Cyber Threats in Modern Enterprise

Zach Coker
UT Austin

Higher Stakes

- Security is straightforward for an individual
  - Few devices
  - Mainstream applications, proven operating systems, updates are minor inconveniences
  - Low value target
- Organizations necessitate more vigilance
  - More machines to exploit
  - More humans to socially engineer
  - More financial incentive to compromise

Adversaries

- Hacktivists
  - Political ideology – spread propaganda, deny services, “do it for the lulz”
- Insider Threats
  - Malcontent employees – stealing, damaging or exposing internal systems and data
- Cyber Criminals
  - Indiscriminate profit – financial data theft, cryptoviral extortion
- Nation States
  - Espionage – targeted data exfiltration over a sustained period of time (Advanced Persistent Threat)

Advanced Persistent Threat (APT)

- Highly sophisticated
- Well-funded
- Often nation-state sponsored

APT List: https://www.fireeye.com/current-threats/apt-groups.html

Tactics, Techniques, & Procedures (TTPs)

- Analyzing an APT's operation
- Profiling a specific threat actor
  - Tactics - how the adversary chooses to carry out their attack from beginning to end
    - Predict upcoming espionage and detect in early stage
  - Techniques - the technological approach of achieving intermediate results during the campaign
    - Identify points of weakness and implement countermeasures
  - Procedures - the organizational approach of the adversary's campaigns
    - Understand adversary's objectives and identify lucrative / critical data

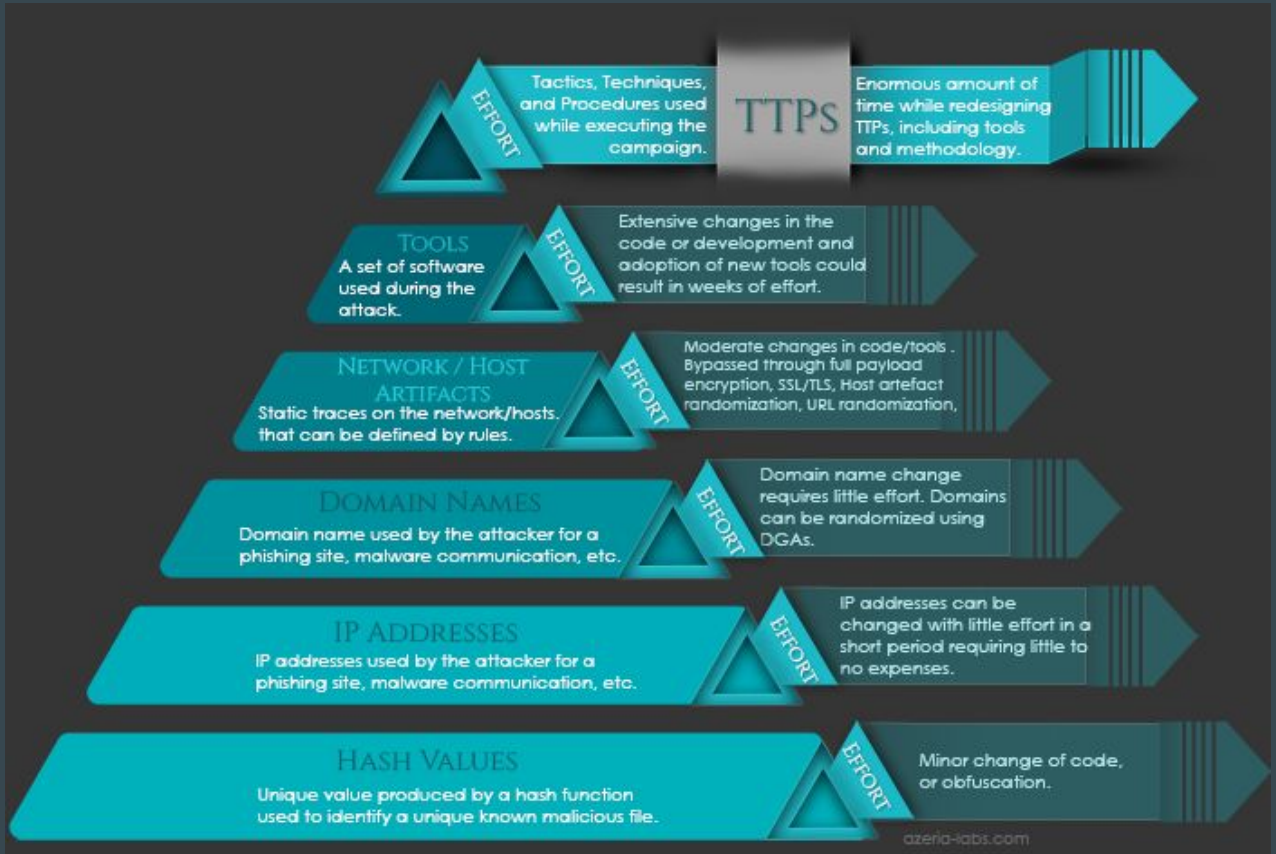
Advanced Persistent Threat Groups

- APT1
  - Chinese PLA “Comment Crew”
  - Stolen hundreds of terabytes of data from at least 141 organizations
  - Large infrastructure, potentially hundreds of human operators
- APT28
  - Russian “Fancy Bear”
  - Targets NATO-aligned states, responsible for DNC Hack
  - Windows & Flash 0-days

TTPs: MITRE ATT&CK Groups

- https://attack.mitre.org/groups/

Tactics, Techniques, & Procedures (TTPs)



Information Operations / Warfare

- Computer Network Operations
  - Computer Network Attack
  - Computer Network Defense
  - Computer Network Exploitation
- Psychological Operations
- Military Deception
- Operational Security
- Electronic Warfare

Computer Network Operations

- Computer Network Attack
- Computer Network Exploitation
- Computer Network Defense

Computer Network Attack

- Activities that deny, destroy, degrade, etc.
- Examples:
  - Denial of Service
  - Stuxnet
  - December 2015 Ukraine power grid cyberattack

Denial of Service

- Flood of traffic to overwhelm victim's resources
- Typically distributed (DDoS) – numerous malware infected machines weaponized by botnet controller to coordinate attack
- Systems and services rendered unavailable to legitimate users
- Types:
  - Syn flood
  - ICMP flood
  - DNS amplification
- Low-Orbit Ion Cannon (LOIC) & Anonymous

Computer Network Defense

- Network Defense
  - Incident response
  - Network security monitoring
  - Threat intelligence
  - Forensics
  - Self assessment
  - Outreach
- CIA Triad
  - Confidentiality - protection of information from unauthorized access
  - Integrity - information is kept accurate and consistent unless authorized changes are made
  - Availability - information is available when and where it is rightly needed

Computer Network Exploitation

- Cyber-espionage, not an act of war
  - US Code Title 50 vs Title 10
- Information gathering, data exfiltration
- Man-in-the-Middle (MITM)
  - Intercepts traffic
  - HTTPS decryption for network traffic monitoring
- Man-on-the-Side (MOTS)
  - Race condition

Anatomy of a hack

- Cyber Kill Chain

Exploitation Terms

- Vulnerability: weakness which can be exploited by a threat actor
- Exploit: software/commands/data that take advantage of vulnerability to cause unintended behavior
- Payload: code to be executed
  - Remote Access Toolkit
  - Keylogger
  - Reverse Shell
- Exploit (missile) targets the vulnerability (target) and delivers the Payload (warhead)

1 - Reconnaissance

Initial Planning Phase

- Research target
- Analyze online activities and public presence
- Observe websites visited and social media networks used
- Harvest email addresses
- Collect publicly available information and news
- Discover scanning for internet facing systems and applications
- Build target profile

Recon & Scanning tools

- Central Ops - https://centralops.net/co/
- Shodan - https://www.shodan.io/
- Nmap / Zenmap
- Nessus
- Metasploit (built-in scanner)
- Burpsuite
- OWASP Zap

2 - Weaponization

Attack Preparation and Staging

- Select appropriate malware payload
- Reuse existing malware families with slight variants
- Build phishing campaign
- Leverage exploit kits and botnets

Exploit kits

- BeEF - http://beefproject.com/
- Metasploit - https://www.metasploit.com/
- OpenVAS - http://www.openvas.org/

3 - Delivery

Launching Attack

- Publish compromised website (watering hole)
- Deliver phishing email
  - Most common attack vector for US victims
- Distribute infected USB sticks
- Execute attack tools against servers and applications

4 - Exploitation

Exploit vulnerability and gain initial access

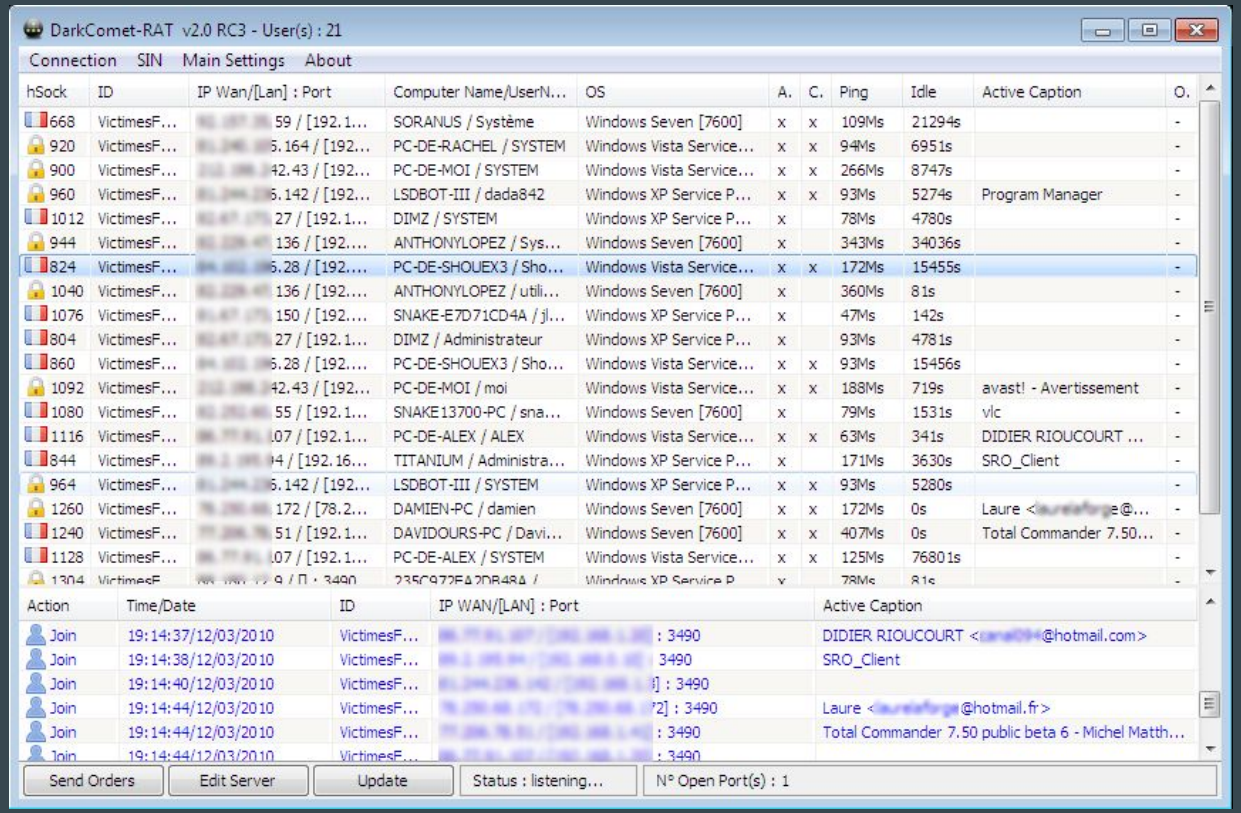
- Exploit a hardware or software vulnerability
  - Zero days (expensive and rare)
  - Most exploited vulnerabilities have known patches available
- Trick user into providing access

5 - Installation

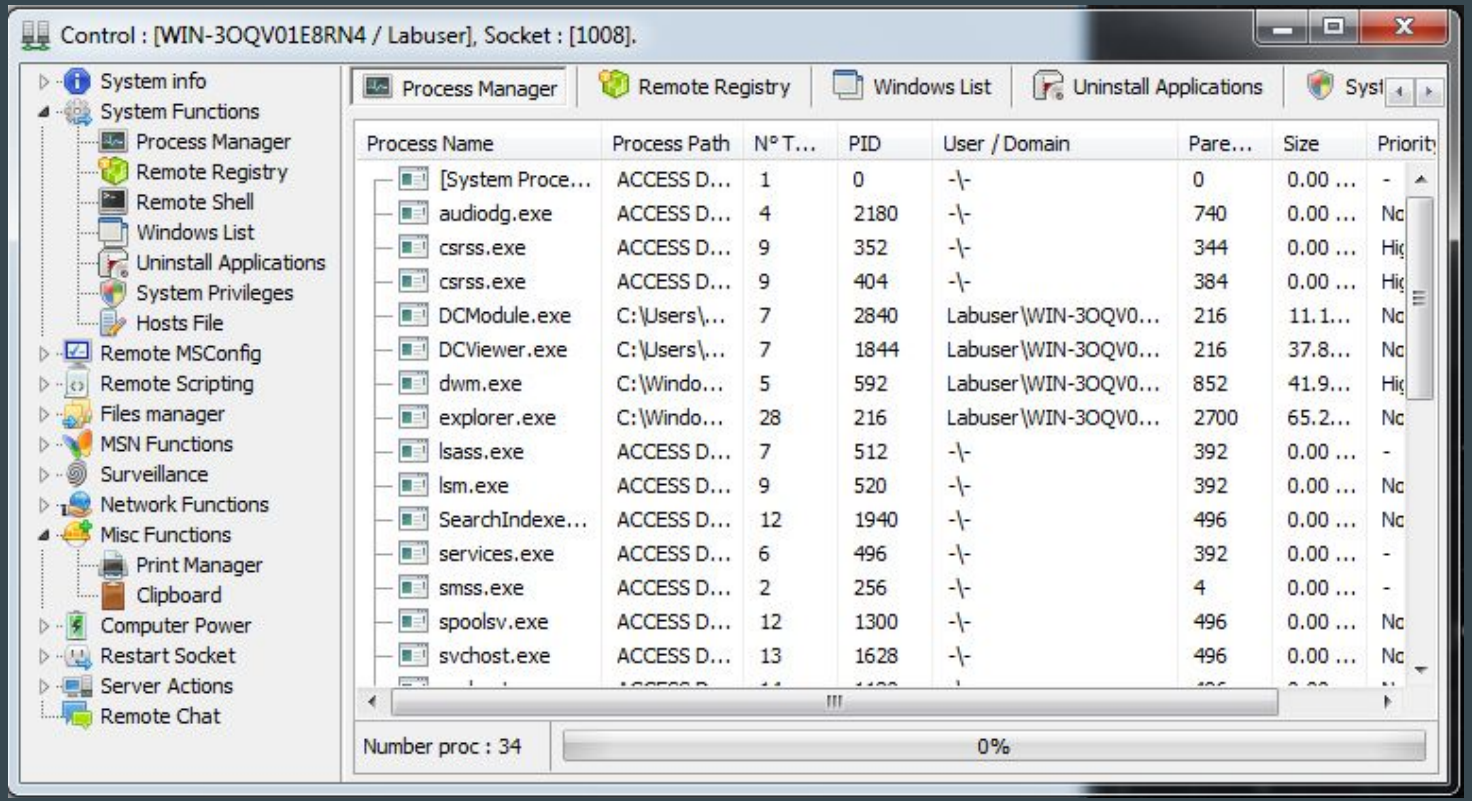
Establish foothold in the environment

- Install persistent backdoor (remote access toolkit)
- Utilize webshells on web servers
- Create additional accounts or services
- Hide/obfuscate malware
- Maintain access for an extended period of time

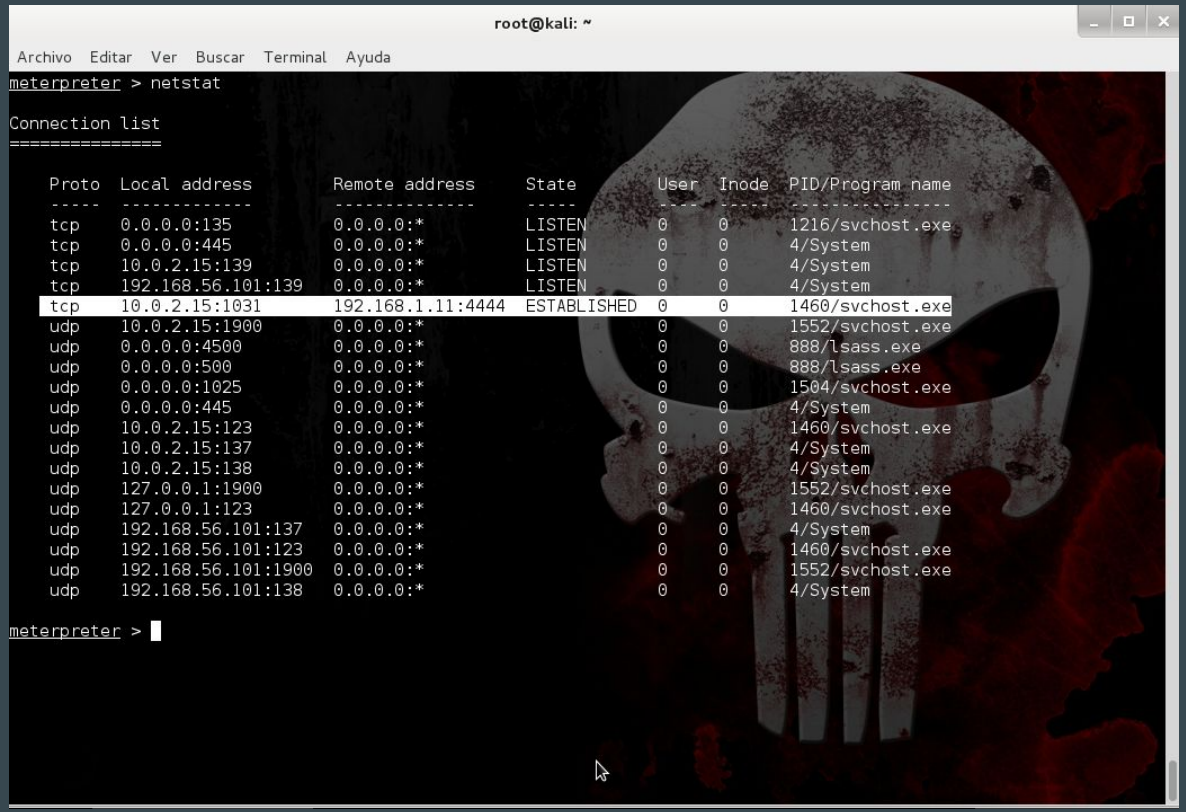
Remote access toolkit - DarkComet



Remote access toolkit - DarkComet (cont'd.)



Remote access toolkit - Meterpreter



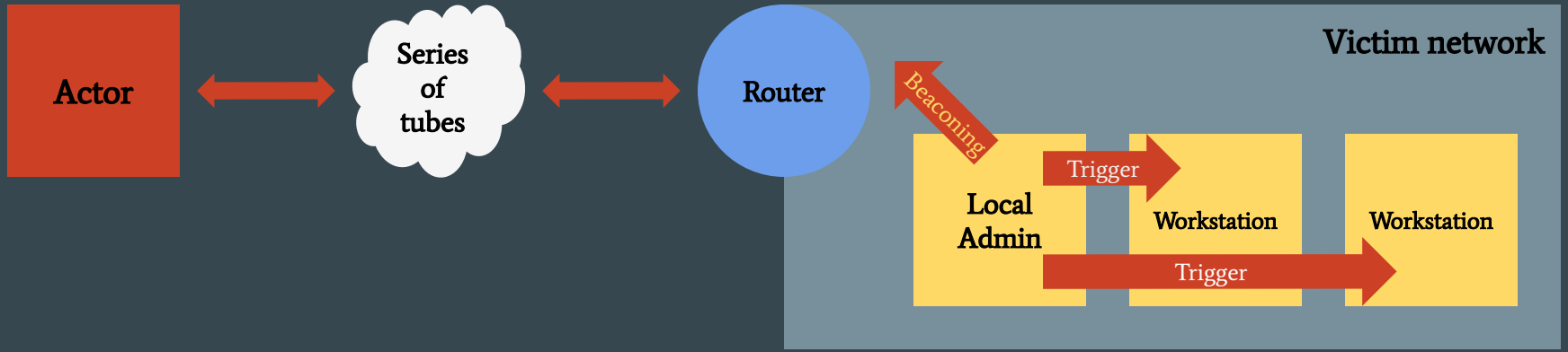
Implants

- Beaconing vs Triggerable
- In-Memory (Non-persistent) vs On-Disk (Persistent)
- Can’t trigger into device behind NAT

Beaconing implant

Triggerable implant

- AKA “trigger-in”, “call-in” malware
- Useful for public-facing servers
- Can’t trigger into device behind NAT



Installation and Persistence considerations

	Beaconing	Triggerable
In-Memory (Non-Persistent)	High uptime, server or workstation within private network	High uptime, internet-facing, advanced behavior-based security tools
On-Disk (Persistent)	Low uptime, high network visibility, valuable data, admin machine on internal network	Low uptime, cursory data collection, expand access, redirect from beacon in network

6 - Command & Control (C2)

Establish remote control

- Two-way communication channel for remote control
- Common channels:
  - Web
  - Email
  - DNS
- Escalate privileges
- Lateral movement
- Obfuscation (anti-forensics activities, hiding tracks)

7 - Actions on Objectives

Achieve mission goals

- Complete end goal
- Exfiltrate data
  - Intellectual property
  - Personally identifiable information
  - Money
- Computer network attack activities
- Co-opt infrastructure for future campaigns

Courses of Action

Phase	Detect	Deny	Disrupt	Degrade	Deceive
Recon	Web analytics	Firewall ACL			
Weaponization	NIDS	NIPS			
Delivery	Vigilant user	Proxy filter	AV	Queuing	
Exploitation	HIDS	Patching	DEP		
Installation	HIDS		AV		
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
Actions	Audit logs		Quality of service	Honeypot	

Network Defense, cont'd.

- Antivirus
  - Signature-based
  - Behavioral-based
  - Cloud
- Anomaly Detection
  - Network-Based Anomaly Detection (NBAD)
  - User and Entity Behavior Analytics (UEBA)
  - Syscall profile-based detection

Considerations for Enterprise

- Router Exploitation
  - Control the network
  - Enables MITM / MOTS
  - 2015 Cisco router vulnerabilities - SYNful Knock
    - Backdoor Implant, relied on stolen/default creds for initial access
- VM Breakout
  - Multiple ESXi vulnerabilities
- APT5 targeting enterprise VPN servers (August 2019)
  - Fortinet, Pulse Secure
  - 0-day was shown at Black Hat
  - APT5 umbrella group set up scanning infrastructure for vulnerabilities

2014 Sony Pictures Hack

- Actor: North Korea
- Nation-state sponsored APT targeting private sector
- Multi-year campaign
- https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/
- https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Ransomware

- Threaten to publish the victim's data or perpetually block access to it unless a ransom is paid
- More advanced malware uses a technique called “cryptoviral extortion”
- 2017 WannaCry ransomware attack
  - Scanned vulnerable systems for EternalBlue exploit, used DoublePulsar to install and execute
  - As of 14 June 2017, a total of 327 payments totaling US$130,634.77 had been transferred

Exploits - Big Money

- https://vuldb.com/?doc.exploitprices
- Example: https://vuldb.com/?id.142139