Visualizing ATT&CK data in Maltego

Christophe Vandeplas
https://github.com/cvandeplas
https://github.com/MISP/

MITRE ATT&CK™ Navigator

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impa
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 ite
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Acco
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defa
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification							
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users							
	Trap	Local Job Scheduling	Sudo	Hidden Window							
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL							
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
				Indicator Removal on Host							

no color

legend

ENTERPRISE

TECHNIQUES

All
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
AppleScript
Application Access Token
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking

Pass the Ticket

Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

In this technique, valid Kerberos tickets for Valid Accounts are captured by Credential Dumping. A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access. [1] [2]

Silver Tickets can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint). [1]

Golden Tickets can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory. [3]

ID: T1097
Tactic: Lateral Movement
Platform: Windows
System Requirements: Requires Microsoft Windows as a target system and Kerberos authentication enabled.
Data Sources: Authentication logs
CAPEC ID: CAPEC-645
Contributors: Ryan Becwar; Vincent Le Toux
Version: 1.0

Procedure Examples

Name	Description
APT29	APT29 used Kerberos ticket attacks for lateral movement. [11]
APT32	APT32 successfully gained remote access by using pass the ticket. [13]
BRONZE BUTLER	BRONZE BUTLER has created forged Kerberos Ticket Granting Ticket (TGT) and Ticket Granting Service (TGS) tickets to maintain administrative access. [12]
Empire	Empire can leverage its implementation of Mimikatz to obtain and use Silver and Golden Tickets. [8]
Ke3chang	Ke3chang has used Mimikatz to generate Kerberos golden tickets. [10]
Mimikatz	Mimikatz's `LSADUMP::DCSync`, `KERBEROS::Golden`, and `KERBEROS::PTT` modules implement the three steps required to extract the krbtgt account hash and create/use Kerberos tickets. [4] [5] [6] [7]
SeaDuke	Some SeaDuke samples have a module to use pass the ticket with Kerberos for authentication. [9]

Mitigations

Mitigation	Description
Active Directory	For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos

GROUPS

Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group
CopyKittens
Dark Caracal

Home > Groups > APT28

APT28

APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]

ID: G0007

Associated Groups: SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Contributors: Drew Church, Splunk, Emily Ratliff, IBM, Richard Gold, Digital Shadows

Version: 2.2

Associated Group Descriptions

Name	Description
SNAKEMACKEREL	[15]
Swallowtail	[10]
Group 74	[18]
Sednit	This designation has been used in reporting both to refer to the threat group and its associated malware JHUHUGIT. [6] [5] [36] [2]
Sofacy	This designation has been used in reporting both to refer to the threat group and its associated malware. [4] [5] [3] [26] [2][18]
Pawn Storm	[5] [26]
Fancy Bear	[3] [36] [26] [2][18][10][23]
STRONTIUM	[36] [26] [29]
Tsar Team	[26][18][18]
Threat Group-4127	[5]
TG-4127	[5]

Techniques Used

ATT&CK™ Navigator Layers

− Pivots | − Galaxy | + Event graph | + Correlation graph | + ATT&CK matrix | − Attributes | − Discussion

84464: OSINT ...

Galaxies

Intrusion Set
- + Tropic Trooper - G0081

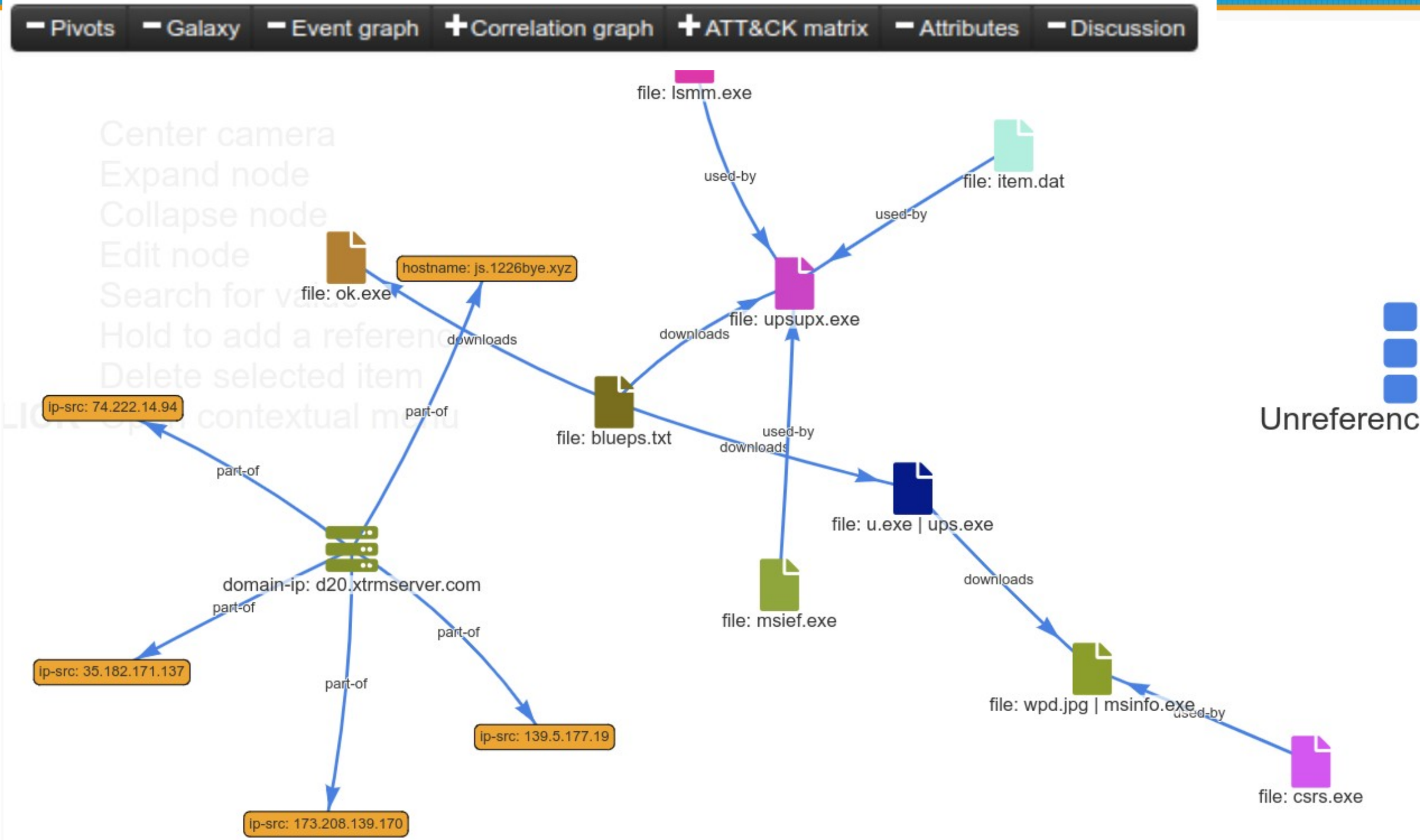
Attack Pattern
- + Valid Accounts - T1078
- + Rundll32 - T1085
- + Web Shell - T1100
- + Registry Run Keys / Startup Folder - T1060
- + Accessibility Features - T1015
- + DLL Side-Loading - T1073
- + Deobfuscate/Decode Files or Information - T1140
- + Application Window Discovery - T1010
- + File and Directory Discovery - T1083
- + Process Discovery - T1057
- + Query Registry - T1012
- + System Information Discovery - T1082
- + System Service Discovery - T1007
- + Standard Cryptographic Protocol - T1032
- + Remote File Copy - T1105
- + Exfiltration Over Command and Control Channel - T1041

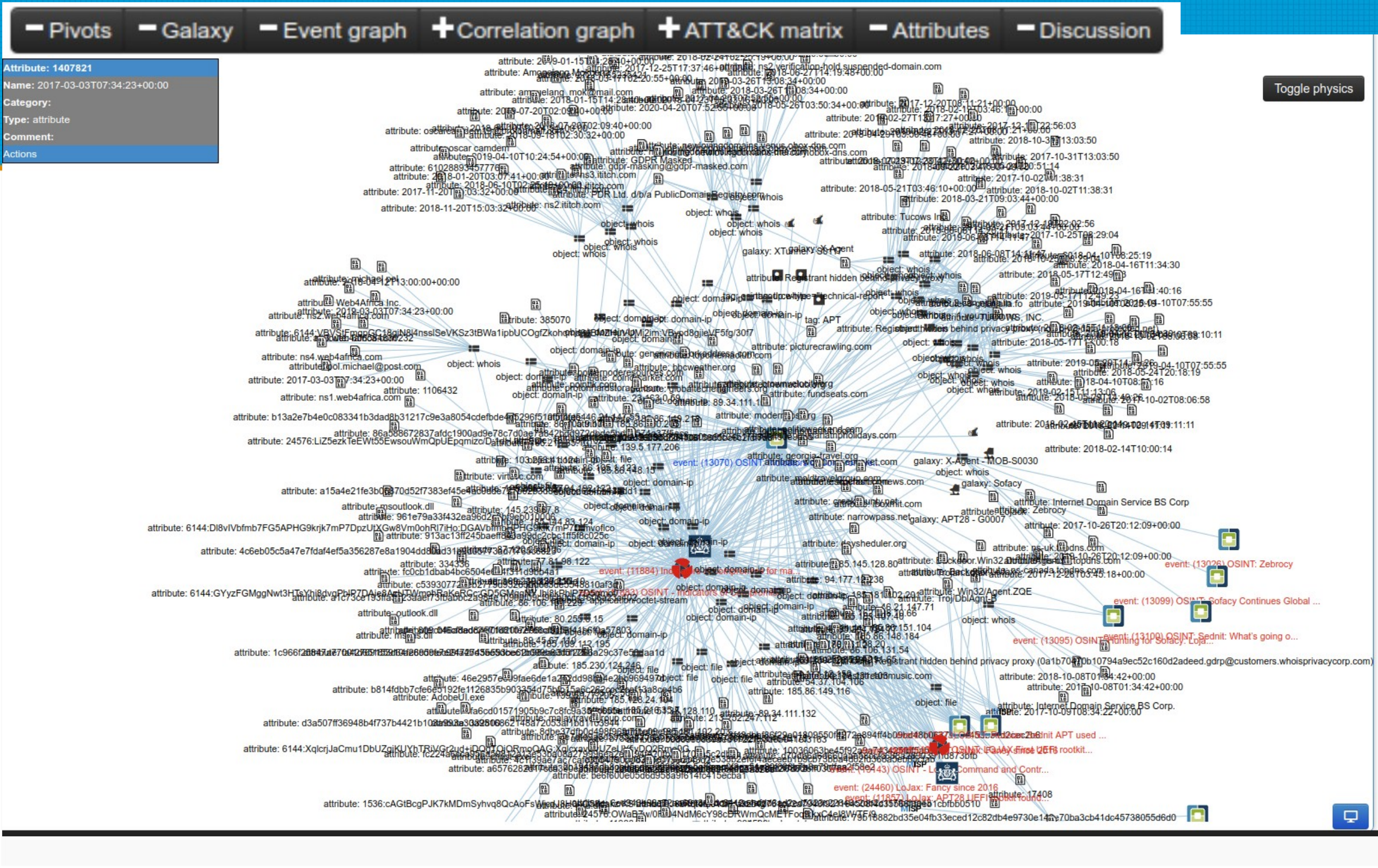
« previous | next » | view all

mitre-mobile-attack | **mitre-attack** | mitre-pre-attack

0 1 Show all

Initial access *(11 items)*	Execution *(33 items)*	Persistence *(59 items)*	Privilege escalation *(28 items)*	Defense evasion *(67 items)*	Credential access *(20 items)*	Discovery *(22 items)*	Lateral movement *(17 items)*	Collection *(13 items)*	Command and control *(22 items)*	Exfiltration *(9 items)*	Impact *(14 items)*
Valid Accounts	Rundll32	Accessibility Features	Accessibility Features	DLL Side-Loading	Account Manipulation	Application Window Discovery	Remote File Copy	Audio Capture	Remote File Copy	Exfiltration Over Command and Control Channel	Data Destruction
Drive-by Compromise	AppleScript	Registry Run Keys / Startup Folder	Valid Accounts	Deobfuscate/Decode Files or Information	Bash History	File and Directory Discovery	AppleScript	Automated Collection	Standard Cryptographic Protocol	Automated Exfiltration	Data Encrypted for Impact
Exploit Public-Facing Application	CMSTP	Valid Accounts	Web Shell	Rundll32	Brute Force	Process Discovery	Application Deployment Software	Clipboard Data	Commonly Used Port	Data Compressed	Defacement
External Remote Services	Command-Line Interface	Web Shell	Access Token Manipulation	Valid Accounts	Credential Dumping	Query Registry	Distributed Component Object Model	Data Staged	Communication Through Removable Media	Data Encrypted	Disk Content Wipe
Hardware Additions	Compiled HTML File	.bash_profile and .bashrc	AppCert DLLs	Access Token Manipulation	Credentials in Files	System Information Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Structure Wipe
Replication Through Removable Media	Control Panel Items	Account Manipulation	AppInit DLLs	BITS Jobs	Credentials in Registry	System Service Discovery	Logon Scripts	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Spearphishing Attachment	Dynamic Data Exchange	AppCert DLLs	Application Shimming	Binary Padding	Exploitation for Credential Access	Account Discovery	Pass the Hash	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing Link	Execution through API	AppInit DLLs	Bypass User Account Control	Bypass User Account Control	Forced Authentication	Browser Bookmark Discovery	Pass the Ticket	Data from Removable Media	Data Encoding	Exfiltration Over Physical Medium	Inhibit System Recovery
Spearphishing via Service	Execution through Module Load	Application Shimming	DLL Search Order Hijacking	CMSTP	Hooking	Domain Trust Discovery	Remote Desktop Protocol	Email Collection	Data Obfuscation	Scheduled Transfer	Network Denial of Service
Supply Chain Compromise	Exploitation for Client Execution	Authentication Package	Dylib Hijacking	Clear Command History	Input Capture	Network Service Scanning	Remote Services	Input Capture	Domain Fronting		Resource Hijacking
Trusted Relationship	Graphical User Interface	BITS Jobs	Exploitation for Privilege Escalation	Code Signing	Input Prompt	Network Share Discovery	Replication Through Removable Media	Man in the Browser	Domain Generation Algorithms		Runtime Data Manipulation
	InstallUtil	Bootkit	Extra Window Memory Injection	Compile After Delivery	Kerberoasting	Network Sniffing	SSH Hijacking	Screen Capture	Fallback Channels		Service Stop
	LSASS Driver	Browser Extensions	File System Permissions Weakness	Compiled HTML File	Keychain	Password Policy Discovery	Shared Webroot	Video Capture	Multi-Stage Channels		Stored Data Manipulation
	Launchctl	Change Default File	Hooking	Component Firmware	LLMNR/NBT-NS Poisoning	Peripheral Device	Taint Shared Content		Multi-hop Proxy		Transmitted Data


Pivots
Galaxy
Event graph
Correlation graph
ATT&CK matrix
Attributes
Discussion
file: lsmm.exe
used-by
file: item.dat
used-by
file: ok.exe
hostname: js.1226bye.xyz
downloads
file: upsupx.exe
downloads
file: blueps.txt
part-of
used-by
downloads
ip-src: 74.222.14.94
part-of
file: u.exe | ups.exe
domain-ip: d20.xtrmserver.com
part-of
part-of
part-of
file: msief.exe
downloads
ip-src: 35.182.171.137
ip-src: 139.5.177.19
file: wpd.jpg | msinfo.exe
used-by
ip-src: 173.208.139.170
file: csrs.exe
Unreferenc


Pivots
Galaxy
Event graph
Correlation graph
ATT&CK matrix
Attributes
Discussion
Attribute: 1407821
Name: 2017-03-03T07:34:23+00:00
Category:
Type: attribute
Comment:
Actions
Toggle physics

Glue with $favorite_tool

- ATT&CK rocks
- MISP rocks

although they do
not cover
EVERYTHING

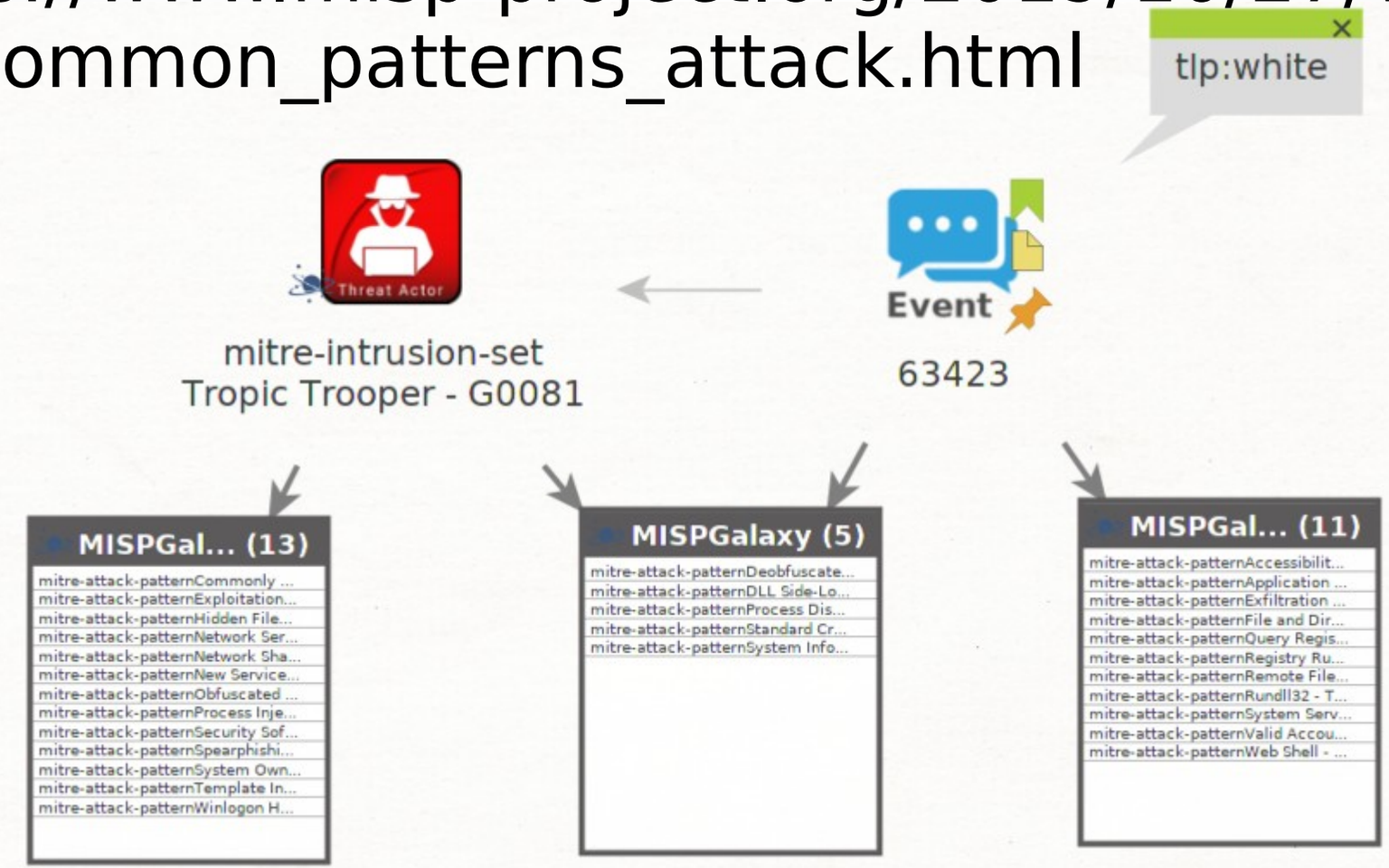
- Glue with favorite toolset
  - MISP Galaxies
  - PyMISP & REST API
  - Visualization tool => Maltego (commercial)

Use-Cases

- Is my IOC in MISP?
- Exploring data from MISP
- Visualize relationships
  - Object / Attribute Relations
  - Event Relations
  - Tags, Galaxies, ATT&CK and more
- Start from Galaxies / Malware / Tools / ...

ATT&CK

- Demo, see here: https://www.misp-project.org/2019/10/27/visualising_common_patterns_attack.html
-



Where ?

- https://github.com/MISP/MISP-maltego
- https://github.com/MISP/misp-galaxy
- Code & documentation
- Installation:
  - pip3 install MISP-maltego
  - canari create-profile MISP_maltego
  - Maltego > home button > Import > Import Configuration & select the MISP_maltego.mtz file
  - $HOME/.canari/MISP_maltego.conf
    set your misp_url and misp_key
- Feedback & Ideas very welcome!