

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

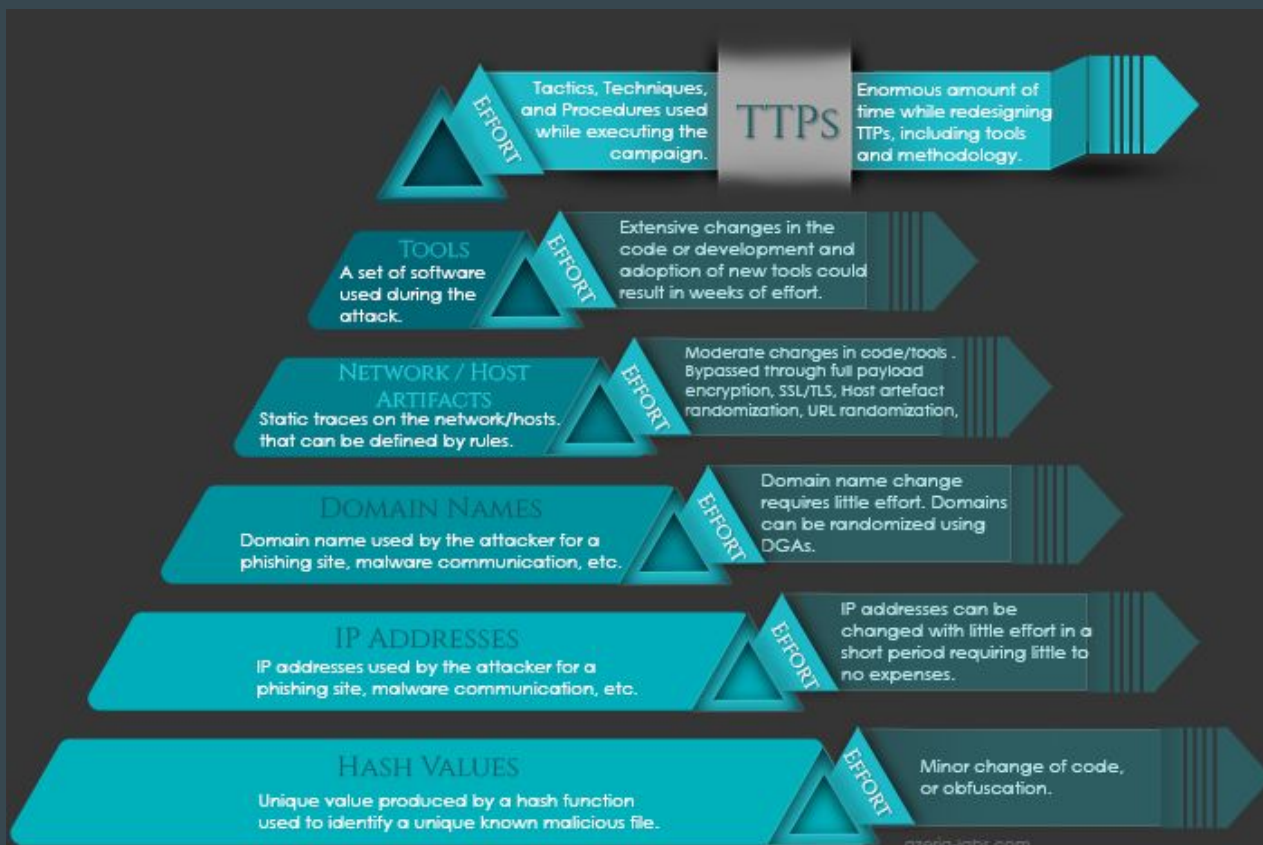
Advanced Persistent Threat Groups

- 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

DarkComet-RAT v2.0 RC3 - User(s) : 21

Connection SIN Main Settings About

hSock	ID	IP Wan/[Lan] : Port	Computer Name/UserN...	OS	A.	C.	Ping	Idle	Active Caption	O.
668	VictimesF...	59 / [192.1...	SORANUS / Système	Windows Seven [7600]	x	x	109Ms	21294s		-
920	VictimesF...	5.164 / [192...	PC-DE-RACHEL / SYSTEM	Windows Vista Service...	x	x	94Ms	6951s		-
900	VictimesF...	42.43 / [192...	PC-DE-MOI / SYSTEM	Windows Vista Service...	x	x	266Ms	8747s		-
960	VictimesF...	6.142 / [192...	LSDBOT-III / dada842	Windows XP Service P...	x	x	93Ms	5274s	Program Manager	-
1012	VictimesF...	27 / [192.1...	DIMZ / SYSTEM	Windows XP Service P...	x		78Ms	4780s		-
944	VictimesF...	136 / [192...	ANTHONYLOPEZ / Sys...	Windows Seven [7600]	x		343Ms	34036s		-
824	VictimesF...	6.28 / [192...	PC-DE-SHOUEX3 / Sho...	Windows Vista Service...	x	x	172Ms	15455s		-
1040	VictimesF...	136 / [192...	ANTHONYLOPEZ / utili...	Windows Seven [7600]	x		360Ms	81s		-
1076	VictimesF...	150 / [192...	SNAKE-E7D71CD4A / j...	Windows XP Service P...	x		47Ms	142s		-
804	VictimesF...	27 / [192.1...	DIMZ / Administrateur	Windows XP Service P...	x		93Ms	4781s		-
860	VictimesF...	6.28 / [192...	PC-DE-SHOUEX3 / Sho...	Windows Vista Service...	x	x	93Ms	15456s		-
1092	VictimesF...	42.43 / [192...	PC-DE-MOI / moi	Windows Vista Service...	x	x	188Ms	719s	avast! - Avertissement	-
1080	VictimesF...	55 / [192.1...	SNAKE13700-PC / sna...	Windows Seven [7600]	x		79Ms	1531s	v/c	-
1116	VictimesF...	07 / [192.1...	PC-DE-ALEX / ALEX	Windows Vista Service...	x	x	63Ms	341s	DIDIER RIOUCOURT ...	-
844	VictimesF...	94 / [192.16...	TITANIUM / Administra...	Windows XP Service P...	x		171Ms	3630s	SRO_Client	-
964	VictimesF...	6.142 / [192...	LSDBOT-III / SYSTEM	Windows XP Service P...	x	x	93Ms	5280s		-
1260	VictimesF...	172 / [78.2...	DAMIEN-PC / damien	Windows Seven [7600]	x	x	172Ms	0s	Laure <laureforge@...	-
1240	VictimesF...	51 / [192.1...	DAVIDOURS-PC / Davi...	Windows Seven [7600]	x	x	407Ms	0s	Total Commander 7.50...	-
1128	VictimesF...	07 / [192.1...	PC-DE-ALEX / SYSTEM	Windows Vista Service...	x	x	125Ms	76801s		-
1304	VictimesF...	9 / [192.16...	2350972F470R4R4 /	Windows XP Service P...	x		78Ms	81s		-

Action	Time/Date	ID	IP WAN/[LAN] : Port	Active Caption
Join	19:14:37/12/03/2010	VictimesF...	3490	DIDIER RIOUCOURT <...@hotmail.com>
Join	19:14:38/12/03/2010	VictimesF...	3490	SRO_Client
Join	19:14:40/12/03/2010	VictimesF...	3490	
Join	19:14:44/12/03/2010	VictimesF...	3490	Laure <laureforge@hotmail.fr>
Join	19:14:44/12/03/2010	VictimesF...	3490	Total Commander 7.50 public beta 6 - Michel Matth...
Join	19:14:44/12/03/2010	VictimesF...	3490	

Send Orders Edit Server Update Status : listening... N° Open Port(s) : 1

Remote access toolkit - DarkComet (cont'd.)

The screenshot displays the DarkComet remote access toolkit interface. The main window title is "Control : [WIN-3OQV01E8RN4 / Labuser], Socket : [1008]". The interface is divided into a left sidebar with various system functions and a main area with a "Process Manager" tab selected.

The "Process Manager" tab shows a list of running processes with the following columns: Process Name, Process Path, N° T..., PID, User / Domain, Pare..., Size, and Priorit. The processes listed include:

Process Name	Process Path	N° T...	PID	User / Domain	Pare...	Size	Priorit
[System Proce...	ACCESS D...	1	0	-\\-	0	0.00 ...	-
audiodg.exe	ACCESS D...	4	2180	-\\-	740	0.00 ...	Nc
csrss.exe	ACCESS D...	9	352	-\\-	344	0.00 ...	Hiq
csrss.exe	ACCESS D...	9	404	-\\-	384	0.00 ...	Hiq
DCModule.exe	C:\Users\...	7	2840	Labuser\WIN-3OQV0...	216	11.1...	Nc
DCViewer.exe	C:\Users\...	7	1844	Labuser\WIN-3OQV0...	216	37.8...	Nc
dwm.exe	C:\Windo...	5	592	Labuser\WIN-3OQV0...	852	41.9...	Hiq
explorer.exe	C:\Windo...	28	216	Labuser\WIN-3OQV0...	2700	65.2...	Nc
lsass.exe	ACCESS D...	7	512	-\\-	392	0.00 ...	-
lsm.exe	ACCESS D...	9	520	-\\-	392	0.00 ...	Nc
SearchIndexe...	ACCESS D...	12	1940	-\\-	496	0.00 ...	Nc
services.exe	ACCESS D...	6	496	-\\-	392	0.00 ...	-
smss.exe	ACCESS D...	2	256	-\\-	4	0.00 ...	-
spoolsv.exe	ACCESS D...	12	1300	-\\-	496	0.00 ...	Nc
svchost.exe	ACCESS D...	13	1628	-\\-	496	0.00 ...	Nc

At the bottom of the window, there is a status bar showing "Number proc : 34" and a progress indicator at "0%".

Remote access toolkit - Meterpreter

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
meterpreter > netstat  
  
Connection list  
=====
```

Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	1216/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	10.0.2.15:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	192.168.56.101:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	10.0.2.15:1031	192.168.1.11:4444	ESTABLISHED	0	0	1460/svchost.exe
udp	10.0.2.15:1900	0.0.0.0:*		0	0	1552/svchost.exe
udp	0.0.0.0:4500	0.0.0.0:*		0	0	888/lsass.exe
udp	0.0.0.0:500	0.0.0.0:*		0	0	888/lsass.exe
udp	0.0.0.0:1025	0.0.0.0:*		0	0	1504/svchost.exe
udp	0.0.0.0:445	0.0.0.0:*		0	0	4/System
udp	10.0.2.15:123	0.0.0.0:*		0	0	1460/svchost.exe
udp	10.0.2.15:137	0.0.0.0:*		0	0	4/System
udp	10.0.2.15:138	0.0.0.0:*		0	0	4/System
udp	127.0.0.1:1900	0.0.0.0:*		0	0	1552/svchost.exe
udp	127.0.0.1:123	0.0.0.0:*		0	0	1460/svchost.exe
udp	192.168.56.101:137	0.0.0.0:*		0	0	4/System
udp	192.168.56.101:123	0.0.0.0:*		0	0	1460/svchost.exe
udp	192.168.56.101:1900	0.0.0.0:*		0	0	1552/svchost.exe
udp	192.168.56.101:138	0.0.0.0:*		0	0	4/System

```
meterpreter > █
```

Implants

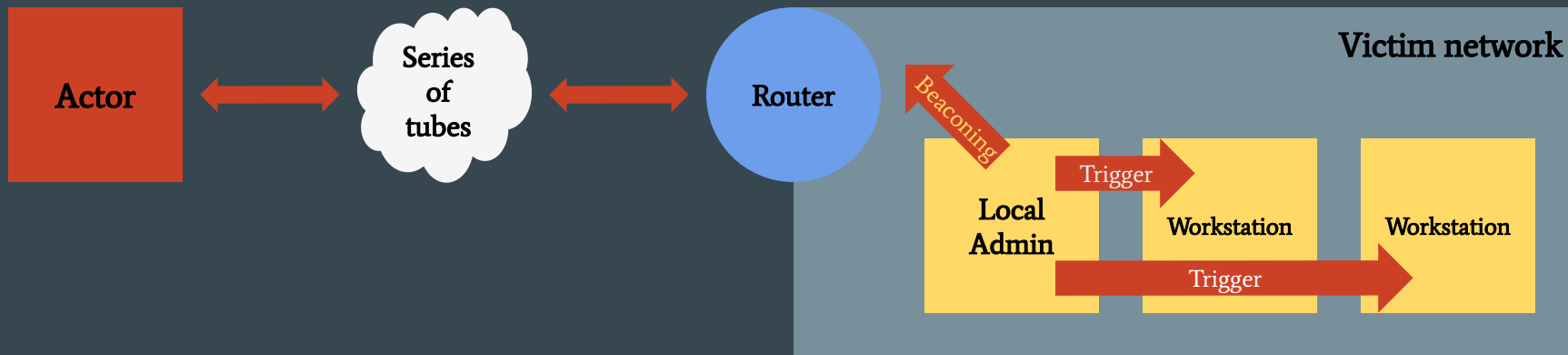
- Beaconing vs Triggerable
- In-Memory (Non-persistent) vs On-Disk (Persistent)
- Can't trigger into device behind NAT

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-picture-s-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>