Cyber Security

“ There are only three types of organizations: those that have been hacked, those that will be hacked, and those that are being hacked right now and don’t know it”

Why Are We Here?

EVERYONE HAS A PLAN UNTIL THEY GET PUNCHED IN THE FACE.

Mike Tyson

- Not IF, but WHEN
- What will you tell the news media?
- 21 connected devices per household[1]

Source: 1. J. D. Powers. 2. Ponemon Institute

6 Fast Facts about Cyber Security

$ 7.3 million

Average cost of a U.S. data breach[1,4]

47%

Of companies had at least 1000 files with sensitive data open to EVERY employee[2]

206 days

A data breach goes undetected on average[1]

64%

Of breaches are reported by a third party[3]

58%

Of former employees retain access to company networks after leaving[4]

7/10

Organizations not prepared to respond to a security incident

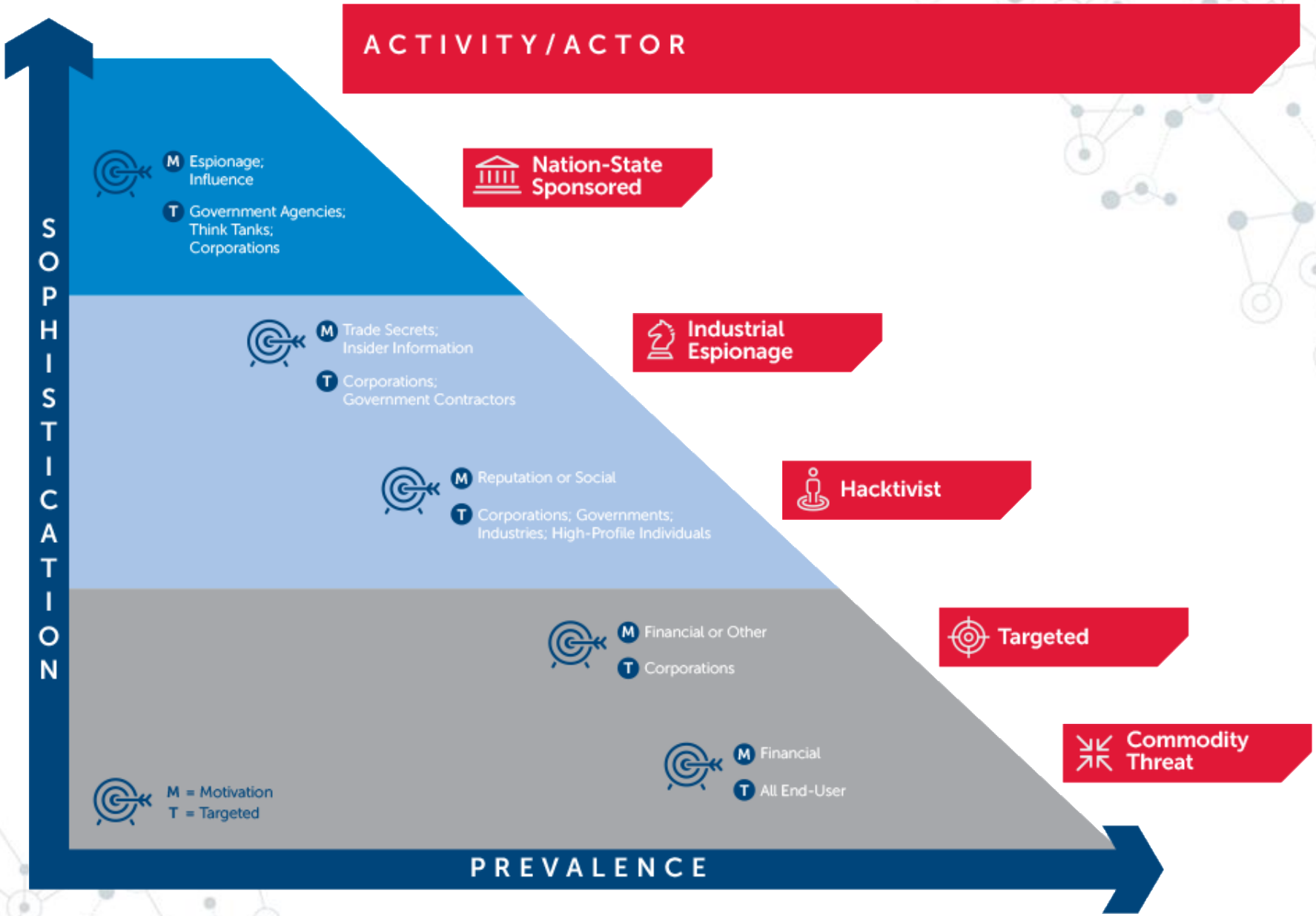
1. Ponemon Institute – 2017 Cost of a Data Breach Report. 2. Varonis. 3. FireEye - 2018 M-Trends Report. 4. Infosecurity and OneLogin. 5. gemalto 6. Hiscox Cyber Risk Report

Organizational Digital Footprint

- Social media
- Public facing websites
- Interactive portals - LMS
- Cloud storage services
- Cloud application services
- Email
- Guest/vendor accounts
- POS terminals
- Integrated systems
- SCADA/Building automation
- Mobile devices + BYOD
- 3rd party and supply chain

1.
Threat Landscape:

Tools, Techniques, Procedures and Adversaries



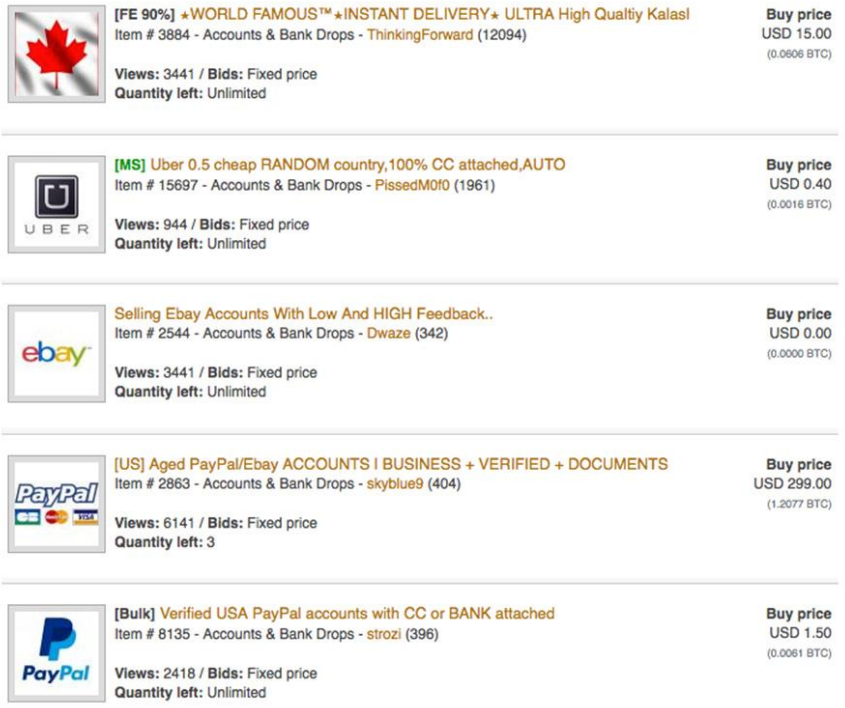
Source: Securew orks

Phishing

- Spear phishing
- Whaling
- Vishing
- Phishing types
  - Clickbait
    - Credential theft
    - Malware delivery
  - Wire fraud
  - W2 fraud
  - Payment/order scam
  - Gift card fraud
  - Sextortion
- Initial contact – more targeted

Credential Theft

- Credentials are easy to steal
- Re-use adds to problems
- Most do not use MFA
- Effective page cloning
- Good resale value
  - Adult sites
  - Netflix, Hulu
  - Social media
  - Gaming



Ransomware

- Successful and easy
  - Pre-built kits
  - Ransomware-as-a-Service
- Shift from scareware
  - Doxware, sextortion
- User to entity focused
  - Targeted
  - Traversing
- 3rd party drive-by, email
- 2nd stage – data breach

“Ransomware is more about manipulating vulnerabilities in human psychology than the adversary’s technological sophistication.”

James Scott

Senior Fellow,

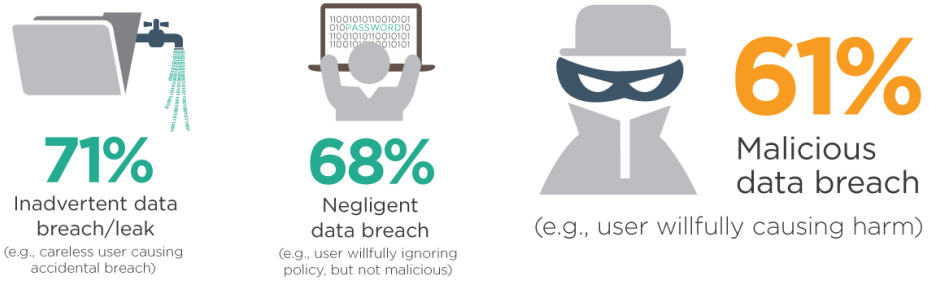
Institute for Critical Infrastructure Technology

Cryptojacking

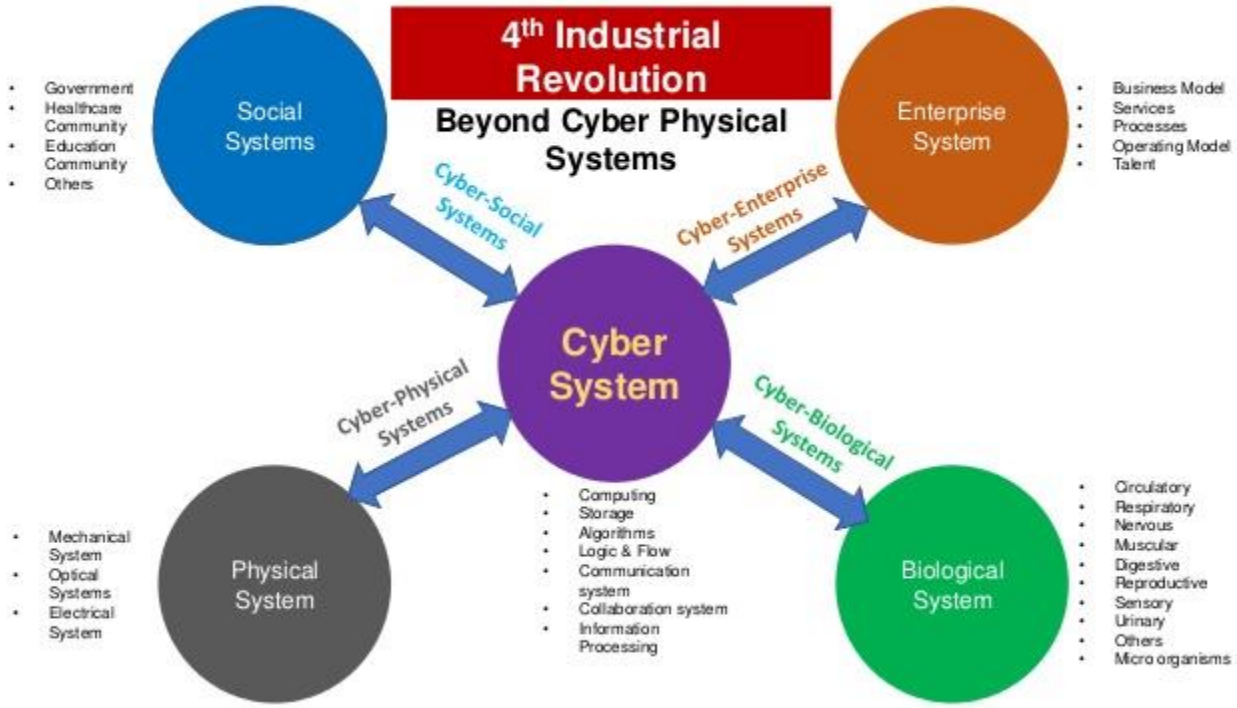
- On the rise
- Browser or device based (malware)
- Smominru Botnet – $3.6 million in 5 months
- Kits for $30
- Less chance of getting caught
- Using leaked NSA exploits
  - But most are unpatched vulns

Insider Threat

- Disgruntled and former employees
- Trusted by default – longest to detect
- Data for ransom, resale, misuse, revenge
- Exfiltration via common methods
- Espionage – rising trend
  - Privilege creep



Cyber-Physical Attacks



Geo-Political Influence – Hacking Elections - Hacktivism

- Shift from random defacements
- Government sponsored
- 90 billion attempts in 30 days – one city
- NotPetya[1] - $ 3 billion, Chernobyl, 76 ports

WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS

Boris Alekseyevich Antonov | Dmitriy Sergeyevich Badin | Anatoliy Sergeyevich Kovalev | Nikolay Yuryevich Kozachek | Aleksey Viktorovich Lukashev | Artem Andreyevich Malyshev

Sergey Aleksandrovich Morgachev | Aleksandr Vladimirovich Osadchuk | Aleksey Aleksandrovich Potemkin | Ivan Sergeyevich Yermakov | Pavel Vyacheslavovich Yershov

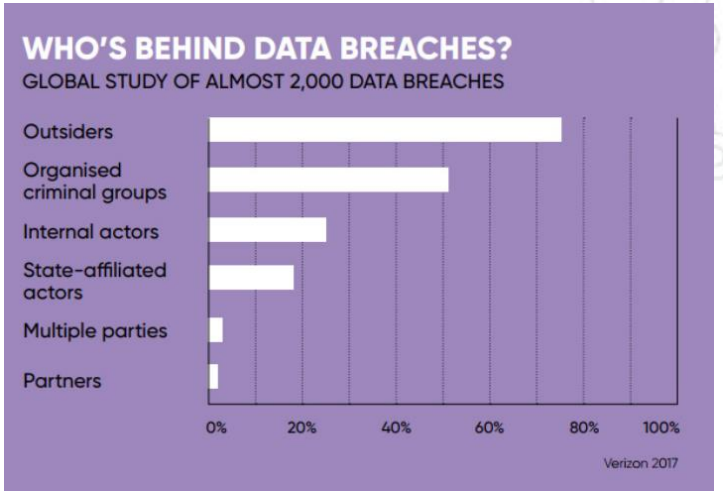
DETAILS

On July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 United States (U.S.) elections. The indictment charges 11 defendants, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Nikolay Yuryevich Kozachek, Aleksey Viktorovich Lukashev, Artem Andreyevich Malyshev, Sergey Aleksandrovich Morgachev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, Ivan Sergeyevich Yermakov,

Source: 1. Cyber Risk Outlook 2018

Actors

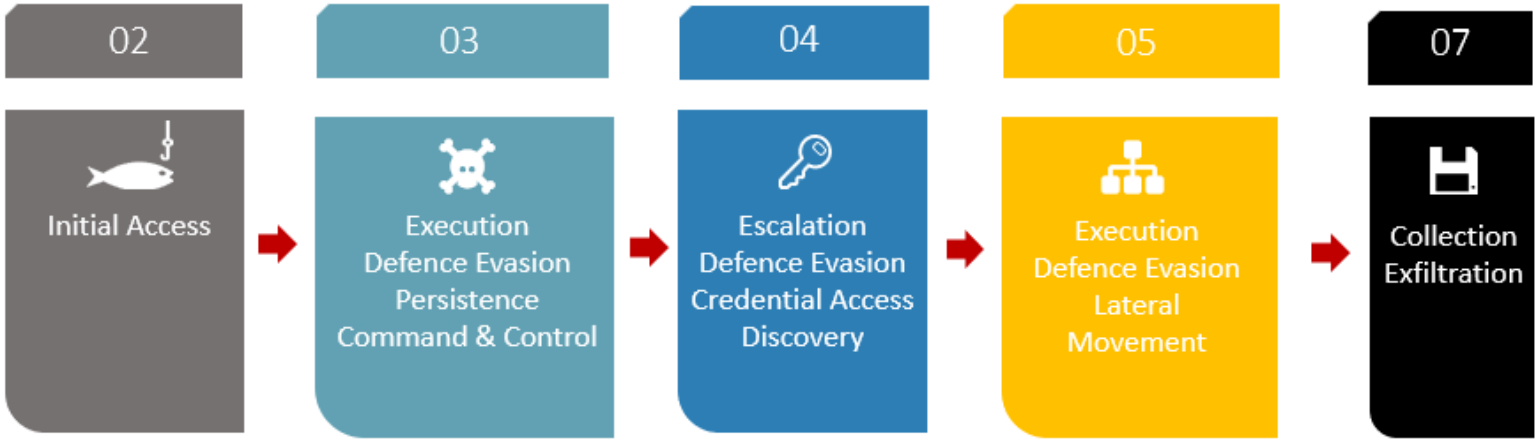
- APTs
  - Government, funding
  - Targeted attacks
  - Fancy Bear
- Financially motivated
  - Cryptojacking, ransomware
  - Wire / transaction fraud
  - DDoS – Swedish transportation, AWS
  - ATM / POS hardware
- Insiders



2.
Defense in Depth:

Know what you are protecting and how

Cyber Kill Chain



“Cyber Security is no longer an IT problem.

It’s a business problem.”

Protect Your Organization

Business

1. **Education and Awareness**
2. Take compliance seriously
3. Data classification
4. Asset prioritization – ”crown jewels”
5. Business process for on/off-boarding of employees
6. Regular review of user roles and access they need
7. Business Continuity and Disaster Recovery plans
8. Establish **Culture of Security**

Technology

1. Regular patching – OS and apps
2. Restrict admin rights
3. Role-based access control
4. Application whitelisting
5. Data/device encryption
6. Layered defense
   - Firewall + HIPS + NIPS + AV + WAF + DLP + SEIM
7. URL/category/location blocking
8. USB port restrictions
9. MFA

Data Governance

1. Identify what data types your organizations collects, generates and stores
   - PII, ePHI, student educational records, federal datasets, credit card
2. Identify which regulations apply to you
   - FERPA, FISMA, HIPAA, PCI
3. Know where your data is
   1. Remote users
4. Follow NIST standards

Make a Plan - BEFORE

- Have written emergency plans and procedures before the incident
  - Cyber Incident Response Plan
  - SOPs for handling specific threats
    - Breach, ransomware, denial of service, etc.
    - Don’t get too specific
  - Communications
    - Designated PIO
    - Communication templates
- Designate an IR team
  - Security, Legal, Privacy, IT, PIO, facilities

Make a Plan - BEFORE

- Conduct training and table top exercises
  - What will you do while things are down?
  - What are your strength gaps?
- Who is going to attack you?
- Phish your users
- Pre-plan a budget and communicate to leadership
- Consider cyber liability insurance
- Have MOUs in place with partner organizations
- How quickly can you get your backups?
  - Test them!

Train your employees

If you do one thing after today...

3.
Incident Response:

You have been pwned, what to do now?

Oh, NO. Something Is Wrong

- Don't panic
- Assess the situation
  - Is it a really a compromise or is it a malfunction?
- Minimize the damage
  - Disconnect from the network or isolate
  - DO NOT turn off the device(s)
- Understand the scale/criticality
- Collect evidence - if you have the resources
- Call for help

Incident Prioritization

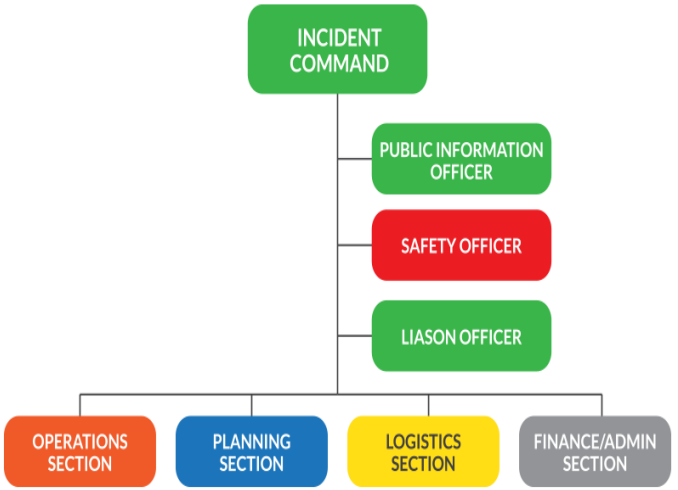
Incident Priority **Impact: People & Service** **Severity: Time**			**Severity**		
			3-Low User cannot perform a portion of their duties.	**2-Medium** User cannot perform critical time sensitive functions	**1-High** Major portion of a critical service is unavailable
Impact	**3-Low**	• One or two personnel • Degraded Service Levels but still processing within SLA constraints	**3-Low**	**3-Low**	**2-Medium**
	2-Medium	• Multiple personnel in one physical location • Degraded Service Levels at or below SLA constraints • Cause of incident falls across multiple functional areas	**2-Medium**	**2-Medium**	**1-High**
	1-High	• All users of a specific service • Personnel from multiple agencies are affected • Public facing service is unavailable • Any item listed in the Crisis Response tables	**1-High**	**1-High**	**1-High**

Forensic Evidence

- Logs
  - Perimeter, IDS/NIPS
  - Web server and application
  - Device – servers and workstations
  - End-point management – AV, HIPS
  - Mail server, including messaging
- Images
  - Server and workstation disk images
  - Memory images
  - Virtual disks and memory – vmdk, vmem
- Samples

Who Is In Charge?

- Do you know who is in charge of the incident?
- Who is on your IR team?
- Do we call our people in?
- Do we call law enforcement?
- What do I tell my boss?
  - Status updates – scheduled
- What do we tell our customers (students, parents, residents)?



After the Initial Stage

- As much as you try to keep this quiet, it will not work
  - Have your communication plans and strategy worked out
- Recover systems and services
  - This will cost you - Atlanta

Date	Notifier	H	M	R	L	Domain	OS
2018/10/11	ErrOr SquaD					blockchain.usc.edu/optimus.txt	Linux
2018/10/09	Sadistic Killer					cbsugobii11.tc.cornell.edu/elF...	Linux
2018/09/20	zakiloup					www.elinc.edu/ASO.html	Linux
2018/09/17	darkshadow-tn					www.phdl.pitt.edu/modules/mod_...	F5 Big-IP
2018/09/10	KingSkrupellos					c006b.orth.uic.edu/support.htm	FreeBSD
2018/09/05	Isal Dot ID					uofac.edu/king.php	Linux
2018/09/04	Sh0uT0u7					gradbursar-p1.stern.nyu.edu/tc...	Unknown
2018/09/04	Sh0uT0u7					zimm-33.unm.edu/tcp_summary.htm	Unknown
2018/09/02	Mr.ToKeiChun69					westhavenuniv.edu/robots.txt	FreeBSD
2018/08/30	DexmoD	H	M			bapuji.bapujidental.edu	Linux
2018/08/27	ErrOr SquaD					footsoldier.uga.edu/optimus.txt	F5 Big-IP
2018/08/23	R3dh34d		M			alumni.mesin.upi.edu/wp-conten...	Linux
2018/08/23	Virus003					naqaba.najah.edu/za.txt	Linux
2018/08/15	Ayyıldız Tim	H				nationaltrainingschools.edu	Win 2008
2018/08/15	Lulz.Father					silc.asu.edu/sites/default/fil...	Linux
2018/08/15	Black_TeamX			R		library.wcsu.edu/wcsu/Distance...	Unknown
2018/08/15	KingSkrupellos					craft-fair.mit.edu/sites/defau...	FreeBSD
2018/08/15	black_teamx		M			digitalhumanities.stanford.edu...	F5 Big-IP
2018/08/15	KingSkrupellos			R		cepa.stanford.edu/sites/defaul...	Win 2012
2018/08/15	KingSkrupellos					music.stanford.edu/sites/defau...	F5 Big-IP
2018/08/15	KingSkrupellos			R		cervantesobservatorio.fas.harv...	Unknown
2018/07/25	KEC0A_T3RBANG		M			jbi.stikom.edu/test.php	Linux
2018/07/24	KEC0A_T3RBANG		M			gerdu.stikom.edu/test.php	Linux
2018/07/24	KEC0A_T3RBANG		M			labkom.stikom.edu/test.php	Linux
2018/07/24	Guardiran Security Team					isso.cornell.edu/index.html	Linux

Post-Incident

- Close security gaps
- Write your report
  - Executive, technical, public
- Conduct a post-mortem
  - SWOT analysis
  - What went well and what went poorly
- Document lessons learned
- Adjust plans, policies and procedures

Who to Call For Help?

- Local Police
  - Make a report – start process
  - Lack of resources
- FBI
  - Investigations
  - Long timeline
  - May not be able to prosecute
  - www.ic3.gov
- DHS Fusion Center
  - Intelligence collection
  - Contact resource
  - gcfc@gcfc.org

Thank you!