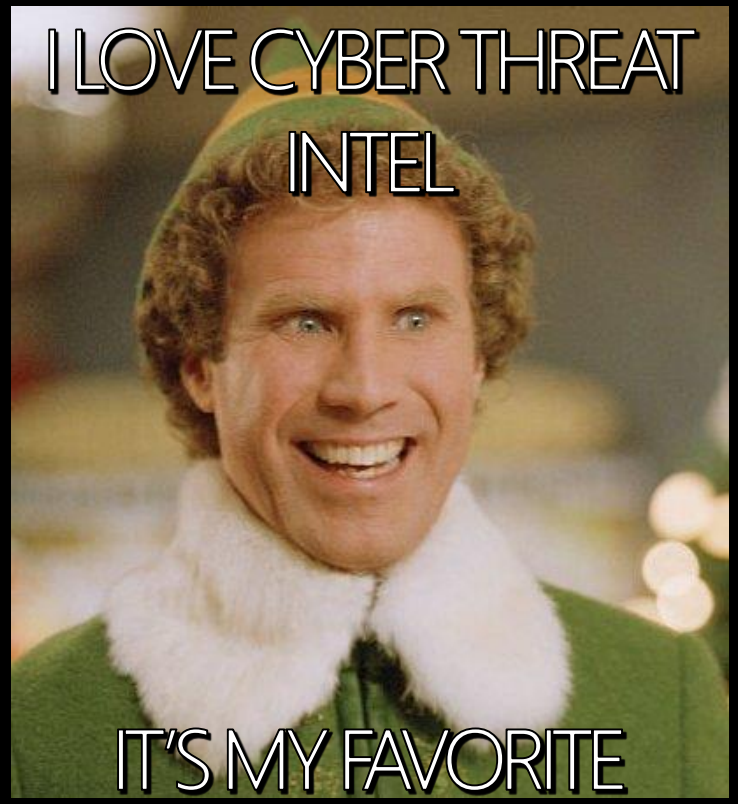
What is Cyber Threat Intelligence?



John Stoner

Cyber Threat Intelligence Analyst

Mr. Stoner has over 18 years of experience in the national security and defense sector working a variety of roles, including most recently as a Cyber Threat Intelligence Analyst, Cyber Counterintelligence Analyst and Cyber Instructor.

His work experience includes IT, instruction and course design, cyber exercise and testing, penetration testing, intelligence collection, threat support, SIGINT (Signals Intelligence), and Cyber Operations. He holds A+, Net+, CEH, CHFI, CEI, CISD, CASP and CISSP and a Computer Studies degree from UMUC.

He is a huge soccer fan and coaches youth soccer. You may see his Zombie response car at unnamed government facilities.

By secretly joining the Army at 19 years old, he got started in military intelligence and then eventually government cybersecurity.






Ronnie Obenhaus

Cyber Threat Intelligence Analyst

Ronnie is a US Army Veteran and is not good at providing additional facts for his bio. He is married and has several children (amount variable). He may or may not have pets, but seems to like dogs.

He currently is a DOD civilian at a federal cyber agency.

Ronnie has met all the famous people, as you can see.

Please visit his movie blog:

http://redeemingbadmovies.com/

Information Technology (IT)

- Setting up computer networks
- Installing Operating Software and programs
- Keeping systems and networks functioning
- Configuration of network devices (routers, firewalls, wireless access points)
- Updating (Patching) systems
- Help Desk tasks
- Integration of new applications
- Programming & Software Development
- Cloud Architecture and configuration

Cybersecurity

- Keeping computer systems secure
- Ensuring proper security configuration
- Security policy creation and enforcement
- Involved with compliance and auditing
- Technical testing of network security (Vulnerability testing/Penetration testing)
- Criminal/Investigative Cyber Analysis
- Forensic Analysis of systems/media/malware
- Proactive analysis of potential cyber threats
- ***Cyber Threat Intelligence (CTI)***

What is Cyber Threat Intelligence?

- Cyber Threat Intelligence (CTI) falls into two broad categories

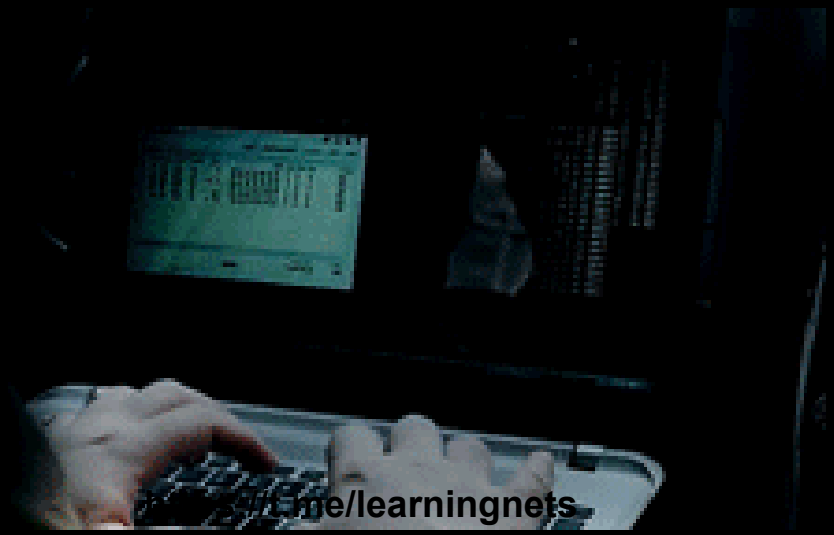
- Operational intelligence is produced by computers
  - Automatic Detection of DDOS (Distributed Denial of Service)
  - Heuristic or Anomaly based detection by IPS (Intrusion Prevention System)
  - Blacklisting/Whitelisting tactics

- Strategic intelligence is produced by human analysts
  - Identifying and Analyzing threats to the core assets
  - Identify threat trends in the same sector of business or government
  - Assist in the cyber education of employees
  - Makes defensive recommendations
  - Stays abreast of emerging changes in attacker techniques
  - *Study attacker TTPs (Tactics, Techniques, and Procedures)*

Okay Okay, so just tell me what is Cyber Threat Intel already!

- CTI is the output of analysis based on identification, collection, and enrichment of relevant data
- Raw data and information do not constitute intelligence
- Analyzed data and information will only qualify as intelligence if the result is directly attributable to identified goals or operational requirements

- Much in the realm of CTI has to do with Advanced Persistent Threats (APT)
- APTs are generally more sophisticated cyber actors that have nation-state association



So what are these CTI human analysts like?

Gotta have the basics first!

ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

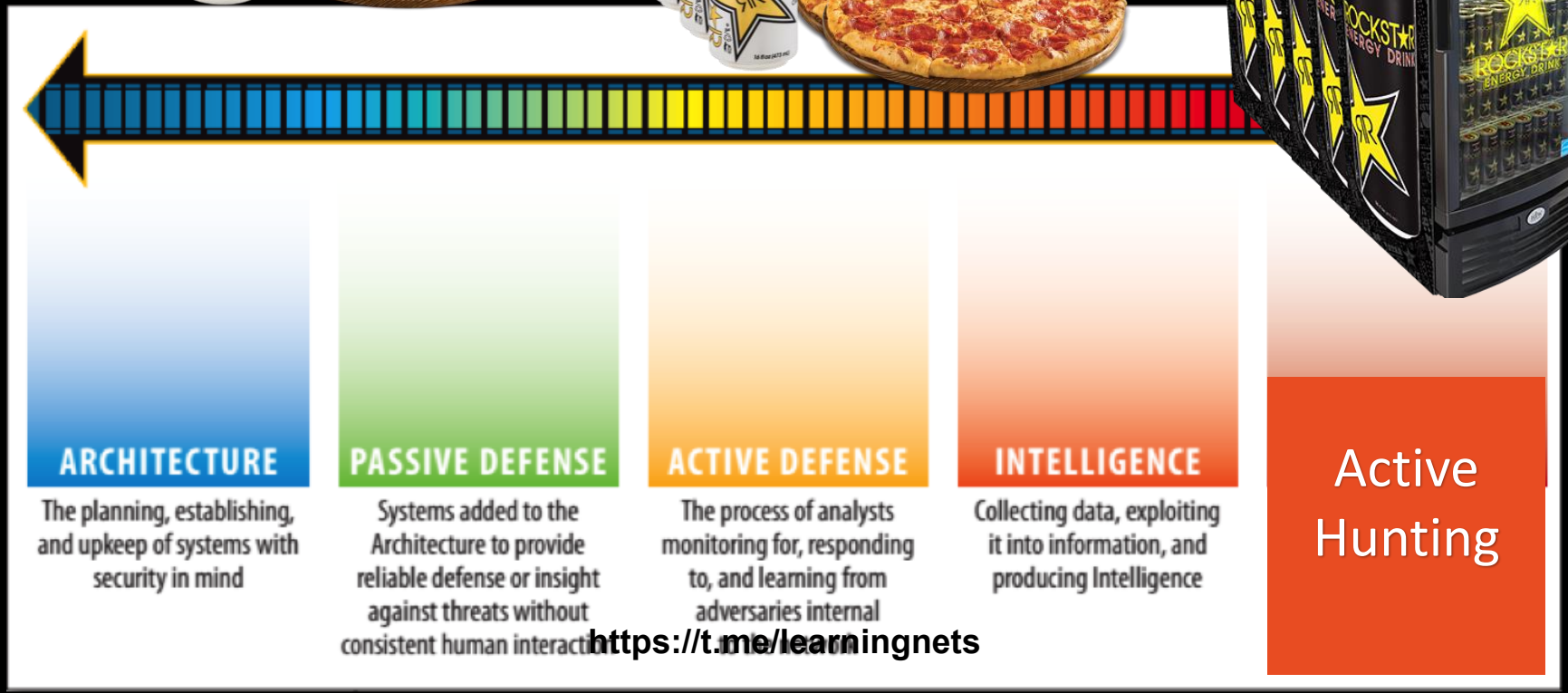
INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

Active Hunting

Don’t be a 1 pizza target!

- **Amount of pizza and energy drinks required for initial foothold in victim network**



Reconnaissance

Weaponization

Delivery

Exploitation

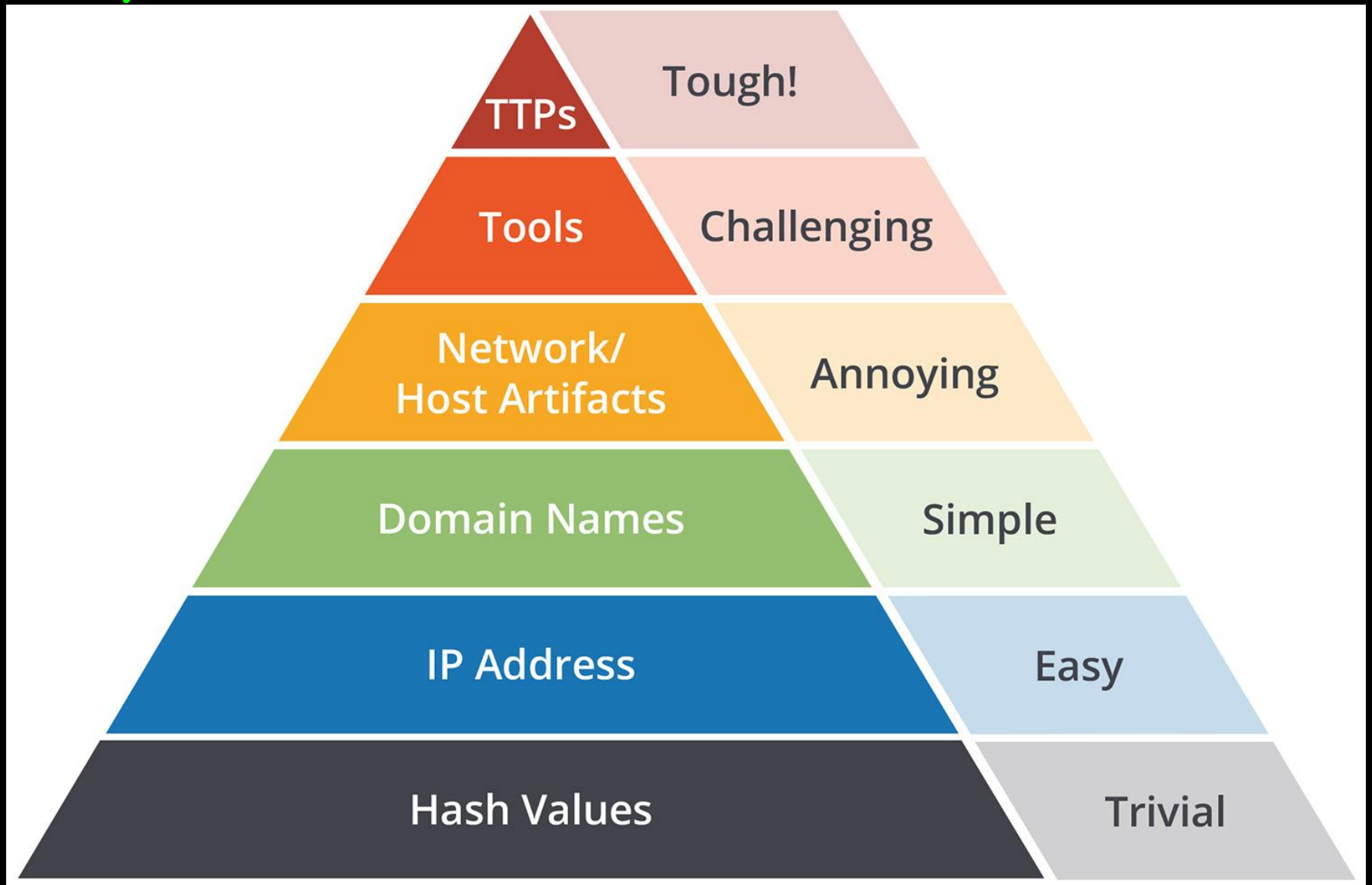
Installation

Command & Control

Actions on Objective

Okay, so if you have the right people this is easy, right?

Bianco's Pyramid of Pain



Source: David J. Bianco, personal blog

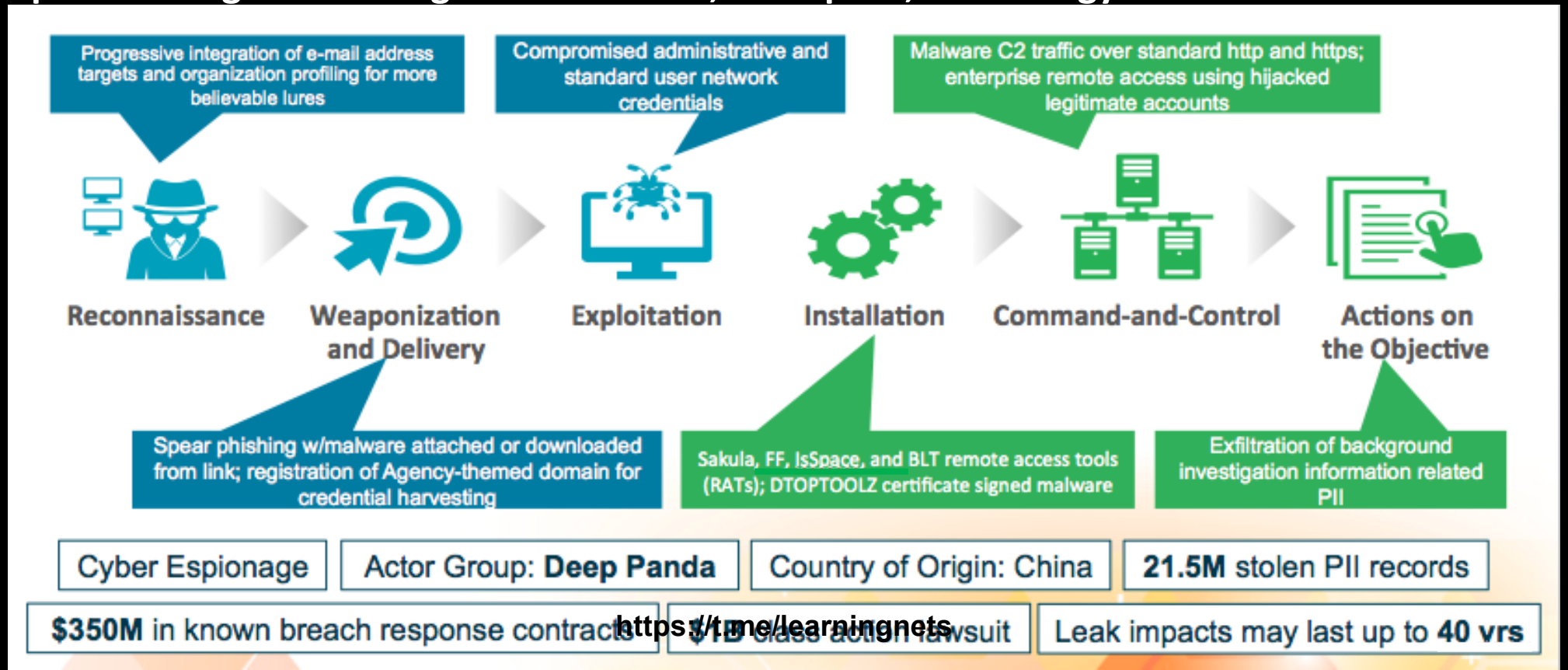
In Russia cyber hacks you

- APT 28 – aka Sofacy and Fancy Bear
- Suspected Russian APT 28 is a state sponsored group active since 2007 Most APT 28 malware was compiled between Monday – Friday from 0800 – 1800 in UTC+4. This parallels working hours in Eastern Europe, Moscow, and Saint Petersburg
- APT 28 relies upon spear phishing or zero-day vulnerabilities to initially compromise victim systems. Spear phishing emails often originate from a typosquatted mail server
- Suspected to be behind the VPNFilter Malware

- APT 29 - aka CosmicDukes, Cozy Bear
- Suspected Russian APT 29 is an adaptive and disciplined threat group that hides its activity on a victim's network, communicating infrequently with obfuscation to resemble legitimate traffic
- By using legitimate popular web services, the group can also take advantage of SSL connections, making detection difficult
- APT 29 is one of the most evolved and capable threat groups. It deploys new backdoors to fix its own bugs and add features

Deep Panda, APT 19, Shell Crew, PinkPanther

- Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications
- The intrusion into Anthem has been attributed to Deep Panda and they are suspected culprits for the OPM hack as well
- Deep Panda began attacking the healthcare, aerospace, and energy sectors around 2012



Intelligence Driven Network Defense

Don’t say goodbye – say until we meet again

- Cyber Threat Intelligence (CTI) is a specialized niche field
- Human analysts are critical (and are poorly depicted on TV)
- Focus on core aspects of network defense first
- Advanced Persistent Threats (APTs) – scary stuff
- Cyber Kill Chain
- Intelligence Driven Defense

Cyber Threat Intel Resources and Links

Original Mandiant APT 1 Report

Rob 'mubix' Fuller - Getting Started in INFOSEC (collection of sites and reference documents)

ICIT Briefing PDF report: Know your Enemies

Ben Benavides Open Source Intelligence (OSINT)2oolKit On The Go

Recorded Future: Understand Your Attacker: A Practical Guide to Identifying TTPs With Threat Intelligence

Attribution of Malicious Cyber Incidents: From Soup to Nuts By Herbert Lin

Cyber Counter Intelligence: An attacker-based approach - Video

Inside the power grid hack in Ukraine

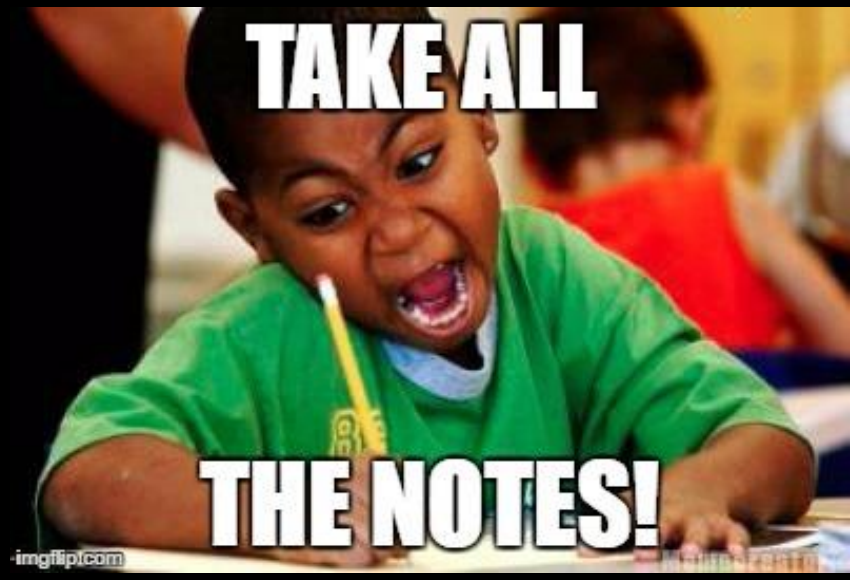
Dell Secure works – Lifecycle of an APT

Advanced Persistent Threats: A Symantec Perspective

Google Doc of Open Source (OSINT) on many APT groups

The real story of NotPetya – a Russian Cyber Attack (Wired.com)

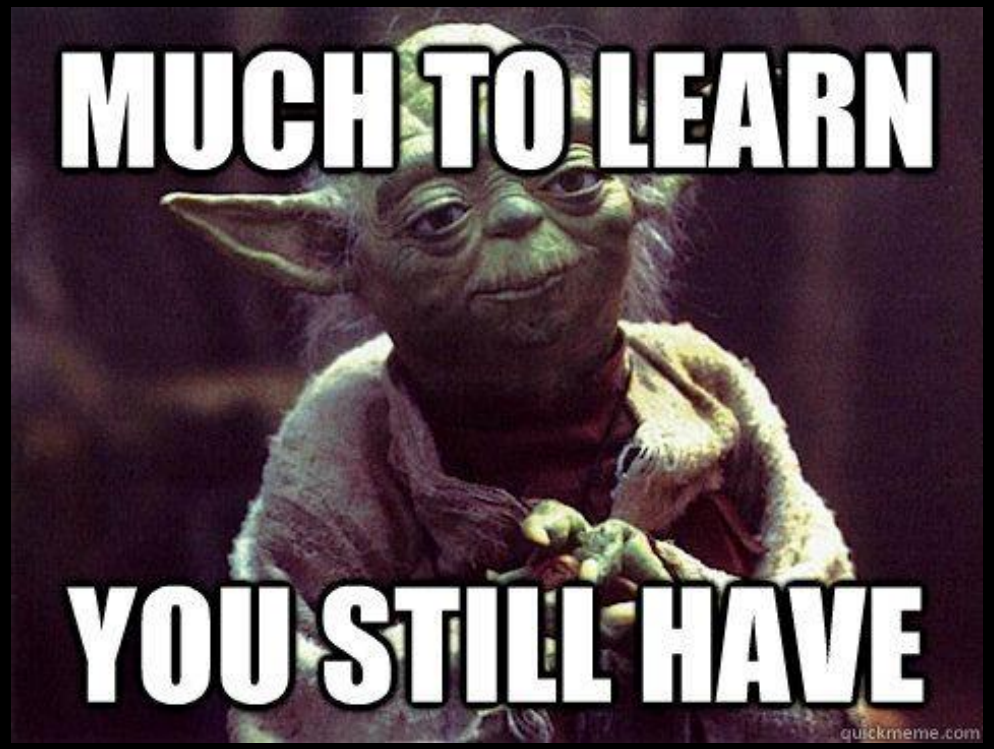
Meet 'Intrusion Truth,' the Group Doxing Chinese Intel Hackers (Wired.com)



Ethical Hacking Resources

- Hacking For Dummies PDF Book
- Hacking: The Art of Exploitation PDF Book
- Certified Ethical Hacker (my site)
- Kali Linux Full PDF – Official Documentation
- Complete Free Hacking Course: Go from Beginner to Expert Hacker (YouTube video – 4.5 hours)
- Ethical Hacking Course on Cybrary
- Social Engineering: A Hacking Story
- The Art of Reconnaissance - Simple Techniques
- https://hack.me/
- Handy Collection of basic ISO Files – For Creating Virtual Machines (VMs)

Questions?



Presenters:

John Stoner
john.e.stoner@gmail.com

Ronnie Obenhaus
ronnie.obenhaus@gmail.com

Sources and References

- http://icitech.org/know-your-enemies-2-0/
- http://motherboard.vice.com/read/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts
- http://www.businesswire.com/news/home/20160209006160/en/Institute-Critical-Infrastructure-Technology-ICIT-Releases-Encyclopedia
- https://countuponsecurity.com/tag/kill-chain/
- https://en.wikipedia.org/wiki/Fancy_Bear
- https://liebsoft.com/blog/winning-cyber-defense-strategies/
- https://nigesecurityguy.wordpress.com/tag/intelligence-driven/
- https://phoenixts.com/blog/reality-russian-hacking-and-apts/
- https://sophos.files.wordpress.com/2014/04/sophos-apt-lifecycle1.png?w=640
- https://sqrrl.com/a-framework-for-cyber-threat-hunting-part-1-the-pyramid-of-pain/
- https://www.alienvault.com/blogs/security-essentials/role-of-cyber-threat-intelligence-analysts-in-an-organization
- https://www.anomali.com/blog/apt-29-put-up-your-dukes
- https://www.buzzfeed.com/sheerafrenkel/meet-fancy-bear-the-russian-group-hacking-the-us-election
- https://www.fireeye.com/current-threats/apt-groups.html#apt29
- https://www.incapsula.com/web-application-security/apt-advanced-persistent-threat.html
- https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
- https://www.netswitch.net/apt-advanced-persistent-threat-what-you-need-to-know/
- https://www.nist.gov/document/draftnationalcybersecurityworkforceframeworkv2xlsx
- https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain
- https://www.secureworks.com/blog/advanced-persistent-threats-apt-a
- https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
- https://www.thecyberwire.com/issues/issues2016/June/CyberWire_2016_06_28.html
- https://www.tripwire.com/state-of-security/security-data-protection/developing-cyber-intelligence-analyst-skills/
- https://attack.mitre.org/wiki/Group/G0009
- https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html
- https://krebsonsecurity.com/tag/deep-panda/
- https://artofthehak.com/deep-panda-apt/
- https://researchcenter.paloaltonetworks.com/2016/02/securing-government-heres-what-we-should-learn-from-2015/