EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

# SPRÁVA A DOHLED NAD POČÍTAČOVOU SÍTÍ

## MITRE ATT&CK

## Metodický list

Autor: doc. Ing. Jaroslav Dočkal, CSc., Metodik: Bc. Jaroslav Tihlařík

Recenzent: Ing. Vladimír Šulc, Ph.D.

Rok vydání: 2023



# Obsah

# Cíle

Úkolem je

- Seznámit se se základní techniky, modely a nástroje společnosti MITRE
- Naučit vyhledávání v Matrix tabulce a pomocí Navigátora

# Dovednosti

Úkolem je získat dovednosti ve

- Vyhledávání softwaru pro realizaci modelu MITRE ATT&CK
- Emulace kyberútočníka v rámci Navigátora
- Vyhodnocování ticketů z hlediska klasifikace MITRE

# Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Cylab JCEKB
- Offline Security Classroom

# Průběh výuky

# 1 Základy provozu MITRE ATT&CK

## 1.1 MITRE Center for Threat Informed Defense (CTID)

Když MITRE poprvé zahájili svůj projekt ATT&CK, netušili, jak populární se stane v bezpečnostní komunitě. Projekt se stal pro odborníky v oblasti informační bezpečnosti natolik důležitým, že si prosadili nekomerční neziskové kontaktní místo, které by udrželo a urychlilo vývoj veřejně dostupných zdrojů důležitých pro kybernetickou obranu.

CTID se zapojuje do společných výzkumných a vývojových projektů s cílem posouvat současný stav a praxi obrany informované o hrozbách. Členové CTID se rekrutují z globálních společností zabývajících se kritickou infrastrukturou, sofistikovaných a inovativních cenných papírů, předních technologických společností a neziskových organizací zabývajících se kybernetickou bezpečností. Všechny výstupy výzkumu a vývoje jsou globálně dostupné, aby se maximalizoval jejich dopad.

CTID zkoumá chování kybernetických útočníků a vytváří seznamy jejich „nejžádanějších" technik. Provádí průběžné hodnocení obranyschopnosti výpočetních systémů a vyvíjí, sdílí a automatizuje playbooky emulující činnost útočníka.

Nejznámějším přínosem MITRE je rámec (model protivníka) ATT&CK (Adversarial Tactics, Techniques a Common Knowledge), kde

- Taktika jsou technické cíle protivníka.
- Techniky jsou způsoby, jak dosáhnout těchto cílů.
- Postupy jsou konkrétní implementace technik.

Samotný rámec MITRE ATT&CK je soubor technik používaných útočníky během narušení. ATT&CK Matrix rozděluje techniky do následujících taktik aktuální verze 11:

- *Initial Access* (počáteční přístup) – Techniky, které využívají různé vstupní vektory k získání opory pro útok. Opory získané počátečním přístupem mohou umožnit nepřetržitý přístup, jako jsou platné účty a používání externích vzdálených služeb, nebo mohou být omezené kvůli změně hesla.
- *Execution* (provedení) – Techniky, jejichž výsledkem je spuštění kódu řízeného protivníkem na místním nebo vzdáleném systému. Techniky, které spouštějí škodlivý kód, jsou často spárovány s technikami ze všech ostatních taktik k dosažení širších cílů.
- *Perzistence* (vytrvalost) – Techniky, které protivníci používají k udržení přístupu k systémům během restartů, změněných přihlašovacích údajů a dalších přerušení, která by jim mohla znemožnit přístup.
- *Privilege Escalation* (eskalace privilegií) – Techniky, které protivníci používají k získání oprávnění vyšší úrovně v systému nebo síti. Techniky se často překrývají s technikami persistence.
- *Defense Evasion* (obranný únik) – Techniky, které protivníci používají, aby se vyhnuli odhalení během jejich kompromitace.

- *Credential Access* (přístup k oprávnění) – Techniky pro krádež přihlašovacích údajů, jako jsou názvy účtů a hesla.
- *Discovery* (nálezy) – Techniky, které protivník používá k získání znalostí o systému a vnitřní síti. K tomuto cíli shromažďování informací po kompromitaci se často používají nástroje nativního operačního systému.
- *Lateral Movement* (úhyb stranou) – Techniky, které protivníci používají ke vstupu a ovládání vzdálených systémů v síti.
- *Collection* (shromažďování) – techniky, které protivníci používají ke shromažďování informací a ze zdrojů se shromažďují informace, které jsou relevantní pro sledování cílů protivníka.
- *Command and Control* (velení a řízení) – Techniky, které protivníci používají ke komunikaci se systémy pod jejich kontrolou v rámci sítě oběti.
- *Exfiltration (exfiltrace)* – Techniky, které protivníci používají ke krádeži dat ze sítě.
- *Impact (dopad)* – Techniky, které protivníci používají k narušení dostupnosti nebo narušení integrity manipulací s obchodními a provozními procesy.

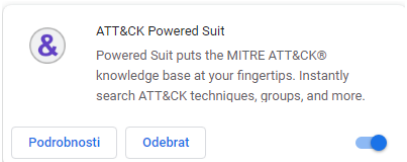
Název CTID vychází z koncepce zvané *Threat Informed Defense*. Ta je tvořena třemi fázemi:

- Cyber Threat Intelligence Analysis (analýza zpravodajských informací)
- Defensive Engagement of the Threat (defenzivní zapojení hrozby)
- Focused Sharing & Collaboration (Zaměřené sdílení a spolupráce)

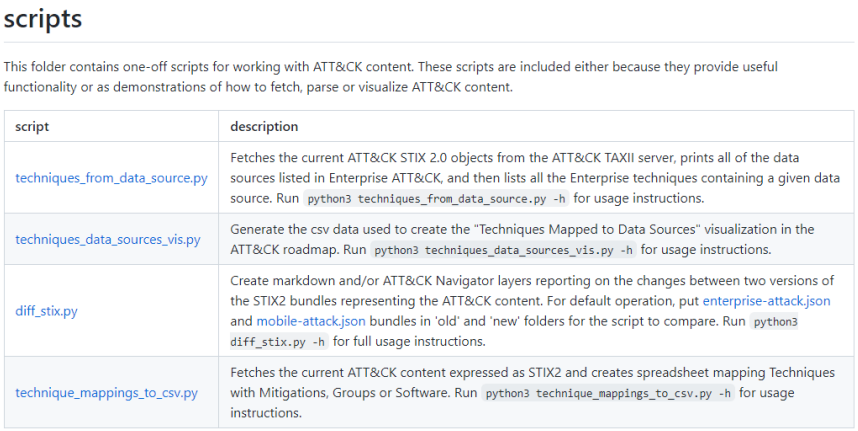
Fáze *Threat Intelligence Analysis* využívá existující zpravodajská data, jako jsou TTP, malware, hashe nebo názvy domén a využívá lidskou inteligenci k posílení kybernetické obrany. To zlepšuje způsoby, jak předcházet kybernetickým útokům, předcházet jim, odhalovat je a reagovat na ně.

*Defensive Engagement of the Threat* (Zapojení informací o hrozbách do obrany) umožňuje hledat indikátory čekajícího, aktivního nebo úspěšného kybernetického útoku. Ve světě Zero-day útoků narůstá význam tzv. **Breach and Attack Simulation** (BAS). BAS se používá k automatizaci testování a podávání zpráv o tom, jak tyto vzorce chování v praxi vypadají. Tyto simulace poskytují zpětnou vazbu do analýzy hrozeb a do dalšího prvku, jímž je Focused Sharing and Collaboration (cílené sdílení a spolupráce).

Na https://github.com/center-for-threat-informed-defense/attack-powered-suit je k dispozici rozšíření pro prohlížeč:



Focused Sharing and Collaboration využívá nástroje jako jsou STIX[1] a TAXII[2] pro sdílení dat v rámci bezpečnotní komunity. Pro sběr dat byly v rámci projektu zpracovány pomocné skripty sloužící pro načtení dat, jejich analýzu a vizualizaci jejich obsahu – viz obr. 1.1.1.



scripts

This folder contains one-off scripts for working with ATT&CK content. These scripts are included either because they provide useful functionality or as demonstrations of how to fetch, parse or visualize ATT&CK content.

| script | description |
|---|---|
| techniques_from_data_source.py | Fetches the current ATT&CK STIX 2.0 objects from the ATT&CK TAXII server, prints all of the data sources listed in Enterprise ATT&CK, and then lists all the Enterprise techniques containing a given data source. Run `python3 techniques_from_data_source.py -h` for usage instructions. |
| techniques_data_sources_vis.py | Generate the csv data used to create the "Techniques Mapped to Data Sources" visualization in the ATT&CK roadmap. Run `python3 techniques_data_sources_vis.py -h` for usage instructions. |
| diff_stix.py | Create markdown and/or ATT&CK Navigator layers reporting on the changes between two versions of the STIX2 bundles representing the ATT&CK content. For default operation, put enterprise-attack.json and mobile-attack.json bundles in 'old' and 'new' folders for the script to compare. Run `python3 diff_stix.py -h` for full usage instructions. |
| technique_mappings_to_csv.py | Fetches the current ATT&CK content expressed as STIX2 and creates spreadsheet mapping Techniques with Mitigations, Groups or Software. Run `python3 technique_mappings_to_csv.py -h` for usage instructions. |

Obr. 1.1.1: Skripty určené pro sběr dat z https://github.com/mitre-attack/attack-scripts/tree/master/scripts

## 1.2 Cyber Analytics Repository (CAR)

Na sběr dat navazuje analýza dat. K ní slouží znalostní báze analýzy vyvinutá na základě modelu MITRE ATT&CK s názvem Cyber Analytics Repository (CAR – http://car.mitre.org). CAR definuje datový model, který využívá ve svých reprezentacích pseudokódu, ale také zahrnuje implementace přímo zacílené na konkrétní nástroje (např. Splunk) ve svých analýzách. S ohledem na pokrytí se CAR zaměřuje na poskytování souboru ověřených a dobře vysvětlených analýz, zejména s ohledem na jejich provozní teorii a zdůvodnění.

Analýzy uložené v CAR obsahují následující informace pro každou analýzu:

- hypotézu, která vysvětluje ideu stojící za analýzou
- informace nebo primární doména, ve které má analytik pracovat (může to být hostitel, síť, proces, externí atd.)
- odkazy do ATT&CK technik a taktik, které analýza detekuje
- slovník
- popis možné implementace výsledku analýzy zapsaný v pseudokódu
- test pro předvedení výsledků analýzy

Kompletní seznam je na stránce https://car.mitre.org/analytics/.

[1] STIX (Structured Threat Information eXpression) je standardizovaný jazyk, který byl vyvinut společností MITER ve spolupráci s cílem reprezentovat strukturované informace o kybernetických hrozbách.

[2] TAXII (Trusted Automated eXchange of Indicator Information) je soubor služeb a výměn zpráv, které umožňují sdílení informací o kybernetických hrozbách napříč hranicemi produktů, služeb a organizací. Jedná se o přepravní prostředek pro strukturované informace o hrozbách STIX a klíčový prostředek pro širokou výměnu informací.

## 1.3 Collaborative Research Into Threats (CRITS)

CRITS je nástroj vyvinutý společností MITRE (https://github.com/crits/crits#readme). Je zdarma a open source. CRITS pomáhá s analýzou zpravodajských informací, jako např.:

- shromažďování a archivace artefaktů útoku
- spojování artefaktů s fázemi životního cyklu kybernetického útoku
- provádění zpětného inženýrství malwaru
- sledování vlivů prostředí
- propojení toho všeho dohromady za účelem utváření a upřednostňování obrany a reakce na incidenty

Wiki CRITS je na https://github.com/crits/crits/wiki.

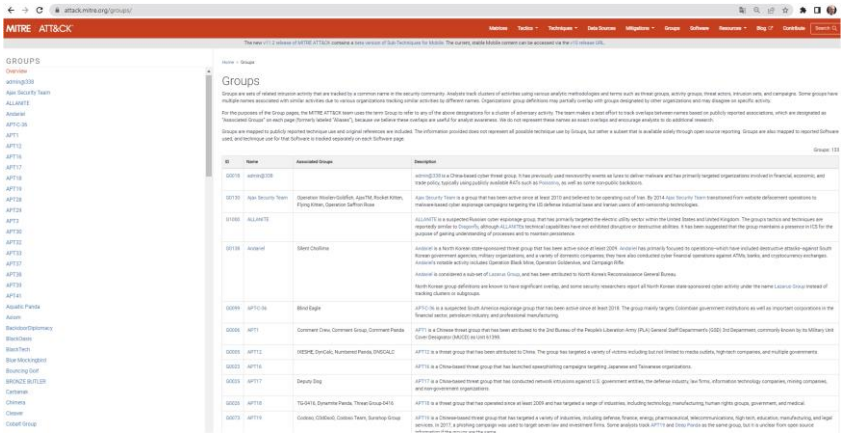
## 1.4 Emulace protivníka

MITRE definuje emulaci protivníka jako „typ zapojení red týmu, který napodobuje známou hrozbu pro organizaci tím, že se snaží určit, jaké akce a chování red tým používá“. Jinými slovy, červený tým zaujímá strukturovaný přístup pomocí zpravodajství o hrozbách k plánování útoku, který je podobný chování známého aktéra hrozby. Pokud organizace nemá červený tým, může využít BAS.

MITRE podporuje projekt CALDERA (https://github.com/mitre/caldera), což je open source BAS. K emulaci protivníka slouží i další open source řešení, např. knihovna testů Atomic Red Team (https://github.com/redcanaryco/atomic-red-team). Z komerčních řešení lze uvést AttackIQ. Nejlepší způsob testování přístupu threat informed defense je ve spolupráci red a blue týmů v rámci purple týmů.

## 1.5 Operacionalizace ATT&CK

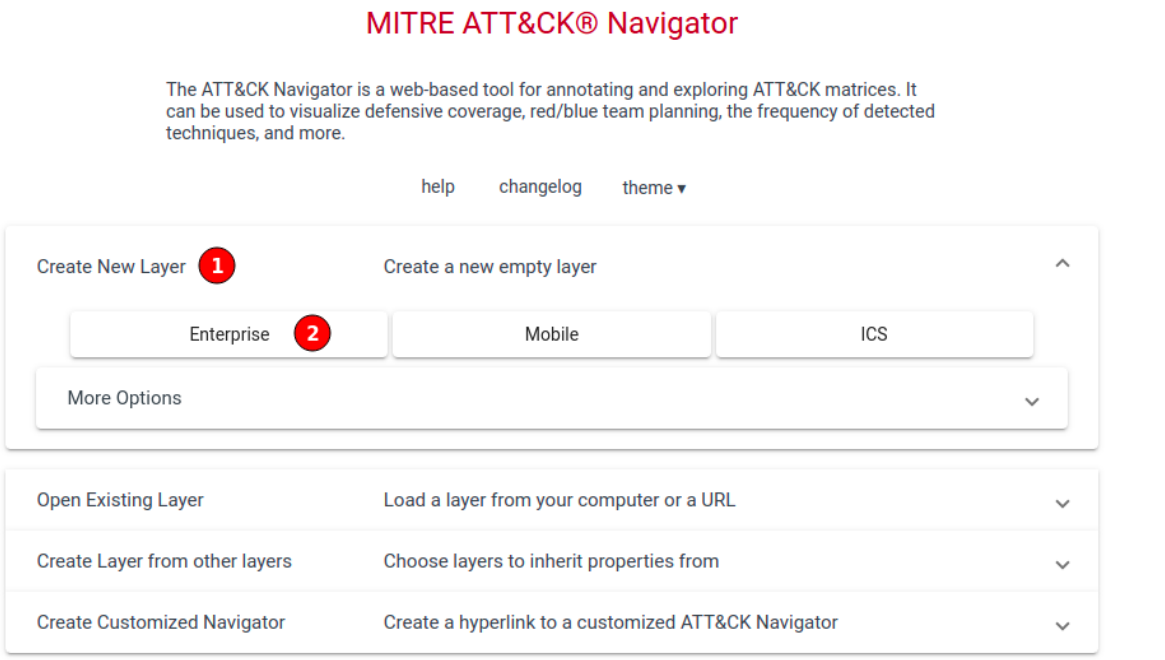
Jedním z nejjednodušších způsobů, jak zprovoznit rámec ATT&CK, je vybrat si skupinu hrozeb, která vás zajímá, a zmapovat jejich techniky v Enterprise ATT&CK Matrix. Stránka skupin hrozeb na webu MITRE ATT&CK (viz obr. 1.5.1) poskytuje seznam všech pokročilých skupin hrozeb, které MITER sledoval. Pro každou skupinu hrozeb proklikejte a získejte další podrobnosti. Některé z podrobností uvedených u každého aktéra hrozby zahrnují použitou taktiku a software a odkazy na další výzkum.




Obr. 1.5.1: Stránka skupin hrozeb na webu MITER ATT&CK (https://attack.mitre.org/groups/)

## 1.6 ATT&CK Navigator

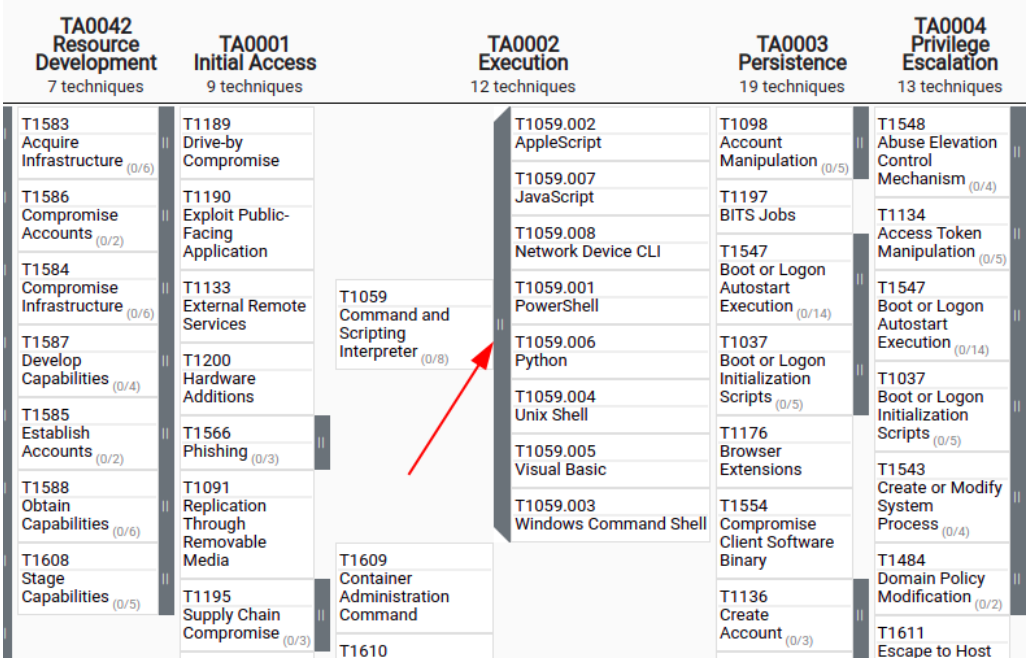
Vedle klasického Matrixu vyvinula firma MITRE online nástroj nabízející různé způsoby použití Matrixu, nazvaný „Navigátor“. Lze jej využít k nasazení obvyklých případů použití Matrixu. Online je k dispozici úvodní video (*https://www.youtube.com/watch?v=pcclNdwG8Vs*), které demonstruje funkce Navigátoru. Samotný Navigátor je k dispozici na *https://mitre-attack.github.io/attack-navigator/*. Chcete-li použít Navigátor, vytvořte nejprve novou vrstvu a vyberte sféru Enterprise.




Obr. 1.6.1 Počáteční nastavení Navigátora

Všechny techniky jsou zobrazeny v jednotlivých buňkách seskupených do sloupců odpovídajících taktice. Buňky obsahují kódy technik typu Txxxx. Tato ID se často zmiňují, případně spolu s názvy, aby jednoznačně odkazovaly na konkrétní techniky.

Tam, kde je to vhodné, byly některé techniky rozděleny do skupin dílčích technik, které jsou v Navigátoru označeny šedou zónou. Kliknutím na tuto šedou zónu se skupina rozbalí (sbalí) a zobrazí se (skryjí) jednotlivé dílčí techniky – viz obr. 1.6.2. To výrazně zlepšuje čitelnost Matrixu.

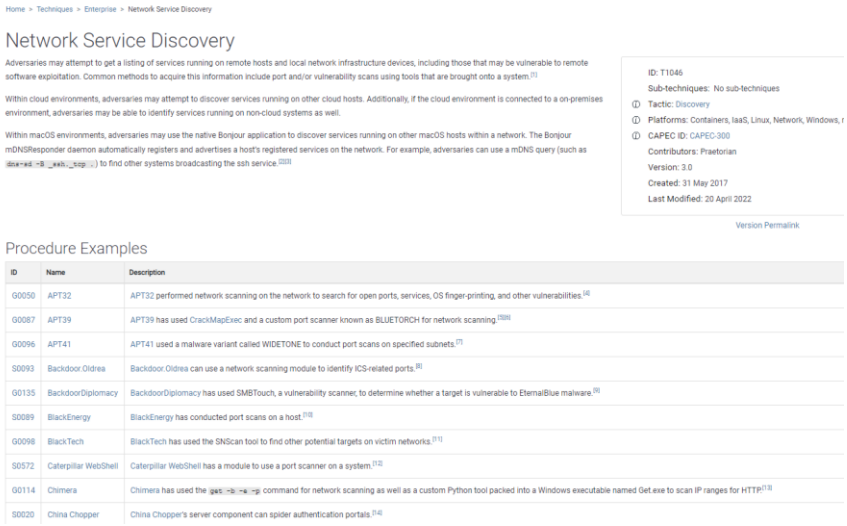



Obr. 1.6.2 Nabídka techniky s možností View Technique

Kliknutím pravým tlačítkem na techniku se otevře nabídka s možností View Technique: výběrem této možnosti se otevře stránka Technique in question příslušné techniky s úplným popisem a vybranými informacemi, které lze shromáždit prostřednictvím forenzní analýzy útoků v reálném světě.

## 1.7 Atomic Red Team

I když však stránka MITRE obvykle poskytuje velmi užitečné a spolehlivé informace, nepopisuje, jak nasadit danou techniku. Vezměme si například techniku „T1046 Network Service Discovery“ – viz obr. 1.7.1. Stránka této techniky nabízí několik málo podrobností o nejlepším způsobu provedení skutečného zjišťování síťových služeb.




Obr. 1.7.1 Technika T1046 Network Service Discovery.

Zde nachází uplatnění **Atomic Red Team** (ART) – *https://github.com/redcanaryco/atomic-red-team*. Atomic Red Team je sbírka úryvků kódu, které umožňují skutečně spustit Techniku, kolekci mapovanou na Mitre Att&ck Framework. Úložiště je spravováno týmem Red Canary a je organizováno s myšlenkou usnadnit testování citlivosti IT systémů na různé techniky útoku.

Atomiky (atomics) jsou seřazeny podle ID techniky a připraveny k nasazení. Každá atomika se skládá ze série testů, které jsou podrobně popsány v souboru yaml pro zpracování a souboru markdwon pro čitelnost. Pro každý test soubor popisuje podporovaný operační systém a příkazy pro příslušný spouštěcí program.

Například v případě výše uvedeného T1046 atomic navrhuje 8 testů (obr. 1.7.2): prvním testem (obr. 1.7.3) je skenování portu, které lze provést na Linuxu nebo MacOS, navrhovaný příkaz by měl být proveden pomocí shellu.


Obr. 1.7.2 Testy pro atomiku T1046 Network Service Discovery.


Obr. 1.7.3 Test pro skenování portu

Ne všechny techniky mají přidružený atomický test, ART navrhuje poměrně hodně testů pro obvyklé použití, např. pro „T1059.001 – PowerShell“ je jich 21.

Úložiště ART lze jednoduše naklonovat a příkazy spouštět ručně. ART však jde dále a poskytuje nástroj nazvaný Invoke-Atomic, který po instalaci automatizuje provádění atomů. Je založen na PowerShellu a lze jej nasadit na Linux nebo MacOS po instalaci PowerShell Core. Po instalaci je k dispozici modul 'Invoke-AtomicTest'.

V úložišti github jsou navrženy různé způsoby použití Invoke-Atomic. Nejběžnější příkazy jsou:

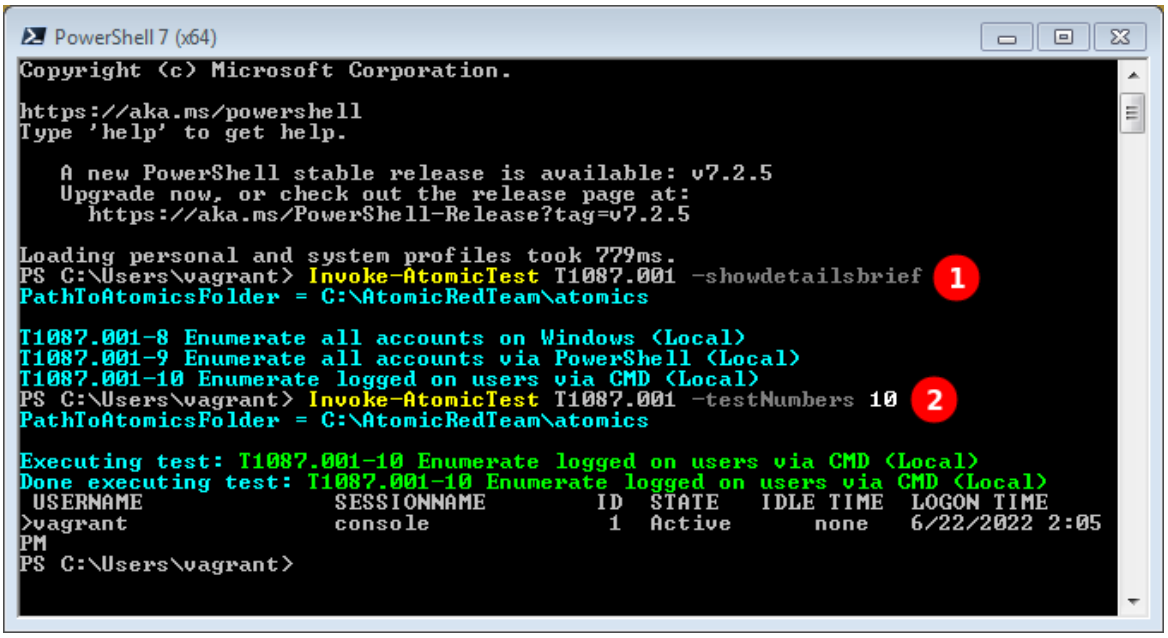
Seznam všech dostupných testů: Invoke-AtomicTest All -ShowDetailsBrief

Seznam atomických testů: Invoke-AtomicTest <atomic code> -ShowDetailsBrief

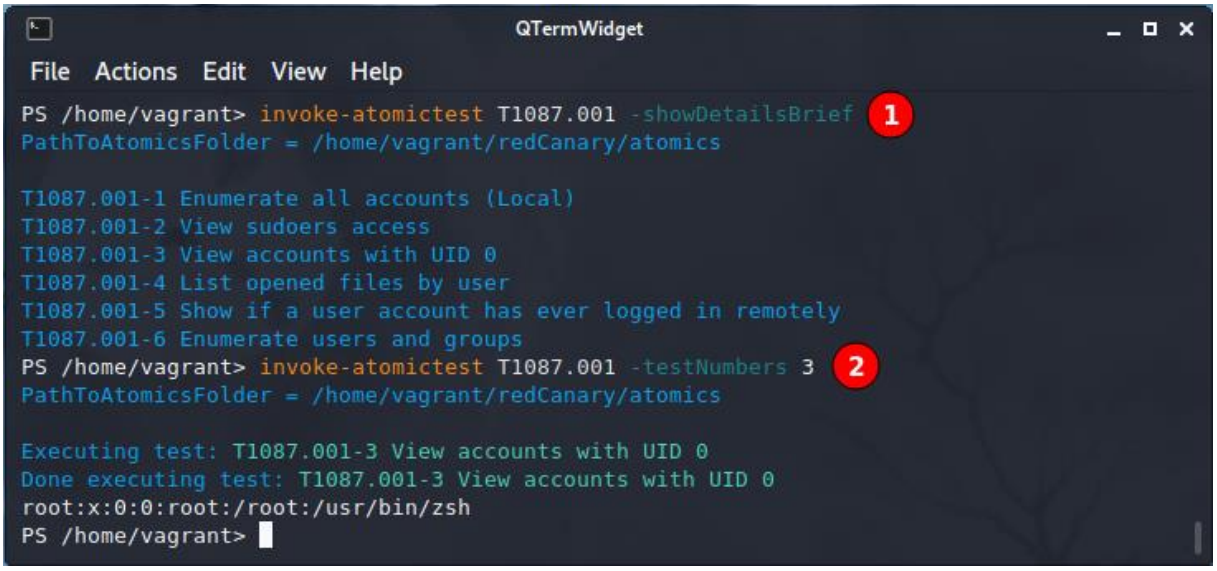
Požadavek na vykování atomového testu: Invoke-AtomicTest <atomic code>

Požadavek na vykování specifických testů: Invoke-AtomicTest <atomic code> -TestNumbers n1,n2

Budou navrženy pouze testy relevantní pro běžící OS. Například atomový T1087.001 odhaluje různé testy na Windows (obr. 1.7.4) a Linux (1.7.5).




Obr. 1.7.4 Invoke-test pro Windows 7




Obr. 1.7.5 Invoke-test pro Linux 2021.3

Tyto dva příklady ukazují, jak se stejný atom nebo stejná technika automaticky spouští odlišně v operačních systémech založených na Windows nebo Linux.

Kombinace MITRE Att&ck Navigátora a ART umožňuje prozkoumat Framework z útočných a obranných pozic více způsoby. Navigátor odráží Att&ck Matrix a usnadňuje prozkoumávání různých kroků Kill Chain. Díky Techniques ID je propojení s ART atomics okamžité a samotné nasazení některých útočných technik na IT systému je jednodušší.

Modul Invoke-AtomicRedTeam obsahuje několik funkcí New-Atomic*, které usnadňují používání nativního prostředí PowerShellu k vytváření a ověřování atomických technik a testů. Tyto funkce byly napsány, aby řešily následující:

- Dříve bylo nutné atomové testy psát ručně, což je v mnoha případech naprosto přijatelné, ale může být náchylné k chybám.
- Dříve při psaní atomových testů neexistoval žádný způsob, jak ověřit YAML proti schématu, kromě spuštění validate-atomics.rb v úložišti atomic-red-team.
- Dříve neexistoval způsob, jak vytvářet techniky/testy automatizovaným způsobem pomocí kódu. Např. pokud je třeba napsat scénář, dle kterého je třeba za běhu generovat stovky testů, psaní tolika testů rukou prostě není možné.

Funkce New-Atomic* vydávají dobře naformátovaný objekt PowerShell, který je navržen tak, aby byl převeden přímo do ConvertTo-Yaml (https://github.com/cloudbase/powershell-yaml), a tím dostat techniku/testy do formátu YAML. Už nikdy nebudete muset psát YAML pro atomy, pokud nechcete.

Repozitář ART nepokrývá všechny techniky Mitre Att&ck Matrix, stále se však jedná o užitečnou sbírku testů, které lze provést za relativně nízkých nákladů. A lze na něj pohlížet i jako na úložiště příkazů pro provádění konkrétních technik v kontextu angažmá Red Teaming.

## 1.8 Attack Flow Designer GUI tool

Nejprve zde bude uvedeno, proč je dnes tak důležité (a zároveň obtížné) trasovat a vizualizovat průběh útoku a v čem se souběžně s novými útoky mění i způsoby jejich detekce.

Ti, kteří sledují vývoj hackingu, stále častěji narážejí na termín „living off the land“ (LOL)[3]. Jak název napovídá, LOL využívají to, co mají kolem sebe (legitimní systémové nástroje a nástroje) pro škodlivé účely. To jim umožňuje splynout s běžnou síťovou aktivitou a zůstat skryté. Některé schopnosti LOL jsou: DLL hijacking, skrytí datových částí, proces dumping, stahování souborů, obcházení UAC keyloggingu, kompilace kódu, úniky do protokolu, provádění kódu a persistence. Existuje několik různých typů technik LOL, včetně LOLBinů, které používají binární soubory Windows ke skrytí škodlivé aktivity; LOLLibs, které používají knihovny; a LOLScripts, které používají skripty.

Dnes se techniky LOL často realizují v podobě bezsouborového malwaru[4], což je typ malwaru, který existuje pouze jako artefakt založený na paměti, přičemž na pevný disk se nezapisuje žádná – nebo alespoň velmi malá – aktivita. Skutečnost, že útoky bez souborů neinstalují škodlivý software, velmi ztěžuje detekci typických AV nástrojů. Dnes útoky bez souborů často (ale ne vždy) zahrnují techniky LOL, protože fungují bez zápisu souborů na disk nebo do souborového systému, což jim pomáhá zůstat déle neodhalené.

Až donedávna byly techniky LOL používány v kontextu činností po kompromitaci, kdy útočníci využívali legitimní nástroje pro správu, jako je Powershell, Windows Management Instrumentation (WMI), CMD, Psxec.exe a další, k provádění průzkumu a bočního pohybu. Dnes jsou součástí i počáteční kompromitační zátěže.

LOLBiny vyžadují vícevrstvou obranu proti spouštěnému malwaru případně použití několika senzorů během jeho životního cyklu. To klade vyšší nároky na trasování průběhu útoku a vyžaduje vhodné nástroje.

Pokud jde o emulaci protivníka a hrozby používá se pro testování několik metod. První metodou je **atomové testování**. Toto je způsob, jak napodobit jeden nebo více scénářů založených na IOC nebo TTP, které jednají nezávisle na sobě. Například pomocí zvolené platformy lze vytvořit hodnocení založené na atomech, vybrat jednu nebo více technik k testování, vybrat více prostředků a pak spustit běh hodnocení. Každý TTP bude spuštěn postupně, jeden po druhém, každý v rámci svého vlastního kontextu procesu. V závislosti na tom, co TTP emuluje, to může vést k testování vestavěných ovládacích prvků zabezpečení operačního systému, jako je User Account Control (UAC – řízení uživatelských účtů), řízení sítě, DLP (Data Loss Prevention), application whitelisting (seznam povolených aplikací) atd.

Další metoda je známá pod názvem **anatomické testování**, u MITRE je označují jako **Attack Flows.** Základní komponenty projektu zobrazuje obr 1.7.1.Tento typ hodnocení umožňuje, aby byly TTP efektivně zřetězeny a prováděny v rámci jednoho kontextu procesu. To znamená, že na rozdíl od atomového testování, kde probíhají nezávisle, jsou anatomické TTP vzájemně propojeny. To je způsobeno povahou IF-ELSE anatomického testování, které umožňuje vlastní větvení a sekvencování pomocí vícefázových vzorců útoků. Anatomické testování umožňuje sestavit vlastní řetězec

[3] Termín „Living off the lend“ (LOL) byl vytvořen výzkumníky malwaru Christopherem Campbellem a Mattem Greaberem, aby vysvětlili použití důvěryhodných, předinstalovaných systémových nástrojů k šíření malwaru.
[4] Frodo, Code Red, červ SQL Slammer, trojan Lurk, POWRUNER, POSHSPY, Astaroth atd.

,

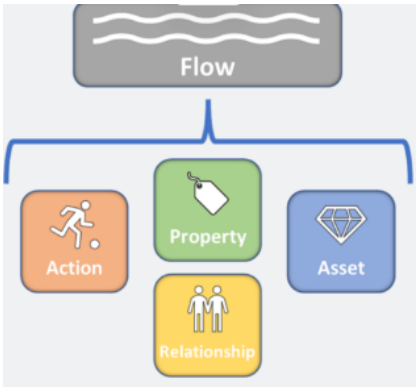
útoků a přizpůsobit jej tak, aby reprezentoval jakoukoli posloupnost hrozeb. Anatomické testování se používá pro testování bezpečnostních kontrol, které zahrnují umělou inteligenci a strojové učení.

Třetí metodou je **testování pomocí odchycených paketů** (PCAP), které se přehrávají za účelem emulace škodlivého provozu. To se provádí mezi dvěma hostiteli a používá se k testování a ověřování ovládacích prvků zabezpečení sítě.

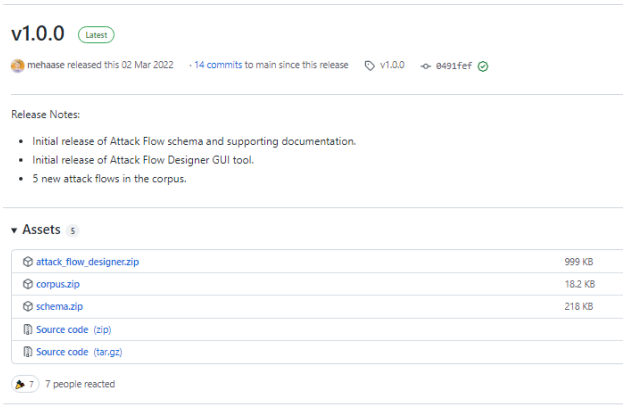
Často je obtížné LOLBinu zabránit, a tak může být úspěchem i jeho detekce a kategorizace jako cesta ku zmírnění či minimalizaci následků útoku.

Jedním ze zakládajících výzkumných partnerů Centre for Threat-Informed Defense (CTID) je společnost AttackIQ. Do svých modelů zahrnuje jak tradiční ovládací prvky, jako je antiviry, IDS a firewally, tak nativní ovládací prvky cloudového zabezpečení, jako jsou Azure, AWS a GCP. Vzhledem k tomu, že AttackIQ je v souladu s ATT&CK, můžete rychle začít vizualizovat ve formě teplotních map a dalších metrik a také začít vytvářet příběh o tom, čemu lze zabránit a/nebo detekovat, neboli kromě detekce zajišťovat i prevenci. Předání výsledků zpět příslušným vlastníkům těchto bezpečnostních kontrol může vést ke konstruktivním diskusím o analýze a nápravě.

Na https://github.com/center-for-threat-informed-defense/attack-flow je popis projektu Attack Flow – základní komponenty tohoto modelu zachycuje obr. 1.8.1. Projekt pomáhá obráncům přejít od individuálního sledování chování protivníka k sekvenci technik, které protivníci používají k dosažení svých cílů. Pochopení kontextu v těchto sekvencích a také vztahů mezi nimi umožňuje další obranné schopnosti, díky nimž jsou obránci mnohem efektivnější. Projekt se snaží demonstrovat, jak toky útoků mohou vedoucím pracovníkům vysvětlit obranný postoj, pomoci obráncům porozumět lekcím získaným z incidentu a podpořit červené týmy, aby snadno sestavovali realistické scénáře emulace protivníka. S cílem vizualizovat, analyzovat a sdílet toky útoků projekt Attack Flow vyvíjí datový formát pro popis sekvencí chování protivníka, sadu příkladů toku útoků a nástroj pro tvorbu toku útoků založený na grafickém uživatelském rozhraní. Projekt je ve verzi 1.0.0 (obr. 1.8.2).




Obr. 1.8.1 Základní komponenty modelu Attack Flow



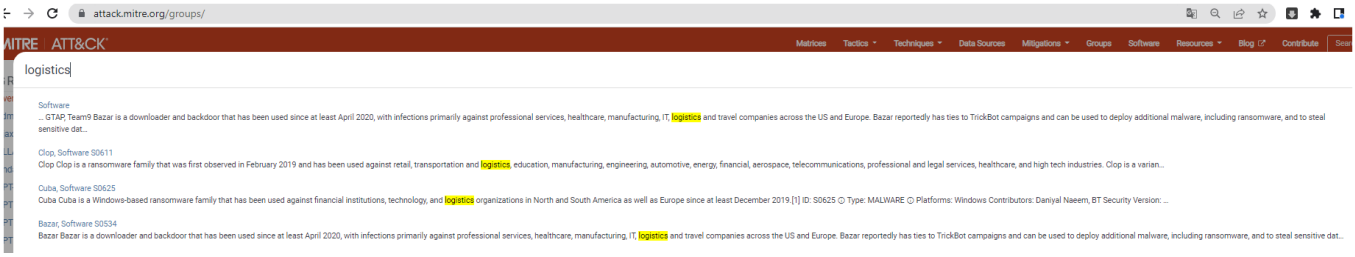

Obr. 1.8.2 Popis verze 1.0.0 projektu Attack Flow (https://github.com/center-for-threat-informed-defense/attack-flow/blob/main/docs/attack-flow-schema.md)

## 1.9 D3FEND

Ukažme si na příkladu jeho použití jako doplnění MITRE ATT&CK:

Společnosti, které teprve začínají a mají v této oblasti málo zdrojů, mohou začít tím, že porozumí obvyklému chování protivníků v jejich odvětví a na základě těchto údajů si ověří, zda implementovaná obrana odhaluje a zmírňuje akce těchto skupin. Abychom pochopili, jak se tato analýza provádí, vezměme si příklad logistické společnosti, které bývají často cílem útoku.

2. Nastavení daného oboru, tj. logistiku.

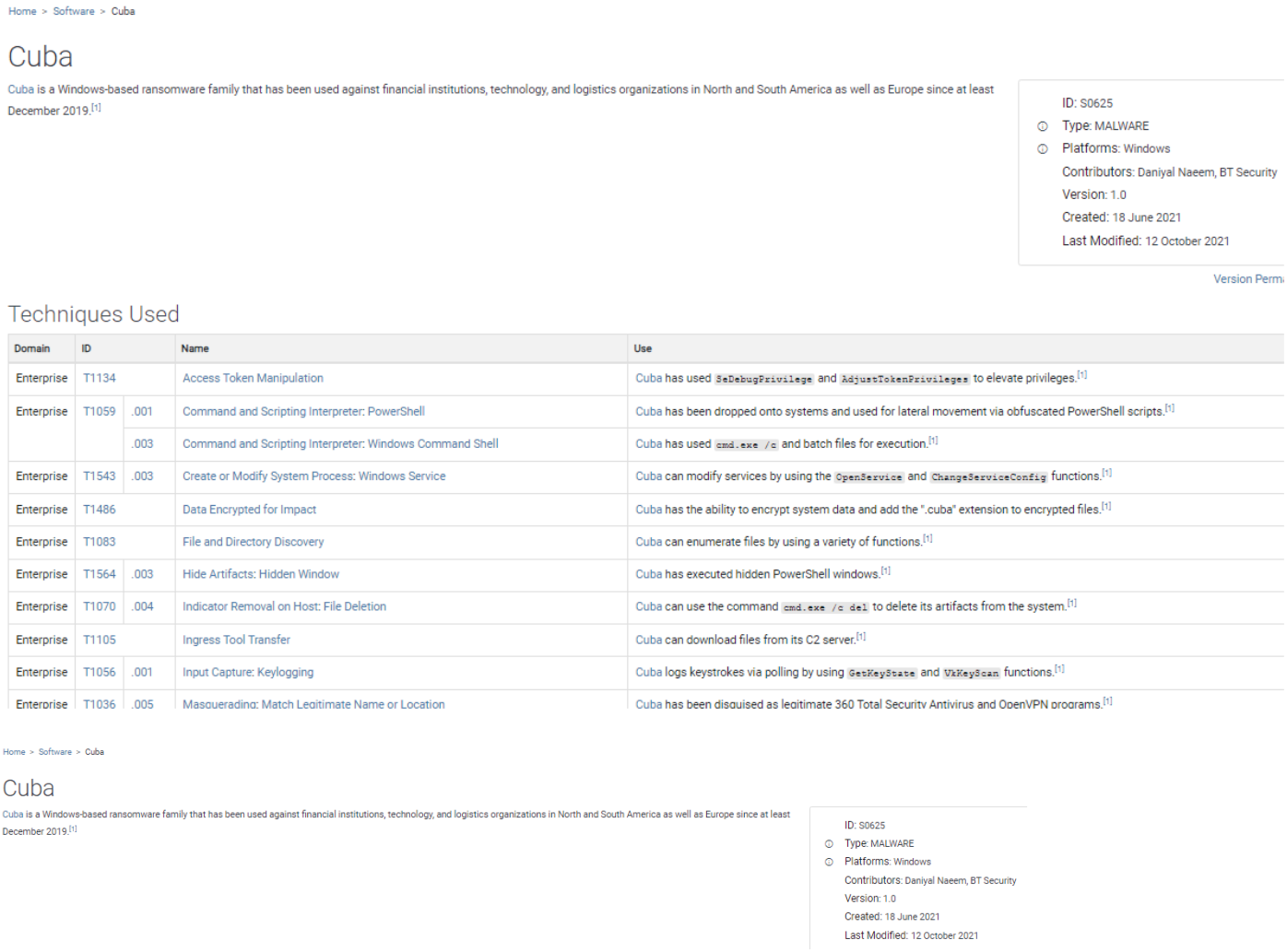



Obr. 1.9.1 Vyhledání útočného softwaru zaměřeného na logistiku na https://attack.mitre.org/groups/

K analýze si vezmeme ransomware Cuba, který označujeme na obrázku. Je jedním z nejpoužívanějších proti středně velkým společnostem.

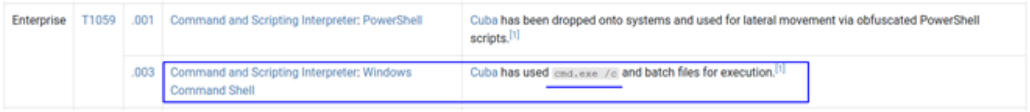
3. Získání informací o protivníkovi.

Jakmile je vybrán software nebo skupina, která má být analyzována, získá se přístup k informacím poskytovaným systémem, jako jsou základní údaje o platformě, která je napadena, kdy byla detekována, kdo ji detekoval a odvětví obětí.




Obr. 1.9.2 Získání informací o protivníkovi

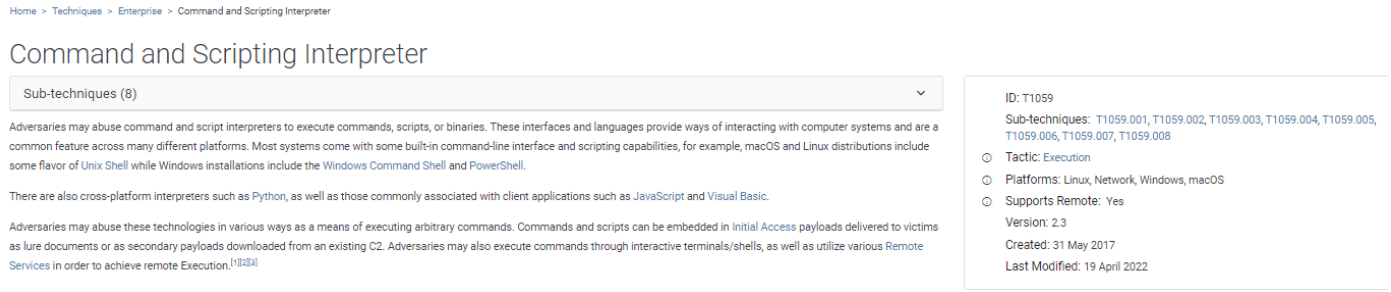
Z daných informací si lze vybrat konkrétní příkaz – viz obr. 1.9.3



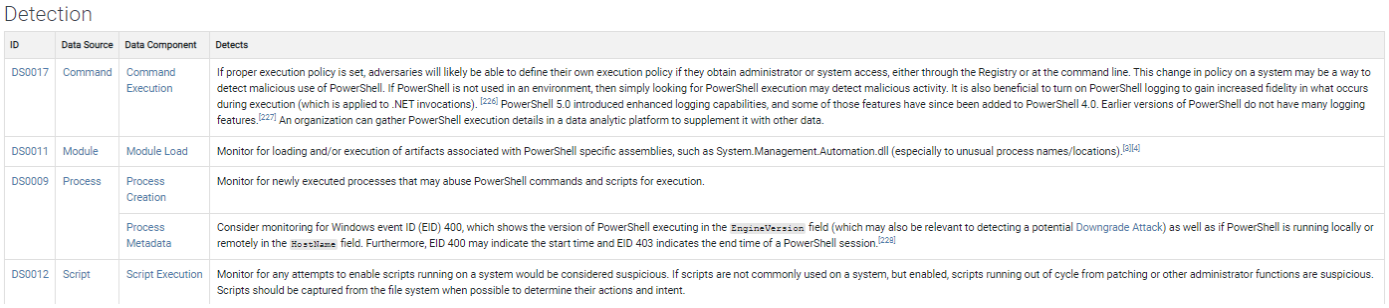

Obr. 1.9.3 Technika jako podklad k další analýze

Protivníci používají příkazovou konzolu Windows ke spouštění programů uvnitř oběti. V konkrétním případě Cuby byl v několika analyzovaných aktivitách detekován příkaz cmd.exe /c.

Přístupem k informacím o technice jsou shromážděna základní data o tom, jak byla použita, některé postupy, kde byla zjištěna, možná zmírnění a způsoby odhalování jejího provedení. V našem příkladu se podíváme přímo na informace a možné způsoby, jak je zjistit.



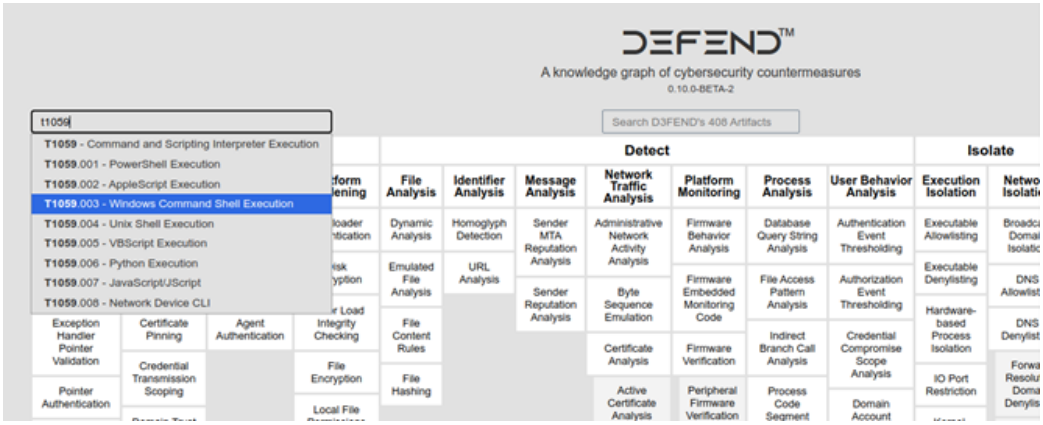

Obr. 1.9.4 T1059.003 Technique data




Obr. 1.9.5 Hledané techniky detekce

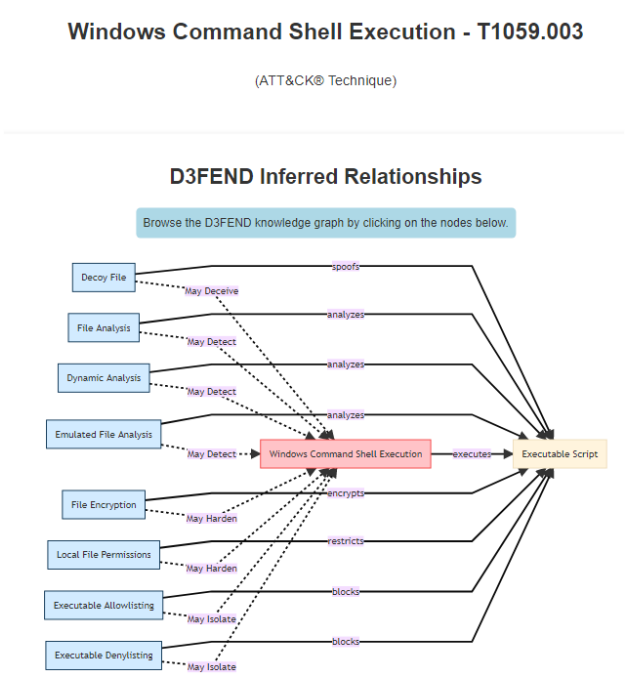
S těmito informacemi může tým kybernetické bezpečnosti rozhodovat o tom, jak jednat, aby zabránil incidentu, který využívá tento software k ovlivnění jejich průmyslového sektoru. Mohou dokonce odkazovat na techniku prohledávání obranné matrice, aby získali další informace o tom, jak se chránit.

Přejděme na https://d3fend.mitre.org/ a do vyhledávače s názvem ATT&CK lookup zadejme techniku, například T1059.003.




Obr. 1.9.4: Vztah k obranné matici.

Tím se dostaneme na mapu forem obrany a detekce, a pro náš příklad to jsou následující.




Obr. 1.9.5 Mapování obrany pro T1059.003

Stručně řečeno, tento nástroj je neocenitelný pro všechny typy podniků a týmy kybernetické bezpečnosti, protože poskytuje informace a data pro rozhodování ve snaze o lepší kybernetickou odolnost.

## 1.10 DeTT&CT

Byl vytvořen v Centru kybernetické obrany Rabobank a postaven na vrcholu MITER ATT&CK. DeTT&CT znamená: DEtect Tactics, Techniques & Combat Threats. V současnosti je ve verzi 1.1. DeTT&CT byl vytvořen s cílem pomoci modrým týmům využívajícím ATT&CK k hodnocení a porovnání kvality zdroje datových protokolů, pokrytí viditelnosti, pokrytí detekcí a chování aktérů hrozeb. To vše může různými způsoby pomoci k větší odolnosti proti útokům zaměřeným na vaši organizaci. DeTT&CT pracuje se soubory typu YAML.

Instalace je pomocí příkazů

```
git clone https://github.com/rabobank-cdc/DeTTECT.git
```

```
cd DeTTECT
```

```
pip install -r requirements.txt
```

a spuštění

```
python3 dettect.py e
```

# 3 Praktická část

## 3.1 Vyhledání softwaru k dané technice

Jste konzultant společnosti, která byla nedávno napadena kybernetickým útokem

Soudíte, že za problémy je zodpovědný APT29

Chcete vědět více o útoku i APT29

Řešení

- Přejděte na https://attack.mitre.org/groups.
- Najděte na stránce skupinu hrozeb APT29 a proklikejte se na stránku APT29.
- Přečtěte si popis pro APT29 a popisy přidružených skupin.
- Najděte softwarovou část na stránce skupiny APT29 a vyhledejte software, který se hodí k technice Dumpingu OS Credential Dumping.
- Proklikejte se na jednu ze součástí softwaru, která odpovídá dané technice (v našem příkladu jsme použili Mimikatz).
- Přečtěte si popis softwaru, který jste si vybrali.
- Otevřete jeden nebo dva odkazy v sekci zdrojů na stránce, abyste lépe porozuměli tomu, jak software funguje.

## 3.2 Použití MITRE ATT&CK Frameworku pro Threat Intelligence

Úvodní ujasnění

MITER ATT&CK Framework umožňuje porozumět chování protivníka tím, že odhalí:

- Jaké jsou jejich motivace?
- Na které země a odvětví se zaměřují?
- Jaké techniky používají?
- Jaké nástroje využívají?

Bez ohledu na úroveň vyspělosti týmů kybernetické bezpečnosti může ATT&CK pomoci jakékoli organizaci (resp. firmě). Tým MITER ATT&CK určil tři různé úrovně zralosti – pro malé střední a velké organizace. Na blogu[5] je vysvětleno, jak mohou organizace využít MITER ATT&CK Framework jako zdroj informací o hrozbách pro každou z těchto tří úrovní.

Threat Intelligence úrovně 1

Pokud daná organizace nemá specializovaný tým pro analýzu hrozeb, může začít s jedinou skupinou hrozeb zaměřenou na danou organizaci, odvětví nebo region. Pak se může podívat na techniky skupiny ohrožení (threat groups).

[5] OZARSLAN, Suleyman. How to Leverage the MITRE ATT&CK Framework for Threat Intelligence. picus-labs-1, 19. dubna 2022. Dostupné z: https://www.picussecurity.com/how-to-leverage-the-mitre-attack-framework-for-threat-intelligence?hsLang=en

Threat Intelligence úrovně 2

Pokud má organizace či firma tým střední úrovně s analytiky hrozeb, lze informace o hrozbách namapovat na ATT&CK a není třeba se spoléhat pouze na to, co na ATT&CK dříve mapovali jiní. Pokud má organizace zprávu o incidentu, může být tato zpráva vynikajícím interním zdrojem pro mapování na ATT&CK. Lze rovněž použít externí zprávu, například příspěvek na blogu.

Threat Intelligence úrovně 3

Pokud má daná firma pokročilý tým Cyber Threat Intelligence (CTI), lze začít mapovat další data do ATT&CK a poté tato data použít k upřednostnění způsobu obrany. Na ATT&CK lze namapovat interní i externí data, jako jsou data odezvy na incidenty, zprávy z OSINT nebo předplatných varování na hrozby, výstrahy v reálném čase a historická data firmy. Po mapování těchto informací lze porovnávat skupiny hrozeb a upřednostňovat běžně používané techniky. Data pak lze zkombinovat tak, aby byly objeveny nejčastěji používané techniky, které obráncům pomohou při rozhodování, na co se zaměřit. To umožňuje upřednostnit taktiku a informovat obránce o tom, na které z nich by se měli soustředit na odhalování a zmírňování následků útoku.

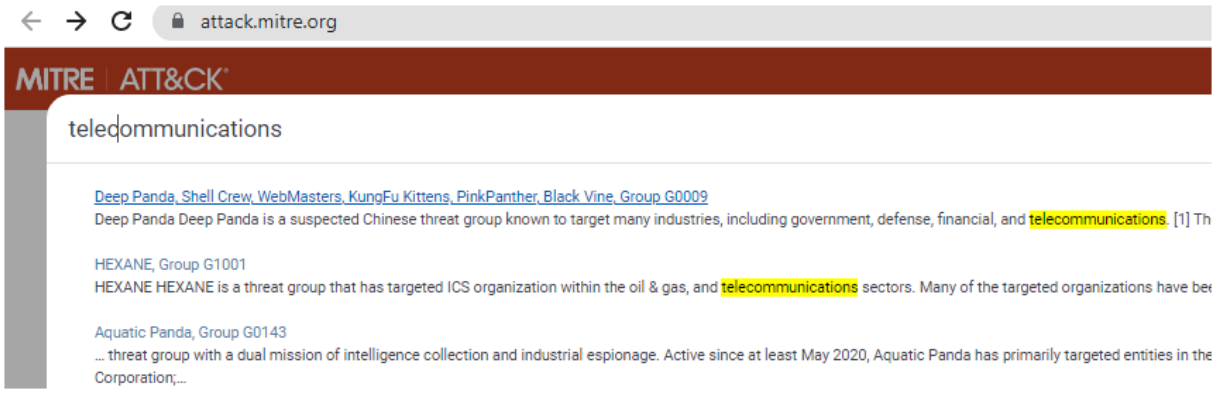
### 3.2.1 Threat Intelligence úrovně 1:

*Zadání*

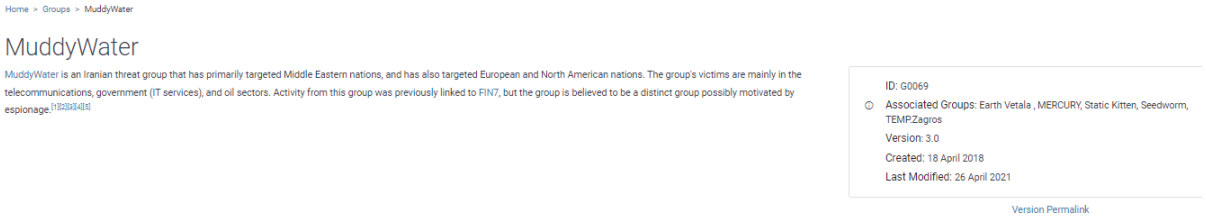
Zjištění technik, používaných danou skupinou ohrožení.

*Postup řešení*

Předpokládejme, že firma, ve které pracuje žák je americká telekomunikační společnost. Přejde tedy na domovskou stránku MITTRE ATT&CK (https://attack.mitre.org/) a zadá klíčové slovo „telecommunications“.




Na daný sektor se zaměřuje několik skupin hrozeb. Nyní může žák tyto skupiny zkontrolovat. Například skupina MuddyWater se zaměřuje na telekomunikační a ropný sektor v USA. Tato skupina je tedy pro telekomunikační firmu velmi relevantní. Žák proto podle zadání začne začít s MuddyWater. Klikne na odkaz MuddyWater a přejde na stránku této skupiny.



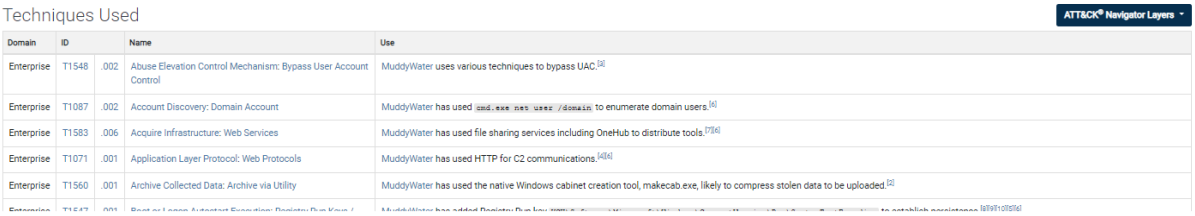

Jak může žák vidět na této stránce, ATT&CK poskytuje přiřazení skupiny, cílených geografických oblastí a cílených sektorů. Skupina MuddyWater APT je připisována Íránu, cílovými regiony jsou Střední východ, Evropa a Severní Amerika a cílovými sektory jsou telekomunikace, vláda a ropa.

Na stránce skupiny ATT&CK také poskytuje přidružené skupiny, což jsou stejné nebo velmi podobné skupiny v různých zprávách o hrozbách. Znalost názvů přidružených skupin je pro zpravodajství o hrozbách zásadní, protože dodavatelé nemají jednotný názor na pojmenování skupin hrozeb.

Associated Group Descriptions

| Name | Description |
|---|---|
| Earth Vetala | [6] |
| MERCURY | [7] |
| Static Kitten | [7][6] |
| Seedworm | [2][7][6] |
| TEMP.Zagros | [8][7][6] |

Na stránce skupiny může žák zjistit více, když se podívá na jejich techniky. Pro každou skupinu hrozeb ATT&CK zahrnuje techniky používané skupinou a stručně popisuje, jak skupina techniky používala.

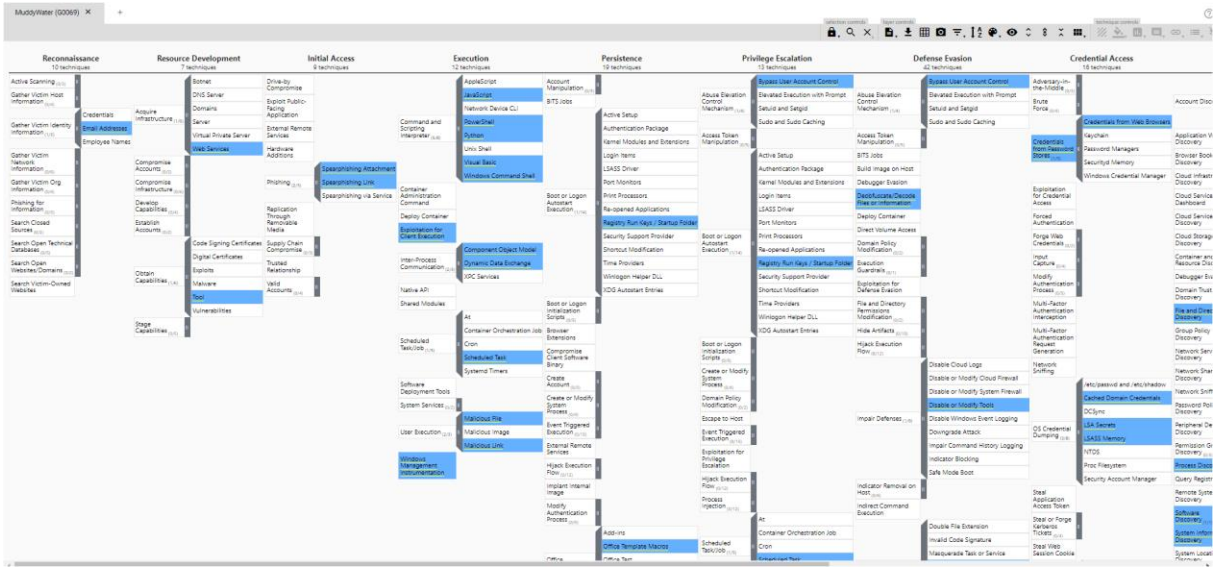


Techniques Used

ATT&CK® Navigator Layers

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1548 | .002 | Abuse Elevation Control Mechanism: Bypass User Account Control | MuddyWater uses various techniques to bypass UAC.[3] |
| Enterprise | T1087 | .002 | Account Discovery: Domain Account | MuddyWater has used `cmd.exe net user /domain` to enumerate domain users.[4] |
| Enterprise | T1583 | .006 | Acquire Infrastructure: Web Services | MuddyWater has used file sharing services including OneHub to distribute tools.[7][6] |
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | MuddyWater has used HTTP for C2 communications.[4][5] |
| Enterprise | T1560 | .001 | Archive Collected Data: Archive via Utility | MuddyWater has used the native Windows cabinet creation tool, makecab.exe, likely to compress stolen data to be uploaded.[2] |

Kromě toho ATT&CK vizualizuje techniky používané skupinou na ATT&CK Navigatoru. Chce-li žák zobrazit techniky v ATT&CK Navigator, může kliknout na tlačítko „ATT&CK Navigation Layers“ na stránce skupiny. Modré techniky označují techniky používané skupinou ohrožení MuddyWater.




Výstupem úlohy je výše uvedený obrázek zobrazení navigátoru „techniky používané skupinou ohrožení MuddyWater“.

### 3.2.2 Threat intelligence úrovně 2 – mapování zprávy o hrozbě do ATT&CK

*Zadání*

Mapování zprávy o hrozbě z blogu do ATT&CK a určen datového zdroje útoku popisovaného v rámci blogu.

*Postup řešení*

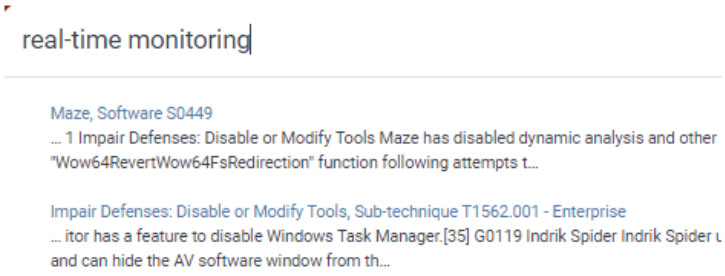
Žák má k dispozici konkrétní blog o vznikající malwarové hrozbě relevantní pro jeho firmu. Tento blog může být cenným zdrojem informací o hrozbách. Žák bude tento blog analýzy malwaru mapovat na MITER ATT&CK.

```
"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul & C:\Windows\System32\WindowsP
owerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntr
usionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -Enabl
eControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Di
sabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows
\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking\a
gent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kw
orking\agent.exe
```

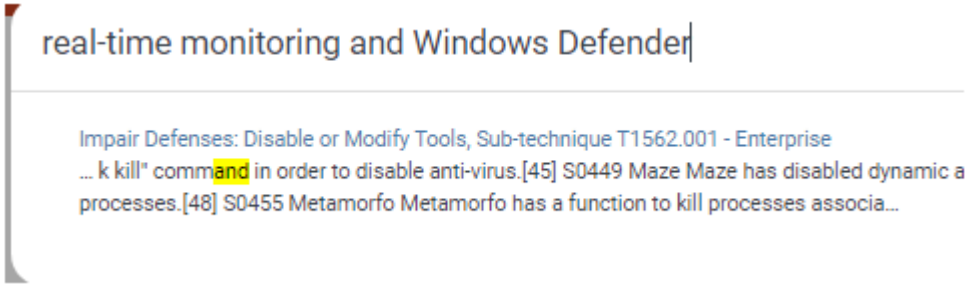
Úkolem je najít první příkaz, který něco vypíná:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeM
onitoring $true
```

Pomocí filtru zjistí, že případy, kdy se tak stává jsou dva:




Žákovi je poskytnuta informace, že vypnutí Real Time Monitoringu je typickou součástí útoku na Windows Defender. Dá si tedy do vyhledávání další klíčové slovo a to „Windows Defender“ – Windows jsou nejtypičtějším objektem útoku.




Přechod na danou subtechniku.

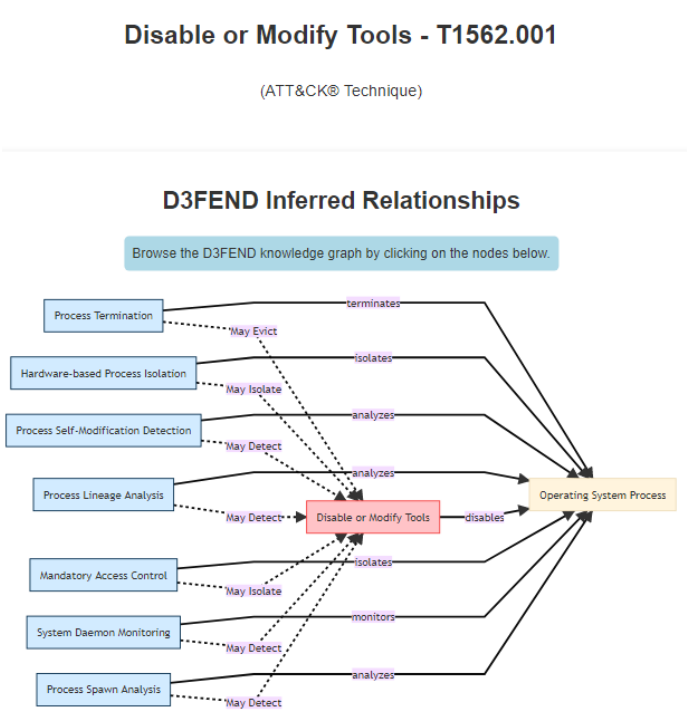

Žák by měl dojít ke zjištění, že útočník použil dílčí techniku MITER ATT&CK „T1562.001 Disable or Modify Tools“ v rámci techniky „T1562 Impair Defenses“.

Posledním úkolem je zjistit datové zdroje pro útok:

Detection

| ID | Data Source | Data Component | Detects |
|---|---|---|---|
| DS0017 | Command | Command Execution | Monitor for the execution of commands and arguments associated with disabling or modification of security software processes or services such as `Set-MpPreference -DisableScriptScanning 1` in Windows, `sudo spctl --master-disable` in macOS, and `setenforce 0` in Linux. |
| DS0009 | Process | Process Termination | Monitor processes for unexpected termination related to security tools/services. |
| DS0013 | Sensor Health | Host Status | Lack of expected log events may be suspicious. Monitor for telemetry that provides context for modification or deletion of information related to security software processes or services such as Windows Defender definition files in Windows and System log files in Linux. |
| DS0019 | Service | Service Metadata | Monitor for telemetry that provides context of security software services being disabled or modified. |
| DS0024 | Windows Registry | Windows Registry Key Deletion | Monitor for deletion of Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as HKLM:\SOFTWARE\Microsoft\AMSI\Providers. |
| | | Windows Registry Key Modification | Monitor for changes made to Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender. |

Výstupem úlohy je výše uvedený obrázek datových zdrojů pro útok popsaný v rámci blogu a následující graf.




## 3.3 Klasifikace údajů z ticketů z hlediska MITRE ATT&CK

Červeně je zde řešení pro učitele, řešení žáka může mít vícevariant

```
Ticket: 473822
Incident: Tangerine Yellow
Date: 2/15/2019 14:54:03
Description: cmd.exe commands via Pineapple RAT
Status: Assigned
The following commands were collected via Sysmon following Pineapple RAT
execution on the beachhead box.
ipconfig /all Discovery - System Network Configuration Discovery (T1016)
Execution - Command-Line Interface (T1059)
arp -a Discovery - System Network Configuration Discovery (T1016)
Execution - Command-Line Interface (T1059)
echo %USERDOMAIN%\%USERNAME% Discovery - System Owner / User
Discovery (T1033)
Execution - Command-Line Interface (T1059)
tasklist /v Discovery - Process Discovery (T1057)
Execution - Command-Line Interface (T1059)
sc query Discovery - System Service Discovery (T1007)
Execution - Command-Line Interface (T1059)
systeminfo Discovery - System Information Discovery (T1082)
Execution - Command-Line Interface (T1059)
net group "Domain Admins" /domain Discovery - Permission Groups Discovery
(T1069)
Execution - Command-Line Interface (T1059)
net user /domain Discovery - Account Discovery (T1087)
Execution - Command-Line Interface (T1059)
net group "Domain Controllers" /domain Discovery - Remote System Discovery
(T1018)
Execution - Command-Line Interface (T1059)
netsh advfirewall show allprofiles Discovery - System Network Configuration
```

```
Ticket: 473845
Incident: Tangerine Yellow
Date: 2/16/2019 10:14:44
Description: Pineapple RAT analysis
Status: Assigned
MD5 = dcf574b977e291e159b3efeddc9e5075
SHA1 = bc50bfce0ad9753a6be7448e350a15c1b7f719cc
SHA256 =
18548a48f2c30070dc3982bb04ab004a9491aa5c1933ad73a84c0de1d816cd13
Filename = winspoo1.exe Defense Evasion - Masquerading (T1036)
Analysis notes:
C2 protocol is base64 encoded commands (Command and Control - Data Encoding
(T1132)) over https (Command and Control Standard Application Layer Protocol
(T1071)). The RAT beacons every 30 seconds
requesting a command.
So far the following commands have been discovered and analyzed:
UPLOAD file (upload a file server->client)
DOWNLOAD file (download a file client->server) Command and Control -
Remote File Copy (T1105)
SHELL command (runs a command via cmd.exe) Execution - Command-Line
Interface (T1059)
PSHELL command (runs a command via powershell.exe) Execution -
Powershell (T1086)
EXEC path (executes a program at the path given via CreateProcess) Execution
- Execution through API (T1106)
SLEEP n (skips n beacons)
Sandbox execution artifacts for winspoo1.exe
Network traffic:
10.1.1.1:12442 -> 8.8.8.8:53 (query A www.m1tre.org)
8.8.8.8:53 -> 10.1.1.1:12442 (response A www.m1tre.org A 129.83.44.12)
10.1.1.1:24123 -> 129.83.44.12:443 Command and Control - Commonly Used Port
(T1043)
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123
File activity:
Copy C:\winspoo1.exe -> C:\Windows\System32\winspool.exe Defense Evasion -
Masquerading (T1036)
Registry keys added:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\winspool
REG_SZ "C:\
```

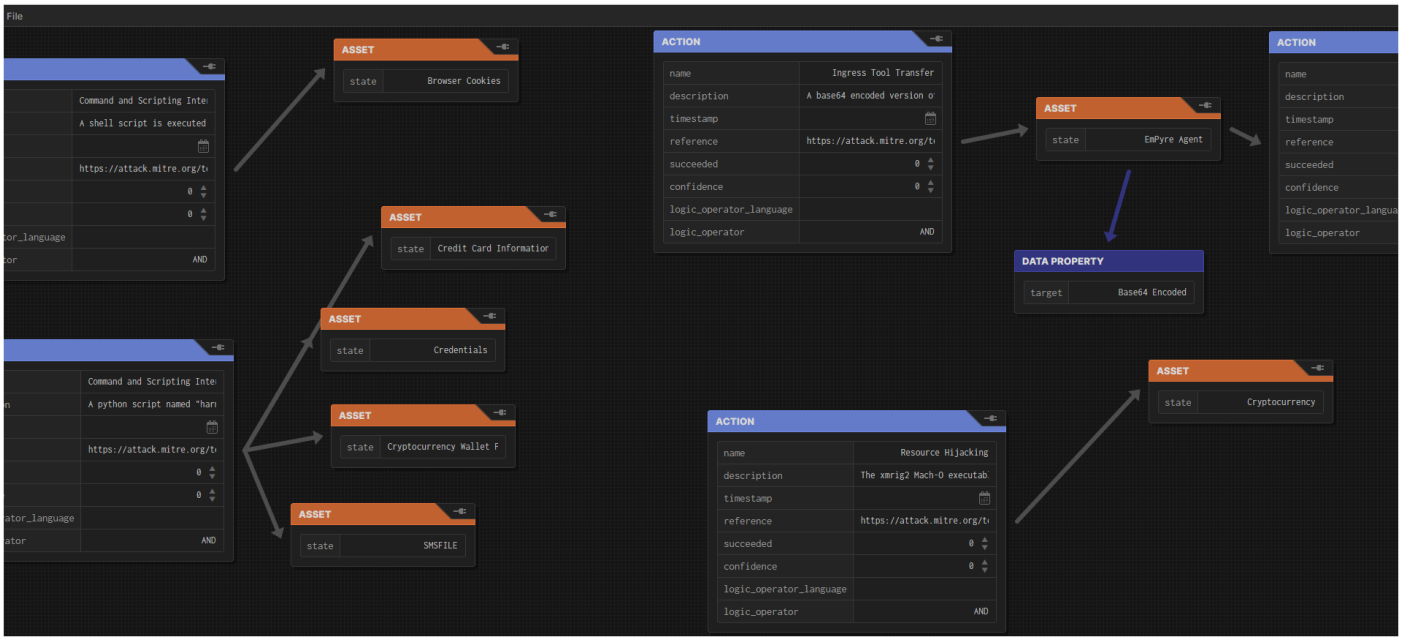
## 3.4 Testování 1. verze projektu Attack Flow

Jakmile se seznámíte se specifikací Attack Flow, zkuste použít Attack Flow Designer GUI k zobrazení nebo vytvoření vlastního Attack Flow podle postupu:

1. Přejděte na stránku vydání a stáhněte si attack_flow_designer.zip a také corpus.zip.
2. Rozbalte tyto dva soubory.
3. V adresáři attack_flow_designer poklepejte na index.html a otevřete jej ve webovém prohlížeči.

4. Uvnitř Attack Flow Designer přejděte do File → Open Attack Flow. Přejděte do adresáře korpusu a otevřete jeden ze souborů *.afd.
5. Chcete-li vytvořit svůj vlastní Attack Flow, obnovte stránku. Klikněte pravým tlačítkem na pracovní plochu Attack Flow a vytvořte uzel. Přetažením z ikony zástrčky spojíte uzly (v souladu s pravidly specifikace Attack Flow).
6. Uložte svůj Attack Flow v jednom ze dvou formátů:
    - File → Save Attack Flow: uloží soubor s příponou *.afd. Tento soubor je vhodný pro otevření pro úpravy v Attack Flow Designer.
    - Soubor → Publikovat Attack Flow: uloží soubor *.json, který odpovídá specifikaci Attack Flow; tento soubor je kompatibilní s dalšími nástroji Attack Flow.

Výstup testování:




# Shrnutí a závěr

MITRE ATT&CK byla v době zpracování materiálu ve verzi 11 – neboli se rychle rozvíjí. Slouží jako základ pro řadu projektů, na kterých pracuje celá řada firem.

# Seznam použitých zdrojů


BACKER, Joe. Attack Flow — Beyond Atomic Behaviors. Dostupné z: Attack Flow — Beyond Atomic Behaviors

NIKOLOV, Georgi. MITRE ATT&CK and the ATT&CK Matrix. Apr 7, 2022, https://cylab.be/blog/212/mitre-attck-and-the-attck-matrix

PALOMA Mitre Att&ck in Practice - Part I : Navigator & Atomic Red Team. Jul 14, 2022, https://cylab.be/blog/224/mitre-attck-in-practice-part-i-navigator-atomic-red-team

OZARSLAN, Suleyman. How to Leverage the MITRE ATT&CK Framework for Threat Intelligence. April 19, 2022. Dostupné z: https://www.picussecurity.com/how-to-leverage-the-mitre-attack-framework-for-threat-intelligence

Atomic Red Team Tutorial: Executing Atomic Test w/ Invoke-Atomic | Open Source Adversary Emulation. Red Canary Dostupné z: https://www.youtube.com/watch?v=7guUoRQEEiE

ATT&CK Deep Dive: Lateral Movement Pt. 1. Red Canary. Dostupné z: https://www.youtube.com/watch?v=nICBX-nzWL10

ATT&CK Deep Dive: Lateral Movement Pt. 1. Red Canary. Dostupné z: https://www.youtube.com/watch?v=M6MvhxKe80Q

Espitia, Diego Samuel. A practical approach to integrating MITRE's ATT&CK and D3FEND.16 February, 2022, https://business.blogthinkbig.com/practical-approach-integrating-mitres-attampck-d3fend/