Monthly Cybersecurity Newsletter

July 2018 Issue

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

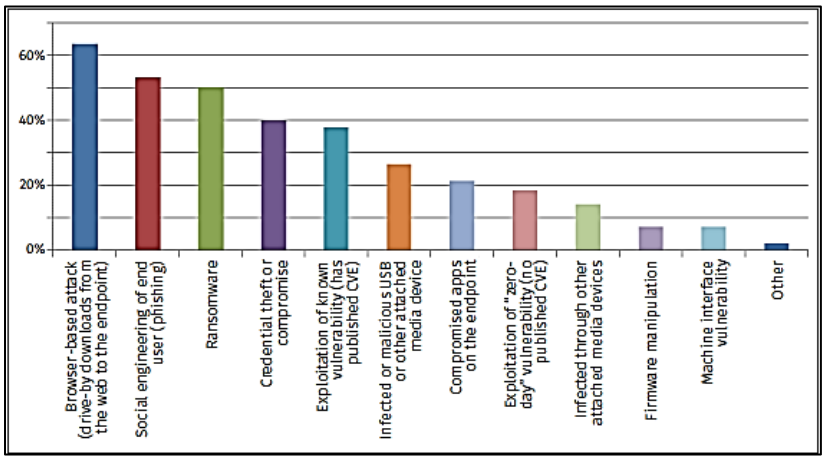
From the Desk of the State Chief Risk Officer – Maria Thompson

---

The End (or Beginning?) of Security

A recent survey conducted by the SANS Institute revealed some interesting things about endpoint protection and response. The connection of desktops, laptops, mobile computing devices, and other devices to an organization's network creates paths of attack. Each of these *endpoints* is a way for an attacker to gain access into an organization's network and data. Endpoint security attempts to ensure that all connected devices are better protected and tries to limit the possible means of attack through those devices. Several hundred professionals recently took a 2018 SANS survey and shared their concerns about endpoint security.

The most successful endpoint compromises leverage a common factor – the *human being*. The end user is the most common denominator to endpoint compromises! The top three paths of attack from the survey results leverage human actions taken on endpoints to achieve success. These top threat vectors are as follows: web drive-by (63%), social engineering/phishing (53%), and ransomware (50%). The survey also revealed that account compromises were used 40% of the time and 90% of unknown, undetected malware is delivered via the web to the user. Another interesting fact is that 84% of endpoint breaches involved *more than one* endpoint. This included desktops, laptops, servers, endpoints in the cloud, and mobile computing devices. What this means is that a compromise of one endpoint or user will most likely lead to a compromise of other end points and users. Thus…*your actions affect others and your entire organization!* The chart below from the report reveals how endpoints are typically exploted.



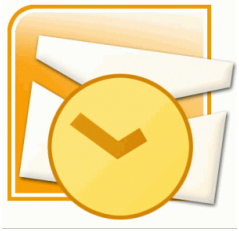
How can we reduce endpoint attacks? Although antivirus (AV) is the most commonly used tool to detect the initial attack, only 47% of attacks were detected this way. Other attacks were detected by security information and event management (SIEM) alerts and network analysis. The survey calls for organizations to augment their capabilities to more proactively defend their assets. It may be difficult for some organizations to implement more robust and more capable solutions to secure their endpoints; however, there are things we all can do to improve our security posture. The key is to practice *Defense in Depth!*

- Increase user training and awareness. Since most successful endpoint compromises involve social engineering, we must raise end user awareness and practice *safer cyber hygiene!*
- Practice the principle of least privilege. Restrict user access to the data / functions that are needed. If an attacker compromises an account, they have the same access as that user!
- Keep anti-virus enabled and up-to-date! Modern AV still catches a great number of threats.
- Keep operating systems and software patched. According to the survey, software vulnerabilities account for about 40% of endpoint exploits.
- Disable / uninstall unused applications, services, and network ports to limit vectors of attack.
- Discover all connected devices on your network and contain any unauthorized or insecure devices. Do not overlook possible points of attack, such as printers and scanners.
- Encrypt sensitive data, both in transit through the network and what is stored on devices.
- Be prepared for *when* an attack occurs! Develop incident response plans / procedures, and *practice them*. Run tabletop exercises on attack scenarios and practice your responses.

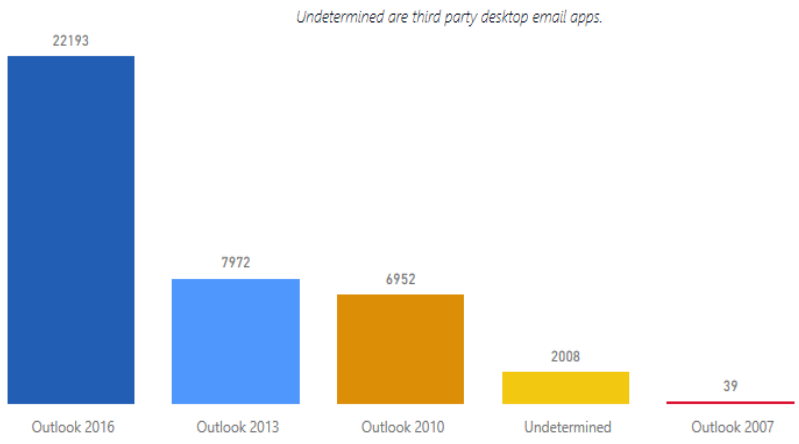
Remember, you can be the strongest protection or the weakest link in the security chain! To read the SANS Endpoint Protection and Response survey report, visit the following link:

https://www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460

Is Your Email Software Too Risky to Use?



The Department of Information Technology (DIT) is working on a project to ensure all end users are using approved and updated email solutions on the network. This is a multi-phased project that will focus on those email clients identified as most risky. As you may know, the use of unmanaged solutions on the network poses a risk to the enterprise and to citizens' data. As part of phase 1, all access to state email using *unauthorized email clients* will be prohibited. The chart below shows the current posture of email software across the enterprise. There are many instances of older or undetermined email clients being used to access State email.



On August 19th 2018, DIT will be implementing a block to restrict access through email solutions that are not part of the standard State approved solution list. After this date, no agency will be able to use third party solutions, (i.e. those identified as undetermined), with the exception of those who have been approved by the State CIO with a verifiable and justified business need.

The table below shows the support lifecycle for Microsoft clients and their end dates. Currently, the only approved Office product is **Office 2016**. All others are considered end of support UNLESS the agency has purchased extended support through Microsoft. DIT will addresss Outlook 2007 - 2013 clients during subsequent phases of the project. You may contact the DIT Unified Communications team for specific details on licensing.

Product	Mainstream Support End	Extended Support End
Office 2013 Service Pack 1	4/10/2018	4/11/2023
Office 2010 Service Pack 2	10/13/2015	10/13/2020
Office 2007 Service Pack 3	10/09/2012	10/10/2017

If there is a business need to use an unsupported or non-standard solution, please work with your agency Security Liaison to submit an exception request by completing the form located at the following link: https://files.nc.gov/ncdit/documents/files/Form-C.pdf. The exception form must detail the Agency's methods to secure the application(s) and the process and procedures in place to maintain patch and configuration compliance. Thank you for your support.

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 ***Sun, Sand, and Cybersecurity***.

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 ***Phone Call Attacks & Scams.***

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

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link: https://securingthehuman.sans.org/resources/votm.

The SANS Institute free webcasts may be accessed via the following link: https://www.sans.org/webcasts/upcoming.

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 addresses PCI in the Cloud as a whole*
Presenter: Dan Stocker

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*

PREPTalks
New perspectives for emergency managers

The Federal Emergency Management Agency (FEMA), in partnership with organizations that collectively represent the emergency management profession, has released two video presentations from the PrepTalks Symposium on May 30, 2018. These presentations are from thought leaders in youth preparedness and provide concrete actions that can reduce children's vulnerability to disasters. "Youth preparedness is the foundation for building a culture of preparedness now and in the future," said Dr. Daniel Kaniewski FEMA Deputy Administrator, Resilience. "Dr. Lori Peek and Sarah Thompson provide their expert advice in the PrepTalks released today. I urge you to click, watch, and take action."

- Peek's PrepTalk, "Children and Disasters: Reducing Vulnerability and Building Capacity," brings to life the progress, ongoing challenges, and possibilities to reduce the vulnerability of children to disasters. Dr. Peek shared her extensive experience working with children during disasters, including a young survivor of Hurricane Katrina. Peek gives emergency managers five specific actions to take to reduce the vulnerability of children to disasters right now.
- Thompson's PrepTalk, "Youth: The Key to Building a Culture of Preparedness," highlights how children are great mobilizers, actors, and connectors within their communities for building a culture of preparedness. Thompson uses her experience and sociological data to show how emergency managers can use the natural curiosity of children to build preparedness in their communities.

Videos of the presentations and question-and-answer sessions, a discussion guide on youth preparedness, and related resources are available at https://www.fema.gov/preptalks. PrepTalks are a partnership between FEMA, the International Association of Emergency Managers, the National Emergency Management Association, the National Homeland Security Consortium, and the Naval Postgraduate School Center for Homeland Defense and Security.

Upcoming Events…

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