NCDIT Cyber Symposium
Emerging Cyber Threats

LTC Seth Barun, Chief of Cyber Operations, NCNG
SPC Isaac Marshall, Penetration Testing Division, NCNG
Agenda

• JCTF Overview
• CSRF Overview
• Cyber Threats
• Prevention Steps
• Open Forum
JOINT CYBER SECURITY TASK FORCE (JCTF)
EO 254

• Formerly established the Joint Cybersecurity Task Force
• Members include:
  • NC Department of Information Technology/Enterprise Security and Risk Management Office
  • NC Division of Emergency Management
  • NC National Guard
  • NC Local Government Information Systems Association Cybersecurity Strike Team
• Partners include:
  • NC Information Sharing and Analysis Center
  • Federal Bureau of Investigation
  • United States Secret Service
  • Other federal agencies, NC state agencies, or other stakeholders as needed
NC JCTF

Upon receiving a report of a significant cyber incident, the NC JCTF will establish a scoping call with the impacted entity to address the following high-level activities:

- **Incident Response.** This includes conducting forensics to identify root-cause, damage assessment and mitigation, and coordination with law enforcement activities as needed. Lastly information sharing of indicators of compromise.

- **Recovery Response.** This effort could include establishing best practice recovery methods, system hardening, restoration of services and infrastructure rebuild.
CYBER SECURITY RESPONSE FORCE (CSRF)
Mission

Conduct Defensive Cyberspace operations to support mission requirements as directed by the TAG or Governor.

- Federal Mission: Provide Defensive Cyberspace Operations capabilities on DODIN and supporting Critical Infrastructure
- State Mission: Provide cybersecurity assistance to State, Local, and Critical Infrastructure providers
NCNG and State of NC cyber partnership

• (2013) Fully executed Network Security Support MOU between TAG and State of NC:
  - NC Chief Information Officer
  - NC Department of Public Safety
  - NC Office of Emergency Management

• Agreement sets forth framework to provide:
  - Cyber Prevention (Policy \ Standards \ Compliance Gap Analysis)
  - Cyber Assessment (Environment \ Culture \ Vulnerability Assessment)
  - Incident Response (Cyber Response Force)
  - Forensics (Cause of Attack, methodology)
NCNG CSRF - Lines of Effort

- Cyber Hygiene Assessment
- Penetration Testing
- Continuous Monitoring
- Training and Outreach
- Quick Reaction Support (Cyber QRF)
- Forensics Support and Malware Analysis

These services are offered free of charge to Critical Infrastructure Partners. That means most of you!
**Strategy - Cyber Hygiene Cycle**

- **Assessment**
  - Utilize assessment report to prioritize and address vulnerabilities
  - Determine acceptable risk levels and document risk mitigation strategy
  - Develop internal processes, policies and procedures to improve security posture
  - Conducted using industry best practices and DOD Security Technical Implementation Guidelines (STIGs)
  - Output is comprehensive report outlining vulnerabilities and recommended solutions

- **Penetration Testing**
  - Address vulnerabilities outlined in penetration testing report
  - Identify additional risk acceptance and document mitigation strategy
  - Evaluate processes, policies, and procedures to ensure comprehensive coverage
  - Leverage report to determine additional resource requirements

- **Remediation**
  - Validate the steps taken during remediation to ensure appropriate resolution
  - Identify additional areas of concern including user awareness and network monitoring capability
  - Output is comprehensive report detailing actions taken and recommended solutions

- **Remediation**
  - Utilize assessment report to prioritize and address vulnerabilities
  - Determine acceptable risk levels and document risk mitigation strategy
  - Develop internal processes, policies and procedures to improve security posture
  - Leverage report to determine additional resource requirements
CYBER THREATS
Shodan Demo

• Avenues of Attack
  • RDP
  • FTP
  • SMB
• Video Feeds
• ICS/SCATA search
Who is the Real Target?

• Targets of opportunity
• Open-source tools make finding vulnerabilities and exploits easier and easier
• Cyber gangs can be sophisticated organizations with interpreters, lawyers, and coders
• Criminal gangs use Ransomware-as-a-Service to rent software and infrastructure for attacks
• Attacks are scripted and often are “fire and forget” until they gain access
Cyber Crime Impact

- 2.4 million North Carolina residents impacted by cyber-attacks in 2021
- In the past 18 months, cyber-attacks cost NC citizens and businesses nearly $92B
- A cyberattack occurs every 39 seconds
- Over 50% of devices that got infected were re-infected in the same year
- Average Ransomware demand rose to $338,669 in 2020
- Average ransomware attack cost company $5M
- 2020 survey of 5000 IT Managers found 51% had been impacted by Ransomware
  - Criminals succeeded in encrypting data in 73% of the attacks
- On average, it takes 228 days to identify cyber breach
Cyber Threats

• Cyber crime is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them
  • Ransomware
  • Business E-mail Compromise
  • Phishing/Spoofing
  • QR Codes
Ransomware

• 39% of global data breaches caused by malware attributed to ransomware
• Malware that encrypts data or threatens to publish data unless ransom is paid
• Ransomware usually is the last step in a larger breach
  • First step is usually a credential theft process
  • Second step is to spread malware throughout network
  • Third step is to exfiltrate data/information
  • Fourth step is to encrypt systems

• Should you pay the ransom?
  • Attackers will almost always send the decryption key once they receive money
  • They still have access to the system, administrator accounts, networks
  • The only real way to ensure attackers are gone is to rebuild the systems
  • It is illegal for Government Entities in NC to pay ransomware
Ransomware

21 DAYS
Average downtime due to ransomware attacks² (Coveware)

287 DAYS
Average days it takes a business to fully recover from an attack³ (Emsisoft)

$350 MILLION
Victims paid in ransom in 2020 — a 311% increase over the prior year¹ (Chainalysis)

$312,493
The average payment in 2020 — a 171% increase compared to 2019⁵ (Palo Alto Networks)

In 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware
Ransomware in NC

• All attacks have had indicators of compromise in their logs weeks to months prior to attack
• Uptick in 3rd party or contractor account compromise
• Known vulnerabilities/end of life equipment
• Underfunded agencies usually the target
• House Bill 813 bans NC State Entities from paying ransomware
Business Email Compromise

• 65% increase in BEC losses from 2019-2021
• In a 5 year period, losses are estimated to be $43B worldwide
• In 2020, the FBI received 19,369 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints
• Carried out by large criminal organizations
• Target is finances of companies
• Scam tries to get companies to perform wire transfers using existing partnerships
• Sophisticated attacks employ lawyers, social engineers, hackers
• CEO impersonator attacks
Business Email Compromise Steps

**Step 1: Identify a Target**
Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

**Step 2: Grooming**
Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).
Perpetrators use persuasion and pressure to manipulate and exploit human nature.
Grooming may occur over a few days or weeks.

**Step 3: Exchange of Information**
The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

**Step 4: Wire Transfer**
Upon transfer, the funds are steered to a bank account controlled by the organized crime group.

---

**Business E-Mail Compromise Timeline**
An outline of how the business e-mail compromise is executed by some organized crime groups.
Archive file attached to email: form.zip
Password: EHGWOARLC

Dear Sir/Madam,

We inform you that we have a new announcement.

'Dear All Valuable Supplier, Hereby we would like to inform you that the attached file has been updated with the latest revision. Please kindly take the lesson and implement it in your company’s business activity. Thank you for your attention and cooperation.'

(Individual Announcement)

Expired: 31 Jul 2021

Please check the announcement on Announcement Link.

Thanks for your attention
Announcement Admin

The attachment named form.zip could not be scanned for viruses because it is a password protected file.
Thread Hijacking

- Uses previously compromised accounts
- Reviews correspondence to find additional email addresses
- Hackers will insert malicious links or attachments into a real email thread
- Emotet is making a comeback utilizing attachments using macros in Excel
- Drops malware for credential harvesting or ransomware
Phishing/Spoofing

- Email or instant message that tries to obtain sensitive information
- Social engineering process that can appear to be from trusted sites or senders
- Multiple types
  - Spear phishing targets specific individuals
  - Whaling targets senior executives or high-profile targets
  - Clone phishing uses a previous email to make malicious identical email
  - Link manipulation changes the URL just enough to appear legitimate
  - Website forgery uses code to appear to be the correct website
COVID Scams

- 18 million COVID-19 themed phishing emails were blocked per day
- Attacks for unemployment benefits, vaccines, at-home tests, etc
- Fake emails for Zoom and other collaboration sites

From: [Email Address]
Sent: Wednesday, December 9, 2020 2:18 PM
To: Updates@cuny.edu
Subject: Re: Covid-19 Benefits

In response to the current hardship in the community due to the COVID-19 pandemic, the City University of New York, have decided to support all Faculty & Staff to get through these hard times.

The City University of New York will award $2000 to all eligible Faculty and Staff of the CUNY public university system, as COVID-19 support, starting from today, Wednesday, December 9, 2020.

Visit the CUNY COVID-19 Benefits page and register with your information to apply for this giveaway.

Note: An ID verification is required, for your application will not be processed if your ID isn’t verified.

Sincerely,

COVID-19 support team
College of Staten Island
Financial Aid Office
2800 Victory Boulevard,
Building 35, Room 261
Staten Island, NY 10314
QR Codes

- Use of QR codes has skyrocketed since COVID
- Very easy to tamper with a code to redirect the link to a malicious site
- Stickers are easy to post over the correct QR code
- Do not download Apps from a QR code (only use the phone’s app store)
- FBI Notice in Jan 22 outlining the risks with QR codes
PREVENTION STEPS
Prevention Steps

- Employee Training
- System patching and maintenance
- Scheduled maintenance periods
- Defense in Depth
- Security Policies
- Incident Response Plan
- Use your tools correctly
Top Issues Identified

• Patch management
• Outdated/End of Life Devices
• RDP Exposure
• Insufficient Backup Procedures
• Network Segmentation Lacking
• Shared or Improper Use of Admin Accounts
• Rogue Device Detection on Wireless
• Anonymous logons
• SMBv1 enabled
• TLS certificates expired
OPEN FORUM