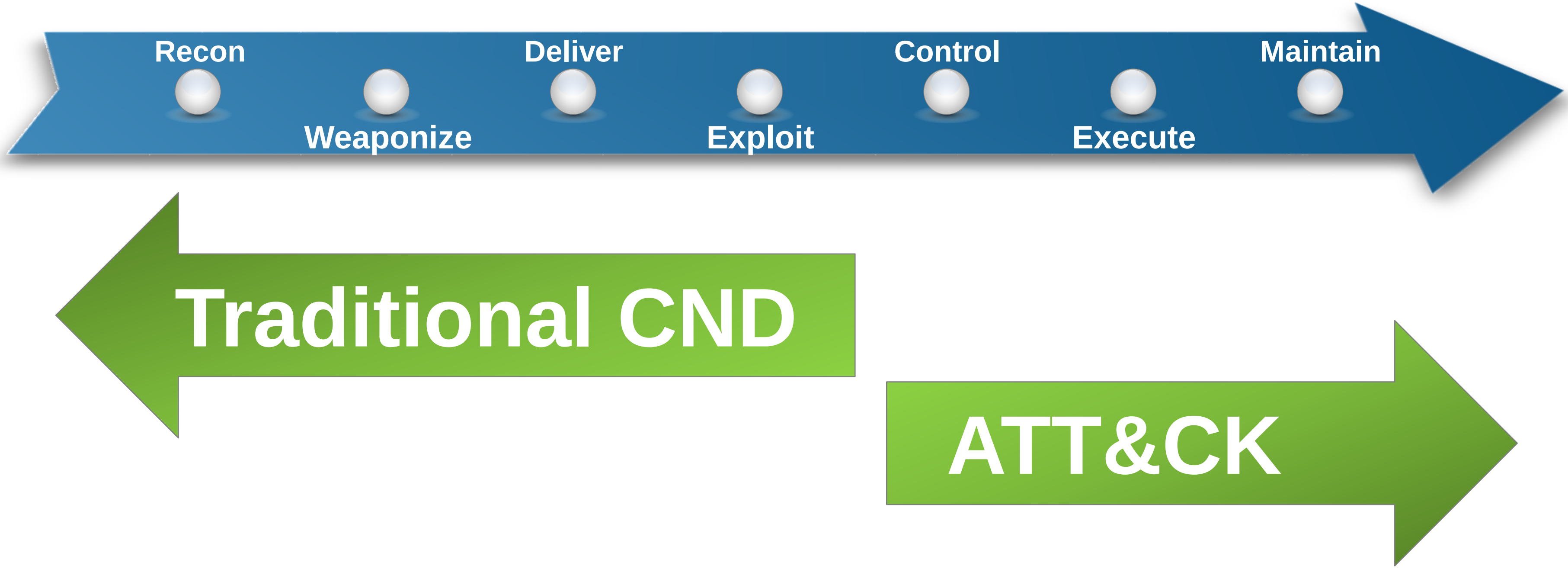
Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™)

Blake Strom

August 2015

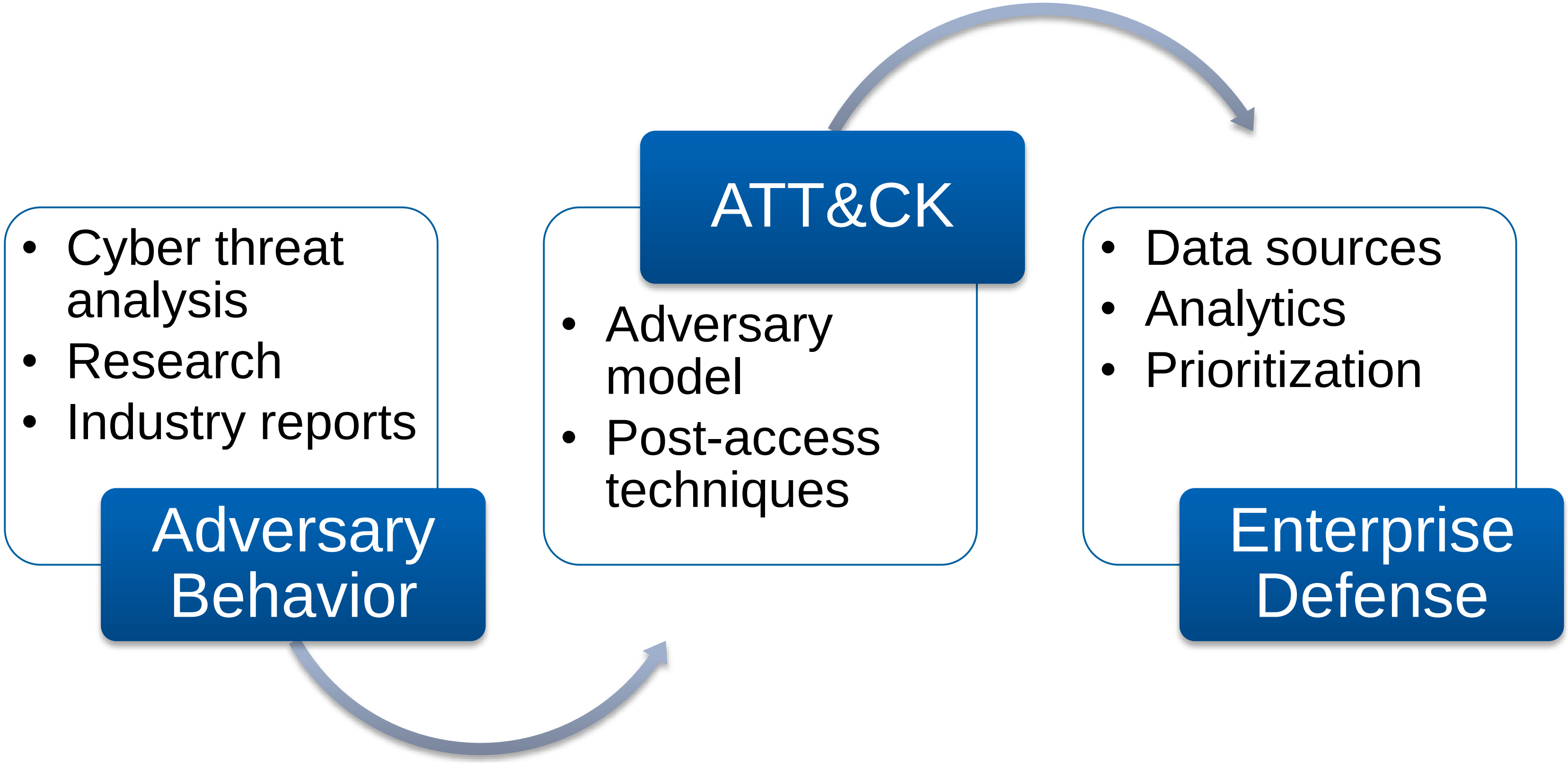
Approved for Public Release; Distribution Unlimited. Case Number 15-1288

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

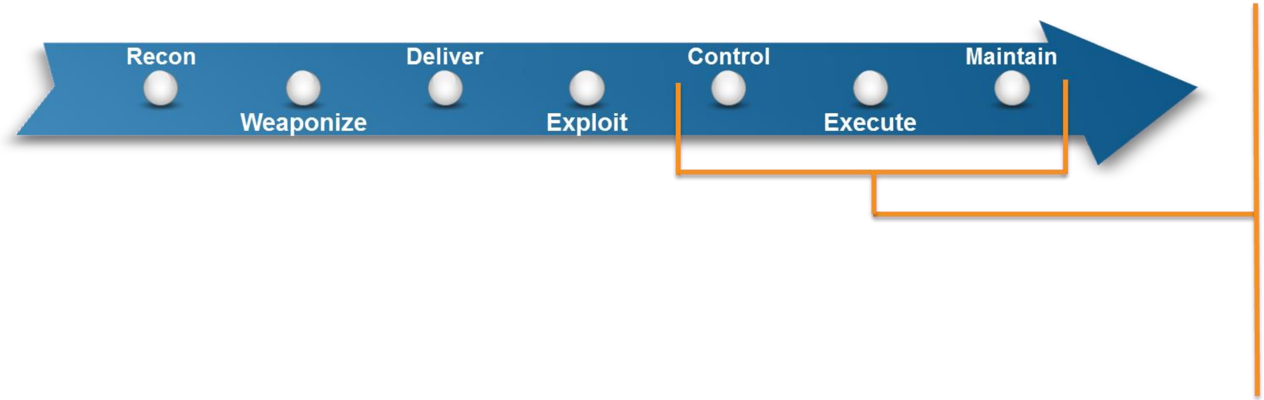
ATT&CK

- 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

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

Image source: www.mrpotatohead.net

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
Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features	Accessibility Features	Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor	AddMonitor	DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack	DLL Search Order Hijack	Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers	Edit Default File Handlers	File System Logical Offsets	Credential manipulation	Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service	New Service	Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception	Path Interception	Rootkit		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task	Scheduled Task	Bypass UAC		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness	Service File Permission Weakness	DLL Injection		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification	Shortcut Modification	Indicator blocking on host		Service enumeration	Remote Services	Windows management instrumentation	Standard app layer protocol	From local system
Web shell	Web shell	Indicator removal from tools		Window enumeration	Replication through removable media	Windows remote management	Standard non-app layer protocol	From network resource
BIOS	Bypass UAC	Indicator removal from host			Shared webroot		Standard encryption cipher	From removable media
Hypervisor Rootkit	DLL Injection	Masquerading			Taint shared content		Uncommonly used port	Scheduled transfer
Logon Scripts	Exploitation of Vulnerability	NTFS Extended Attributes			Windows admin shares			
Master Boot Record		Obfuscated Payload						
Mod. Exist’g Service		Rundll32						
Registry Run Keys		Scripting						
Serv. Reg. Perm. Weakness		Software Packing						
Windows Mgmt Instr. Event Subsc.		Timestomp						
Winlogon Helper DLL								

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

Publically Reported Technique Use

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features	Accessibility Features	Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor	AddMonitor	DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack	DLL Search Order Hijack	Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers	Edit Default File Handlers	File System Logical Offsets	Credential manipulation	Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service	New Service	Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception	Path Interception	Rootkit		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task	Scheduled Task	Bypass UAC		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness	Service File Permission Weakness	DLL Injection		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification	Shortcut Modification	Indicator blocking on host		Service enumeration	Remote Services	Windows management instrumentation	Standard app layer protocol	From local system
Web shell	Web shell	Indicator removal from tools		Window enumeration	Replication through removable media	Windows remote management	Standard non-app layer protocol	From network resource
BIOS	Bypass UAC	Indicator removal from host			Shared webroot		Standard encryption cipher	From removable media
Hypervisor Rootkit	DLL Injection	Masquerading			Taint shared content		Uncommonly used port	Scheduled transfer
Logon Scripts	Exploitation of Vulnerability	NTFS Extended Attributes			Windows admin shares			
Master Boot Record		Obfuscated Payload						
Mod. Exist’g Service		Rundll32						
Registry Run Keys		Scripting						
Serv. Reg. Perm. Weakness		Software Packing						
Windows Mgmt Instr. Event Subsc.		Timestomp						
Winlogon Helper DLL								

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

Notional Defense Gaps

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
🟨 Legitimate Credentials	🟨 Legitimate Credentials	🟨 Legitimate Credentials	🟨 Credential Dumping	🟨 Account enumeration	🟥 Application deployment software	🟥 Command Line	🟥 Commonly used port	🟥 Automated or scripted exfiltration
🟥 Accessibility Features	🟥 Accessibility Features	🟥 Binary Padding	🟥 Credentials in Files	🟨 File system enumeration	🟨 Exploitation of Vulnerability	🟥 File Access	🟥 Comm through removable media	🟩 Data compressed
🟥 AddMonitor	🟥 AddMonitor	🟥 DLL Side-Loading	🟥 Network Sniffing	🟨 Group permission enumeration	🟨 Logon scripts	🟨 PowerShell	🟨 Custom application layer protocol	🟥 Data encrypted
🟥 DLL Search Order Hijack	🟥 DLL Search Order Hijack	🟨 Disabling Security Tools	🟨 User Interaction	🟨 Local network connection enumeration	🟨 Pass the hash	🟥 Process Hollowing	🟥 Custom encryption cipher	🟥 Data size limits
🟩 Edit Default File Handlers	🟩 Edit Default File Handlers	🟥 File System Logical Offsets	🟨 Credential manipulation	🟨 Local networking enumeration	🟨 Pass the ticket	🟨 Registry	🟥 Data obfuscation	🟥 Data staged
🟩 New Service	🟩 New Service	🟥 Process Hollowing		🟨 Operating system enumeration	🟨 Peer connections	🟨 Rundll32	🟨 Fallback channels	🟨 Exfil over C2 channel
🟥 Path Interception	🟥 Path Interception	🟨 Rootkit		🟨 Owner/User enumeration	🟩 Remote Desktop Protocol	🟩 Scheduled Task	🟨 Multiband comm	🟨 Exfil over alternate channel to C2 network
🟩 Scheduled Task	🟩 Scheduled Task	🟥 Bypass UAC		🟨 Process enumeration	🟨 Windows management instrumentation	🟨 Service Manipulation	🟥 Multilayer encryption	🟥 Exfil over other network medium
🟩 Service File Permission Weakness	🟩 Service File Permission Weakness	🟨 DLL Injection		🟩 Security software enumeration	🟨 Windows remote management	🟥 Third Party Software	🟥 Peer connections	🟥 Exfil over physical medium
🟥 Shortcut Modification	🟥 Shortcut Modification	🟥 Indicator blocking on host		🟨 Service enumeration	🟩 Remote Services	🟨 Windows management instrumentation	🟥 Standard app layer protocol	🟨 From local system
🟨 Web shell	🟨 Web shell	🟥 Indicator removal from tools		🟨 Window enumeration	🟥 Replication through removable media	🟨 Windows remote management	🟥 Standard non-app layer protocol	🟨 From network resource
🟥 BIOS	🟥 Bypass UAC	🟥 Indicator removal from host			🟥 Shared webroot		🟥 Standard encryption cipher	🟨 From removable media
🟥 Hypervisor Rootkit	🟨 DLL Injection	🟥 Masquerading			🟥 Taint shared content		🟨 Uncommonly used port	🟨 Scheduled transfer
🟩 Logon Scripts	🟨 Exploitation of Vulnerability	🟨 NTFS Extended Attributes			🟩 Windows admin shares			
🟥 Master Boot Record		🟥 Obfuscated Payload						
🟩 Mod. Exist’g Service		🟨 Rundll32						
🟩 Registry Run Keys		🟥 Scripting						
🟩 Serv. Reg. Perm. Weakness		🟥 Software Packing						
🟩 Windows Mgmt Instr. Event Subsc.		🟩 Timestomp						
🟩 Winlogon Helper DLL								

🟩 Detect	🟨 Partially Detect	🟥 No Detect

Adversary Visibility at the Perimeter

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
🟥 Legitimate Credentials	🟥 Legitimate Credentials	🟥 Legitimate Credentials	🟥 Credential Dumping	🟥 Account enumeration	🟥 Application deployment software	🟥 Command Line	🟨 Commonly used port	🟥 Automated or scripted exfiltration
🟥 Accessibility Features	🟥 Accessibility Features	🟨 Binary Padding	🟥 Credentials in Files	🟥 File system enumeration	🟥 Exploitation of Vulnerability	🟥 File Access	🟨 Comm through removable media	🟥 Data compressed
🟥 AddMonitor	🟥 AddMonitor	🟥 DLL Side-Loading	🟥 Network Sniffing	🟥 Group permission enumeration	🟥 Logon scripts	🟥 PowerShell	🟨 Custom application layer protocol	🟥 Data encrypted
🟥 DLL Search Order Hijack	🟥 DLL Search Order Hijack	🟥 Disabling Security Tools	🟥 User Interaction	🟥 Local network connection enumeration	🟥 Pass the hash	🟥 Process Hollowing	🟨 Custom encryption cipher	🟨 Data size limits
🟥 Edit Default File Handlers	🟥 Edit Default File Handlers	🟥 File System Logical Offsets	🟥 Credential manipulation	🟥 Local networking enumeration	🟥 Pass the ticket	🟥 Registry	🟨 Data obfuscation	🟥 Data staged
🟥 New Service	🟥 New Service	🟥 Process Hollowing		🟥 Operating system enumeration	🟥 Peer connections	🟥 Rundll32	🟨 Fallback channels	🟨 Exfil over C2 channel
🟥 Path Interception	🟥 Path Interception	🟥 Rootkit		🟥 Owner/User enumeration	🟥 Remote Desktop Protocol	🟥 Scheduled Task	🟨 Multiband comm	🟨 Exfil over alternate channel to C2 network
🟥 Scheduled Task	🟥 Scheduled Task	🟥 Bypass UAC		🟥 Process enumeration	🟥 Windows management instrumentation	🟥 Service Manipulation	🟨 Multilayer encryption	🟨 Exfil over other network medium
🟥 Service File Permission Weakness	🟥 Service File Permission Weakness	🟥 DLL Injection		🟥 Security software enumeration	🟥 Windows remote management	🟥 Third Party Software	🟨 Peer connections	🟥 Exfil over physical medium
🟥 Shortcut Modification	🟥 Shortcut Modification	🟥 Indicator blocking on host		🟥 Service enumeration	🟥 Remote Services	🟥 Windows management instrumentation	🟨 Standard app layer protocol	🟥 From local system
🟥 Web shell	🟥 Web shell	🟨 Indicator removal from tools		🟥 Window enumeration	🟥 Replication through removable media	🟥 Windows remote management	🟨 Standard non-app layer protocol	🟥 From network resource
🟥 BIOS	🟥 Bypass UAC	🟥 Indicator removal from host			🟥 Shared webroot		🟨 Standard encryption cipher	🟥 From removable media
🟥 Hypervisor Rootkit	🟥 DLL Injection	🟥 Masquerading			🟥 Taint shared content		🟨 Uncommonly used port	🟨 Scheduled transfer
🟥 Logon Scripts	🟥 Exploitation of Vulnerability	🟥 NTFS Extended Attributes			🟥 Windows admin shares			
🟥 Master Boot Record		🟥 Obfuscated Payload						
🟥 Mod. Exist’g Service		🟥 Rundll32						
🟥 Registry Run Keys		🟥 Scripting						
🟥 Serv. Reg. Perm. Weakness		🟨 Software Packing						
🟥 Windows Mgmt Instr. Event Subsc.		🟥 Timestomp						
🟥 Winlogon Helper DLL								

🟩 Full Visibility 🟨 Partially Visibility 🟥 No Visibility

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

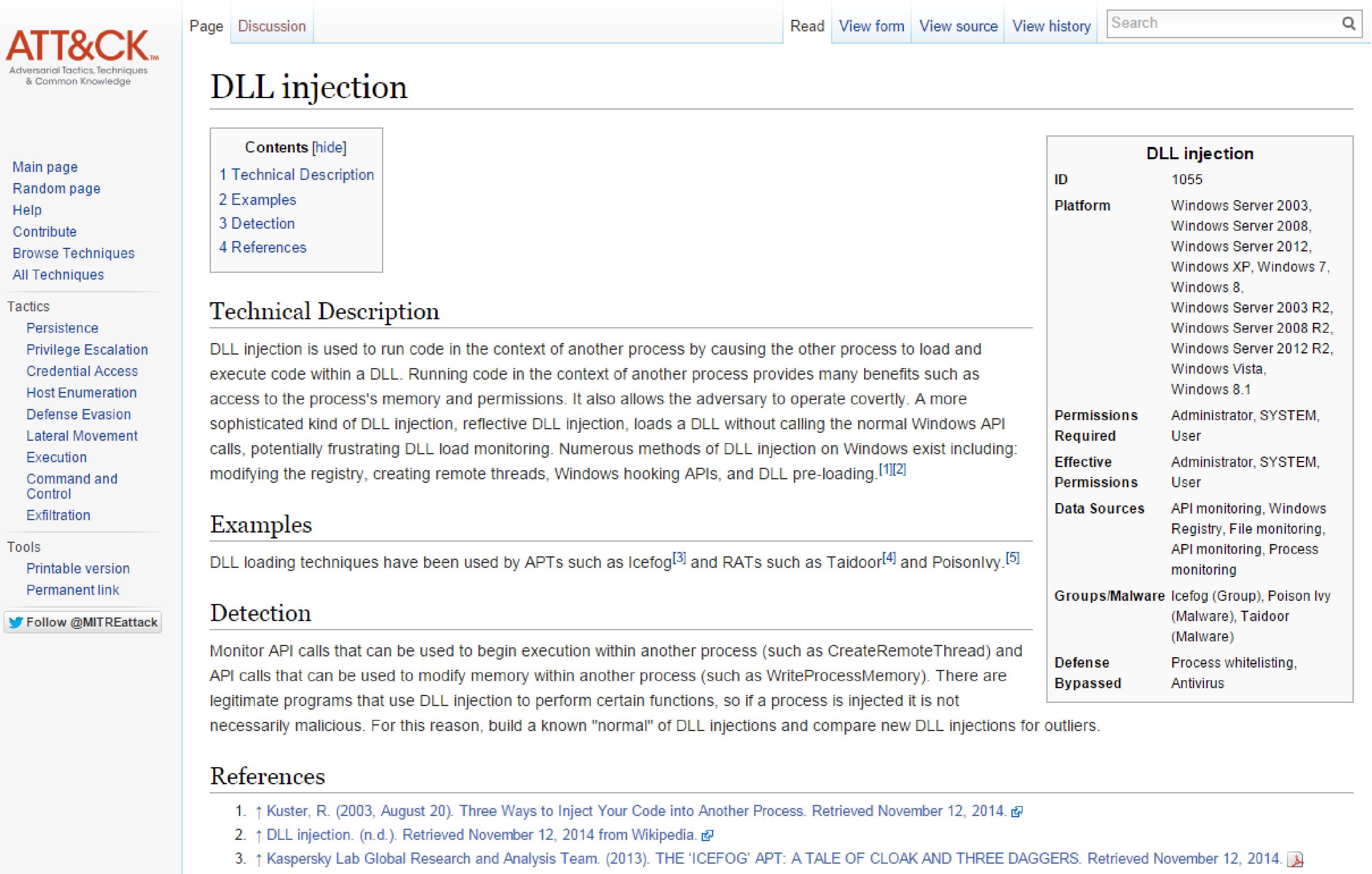
Adversary Visibility at the Perimeter

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

🟩 **Full Visibility** 🟨 **Partially Visibility** 🟥 **No Visibility**

Public Website – attack.mitre.org



DLL injection

DLL injection	
ID	1055
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 Required	Administrator, SYSTEM, User
Effective Permissions	Administrator, SYSTEM, User
Data Sources	API monitoring, Windows Registry, File monitoring, API monitoring, Process monitoring
Groups/Malware	Icefog (Group), Poison Ivy (Malware), Taidoor (Malware)
Defense Bypassed	Process whitelisting, Antivirus

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.

Questions?

More information:

attack.mitre.org

Questions and contributions:

attack@mitre.org

Twitter:

@MITREattack