Cyber Security Outreach

NCNG Cyber Security Response Force

Agenda

- Security Trends
- Cyber Threats
- Cyber Incident Handling
- Open Forum

SECURITY TRENDS

Observations from recent events

- Organizations do not have an accurate network topology
  - Unknown number of devices
  - IP range and scope lacks oversite
  - Often a result of turnover and changing priorities
- Network configuration does not implement security standards
  - Network is not segmented to keep high value targets behind stronger security controls
  - Devices can talk to other devices without a business need (i.e. internal servers can reach the internet without valid need)
- Security devices are misconfigured
  - Firewalls are in place but either not configured correctly or not monitored
  - End user device security (i.e. McAfee, Symantec) not enabled or not configured

Observations from recent events

- End of life equipment/software still being utilized
  - Outdated operating systems used to support legacy software
  - Outdated or unpatched third party software
  - Old hardware that no longer meets security standards
- Security logs only extend back a short time period
  - Limited log access makes it difficult to pin down root cause analysis
  - Hard to validate if backups are safe without known entry point of attack
- Focus on availability more than security
  - Organizations that are under-staffed prioritize system up-time over security
  - Risk is often unknown or unclear to senior management
  - If security is an additional duty, it usually gets skipped due to higher priority taskings

Observations from recent events

- System patching not done regularly
  - Attacks are taking advantage of known vulnerabilities
  - Critical vulnerabilities still exist on some networks for more than two years
  - SysAdmins afraid to patch for fear of breaking systems and do not have a test environment
  - Organizations lack patching policy or vulnerability scan review
- Cloud services are not a fix-all solution
  - Organizations need to understand who has responsibility for maintenance and security implementation based on services rendered
  - Cloud environment still requires updates and patching
- Poor cyber hygiene
  - Accounts with admin privileges accessing the internet
  - Anonymous privilege accounts used by third parties/vendors
  - Regular users accessing admin credentials to run out of date applications

CYBER THREATS

```
C:\Documents and Settings\run
```

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
  - Business E-mail Compromise
  - Data Breach
  - Denial of Service
  - Malware/Scareware
  - Phishing/Spoofing
  - Ransomware

Cyber Crime Impact

- 137 million new malware samples in 2018
- Over 50% of devices that got infected were re-infected in the same year
- Cybercrime accounts for more than 50% of all crimes in the UK
- One attack every 39 seconds
- 92% of malware delivered by email
- Average ransomware attack cost company $5M
- 61% of organizations have experienced a cyber security incident
- On average, it takes 191 days to identify cyber breach

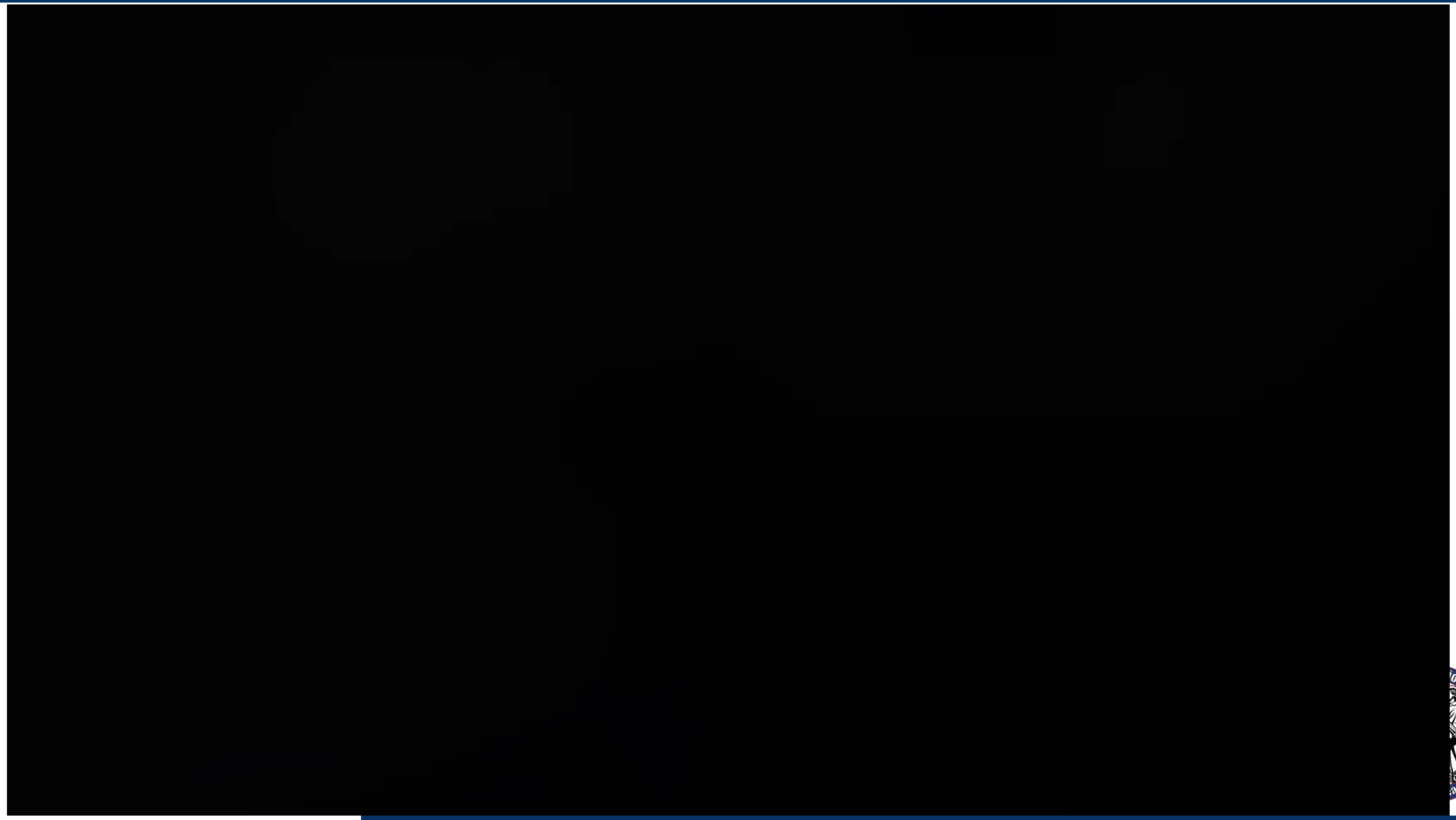
Business Email Compromise

- As of 2015, BEC losses exceed $3B
- 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
- Malware utilized through spear-phising

Business Email Compromise Steps

Business Email Compromise Prevention

- Safeguards against email only directives
- Employee training
- Intrusion detection systems on email
- Two-factor authentication for changes in payments
- Multiple verifications for wire transfers



Scoular Co

- Attack targeted company corporate controller
- Emails appeared to originate from CEO, but not from normal company email
- Emails refer to secret international deal and should be kept private to avoid SEC regulations
- Controller then received email from accounting firm with wire instructions that appeared to be from real accounting firm
- Sophisticated research done to understand corporate structure and payment patterns
- More than $17.2M wired to bank in China

Data Breach

- Incident in which information is stolen or taken from a system without authorization
- Information can be financial, personal, proprietary…
- Often results in financial loss, as well as a betrayal of trust perception
- Multiple types of data breaches
  - Hacking
  - Malware
  - Phishing
  - Insider Attack
  - Human Error

Data Breach Cycle

Data Breach Prevention

- Patch systems and networks
- Implement security standards and monitor activity
- Educate and enforce policies
- Perform regular audits and assessments
- Develop and practice disaster recovery plan

Target

- Attack started on Nov 27, 2013 and discovered on Dec 13, 2013
- 110M shoppers had information compromised
- 11GB data taken from network
- Microsoft website details Target's technical infrastructure, including POS information
- Third party vendor (Fazio Mechanical) compromised through phishing email installed malware which stole credentials
- Enterprise anti-malware would have discovered malware (Citadel), free version did not
- Web portal then compromised, alert of possible malware went unnoticed
- Servers and then POS systems compromised through multiple vulnerabilities

Denial of Service

- Attack prevents users from being able to access systems, services, devices, or network
- Most common attack is a flood of network server to the point of overload
- Distributed Denial of Service (DDOS) uses multiple machines to attack a target
  - Usually hijacked machines
  - Makes finding source very difficult
  - Can be traded between hackers

Denial of Service Prevention

- Use and maintain antivirus software
- Keep firewall updated and configured correctly
- Monitor network traffic
- Use DoS protection services
- Create and practice disaster recovery plan

Rio Olympics

- Sep 2015, multiple organizations affiliated with Olympics started receiving DDOS attacks
- LizardStresser is a DDOS-for-hire service that previously took down Xbox Live and Sony Playstation networks
- Utilized botnets to send up to 540Gbps attacks to flood network
- Arbor Networks had done network baselines and understood traffic prior to attacks
- Knowledge allowed them to mitigate attacks

Malware/Scareware

- Malware is short for malicious software
- Designed to gain access to or damage a computer
- Multiple types
  - Spyware-monitor activities
  - Viruses-usually harmful activities such as data destruction
  - Backdoors-allows for unauthorized access to systems
  - Trojan horse-hidden software that looks normal that can be destructive or provide access
  - Adware-installs forced advertising or additional browsers
- Scareware tries to trick you into buying fake or unnecessary software such as antivirus which will then install additional malware

Malware Prevention

- Anti-virus software is critical
- Keep anti-virus updated
- Ensure browser is updates
- Be conscious of emails with attachments or links
- Keep computer updated
- Don’t plug unknown devices into computer

Stuxnet

- Worm that targeted Programmable Logic Controllers built by Siemens
- Iran used the PCLs in their nuclear centrifuges
- Worm designed to speed up centrifuges past tolerance, causing them to shatter
- Worm had three parts
  - Execute payload
  - Spread the worm
  - Hide all evidence
- Introduced via USB to bridge Air Gap
- Accidentally spread outside of Natanz facilities

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

Phishing Prevention

- **User training**
- Spam filter rules
- Safe browsing services
- Multi-factor authentication

Operation Phish Phry

- Egyptians set up phishing scam that sent emails to people getting them to log into their bank accounts
- The link in the email went to a fake site that stole the credentials
- Only used banks that did not have two-factor authentication
- Egyptians sent credentials to criminals in California, who opened bank accounts at the same institutions, then transferred money from the compromised accounts
- Money then wired to Egypt
- Involved more than 100 people and $1.5M

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 malware
  - Second step is to spread malware throughout network
  - Third step is to steal 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 was to ensure attackers are gone is to rebuild the systems

Ransomware Prevention

- Employee training
- Keep your systems patched and updated
- Segment the network
- Enforce smart security policies
- Pay attention to system logs and network traffic
- Use proper backup procedures, including validation and keeping them offsite

Baltimore

- Ransomware victim that will cost more than $18M
- RobbinHood variant of ransomware, same used in Greenville, NC
- Hackers asked for $76,280 which city refused to pay
- Second attack in two years
- Speculation around how attack happened either exploited unpatched server or phishing email
- EternalBlue is suspected to have been used in attack in some way


NBC NEWS

Unnamed Agency

- Agency noticed unusual activity from an administrator account
- Agency tried to isolate activity of user
- When specific unknown IP addresses were identified, they were blocked at the firewall
- Blocking the beaconing triggered the encryption protocol which then encrypted their entire infrastructure, including backups
- Agency then received popup message on systems with two email addresses
- Agency breach traced back to administrator allowing user access to admin credentials to run application
- Breach traced back at least four weeks prior to encryption

Prevention Trends

- Employee Training
- System patching and maintenance
- Security Policies
- Incident Response Plan
- Use your tools correctly

OPEN FORUM