EVOLVE
Security Academy

Presents:

Cyber Intelligence Analysis and Russian Election Hacking

Patrik Maldre

Managing Partner, Retel Partners

@pmaldre

Overview

- Basics of cyber intelligence analysis
- Several types of analytic tradecraft
- Overview of Russian election hacking case
- Forecasting Russian use of cyber capabilities

What is Intelligence?

Information that is collected, analyzed, and disseminated in order to reduce uncertainty and enable decision-making advantages

What is Cyber (Threat) Intelligence?

Knowledge about adversaries and their capabilities, motivations, and intentions that helps organizations protect themselves in the cyber domain

Where Did It Come From?

- Increasing number and sophistication of cyber threats
- Transition from perimeter-based to layered defense (defense-in-depth)
- Rise of targeted attacks in mid-2000s
- From reactive to proactive defense

Identifying and Analyzing Adversaries

- Know your network and your critical assets
- Understand the threat landscape:
  - Adversaries: Script kiddies, cybercriminals, terrorists, hacktivists, competitors, insiders, nation-states
  - Capability and Intent
- Analyze past attacks on your network
- Compile internal and external data to create profiles of adversaries
- Associate indicators of compromise (IP addresses, file hashes, etc.) with adversaries
- Identify specific tools, techniques, and procedures (TTPs)
- Infer motivations and intentions
- Forecast future adversary behavior and invest resources accordingly

Threat Intelligence Levels

- Tactical – Intelligence that supports NOC, SOC, Infrastructure Ops
- Operational – Intel that supports IR, forensics, and fraud detection, IT management
- Strategic – Intel that supports CISO and other executives/board
  - Source: Friedman, Jon and Bouchard, Mark (2015).“The Definitive Guide to Cyber Threat Intelligence”. P.15-16.

Using Cyber (Threat) Intelligence

- Tactical
  - Validate and prioritize indicators
  - Prioritize patches
  - Prioritize alerts
- Operational
  - Provide context to reconstruct attacks quickly
  - Provide data to identify damage and related breaches
- Strategic
  - Provide priorities based on business risks and likely attacks
  - “Put a face” on adversaries and threats

Benefits of Cyber (Threat) Intelligence

- Tactical
  - Removing invalid indicators so they don't create false positives
  - Prioritizing patches so the most dangerous vulnerabilities can be fixed first
  - Automating the flow of valid information to SIEMs so they can correlate events with attacks more quickly and accurately
  - Prioritizing indicators so SOC analysts can rapidly identify alerts that need to be escalated
- Operational
  - Providing situational awareness and context so IR teams can expand their investigations from individual indicators to determine attackers' intentions, methods, and targets
  - Allowing IR and forensics teams to quickly remediate damage done by breaches and prevent additional attacks in the future
- Strategic
  - Providing managers with an understanding of actual threats to the business (which are different from those hyped by the press) so they can allocate budget and start to protect the most critical assets and business processes
  - Helping CISOs communicate with top executives and board members about risks to the business, the probable actions of adversaries in the future, and the return on investments in security

➢ Source: Friedman, Jon and Bouchard, Mark (2015)."The Definitive Guide to Cyber Threat Intelligence". P.8

Sources of Threat Intelligence

- Internal
  - Logs (firewall, DNS, event)
  - SIEM/IDS alerts, IR reports
  - Pcap (esp. malware)
  - Netflow
- External
  - Vendor reports and security blogs
  - Reputation and block lists,
  - VirusTotal & analogous sites
  - Sharing arrangements
- Critical characteristics
  - Accurate
  - Timely
  - Relevant
  - Diverse?

Threat Intelligence Tools

- Open-source
  - OpenIOC/Soltra/ThreatConnect(+), etc.
  - VirusTotal/Malwr/VirusShare
  - Abuse.ch
  - Passive DNS
  - Google/Twitter (Alerts, APIs)
- Proprietary
  - AV/IDS/FW/SIEM provider + their UTM
  - Specialized providers: FireEye, ThreatConnect, CrowdStrike, Recorded Future, etc.

Intelligence Sharing

- Trust groups
  - Networks of personal contacts
  - Industry sharing arrangements
- Subscriptions to threat intelligence providers
- Public-private partnerships
  - Information Sharing and Analysis Centers/Organizations (ISACs/ISAOs)
  - State fusion centers
  - Infragard
  - FBI Flash Alerts
- Community
  - Vendor Reports
  - Security Research
  - Conference Presentations
- Formats
  - Plaintext
  - STIX/TAXII

Tradecraft – Cyber Kill Chain (1)

- Lockheed Martin White Paper (2011): “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”
- “Kill chain” describes the structure of the intrusion
- The corresponding model guides analysis to inform actionable security intelligence
- Each discrete phase of the intrusion is mapped to courses of action for detection, mitigation, and response
- The adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary

Tradecraft – Cyber Kill Chain (2)

Phase	Example
Reconnaissance	Google, LinkedIn, social engineering, “dumpster diving”, etc.
Weaponization	Adding remote access trojan (RAT) and exploit to PDF
Delivery	E-mail attachment, USB, website
Exploitation	Auto-execution (USB), attachment opening, etc.
Installation	Creation of new files, establishing persistence
Command & Control	Beacon to C&C server for further instruction
Actions on Objectives	Data exfiltration, lateral movement, confidentiality and availability violations, etc.

Tradecraft – Cyber Kill Chain (3)

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

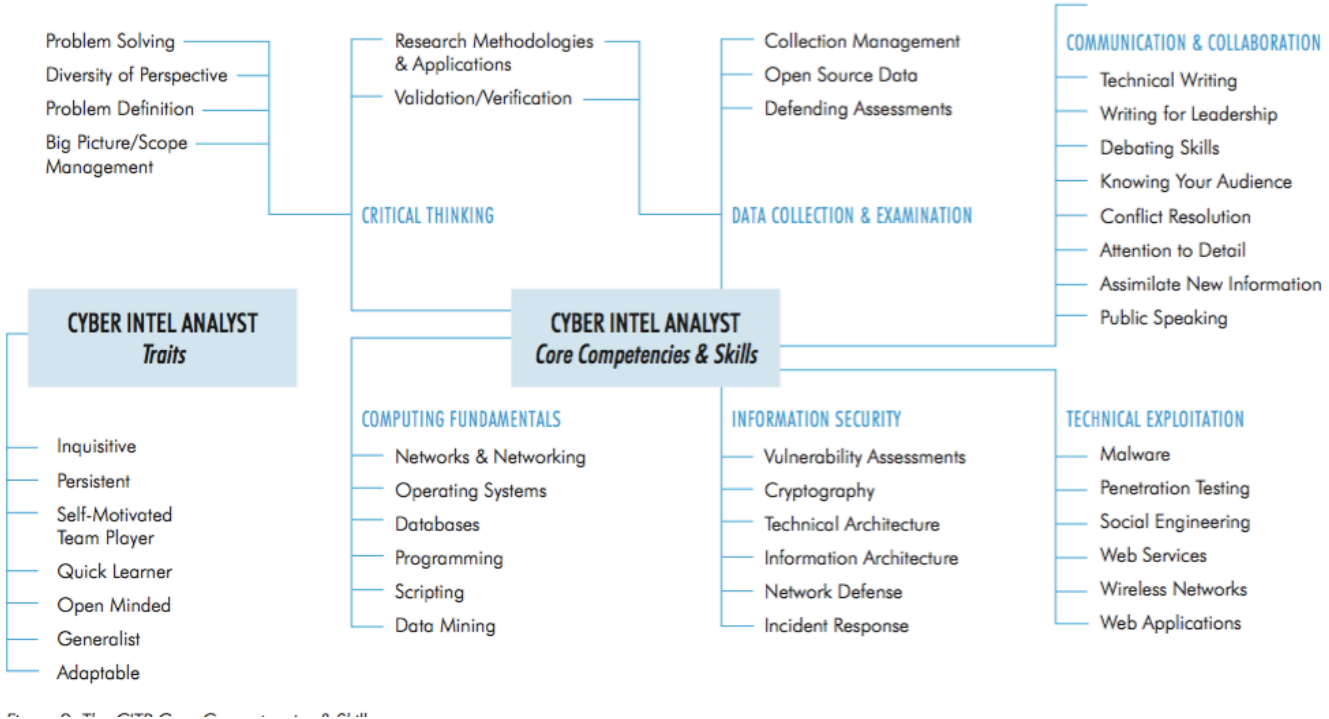
Tradecraft – Analysis of Competing Hypotheses (1)

- Formalized by Richard Heuer, Jr. in Ch. 8 of his seminal "Psychology of Intelligence Analysis" (1999)
- Grounded in insights from cognitive psychology, decision analysis, and the scientific method
- Helps analysts overcome limitations and avoid common pitfalls
- Particularly appropriate for controversial issues

Tradecraft – Analysis of Competing Hypotheses (2)

- *1. Identify possible hypotheses.*
- *2. Make a list of significant evidence and arguments for and against each hypothesis.*
- *3. Prepare a matrix with hypotheses.*
- *4. Refine the matrix.*
  - *Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.*
- *5. Draw tentative conclusions about the relative likelihood of each hypothesis.*
  - *Proceed by trying to disprove the hypotheses rather than prove them.*
- *6. Analyze how sensitive your conclusion is to a few critical items of evidence.*
  - *Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.*
- *7. Report conclusions.*
  - *Discuss the relative likelihood of all the hypotheses, not just the most likely one.*
- *8. Identify milestones for future observation that may indicate events are taking a different course than expected.*

Cyber Intelligence Skills



- Source: Carnegie Mellon University Cyber Intelligence Tradecraft Project

Russian Cyber Capabilities

1. Snake/Turla/Uroborus (2007-)
2. APT 28/The Dukes/Cozy Bear (2008-)
3. APT 29/Sofacy/Fancy Bear (2007-)
4. Red October/Cloud Atlas (2012-)
5. Energetic Bear/Dragonfly/Energetic Bear (2011-)
6. Sandworm Team (2014-)
7. CyberBerkut, Operation Potao, Armageddon, etc.

- Creation of “Cyber Command”, FOC 2017

Case Study: Previous Russian Election Interference

- Ukraine – May 22-26, 2014
  - First Ukrainian Presidential Election since Maidan and annexation of Crimea in March 2014.
    1. May 22nd – CyberBerkut deletes key files, renders voting system inoperable
    2. May 25th – "40 minutes before election results were to go live on television at 8 p.m., government experts removed a "virus" installed on Central Election Commission (CEC) computers"
    3. May 25th – Russian Channel One story with faked results
    4. DDoS Attack early morning after polls closed

    ➢ Source: Christian Science Monitor Passcode, "Ukraine election narrowly avoided 'wanton destruction' from hackers", June 17, 2014.

  - "CERT-UA discovered advanced cyber espionage malware on the CEC network (Sofacy/APT28)"
    ➢ Source: Nikolay Koval, "Revolution Hacking", *Cyber War in Perspective: Russian Aggression in Ukraine,* p.56.

Timeline – Russian Election Hacking

- Summer 2015 – Cozy Bear intrusion into DNC network
- March 2016 – APT28/Fancy Bear Spear-Phishing Campaign against Dems
- April 2016 – Fancy Bear intrusion into DNC network
- April 2016 – "DCLeaks" created
- June 14th, 2016 – CrowdStrike report on Fancy Bear/Cozy Bear
- June 15th, 2016 – "Guccifer 2.0" emerges
- July 10th, 2016 – WikiLeaks Podesta e-mails emerge
- December 29th, 2016 – FBI/DHS GRIZZLY STEPPE report
- December 29th, 2016 – US sanctions/countermeasures against Russia
- January 6th, 2016 - FBI/CIA/NSA report

Tradecraft – Cyber Kill Chain (APT29/Cozy Bear)

- Reconnaissance – Extensive, targeted, based on political priorities
- Weaponization – Long history of development, deployment
- Delivery – Spear-phishing
- Exploitation – Links to malicious dropper
- Installation – SeaDaddy implant; Powershell backdoor via Windows Management Instrumentation (WMI)
- Command & Control – Powershell command to establish encrypted C2 connection, download additional tools
- Actions on Objectives – Establish persistence, enumerate AD accounts, Powershell Mimikatz for credential acquisition and lateral movement; exfiltration of data

Tradecraft – Cyber Kill Chain (APT28/Fancy Bear)

- Reconnaissance – Extensive, targeted, based on political priorities
- Weaponization – Long history of development, deployment
- Delivery – Spear-phishing with weaponized document or link to spoofed/breached website, security warning with link to spoofed e-mail page
- Exploitation – Document with exploit, web-based exploit, or using legitimate credentials from e-mail spoof
- Installation – X-Agent malware, X-Tunnel tool via RemCom tool
- Command & Control – Remote command execution via X-Agent and X-Tunnel, IP addresses enumerated
- Actions on Objectives – Anti-forensics measures (log clearing and resetting timestamps), exfiltration of data

Tradecraft – Analysis of Competing Hypotheses

- Russian government-sponsored actors
  - Abundance of supporting evidence over the course of nearly a decade
- False-flag attack?
  - Need to attain possession of Fancy Bear tools, compromise C&C infrastructure, emulate TTPs, etc.
  - No public record of ever being done at nation-state vs. nation-state level
- Independent hacker/hacktivist – Guccifer 2.0?
  - Romanian language weakness
  - Claimed tools/exploit impossible
  - Deviation from observed hacktivist behaviors
- "400-pound hacker" ???

Tradecraft – GRIZZLY STEPPE Report

- Intended for “Network defenders”, not attribution proof
- Described APT28/APT29 operations
- Listed names associated with Russian Intelligence Services
- Provided indicators, suggestions and best practices
- Detailed DHS programs and communications methods
- Pushed out with .csv and .stix files of IoCs (IP addresses, file hashes, signatures)

Criticism – GRIZZLY STEPPE

- Relevant, timely, accurate?
- Context for indicators
- Distinguishing between private-sector and declassified data
- Too much plugging of DHS initiatives
  - Source: Lee, Robert M. (2016). “Critiques of the DHS/FBI’s GRIZZLY STEPPE Report”

Strategic Forecasting

- Russia will continue to integrate cyber capabilities into their broader foreign and security policy
  - Cyber attacks combined with information/influence operations
  - Attacks on critical infrastructure (energy, water, transport, finance)
  - Operations in support of strategic sectors (energy, defense, etc.)
- Geopolitical analysis will continue to be a very relevant predictor of Russian cyber threat activity (elections, WADA, Ukraine, Syria, etc.)