply chains. We may be entering into a new age of hacking, where the hack happens before the computer is even turned on.

[2] https://www.theverge.com/2018/10/4/17935868/chinese-spies-microchip-hack-servers-apple-amazon-supermicro
[3] https://www.theverge.com/2018/10/4/17936968/apple-amazon-deny-servers-chinese-spy-chips
[4] https://arstechnica.com/information-technology/2018/12/supermicro-refutes-report-of-malicious-implants-with-audit/
[5] https://krebsonsecurity.com/2018/10/supply-chain-security-is-the-whole-enchilada-but-whos-willing-to-pay-for-it/
[6] Ibid.
[7] Ibid.

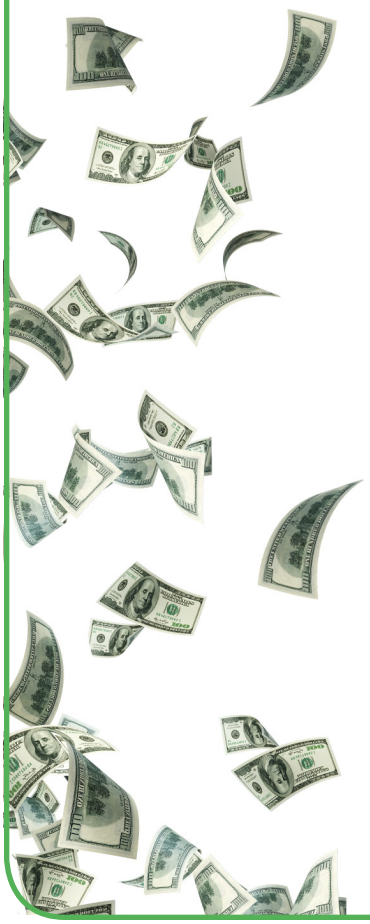
# Cyber Highlights

## IRS: Internal Revenue ~~Scams~~ Service

Internal Revenue Service (IRS) scams are a growing concern, especially with the tax season ahead. These scams can impact anyone and can occur over the telephone or through email. There are also many variations of IRS scams making it even more challenging to identify fact from fiction.

Various tactics are used by scammers, including using fake names and IRS badge numbers. In some instances, scammers may also know the last four digits of the victim's social security number (likely gained from hacked records), use a spoofed toll-free number so when it comes up on caller ID it appears the IRS is calling you, or send bogus IRS emails.[1] The IRS generally sends certified letters to citizens with announcements of an audit or discrepancy in a return. Some scammers are now taking advantage of this fact by calling potential victims to inquire why they have not responded to the certified letter (which was not actually sent by the IRS or anyone else).[2] The scammers contact victims and claim that they owe money in back taxes and penalties, but if they pay a small fee, they are eligible for a big refund.

Below are a few facts to know to protect yourself from being a victim of an IRS scam:



- The IRS will not call you and demand immediate payment
- The IRS will not demand that you pay without the opportunity to appeal first
- The IRS will not ask for credit or debit card information over the phone
- The IRS will not require you to pay (if you owe taxes) with a specific type of payment method (i.e. gift cards, prepaid debt card, green dot prepaid card, electronic wire transfer, etc.)
- The IRS will not threaten to bring law enforcement to arrest you for not paying taxes[3]

The IRS implemented an operational change in 2015 and uses four private debt collectors to collect overdue tax debts. The first step of this process includes written notification from the IRS that your case was transferred to a private collection agency. The collection agency then sends a separate letter to the taxpayer notifying the individual that the agency will be their representative.[4]

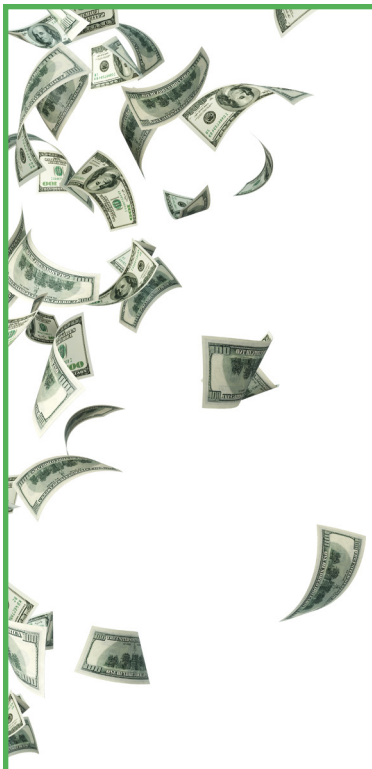
These scams can be financially and emotionally draining to the victim. Past victims of IRS scams have lost thousands of dollars and/or had

[1] https://www.irs.gov/newsroom/irs-repeats-warning-about-phone-scams
[2] https://www.aging.senate.gov/imo/media/doc/2018%20Fraud%20Book.pdf
[3] https://www.irs.gov/newsroom/irs-urges-public-to-stay-alert-for-scam-phone-calls
[4] https://www.irs.gov/businesses/small-businesses-self-employed/private-debt-collection



Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

**Contact us:**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us

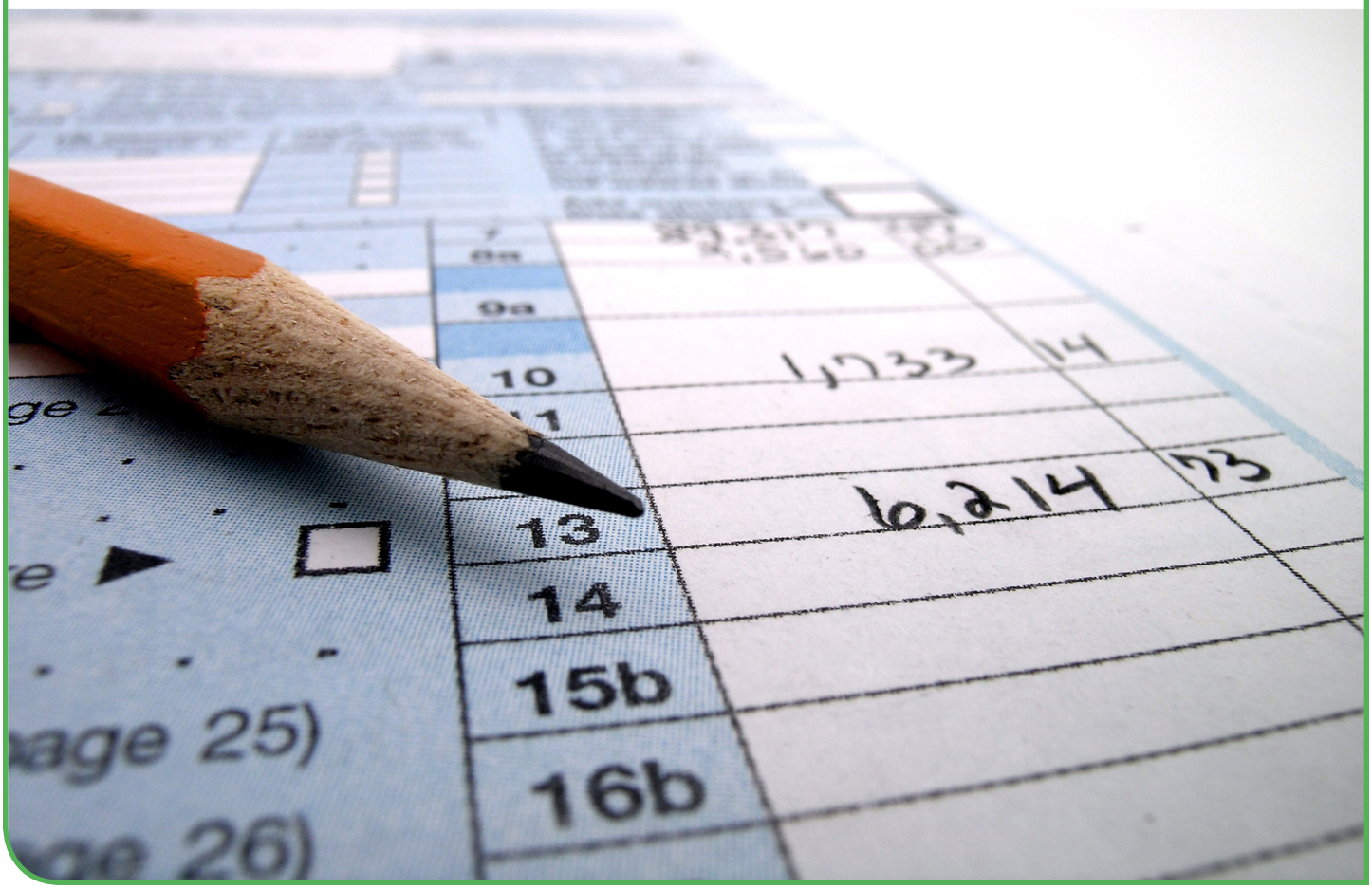


personal identifying information stolen. Below are some tips for reducing the risk of being vulnerable to IRS scams:

- Always use security software with firewall and anti-virus protections
- Maintain strong passwords
- Learn to recognize phishing emails or threatening calls
- Avoid clicking on downloads or attachments from unknown or suspicious emails
- Ensure that you protect your personal information (birth certificate or social security card) at all times[5]

Report potential IRS tax scams to the Treasury Inspector General for Tax Administration at 1-800-366-4484 or online at treasury.gov/tigta.[6] If you believe you may owe taxes, and you want to ensure you are talking to a legitimate representative, you are asked to reach out to the IRS directly at 1-800-829-1040.

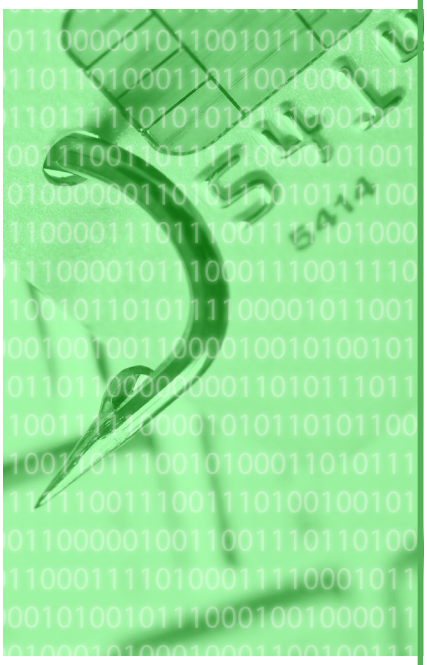
[5] Ibid.
[6] https://www.treasury.gov/tigta/



# Business Email, Compromised

Business Email Compromise, or BEC, is a scam in which a bad actor uses email and social engineering tactics to mimic legitimate business in an effort to convince employees into wiring them money. These scams can be highly costly and can impact businesses in any industry. Between October 2013 and May 2018, BECs impacted 41,058 U.S. victims with a reported loss of $3 billion.[1] BEC scams are often conducted by transnational criminal organizations, sometimes going so far as to employ scammers, lawyers, hackers and linguists to retrieve money through deception, open source intelligence and social engineering (the use of deception to manipulate individuals into giving up access or information).[2]

BEC relies on social engineering tactics through email to convince employees to wire funds to a requested account. Actors use publicly available information to identify and learn about a company before attempting contact. Then, they use this information to fool employees of the company into thinking they are fellow employees, a client or trusted partner. Some hackers may also conduct intrusion or spear-phishing attacks to give the actor(s) access to the company's network to study the organization structure, finances, and vendor information. This information may be used to send emails as the company's CEO or an executive, particularly when the executive is out of the office. These emails often request a wire transfer and may use terms terms like urgent or confidential to pressure the employee into complying without verifying the request.[3, 4]



[1] "Business E-Mail Compromise The 12 Billion Dollar Scam." Internet Crime Complaint Center (IC3) | Business E-Mail Compromise The 12 Billion Dollar Scam, www.ic3.gov/media/2018/180712.aspx
[2] "Business E-Mail Compromise." FBI, FBI, 27 Feb. 2017, www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
[3] Ibid.
[4] "FBI Report: Global BEC Losses Exceeded US $12 Billion in 2018." Security News - Trend Micro USA, 18 Jan. 2018, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fbi-report-global-bec-losses-exceeded-us-12-billion-in-2018



Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

**Contact us:**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us

The email address and account number may appear to be legitimate but actually sends funds to the actors' account.[5, 6] During investigations of BEC fraud, transferred funds were located in China, Hong Kong, Mexico, Turkey and the United Kingdom.[7, 8]

In spite of the name, individuals may also be targeted by this scam. Individuals involved in real estate transactions, such as buying or selling a home, have been most frequently reported.[9] If the fraudulent wire transfer is not discovered quickly, funds can be lost and tracking the perpetrators becomes difficult. Bad actors may also utilize unsuspecting money mules into opening bank accounts, not knowing that the account will be used for criminal activity.[10] Many of these people are tricked into serving as money mules by a confidence or romance scam (where an actor pretends to be someone else to manipulate the emotions of the victim, extracting material support from them).

The following safety tips are used to ensure the company is protected from a BEC intrusion:

- Always verify suspicious urgent/non-urgent wire transfer requests with all parties by a phone or in person for secondary verification.
- Use the computer contact list by using forward instead of reply. This is to make sure you are not replying to a spoofed address.[11]
- Education and training of all employees.
- Report suspicious activity to law enforcement and the Internet Crime Complaint Center at (www.ic3.gov)[12, 13]

[5] "Security 101: Business Email Compromise (BEC) Schemes." Security News - Trend Micro USA, 16 Jan. 2016, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes
[6] "FBI Report: Global BEC Losses Exceeded US$12 Billion in 2018." Security News - Trend Micro USA, 18 Jan. 2018, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fbi-report-global-bec-losses-exceeded-us-12-billion-in-2018
[7] Ibid.
[8] "Business E-Mail Compromise." FBI, FBI, 27 Feb. 2017, www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
[9] "Business E-Mail Compromise The 12 Billion Dollar Scam." Internet Crime Complaint Center (IC3) | Business E-Mail Compromise The 12 Billion Dollar Scam, www.ic3.gov/media/2018/180712.aspx
[10] "Red Flags: How to Spot a Business Email Compromise Scam." Security News - Trend Micro USA, 30 Jan. 2017, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-to-spot-business-email-scam
[11] Ibid.
[12] "Security 101: Business Email Compromise (BEC) Schemes." Security News - Trend Micro USA, 16 Jan. 2016, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes
[13] "Business E-Mail Compromise." FBI, FBI, 27 Feb. 2017, www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

# Critical Infrastructure

## Nyet So Fast!: U.S. Response to Russia's Cyber Activities

For years, Russia has attempted to destabilize the United States and other countries using cyberattacks. These cyberattacks involve one actor attacking another actor's computer and/or network systems. This can be done through viruses, denial-of-service attacks, and other varying methods. Russian cyberattack campaigns pose a serious threat to the U.S. intelligence and law enforcement communities due to their goals of disrupting operations, attaining sensitive information, and ultimately causing unrest across the U.S. and Europe.

### Targeting Critical Infrastructure

Russia cyberattack campaigns have been known to target other nations' critical infrastructure sectors. Ukraine, for example, has been a victim of these attacks on multiple occasions. In 2015, the country's power grids were hacked by Russian cyber-operatives causing the loss of power for hundreds of thousands of people. Similar attacks have been reported, not only on the power grid but also the finance, transportation, media, military, and political sectors as well. Experts theorize that the ultimate goal of these attacks is to test out methods in preparation for potential future cyberattacks against other targets.[1] The malicious software used to cause the second Ukrainian outage, CrashOverride, is reported to be capable of a fully-automated power grid attack on multiple grids simultaneously and could be used on larger grids in other parts of the world.[2]

The Russian government has already targeted various U.S. critical infrastructure sectors, including energy, nuclear, water, aviation, commercial facilities, and critical manufacturing sectors.[3] In these cyberattacks, Russian actors first targeted individuals in peripheral roles (i.e. suppliers) with less-secure networks by sending spear phishing (Spear phishing is posing as a trusted source in an email to gain access to private information) emails. From here, actors were able to deposit malware for their intended targets.[4] There are also concerns about vulnerabilities in software and

[1] Greenberg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyberwar." Wired, June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/
[2] Gross, Terry. "Experts Suspect Russia is Using Ukraine as a Cyber Testing Ground." NPR, June 22, 2017. https://www.npr.org/2017/06/22/533951389/experts-suspect-russia-is-using-ukraine-as-a-cyberwar-testing-ground
[3] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." US-CERT, March 15, 2015. TA18-074A. https://www.us-cert.gov/ncas/alerts/TA18-074A
[4] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." US-CERT, March 15, 2015. TA18-074A. https://www.us-cert.gov/ncas/alerts/TA18-074A

hardware with ties to Russia, and other countries, which could be used to obtain sensitive information or engage in an attack.[5] Last year, concerns arose regarding the security of U.S. computer networks using Kaspersky-branded products. Though the company has denied any wrongdoing, the U.S. government ordered that Kaspersky-branded products be removed from government use due to the potential that the Russian government could exploit cyber-vulnerabilities in these systems.[6]

**Disinformation Campaigns**

Actions attributed to Russian operatives have probed U.S. infrastructure in other ways. For example, in 2017, suspected Russian actors attempted to target U.S. congressional candidates through the establishment of fake websites. Law enforcement officials were alerted to the sites, and they were immediately removed.[7] Operatives have also undertaken a widespread disinformation campaign addressing many controversial issues, but mainly those related to politics and elections. Operatives have spread false information in order to heighten tensions and encourage discord amongst U.S. citizens by utilizing controversial topics to exploit Western political pressure points.[8]

To counter tactics targeting critical infrastructure, the U.S. Computer Emergency Response Team (U.S. CERT) has provided a list of best practices to better protect networks. Recommendations include using two-factor identification, especially for external-facing interfaces; establish training to inform users of current indicators of phishing, and establishing least-privilege controls (giving people access only to what they need).[9] To counter tactics targeting individuals, such as disinformation campaigns, make sure you use a variety of news sources, question information that seems incorrect or shocking, and fact check information before sharing it online.[10] Though Russia is unlikely to let up in their cybertattacks, these countermeasures can help to protect U.S. citizens and institutions.

[5] Lyngaas, Sean. "Senate Bill Hopes to Sort Out Supply-Chaing Cybersecurity Risks, Prevent Next Kaspersky Drama." CyberScoop, June 19, 2018. https://www.cyberscoop.com/senate-bill-hopes-sort-supply-chain-cybersecurity-risks-prevent-next-kaspersky-drama/

[6] "Binding Operational Directive 17-01." Department of Homeland Security, September 13, 2017. https://cyber.dhs.gov/bod/17-01/

[7] Gallagher, Sean. "Microsoft Exec: We Stopped Russia From Hacking 3 Congressional Campaigns." ARS Technica, July 20, 2018. https://arstechnica.com/information-technology/2018/07/microsoft-detected-russian-attempt-to-hack-3-congressional-candidates-this-year/

[8] Hawkins, Eric. "The Cybersecurity 202: Voter Confidence is the biggest election security challenge, DHS cybersecurity official says." The Washington Post, June 13, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/13/the-biggest-election-security-challenge-dhs-cybersecurity-official-says/5b1fece91b326b6391af09be/?utm_term=.66b1373e1e4&noredirect=on

[9] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." US-CERT, March 15, 2015. TA18-074A. https://www.us-cert.gov/ncas/alerts/TA18-074A

[10] Mak, Tim. "What Can Citizens Do To Fight Foreign Disinformation Campaigns." NPR, October 1, 2018. https://www.npr.org/2018/10/01/653264175/what-can-citizens-do-to-fight-foreign-disinformation-campaigns

# Dispatch Highlights

This section highlights articles from past *FIPC Dispatches* that our analysts think are noteworthy based on trends we're seeing in Florida. *The FIPC Dispatch* is a list of open-source articles that is sent out twice weekly. If you are interested in receiving *The FIPC Dispatch*, **let us know.**

To sign up for the *FIPC Dispatch*, visit SecureFlorida.org and click the **Sign up for The FIPC Dispatch** link at the bottom of the homepage or send an email to **FIPC@fdle.state.fl.us**.

*This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.*

## Overall Volume of Thanksgiving Weekend Malware Attacks Lower This Year

https://www.darkreading.com/attacks-breaches/overall-volume-of-thanksgiving-weekend-malware-attacks-lower-this-year-/d/d-id/1333373

- The overall rate of reported malware attacks has decreased; it was 34% lower in 2018 over 2017.
- The rate of ransomware, phishing, and cryptojacking rose dramatically in 2018 versus the previous year.
- Despite being lower for the Thanksgiving weekend, malware rates are up significantly for the year.

**Analyst Note: The news of less malware is great, but it could mean that bad actors are using more targeted attacks or are switching tactics. Be sure to use antivirus software and only shop on sites that have an encrypted connection.**

## Who's In Your Online Shopping Cart?

https://krebsonsecurity.com/2018/11/whos-in-your-online-shopping-cart/

- Compromised e-commerce sites may contain malicious code designed to appear harmless.
- The script embedded in the sites skims data that is submitted in online forms, such as personal data and payment information.
- These attacks are referred to as "formjacking."

**Analyst Note: Think of this attack as something almost akin to digital card skimming. While it's hard for customers to detect and avoid this attack on their end, there are many tools available to site administrators that can tell them if changes have been made to coding on their site.**

## Voting machine manual tells officials to reuse weak passwords

https://nakedsecurity.sophos.com/2018/11/07/voting-machine-manual-tells-officials-to-reuse-weak-passwords/

- Vendor manuals for voting machines used in more than 10 states suggested using weak, easy-to-guess passwords to access the devices.
- The practice of reusing old, simple passwords makes hacking a system easier.

**Analyst Note: Passwords should be 15 characters or longer, and try not to use old passwords. Using different types of characters is also a good idea, but longer passwords will take more time for hackers to crack, making you a less-appealing target. Never share passwords with anyone!**

## Do You Still Just Hand Over Your Data?

https://gizmodo.com/do-you-still-just-hand-over-your-data-1831199563

- Creating new user accounts on apps is easier than ever now that you can sign in with existing social media apps, but keep in mind that this shares all of your profile data with the app.
- Some apps may even have access to your friend's data, depending on the app permissions.

**Analyst Note: It's always a good idea to read the permissions an app is asking for when you download it. You should also check which apps have access to your social media profile regularly, and delete apps that you no longer use.**

## Phishing warning: If you work in this one industry you're more likely to be a target

https://www.zdnet.com/article/phishing-warning-if-you-work-in-this-one-industry-youre-more-likely-to-be-a-target/

- Hackers are launching cyber-attack campaigns in the pharmaceutical sector more than any other, targeting firms that make drugs, specifically.
- Pharmaceutical companies are a tempting target for their intellectual property, which can be sold on the black market.
- Construction firms were the second most attacked industry after pharmaceuticals, followed by real estate.

**Analyst Note: All industries report constant attacks by attempted phishers; no one is immune. Be vigilant for social engineering schemes, especially if you have access to sensitive information.**



**Contact us:**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us

# What is TLP?

The **Traffic Light Protocol (TLP)** is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

***This Beacon is TLP: White and is intended for wide distribution.*** If you would like to read past issues of the *The Beacon*, visit the Secure Florida website.

**www.SecureFlorida.org/The_Beacon**

The following is from the United States Computer Emergency Readiness Team (US-CERT):


Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.


Recipients may only share TLP: AMBER information of their own organization who need to know, and only as widely as necessary to act on that information.


Recipients may share TLP: GREEN information with peers, partner organizations, and with their sector or community, but not via publicly accessible channels.


TLP: WHITE information may be distributed without restriction, subject to copyright controls.

THE BEACON

Editing by: Ashley Grover
Designed by: Maria Olivella

January 2019

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)



**Contact us:**
**Phone:** (850) 410-7645
**Email:** FIPC@fdle.state.fl.us