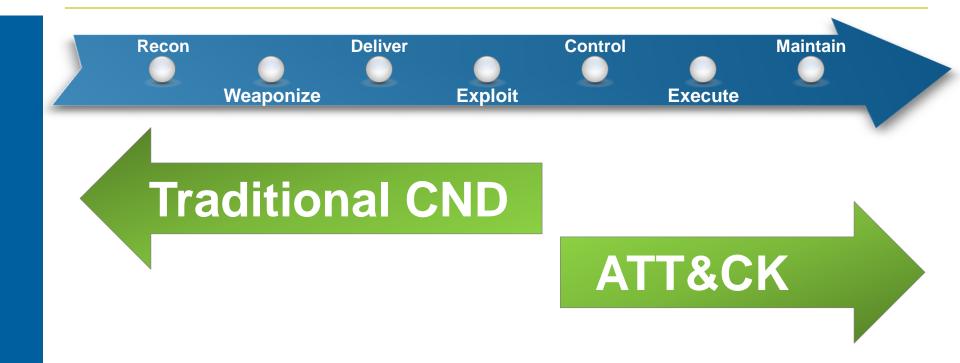
# Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™)

**Blake Strom** 

August 2015



#### **Cyber Attack Lifecycle**



Better understand tactics used by the adversary already operating within a network



### **Threat Based Modeling**

- Cyber threat analysis
- Research
- Industry reports

Adversary Behavior

#### ATT&CK

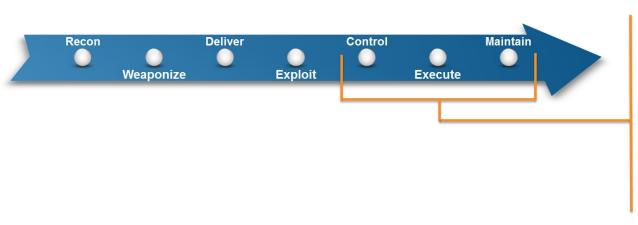
- Adversary model
- Post-access techniques

- Data sources
- Analytics
- Prioritization

Enterprise Defense



### **Cyber Attack Lifecycle – Enhanced**



- Persistence
- Privilege Escalation
- Credential Access
- Host Enumeration
- Defense Evasion
- Lateral Movement
- Execution
- Command and Control
- Exfiltration

Threat data informed adversary model

Higher fidelity on right-of-exploit, post-access phases

Describes behavior sans adversary tools

**MITRE** 

### **ATT&CK Adversary Model**

#### Consists of:

- 1. Decomposed post-exploit phases of Cyber Attack Lifecycle
- 2. List of techniques available to adversaries for each phase
- 3. Possible methods of detection and mitigation
- 4. Apply documented adversary use of techniques
- Publically available adversary information is a problem
  - Not granular enough
  - Insufficient volume



Mr. Potato Head is a registered trademark of Hasbro Inc.



### **Use of Public Adversary Information**

- Publicly reported adversary group and tool coverage:
  - 16 groups and counting
    - Examples: APT28, APT30, DarkHotel, Hurricane Panda, Ke3chang, Cleaver, Axiom
  - 30 tools and counting
    - Examples: Mimikatz, PsExec, dsquery, Hikit, PlugX, Poison Ivy



#### **Technique Details**

#### Persistence –New Service

- Description: Installation of a new service. May use service name from previous or newer OS or create entirely new service name.
- Platform: Windows
- Permissions required: Administrator, SYSTEM
- Effective permissions: SYSTEM
- Use: Part of initial infection vector or used during operation to locally or remotely execute persistent malware.
- Detection: Monitor new service creation. Look for out of the ordinary service names and activity that does not correlate with known-good software, patches, etc. New services may show up as outlier processes that have not been seen before when compared against historical data.
- Data Sources: Windows Registry, process information



# **ATT&CK: The Tactics and Techniques**

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Leg	gitimate Credenti	als	Credential	Account	Application	Command	Commonly	Automated
Accessibilit	ty Features	Binary	Dumping	enumeration	deployment	Line	used port	or scripted
AddMo	•	Padding	Credentials	File system	software	File Access	Comm	exfiltration
DLL Search		DLL Side- Loading	in Files	enumeration	Exploitation of	PowerShell	through removable	Data compressed
Edit Default F		Disabling	Network	Group	Vulnerability	Process	media	Data
New S		Security	Sniffing	permission	Logon	Hollowing	Custom	encrypted
Path Inte		Tools	User	enumeration	scripts	Registry	application	Data size limits
Schedul	<u> </u>	File System	Interaction	Local	Pass the hash	Rundll32	layer	
Service File		Logical Offsets	Credential	network	Pass the	Scheduled	protocol	Data staged
Weak		Process	manipulation	connection	<u>ti</u> cket	Task	Custom	Exfil over C2
Shortcut M	odification	Hollowing	mampalation	enumeration	Peer	Service	encryption	<u>channel</u> Exfil over
Web		Rootkit		Local	connections Remote	Manipulation	cipher Data	alternate
		s UAC		networking	Desktop	Third Party	obfuscation	channel to
BIOS		jection		enumeration	Protocol	Software	Fallback	C2 network
Hypervisor		Indicator			Windows m		channels Multiband	Exfil over
Rootkit	Exploitation of	blocking on		Operating system	instrum	_	comm	other
Logon Scripts	Vulnerability	host		enumeration	Windows		Multilayer	network
	Valificiability	Indicator		Owner/User		s remote Jement	encryption Peer	medium Exfil over
Master Boot Record		removal from		enumeration	Remote	Jennem.	connections	physical
		tools Indicator			Services		Standard app	medium
Mod. Exist'g Service		removal from		Process enumeration	Replication		layer	
		host			through		protocol Standard	From local
Registry Run		Masquerad-		Security	removable		non-app	system
Keys		ing NTFS		software enumeration	media Shared		layer	From
Serv. Reg. Perm.		Extended			webroot		protocol	network
Weakness		Attributes		Service	Taint shared		Standard	resource
Windows Mgmt Instr. Event		Obfuscated		enumeration	content		encryption	From
Subsc.		Pavload		Window	Windows admin		cipher	removable
Winlogon Helper		Rundll32		enumeration	shares		Uncommonly	media
DLL		Scripting			<u> </u>		used port	Scheduled
		Software Packing						transfer



**Timestomp** 

### **Applications**

- Gap analysis with current defenses
- Prioritize detection/mitigation of heavily used techniques
- Information sharing
- Track a specific adversary's set of techniques
- Simulations, exercises
- New technologies, research



#### **Tactic Breakdown**

Persistence	20	Lateral Movement	14
Privilege Escalation	14	Execution	11
Credential Access	5	Command and Control	13
Host Enumeration	11	Exfiltration	13
Defense Evasion	19		



### **Publicly Known Adversary Use**

Persistence	20	5	Lateral Movement	14	6
Privilege Escalation	14	4	Execution	11	5
Credential Access	5	3	Command and Control	13	10
Host Enumeration	11	8	Exfiltration	13	4
Defense Evasion	19	12	-		



### **Publically Reported Technique Use**

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Leç	gitimate Credenti		Credential	Account	Application	Command	Commonly	Automated
Accessibilit	ty Features	Binary	Dumping	enumeration	deployment	Line	used port	or scripted
AddMe	onitor	Padding DLL Side-	Credentials	File system	software	File Access	Comm	exfiltration Data
DLL Search	Order Hijack	Loading	in Files	enumeration	Exploitation of	PowerShell	through removable	compressed
Edit Default F	-	Disabling	Network	Group	Vulnerability	Process	media	Data
New S		Security	Sniffing	permission	Logon	Hollowing	Custom	encrypted
Path Inte		Tools	User	enumeration	scripts	Registry	application	Data size
Schedul	<u> </u>	File System	Interaction		Pass the	Rundli32	laver	limits
		Logical		Local	hash Pass the		protocol	Data staged
Service File Weak		Offsets	Credential	network	ticket	Scheduled	Custom	Exfil over C2
		Process	manipulation	connection enumeration	Peer	Task	encryption	channel
Shortcut M		Hollowing		enumeration	connections	Service	cipher	Exfil over
Web		Rootkit		Local	Remote	Manipulation	Data obfuscation	alternate channel to
BIOS	Bypas	s UAC		networking	Desktop	Third Party	Fallback	C1 network
I bernamia au	DLL In	jection		enumeration	Protocol	Software	channels	Exfil over
Hypervisor Rootkit	Exploitation	Indicator		Operating	Windows m	anagement	Multiband	other
	of	blocking on		system	instrum	entation	comm Multilayer	network
Logon Scripts	Vulnerability	host Indicator		enumeration	Windows	s remote	encryption	medium
Master Boot		removal from		Owner/User	manag	ement	Peer	Exfil over
Record		tools		enumeration	Remote		connections	physical
Mod. Exist'q		Indicator		Process	Services		Standard app	medium
Service		removal from		enumeration	Replication		layer protocol	From local
Dogiotay Dua		host		Security	through		Standard	system
Registry Run Keys		Masquerad-		software	removable media		non-app	From
		ing NTFS		enumeration	Shared		layer	network
Serv. Reg. Perm. Weakness		Extended			webroot		protocol	resource
		Attributes		Service	Taint shared		Standard	
Windows Mgmt Instr. Event		Obfuscated		enumeration	content		encryption	From
Subsc.		Pavload		Window	Windows admin		cipher	removable
Winlogon Helper		Rundll32		enumeration	shares		Uncommonly	media
DLL		Scripting			Silaits		used port	Scheduled
		Software Packing						transfer



## **Notional Defense Gaps**

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Le	gitimate Credenti	als	Credential	Account	Application	Command	Commonly	Automated
Accessibili	ty Features	Binary	Dumping	enumeration	deployment	Line	used port	or scripted
AddM	<del>-</del>	Padding	Credentials	File system	software	File Access	Comm	exfiltration
DLL Search		DLL Side- Loading	in Files	enumeration	Exploitation	PowerShell	through removable	Data compressed
Edit Default I		Disabling	Network	Group	of Vulnerability	Process	media	Data
New S		Security	Sniffing	permission	Logon	Hollowing	Custom	encrypted
Path Inte		Tools	User	enumeration	scripts	Registry	application	Data size
Schedul		File System	Interaction		Pass the	Rundli32	layer	limits
		Logical		Local	hash Pass the		protocol	Data staged
Service File Weak		Offsets	Credential	network	ticket	Scheduled	Custom	Exfil over C2
		Process Hollowing	manipulation	connection	Peer	Task	encryption	channel
	Shortcut Modification			enumeration	connections	Service	cipher	Exfil over
Web	Web shell Rootl			Local	Remote	Manipulation	Data Data	alternate channel to
BIOS	Bypas	s UAC		networking	Desktop	Third Party	Fallback	C2 network
	DLL In	jection		enumeration	Protocol	Software	channels	Exfil over
Hypervisor Rootkit	Exploitation	Indicator		Operating	Windows m	nanagement	Multiband	other
	of	blocking on		system	instrum	entation	comm Multilayer	network
Logon Scripts	Vulnerability	host Indicator		enumeration	Window	s remote	encryption	medium
Master Boot		removal from		Owner/User	manag	gement	Peer	Exfil over
Record		tools		enumeration	Remote		connections	physical
Mod. Exist'q		Indicator		Process	Services		Standard app	medium
Service		removal from		enumeration	Replication		layer	From local
		host			through		<u>protocol</u> Standard	system
Registry Run Keys		Masquerad-		Security software	removable		non-app	
		ing NTFS		enumeration	media Shared		layer	From
Serv. Reg. Perm.		Extended			webroot		protocol	network
Weakness		Attributes		Service	Taint shared		Standard	resource
Windows Mgmt Instr. Event		Obfuscated		enumeration	content		encryption	From
Subsc.		Pavload		Window	Windows		cipher	removable
Winlogon Helper		Rundll32		enumeration	admin		Uncommonly	media
DLL		Scripting			shares	I	used port	Scheduled
		Software						transfer
		Packing						



**Timestomp** 

**No Detect** 

## **Adversary Visibility at the Perimeter**

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Leg	gitimate Credenti	als	Credential	Account	Application	Command	Commonly	Automated
Accessibili	ty Features	Binary	Dumping	enumeration	deployment	Line	used port	or scripted
AddM		Padding	Credentials	File system	software	File Access	Comm through	exfiltration
DLL Search	Order Hijack	DLL Sidĕ- Loading	in Files	enumeration	Exploitation of	PowerShell	removable	Data compressed
Edit Default I		Disabling	Network	Group	Vulnerability		media	Data
New S		Security	Sniffing	permission	Logon	Hollowing	Custom	encrypted
Path Inte		Tools	User	enumeration	scripts	Registry	application	Data size
Schedul		File System	Interaction		Pass the	Rundli32	layer	limits
Service File		Logical	Credential	Local network	hash Pass the	Scheduled	protocol	Data staged
Service File Weak		Offsets	manipulation	connection	ticket	Task	Custom	Exfil over C2
Shortcut M		Process	Illallipulation	enumeration	Peer		encryption	channel Exfil over
		Hollowing			connections	Service	cipher Data	alternate
Web		Rootkit		Local	Remote	Manipulation	obfuscation	channel to
BIOS		s UAC		networking	Desktop	Third Party	Fallback	C2 network
Hypervisor		jection		enumeration	Protocol	Software	channels Multiband	Exfil over
Rootkit	Exploitation	Indicator		Operating		nanagement	comm	other
Logon Corinto	of	blocking on host		system		entation	Multilayer	network
Logon Scripts	Vulnerability	Indicator		enumeration	Window	s remote	encryption Peer	medium
Master Boot		removal from		Owner/User		jement		Exfil over
Record		tools		enumeration	Remote		connections Standard app	physical
Mod. Exist'g		Indicator		Process	Services Replication		layer	medium
Service		removal from		enumeration	through		protocol	From local
Registry Run		host Masquerad-		Security	removable		Standard	system
Keys		ing		software	media		non-app	From
Serv. Reg. Perm.		NTFS		enumeration	Shared		layer	network
Weakness		Extended		Service	webroot Taint shared		protocol Standard	resource
Windows Mamt		Attributes		enumeration	content		encryption	From
Instr. Event		Obfuscated Payload		Window	Windows		cipher	removable
Subsc.		Rundli32		enumeration	admin		Uncommonly	media
Winlogon Helper		Scripting			shares		used port	Scheduled
DLL		Software					acca port	transfer
		Packing						transion



**Full Visibility** 

#### **Adversary Visibility at the Perimeter**

- Adversary has the most latitude for variation at the network level
- Firewall, IDS/IPS, netflow, proxy, mail gateway, WCF, SSL MitM, protocol decoders, anomaly detection etc...
- All partial solutions
  - Don't add up to a complete one
- Often require specific prior knowledge
  - IPs, domains, malware changed easily
    - Sector, organization specific infrastructure
    - Frequently modify tools
    - Use legitimate channels
- Better coverage with host sensing

Defense Evasion	C2	Exfiltration
Legit. Cred.	Commonly	Automated
Binary	used port	or scripted
	Comm	exfiltration
Padding DLL Side-	through	Data
Loading	removable	compressed
Disabling	media	Data
Security	Custom	encrypted Data size
Tools	application	
File System	layer	limits
Logical	protocol	Data staged
Offsets	Custom	Exfil over C2
Process	encryption	channel
Hollowing		Exfil over
	cipher Data	alternate
Rootkit		channel to
Bypass UAC	obfuscation Fallback	C2 network
DLL Injection	channels Multiband	Exfil over
Indicator	Multiband	other
blocking on	comm Multilayer	
host		network
Indicator	encryption Peer	medium
removal from		Exfil over
tools	connections Standard app	physical
Indicator	layer	medium
removal from	,	From local
host	protocol Standard	
Masquerad-		system
ing	non-app	From
NTFS	layer	network
Extended	protocol	resource
Attributes	Standard	From
Obfuscated	encryption	
Payload	cipher	removable 
Rundll32	Uncommonly	media
Scripting	used port	Scheduled
Software		transfer
Packing		
Timestomn		



Q

#### Public Website – attack.mitre.org



Main page
Random page
Help
Contribute
Browse Techniques
All Techniques

Persistence

Tactics

Privilege Escalation Credential Access Host Enumeration Defense Evasion Lateral Movement Execution Command and Control

Tools

Printable version Permanent link

Exfiltration

Follow @MITREattack

DLL injection

#### Contents [hide]

- 1 Technical Description
- 2 Examples

Page Discussion

- 3 Detection
- 4 References

#### Technical Description

DLL injection is used to run code in the context of another process by causing the other process to load and execute code within a DLL. Running code in the context of another process provides many benefits such as access to the process's memory and permissions. It also allows the adversary to operate covertly. A more sophisticated kind of DLL injection, reflective DLL injection, loads a DLL without calling the normal Windows API calls, potentially frustrating DLL load monitoring. Numerous methods of DLL injection on Windows exist including: modifying the registry, creating remote threads, Windows hooking APIs, and DLL pre-loading. [1][2]

#### Examples

DLL loading techniques have been used by APTs such as Icefog $^{[3]}$  and RATs such as Taidoor $^{[4]}$  and PoisonIvy. $^{[5]}$ 

#### Detection

Monitor API calls that can be used to begin execution within another process (such as CreateRemoteThread) and API calls that can be used to modify memory within another process (such as WriteProcessMemory). There are legitimate programs that use DLL injection to perform certain functions, so if a process is injected it is not necessarily malicious. For this reason, build a known "normal" of DLL injections and compare new DLL injections for outliers.

#### References

- 1. ↑ Kuster, R. (2003, August 20). Three Ways to Inject Your Code into Another Process. Retrieved November 12, 2014. ₺
- 2. ↑ DLL injection. (n.d.). Retrieved November 12, 2014 from Wikipedia. 

  ☑
- 3. ↑ Kaspersky Lab Global Research and Analysis Team. (2013). THE 'ICEFOG' APT: A TALE OF CLOAK AND THREE DAGGERS. Retrieved November 12, 2014. 🔼

#### DLL injection

1055

Search

Read View form View source View history

Platform Windows Server 2003, Windows Server 2008.

> Windows Server 2012, Windows XP, Windows 7,

Windows 8,

Windows Server 2003 R2,

Windows Server 2008 R2, Windows Server 2012 R2.

Windows Vista Windows 8.1

Permissions Administrator, SYSTEM,

Use

Effective Administrator, SYSTEM,

Permissions Use

Required

Data Sources API monitoring, Windows

Registry, File monitoring, API monitoring, Process

monitoring

Groups/Malware Icefog (Group), Poison Ivy

(Malware), Taidoor

(Malware)

Defense Process whitelisting, Bypassed Antivirus

Alluvilus



#### **Questions?**

# More information: attack.mitre.org

Questions and contributions: attack@mitre.org

**Twitter:** 

**@MITREattack** 

