North Carolina National Guard

Cyber Security Response Force(CSRF)

IA/IT Professional Training Series
Phishing – Ransomware Table Top Exercise

September 2020

This table top exercise is not classified or Law Enforcement Sensitive (LES). All materials came from open source (publically available) materials

ng.nc.ncarng.mbx.g6-ncat@mail.mil

AGENDA

- Introductions
- Ground Rules
- Recent high profile ransomware attacks
- Table Top Scenario and Injects
- Questions

- Additional ransomware information (read at your leisure)

Introduction

This Table Top exercise is designed for Information Assurance or Information technology (IA/IT) professionals. Personnel in roles that defend, maintain, train or plan for secure operations and defense of their agencies’ IA/IT posture may benefit from this presentation.

Protecting your organization from ransomware is vital to maintaining secure operations and sustaining credibility, within and external to, your organization.

ASSUMPTIONS AND ARTIFICIALITIES

- This exercise will be conducted in a no-fault, non-attribution environment.
- Evaluate existing plans, policies, and procedures from your agency as if this were a real-world emergency.
- Earnest effort has been made to create a plausible and realistic scenario.
- In general, this scenario response follows the technical Cyber Incident Response phases described in the State Significant Cyber Incident Response Plan [12]
    - (Preparation, Detection & Analysis, Containment, Eradication, Recovery, Lessons Learned)
- The exercise is not to be viewed as an assessment of individual performance.
- There is no hidden agenda and there are no trick questions.

Table Top Exercise – Ground Rules

Do not critique the scenario. Trying to find holes in the scenario is counter-productive.

Do draw from your previous experience. Utilize your knowledge of how the Whole Community works together in response and recovery situations

Do NOT assume information. If questions arise, please ask the facilitator

Participation is encouraged. Speak freely, respect others when they are speaking

This is intended to enhance your ability to: classify incidents based on impact and scope, notify the appropriate individuals, collect artifacts, escalate the event when necessary, and respond from both a technical and organizational perspective.

We will focus more on process, and less on tactical techniques and technical solutions

The facilitator may ask you to drop " the squeaky toy" to keep the event moving

Recent high profile (known) ransomware attacks

3/20 Durham, NC a suspected Ryuk style attack impacts city and county services

1/20 Albany NY Airport pays ‘< 6 figures’ ransom to Sodinokibi. Fired IT svcs provider

7/19: Lake City, Fla. pays $500k ransom

5/19: Riviera Beach, Fla pays approx. $600k ransom

5/19: Baltimore city services disrupted over 6 weeks while fighting ransomware

4/19 Greenville, NC city services down for weeks from a Robbinhood attack

4/19: Cleveland Hopkins Int’l Airport mitigated an attack impacting email & signage

4/19: Augusta, Maine, city services down 2 days while re-imaging and restoring data

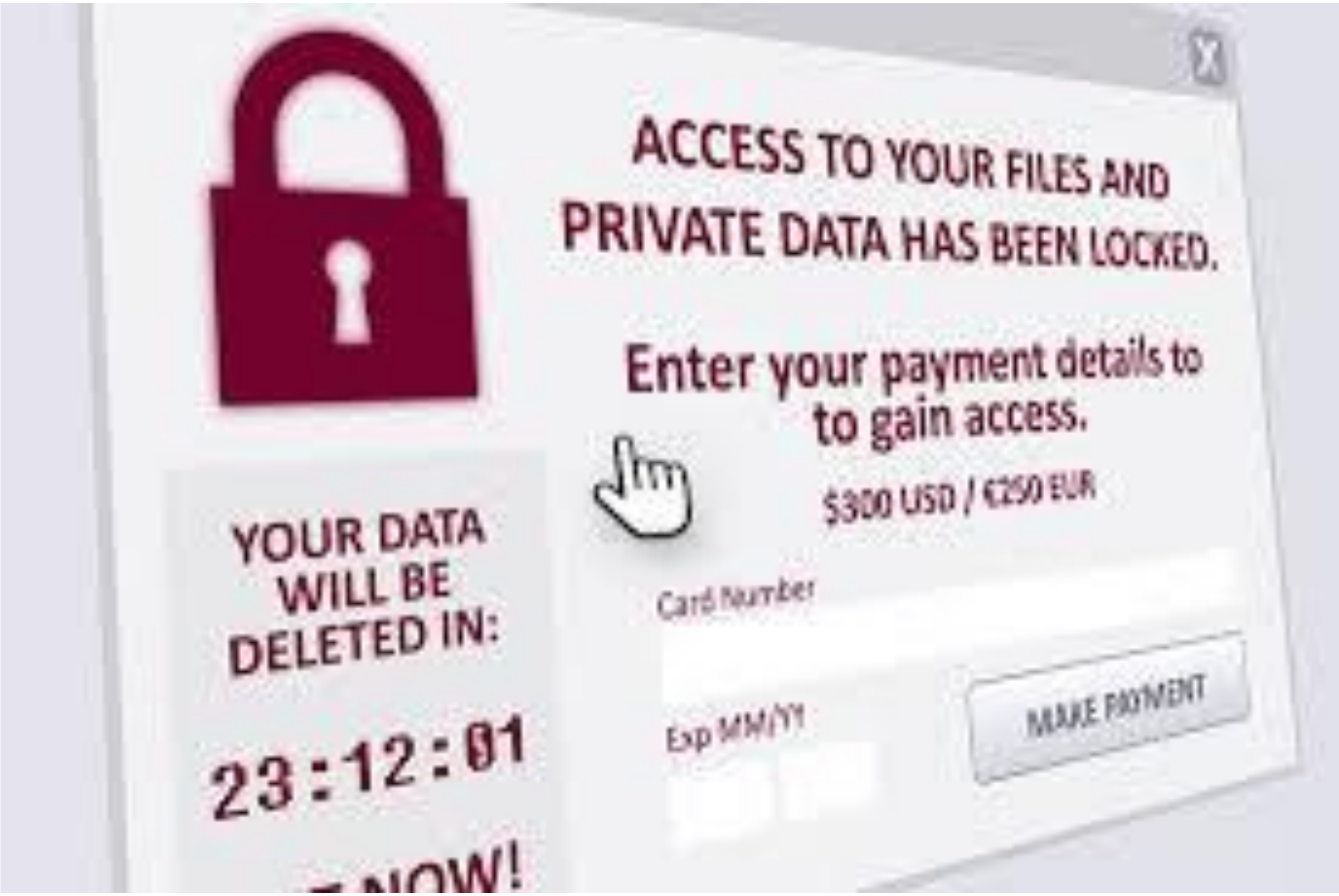
3/19: Albany, New York, avoids paying ransom by having strong backup-restore plans

3/19: Jackson County, Ga. paid $400k to regain network access from a Ryuk attack

3/19: Orange Co, NC Sheriff and county services impacted from ransomware

3/18: Atlanta, Georgia hit with SamSam. No ransom paid, rebuild costs estimated at $17 million[11, 13]

Table Top Scenario



ACCESS TO YOUR FILES AND PRIVATE DATA HAS BEEN LOCKED.

Enter your payment details to to gain access.

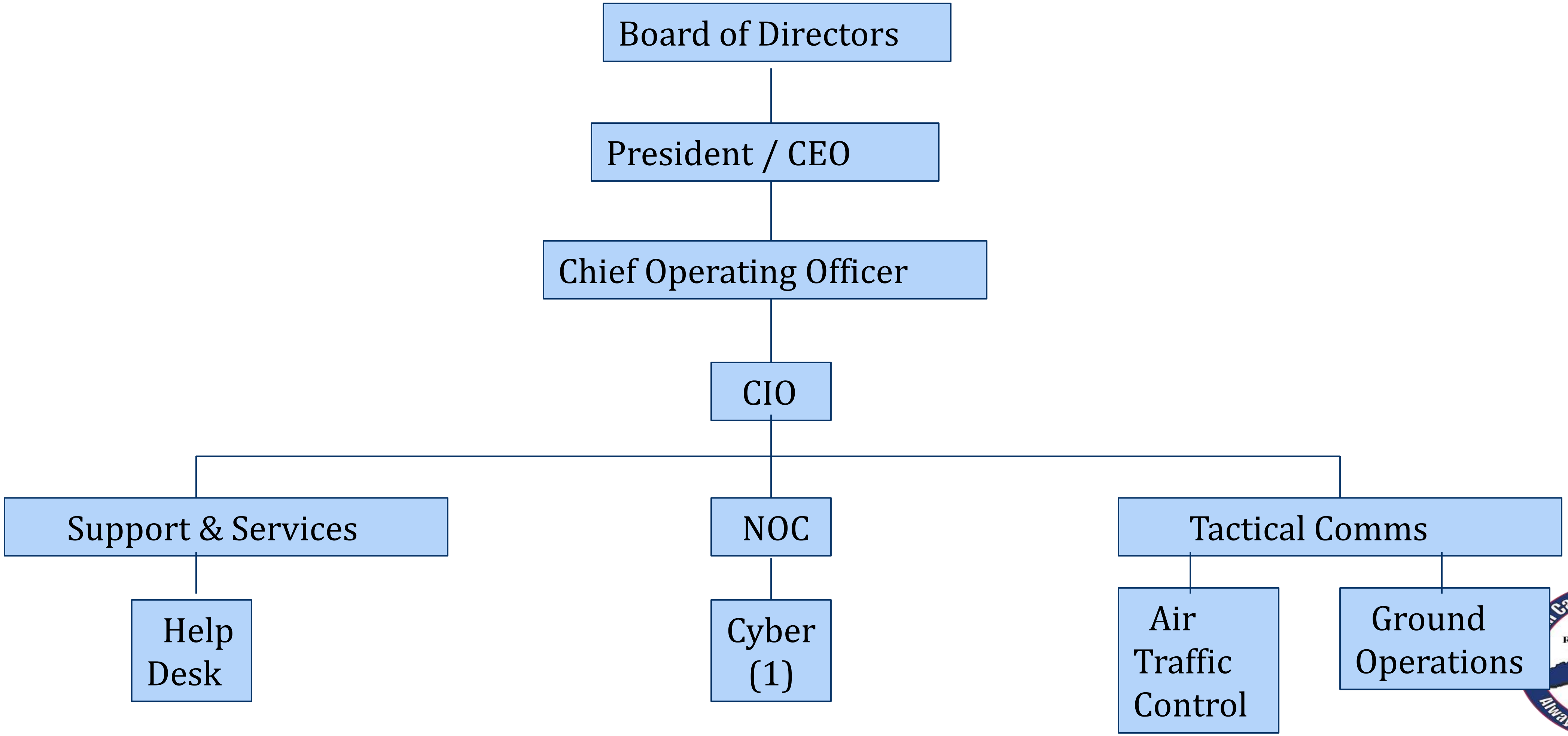
$300 USD / €250 EUR

YOUR DATA WILL BE DELETED IN:

23:12:01

NOW!

Dean Smith Airport Organizational Structure



Board of Directors

President / CEO

Chief Operating Officer

CIO

Support & Services

Help Desk

NOC

Cyber (1)

Tactical Comms

Air Traffic Control

Ground Operations

A typical day in Accounts Payable….

Tuesday, 9:15 a.m. Kim, a Dean Smith Airport accounts payable employee, opens an email from “HR” directing her to update her W4 withholding form. “Ensuring employees qualify for new federal COVID19 stimulus cheques” was the reason provided for updating it immediately. A link to her W4 is provided, with a caption stating “update and return to HR Today”.

She clicks the link, and a message appears saying she needs to authenticate her identity, with boxes for her username, and password. She enters both, and sees a spinning blue circle for several seconds, followed by this message: **SERVER ERROR: The server encountered an error and could not complete your request. If the problem persists, please try again.** Kim shrugs and mutters ‘buncha idiots’ to herself, and returns to reconciling invoices. “I guess I’ll get an updated email when they fix it”.

Discussion

What are tips or signs this might not be legitimate?

What should the employee have done upon reading this email?

Where is the scenario in the NIST 7 phases of a cyber attack? [15]

(Recon, Weaponize, Deliver, Install, Exploit, Command and Control, Act on Objective)

What is the hacker or malware possibly doing now?

Detection – sort of……

Thurs, 7:30 a.m. Sam, an intern in the SOC team, is casually scrolling through IDS logs. He is supposed to ‘roll the logs’ every morning, but in reality it gets done about twice a week. The last time anyone looked at alarms and events was last Friday, nearly a week ago. “Holy crap, what is that!” Two solid pages of email traffic, starting Tuesday at 5:01 am, paint the screen. “Where is all this email coming from at once?” he muses. Just then his cell phone rings, and he sees his girlfriends number displayed. Grinning, he spins in his chair and chats for 10 minutes or so. Realizing he is about to be late, again, for the 8am staff call, he hangs up and sprints upstairs, two steps at a time, logs and emails forgotten.

Detection

Friday, 9:02 p.m. Phil is having a great night. He’s the only help desk tech on duty, and there have hardly been any calls since he came in at 5. The phone rings. “I can’t hit flight status pages on the operations website, and I was just on it before supper. Now I’m getting a 404 page not found error message”.
Phil puts the caller on hold to check the url, and another call comes in. “My ‘Z’ drive is not found, I was in it all day. I need to send an fuel forecast in by tomorrow, can you get me in there, man?” And the phone rings again. “It looks like the concourse flight arrival and departure signs are not updating, can you get them moving again?”

Phil gets the same result when he hits the flight status url. He does not have access to the digital signage suite, but the network bandwidth monitoring appliance is showing significantly lower network traffic in the concourse network segments. He texts the help desk manager, Lisa, and asks “is there maintenance going on tonight that’s not on the schedule?

Friday, 9:29 p.m.

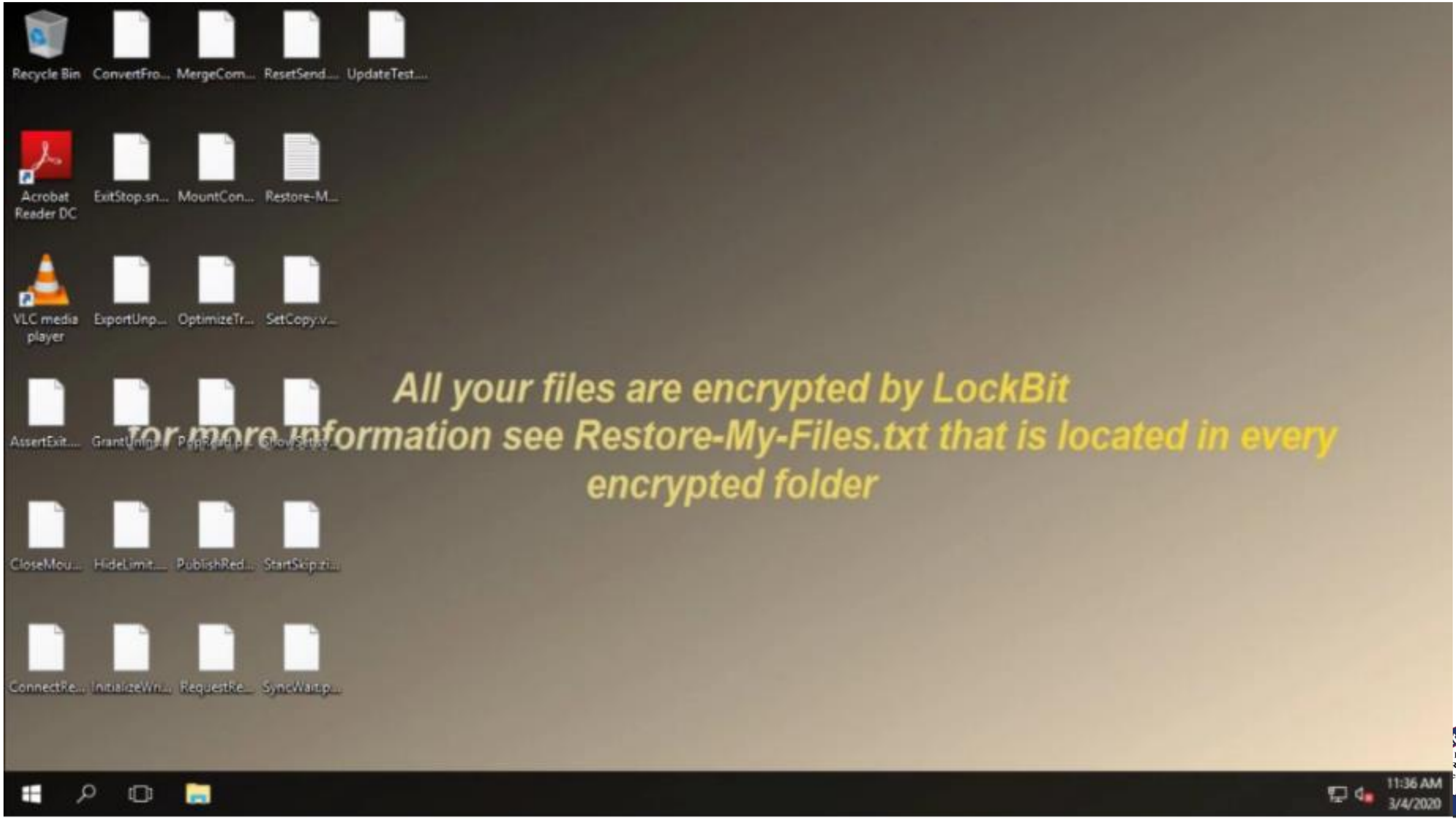
Lisa's phone chimes, a text from one of her help desk techs. "I'm seeing weird stuff going on – is NOC doing unscheduled network maintenance"?

After a brief discussion, Lisa agrees something strange is happening. There is no weekend maintenance. She tries to remote in and look around. Lisa gets an '**Unable to complete this request, try again**' error three times in a row. She calls her boss, Sue, the Support and Services supervisor. After listening for a few minutes, Sue puts Phil and Lisa on hold and conferences in Earl, the NOC chief. In less than a minute, Earl has a bad feeling. "Something ain't right. You all hang on, I'm pulling Lori into the call."

Lori, airport CIO, agrees, something is wrong. She talks quickly through a mental checklist of possible explanations, all quickly rejected by her staff. "OK, team, what do you all recommend we do now?"

As the group talks through who is available to go in and see firsthand what is happening, Phil loudly interrupts:

"I just got a call from the weather lady in the control tower, she tried logging in, and got this on the screen":



All your files are encrypted by LockBit
for more information see Restore-My-Files.txt that is located in every encrypted folder

Friday, 10:14 p.m.

Lori calmly says “Ok people, I need everyone in the conference room ASAP. Come as you are, be prepared to stay a while. Have good recommendations ready for review ”

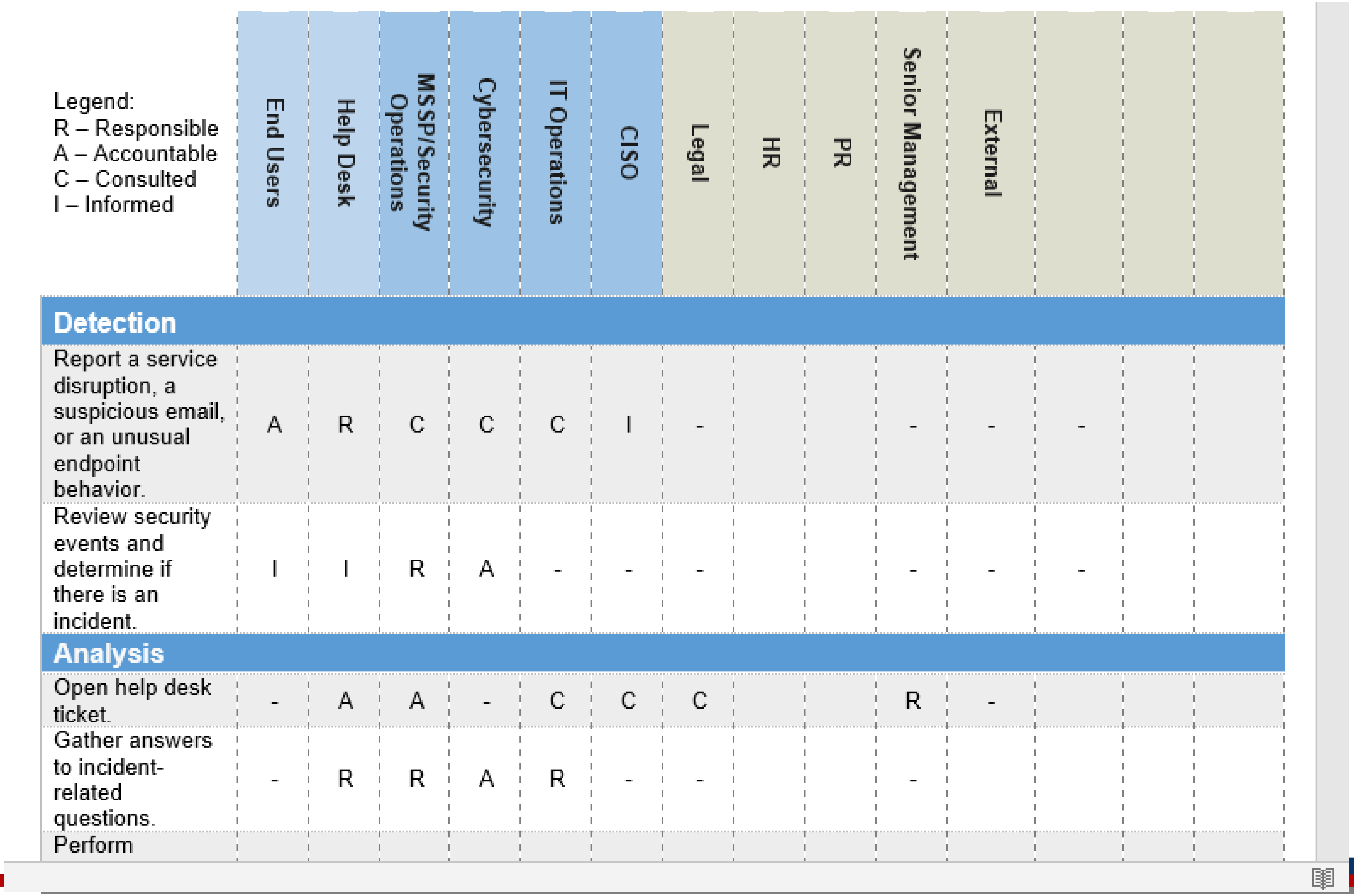
What are key questions, and initial response actions, to discuss tonight?

RACI Chart

Actions have specific individuals assigned, they are responsible and accountable for it. Individuals are also listed as consulted or informed on the measure.

- **Responsible** – The person(s) who does the work to accomplish the activity; they have been tasked with completing the activity or getting a decision made.
- **Accountable** – The person(s) who is accountable for the completion of the activity. Ideally, this is a single person and is often an executive or program sponsor.
- **Consulted** – The person(s) who provides information. This is usually several people, typically called subject-matter experts (SMEs).
- **Informed** – The person(s) who is updated on progress. These are resources that are affected by the outcome of the activities and need to be kept up to date.

RACI Chart

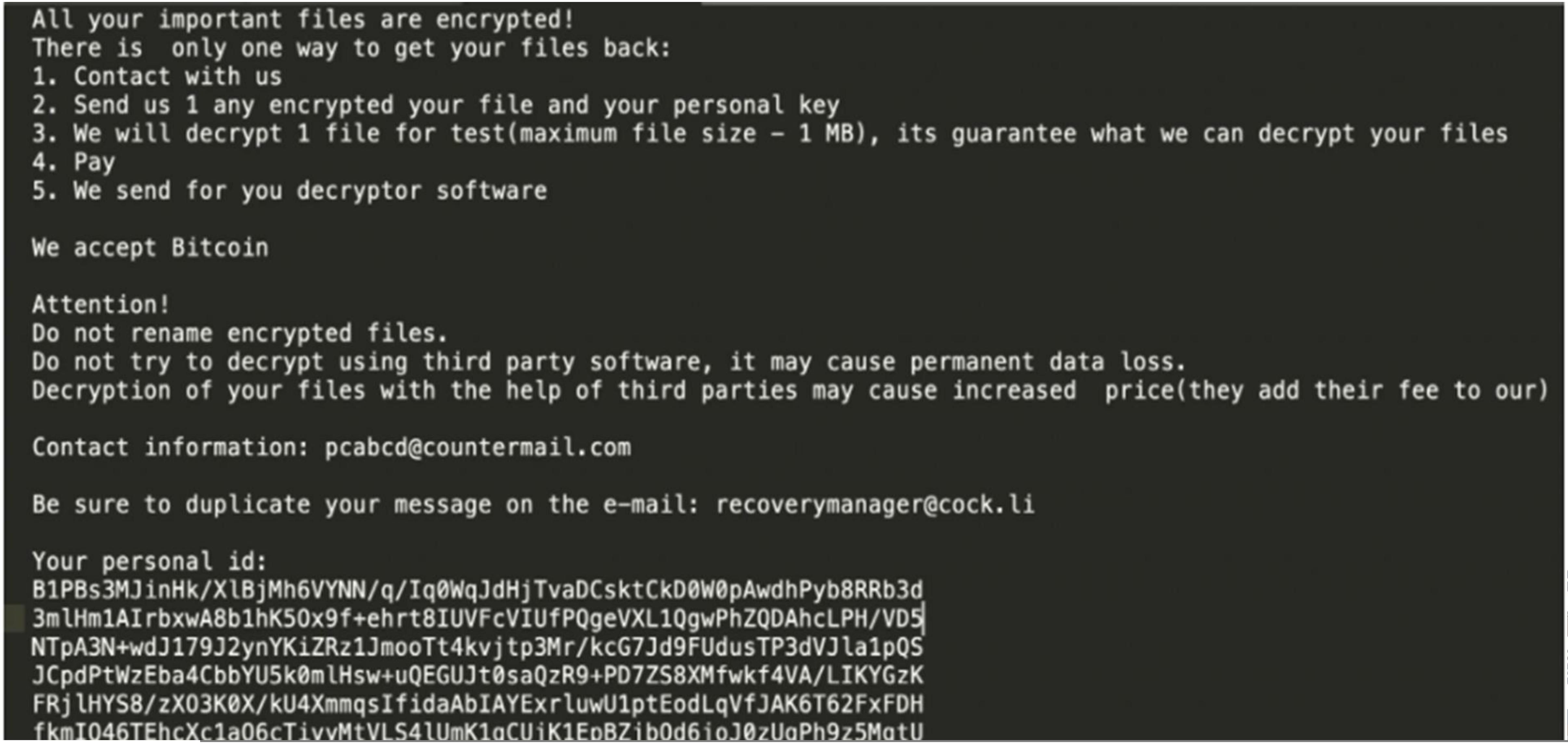


Legend:
R – Responsible
A – Accountable
C – Consulted
I – Informed

	End Users	Help Desk	MSSP/Security Operations	Cybersecurity	IT Operations	CISO	Legal	HR	PR	Senior Management	External			
Detection														
Report a service disruption, a suspicious email, or an unusual endpoint behavior.	A	R	C	C	C	I	-			-	-	-		
Review security events and determine if there is an incident.	I	I	R	A	-	-	-			-	-	-		
Analysis														
Open help desk ticket.	-	A	A	-	C	C	C			R	-			
Gather answers to incident-related questions.	-	R	R	A	R	-	-			-				
Perform														

Saturday, 1:14 a.m.

The weather workstation has been pulled off net, the ransom instructions say:



```
All your important files are encrypted!
There is  only one way to get your files back:
1. Contact with us
2. Send us 1 any encrypted your file and your personal key
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files
4. Pay
5. We send for you decryptor software

We accept Bitcoin

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased  price(they add their fee to our)

Contact information: pcabcd@countermail.com

Be sure to duplicate your message on the e-mail: recoverymanager@cock.li

Your personal id:
B1PBs3MJinHk/XlBjMh6VYNN/q/Iq0WqJdHjTvaDCsktCkD0W0pAwdhPyb8RRb3d
3mlHm1AIrbxwA8b1hK5Ox9f+ehrt8IUVFcVIUfPQgeVXL1QgwPhZQDAhcLPH/VD5
NTpA3N+wdJ179J2ynYKiZRz1JmooTt4kvjtp3Mr/kcG7Jd9FUdusTP3dVJla1pQS
JCpdPtWzEba4CbbYU5k0mlHsw+uQEGUJt0saQzR9+PD7ZS8XMfwkf4VA/LIKYGzK
FRjlHYS8/zXO3K0X/kU4XmmqsIfidaAbIAYExrluwU1ptEodLqVfJAK6T62FxFDH
fkmIO46TEhcXc1aO6cTiyyMtVLS4lUmK1qCUjK1EpBZibOd6joJ0zUqPh9z5MqtU
```

Analysis Phase

What are the two primary courses of action to consider?

What other questions, or actions, at the CIO level should Lori be contemplating?

Analysis Phase

Saturday, 7:48 a.m.

After all night conference calls with the Executive staff and legal team, everyone is tired, confused and uncertain as to how to proceed. A decision is needed now, but there is no consensus on the next steps. Lori pushes for, and gets authorization, to get external support.

Now that they have agree to get external help, what is their next step?

Saturday, 8:07 a.m.

Lori calls the NC DIT Service Desk and reports a ransomware incident. An Enterprise Security and Risk Management Office (ESRMO) incident responder arranges a conference call with her for 9 am. The responder advises her to notify the NC ISAC Cyber Analysis Center of the incident as well.

Lori learns the response process follows the Significant Cyber Incident Response Plan, also known as the state disruption plan. She is instructed to have key people on the call, and to ensure her team does not discuss the incident using airport email or messaging systems.

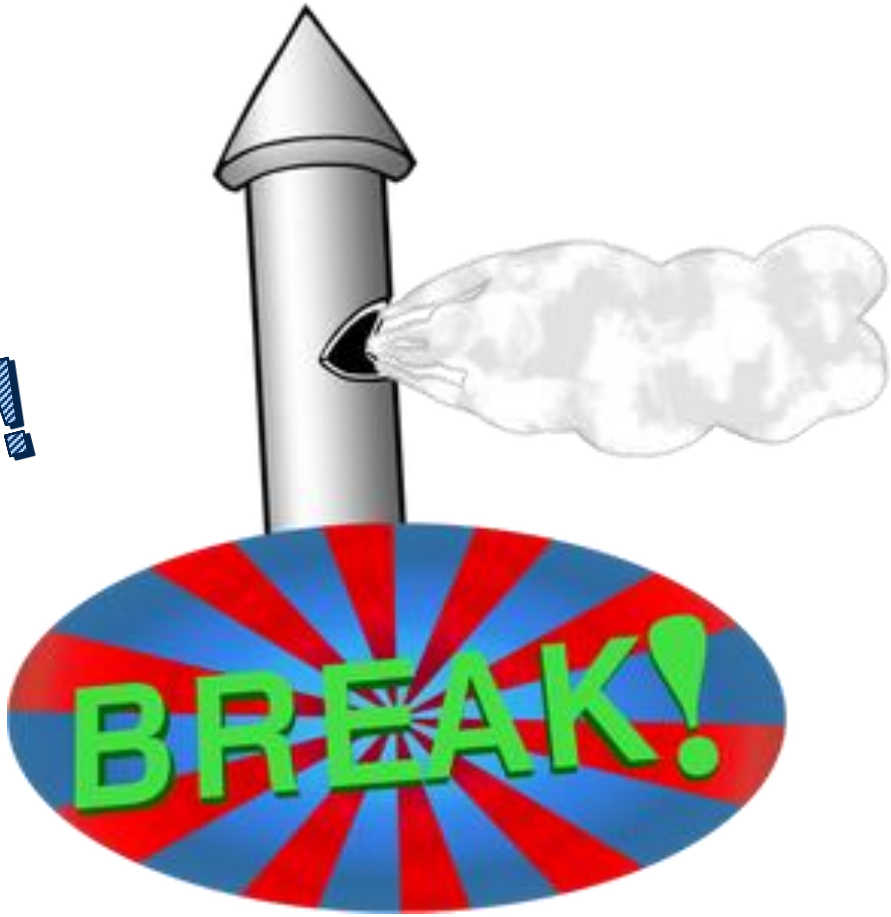
Analysis Phase

Saturday, 9:00 a.m.

The call starts at 9am. Brief introductions are followed by descriptions of what has been observed so far. After asking more questions regarding the scope, and impact the event may have on airport operations, the ESRMO team hangs up to assesses the incident.

At 9:56 the meeting reconvenes. The ESRMO team lead advises Lori that commercial enterprises are not normally supported by state resources. “However, we waive that in this case, due to the probability of it having a demonstrable impact to public health or safety in this COVID environment. We categorize this as a High level event, your request for support is approved. ESRMO will make appropriate notifications to lead and supporting agencies, and any other external entities as required. Right now, we need a lot of data from your team very quickly. Do you have any questions before we move further?”

Break Time!!



- Break’s Over!
- Please put your microphones on mute, and update the chat log with your name and organization if you have not done so already.
- We will now move into another inject, I’ll leave it on the screen for a few minutes for all to go over.

Analysis Phase

To refresh the scenario:

“We categorize this as a High level event, your request for support is approved. ESRMO will make appropriate notifications to lead and supporting agencies, and any other external entities as required. Right now, we need a lot of data from your team very quickly. Do you have any questions before we move further?”

What questions would you ask DIT at this point in the event?

What data would you expect to be asked for at this juncture?

What is the malware most likely doing during this timeframe?

Analysis Phase

Saturday, 10:50 a.m.

The NCNG Cyber Security Response Force (CSRF) duty officer is talking to Lori on her cell. “We got a call from State Emergency Management that you have a situation, what are you seeing?” They discuss the events of the past few days, and the duty officer asks for the names and contact numbers for her key team members.

“We will start taking images as soon as we get there, and we’ll need signatures on some NDA’s coming to your inbox soon. I’ll be your POC this weekend to coordinate work and answer any questions. As we get deeper into this, more specialists will likely be engaged. Call me with any concerns or issues, you have my number”.

Analysis Phase

What devices will need to be forensically imaged?

What are some primary areas of concern the airport team should be verifying or validating at this point?

What are other key actions to plan for, or begin taking now?

Sun 8:45 a.m. The CSERF provides this update:

Patient zero is the accounts payable workstation used early Tues to open the “W4”, an infected Word document. The stolen user credentials enabled access to three different network shares, VPN, and a web server not configured for MFA.

Log data has been scoured. The phishing emails ceased after the initial wave early Tues. The mail server they originated from is no longer visible. The phishing email was opened on 8 endpoints. 4 of those 8 also attempted to update their W4. Those stolen credentials allowed even greater movement and access in the network.

Privilege escalation was gained by a brute force attack on the Administrator account Tuesday night. Once credentials were stolen, SMB was then used to recon accessible hosts. The attacker used RAS to move laterally to those hosts. LockBit was downloaded from each host with a PowerShell script, and compiled with VBC. CPU usage exploded on each host during the compile. Wednesday thru Friday, packets went to and from an IP in Belarus. Numerous Emotet and LockBit IOCs were noted. This version of LockBit is generation three, with enhanced lateral movement, code execution and obfuscation measures over previous versions.” [14]

Containment

Where does the team focus its efforts now?

What should the CIO be focusing on, or coordinating now?

Monday, 12 p.m. Containment complete

The team took 6 hours to rest and change clothes Sunday night before going back to Containment work at 7am. They push through and complete Containment efforts mid-morning.

Eradication efforts get underway around 11 a.m. Monday.

Before beginning eradication activities, what steps would you take to ensure all infected or impacted systems and infrastructure were identified?

Eradication

What actions and processes would you focus on in the Eradication phase?

Monday, 10:15 p.m. Eradication continues

Forensic analysis and malware scans have been completed on all endpoints, network devices, servers, VM’s and backup data. Several instances of Emotet and LockBit were discovered and remediated. In addition, a Trickbot loader masked as a .png file was discovered on the webserver that was not configured for MFA. Although the infiltration method is unknown, Forensics theorizes an employee browsing the internet opened or downloaded a file containing malicious code that got the loader down to the webserver. Log activity had no clues on this event, it may have occurred outside the time window that log data is retained.

Reimaging activities will begin immediately, followed by data restoration.

What is the priority of effort needed to efficiently accomplish reimaging and restore operations?

Tuesday, 10:45 a.m. Eradication Complete

Re-imaging is complete, current patches verified on all OS’s.

Documentation of new controls (temporary and permanent), forensic analysis and evidence is being collected and secured.

Lori announces Eradication efforts are a success, and gives the green light to start data restoration. The team is now in the Recovery Phase.

What are some areas of concern or emphasis during the Recovery phase?

Recovery

Tuesday, 5:15 p.m.

Affected entity configurations were validated using approved configuration baselines, Security and Technical Implementation Guides (STIGS), NIST 800-53, or the latest version of CIS controls. Vulnerability testing was completed to ensure they are not susceptible to various methods of attack, prior to being placed into production. [12]

Server OS's, DC's, VM's and backup systems have been restored, tested and validated.

Data restoration went smoothly, managers or subject matter experts in the major business areas verified and validated the restored data is 'good'.   **Recovery is successful.**

Who declares the incident is over?

What are the criteria for declaring the response complete?

What should the Airport cabinet staff be planning and preparing for next?

Lessons Learned

- Who should participate in the lessons learned event? How soon should the event occur?
- Are there any aspects of the event that should not be captured in the discussions?
- What corrective or mitigation actions need to be brought out in lessons learned?
- Are there training or educational efforts needed moving forward?
- What documents, processes and plans may need to be updated from the lessons learned exercise?
- Where will the outputs from the lessons learned be archived?
- Do your information security officers and emergency managers jointly plan for cybersecurity incidents?
- Are IA/IT and business continuity functions coordinated with physical security?
- Are all three then collaborating with public relations, human resources, and legal departments?

Preparation Phase Defensive Measures

Prevention is your best defense. Be proactive, be vigilant, be suspicious.

Maintain network and infrastructure diagrams, authorized device lists, authorized software lists, lists of elevated permissions users (SA's, NA's, etc..), COOP and Disaster Recovery Plans

Monitor firewall, IPS/IDS, anti-virus, anti-malware, web proxy and email scan log data

Establish relationships **now** with your Regional NICLGISA Strike Tm leader, NC Fusion, the FBI, your local Sherriff or Police cyber specialist, the NCDIT, and the NCNG CSERF. These are the support teams you may work with in the event of a cyber attack or incident. See slides 59-60 for contact info.

Implement an awareness and training program

Enable strong spam filters.

Authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing [8]

Preparation Phase Defensive Measures

Scan incoming and outgoing email to detect threats and filter executable files

Configure firewalls to block access to known malicious IP addresses

Patch operating systems, software, and firmware on devices

Set anti-virus / anti-malware programs to conduct regular scans automatically

Manage the use of privileged accounts based on the principle of least privilege [1]

Configure access controls (file, directory, network share permissions) with least privilege in mind.

Disable macro scripts from office files transmitted via email.

Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder. [8]

Preparation Phase Defensive Measures

Disable Remote Desktop protocol (RDP) if it is not being used

Use application whitelisting, which only allows systems to execute programs known and permitted by security policy

Execute operating system environments or specific programs in a virtualized space

Categorize data based on organizational value, implement **physical and logical** separation of networks and data for different organizational units

Subscribe to alerts from www.us-cert.gov/Ransomware

Back up data. **Regularly.** Verify the integrity of backups, test restoration processes

Conduct annual penetration tests and vulnerability assessments

Secure backups. Ensure backups are not connected permanently to devices and networks. Backups are critical in ransomware recovery and response; if infected, a backup may be the best (or only) way to recover critical data [8]

Preparation Phase Defensive Measures

And last, but not least:

Mandatory employee accountability and Safe Computing training.

Implement, and maintain, accountability via an Authorized User Policy or Agreement. Put teeth into your policies and user best computing practices.

Training, conducted annually. We recommend policy requiring users to successfully pass annual cyber and safe computing training to retain network access.

Exercise Conclusion

This was a fictional event at a fictional location. The scenario is a fictional compilation of actual attacks, interwoven for training purposes. Any similarity to actual agencies, personnel or commercial companies is unintentional.

There are dozens of additional slides with ransomware related information for your viewing pleasure following the References, peruse them at your pleasure.

Are there any questions or final comments?

We thank you for your participation today, and hope this was a helpful event.

If you have suggestions for areas to improve, or sustain, please email them to the NCAAT organizational email at the bottom of this slide.

CSRF Contacts
LTC Robbie Felicio, NCNG CIO, robert.n.felicio.mil@mail.mil
LTC Seth Barun, NCNG DCOE Chief, seth.a.barun.mil@mail.mil
CPT Steven Schmidt, NCNG DCOE Mission Planner, steven.j.schmidt3.mil@mail.mil
ng.nc.ncarng.mbx.g6-ncat@mail.mil

References

1. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/ransomware-malware

2. https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html

3. https://www.us-cert.gov/Ransomware

4. https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

5. https://searchsecurity.techtarget.com/definition/ransomware

6. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

7. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

References continued

8. https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf **

9. https://www.infotech.com/

10. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

11. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/attack-list-cities-government-agencies/

12. https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf

13. https://www.seculore.com/cyber-attacks-north-carolina

14. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/

15. https://csrc.nist.gov/publications/detail/sp/800-150/final

Effects of a ransomware attack

- Downtime as a result of compromised infrastructure
- Lost productivity as a result of downtime
- Costly recovery efforts that potentially outweigh the ransom itself
- Long-term damage to both data and data infrastructure
- Damage to agency/business/organization's reputation
- Legal actions from impacted clients or public served by the agency
- Loss of customers, and in worst cases, the potential for personal harm if the malware interfered with public services such as EMS/911 or healthcare [5]

What is Ransomware?

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by visiting an infected website.[3]

Ransomware typically encrypts files and folders, preventing access to important files. Ransomware attempts to extort money from victims, often in the form of cryptocurrencies, in exchange for the decryption key.

Ransomware is one of the most lucrative revenue channels for cybercriminals, so malware authors continually improve their malware code to better target enterprise environments. For cybercriminals, ransomware is lucrative, at the expense of individuals and businesses.

Most ransomware infections propagate via phishing campaigns, or through websites with malware that use vulnerabilities in your agencies web browsers or other software to install ransomware. Once ransomware infects a device, it starts encrypting files and folders, or in some cases, the entire hard drive.

What is Phishing?

Sending email messages, designed to trick the recipient into opening an attachment or link, that tries to install ransomware. Phishing attacks attempt to steal sensitive information through emails, websites, text messages, or other forms of electronic communication that often look to be official communication from legitimate companies or individuals. [7]

These emails often impersonate mail from a trusted or easily recognizable source. For example, a common phishing email purports to come from the Social Security Administration (SSA). It looks exactly like a real SSA message, and requests the recipient to verify some data point (usually address), by clicking a link or attachment. Once the link or attachment is opened, malware is loaded on the device, and the system is compromised. Phishing emails masquerading as messages from banks, utilities, government agencies and non-profit agencies have all been utilized over the years to gain access to unsuspecting recipients computers.

Types of Ransomware

Ransomware can be deployed in different forms. Some variants may be more harmful than others, but they all have one thing in common: a ransom. Here are seven common types of ransomware.

Crypto malware. This form of ransomware is capable of encrypting files, folders, and hard-drives. A recent example is the 2017 WannaCry ransomware attack. It targeted thousands of Windows systems around the world, and spread within corporate networks globally. Victims were asked to pay ransom in Bitcoin to retrieve their data.

Lockers. Locker-ransomware is known for infecting your operating system to completely lock you out of your computer or devices, making it impossible to access any of your files or applications. This type of ransomware is most often Android-based.

Types of Ransomware

Scareware. Scareware mimics an antivirus or virus cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the problems. Some types of scareware lock your computer. Others flood your screen with annoying alerts and pop-up messages.[4]

Master boot record (MBR) ransomware: The entire hard drive is encrypted, making it impossible to access the operating system.[5]

Doxware. Commonly referred to as leakware or extortionware, doxware threatens to publish your stolen information online if you don’t pay the ransom. With sensitive files and personal photos at risk, it’s understandable why some people pay the ransom. [4]

Types of Ransomware

RaaS. Ransomware-as-a-service is a cybercriminal business model. Malware creators sell their ransomware and other services to cybercriminals, who operate the ransomware attacks. The business model also defines profit sharing between the malware creators, ransomware operators, and other parties that may be involved. [1]

Mac ransomware. Mac operating systems were infiltrated by their first ransomware, KeRanger, in 2016. Mac devices were infected via an app called Transmission, which was able to encrypt its victims files after being launched. [6]

Mobile device. Ransomware infiltrated mobile devices on a large scale in 2014. Mobile ransomware often enters via a malicious app, displaying a message stating the device has been locked due to illegal activity. [4]

Ransomware Variants

Variant information is found at https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

1. SamSam

Attacks using software known as SamSam started appearing in late 2015, but really ramped up in the next few years, gaining some high-profile scalps, including the Colorado Department of Transportation, the City of Atlanta, and numerous health care facilities. SamSam is the perfect example of how attackers' organizational prowess is as important as their coding skills. SamSam doesn't indiscriminately look for some specific vulnerability, as some other ransomware variants do, but rather operates as ransomware-as-a-service whose controllers carefully probe pre-selected targets for weaknesses, with the holes it has exploited running the gambit from vulnerabilities in IIS to FTP to RDP. Once inside the system, the attackers dutifully work to escalate privileges to ensure that when they do start encrypting files, the attack is particularly damaging.

Ransomware Variants

Although the initial belief among security researchers was that SamSam had an Eastern European origin, the overwhelming majority of SamSam attacks targeted institutions within the United States. In late 2018, the United States Department of Justice indicted two Iranians that they claim were behind the attacks; the indictment said that those attacks had resulted in over $30 million in losses. It's unclear how much of that figure represents actual ransom paid; at one point the Atlanta city officials provided local media with screenshots of ransom messages that included information on how to communicate with the attackers, which led them to shut that communications portal down, possibly preventing Atlanta from paying ransom even if they wanted to.

2. Ryuk

Ryuk is another targeted ransomware variant that hit big in 2018 and 2019, with its victims being chosen specifically as organizations with little tolerance for downtime; they include daily newspapers and a North Carolina water utility

Ransomware Variants

struggling with the aftermath of Hurricane Florence. The Los Angeles Times wrote a fairly detailed account of what happened when their own systems were infected. One particularly devious feature in Ryuk is that it can disable the Windows System Restore option on infected computers, making it all the more difficult to retrieve encrypted data without paying a ransom. Ransom demands were particularly high, corresponding to the high-value victims that the attackers targeted; a holiday season wave of attacks showed that the attackers weren't afraid to ruin Christmas to achieve their goals.

Analysts believe that the Ryuk source code is largely derived from Hermes, which is a product of North Korea's Lazarus Group. However, that doesn't mean that the Ryuk attacks themselves were run from North Korea; McAfee believes that Ryuk was built on code purchased from a Russian-speaking supplier, in part because the ransomware will not execute on computers whose language is set to Russian, Belarusian, or Ukrainian. How this Russian source acquired the code from North Korea is unclear.

Ransomware Variants

3. PureLocker

PureLocker is a new ransomware variant that was the subject of a paper jointly put out by IBM and Intezer in November 2019. Operating on either Windows or Linux machines, PureLocker is a good example of the new wave of targeted malware. Rather than taking root on machines via broad-range phishing attacks, PureLocker appears to be associated with more_eggs, a backdoor malware associated with several well-known cyber-criminal gangs. In other words, PureLocker is installed on machines that have already been compromised and are fairly well understood by their attackers, and then proceeds to make a number of checks on the machine where it finds itself before executing, rather than opportunistically encrypting data wherever it can.

While IBM and Intezer didn't disclose how widespread PureLocker infections were, they did reveal that most took place on enterprise production servers, which are obviously high-value targets. Because of the high-skill human control

Ransomware Variants

this kind of attack entails, Intezer security researcher Michael Kajiloti believes that PureLocker is a ransomware as a service offering that's only available to criminal gangs who can pay well up front.

4. Zeppelin

Zeppelin was is an evolutionary descendent of the family known as Vega or VegasLocker, a ransomware-as-a-service offering that wreaked havoc across accounting firms in Russia and Eastern Europe. Zeppelin has some new technical tricks up its sleeve, especially when it comes to configurability, but what makes it stand out from the Vega family is its targeted nature. Where Vega spread somewhat indiscriminately and mostly operated in the Russian-speaking world, Zeppelin is specifically designed to not execute on computers running in Russia, Ukraine, Belarus, or Kazakhstan. Zeppelin can be deployed in a number of ways, including as an EXE, a DLL, or a PowerShell loader, but it appears that at least some of its attacks came via compromised managed security service providers

Ransomware Variants

which ought to send a chill down anyone's spine.

Zeppelin began to appear on the scene in November 2019, and as more proof of its difference from Vega, its targets seemed carefully chosen. Victims were mostly in the health care and technology industries in North America and Europe, and some of the ransom notes were written to specifically address the infected target organization. Security experts believe the shift from Vega's behavior is the result of the codebase being used by a new and more ambitious threat actor, probably in Russia; while the number of infections isn't that high, some believe what we've seen so far has been a proof of concept for a larger set of strikes.

5. REvil/Sodinokibi

Sodinokibi, also known as REvil, first emerged in April of 2019. Like Zeppelin, Sodinokibi appeared to be the descendent of another malware family, this one called GandCrab; it also had code that prevented it from executing in Russia and

Ransomware Variants

several adjacent countries, as well as Syria, indicating that its origin is in that region. It had several methods of propagation, including exploiting holes in Oracle WebLogic servers or the Pulse Connect Secure VPN.

Sodinokibi's spread again indicated an ambitious command and control team behind it, probably as a ransomware as a service offering. It was responsible for shutting down more than 22 small Texas towns in September, but it truly hit notorious status on New Year’s Eve 2019 when it took down the UK currency exchange service Travelex, forcing airport kiosks to resort to pen and paper and leaving customers in limbo. The attackers demanded a stunning $6 million ransom, which the company refuses to confirm or deny it paid.

Ransomware Variants

When asked, Juniper's Hahad for his pick for the worst ransomware of 2019, Sodinokibi was his choice, because of an extra twist that Sodinokibi's controllers put into their attacks. "The one thing that really makes this a little bit special is that this particular group has taken on a new approach of not only telling people, 'You're not going to get your data back if you do not pay the ransom,' but also, 'We are going to publish that confidential data on the web or sell it in an underground forum to whomever is the highest bidder.' That takes the ransomware approach to the next level in their business model." This is a huge departure from the usual ransomware model — after all, one of its big advantages is that you can lock down your victim's data without going through the difficult process of exfiltrating it — but they've already followed through on the threat at least once. The new era of hyper-targeted, custom-tailored ransomware appears to be reaching new and dangerous depths.

Data on previous 8 slides is from https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

We are infected – now what?

Should preventive measures fail, US-CERT recommends considering these steps:

- Isolate the infected computer immediately
- Isolate or power-off affected devices that have not yet been completely corrupted
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware
- Contact law enforcement immediately
- If available, collect and secure partial portions of the ransomed data that exist
- Change online account & network passwords after removing the unit from the network
- Change all system passwords once the malware is removed
- Delete Registry values and files to stop the program from loading
- Implement incident response and business continuity plans. Ideally, recent, un-infected backups are available, minimizing the impact of the infection, and recovery processes [8]

We are infected – now what? continued

Do not pay until fully assessing the situation, some ransomware is less difficult to mitigate than others. Forge relationships with the agencies below **now**, so you are not meeting them for the first time during a live event.

NC DIT – NC Dept of Information Technology, is the primary contact for state and local government requiring incident support with access to state and federal resources applicable to your event. DIT Service Desk 919-754-6000, toll free 800-722-3946, or request support online at   https://it.nc.gov/service-desk

NCISAAC– NC Information Sharing and Analysis Center. Cyber professionals and LEA's monitoring, reporting and responding to cyber events in NC. 888-624-7222 email: ncisaac@ncsbi.gov

NCNG- Home of the nation's best Cyber Security Response Force. Army and Air National Guard cyber Warriors of the highest caliber.
POC: G6-CSRF, 984-664-6000, ng.nc.ncarng.mbx.g6-csrf@mail.mil

We are infected – now what? (continued)

NCLGISA Strike Team: North Carolina Local Government Information Systems Association. The Strike Team is a volunteer team of regional ‘cyber first responders’ willing to assist with incident response. Immediate response 24x7x365: (919) 726-6508 Non-critical requests: itstriketeam@nclgisa.org

Research commercial sources for cyber incident support. Get quotes for service BEFORE you have an event. Quotes, or service, may be slow during a widespread cyber event. Be proactive

We are infected – Should we pay?

There are serious risks to consider before paying the ransom. US-CERT does not encourage paying a ransom to criminal actors. Executives will look to the technical staff for a recommendation, evaluate the technical feasibility, timeliness, and cost of restarting systems from backup. Ransomware victims need to consider the following factors:

- Paying a ransom does not guarantee regaining access to data; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom
- Some victims who paid the demand were targeted again by cyber actors
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key
- Paying could inadvertently encourage this criminal business model [8]

Future trends

Ransomware has surged in the past two years, with many high profile events making headlines around the world. Recent, more advanced attacks have often focused on production servers, critical to daily operations. Once a key production server is taken for ransom, the odds this will remain a privately managed event are slim.[2]

In late 2019, another nasty variant named Zeppelin surfaced. It can be deployed in a number of ways, including as an EXE, a DLL, or a PowerShell loader, and it appears some of its attacks came via compromised managed security service providers. That adds a whole new twist to your defense preparations. [2]

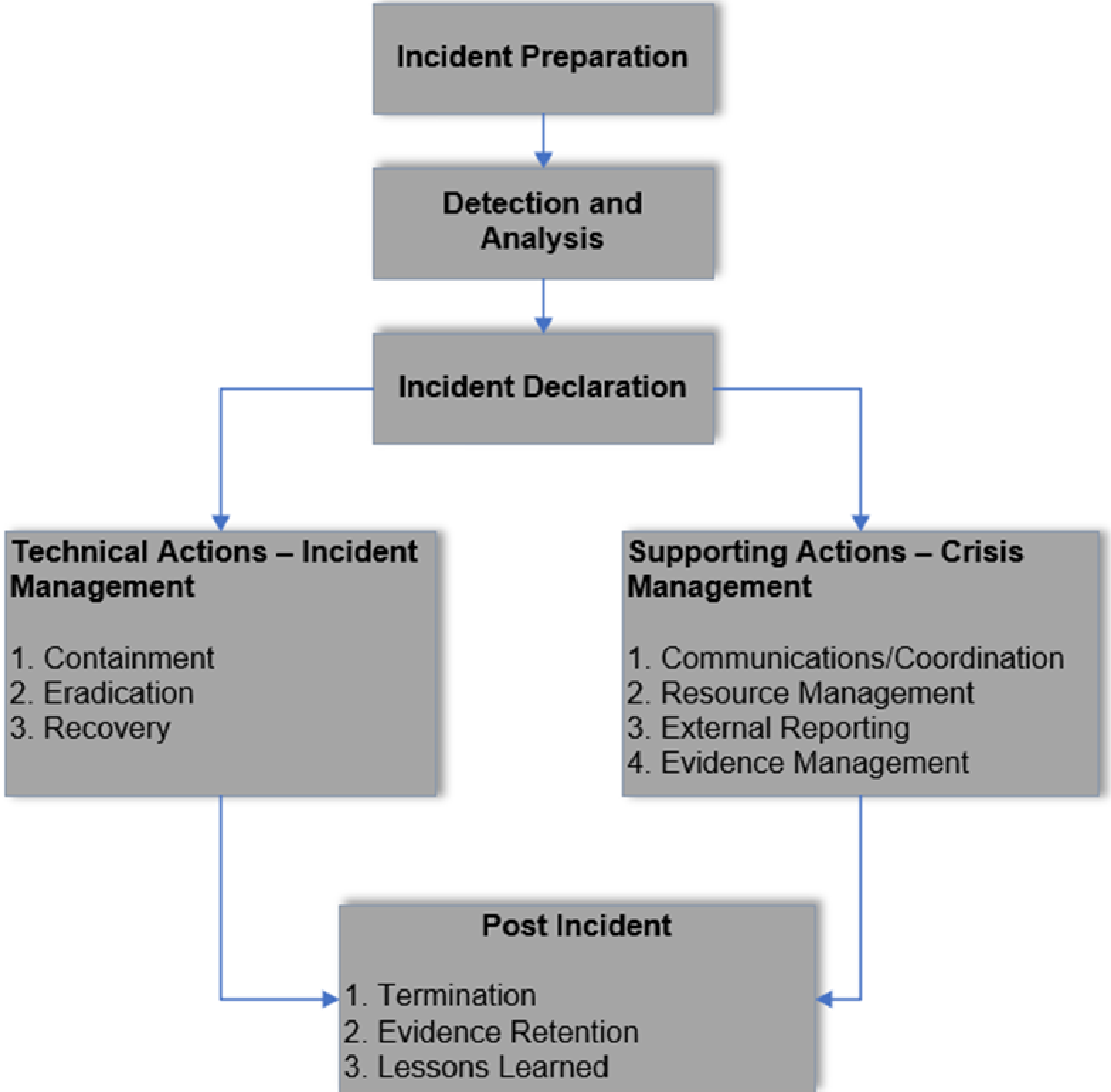
IoT ransomware may not be far behind. Two researchers, Andrew Tierney and Ken Munro, demonstrated malware that attacked, locked and demanded a one-bitcoin ransom on a generally available smart thermostat at the 2016 Def Con hacking conference.[5]

Pop Quiz!

Which of the following are not viable preventative measures for ransomware?

- Implement an awareness and training program. Require users to re-train annually.
- Enable strong spam filters to prevent phishing emails from reaching end users
- Require all employees to maintain a current NC Dept of Wildlife Phishing License
- Scan incoming and outgoing email to detect threats and filter executable files
- Configure firewalls to block access to known malicious IP addresses
- Patch operating systems, software, and firmware on devices
- Set anti-virus / anti-malware programs to conduct regular scans automatically
- Manage the use of privileged accounts based on the principle of least privilege
- Configure access controls (file, directory, network share permissions) with least privilege in mind
- Require users to call the Help Desk before clicking links in email

NC DIT Incident Response Process



Incident Preparation

Detection and Analysis

Incident Declaration

Technical Actions – Incident Management

1. Containment
2. Eradication
3. Recovery

Supporting Actions – Crisis Management

1. Communications/Coordination
2. Resource Management
3. External Reporting
4. Evidence Management

Post Incident

1. Termination
2. Evidence Retention
3. Lessons Learned

Ransomware Cyber-kill Chain

1. The ransomware executable is delivered via:

- Attachments or web links in phishing emails
  Block incoming emails on the SMTP server, removing emails from user inboxes, warn users to not click on certain links and attachments
- Malvertising on innocuous web pages
  Block malicious URLs on the web proxy, identify computers that visited malicious websites on certain URLs using the proxy logs
- Drive-by downloads (e.g. fake antivirus)
  Block malicious URLs on the web proxy, identify computers that visited malicious websites using the proxy logs, deploy custom AV signatures to block certain files to be downloaded, identify PCs with ETDR that downloaded files with certain IoCs

2. The payload is executed on the end user's device and the ransomware installs itself

Application whitelisting, identify PCs using the HIDS logs that executed certain files

3. The ransomware generates a unique encryption/decryption key pair

4. The ransomware contacts a C2 server on the Internet to deposit the decryption key

Identify and/or block traffic on NIDS and the proxy

5. The malware starts encrypting the files on the hard disk, mapped network drives and USB devices with the encryption key

Monitor end-user devices and shared folders for certain file extensions, such as .abc, .xxx, .yyy, .zzz

6. Once the process finishes, the files become inaccessible. The malware places a text file on the desktop and/or a splash screen pops-up with the instructions to pay and restore the original files.

Monitor endpoints for ransomware related text or HTML files in the desktop folder

https://www.demisto.com/playbook-for-handling-ransomware-infections/

Detection – sort of……

What should Sam have done with the log observations?

What appears to be wrong with the log and event monitoring process?

What should be monitored (in the Preparation phase) for unusual activities?

Firewalls, IDS/IPS devices/services, web proxy’s for suspicious connections, Antivirus logs, anti-malware logs, email gateways

How would this be observed or detected in your environment?

What might the malware be doing now?

Detection Phase

Does the airport help desk respond appropriately to these calls?

What indicators are presented that should alarm the help desk?

What tools, policies or procedures could be in place to assist the help desk assess the situation?

How would you want your helpdesk to respond to these calls?

Analysis Phase

Assign documentation management duties (track control measures, eradication actions, topology changes, forensic data, evidence collection and evidence security)

Determine endpoint exposures or compromises, and potential risk implications.

Assess all internet-facing endpoints, close unnecessary endpoint ports/services.

Maintain a dynamic, frequently updated list of active endpoint ports.

Restrict local admin rights. Close unnecessary server ports/services, implement least privilege access

Search web proxy logs to identify any outbound command and control traffic.

Perform IOC search in firewall, IDS, IPS, email gateway, and system and server logs.

Assess if servers were impacted. Decide who addresses infected servers (NOC, SOC, Cyber)

Determine if any local or server data was encrypted.

Pop Quiz! Ask yourself:

Does my organization have a Cyber Incident Response Plan (CIRP)?

If yes, has it been updated and rehearsed within the 12 months?

If a cyber incident (of any type) were to occur in your organization today, how do you rate your understanding of your cyber incident response plan (CIRP)? On a scale of 1 (lowest) to 5 (highest understanding)

Does my organization comply with Agency IA/IT policies and regulations at all levels?

Has my IT & IA environments had an assessment or audit in the last 24 months?

If yes, were deficiencies noted in the assessment addressed?

What percentage of your servers, endpoints and networked devices and applications are CAT1 patched?