Monthly Cybersecurity Newsletter

June 2018 Issue

NC DIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

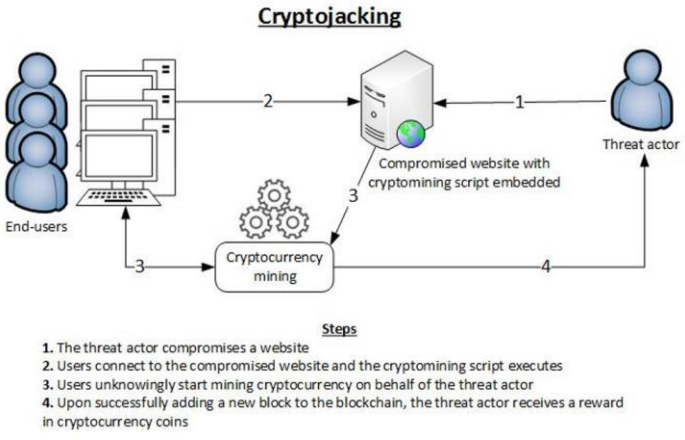
---

Is Your Computer Working for Someone Else?

Did you know your computer can be "hijacked" to work for others? It is true! It is called "cryptojacking" and it happens when your computer is used *without your consent* to mine cryptocurrency. Cryptocurrency is a kind of *digital currency* that uses encryption, or cryptography, and is designed to make secure financial transactions. Cryptocurrencies, such as Bitcoin and Monero, use decentralized control, as opposed to a centralized banking system, like the Federal Reserve System, and can be used like money to purchase or exchange goods. In cryptocurrency, *mining* is a validation of transactions that involves performing complex mathematical calculations and securely recording those transactions. Successful miners receive a *reward* in the form of new cryptocurrency that they can use like money.

To mine cryptocurrency, computers compete to solve complex mathematical calculations and confirm transactions to generate digital tokens. However, mining requires substantial processing power, or CPU usage. For instance, Bitcoin has become very difficult to mine and now requires massive warehouses stocked with specialized computers to be mined successful. One may have to spend a lot of money for the necessary hardware to mine most cryptocurrencies with any success. On top of that, the amount of energy consumed to mine cryptocurrency is substantial as these expensive high-powered machines are usually running 24/7. By one estimate, the power needed to mine a single Bitcoin would run the average household for *ten days*. Most *legitimate* cryptominers will spend a substantial amount of money to maintain and run their equipment. Thus, some enterprising individuals get cryptocurrency *illegally*.

For instance, a legitimate bitcoin mining service was hacked in December 2017 that resulted in a loss of *$64 million dollars*. Criminals can also use malicious software to "cryptojack" your computer – and your electricity – to generate money for themselves, *without your consent*. One way to do this is to trick a person into downloading a malicious mining application to their computer. This can even be done on a large scale, such as when a malware called Xbooster used Amazon's cloud to install itself and then steal processing power from a fleet of computers. However, criminals may just lure visitors to a webpage that causes the victim's web browser to run an embedded mining script (*see image to the left*). This latter tactic is found in ad networks that legitimate websites *unknowingly* serve to their visitors. It is less noticeable to surreptitiously run a script from within the user's browser — no exploits or vulnerabilities are needed.



How do you know if you have been cryptojacked? More importantly, how can you avoid it? If your computer is running slow, the processor has a higher than normal usage, the computer's temperature is higher, and/or the computer's fan is running more quickly, you may have been cryptojacked. The following steps may help reduce the likelihood that you will become a victim of cryptojacking:

- **Disable JavaScript** – You can block JavaScript for specific sites **or** disable it altogether. The problem with *disabling* is that it is a very aggressive way to block mining and will break legitimate websites.
- **Enable Coin Mining Blockers** – There are several browser extensions available, such as No Coin and Coin-Hive Blocker, that blacklist known domains and mining scripts and are regularly updated.
- **Keep Up-to-Date Anti-Malware Software** – Some anti-malware software detects and blocks cryptominig malware. Install a legitimate anti-malware program and keep it up-to-date.
- **Install Software Updates** – Installing operating system (OS) updates may help you block attacks that try to download cryptojacking software or other malicious programs to your computer.
- **Disable Remote Services** – Consider turning off remote services to your computer.
- **Don't Click On Unsuspecting Links** – Be leery of links in email or clicking links to unsolicited web sites. Use known bookmarks or manually enter web addresses to access favorite sites.

For more information, visit the security tip at https://www.us-cert.gov/ncas/tips/ST18-002.

What Is Threatening You Now?

According to a new Quarterly Threat Report by Proofpoint, there are some new trends of cyber threats. The report is based on a daily analysis of more than 5 billion email messages, hundreds of millions of social media posts, and more than 250 million malware samples. The following are some key take aways from that report:

- Banking trojans, malware specifically designed to break into online bank accounts and transfer money to other accounts controlled by criminals, has displaced ransomware as the top malware in email. Emotet was the most widely distributed banking Trojan.
- Social engineering is on the rise! According to the report, roughly 95% of web-based attacks now redirect into social engineering schemes instead of exploit kits.
- Social media support fraud, called "angler phishing," doubled from the previous quarter. This threat uses fake customer-support accounts to promise help, but instead attempts to steal credentials.

On a positive note, exploit kits are rapidly declining in popularity as malware creators find other attacks to be easier and more profitable. Could it be that criminals are turning more to cryptojacking as an easier payout? Unfortunately, the Proofpoint report claims that users are going to continue doing things to make themselves more supseptible to cyber threats, such as clicking on suspicious links, visiting dangerous web sites on the Internet, and downloading files that they probably should not.

What can you do to beat the trend of cyber threats? Be vigilant to ongoing phishing attacks, especially as social engineering grows more numerous and more convincing. Guard account passwords like you would guard the keys to your house or safe – never share passwords with anyone! Be leery of clicking links in email, especially if it is within an unsolicited message. Keep up-to-date software. Avoid insecure public Wi-Fi networks and never conduct sensitive business on public networks without a VPN or other secure communications method. Remember…*Cybersecurity Is Our Shared Responsibility!* You may view the Proofpoint report via the following link: https://go.proofpoint.com/Threat-Report-Q12018.html.

Don't forget the other **monthly newsletters** that are available to you! The following are the various cybersecurity newsletters the ESRMO distributes each month. We hope you find them beneficial.

- **SECURITYsense Newsletter:** A licensed newsletter for State employees that contains several articles involving current cybersecurity issues. **Note:** *You must have a Microsoft O365 account with access to the ESRMO external SharePoint site to access this resource*.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access) or any other public access network is strictly prohibited.

- **Security Tips Newsletter:** A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is ***How to Spot Phishing Messages Like a Pro***.

https://www.cisecurity.org/resources/newsletter

- **SANS OUCH! Newsletter:** A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Stop That Malware.***

https://www.sans.org/security-awareness-training/ouch-newsletter

---

Did you know that The SANS Institute also provides *free* awareness **videos** and **webcasts**? The SANS Video of the Month may be accessed at https://securingthehuman.sans.org/resources/votm.

Also, The SANS Institute offers free webcasts on a variety of topics that may be accessed at https://www.sans.org/webcasts/upcoming.

Tentative PCI Webinars by Coalfire

The following is a *tentative* schedule for webinars on PCI-DSS that will be presented in 2018. An announcement regarding each webinar will be sent about three (3) weeks prior to the scheduled date.

Date/Time: 8/14/2018 @ 10:00-11:00 AM ET
Topic: *PCI in the Cloud - Coalfire can address PCI in the Cloud as a whole, and/or address both AWS & Azure*

Date/Time: 10/9/2018 @ 10:00-11:00 AM ET
Topic: *Updates to the PCI DSS and PCI Hot Topics*
Presenter: Joseph D. Tinucci

Date/Time: 12/4/2018 @ 10:00-11:00 AM ET
Topic: *Managing Service Providers - Also address new Service Provider requirements in PCI*

Emergency Management Institute Cyber Virtual Tabletop Exercise

FEMA's Emergency Management Institute (EMI) Virtual Tabletop Exercise (VTTX) Program will offer three cyber security breach scenarios **August 7, 8, and 9, 2018**. The VTTX occurs 12 p.m. – 4 p.m. ET. To participate, send an email to Doug Kahn at douglas.kahn@fema.dhs.gov or call 301-447-7645. Also, send a courtesy copy email to the Integrated Emergency Management Branch at fema-emi-iemb@fema.dhs.gov or call 301-447-1381. Content is the same each day and participants would attend only one session. Additional information is available at https://training.fema.gov/programs/emivttx.aspx. The registration deadline is **July 20**.

The VTTX:

- Is designed to examine the ability of federal, state, local, tribal, and territorial jurisdictions to a respond to a cyber attack
- Involves key personnel discussing simulated scenarios in an informal setting
- Can be used to assess plans, policies, training, and procedures during a cyber attack

The VTTX is designed for a group of 10 or more representatives from state, local, tribal, and territorial emergency management communities of practice. It provides a unique opportunity for responders across the nation to simultaneously participate in a hazard-specific, facilitated discussion. Participants will need to connect via a site equipped with the appropriate VTC capability (not Adobe Connect or FaceTime-based), but alternate ways to participate are also available upon request.

Other Events To Remember…

June 25: Assurance CM UAT – Application updates rolled out

June 28: Assurance CM Production – Application updates rolled out

June 28 (10:00am – 11:00am): Assurance NM Demonstration; DIT, 3900 Wake Forest Road, Conference Room Flag

- Contact Debora.Chance@nc.gov to attend. Open to all Executive Branch agencies

August 7-9: Emergency Management Institute Cyber Virtual Tabletop Exercise

August 29-30: Digital Government Summit, Hilton North Raleigh, Raleigh, NC

September 1: Agency Compliance Reports Due

September 1-30: National Preparedness Month

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.