CYBERSECURITY: PLANNING FOR AND RESPONDING TO AN ATTACK

2021 COUNCIL OF CHIEF JUDGES OF THE STATE COURTS OF APPEAL

BOSTON, MASSACHUSETTS

OCTOBER 28, 2021

ABOUT THE SESSION

This session will cover the stories of courts that have experienced cyber events that highlight the importance of planning. These experiences have valuable lessons learned that will be shared, which may help courts improve existing plans or get started on the planning process. Some key actionable steps that are high value and moderate effort cyber security hygiene practices will be recommended, and a take-away score card that can be used to evaluate current court technology cybersecurity status will be provided. This Center for Internet Security score card may help identify gaps and assist with prioritizing future cyber security initiatives.

THE PANEL

- **Charles Byers**, Chief Information Officer, Kentucky Court of Justice
- **Jorge Basto**, Director of IT Programs, Cherokee County Clerk of Courts
- **Tim Holthoff**, Chief Information Officer, Arkansas Administrative Office of the Courts

ARKANSAS

- Non-unified judiciary
- Administrative Office of the Courts (AOC)
- Court applications at all levels
- AOC hosts Arkansas Judiciary website

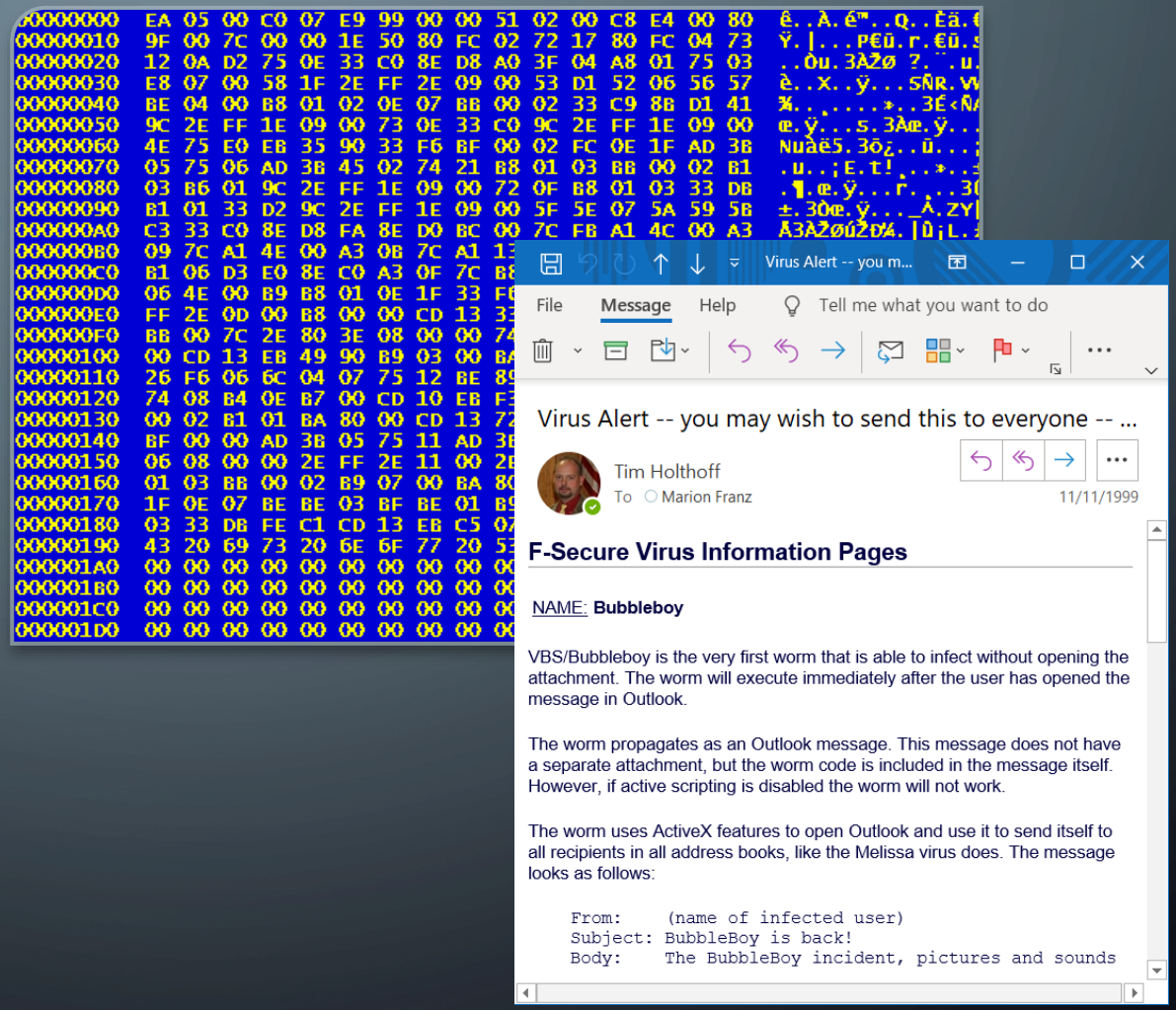
NOT TOO BIG FOR OUR BREACHES

- Compromised virtual machine
- Cryptocurrency mining operation
- Website defaced
- Surrendered credentials from phishing

CYBERSECURITY IS NOTHING NEW

The 1990's brought us

- Monkey Virus
- Melissa Virus
- Bubble Boy Worm



MORE THREATS

Early 2000's

- Love Bug Virus
- More networked devices
- More networked services
- More malicious actors
- More email traffic
- Virtual servers
- More tools to respond to threats

THREATS INCREASING

2018 ARKANSAS JUDICIARY WEBSITE PAGE WAS DEFACED

TODAY'S CONSTANT BATTLE

- Phishing attempts
- Several successful
- No ransomware… YET…but…

KENTUCKY COURT OF JUSTICE

- A Unified Court System
- Very Broad Responsibilities
- Centralized Information Technology
- Over 250 internally-developed Applications
- Primary and Secondary Data Centers
- Network Covering over 380 Nodes
- Tech Team of over 170 Staff
- Supporting nearly 3300 Court Personnel and 406 Elected Officials

KENTUCKY'S FIRST BRUSH WITH RANSOMWARE

- First exposure to Crypto Locker in 2014
- Delivered as an e-mail to a distribution group of Managers and Executives

DO NOT OPEN FAX - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward

Move to: ? To Manager Team Email Done Reply & Delete Create New

Move Assign Policy Mark Unread Categorize Follow Up Translate Read Aloud Zoom Reply with Meeting Poll Send to OneNote

Delete Respond Quick Steps Move Tags Editing Speech Zoom FindTime OneNote

Mon 4/7/2014 10:38 AM

Byers, Charles

DO NOT OPEN FAX

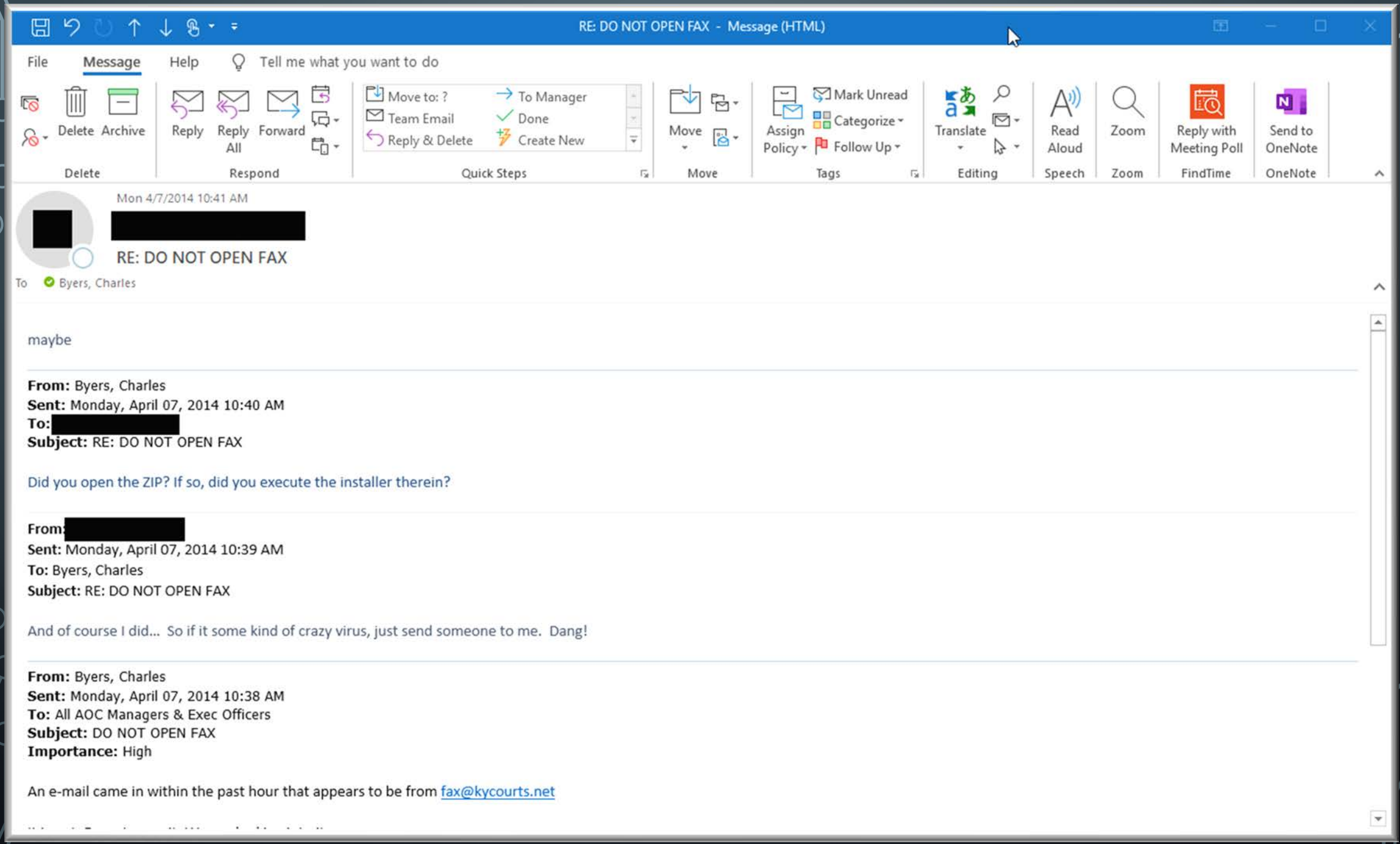
To All AOC Managers & Exec Officers

This message was sent with High importance.

An e-mail came in within the past hour that appears to be from fax@kycourts.net

It is not. Do not open it. We are looking into it now...

Charles P Byers
Chief Information Officer
Administrative Office of the Courts
1001 Vandalay Drive
Frankfort, KY 40601
(502) 573-2350 ext. 50111
(502) 330-6822 cell
(502) 782-8700 fax


RE: DO NOT OPEN FAX - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Move to: ?
To Manager
Team Email
Done
Reply & Delete
Create New
Move
Assign Policy
Mark Unread
Categorize
Follow Up
Translate
Read Aloud
Zoom
Reply with Meeting Poll
Send to OneNote
Delete
Respond
Quick Steps
Move
Tags
Editing
Speech
Zoom
FindTime
OneNote
Mon 4/7/2014 10:41 AM
[redacted]
RE: DO NOT OPEN FAX
To Byers, Charles
maybe
From: Byers, Charles
Sent: Monday, April 07, 2014 10:40 AM
To: [redacted]
Subject: RE: DO NOT OPEN FAX
Did you open the ZIP? If so, did you execute the installer therein?
From: [redacted]
Sent: Monday, April 07, 2014 10:39 AM
To: Byers, Charles
Subject: RE: DO NOT OPEN FAX
And of course I did... So if it some kind of crazy virus, just send someone to me. Dang!
From: Byers, Charles
Sent: Monday, April 07, 2014 10:38 AM
To: All AOC Managers & Exec Officers
Subject: DO NOT OPEN FAX
Importance: High
An e-mail came in within the past hour that appears to be from fax@kycourts.net


CHAOS

Your personal files are encrypted!

Private key will be destroyed on
9/24/2013
6:21 PM

Time left

54 : 15 : 15

Your important files **encryption** produced on this computer: photos, videos, documents. etc. **Here** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

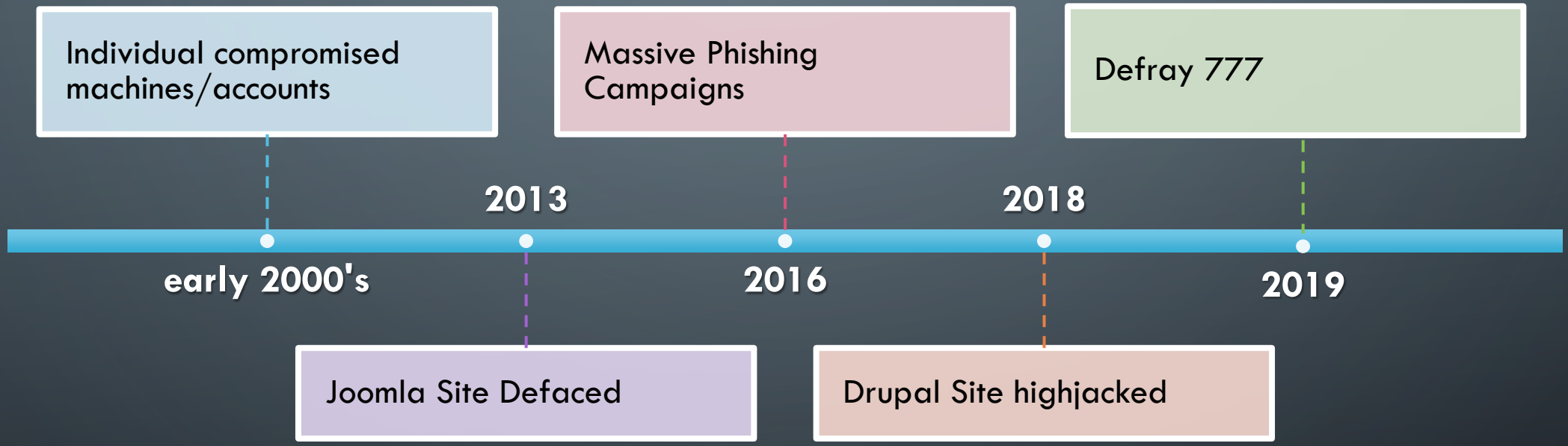
"I ASKED OUR TOP SECURITY ANALYST AND THERE IS A TECHNICAL TERM FOR IT.

HE SAID YOU ARE 'SCREWED'."

Judicial Council of Georgia AOC
Administrative Office of the Courts

- Decentralized Judiciary (10 Districts, 49 Circuits, 159 Counties)
- <1% of State Budget (20th in Salaries and Budgets)
- Separate IT Departments supporting the Supreme Court, Court of Appeals and Administrative Office of the Courts
- Physical Data Center and Colocation Site
- AOC directly supports all courts but limited hands-on services
  - 17 IT Staff support the AOC, partner organizations and courts

PREVIOUS EXPOSURES TO CYBERATTACKS



SECURITY PROGRAM LIFECYCLE

Preparation: What are you doing right now?

Detection & Analysis: Uh Oh, Something is wrong.

Containment & Eradication: Limit the damage and expel the threat.

Recovery: Back to business! Back-Ups are not "Recovery"

Post-Incident Activity: Never let a good crisis go to waste.

Detection and Analysis

SATURDAY
JUNE 29, 2019

Prepping for CMS Court Staff Training

CIO notified of malware discovered on the AOC Servers

Review of environment exposed the ransomware note and scope of the breach

Mobilized AOC and IT Management Teams

Launched response protocols to contact external resources

SUNDAY
JUNE 30, 2019

Containment and Eradication

- MS-ISAC, GTA and National Guard Resources reviewing activity logs
- Outgoing requests prompted a complete severing of the Data Center
- SecureWorks was contracted to perform additional remediation efforts
- CIO briefed the Chief, AOC Director and State CISO as to findings
- FBI was contacted and scheduled to be onsite Monday, July 1st

WEDNESDAY JULY 3, 2019

Recovery

- No affected systems have been brought back online
- Discussions led to the decision to have Internal IT take over and start Recovery
- Started rebuilding in AWS Cloud
- Stood up Judicial Council Website on Thursday July 4th
- Brought in AWS Resources to assist with “Lift and Shift” on the AOC Network

HOW DID THIS HAPPEN?

Thursday the 27th:

> Authorized access by Clerk to the AOC Network

> Authorized connection to a Citrix Server

> Unauthorized "backdoor" installed on CITRIX Server to provide continued access

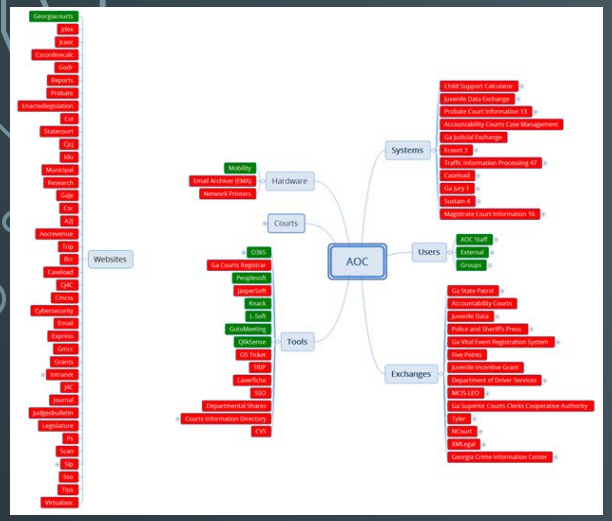
Friday the 28th:

> Unauthorized Persistence and Harvesting Tools

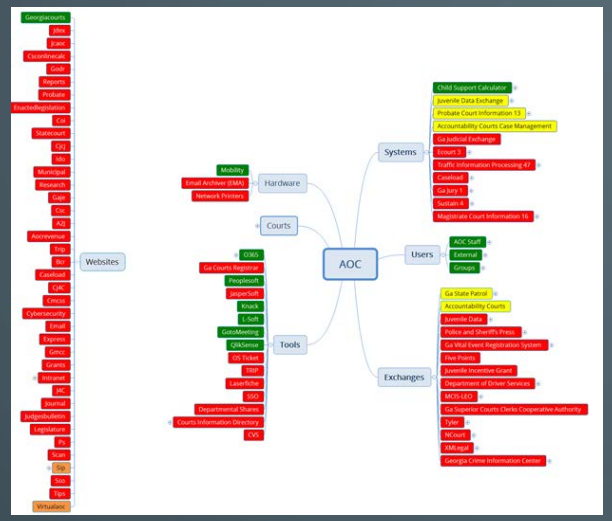
> Unauthorized Cobalt Strike functionality launched

Defray777 installed!

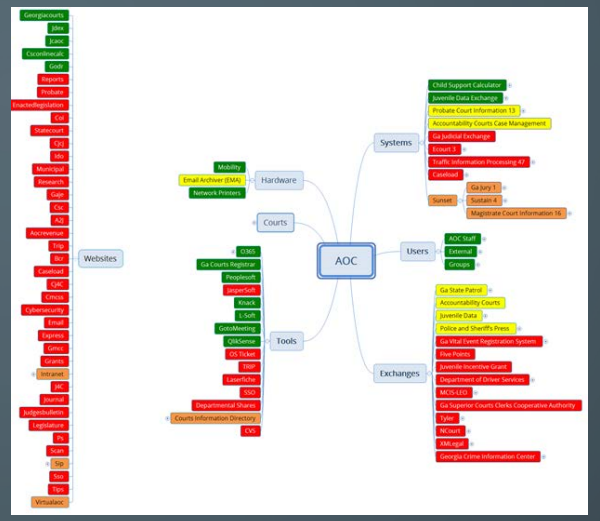
Week One



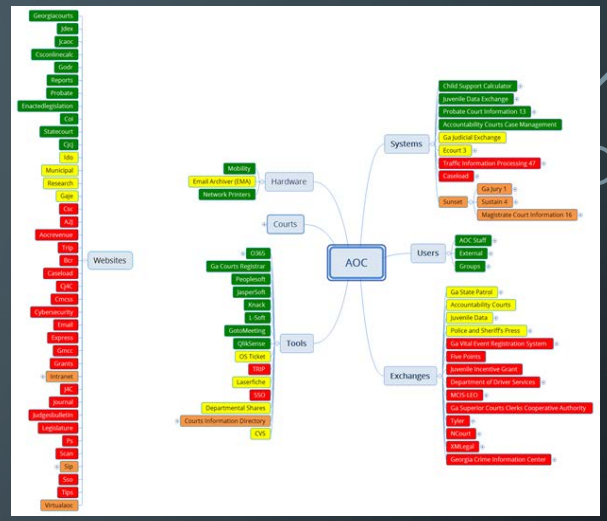
Week Two



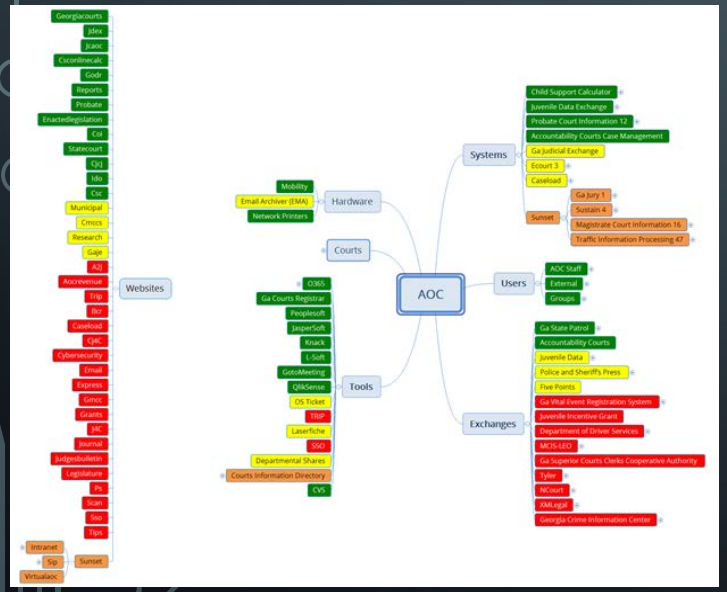
Week Three



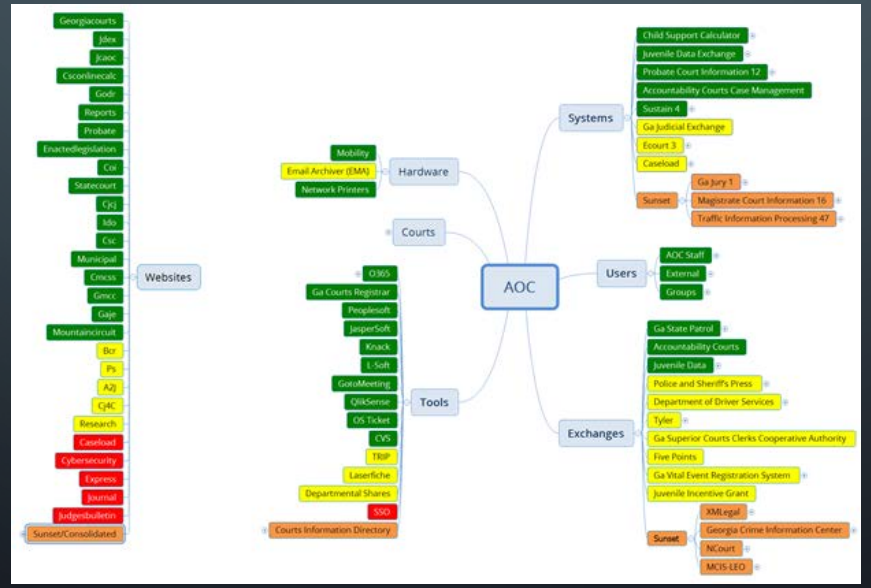
Week Four



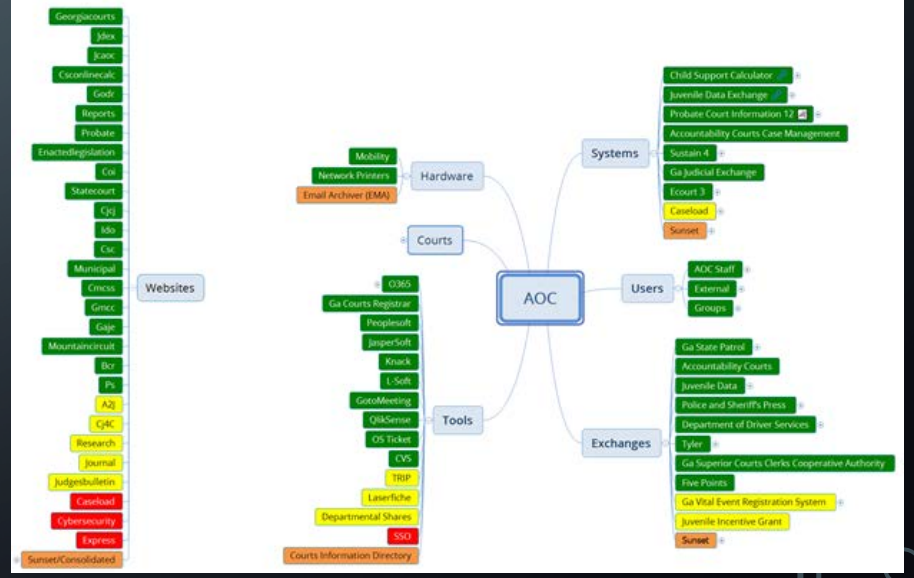
Week Five



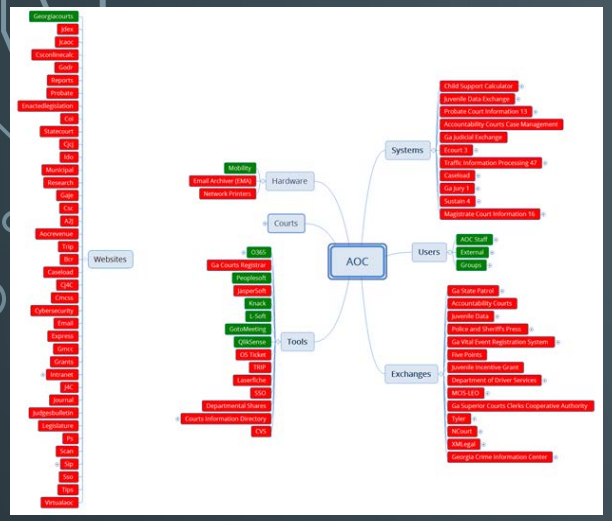
Week Six



Week Seven

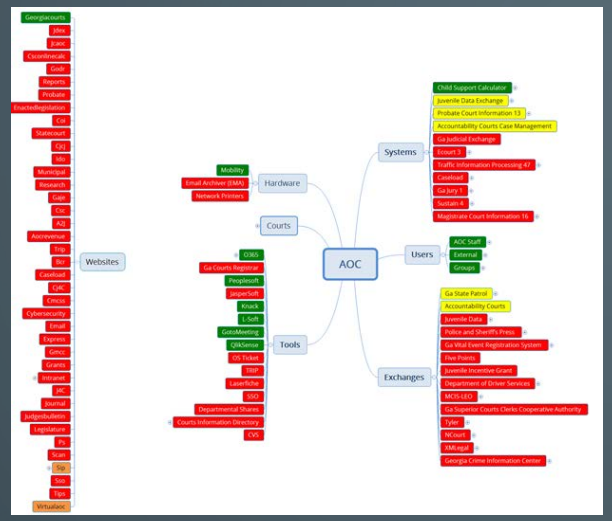


Week One

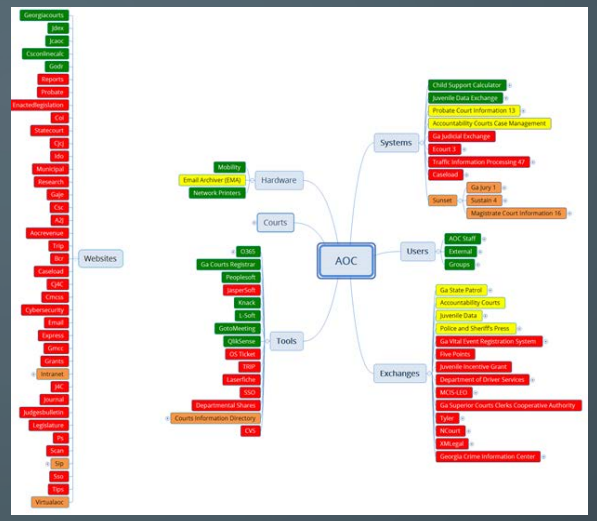


1. Law Enforcement has a different Job/Role
2. Communicate with Vendors and Partners ASAP
3. Determine the True Scope and Impact
4. Incident Response Plan Execution – Be Ready to Flex
5. Communication Plans. Who, What, Where, Why and How?
6. There is no Clear Distinction in Phases

Week Two

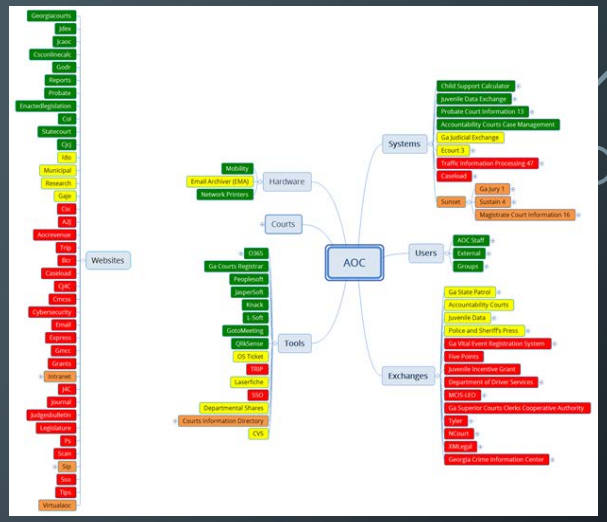


Week Three



1. Staff Management is Essential to Maintain Engaged Resources
2. Customer Management is Essential to Determine Next Steps
3. Media Wants Gory Details
4. Prioritization of Systems and Focus

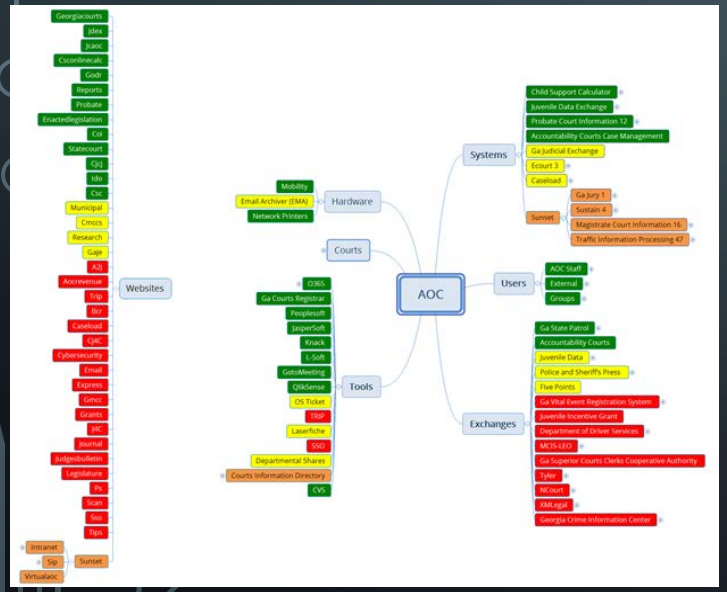
Week Four



1. Budgets Need to be Organized
2. Internal Communication becomes More Important
3. New Rules need to be Implemented and Communicated
4. Your Partners, Vendors and even Customers have a lot of Resources, Data, Back Ups
5. Email is a Treasure Chest
6. Started Making Tough Decisions on Legacy (Unsupported) Systems

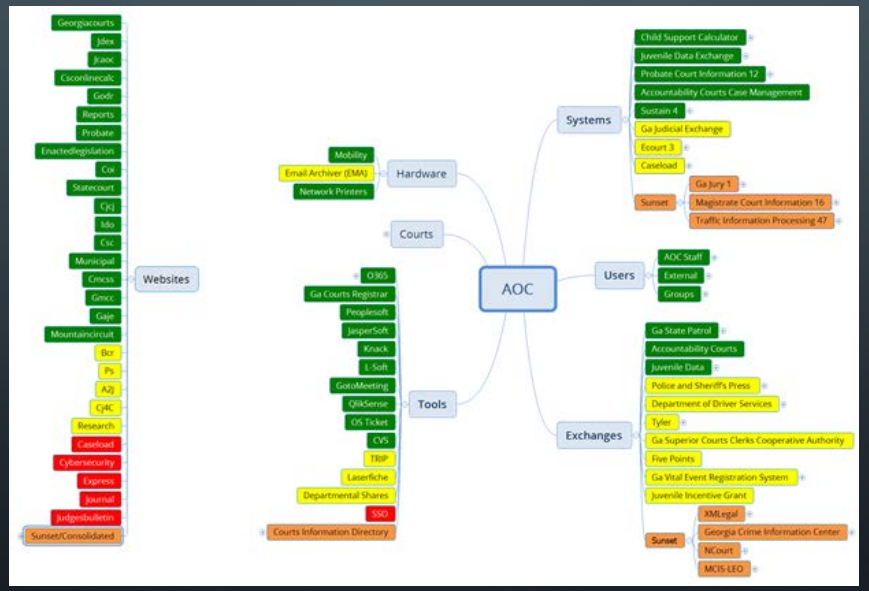
1. Staff Issues Related to Fatigue and Frustration
2. Thanks but No Thanks
3. Alternative Vendors / Processes for Customers

Week Five

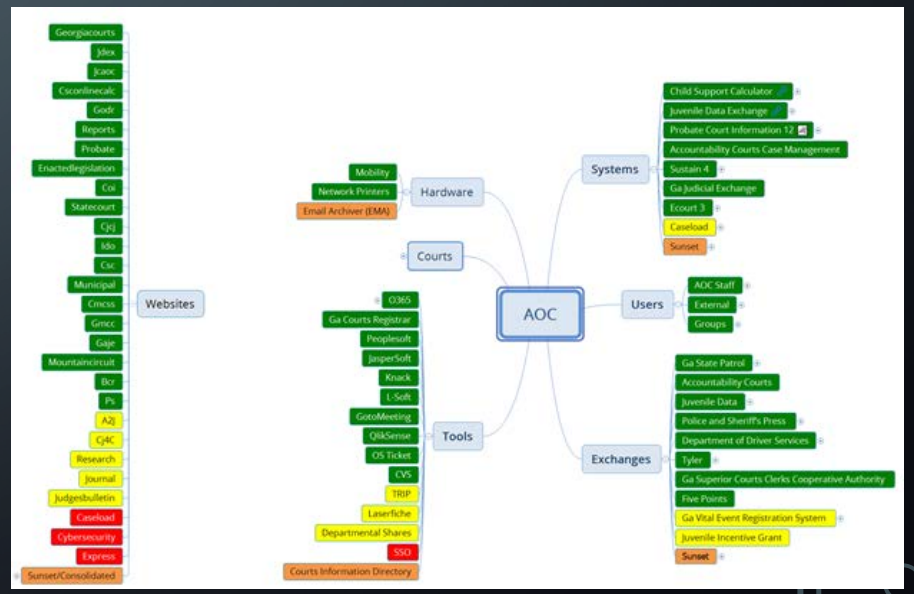


1. Determine Viability of Recovered Services
2. Determine what Vendor Services to Continue
3. Start pushing normalcy
4. Re-established exchanges, data sharing and communications
5. Expect questions and concerns from partners

Week Six



Week Seven



LESSONS LEARNED FROM THE 2019 GEORGIA ATTACK

THINK ABOUT THE PHASES AND PACE THE ACTIVITY. COMMUNICATION AND EXPECTATION MANAGEMENT WILL BE KEY WITH STAKEHOLDERS.

LEAN ON VENDORS / PARTNERS AND UTILIZE EMAIL FOR SPECIFIC RECOVERY EFFORTS. FOCUS ON WHAT IS TRULY LOST.

MAKE SURE ALL RESOURCES ARE DIRECTED TOWARDS THE DETERMINED OBJECTIVE. ITS NOT ALWAYS AS CLEAR AS YOU THINK.

EVERYONE BECOMES A COURT CONSULTANT. EVERYONE WITH AN ORGANIZATION ACCOUNT IS ON THE SECURITY TEAM.

TIME IS NOT JUST MONEY, ITS PEOPLE LIVELIHOODS. PREPARATION IS ESSENTIAL.

THINK ABOUT…

- A Cyberattack is not always a full blown, sensational takeover of an entire network.
- Not something you buy and plug in or install. Ransomware is typically not a single piece of software.
- Cannot ‘guarantee’ Security.
- Three Pillars of Preparation:
  - Controls
  - Segmentation
  - Recovery
- ~~“It’s Not If, it’s When”~~ “Not When, but How Bad?”

KENTUCKY'S INCIDENT RESPONSE PLAN

2014

- First developed in 2014 in response to brush with Ransomware #1

2015

- Revised after tabletop exercises

2019

- Revised again after incident

Ongoing

- A living document

TOOK A HOLISTIC VIEW OF SECURITY OPERATIONS

Security operations is part of what we call a *threat collaboration environment*, where members must actively collaborate to address cyberthreats affecting the organization's brand, business operation, and technology infrastructure on a daily basis.

Prevent: Defense in depth is the best approach to protect against unknown and unpredictable attacks. Diligent patching and vulnerability management, endpoint protection, and strong human-centric security (amongst other tactics) are essential.

Detect: There are two types of companies – *those who have been breached and know it, and those who have been breached and don't know it*. Ensure that monitoring, logging, and event detection tools are in place and appropriate to your organizational needs.

Analyze: Raw data without interpretation cannot improve security and is a waste of time, money, and effort. Establish a tiered operational process that not only enriches data but also provides visibility into your threat landscape.

Respond: Organizations can't rely on an ad hoc response anymore – don't wait until a state of panic. Formalize your response processes in a detailed incident runbook in order to reduce incident remediation time and effort.

THE SECURITY INCIDENT RESPONSE

PREPARE
Ensure the appropriate resources are available to best handle an incident.

ANALYSIS
Distill real events from false positives

ERADICATE
Eliminate the threat from your operating environment.

POST-INCIDENT ACTIVITIES
Conduct a lessons-learned post-mortem analysis.

DETECT
Leverage monitoring controls to actively detect threats.

CONTAIN
Isolate the threat before it can cause additional damage.

RECOVER
Restore impacted systems to a normal state of operations.

Process adapted from NIST SP 800-61 Rev. 2

SECTION OF THE CIRP

- Introduction and Purpose
- Cybersecurity Incident Response Team
- Communications
- Incident Response Procedures
- Glossary & Appendices

IDENTIFY ROLES AND TEAMS

COMMUNICATIONS PLAN

Define Operational Tempo Timeline

Who and to Whom, When and How Often, Contents and Methods

War Room Location and Procedures

INCIDENT RESPONSE

1. Incident Types
2. Incident Severity
3. Priorities (life & safety, critical operations and data, the rest)
4. Maps out Lifecycle, Tasks and Communications

SECOND BRUSH WITH RANSOMWARE

March 11, 2019

1:29 a.m.

Most recent exposure

SecureWorks reports activity on a server in the Azure Cloud

Investigation reveals a privileged account has been compromised

8:01 a.m.

Declare Potential Cybersecurity Incident

8:47 a.m.

Upon full investigation, INCIDENT is confirmed

PULLED OUT THE CIRP

- Containment efforts to maximum
- Notify the Cybersecurity Incident Response Team
- Establish the War Room – Call CIRT 10:30 a.m. meeting
- Cancel everything possible

WORKING THE CIRP

3:00 p.m.
- Full containment and eradication

7:00 p.m.
- Well into recovery

10:30 p.m.
- Looked like recovery was on auto-pilot

- CIRT patted themselves on the back and went home

BUT . . .

RETURN TO FULL SERVICE

8:00 a.m.	the replication failed
	War room augmented with engineers to manually push fix
9:00 p.m.	200+ servers manually “fixed” and all services restored
	Ample list of items for post-incident analysis compiled

Just under 44 hours

LESSONS LEARNED IN KENTUCKY AND CHANGES IMPLEMENTED

- Enable Multi-Factor Authentication (MFA)
- Institutionalize Information Security Practices, Augment InfoSec Team
- Audit Select Aspects (Account Permissions, Stale Accounts, Backups etc.)
- Join Groups and Mailing Lists (MS-ISAC, KnowB4, etc.)
- Formalize Business Impact Analysis and Business Continuity Plans
- Has helped as turnover continues in the Tech space

LESSONS LEARNED - ARKANSAS

EDUCATION

POLICY

TECHNOLOGY

PREPAREDNESS

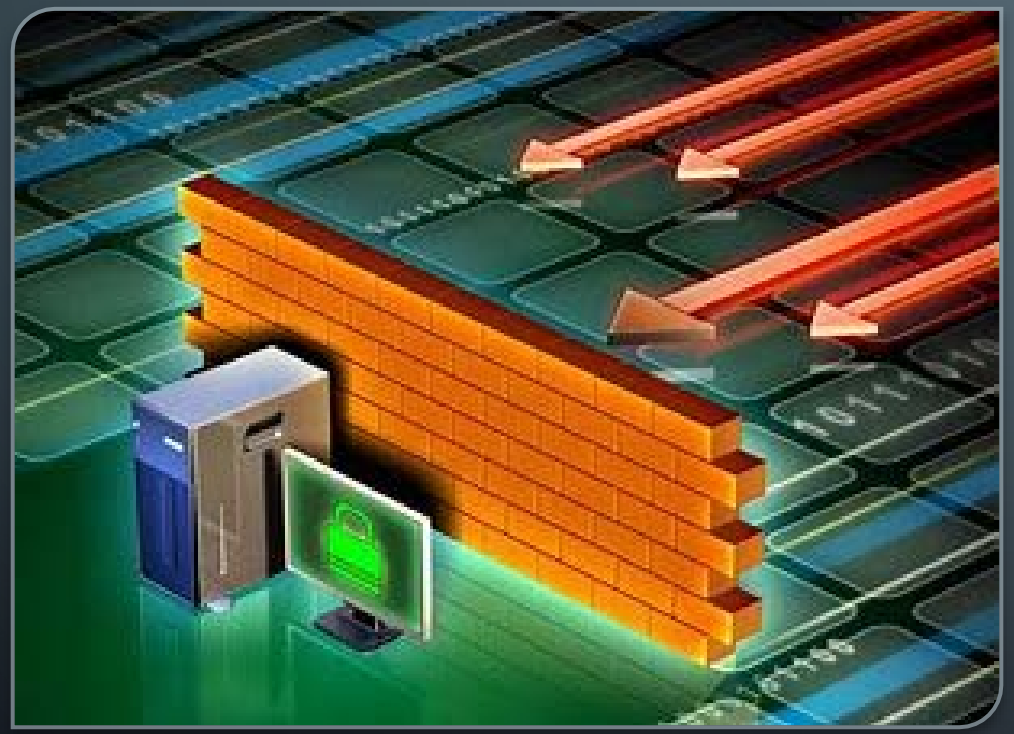
EDUCATION

- Cybersecurity training for IT staff
- Cybersecurity awareness training for court staff
- Rolling out KnowBe4

POLICY

- VPN clients
- Personal devices
- Password policies
- Software policies
- Patching and update policies
- Remote work

TECHNOLOGY

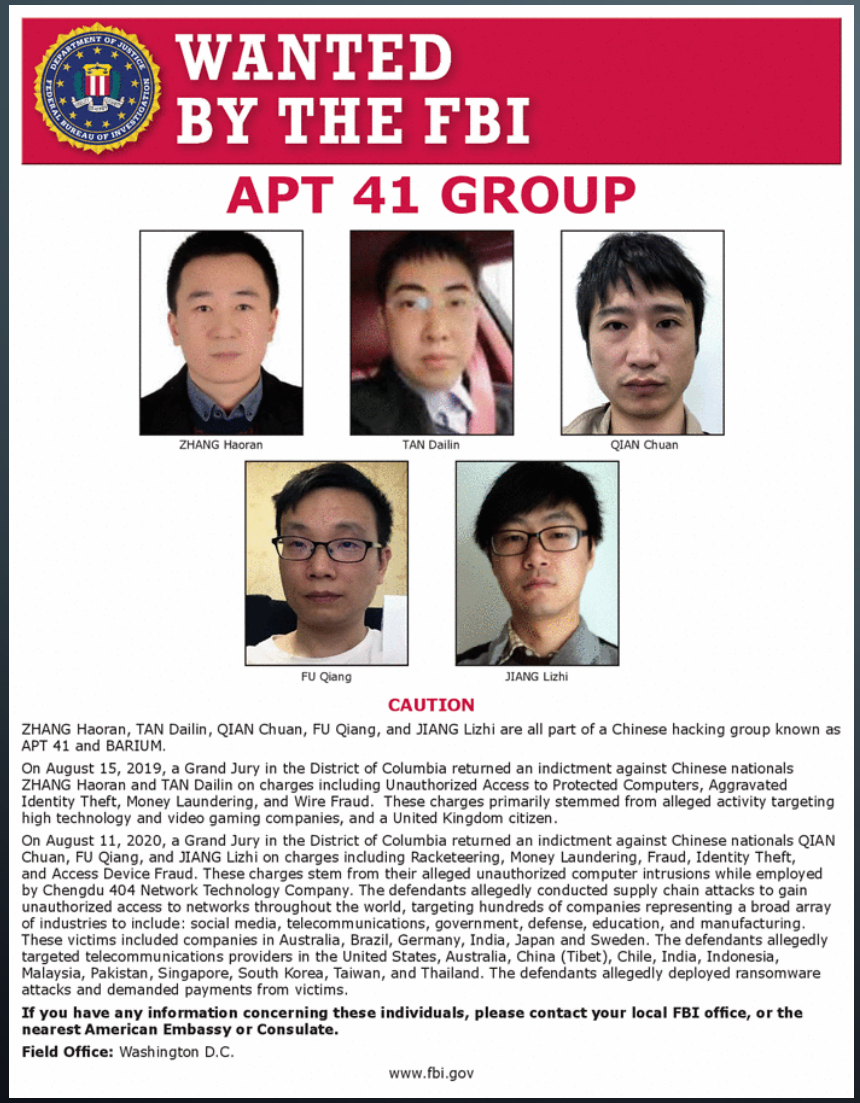


- Invest in technology security professionals
- Scanning technologies
- System Incident and Event Management technologies
- Keep hardware and software current
- Cloud technologies

PREPAREDNESS

- Incident response planning
- Disaster recovery
- Continuity of operations
- Cyber insurance

ARKANSAS SUMMER 2021



WANTED BY THE FBI

APT 41 GROUP

ZHANG Haoran | TAN Dailin | QIAN Chuan

FU Qiang | JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

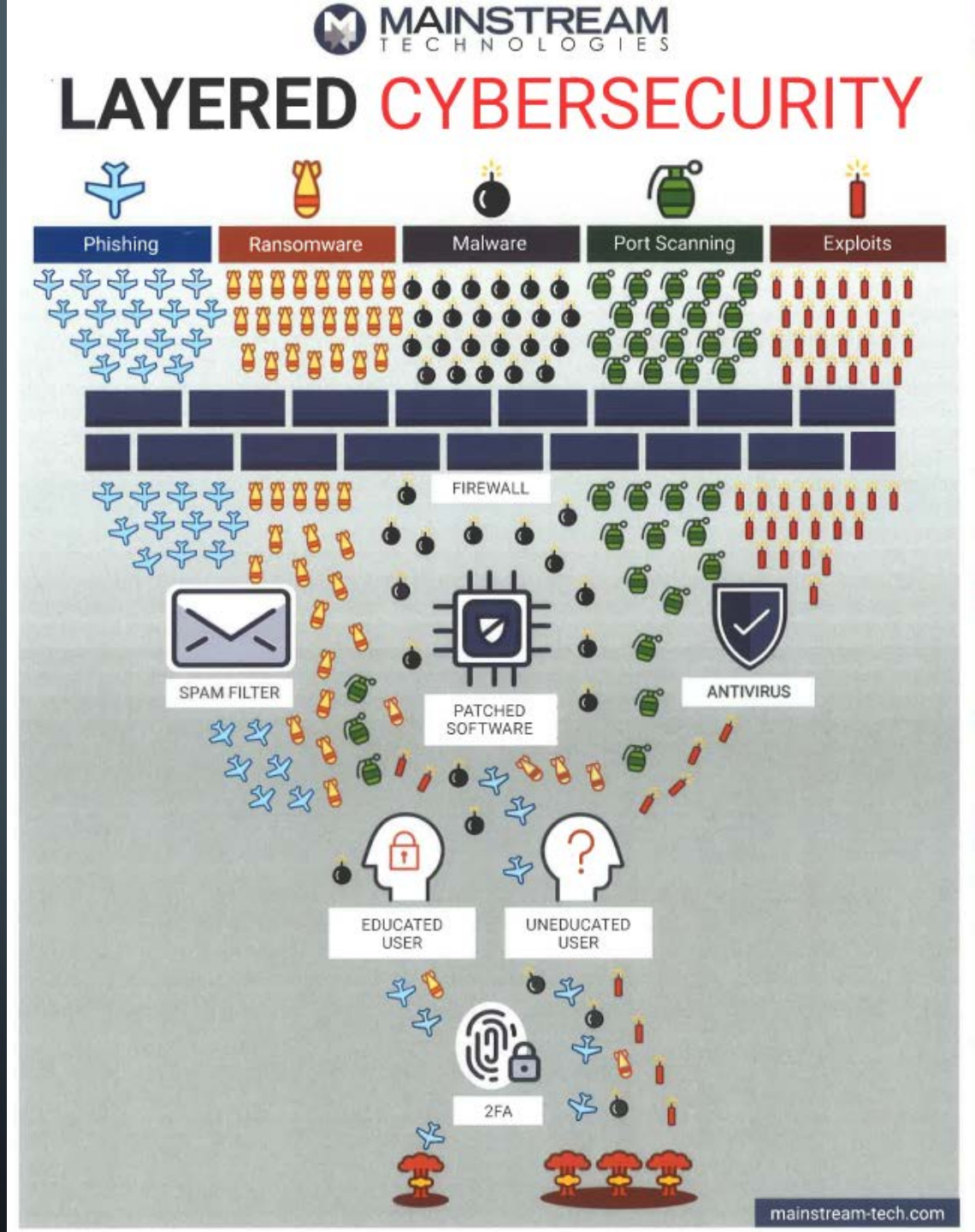
On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

- Call from State CIO
- Mandiant Suspect Traffic
- Activated Response Plan
- Activated Cyber Claim
- Forensic Investigation
- Conclusion


MAINSTREAM
TECHNOLOGIES
LAYERED CYBERSECURITY
Phishing
Ransomware
Malware
Port Scanning
Exploits
FIREWALL
SPAM FILTER
PATCHED SOFTWARE
ANTIVIRUS
EDUCATED USER
UNEDUCATED USER
2FA
mainstream-tech.com

CIS Center for Internet Security

CIS Controls Version 8

Implementation Groups

The CIS Controls are internationally recognized for bringing together expert insight about threats, business technology, and defensive options into an effective, coherent, and simpler way to manage an organization's security improvement program. But in our experience, organizations of every size and complexity still need more help to get started and to focus their attention and resources.

To that end, we developed Implementation Groups (IGs). IGs are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls), that they need to implement. There are 153 Safeguards in CIS Controls v8.

Every enterprise should start with IG1. IG1 provides effective security value with technology and processes that are generally already available while providing a basis for more tailored and sophisticated action if that is warranted. Building upon IG1, we then identified an additional set of Safeguards for organizations with more resources and expertise, but also greater risk exposure. This is IG2. Finally, the rest of the Safeguards make up IG3.

These IGs provide a simple and accessible way to help organizations of different classes focus their scarce security resources, and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Total Safeguards **153**

Basic Cyber Hygiene

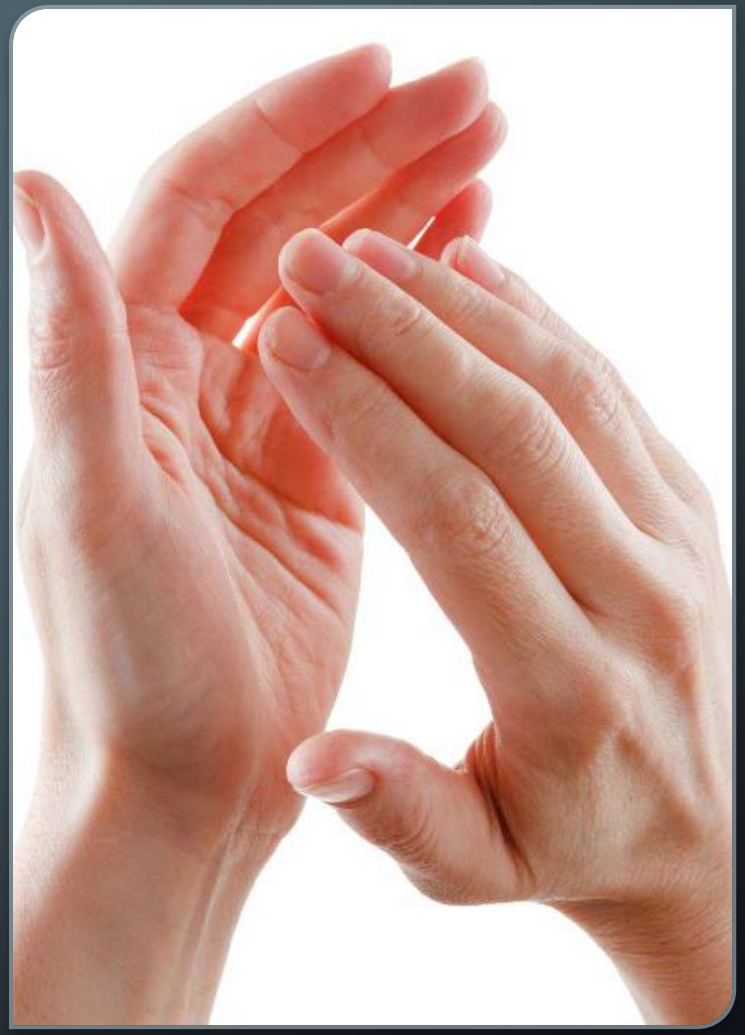
CIS Controls v8 defines Implementation Group 1 (IG1) as basic cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

For more information, visit www.cisecurity.org/controls.


Let's
Talk

CONTACTING YOUR PANEL

- **Charles Byers** 502-573-2350, charlesbyers@kycourts.net
- **Jorge Basto** 678-493-6545, jlbasto@cherokeega.com
- **Tim Holthoff** 501-410-1919, tim.holthoff@arcourts.gov



ADDITIONAL RESOURCES

- JTC Resource Bulletin Responding to Cyber Attack
  https://tinyurl.com/y2x7f634
- National Cyber Incident Response Plan
  https://www.us-cert.gov/ncirp
- Court Information Technology Officers Consortium (CITOC)
  http://www.citoc.org/