Monthly Cybersecurity Newsletter

April 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

---

Be Careful What You Type

You should be careful when typing a web address into your browser. It is very easy to enter a similar but incorrect domain name and end up somewhere you do not want to be. Unscrupulous individuals use domain names similar to more popular ones on the Internet in order to entice individuals who mistakenly type the wrong web address. This practice of using similar domain names and relying on individuals to type the wrong address is called *typosquatting*. A typosquatter's URL will usually be one of several kinds: a common misspelling of the known name (e.g. exemple.com), a differently phrased name (e.g. examples.com), a different top-level domain name (e.g. example.org), or an abuse of a country code (example.cm). In fact, a report published in December 2009 by McAfee found that .cm was the riskiest domain in the world, with 36.7% of the sites posing a security risk to users.

Once on a typosquatter's site, the user may be tricked into thinking he or she is on the intended site, through the use of similar logos, website layouts or content. Visiting such a site, however, may result in malicious software (malware) to be downloaded and installed on the end user's machine, or it may entice the end user to disclose private information. Most typosquatters are probably just aiming to make money by taking advantage of your errors. They will sometimes use spam emails with typosquatting URLs within the messages to trick others into visiting their sites. Under the Uniform Domain-Name Dispute-Resolution Policy (UDRP), trademark holders can lodge typosquatting complaints in order to wrest control over a disputed domain name. The legitimate domain holder will need to show that the registered typosquatted domain name is identical or "confusingly similar" to their trademark, that the registrant has no legitimate interest in the domain name, and that the domain name is being used in bad faith.

The scale of typosquatting is unfortunately very large. For instance, over 80% of all possible one-character variants of the domains for Facebook, Google and Apple are both registered and resolved. This means that those typosquatted variations will take you to some web page, one you may wish you did not visit! Everyone makes typos from time to time. If you find yourself somewhere you didn't intend to go due to a fat-finger error, do not be tempted to click through the unexpected page, even if what you are offered is a link to your intended destination. Simply close your browser and try again. It is a good idea to avoid directly navigating to web sites you frequent. Instead, bookmark the sites you visit most often, particularly those that store your personal and financial information, or that require a login for access. If you must type a URL, be very careful what you type. Making a mistake may cause you to regret it later.

Ransomware – It's Only Getting Worse!

According to experts, it seems that ransomware is only going to get worse. Ransomware is a type of malicious software designed to deny access to a computer system or data until a ransom is paid. This type of malware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware can be devastating to an individual or to an organization. Anyone with important data stored on their computer systems is at risk, including government agencies, healthcare systems and other critical infrastructure entities. Some recent ransomware victims include the city of Atlanta, Mecklenburg County, and the Colorado Department of Transportation (CDOT).

The National Cybersecurity and Communications Integration Center (NCCIC), a component of the Department of Homeland Security (DHS), has observed an increase in ransomware attacks across the world. We can expect criminals to continue launching successful, widespread attacks. According to one source, 45% of US companies hit with ransomware last year paid at least one ransom, but only 26% of these companies had their files unlocked. This confirms that paying a ransom does not guarantee data recovery. In fact, companies paying a ransom were attacked again 73% of the time. Almost every company reporting an attack (97%) said they had backups for the files affected by the ransomware, and 51% said the ability to recover on their own was the reason for not paying the ransom. Ransomware is a multi-billion dollar business with the number of new ransomware variants continuing to grow every quarter. It is not going away or slowing down soon. Organizations continue to fall victim to ransomware attacks.

NCCIC recommends the following precautions to protect against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Backup data on a regular basis and keep it on a separate device and store it offline.
- Follow safe practices when browsing the Internet.

In addition, NCCIC also recommends that organizations employ the following best practices:

- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

Following these steps can lower the risk of you becoming a victim to ransomware.

Spring 2018 Disaster Recovery Exercise

The Department of Information Technology (DIT) invites your State agency to participate in the Spring 2018 Disaster Recovery Exercise scheduled for **June 11 – 14, 2018**. This exercise is for agency mainframe customers. Please share this announcement with your mainframe application testers. The kickoff meeting date will be announced soon.

Thomas Tomczak with DIT will be leading this exercise; please contact him with any questions you may have about the event. Thomas can be reached via email Thomas.Tomczak@nc.gov or by phone 919-754-6349. We look forward to your participation!

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), 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 on ***Securing Devices by Making Simple Changes***.

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 ***Stop That Phish.***

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

---

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.

Cyber Virtual Tabletop Exercise

FEMA's Emergency Management Institute (EMI) Virtual Tabletop Exercise (VTTX) Program will offer three cyber security breach scenarios **June 5, 6, and 7.** The VTTX occurs **12 p.m. – 4 p.m. ET**. To participate, send an email to Doug Kahn at douglas.kahn@fema.dhs.gov or call 301-447-7645. Also, send a courtesy copy email to the Integrated Emergency Management Branch at fema-emi-iemb@fema.dhs.gov or call 301-447-1381. Content is the same each day and participants would attend only one session. Additional information is available at https://training.fema.gov/programs/emivttx.aspx.

Each month, EMI conducts a VTTX series using a Video Teleconference (VTC) platform to reach community-based training audiences around the country by providing a virtual forum for interactive disaster training. The VTTX is designed for a group of 10 or more representatives from state, local, tribal, and territorial emergency management communities of practice. It provides a unique opportunity for responders across the Nation to simultaneously participate in a hazard-specific, facilitated discussion. Participants will need to connect via a site equipped with the appropriate VTC capability (not Adobe Connect or FaceTime-based), but alternate ways to participate are also available upon request.

~~~

Also, don't forget the EMI e-Forums! These are 1-hour, moderated, webinar discussion forums that provide an opportunity for the EMI and the emergency management community to discuss matters of interest on national preparedness training. These exchange of ideas and best practices are free of charge and available to anyone who wishes to participate. The forums are scheduled on **Wednesdays in March** from 3:00pm– 4:00pm ET.

- Login link: https://fema.connectsolutions.com/emieforums
- Conference call-in: 800-320-4330, PIN 107622

Don't forget the following resources…

- Department of Information Technology (DIT) Site: https://it.nc.gov/
- Cybersecurity and Risk Management Site: http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management
- Cybersecurity Awareness Page: https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness
- State of NC Cybersecurity Situation Report: https://it.nc.gov/cybersecurity-situation-report

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.