CALDERA

Scott Taylor

EU ATT&CK Community Workshop

May 19th, 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

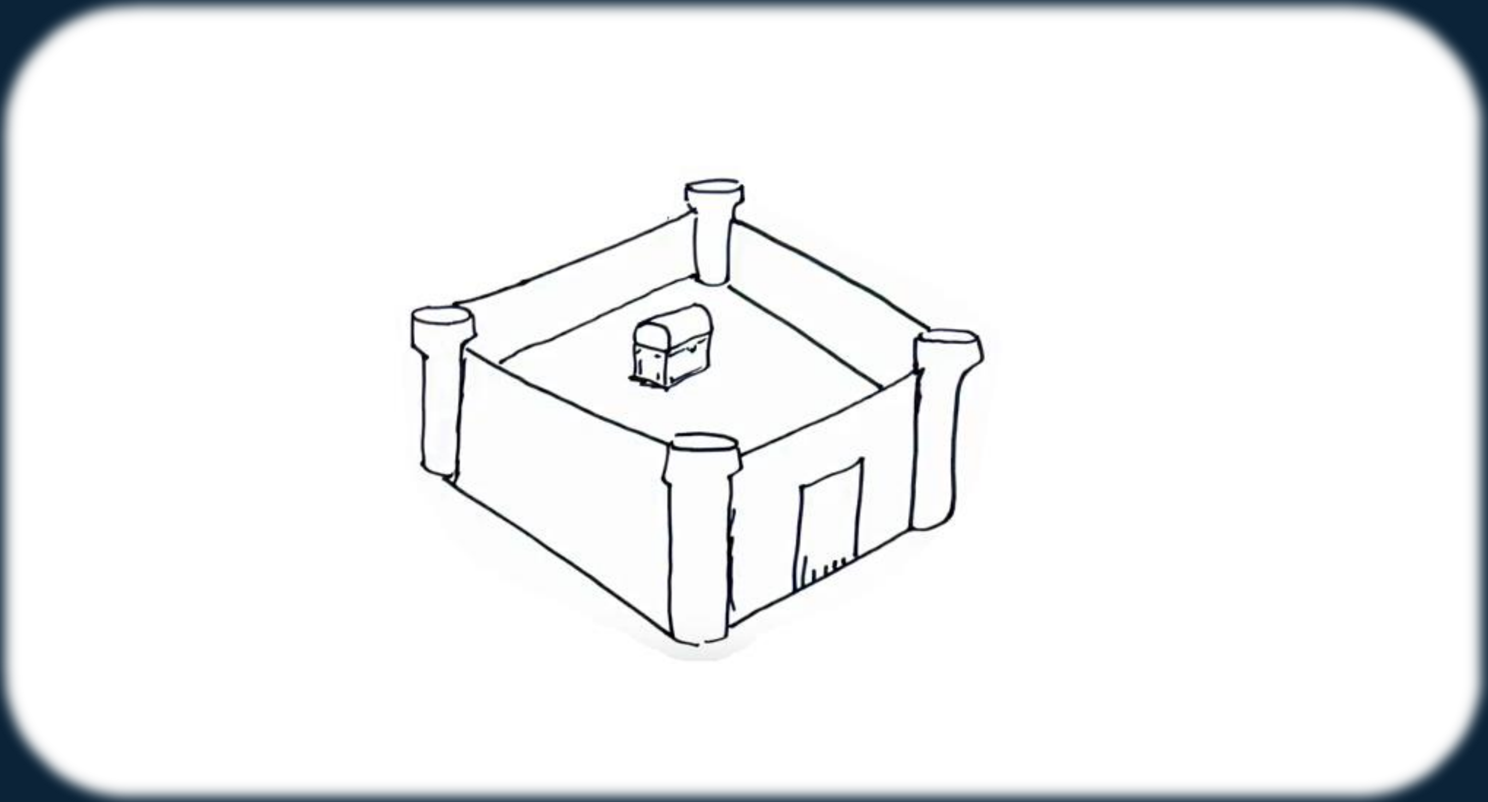
Speaker Background

- Squad Leader for MITRE CALDERA team
- Background in system administration
- Cisco, Splunk, Red Hat, OSCP certifications
- Twitter & GitHub: @scottctaylor12

MITRE

The False Negative Problem

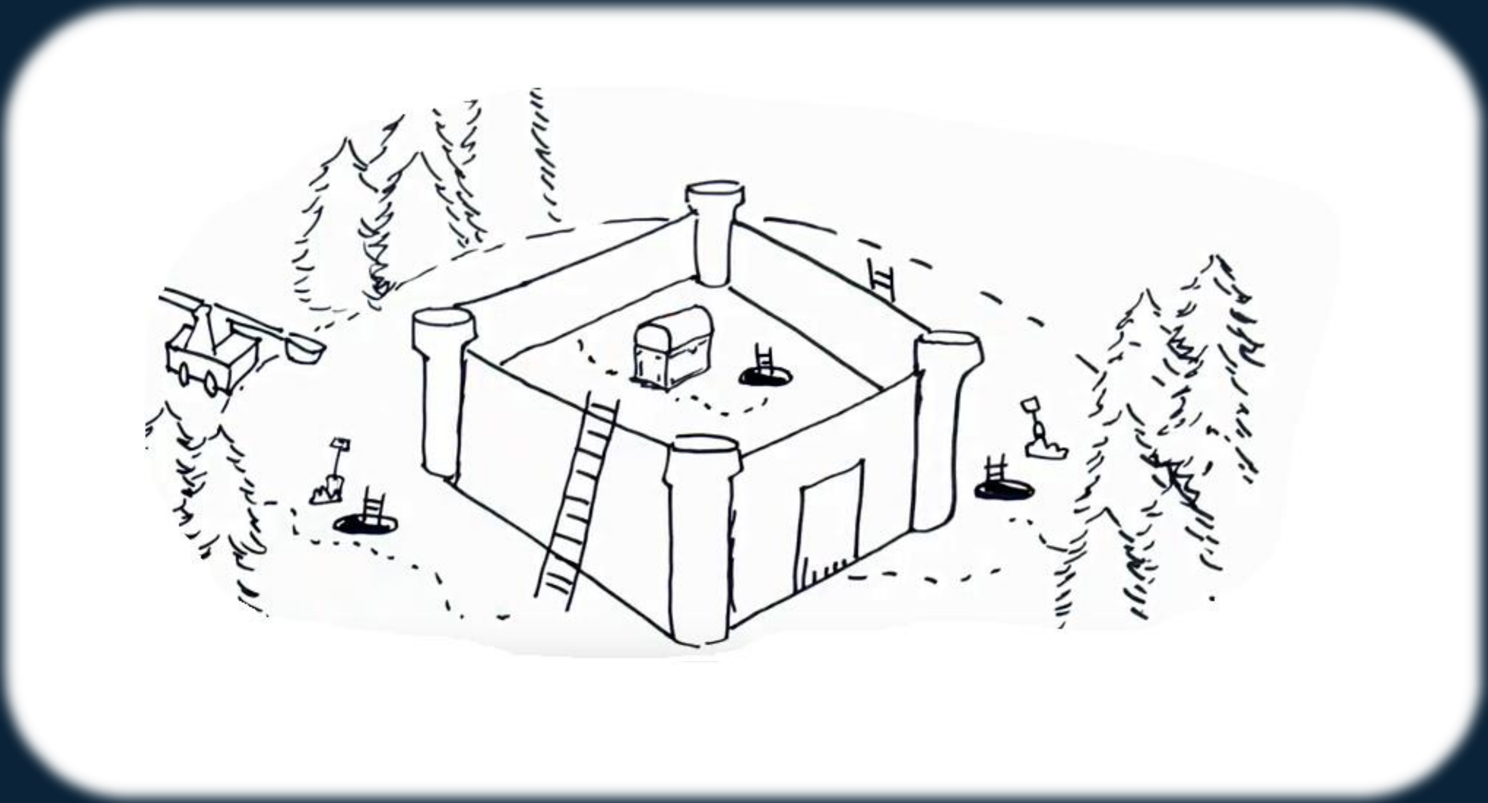
(or: the Challenge in Measuring Security)



As a defender, it’s hard to assess what you miss

The False Negative Problem

(or: the Challenge in Measuring Security)



As a defender, it's hard to assess what you miss

Cue: Offensive Assessments

Stress test your network by executing a real attack

Now you can determine what happens if a real attacker gets on your network

- Did I detect them?
- How far did they get?
- How can I improve my detection and prevention?

The Problem with Offensive Testing

…is that it's *hard*

- Exercises **cost** a lot to run
- They require a significant **time** investment
- Results are dependent on the capabilities of involved **personnel**
- Exercises can be difficult to **repeat** unless extensively documented
- **Design** (e.g., TTPs, in-scope, out-of-scope, etc.) can be challenging

Automation Makes Offensive Testing Easier!

- Lowers the cost to run exercises
- Less time intensive – can run and plan exercises faster
- Dependent now on attacker model, not on personnel
- Can repeat tests at the push of a button
- Designs can be saved, re-used, and designed with easy interfaces

Automated Adversary Emulation with CALDERA

- **Program that acts like a realistic adversary**
  - Leverages ATT&CK as the core threat model
  - Uses AI to make decisions during an exercise
  - Configurable, easy to mix-and-match new adversary capabilities/change behavior
- **Low install overhead – can run on a laptop**
  - No need for complex hardware/custom VMs
  - No need for host softening/whitelisting
  - No need for ingesting complex network maps
- **Modular plugin architecture**
  - Can be integrated with third-party tools
  - Can extend with new abilities/adversaries/etc.

Building on ATT&CK

Publicly Available
attack.mitre.org

Tactics – Adversary’s technical goal

Techniques – How goal is achieved

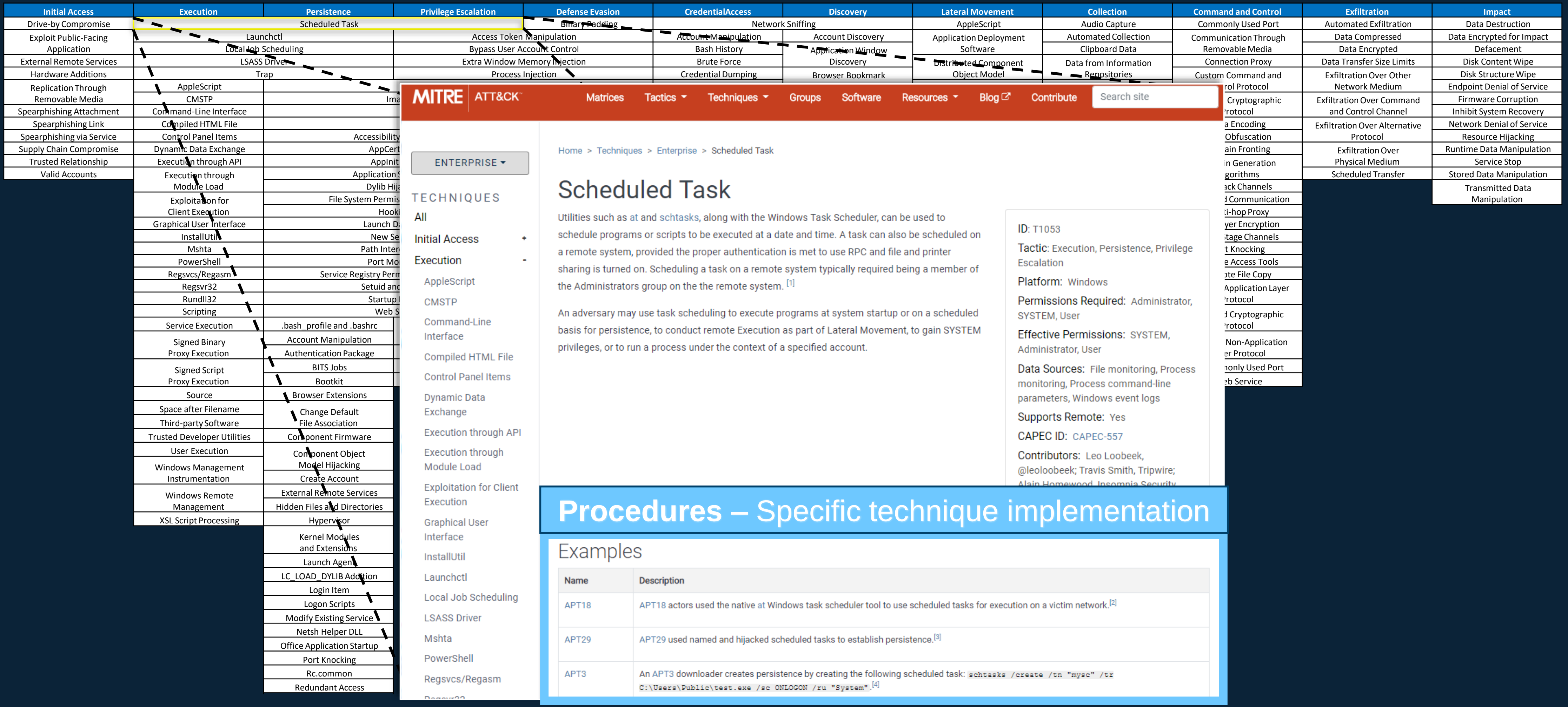
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task	Scheduled Task	Scheduled Task	Binary Padding	Network Sniffing	Network Sniffing	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl	Launchctl	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Local Job Scheduling	Local Job Scheduling	Bypass User Account Control	Bypass User Account Control	Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	LSASS Driver	LSASS Driver	Extra Window Memory Injection	Extra Window Memory Injection	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Trap	Trap	Process Injection	Process Injection	Credential Dumping	Domain Trust Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Attachment	AppleScript	DLL Search Order Hijacking	DLL Search Order Hijacking	DLL Search Order Hijacking	Credentials in Files	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	CMSTP	Image File Execution Options Injection	Image File Execution Options Injection	Image File Execution Options Injection	Credentials in Registry	Network Service Scanning	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Command-Line Interface	Plist Modification	Plist Modification	Plist Modification	Exploitation for Credential Access	Network Share Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Compiled HTML File	Valid Accounts	Valid Accounts	Valid Accounts	Forced Authentication	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Control Panel Items	Accessibility Features	Accessibility Features	BITS Jobs	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	Dynamic Data Exchange	AppCert DLLs	AppCert DLLs	Clear Command History	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multiband Communication		Runtime Data Manipulation
	Execution through API	AppInit DLLs	AppInit DLLs	CMSTP	Input Prompt	Process Discovery	Shared Webroot	Screen Capture	Multi-hop Proxy		Service Stop
	Execution through Module Load	Application Shimming	Application Shimming	Code Signing	Kerberoasting	Query Registry	SSH Hijacking	Video Capture	Multilayer Encryption		Stored Data Manipulation
	Exploitation for Client Execution	Dylib Hijacking	Dylib Hijacking	Compiled HTML File	Keychain	Remote System Discovery	Taint Shared Content		Multi-Stage Channels		Transmitted Data Manipulation
	Graphical User Interface	File System Permissions Weakness	File System Permissions Weakness	Component Firmware	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Third-party Software		Port Knocking		
	InstallUtil	Hooking	Hooking	Component Object Model Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Mshta	Launch Daemon	Launch Daemon	Control Panel Items	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	PowerShell	New Service	New Service	DCShadow	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Regsvcs/Regasm	Path Interception	Path Interception	Deobfuscate/Decode Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Regsvr32	Port Monitors	Port Monitors	Disabling Security Tools		System Service Discovery			Standard Non-Application Layer Protocol		
	Rundll32	Service Registry Permissions Weakness	Service Registry Permissions Weakness	DLL Side-Loading		System Time Discovery			Uncommonly Used Port		
	Scripting	Setuid and Setgid	Setuid and Setgid	Execution Guardrails		Virtualization/Sandbox Evasion			Web Service		
	Service Execution	Startup Items	Startup Items	Exploitation for Defense Evasion							
	Signed Binary Proxy Execution	Web Shell	Web Shell	File Deletion							
	Signed Script Proxy Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	File Permissions Modification							
	Source	Account Manipulation	SID-History Injection	File System Logical Offsets							
	Space after Filename	Authentication Package	Sudo	Gatekeeper Bypass							
	Third-party Software	BITS Jobs	Sudo Caching	Group Policy Modification							
	Trusted Developer Utilities	Bootkit		Hidden Files and Directories							
	User Execution	Browser Extensions		Hidden Users							
	Windows Management Instrumentation	Change Default File Association		Hidden Window							
	Windows Remote Management	Component Firmware		HISTCONTROL							
	XSL Script Processing	Component Object Model Hijacking		Indicator Blocking							
		Create Account		Indicator Removal from Tools							
		External Remote Services		Indicator Removal on Host							
		Hidden Files and Directories		Indirect Command Execution							
		Hypervisor		Install Root Certificate							
		Kernel Modules and Extensions		InstallUtil							
		Launch Agent		Launchctl							
		LC_LOAD_DYLIB Addition		LC_MAIN Hijacking							
		Login Item		Masquerading							
		Logon Scripts		Modify Registry							
		Modify Existing Service		Mshta							
		Netsh Helper DLL		Network Share Connection Removal							
		Office Application Startup		NTFS File Attributes							
		Port Knocking									
		Rc.common									
		Redundant Access									

Building on ATT&CK

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal

Techniques – How goal is achieved



Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- Scheduled Task
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Trap
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence
- Ima
- Accessibility
- AppCert
- AppInit
- Application S
- Dylib Hij
- File System Permis
- Hooki
- Launch D
- New Se
- Path Inter
- Port Mo
- Service Registry Perm
- Setuid and
- Startup
- Web S
- .bash_profile and .bashrc
- Account Manipulation
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- External Remote Services
- Hidden Files and Directories
- Hypervisor
- Kernel Modules and Extensions
- Launch Agent
- LC_LOAD_DYLIB Addition
- Login Item
- Logon Scripts
- Modify Existing Service
- Netsh Helper DLL
- Office Application Startup
- Port Knocking
- Rc.common
- Redundant Access

Privilege Escalation
- Access Token Manipulation
- Bypass User Account Control
- Extra Window Memory Injection
- Process Injection

Defense Evasion
- Binary Padding

CredentialAccess
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Network Sniffing

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark

Lateral Movement
- AppleScript
- Application Deployment Software
- Distributed Component Object Model

Collection
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories

Command and Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and rol Protocol
- Cryptographic rotocol
- a Encoding
- Obfuscation
- ain Fronting
- in Generation gorithms
- ack Channels
- d Communication
- i-hop Proxy
- yer Encryption
- tage Channels
- t Knocking
- e Access Tools
- ote File Copy
- Application Layer rotocol
- d Cryptographic rotocol
- Non-Application er Protocol
- nonly Used Port
- eb Service

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Other Network Medium
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system.[1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: SYSTEM, Administrator, User

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Windows event logs

Supports Remote: Yes

CAPEC ID: CAPEC-557

Contributors: Leo Loobeek, @leoloobeek; Travis Smith, Tripwire; Alain Homewood, Insomnia Security

Procedures – Specific technique implementation

Examples

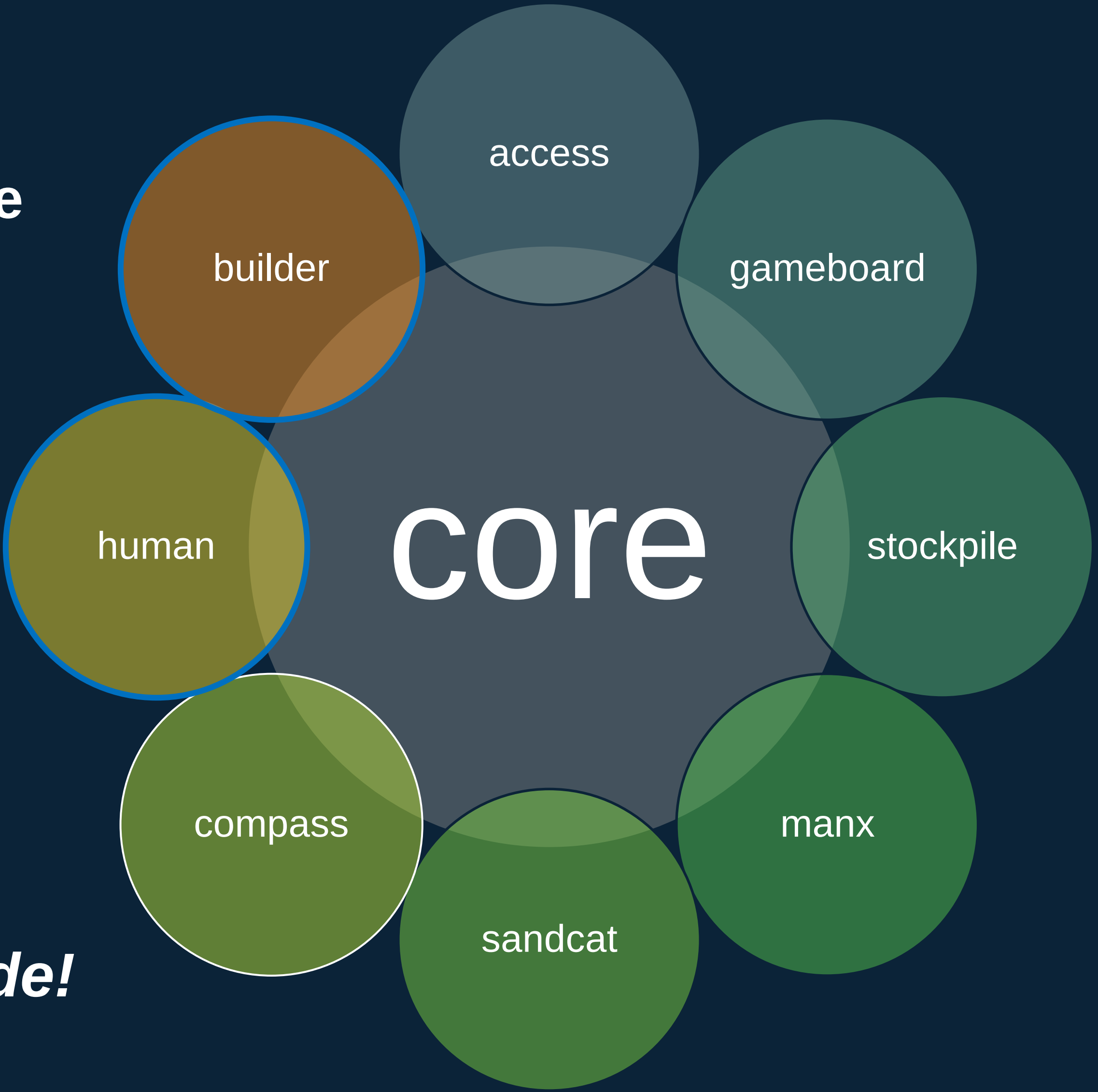
Name	Description
APT18	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.[2]
APT29	APT29 used named and hijacked scheduled tasks to establish persistence.[3]
APT3	An APT3 downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`.[4]

Modular Plugin Architecture

Core system with modular plugin architecture

- ***access***: initial access capabilities
- ***atomic***: pull atomic tests and turn into abilities
- ***gameboard***: simulate red vs blue activity
- ***human***: simulate user/admin behavior
- ***stockpile***: open source adversaries + abilities
- ***sandcat***: CALDERA execution agent
- ***manx***: terminal access to compromised hosts
- ***compass***: host the ATT&CK navigator in CALDERA
- ***builder***: dynamically compile code into abilities
- ***training***: interactive CTF to learn CALDERA

Impact: can rapidly integrate/partition code!



Demo

Use Cases

- Automate the manual portions of red teaming
- Training blue team personnel
- Test defensive detections and analytics
- Test and evaluation scenarios

https://github.com/mitre/caldera