



Systems and Internet Infrastructure Security

Network and Security Research Center
Department of Computer Science and Engineering
Pennsylvania State University, University Park PA

CMPSC 447 ***Anatomy of*** ***an Attack***

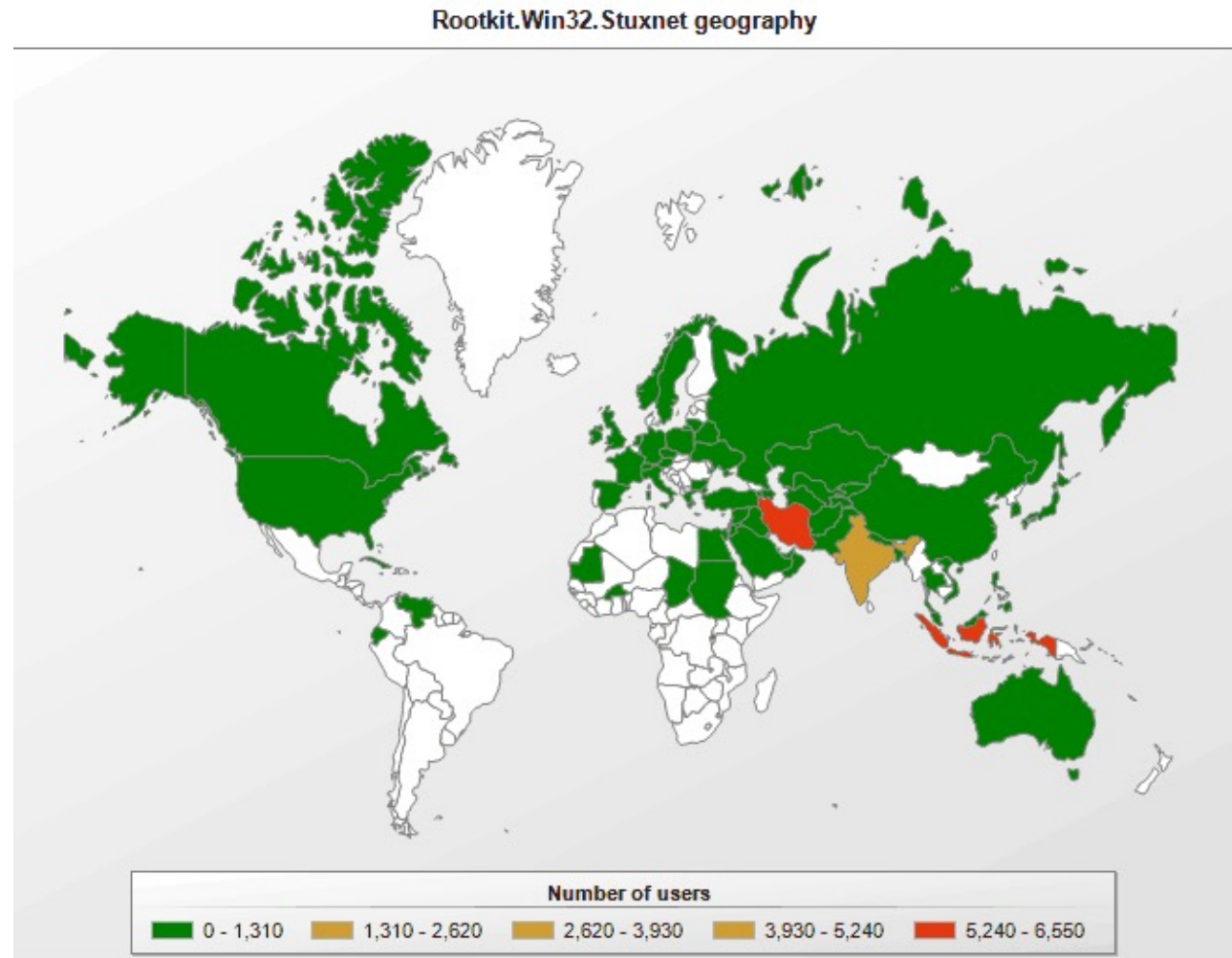
Trent Jaeger

*Systems and Internet Infrastructure Security (SIIS) Lab
Computer Science and Engineering Department
Pennsylvania State University*

Adversarial Operations

- We have examined a variety of attack types
 - ▶ **Question:** How do adversaries really use such attacks in practice to execute attacks
- Today, we examine one of the more elaborate attacks executed
 - ▶ Where we have a good idea how it performed
- Then, we will examine the what defenders think about how attacks proceed
 - ▶ **MITRE ATT&CK**

Real World Example: Stuxnet Worm



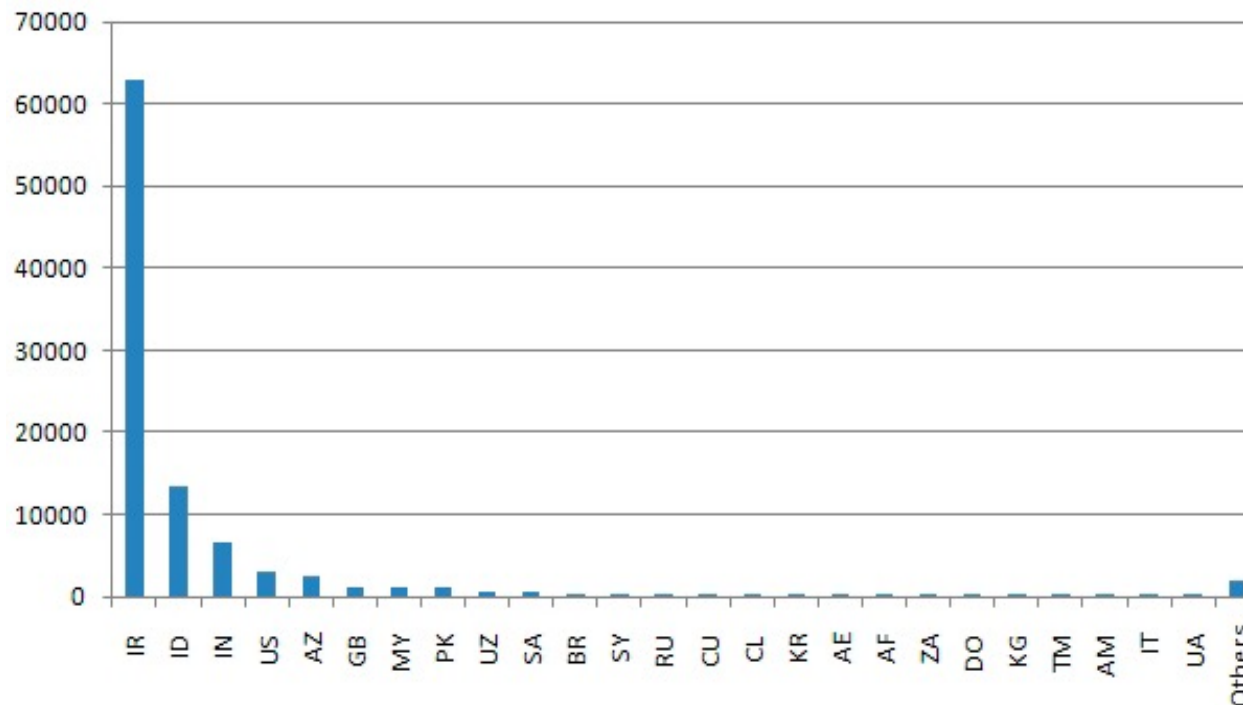
Slides by pmateti@wright.edu from many sources

Stuxnet: Overview

- June 2010: A worm targeting Siemens WinCC industrial control system.
- Targets high speed variable-frequency programmable logic motor controllers from just two vendors: Vacon (Finland) and Fararo Paya (Iran)
- Only when the controllers are running at 807Hz to 1210Hz. Makes the frequency of those controllers vary from 1410Hz to 2Hz to 1064Hz.
- <http://en.wikipedia.org/wiki/Stuxnet>

Stuxnet Infection Statistics

- 29 September 2010, From Symantec
- Infected Hosts



Industrial Control Systems (ICS)



- ICS are operated by a specialized, assembly-like code on programmable logic controllers (PLCs).
- The PLCs are programmed typically from Windows computers (PCs).
- The ICS are not connected to the Internet – even the PCs used.
- ICS usually consider availability and ease of maintenance first and security last.
- ICS consider the “**airgap**” as sufficient security.

Seimens SIMATIC PLCs



Nuclear Centrifuges

- Uranium-235 separation efficiency is **critically dependent on the centrifuges' speed of rotation**
- Separation is theoretically proportional to the peripheral speed raised to the 4th power. So any increase in peripheral speed is helpful.
- That implies you need strong tubes, but brute strength isn't enough: centrifuge designs also run into **problems with “shaking”** as they pass through naturally resonant frequencies
 - ▶ “shaking” at high speed can cause catastrophic failures to occur.
 - ▶ www.fas.org/programs/ssp/nukes/fuelcycle/centrifuges/engineering.html

Timeline

- 2009 June: Earliest Stuxnet seen
 - Does not have signed drivers
- 2010 Jan: Stuxnet driver signed
 - With a valid certificate belonging to Realtek Semiconductors
- 2010 June: Virusblokada reports WV32.Stuxnet
 - Verisign revokes Realtek certificate
- 2010 July: Anti-virus vendor Eset identifies new Stuxnet driver
 - With a valid certificate belonging to JMicon Technology Corp
- 2010 July: Siemens report they are investigating malware SCADA systems
 - Verisign revokes JMicon certificate



Stuxnet: Tech Overview

- Components used
 - ▶ Zero-day exploits
 - ▶ Windows rootkit
 - ▶ PLC rootkit (first ever)
 - ▶ Antivirus evasion
 - ▶ Peer-to-Peer updates
 - ▶ Signed driver with a valid certificate
- Command and control interface
- Stuxnet consists of a large .dll file
- Designed to sabotage industrial processes controlled by Siemens SIMATIC WinCC and PCS 7 systems.

Stuxnet: Steps

- What do we need to know to launch an attack?
- What do we need to do to initiate an attack?
- How do we get the malware onto a disconnected host?
- How to we change the operation of the PLC?
- Without being detected?

Attack Scenario (Conjecture)

- Reconnaissance
 - Each PLC is configured in a unique manner
 - Targeted ICS's schematics needed
 - Design docs stolen by an insider?
 - Retrieved by an early version of Stuxnet
 - Stuxnet developed with the goal of sabotaging a specific set of ICS.
- Development
 - Mirrored development environment needed
 - ICS Hardware
 - PLC modules
 - PLC development software
 - Estimation
 - 6+ man-years by an experienced and well-funded development team

Attack Scenario (2)

- The malicious binaries need to be signed to avoid suspicion
 - ▶ Two digital certificates were compromised.
 - ▶ High probability that the digital certificates/keys were stolen from the companies' premises.
 - ▶ Realtek and JMicron are in close proximity.
- Initial Infection
 - ▶ Stuxnet needed to be introduced to the targeted environment
 - Insider
 - Third party, such as a contractor
 - ▶ Delivery method
 - USB drive
 - Windows Maintenance Laptop
 - Targeted email attack

Attack Scenario (3)

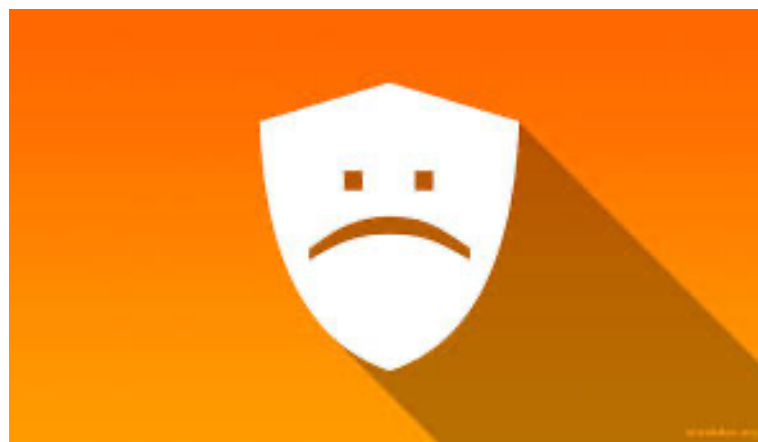
- Infection Spread
 - ▶ Look for Windows computer used to program the PLC's
 - The Field PG are typically not connected to network
 - Spread the Infection on computers on the local LAN
 - ▶ Zero-day vulnerabilities
 - ▶ Two-year old vulnerability
 - ▶ Spread to all available USB drives
 - ▶ When a USB drive is connected to the Field PG, the Infection jumps to the Field PG
 - The “airgap” is thus breached

Attack Scenario (4)

- Target Infection of Field PG
 - ▶ Look for Specific PC
 - Running Step 7 Operating System
 - ▶ Change PLC code
 - Sabotage system
 - Hide modifications
 - ▶ Command and Control may not be possible
 - Due to the “airgap”
 - Functionality already embedded

Bypassing Intrusion Detection

- Antivirus software monitors library calls
 - ▶ Especially for loads of new libraries
 - ▶ How evade that? And stay away from detection?



Bypassing Intrusion Detection

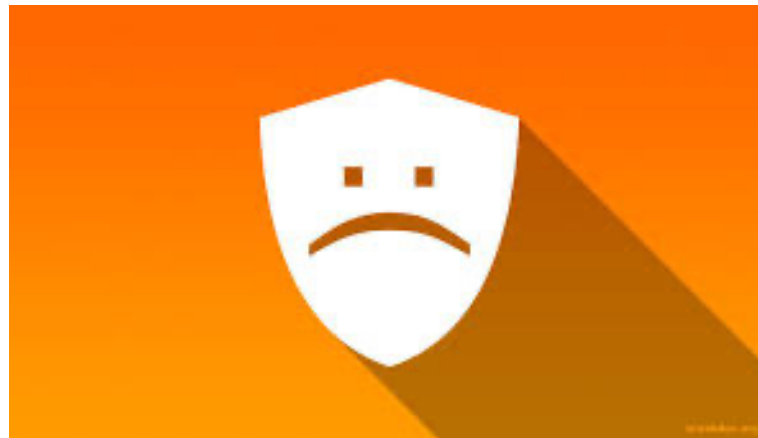
- Stuxnet calls LoadLibrary
 - ▶ With a specially crafted file name that does not exist
 - ▶ Which causes LoadLibrary to fail.
- However, W32.Stuxnet has hooked Ntdll.dll
 - ▶ To monitor specially crafted file names.
 - ▶ Mapped to a location specified by W32.Stuxnet.
 - ▶ Where a .dll file was stored by the Stuxnet previously.

Code Injection

- Stuxnet accounted for trusted Windows processes or security products
 - ▶ Lsass.exe, Winlogin.exe, Svchost.exe
 - ▶ Kaspersky KAV (avp.exe), McAfee (Mcshield.exe), AntiVir (avguard.exe)
 - ▶ BitDefender (bdagent.exe), Etrust (UmxCfg.exe), F-Secure (fsdfwd.exe)
 - ▶ Symantec (rtvscan.exe), Symantec Common Client (ccSvcHst.exe)
 - ▶ Eset NOD32 (ekrn.exe), Trend Pc-Cillin (tmpproxy.exe)
- Stuxnet detects the version of the security product and based on the version number **adapts its injection process**

Guiding the Malware

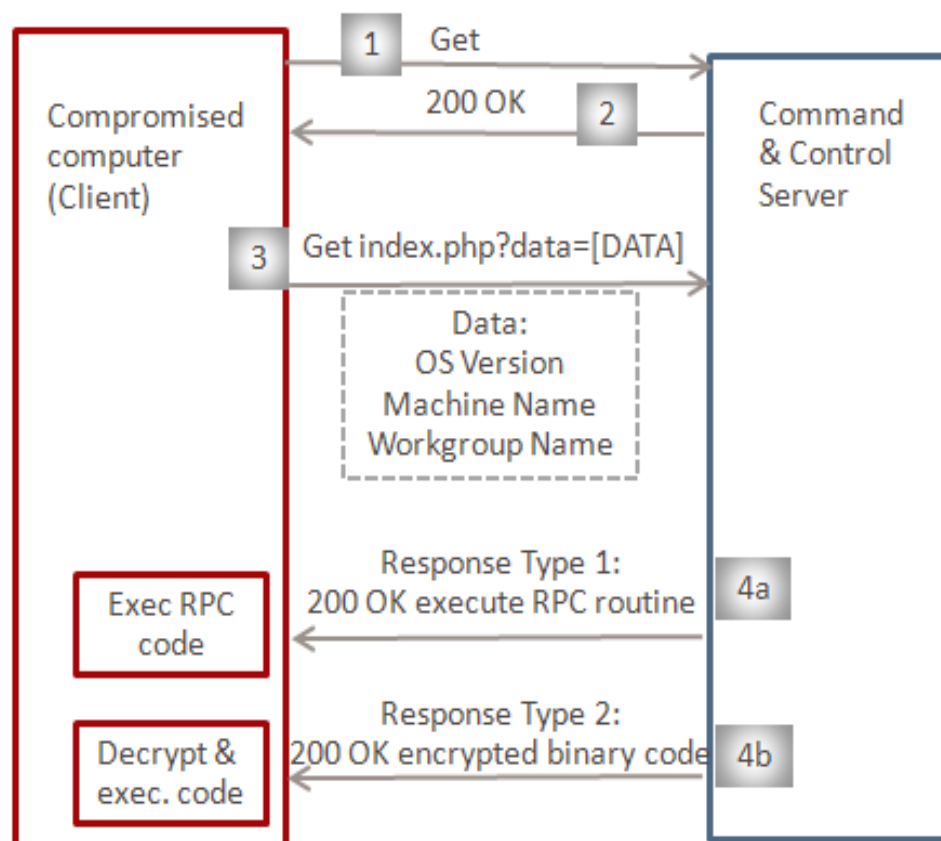
- The malware may need to reconfiguration to propagate the attack
 - ▶ How do we do that?



Command & Control

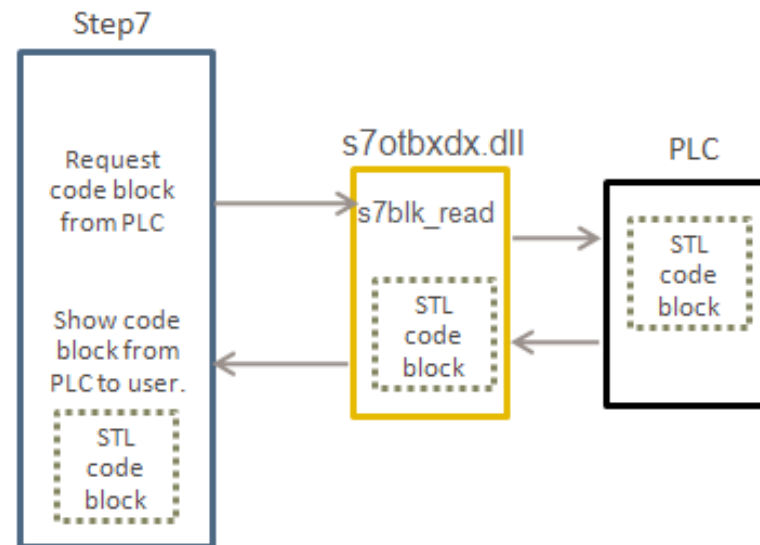
- Stuxnet tests if it can connect to
 - ▶ www.windowsupdate.com
 - ▶ www.msn.com
 - ▶ On port 80
- Contacts the **command and control** server
 - ▶ www.mypremierfutbol.com
 - ▶ www.todaysfutbol.com
 - ▶ The two URLs above previously pointed to servers in Malaysia and Denmark
 - ▶ Sends info about the compromised computer

Command & Control (2)



1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code

Modifying PLC code



Modifying PLC's

- The end goal of Stuxnet is to infect specific types of PLCs
- Original s7otbx.dll is responsible for handling exchange between the programming device and the PLC
 - ▶ By replacing this .dll file with its own, Stuxnet is able to perform the following actions:
 - Monitor PLC blocks being written to and read from the PLC
 - Infect a PLC by inserting its own blocks
 - Remove infected statements when reading from the PLC

Stuxnet Conclusion

- Stuxnet is a significant milestone in malicious code history
 - ▶ It is the first to exploit multiple zero-day vulnerabilities.
 - ▶ Used two (compromised) digital certificates.
 - ▶ Injected code into industrial control systems.
 - ▶ Hid the code from the operator for several months
- Stuxnet is of great complexity
 - ▶ Requiring significant resources to develop
- Stuxnet has highlighted that direct attacks on critical infrastructure are possible.

References

- Nicolas Falliere, Liam O Murchu, and Eric Chie, “W32.Stuxnet Dossier”, February 2011, Symantec.com
- Ralph Langner, “Cracking Stuxnet, a 21st-century cyber weapon”, <http://www.ted.com/>, Mar 31, 2011.
- Eric Byres, Andrew Ginter and Joel Langill, Stuxnet Report: A System Attack, A five part series, www.isssource.com/stuxnet-report-a-system-attack/, March 2011
- “Cyber War, Cyber Terrorism and Cyber Espionage,” <http://pages.uoregon.edu/joe/cyberwar/cyberwar.ppt>
- ACK: Many sources on the web. I (pmateti@wright.edu) merely assembled the slides. May 2011.

MITRE ATT&CK Framework

- Knowledge base of adversary tactics and techniques based on real-world observations
 - ▶ <https://attack.mitre.org>
- Tactics and the techniques adversaries may use to implement those tactics
 - ▶ And mitigations for those techniques
 - ▶ Hopefully, helping defenders to prevent and detect attacks

MITRE ATT&CK Framework



- MITRE ATT&CK Philosophy Document
 - ▶ https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- Originated out of a project to document and categorize post-compromise adversary tactics and techniques
 - ▶ And procedural methods to implement techniques
- Ideally, a defender would have coverage for all attack tactics and techniques (**attack coverage**)
 - ▶ But “is unrealistic”, so monitor where use is possible

ATT&CK Matrix

- MITRE ATT&CK Matrix

► <https://attack.mitre.org/matrices/enterprise/>

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 23 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection			Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Group Policy Modification	Exploitation for Defense Evasion	Modify Authentication Process (2)	File and Directory Permissions Modification (2)	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Firmware Corruption	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Hijack Execution Flow (10)	File and Directory Permissions Modification (2)	Network Sniffing	OS Credential Dumping (8)	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Inhibit System Recovery	
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Impair Defenses (5)	Group Policy Modification	Steal Application Access Token	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Removable Media	Ingress Tool Transfer	Network Denial of Service (2)	
	Windows Management Instrumentation	External Remote Services	Indicator Removal on Host (6)	Hide Artifacts (4)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
		Hijack Execution Flow (10)	Indirect Command Execution	Hijack Execution Flow (10)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop
		Implant Container Image	Masquerading (6)	Impair Defenses (5)	Unsecured Credentials (6)	Password Policy Discovery		Input Capture (4)	Non-Standard Port		System Shutdown/Reboot
		Office Application Startup (6)	Modify Authentication Process (2)	Indicator Removal on Host (6)		Peripheral Device Discovery		Man in the Browser	Protocol Tunneling		
		Pre-OS Boot (3)	Modify Registry	Indirect Command Execution		Process Discovery		Man-in-the-Middle (1)	Proxy (4)		
		Scheduled Task/Job (5)	Obfuscated Files or Information (5)	Indirect Command Execution		Query Registry		Screen Capture	Remote Access Software		
		Server Software Component (3)	Pre-OS Boot (3)	Indirect Command Execution		Remote System Discovery		Video Capture	Traffic Signaling (1)		
		Traffic Signaling (1)	Process Injection (11)	Indirect Command Execution		Software Discovery (1)			Web Service (3)		
		Valid Accounts (4)	Revert Cloud Instance	Indirect Command Execution		System Information Discovery					
			Rogue Domain Controller	Indirect Command Execution		System Network Configuration Discovery					
			Rootkit	Indirect Command Execution		System Network Connections Discovery					
			Signed Binary Proxy Execution (10)	Indirect Command Execution		System Owner/User Discovery					
			Signed Script Proxy Execution (1)	Indirect Command Execution		System Service Discovery					
			Subvert Trust Controls (4)	Indirect Command Execution							
			Template Injection	Indirect Command Execution							
			Traffic Signaling (1)	Indirect Command Execution							
			Trusted Developer Utilities	Indirect Command Execution							

ATT&CK Matrix

- Organized by **tactics** (columns) with **techniques**
 - Where there are **procedures** to implement techniques
- Tactics
 - Adversary's tactical objective: the reason for performing an action
- Techniques
 - “how” an adversary may achieve a tactical objective
- Procedures
 - Specific implementation of a technique

ATT&CK Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- Reconnaissance
- Resource Development

ATT&CK Tactics in Action



- Initial Access, Discovery, and Credential access
 - Gain and expand access (via secrets) in an environment
 - What was that for Stuxnet?
- Execution
 - “Execution of adversary-controlled code”
 - How Stuxnet?
- Collection and Exfiltration
 - Steal data from the domain
 - Did Stuxnet do that?

ATT&CK Tactics in Action

- Persistence and Defense Evasion
 - ▶ “to persist in the target environment” “undetected”
 - ▶ How did Stuxnet do that?
- Privilege Escalation and Lateral Movement
 - ▶ Gain more permissions in the environment and control more components of same privilege
 - ▶ How for Stuxnet?
- Command and Control
 - ▶ Method to obtain commands for malware
 - ▶ Did Stuxnet do that?

ATT&CK Matrix

- Familiarize yourself with the concepts in the ATT&CK Matrix
 - And use of each type of tactics in the matrix
- I can give you attack scenarios and ask questions about how those scenarios relate to tactics, etc.

Take Away

- Today, we examined attacks “in the large”
- From the perspective of one of the more complex attack campaigns launched
 - ▶ [Stuxnet](#)
- Stuxnet demonstrates several features of an attack
 - ▶ Articulated in the MITRE ATT&CK Framework
 - ▶ [Tactics](#), [Techniques](#), and [Procedures](#)
- Not practical to articulate all the attack procedures or perhaps even techniques yet