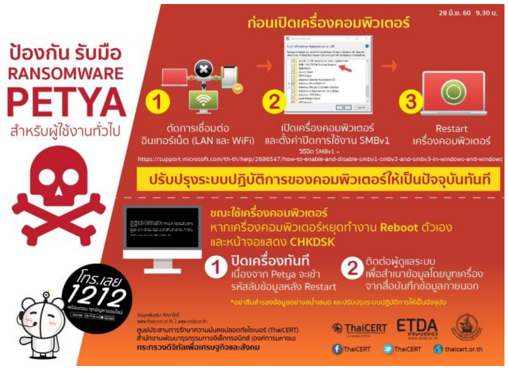
Monthly Cybersecurity Newsletter

July 2017
Issue

Enterprise Security and Risk Management Office (ESRMO)

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

Petya/NotPetya Ransomware Attacks


28 มิ.ย. 60 9.30 น.
ป้องกัน รับมือ
RANSOMWARE
PETYA
สำหรับผู้ใช้งานทั่วไป
ก่อนเปิดเครื่องคอมพิวเตอร์
1 ตัดการเชื่อมต่ออินเทอร์เน็ต (LAN และ WiFi)
2 เปิดเครื่องคอมพิวเตอร์และตั้งค่าปิดการใช้งาน SMBv1
วิธีปิด SMBv1 -
https://support.microsoft.com/th-th/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows
3 Restart เครื่องคอมพิวเตอร์
ปรับปรุงระบบปฏิบัติการของคอมพิวเตอร์ให้เป็นปัจจุบันทันที
ขณะใช้เครื่องคอมพิวเตอร์
หากเครื่องคอมพิวเตอร์หยุดทำงาน Reboot ตัวเอง และหน้าจอแสดง CHKDSK
1 ปิดเครื่องทันที เนื่องจาก Petya จะเข้ารหัสลับข้อมูลหลัง Restart
2 ติดต่อผู้ดูแลระบบ เพื่อสำเนาข้อมูลโดยบูทเครื่องจากสื่อบันทึกข้อมูลภายนอก
*อย่าลืมสำรองข้อมูลอย่างสม่ำเสมอ และปรับปรุงระบบปฏิบัติการให้เป็นปัจจุบัน
โทร.เลย 1212
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ThaiCERT
ETDA
ThaiCERT
ThaiCERT
thaicert.or.th

Ransomware is a serious problem! One particularly nasty one, called Petya, was discovered in March 2016. Like other ransomware, Petya encrypts a computer's file system, holding the data hostage, and demands payment to decrypt the victim's data. Petya is also capable of gathering account passwords from Windows computers and domain controllers on a network. In late June 2017, a new variant of Petya, oddly called *NotPetya*, crippled thousands of computers across the world, with FedEx being among those hit the hardest. FedEx reported that NotPetya disrupted services at one of its units, causing widespread service delays, loss of revenue due to decreased business, and a drop in shares of stock. They also claimed that some damage from the new variant of Petya may be permanent.

NotPetya began infecting computers in Ukraine, compromising more than 12,500 machines. Infections of the ransomware were then observed in 64 other countries, including the United States. NotPetya exploits a known vulnerability in Microsoft Windows, the same one that the recent WannaCry ransomware exploited. Fortunately, Microsoft released a patch for what is called the "EternalBlue" exploit in March 2017 (MS17-010); however, many organizations delayed installing the fix. As of early mid-July 2017, about *50,000 machines* were still vulnerable to the EternalBlue exploit! Many of those machines that were not patched had already been hit with the WannaCry ransomware attacks in May 2017. NotPetya was actually worse than WannaCry. Not only did it use the same exploit WannaCry used, but it also traversed through a network using credentials from memory or the file system. It seems that ransomware attacks are going to become more commonplace – and more sophisticated – in the years ahead. So, what can you do to prevent a ransomware infection? The following tips may help:

- Make sure your computer's operating system (OS) and applications are up to date.
- Make sure your anti-virus (AV) software is up to date with the latest virus signatures.
- Use an up to date web browser that has safe searching capabilities.
- Avoid clicking links that are within unsolicited email ***and*** text messages.
- Make sure your data is backed up ***and*** can be restored when needed.

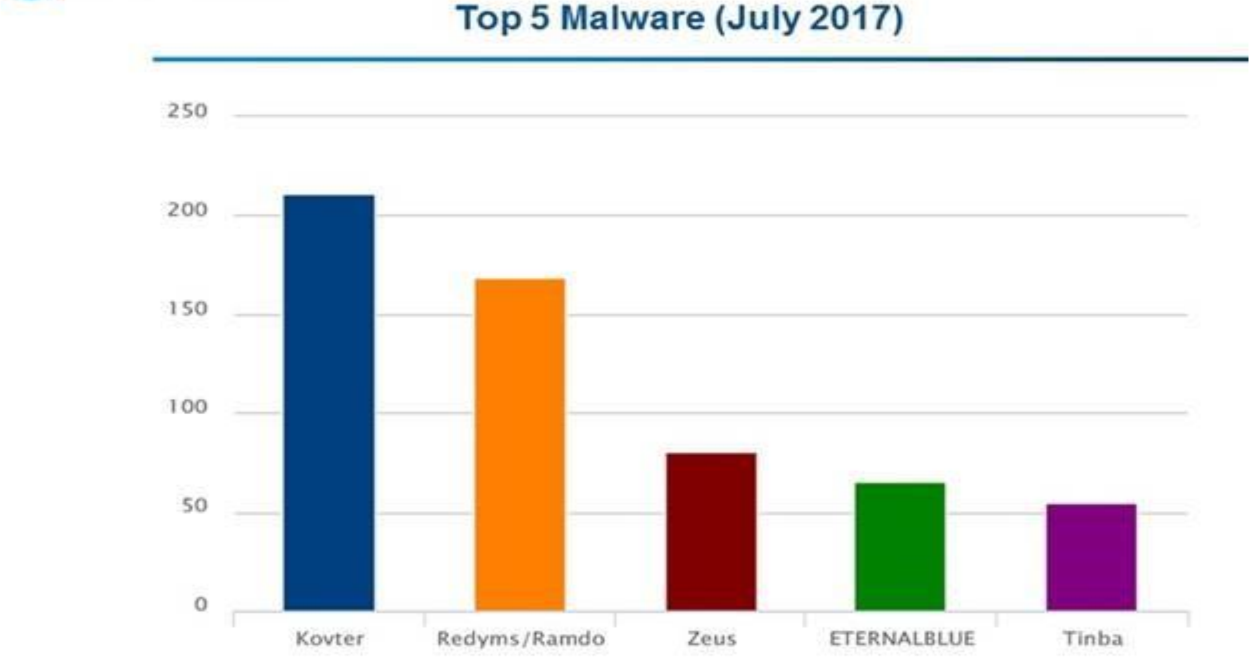
Malicious Doc Makes a House Call

Earlier this year, a sophisticated phishing scam began targeting Google users and spread rapidly across the Internet. The bad thing with this particular phishing scam was that the message did not immediately look like a phishing email. The phishing campaign worked by sending individuals a message that appeared to come from someone within *their contacts list*, and which indicated that the contact had shared a Google Doc with them. The message contained a malicious link to a file shared on the Google Docs online service. Clicking the link in the message would take the user to a *real Google web address* and prompt the user to sign-in and authorize a malicious third-party web application that was *impersonating* Google Docs. Once authorized, the app would have access to the user's emails and contact list, and be able to send emails on the person's behalf.

In response to this scam, Google disabled offending accounts that participated in it. Google also removed fake pages and they pushed updates to their Safe Browsing service, a service which identifies unsafe websites across the web. Going forward, anytime a user encounters an *unverified application* seeking to link itself to Google's own applications, users will be presented with a warning indicating that the app is unverified. These new notices will inform users that they may be at risk. Hopefully, this will help people make better decisions to keep their information safe. Users do have the option to dismiss the alert. So far, though, resisting the urge to click on a link remains the ***best line of defense*** to these types of scams. If you receive a message that you were not expecting, even if it is from an email address that you supposedly know, do not click on a link until you verify that it is legit. *Thinking before clicking may save you a lot of trouble!*

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

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 edition is ***Identifying and Reporting Common Scams***.

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 ***Gaming Online Safely & Securely***.

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

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.

- **August** – Mobile Security: Mobile Devices – The Future is Now
- **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.

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT

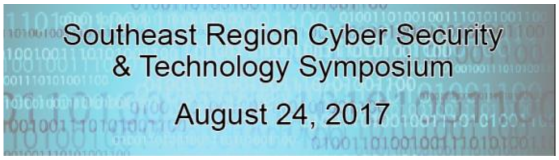
Looking for more training? Have you considered FedVTE? The Department of Homeland Security (DHS) provides FedVTE courses at no cost to government personnel, including contractors, and to U.S. Veterans. Courses include a variety of cybersecurity related topics and certification preparation courses ranging 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

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 following are some of the remaining training opportunities that are coming soon:

- **August 15** at 10:00am – What is a Physical Security Assessment and Benefits?
- **October 24** at 10:00am – Implementing an Effective Employee Security Training Program

Each webinar will last approximately **1 hour**. Additional information for each of the webinars, along with a registration link, will be distributed a few weeks prior to each scheduled event.



The Offices of United States Senator Richard Burr and United States Senator Thom Tillis, the North Carolina Defense Technology Transition Office (DEFTECH), the North Carolina Military Business Center, and the North Carolina Military Foundation will be hosting the **Southeast Region Cyber Security & Technology Symposium** on **August 24** in Chapel Hill, North Carolina. This symposium will provide commercial and government entities information about operational cyber perspectives, threats, needs, teaming and business opportunities. More information about this event may be found at the following link: http://www.ncmbc.us/17cyber/

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 (NCSAM)

➢ **October 27, 2017** – Triangle InfoSeCon

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.