Monthly Cybersecurity Newsletter

August 2017 Issue

Enterprise Security and Risk Management Office (ESRMO)

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

---

Say Goodbye to Adobe Flash!

Software vendor, Adobe, has announced that it is ending their Flash software. They are targeting 2020 as the year Flash dies! The main reason Adobe announced this move is that Flash has seen a decline in its use in the past few years. Adobe stated that more sites are turning away from proprietary code like Flash toward open standards like HTML5, WebGL and WebAssembly, and that these components now provide many of the capabilities and functionalities that plugins pioneered. While that is true, a more serious reason to phase out Flash is the security vulnerabilities that are *consistently* found in the software. For years, unpatched vulnerabilities in Flash plugins have been the top moneymaker for those creating various commercial "exploit kits." According to one security firm, Flash Player vulnerabilities provided six of the top ten vulnerabilities used by exploit kits in 2016. Exploit kits offer an expedited crimeware-as-a-service (CaaS) means where users pay per install of their malware which can be included into hacked or malicious sites and exploit browser plugin flaws.

Apple stopped years ago pre-installing Adobe Flash in its iOS products (e.g. iPod Touch, iPhone, iPad) amid performance and security issues. Microsoft also said it has begun phasing out Flash from its Microsoft Edge and Internet Explorer web browsers. They will remove Adobe Flash from the Windows OS entirely by the end of 2020. For now, Microsoft Edge, the default browser on newer versions of Windows, will continue to prompt users for permission to run Flash on most sites the first time the site is visited. Windows will remember the user's preference on any subsequent visits. Other browser makers have been more aggressive with their move away from Adobe Flash. Google Chrome has been automatically blocking Flash ads from running since September 2015, meaning you have to click to play them. Mozilla Firefox started blocking some Flash elements in 2016. Of course, the removal of support for Flash does not actually remove Flash from the Internet. That is up to developers *and* end users! The best advice is to completely remove Adobe Flash from your computer system unless you absolutely need to use it. If Flash is needed, it is recommended to enable it only when necessary. Users should be sure to disable Flash again when it is not needed. Another solution is to keep Flash installed in a browser that you do not normally use, and then to only use that browser on sites that require it.

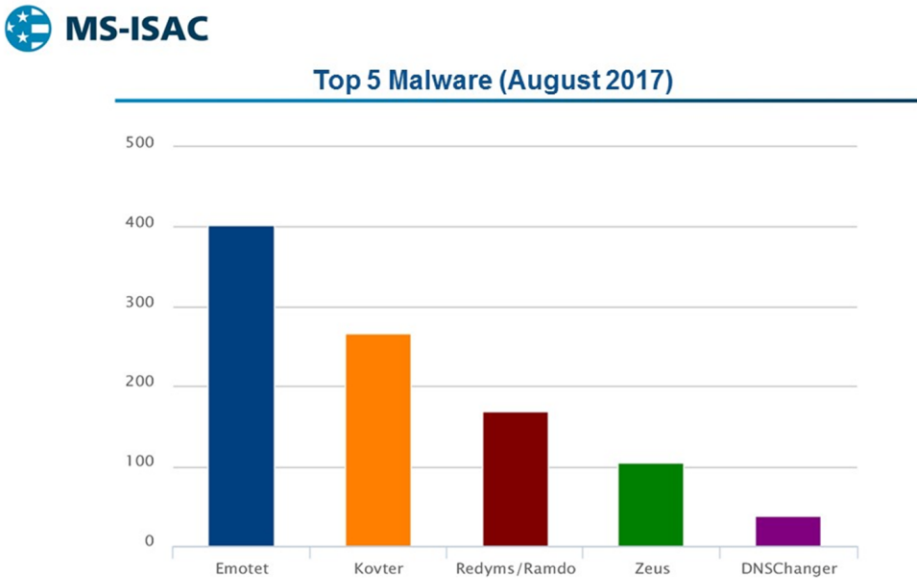
Don't Take The Bait!

One of the articles in this month's SECURITYsense Newsletter is about the top attractive "phishing lures". Phishing is a *daily* problem that presents a serious risk to everyone. Phishing is used to attack government entities, businesses, and individuals, and it was even a vector of attack in the recent presidential election. One security company compiled data on phishing attempts and found the following list to be the most successful lures in those attempts. Given the pervasiveness of the threat, we thought we would share this list of the most common types of "lures" that attackers use to bait people into gaining access to sensitive information.

1. Security Alert – 21%
2. Revised Vacation and Sick Time Policy – 14%
3. UPS Label Delivery 1ZBE312TNY00015011 – 10%
4. BREAKING: United Airlines Passenger Dies from Brain Hemorrhage – VIDEO – 10%
5. A Delivery Attempt was made – 10%
6. All Employees: Update your Healthcare Info – 9%
7. Change of Password Required Immediately – 8%
8. Password Check Required Immediately – 7%
9. Unusual sign-in activity – 6%
10. Urgent Action Required – 6%

The above list shows that we must remain vigilent in spotting phishing or spoofed email. Don't take the bait as it could result in some very malicious activity.

For Your Situational Awareness: The following is a list of malware that State, Local, Tribal, and Territorial (SLTT) governments reported for the month of August 2017. This information is provided by the Multi-State Information Security and Analysis Center (MS-ISAC).



Don't forget, there are other **monthly newsletters** available to you that contain a wealth of information! The following are the various cybersecurity newsletters the ESRMO distributes each month. These newsletters contain information we hope you find beneficial.

- **SECURITYsense Newsletter:** A licensed monthly newsletter that contains several articles involving current cybersecurity issues.

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), Extranet, or 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 is on ***Connected Home Devices: The Internet of Things***.

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 ***Backup & Recovery.***

http://securingthehuman.sans.org/resources/newsletters/ouch/2017

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.

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT

Looking for more training? Have you considered FedVTE? The Department of Homeland Security (DHS) provides FedVTE courses at no cost to government personnel, including contractors, and to U.S. Veterans. Courses include a variety of cybersecurity related topics and certification preparation courses ranging from beginning to advanced level. New courses are added or updated on a rolling basis. If you are interested in this education opportunity, more information about the FedVTE offering may be found at the following link: https://fedvte.usalearning.gov/pdf/FedVTE_FAQs-Spring%202016.pdf

---

PCI DSS COMPLIANT

The NC Office of the State Controller (OSC) is promoting **E-commerce/ PCI Data Security Standards (DSS)** educational opportunities this year with the help of Coalfire. The next training opportunity will be on **October 24** from 10:00am – 11:00am and will be ***Implementing an Effective Employee Security Training Program***. Additional information for each of the webinars, along with a registration link, will be distributed a few weeks prior to each scheduled event.

The following training opportunities will be available through the statewide **Learning Management System (LMS)**. These courses are designed to meet the 2017 annual cyber awareness training requirement for State employees.

- **October** – Public Wi-Fi: Be Careful Out There
- **December** – Office Security: Keeping Your Office Secure

If you have questions about the training schedule or the training content, please contact Maria Thompson, State Chief Risk Officer, at maria.s.thompson@nc.gov or at (919) 754-6578.

The Virginia Space Grant Consortium (VSGC) has made five short videos to provide background on the importance of cybersecurity in our computer and data-driven world. In the videos, practicing cyber professionals from the National Institute of Standards and Technology (NIST) and elsewhere discuss their work, their career paths, and offer tips on how to prepare for a career in cybersecurity. To view these videos, visit the following link:

https://www.youtube.com/playlist?list=PLKrkeCUPIKhuJxqo-CCSdKT35Qa568VIl

---

Upcoming Events…

- **September 1, 2017** – Agency Compliance Reports due!
- **October 2017** – National Cyber Security Awareness Month
- **October 19-20** – Cyber Awareness Day @ NC Rural Center
- **October 27, 2017** – Triangle InfoSeCon 2017 – More information may be found at http://www.triangleinfosecon.com/

Do you have something to share? Is there a topic you think we should cover in a future newsletter? The ESRMO encourages all security professionals to share topics that will be of value to other 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.