NC Cybersecurity Awareness Symposium Emerging Cybersecurity Threats

LTC Seth Barun, Chief of Cyber Operations, NCNG

Agenda

- JCTF Overview
- CSRF Overview
- Cyber Threats
- Prevention Steps
- Open Forum

JOINT CYBER SECURITY TASK FORCE (JCTF)

NC JCTF

- State's Cyber Quick Reaction Force
- Scalable depending on mission
- Partnership between state and federal agencies
- Can be activated with a phone call
- Previous missions include Ransomware Attacks, Business Email Compromise, Stolen Credentials, Malware Analysis, etc.

North Carolina Joint Cyber Security Task Force is composed of:

NCNG
NCLGISA Strike Team
NC DIT
FBI

Fusion Center
NCEM ESF2
CISA

Other Partners:
911, NC SBI, SBE, DHHS, DPI, MCNC, NC Community College System, Vendors

CYBER SECURITY RESPONSE FORCE (CSRF)

Mission

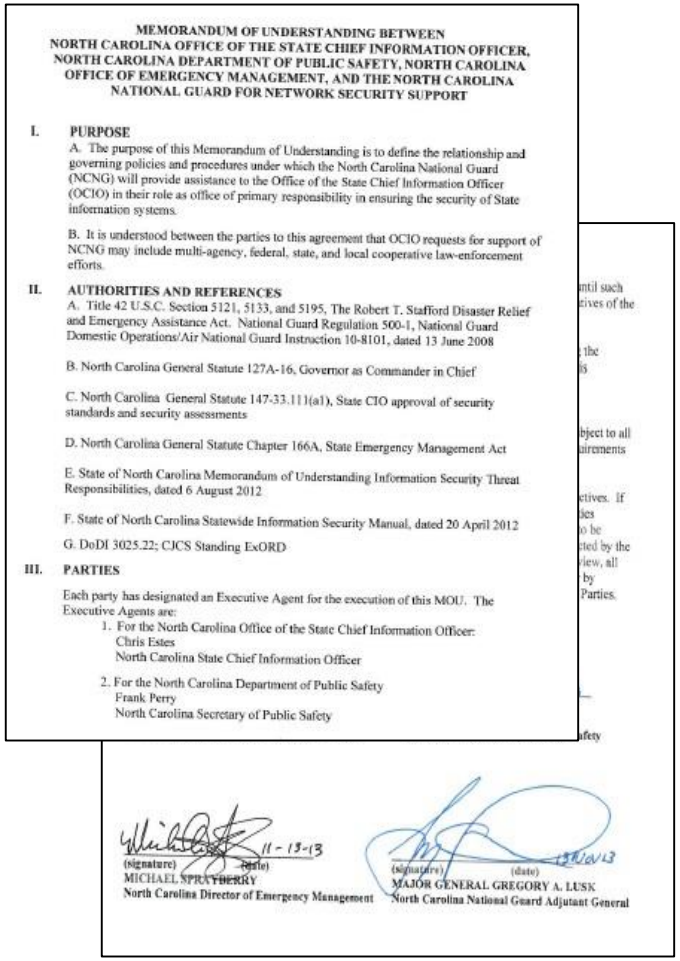
Conduct Defensive Cyberspace operations to support mission requirements as directed by the TAG or Governor.

- 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)



MEMORANDUM OF UNDERSTANDING BETWEEN
NORTH CAROLINA OFFICE OF THE STATE CHIEF INFORMATION OFFICER, NORTH CAROLINA DEPARTMENT OF PUBLIC SAFETY, NORTH CAROLINA OFFICE OF EMERGENCY MANAGEMENT, AND THE NORTH CAROLINA NATIONAL GUARD FOR NETWORK SECURITY SUPPORT

I. PURPOSE

A. The purpose of this Memorandum of Understanding is to define the relationship and governing policies and procedures under which the North Carolina National Guard (NCNG) will provide assistance to the Office of the State Chief Information Officer (OCIO) in their role as office of primary responsibility in ensuring the security of State information systems.

B. It is understood between the parties to this agreement that OCIO requests for support of NCNG may include multi-agency, federal, state, and local cooperative law-enforcement efforts.

II. AUTHORITIES AND REFERENCES

A. Title 42 U.S.C. Section 5121, 5133, and 5195, The Robert T. Stafford Disaster Relief and Emergency Assistance Act. National Guard Regulation 500-1, National Guard Domestic Operations/Air National Guard Instruction 10-8101, dated 13 June 2008

B. North Carolina General Statute 127A-16, Governor as Commander in Chief

C. North Carolina General Statute 147-33.111(a1), State CIO approval of security standards and security assessments

D. North Carolina General Statute Chapter 166A, State Emergency Management Act

E. State of North Carolina Memorandum of Understanding Information Security Threat Responsibilities, dated 6 August 2012

F. State of North Carolina Statewide Information Security Manual, dated 20 April 2012

G. DoDI 3025.22; CJCS Standing ExORD

III. PARTIES

Each party has designated an Executive Agent for the execution of this MOU. The Executive Agents are:

1. For the North Carolina Office of the State Chief Information Officer:
   Chris Estes
   North Carolina State Chief Information Officer
2. For the North Carolina Department of Public Safety
   Frank Perry
   North Carolina Secretary of Public Safety

11-13-13
(signature) (date)
MICHAEL SPRATHERLY
North Carolina Director of Emergency Management

(signature) (date)
MAJOR GENERAL GREGORY A. LUSK
North Carolina National Guard Adjutant General

NCNG CSRF - Lines of Effort

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

These services are offered free of charge to Critical Infrastructure Partners. That means most of you!

Contact information for CSRF

Deliverables

- Non-disclosure agreements prior to start of on-site assessments
- Statement of work signed prior to start of on-site assessments
- Periodic written and/or verbal status updates
- Assessment presentation
- Executive level report with summarized results
- Detailed technical report with specific findings and recommendations
- Detailed training curriculum and objectives

Outreach

- Monthly training focused on current security trends
- Quarterly table top exercises
- Expanding publically available information sharing capabilities and resources

Threat Environment

The frequency and severity of cyber threats are growing at an alarming rate.

The barrier to entry into cyberspace for cyber-crime, espionage, and attack is low, incentives high, and vulnerabilities abundant.

Vulnerabilities are often related to outdated software or misconfigured networks threaten vectors against the confidentiality, integrity, and availability of critical systems throughout the United States.

1636 Gold Star Drive,
Raleigh, NC 27607
Phone: 984-664-7687

North Carolina Assessment and Assistance Team (NCAAT)

North Carolina National Guard
Ready Reliable Responsive
Relevant Since 1663
Always Ready - Ready Team

North Carolina National Guard

Ready
Reliable
Responsive
Relevant
at Home and Abroad

CSRF Accomplishments

CSRF has validated NCNG's ability to support cyber force infrastructure.

- 10 full-time cyber specialists at Joint Force Headquarters.
- Over 400 Army and Air cyber specialists available for immediate state duty.
- Since 2018, 75 cyber missions executed supporting state, federal and industry partners.
- North Carolina's IT industry feeds qualified and experienced cyber specialists to the NCNG.

Threat Environment

The frequency and severity of cyber threats are growing at an alarming rate.

The barrier to entry into cyberspace for cyber-crime, espionage, and attack is low, incentives high, and vulnerabilities abundant.

Vulnerabilities are often related to outdated software or misconfigured networks threaten vectors against the confidentiality, integrity, and availability of critical systems throughout the United States.

1636 Gold Star Drive,
Raleigh, NC 27607
Phone: 984-664-7687

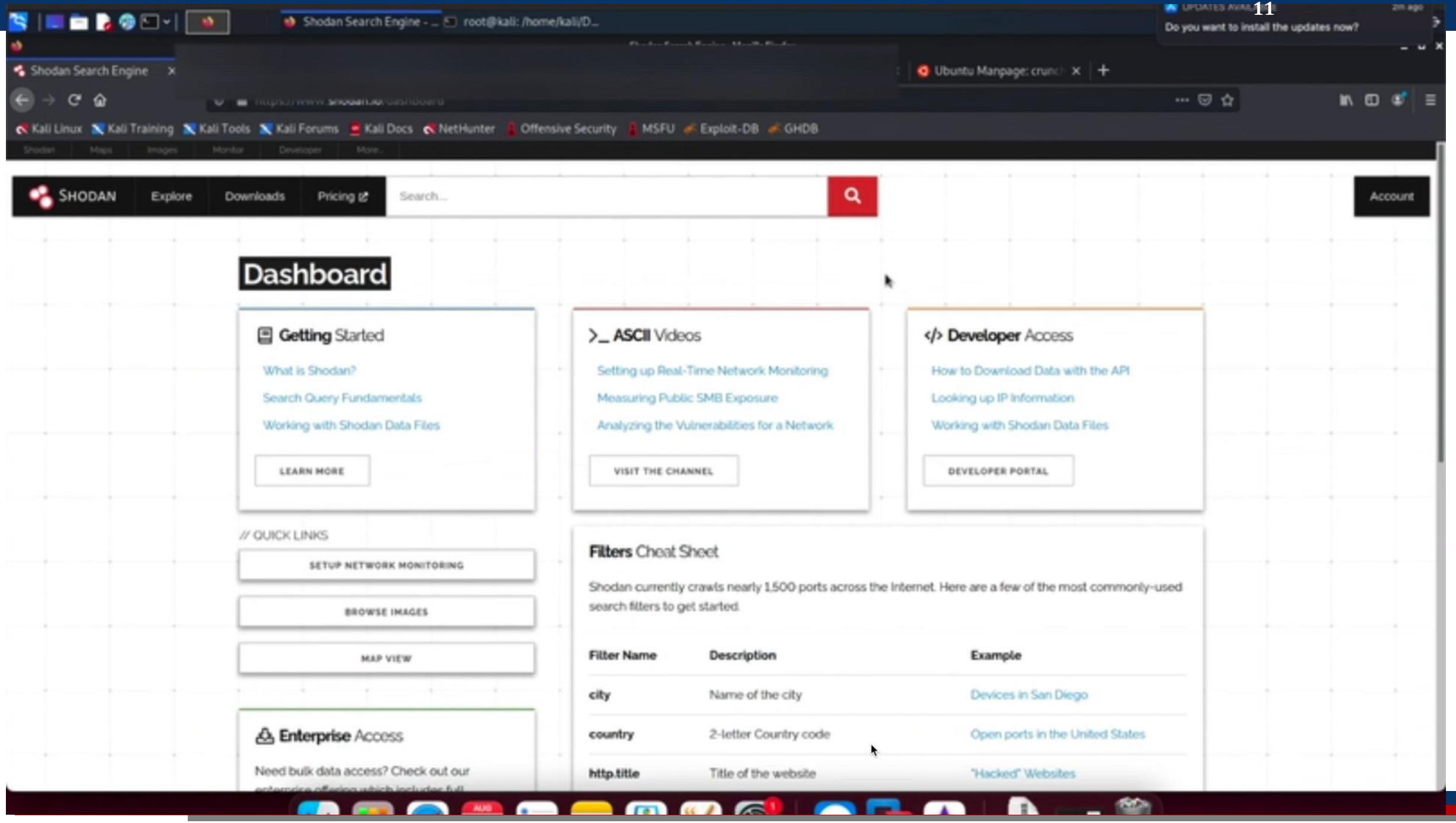
Cyber Security Response Force (CSRF)

North Carolina National Guard
Ready Reliable Responsive
Relevant Since 1663
Always Ready - Ready Team

North Carolina National Guard

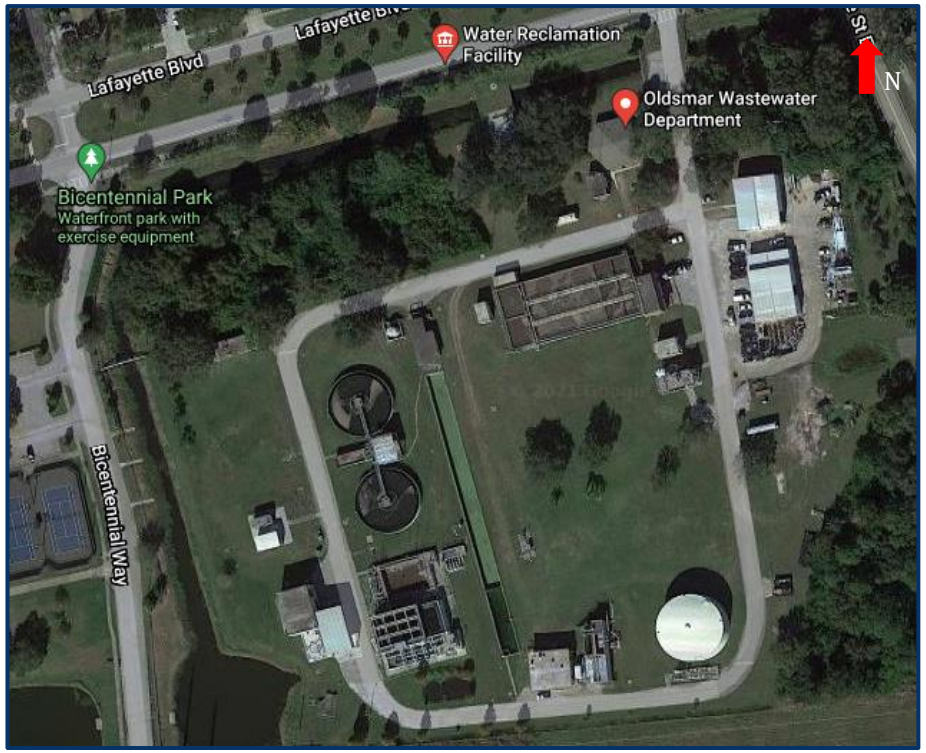
Ready
Reliable
Responsive
Relevant
at Home and Abroad

CYBER THREATS


Shodan Search Engine - _ root@kali: /home/kali/D...
Do you want to install the updates now?
Shodan Search Engine
Ubuntu Manpage: crunch
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
SHODAN Explore Downloads Pricing Search... Account
Dashboard
Getting Started
What is Shodan?
Search Query Fundamentals
Working with Shodan Data Files
LEARN MORE
>_ ASCII Videos
Setting up Real-Time Network Monitoring
Measuring Public SMB Exposure
Analyzing the Vulnerabilities for a Network
VISIT THE CHANNEL
</> Developer Access
How to Download Data with the API
Looking up IP Information
Working with Shodan Data Files
DEVELOPER PORTAL
// QUICK LINKS
SETUP NETWORK MONITORING
BROWSE IMAGES
MAP VIEW
Enterprise Access
Need bulk data access? Check out our
Filters Cheat Sheet
Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.
Filter Name Description Example
city Name of the city Devices in San Diego
country 2-letter Country code Open ports in the United States
http.title Title of the website "Hacked" Websites

Oldsmar, FL Water Treatment Facility Compromise

- Attacker gained remote access to a computer that controlled equipment inside facility
- Attacker changed the level of sodium hydroxide (lye) in the water from 100 parts per million to 11,100 parts per million on 05 FEB 2021
- Facility used Windows 7 for remote access to SCADA systems (Win 7 stopped being updated Jan 2020)
- Shared password for all computers and TeamViewer
- No firewall on computer allowed access from anywhere
- Noticed attack when mouse started moving without being controlled



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

- The FBI received 791,790 cyber crime complaints in 2020
- FBI reports American losses in 2020 exceeding $4.1 billion
- 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

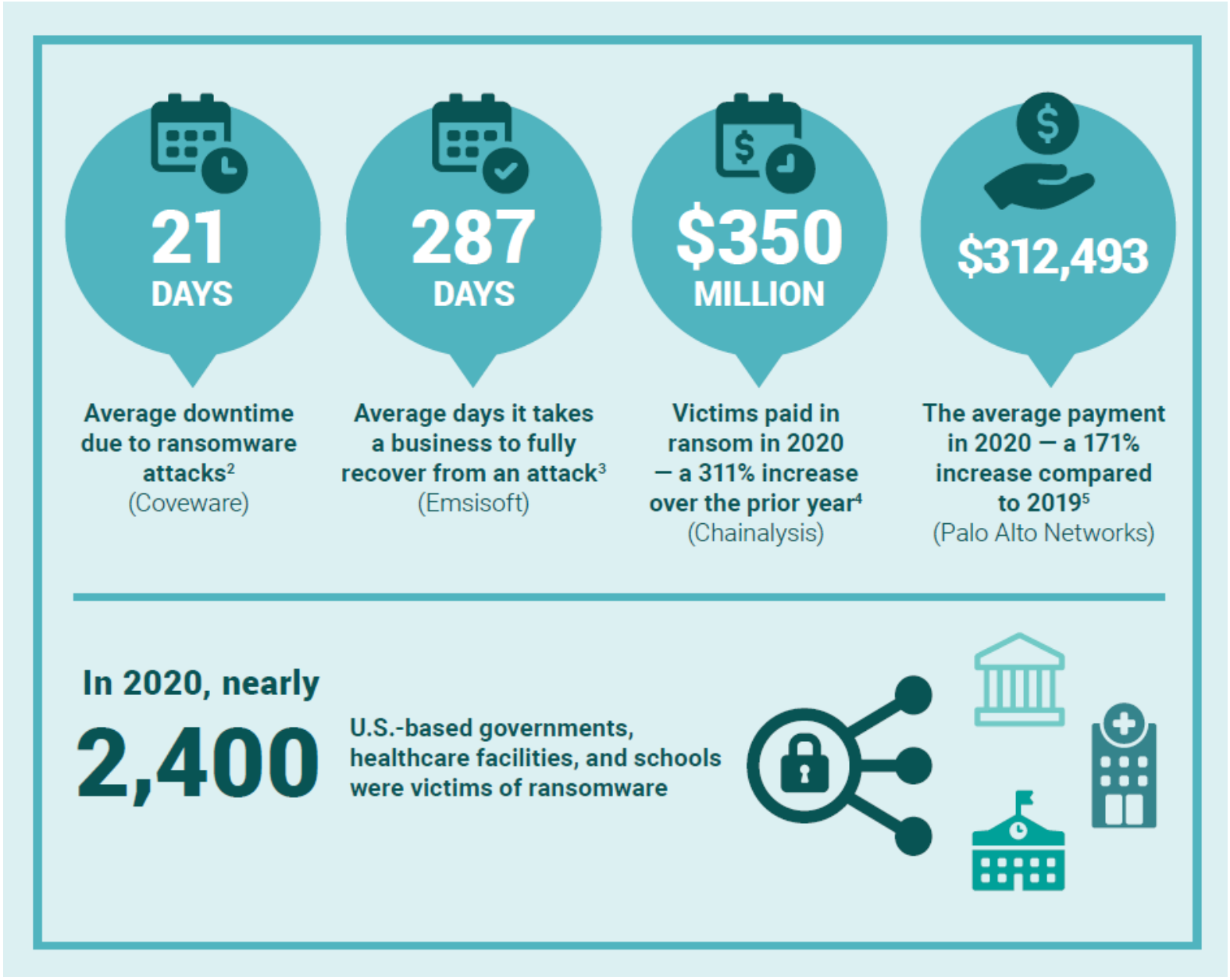
Cyber Threats

- 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
  - Denial of Service
  - Malware/Scareware

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 was to ensure attackers are gone is to rebuild the systems

Ransomware


21
DAYS
Average downtime due to ransomware attacks[2]
(Coveware)
287
DAYS
Average days it takes a business to fully recover from an attack[3]
(Emsisoft)
$350
MILLION
Victims paid in ransom in 2020 — a 311% increase over the prior year[4]
(Chainalysis)
$312,493
The average payment in 2020 — a 171% increase compared to 2019[5]
(Palo Alto Networks)
In 2020, nearly
2,400
U.S.-based governments, healthcare facilities, and schools were victims of ransomware

Agency X

Assessment and Monitoring

Identified Cyber Vulnerabilities

- Bad logon attempts configuration
- Remote Desktop Protocol (RDP) being enabled
- Use of outdated/insecure protocols
- Use of end-of-life technologies
- Vulnerability/patch management concerns

Incident

2021 – Phobos Ransomware Attack

- 30,000 Brute force RDP attempts by malicious actors over two days
- Malicious actors completed lateral movement throughout the network utilizing RDP
- Attackers obtained access to an End-Of-Life Server 2003 R2 machine
- Machine had service pack 2 out of 4 installed

Impact

- Unmitigated identified vulnerabilities resulted in successful ransomware attack on county
- Average ransom demand $338,669
- Average cost of remediation is $622,596.18.

Ransomware impacts to ONWASA

- Ransomware attack impacted all digital operations for a Water Utility
- Utility spent approximately $277,000 on recovery following the incident
- Utility had to operated all systems manually
- Email service was interrupted
- Interruption to service orders and transition to all manual work orders

Business Email Compromise

- 2020 BEC losses exceed $1.8B
- 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
- Malware utilized through spear-phishing

Business Email Compromise Steps

Unnamed NC County

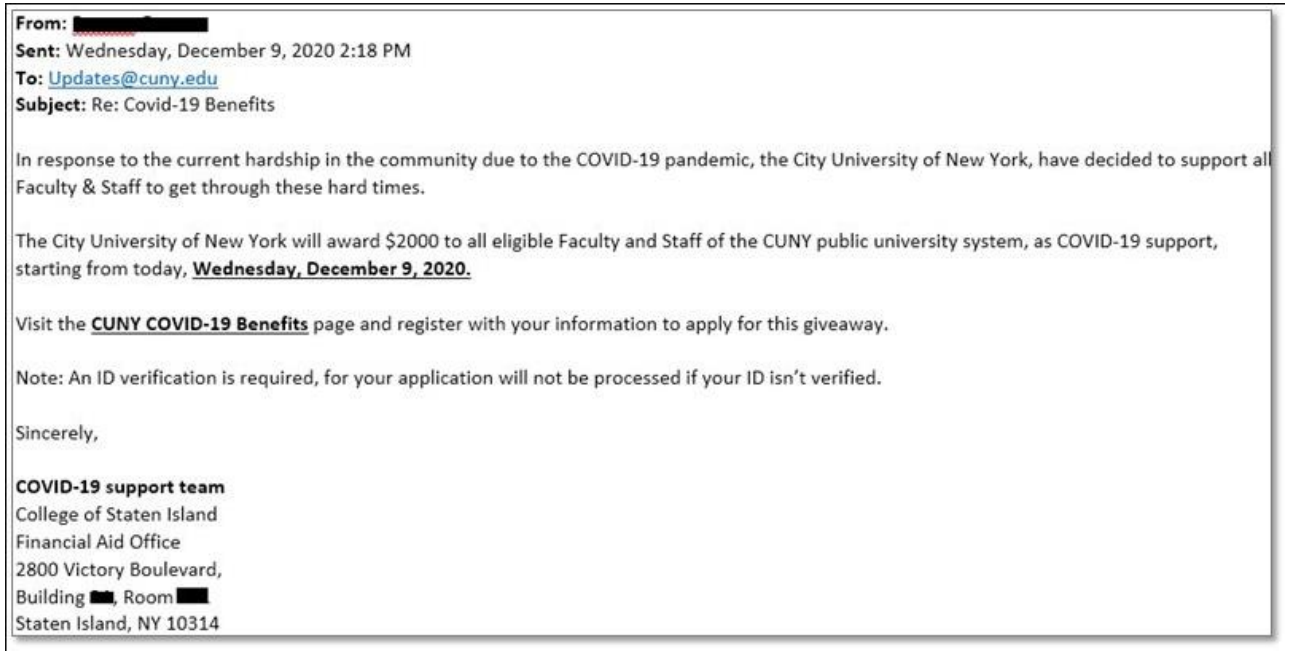
- County was working with a real vendor for road repairs
- County was communicating and sending invoices to real email address (i.e. jim@wolfpackpaving.com)
- At some point in the transaction, a new email appears for jim@wolfpackspaving.com
- New bank details and ACH transfer routing were sent to county from that email
- More than $200k was sent to the cyber criminal's account
- Only discovered when real vendor called about unpaid invoices

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: [redacted]
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,

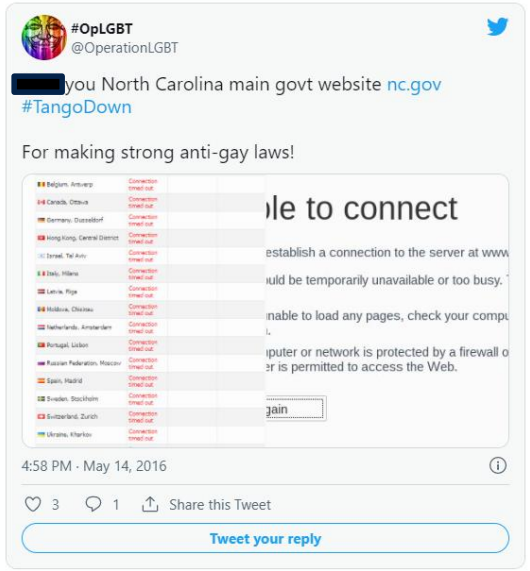
COVID-19 support team
College of Staten Island
Financial Aid Office
2800 Victory Boulevard,
Building [redacted], Room [redacted]
Staten Island, NY 10314

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
- DDOS increased as COVID 19 forced more people online
- 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
  - 12.5 million variations of DDOS attacks on the web

Anonymous attack North Carolina

- In response to House Bill 2, the hacktivist group Anonymous targeted NC government domains
- Main target was governor Pat McCrory
- Goal was to disrupt traffic to NC government sites



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

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

PREVENTION STEPS

Prevention Steps

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

Common Vulnerabilities and best practices to remediate the vulnerabilities
North Carolina Joint Cyber Security Task Force

Vulnerability	Risk Assumed	Mitigation Measures
Insecure Network Design / vulnerable LEGACY equipment.	When a network is compromised a threat actor has access to compromise all network resources.	Implement network segmentation and enforce network topology changes to include a Demilitarized Zone (DMZ) and a layered defense model.
Insecure Remote Desktop Protocol (RDP) practices	Exposed RDP can allow a threat actor initial access to an organization's network	Place a limit on failed password attempts; limit access to RDP.
Unpatched Network Devices	Cyber Criminals scan for unpatched network devices with known vulnerabilities to target.	Apply aggressive patching methodologies to protect SLTT infrastructure.
Lack of offsite "air-gapped" back ups IAW security baseline and NIST SP 800-53.	Cyber Criminals target backups for encryption in ransomware attacks. If backups are connected to a network they are vulnerable	Maintain offsite backups that can be used in your business continuity plan.
Lack of 802.1x Network Port Control Solution	Devices not managed by the organization can join the network and gain unauthorized access or introduce malicious code to the network	Enable this port control solution for network devices.
Anonymous enumeration of shares must be restricted.	Allowing anonymous logon users (null session connections) to list all account names and enumerate all shared resources can provide a map of potential points to attack the system.	Disable this functionality for all managed assets.
Critical Assets such as domain controllers must be blocked from direct internet access	Domain controllers provide access to highly privileged areas of a domain. Such systems with Internet access may be exposed to numerous attacks and compromise the domain. Restricting Internet access for domain controllers will aid in protecting these privileged areas from being compromised.	Adjust system architecture and implement industry best practices.
The default AutoRun behavior must be configured to prevent AutoRun commands.	Allowing Autorun commands to execute may introduce malicious code to a system. Configuring this setting prevents Autorun commands from executing.	Disable this functionality for all managed assets.
AutoPlay must be disabled for all drives.	Allowing AutoPlay to execute may introduce malicious code to a system.	Disable this functionality for all managed assets.
The Windows Installer Always install with elevated privileges must be disabled.	Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.	Disable this functionality for all managed assets.
The use of default or shared administrator accounts	When ever users share accounts or use administrator accounts for routine uses they risk those credentials being compromised. It also limits network defender's ability to conduct investigations	Disable accounts no longer in use; use unique administrative accounts and unique user accounts for each individual.

OPEN FORUM