Monthly Cybersecurity Newsletter

September 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 Aware of Disaster Scams

Hurricane Florence has caused widespread damage throughout the state of North Carolina that will be felt for some time. To make things worse, malicious actors will take advantage of people impacted by this disaster to carry out their cybercrime schemes. State Chief Information Officer (CIO) Eric Boyette and State Chief Risk Officer Maria Thompson urge North Carolinians to be cautious of cybercrime in the aftermath of Hurricane Florence.

Cyber criminals take advantage of natural disasters such as hurricanes to solicit personal information illegally and to take advantage of vulnerable infrastructures, disaster victims, and volunteers by phishing. Phishing is when a criminal sends out an email, text message, or even a phone call pretending to be a reputable and legitimate source in order to obtain personal information such as credit card and Social Security numbers. "Be cautious and stay vigilant," said State Chief Risk Officer Maria Thompson. "*Let's ensure one disaster does not lead to another*. Phishing threats are real. Cyber criminals will use every tactic in their arsenal to deprive citizens of their information and ultimately their financial assets."

Take the following steps to prevent being taken advantage of by cybercriminals:

- Carefully look at email and web addresses since cybercriminals will make them look as legitimate as possible, often using variations of spellings. The URL may have a different domain, such as .gov instead of .net.
- Do not click on links in emails from anyone unless you know and have verified the sender of the email.
- Take time to look at the sender's email address. Do not click on any links until you are certain the organization is real. Check the organization's website for its contact information and use sites such as www.charitynavigator.org to verify a charity organization.
- Make sure all your anti-virus software is up to date and you have enabled the anti-phishing software provided by your email client.
- Phishing emails and phone calls may also try to pose as official disaster aid organizations such as FEMA. A true FEMA representative will never ask for personal banking information, a Social Security number, or a registration number.

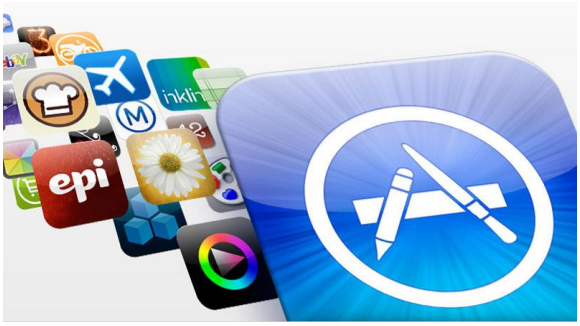
"We all need to be mindful of the value the data we have and use every day," said Eric Boyette, State CIO and Secretary of the Department of Information Technology (DIT). "Too many people

are vulnerable during natural disasters and it is imperative to take necessary precautions to protect yourself. Think of it as preparing an emergency kit for your personal data."

For more information about staying safe from cybercriminals in the aftermath of a disaster, be sure to review the cyber alert from US-CERT and the Cyber Intel Advisory from The Multi-State Information Sharing and Analysis Center (MS-ISAC) attached to the end of this newsletter.

Triangle InfoSeCon

The 14th Annual Triangle InfoSeCon will be held at the Raleigh Convention Center in Downtown Raleigh, North Carolina from 8:00 AM to 6:00 PM on **October 26, 2018**. For more information about this event, please visit http://www.triangleinfosecon.com/.

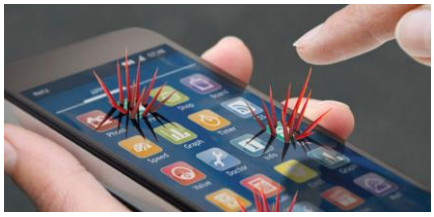


Are Your Mobile Apps Safe to Use?

Are you running applications on you mobile device that are safe to use? American technology company, Apple, recently booted several applications off of its App Store after discovering they were collecting user data. What is surprising is that some of those applications were from a *well-known* cyber security company, Trend Micro. Apple removed Trend Micro's applications Dr. Antivirus, Dr. Cleaner, and Dr. Unarchiver from the App Store after researchers discovered they were collecting data from users' browser histories and different applications stored on their machines.

Trend Micro confirmed that the apps collected and uploaded a "small snapshot of the browser history on a one-time basis" from the 24-hour period prior to installation. The company claimed this was a one-time data collection to be used to analyze whether a user had recently encountered adware or other threats. They also claim the data collected was explicitly identified to end users in the data collection policy and was highlighted to the user during the install. Trend Micro has since removed the browser history collection capability from the apps. Normally, applications from Apple's App Store are limited in the data they can access. Since the Trend Micro apps were designed to scan for security issues and to clean up devices, they need information other apps do not receive, so they request access to files on the user's system.

The fact that these applications were signed off by Trend Micro and approved for Apple's App Store should give users reason to be cautious when looking to download new software. One of the benefits of downloading apps from the Apple Store is that Apple supposedly vets all applications that are submitted to the store. Apparently, Apple does not catch all security issues from submitted apps. Fortunately, the newest version of Apple's iOS may address some issues, such as preventing apps from tracking you without your permission and preventing advertisers from collecting data on your iOS device's unique characteristics.



The following are some things you can do to minimize the risk of downloading apps:

- Be cautious about downloading applications you do not need.
- Be sure to only download applications from trusted vendors.
- Be aware of the app's data collection policy.
- Be leery of allowing permissions to any applications. Does the app really need it?
- Be certain to keep your mobile device up-to-date with the latest OS version and patches.

For more information about keeping your mobile devices secure, be sure to review the information at Stay Safe Online.

Don't forget the other **monthly newsletters** that are available to you. The following are some other cybersecurity newsletters the ESRMO recommends to you. We hope you find them beneficial.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is ***Avoiding Many Types of Malware.***

- 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 ***CEO Fraud/BEC.***

- 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://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.

Statewide 918A Contract Satisfaction Survey

The State Term Contract 918A is a convenience contract to help State of NC agencies procure security assessment services and other cybersecurity related services. Services available from the contract include, but are not limited to, the following: *risk assessments, remediation suggestions, policy development services, security consultation services, incident response services,* and *training services*. Additional information about the 918A contract may be found at the following link:

https://it.nc.gov/documents/contract-918a-security-assessment-services

The Enterprise Security and Risk Management Office (ESRMO) with the Department of Information Technology (DIT) would like to better understand each agency's experience with vendors on the 918A contract. We would also like to receive any recommendations you may have for improving the contract. A brief survey to collect your feedback is available at the following link: https://www.surveymonkey.com/r/V6SJNXX

We request you submit a separate survey response for each vendor your agency has used from STC 918A. Responses to the survey are due **October 1, 2018**. If you have any questions about the 918A contract or the customer satisfaction survey, please contact Michael McCray at michael.mccray@nc.gov. Thank you!

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: 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*

Other Upcoming Events…

September 20: FEMA's Nationwide EAS and WEA Test

September 26: National Situational Awareness Day

October 1-31: National Cyber Security Awareness Month

October 18-19: NC Cyber Awareness Stand-down

October 26: Triangle InfoSeCon

November 8: Fall Spotlight: Women in BCM Focus on Education and Safety

---

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.

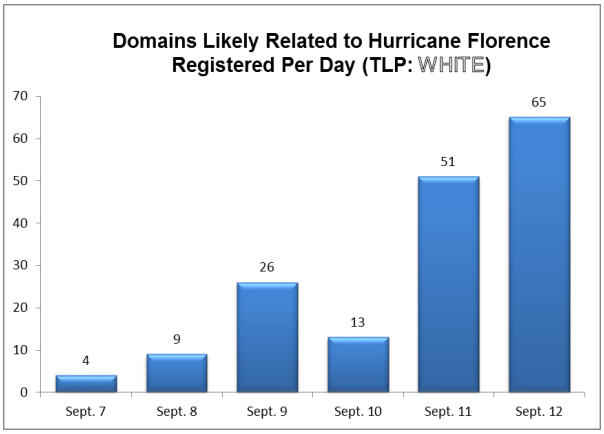
Cyber Intel Advisory
September 14, 2018 – IA2018-0338

Cyber Threat Actors Expected to Leverage Major Storms for Fraud

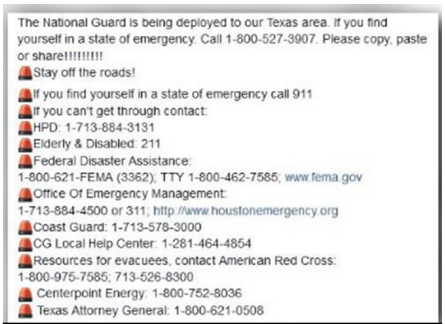
TLP: WHITE Malicious actors leverage public interest during natural disasters and other high profile events in order to conduct financial fraud and disseminate malware. The landfalls and impending landfalls of Hurricanes Florence, Isaac, and Helene, Tropical Storm Olivia, and Typhoon Mangkhut will highly likely propel the emergence of new and recycled scams involving financial fraud and malware.

TLP: WHITE Malicious actors often post links to fake charities and fraudulent websites that solicit donations for victims of the hurricane or deliver malware. The Multi-State Information Sharing and Analysis Center (MS-ISAC) previously observed similar scams and malware dissemination campaigns in response to high profile events including the Boston Marathon bombing, Hurricane Harvey, and the Tennessee wildfires. It is highly likely that more scams and malware will follow over the course of the recovery period, so Internet users need to exercise caution before opening related emails, clicking links, visiting websites, or making donations to relief efforts.

- From September 6-11, 2018, the MS-ISAC observed an increase in registered domains likely related to Hurricane Florence. The most recently registered domains include the words, “claims,” “compensation,” “lawyers,” “relief,” and “funds,” which could indicate the domains use in possible scams or other malicious activity, so they should be viewed with caution. It is likely that these domain registrations will continue, especially after Hurricane Florence makes landfall. We believe that these domain registrations will also likely occur for the other storms.



- During and after disasters, the potential of misinformation disseminated by malicious actors is high and users should verify information before reacting to posts seen on social media. Some of these posts may go viral, as did the one to the right during Hurricane Harvey, which hit Houston, Texas, in 2017. In this example, the number provided for the National Guard is incorrect and when dialed, connects to an insurance company. The insurance company corrects the misinformation and instructs the caller to contact 9-1-1.
- It is highly likely that malicious actors will also capitalize on this disaster to send phishing emails with links to malicious websites advertising relevant information, pictures, and videos, but containing phishing webpages or malware. Other phishing emails are highly likely to contain links to, or attachments with, embedded



(TLP: WHITE) Viral scam targeting Hurricane Harvey victims

malware. Victims who click on links or open malicious attachments risk compromising their computer.

USER RECOMMENDATIONS:

TLP: WHITE The MS-ISAC recommends that users adhere to the following guidelines when reacting to high profile events, including news associated with the disasters and solicitations for donations:

- Users should exercise extreme caution when responding to individual pleas for financial assistance such as those posted on social media, crowd funding websites, or in an email, even if it appears to originate from a trusted source. When making donations, users should consult the Federal Trade Commission Consumer Information website for guidance or the National Voluntary Organizations Active in Disaster website.
- Be cautious of emails or websites that claim to provide information, pictures, and videos.
- Do not open unsolicited (spam) emails or click on the links or attachments in those emails.
- Never reveal personal or financial information in an email or to an untrusted website.
- Do not go to an untrusted or unfamiliar website to view the event or information regarding it.
- Malicious websites often imitate a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs .org) so ensure the link goes to the correct website.

TECHNICAL RECOMMENDATIONS:

TLP: WHITE The MS-ISAC recommends that technical administrators adhere to the following guidelines when reacting to high profile events, including news associated with any of these disasters, and solicitations for donations:

- Issue warnings to users about potential scams, implement filters on emails, block suspicious IP addresses and domains at your firewall and on your webserver proxy, and flag emails from external sources with a warning banner
- Use antivirus programs on clients and servers, with automatic updates of signatures and software.
- Apply appropriate patches and updates immediately after appropriate testing.

More information regarding emergency preparedness for cyber infrastructure is available in the associated MS-ISAC Security Primer.

(U) TLP: WHITE The information in this document is current as of September 13, 2018. The information provided above is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. Organizations have permission and are encouraged to brand and redistribute this advisory in whole for educational, non-commercial purposes. The MS-ISAC is interested in your comments - an anonymous feedback survey is available.

Citations and more information regarding potential threats are available by contacting:

MS-ISAC
866-787-4722 · SOC@cisecurity.org