Monthly Cybersecurity Newsletter

September 2017 Issue

Enterprise Security and Risk Management Office (ESRMO)

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

---

The Equifax Breach – Why Patching is Important!

We have probably all heard about the Equifax breach that was disclosed in early September. The consumer credit reporting agency said it discovered an intrusion on July 29, 2017 where hackers broke in through a new vulnerability in the software that runs some of its applications. The hackers downloaded Equifax data in one fell swoop sometime in May 2017. The vulnerability (CVE-2017-5638) was disclosed in March 2017, *two months earlier*, in a popular open-source software package called Apache Struts that is used to create server side Java-based web applications. The vulnerability was first revealed around March 7, 2017, when security firms began warning that attackers were actively exploiting a new "zero-day" vulnerability in Apache Struts. Zero-day vulnerabilities refer to software flaws that hackers discover and figure out how to exploit before the vendor knows about them. Apache had released new versions of the software *the next day* to mitigate the flaw. Equifax claims its "security organization" was aware of the vulnerability at the time it was disclosed and worked to identify and to patch any vulnerable systems it had. However, according to a company statement, they did not patch the affected servers until July 30, 2017, some time after the instrusion was discovered and the hacker(s) were able to explot the vulnerability.

The Equifax breach shows us just how important it is to patch vulnerable systems! This incident potentially impacts personal information of about 143 million U.S. consumers – primarily names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, the hackers potentially accessed credit card numbers for approximately 209,000 U.S. consumers, and certain documents with personally identifiable information (PII) for approximately 182,000 U.S. consumers. Equifax also found unauthorized access to limited personal information for about 400,000 U.K. people. Both Visa and MasterCard are sending alerts to financial institutions across the United States, warning them about the credit card information that were stolen in the Equifax data breach. Fraudsters can use this information to conduct e-commerce fraud at online merchants. Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. Even if a person's data has not been compromised, experts strongly urge people to consider freezing access to their credit. To learn more about free security freezes and free annual credit reports, visit www.ncdoj.gov. If you have been victimized by a scam or an unscrupulous business, you should file a complaint or contact the NC Attorney General's office at 1-877-5-NOSCAM.

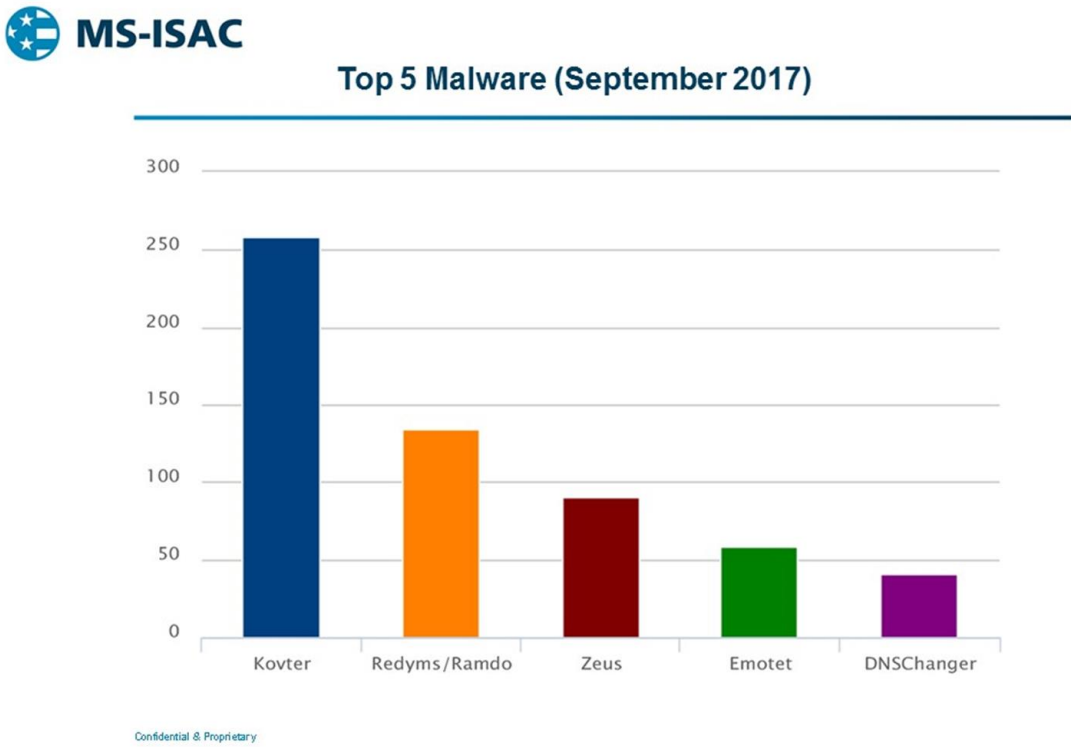
Beware of Hurricane Fraud!

2017 has been a busy and disasterous year for hurricanes. Our hearts go out to those who have been impacted by the recent storms. It seems these dangerous storms have also brought with them many scams that take advantage of these disasters and the good will of people. The United States Computer Emergency Readiness Team (US-CERT) warns people to be watchful for malicious activity that targets both disaster victims and potential donors. People should be cautious when receiving and responding to emails about recent hurricanes and disasters, even if those emails appear to originate from trusted sources. Disaster-related phishing emails may trick users into sharing sensitive information, and they may contain links or attachments directing people to malware-infected websites. Individuals should also be cautious of social media requests, calls, texts, or door-to-door solicitations related to the recent hurricanes. The Federal Emergency Management Agency (FEMA) has also provided a list of disaster fraud guidelines that specifically advises the public to beware of individuals posing as staffers of the government agency. FEMA states that none of its personnel will charge a fee for helping storm victims, adding that those in need of aid should ask to see employee ID badges or other identification. For more information about how to avoid becoming a victim of fraudulent activity and taking preventive measures, review the information at the following sources:

- https://www.us-cert.gov/ncas/current-activity/2017/09/08/Hurricane-Related-Scams
- https://www.fema.gov/news-release/2017/09/24/fema-advises-disaster-applicants-beware-rumors-misinformation-and-fraud

---

For Your Situational Awareness: The following chart shows the top malware State, Local, Tribal, and Territorial (SLTT) governments reported for the month of September 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 about ***Staying Secure on Social Media***.

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 about ***Password Managers.***

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.

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 the webinar, along with a registration link, will be distributed a few weeks prior to the 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.

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at no cost to government staff, including contractors. With 60+ courses at varying levels of proficiency – from beginners to advanced – all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated on a rolling basis.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available courses of varying proficiency – beginner to advanced
- ✓ Self-paced
- ✓ Many popular certification courses including:
  - Network +
  - Security +
  - Certified Information Systems Professional (CISSP)
  - Windows Operating System Security
  - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework
- ✓ Individuals can take courses to build the required knowledge, skills, and abilities in the cybersecurity field
- ✓ Taught by experienced cybersecurity subject matter experts

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

Upcoming Events…

- **September 28 – October 1:** 2017 National Emergency Management Association (NEMA) Annual Forum
- **October 2017:** National Cyber Security Awareness Month (NCSAM)
- **October 8-14, 2017:** Fire Prevention Week
- **October 19, 2017:** International Shakeout Day
- **October 19-20:** Cybersecurity Awareness Symposium @ NC Rural Economic Development 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 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.

OCTOBER 19 – 20, 2017

CYBER AWARENESS SYMPOSIUM

How to become more proactive in breach-fatigued world

In support of National Cyber Awareness Month, the Department of Information Technology (DIT), Enterprise Security and Risk Management Office (ESRMO) will be hosting a **two-day** Cyber Awareness Symposium **open to all state and local government employees**. Attendees will learn about the current threat landscape participate in cyber workshops on “Threat Hunting and Incident Response" sponsored by industry partners. Signup sheets for Attendance and full agenda will be provided.

Opening Remarks: State Chief Information Officer

Meet your CISO. Panel Discussion by Agency CISOs – Life in the Trenches

Cyber Threat Insights: Tales from the Frontlines Dir. Counter Threat Unit – Dell SecureWorks

Threat Hunting Workshop – Finding Insider Threats

IBM SIEM (QRadar) Workshop

Location: NC Rural Economic Development Center, Room 150/151, 4021 Carya Drive, Raleigh, NC 27610

Oct. 19 – 9 a.m. – 4:30 p.m.

Oct. 20 – 9 a.m. –1 p.m.

FOR MORE INFO AND AWARENESS TIPS VISIT: https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management