Monthly Cybersecurity Newsletter

January 2019
Issue

Enterprise Security and Risk Management Office (ESRMO)

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

---

Secure Those New Devices!

During the holidays, many people give and receive internet-connected devices that are known as Internet of Things (IoT) — such as smart TVs, watches, toys, phones, and tablets. IoTs provide a level of convenience to our lives, but they can also increase the risk to our privacy and security. These connected devices can also require that we share more information than we have previously shared. The National Cybersecurity and Communications Integration Center (NCCIC), part of the Cybersecurity and Infrastructure Security Agency (CISA), recommends the following important steps to make your new IoTs more secure:

1. **Use strong passwords.** Passwords are a common form of authentication and are often the only barrier between you and your personal information. Some internet-enabled devices are configured with *default passwords* to simplify setup, but these can be easily found online. Therefore, choose strong passwords to better secure your device.
2. **Configure the security settings.** Most devices offer a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more at risk. Therefore, examine the settings, particularly the security settings, and select options that meet your needs but do not increase your risk.
3. **Keep software up-to-date.** When manufacturers become aware of vulnerabilities in their products, they often issue patches to fix the problem. Patches are software updates that can fix known vulnerabilities within your device's software. Be sure to apply relevant patches as soon as possible to protect your devices.
4. **Connect carefully.** Once your device is connected to the internet, it is also connected to millions of other computers, which could allow attackers access to your device and data. Consider whether continuous connectivity to the internet is really needed.

For more information, review the following helpful tips from US-CERT:

- Choosing and Protecting Passwords: https://www.us-cert.gov/ncas/tips/ST04-002
- Good Security Habits: https://www.us-cert.gov/ncas/tips/ST04-003
- Understanding Patches and Software Updates: https://www.us-cert.gov/ncas/tips/ST04-006

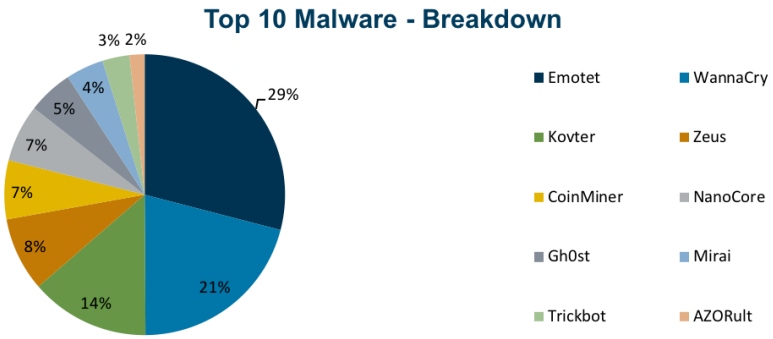
Threat of the Quarter - Emotet

2018 saw a proliferation of malicious software (malware) attacks. One of the most costly and destructive examples of malware that affected state, local, tribal, and territorial (SLTT) governments in 2018 was **Emotet**. Experts predict that it will likely continue to be prevalent in 2019.

Emotet is highly infectious, due to its worm-like features that result in rapidly spreading across a network. This makes it difficult to combat and costing SLTT governments up to *$1 million per incident* to remediate. By the time an Emotet infection is discovered, most of the network has already been compromised, with up to 90% of the system infected. At that level, it is very difficult to remove the infection. Recovery often requires creating a separate, clean network of cleaned computers – an expensive and time-consuming process.

Emotet is disseminated through malspam (emails containing malicious attachments or links) and imitates third parties that may seem familiar to the recipient. A system is initially infected with Emotet when a user opens or clicks a malicious link, PDF, or macro-enabled document that is included in the malspam. To make matters worse, Emotet's persistence relies on its ability to constantly evolve and to be updated through communication with its command and control (C2) server. An Emotet infection could also mean a data breach, because it can exfiltrate email data, accessing the body and subject of emails up to 180 days in the mail history.

Emotet is an advanced, modular banking trojan that primarily functions as a downloader or dropper of *other* banking trojans and types of malware. Once Emotet infects a system, it uses its worm-like abilities to infect the rest of the network and drop other types of malware across the network. The ability to drop other types of malware can lead to other infections, such as ransomware, but most often other banking trojans, which increases the cost of recovery. For the past year, Emotet appeared on the Center for Information Security's (CIS) monthly Top Ten Malware list every month and has helped other types of malware stay or make it onto the list.



Recommendations

CIS recommends the following steps to reduce the risk of becoming infected by Emotet:

1. Restrict SMB inbound communication between client systems
2. Disable all macros except those which are digitally signed
3. Apply patches to all systems after appropriate testing
4. Maintain up-to-date antivirus program

5. Implement filters at the email gateway to filter email with known malspam indicators
6. Mark external emails with a banner denoting it is from an external source
7. Raise awareness among staff and peers to do the following:
    - ✓ Recognize suspicious emails,
    - ✓ Do not click on links in such emails,
    - ✓ Do not post sensitive information online,
    - ✓ Never provide usernames, passwords or other personal information to unsolicited requests.

More information about Emotet may be found in the MS-ISAC Security Primer – Emotet.

Don't forget the following resources available to you. The following are some other **cybersecurity newsletters** the ESRMO recommends. We hope you find them beneficial and share them with your peers!

Security Awareness Newsletter: A monthly security awareness newsletter that is provided by KnowBe4 for all State employees. ***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS).

- 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 ***Search Yourself Online.***

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

---

Do you know what information is publicly known about you?
What information can attackers found about you by simply searching the internet? This month's SANS OUCH! Newsletter explores some tools and techniques you can use to discover what information is on the internet about you. Consider what you share publicly and the impact that could have on you and your family.

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link:

https://www.sans.org/webcasts/upcoming.

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 and contractors. With 60+ courses, all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated regularly.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available self-paced courses of varying proficiency – beginner to advanced
- ✓ 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 their knowledge, skills, and abilities in cybersecurity
- ✓ Taught by experienced cybersecurity subject matter experts

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

Upcoming Events…

January 21: Martin Luther King Day

January 28: Data Privacy Day

January 30: EMI e-Forums - Topic: Diversity and Inclusion in Emergency Management. For questions, contact FEMA-EMI-eforums@fema.dhs.gov

January 31: SANS Webinar: Best Practices to Get You CloudFit - 12 AWS Best Practices for Cloud Security

February 5: SANS Webinar: CTI Requirements and Inhibitors: Part 1 of the 2019 SANS Cyber Threat Intelligence Survey

February 7: SANS Webinar: CTI Tools, Usage and a Look Ahead: Part 2 of the 2019 SANS Cyber Threat Intelligence

---

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 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.