Monthly Cybersecurity Newsletter

September 2021 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Rob Main

---

Phishing Attacks Have Increased By 22% This Year

The volume of phishing attacks has increased 22% this year compared to the first half of 2020, according to researchers at PhishLabs, a cybersecurity threat intelligence company that offers anti-phishing, anti-malware, and other ecrime management services. Researchers say, "Phishing continues to be one of the top threats to enterprises with attack volume outpacing the first half of 2020 by 22%." They report that phishing is the primary way that cyber attackers use to steal credentials, hijack accounts, and compromise organizations.

While phishing continues to thrive, social media is increasingly being used for impersonation, fraud, and other cyber threats. Threats targeting enterprises via social media grew 47% in the first half of 2021, showing that to be a top threat vector. The researchers found that fraud-related attacks were the most common form of phishing on social media, while payment services and the healthcare industry were highly targeted by these attacks.

"Payment services and healthcare experienced the steepest increases in social media attacks per business in Q2," the researchers write. "Payment services, which ranked the highest of all industries, increased threat activity by over 500% when compared to Q1. Healthcare experienced the second highest increase in activity from Q1 to Q2, moving up in rank from 17th to 10th, due to a 188% increase in attacks per business in Q2."

PhishLabs also found that attacks targeting single sign-on (SSO) solutions rose by 40% in Q2 compared to Q1. The greatest risk to corporate email users, however, are credential theft phishing and response-based attacks, such as Business Email Compromise (BEC). According to PhishLabs, BEC-type attacks accounted for 96% of threats found in enterprise inboxes. Researchers say, "These threats continue to evade email security controls at a high rate."

One of the best ways to reduce the risk of these phishing attacks is to provide security awarenss training with realistic phishing emails that mimic real threats. By providing individuals the opportunity to see and respond to these types of attacks in a safe environment, it reduces the risk when a real threat occurs.

The report from PhishLabs may be found via the link below:
https://www.phishlabs.com/blog/new-quarterly-threat-trends-intelligence-report-now-available/

September is National Preparedness Month

September is National Preparedness Month. Managed by FEMA's Ready Campaign, in association with the Ad Council, the month is observed to encourage everyone to take steps to prepare for disasters that could at any time.

This year's theme, "Prepare to Protect," highlights how preparing for disasters is protecting everyone you love. Throughout the month, Ready.gov/September will feature weekly themes that highlight basic preparedness activities that every everyone can do.

For the first-time ever, National Preparedness Month will include a series of Hispanic public service advertisements (PSAs), which will be released (in English and Spanish) mid-month, near the start of Hispanic Heritage Month. The PSAs will air during the peak of the hurricane and wildfire seasons.

Encourage your friends and family to prepare for disasters and emergencies today. Together, we can prepare to protect. For free, easy to use social media content, and more information, visit Ready.gov/September.

Hurricane-Related Scams

The 2021 Atlantic hurricane season began on June 1, 2021 and will end on November 30, 2021. This is when cyber attackers take advantage of this dangerous time of year and promote malicious hurricane themed attacks.

The Cybersecurity and Infrasructure Security Agency (CISA) warns users to remain on alert for malicious cyber activity targeting potential disaster victims and charitable donors following a hurricane. Fraudulent emails, often containing malicious links or attachments, are common after major natural disasters. Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events.

To avoid becoming victims of malicious activity, users and administrators should review the following resources and take preventative measures.

- Staying Alert to Disaster-related Scams
- Before Giving to a Charity
- Staying Safe on Social Networking Sites
- Avoiding Social Engineering and Phishing Attacks
- Using Caution with Email Attachments

If you believe you have been a victim of cybercrime, file a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) at www.ic3.gov.

Wanted: Disgruntled Employees to Deploy Ransomware

Krebsonsecurity recently posted an article about a tactic to deploy ransomware using someone from ***within*** an organization they are wanting to attack. Criminal cyber attackers try many ways to infiltrate a profitable enterprise to get a good return from a ransomware infection. One tactic that is causing concern is cyber attackers contacting employees directly and asking them to help unleash malware inside their employer's network. These desperate cyber criminals offer the potential "insider threat actors" a percentage of any ransom they receive.

Cybercriminals have been known to use disgruntled employees to help them in their nefarious plans. For instance, there has been a threat of disgruntled employees creating identities on darknet sites (i.e. sites that can only be accessed with specific software, configurations, authorization and oftentimes used for both illegal and legitimate reasons), and then offering to trash their employer's network for a fee.

Several established ransomware affiliate gangs have recently started soliciting illicit access to corporate networks. For example, the Lockbit 2.0 ransomware-as-a-service gang includes a solicitation for insiders in the desktop wallpaper left behind on systems encrypted with the malware.

To read the full article, please visit the following link:
https://krebsonsecurity.com/2021/08/wanted-disgruntled-employees-to-deploy-ransomware/

FEMA Offers Exercise Assistance to Stakeholders

The Federal Emergency Management Agency (FEMA) is accepting requests for exercise support through the National Exercise Program. State, local, tribal, and territorial (SLTT) jurisdictions can request no-cost assistance for exercise design, development, conduct and evaluation to validate capabilities across all mission areas.

FEMA is hosting webinars for all interested governments and other community partners on the exercise support process. Please visit the webinar webpage to register. The webinar dates are as follows:

- Webinar 1: 1 p.m. ET on Aug. 30.
- Webinar 2: 2 p.m. ET on Sept.7.
- Webinar 3: 3 p.m. ET on Sept. 15.
- Webinar 4: 4 p.m. ET on Sept. 23.
- Webinar 5: 1 p.m. ET on Oct. 1.

Fall 2021 requests for support are due no later than November 1. To submit a request for exercise support, download the nomination form, then email the completed form with any supporting documentation to NEP@fema.dhs.gov. Awardees will be notified by December 10. FEMA will hold additional exercise support rounds in the spring and fall of 2022. For questions, contact FEMA at NEP@fema.dhs.gov

2021 N.C. Cybersecurity Awareness Symposium – October 6-7, 2021

October will be National Cybersecurity Awareness Month (NCSAM). The overarching theme will be "Do Your Part. #BeCyberSmart." This theme encourages individuals and organizations to own their role in protecting their part of cyberspace, stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity.

In support of this national campaign, the N.C. Department of Information Technology (DIT) will be hosting a two-day virtual N.C. Cybersecurity Awareness Symposium on **October 6-7, 2021**. This will be an opportunity for attendees to learn from cyber leaders and subject matter experts in the private, public and academic sectors on various topics related to maximizing cyber spend while protecting data and systems from compromise.

Triangle InfoSeCon Virtual Conference October 28-29, 2021

Triangle InfoSeCon is the largest annual Information Security conference in the Triangle area and is the flagship event of the Raleigh Chapter of the Information System Security Association (ISSA). This year's event will be **Thursday October 28** and **Friday October 29**.

The chapter holds training events during their monthly meetings and provides an annual Certified Information Systems Security Professional (CISSP) review. As an organization, they believe that Information Security is both the present and the future, and it is incumbent upon cybersecurity professionals to try to influence the decision makers of today and to train the security leaders of tomorrow. In addition to several cybersecurity presentations, the Triangle InfoSeCon event will host an IT Leadership Forum and a Capture the Flag exercise.

For more information and to register for this event, please visit here.

PCI Webinars by Coalfire

The N.C. Office of the State Controller is pleased to announce that Coalfire, a PCI compliance validation services vendor for the state of North Carolina, will be presenting the following webinars.

Date	Time	Topic (Tentative)
Sept. 7, 2021	10-11 a.m. EST	Authentication and Access Control – Who Are You?
Dec. 7, 2021	10-11 a.m. EST	Risk Assessments – Do You Feel Lucky?

Additional details, including registration information, will be sent out in advance of each webinar. To be notified, sign up for PCI webinar announcements via the eCommerce listserv, which also provides updates about products and services on the Merchant card and enhanced file transfer (EFT) master services agreements, annual PCI compliance, self-assessment questionnaires and quarterly scans.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment
  - https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service
  - https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies
  - https://niccs.cisa.gov/
- ICS-CERT Training
  - https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2021

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/security-awareness-training/ouch-newsletter

September 7: Coalfire Webinar: Authentication and Access Controlebinar: Authentication and Access Control

September 9: September Best Practice Webinar: Purdue Cyber Apprenticeship Program (PCAP)

October 6-7: 2020 N.C. Cybersecurity Awareness Symposium

October 18-22: Cyberweek

October 28-29: Triangle InfoSeCon Virtual Conference

Also, for a list of upcoming SANS webcasts, visit here.

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember… Stop. Think. Connect.*

***Disclaimer**: Vendors, references, and links in this newsletter are for informational purposes only and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*