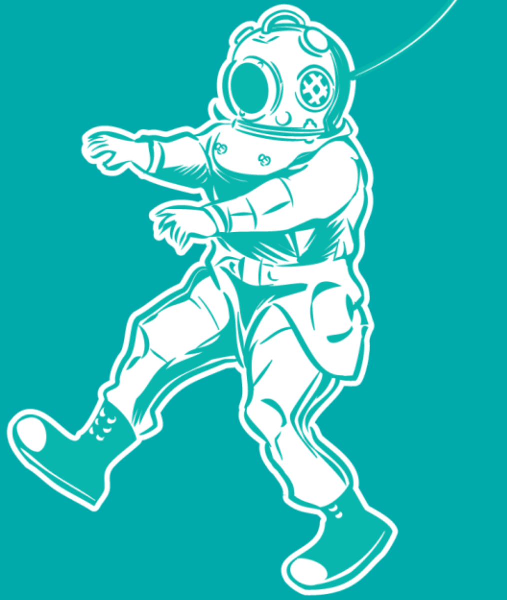
Vítejte

Chráníte svůj vzduch?



ℵ ALEF

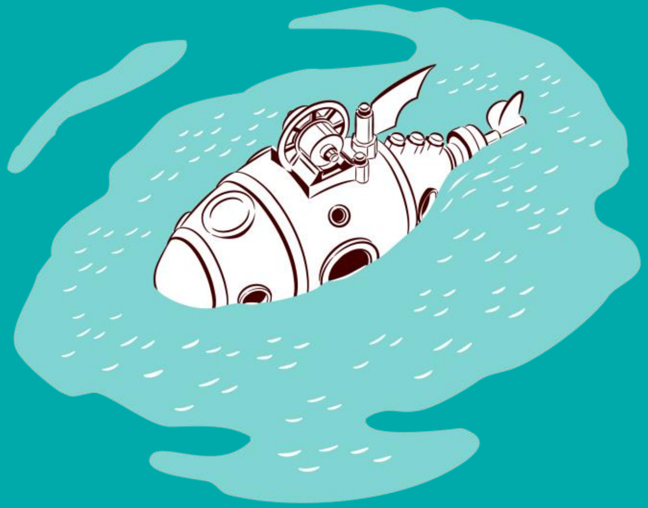
Introduction

$whoami

Martin Šišmiš

Email: martin.sismis@alef.com

Tel.: +420 778 007 608



Nejpoužívanější techniky útočníků (dle Palo Alto)

Časté techniky

- **Command and Scripting Interpreter (T1059)** – provádění příkazů za pomoci nativních nástrojů (PowerShell, cmd.exe).
- **Process Injection (T1055)** – Injektování škodlivého kódu do běžícího legitimního procesu. Slouží pro zvýšení oprávnění, utajení aktivit, či pro vytvoření perzistence.
- **Data from Local System (T1005)** – Sbírání dat přímo ze systému s úmyslem jeho extrakce.
- **Application Layer Protocol (T1071)**: Používání legitimních aplikačních protokolů (DNS, HTTP, HTTPS, atp.) pro extrakci dat a komunikaci s Command and Control (C2) servery.
- **Impair Defenses (T1562)** – Vyřazení či modifikace bezpečnostních aplikací pro upevnění přístupu na systém a snížení pravděpodobnosti detekce.

Techniky, které se objevují častěji

- **Living-off-the-Land Binaries (LOLBins)** – Použití legitimních nástrojů a aplikací k provádění škodlivých aktivit, což znesnadňuje detekci
- **Cloud-Specific Techniques** – Techniky spojené s cloudovým prostředím, jako například útoky na identitu, API, či zdroje v cloudu.
- **Supply Chain Compromise (T1195)** – Techniky útoků na dodavatelský řetězec obsahuje několik sub-technik, které se v poslední době objevují čím dál častěji (software, hardware, vývojářské nástroje a knihovny).

Nejpoužívanější techniky útočníků (top 10 MITRE dle obránců)

1. T1059 COMMAND AND SCRIPTING INTERPRETER
2. T1078 VALID ACCOUNTS
3. T1021.001 REMOTE DESKTOP PROTOCOL
4. T1047 WINDOWS MANAGEMENT INSTRUMENTATION
5. T1490 INHIBIT SYSTEM RECOVERY
6. T1105 INGRESS TOOL TRANSFER
7. T1083 FILE AND DIRECTORY DISCOVERY
8. T1486 DATA ENCRYPTED FOR IMPACT
9. T1190 EXPLOIT PUBLIC-FACING APPLICATION
10. T1489 SERVICE STOP

DOWNLOAD

T1059 COMMAND AND SCRIPTING INTERPRETER

DESCRIPTION

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

SUBTECHNIQUES

- T1059.001 POWERSHELL
- T1059.002 APPLESCRIPT
- T1059.003 WINDOWS COMMAND SHELL
- T1059.004 UNIX SHELL
- T1059.005 VISUAL BASIC
- T1059.006 PYTHON
- T1059.007 JAVASCRIPT
- T1059.008 NETWORK DEVICE CLI
- T1059.009 CLOUD API

APT - cílené útoky a sabotáž vzdušnou cestou

Příklady exfiltrace dat a sabotáže za pomoci bezdrátových technologií:

- Exfiltrace dat z laboratoře (napojené na NASA) – **implantované zařízení** v síti, exfiltrace z parkoviště.
- Zneužití „**radio-stop**“ signálu na polské železnici – zastaveno přes dvacet vlaků.
- U.S. Interior Department napadeno za pomoci **Evil Twin** techniky
- Zaznamenány nearest-neighbor útoky APT28
- Případy **špionážních dronů** nad kritickou infrastrukturou v Německu

MITRE ATT&CK – over the air

Initial Access	Execution
11 techniques	16 techniques
Content Injection	Cloud Administration Command
Drive-by Compromise	Command and Scripting Interpreter (12)
Exploit Public-Facing Application	Container Administration Command
External Remote Services	Deploy Container
Hardware Additions	ESXi Administration Command
Phishing (4)	Exploitation for Client Execution
Replication Through Removable Media	Input Injection
Supply Chain Compromise (3)	Inter-Process Communication (3)
Trusted Relationship	Native API
Valid Accounts (4)	Scheduled Task/Job (5)
Wi-Fi Networks	Serverless Execution
	Shared Modules
	Software Deployment Tools
	System Services (3)
	User Execution (4)
	Windows Management Instrumentation

Hardware Additions

Adversaries may physically introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and distributing payloads via removable storage (i.e. Replication Through Removable Media), more robust hardware additions can be used to introduce new functionalities and/or features into a system that can then be abused.

While public references of usage by threat actors are scarce, many red teams/penetration testers leverage hardware additions for initial access. Commercial and open source products can be leveraged with capabilities such as passive network tapping, network traffic modification (i.e. Adversary-in-the-Middle), keystroke injection, kernel memory reading via DMA, addition of new wireless access points to an existing network, and others.[1][2][3][4]

ID: T1200
Sub-techniques: No sub-techniques
ⓘ Tactic: Initial Access
ⓘ Platforms: Linux, Windows, macOS
Version: 1.7
Created: 18 April 2018
Last Modified: 15 April 2025

Procedure Examples

ID	Name	Description
G0105	DarkVishnya	DarkVishnya physically connected Bash Bunny, Raspberry Pi, netbooks, and inexpensive laptops to the target organization's environment to access the company's local network.[5]

MITRE ATT&CK – over the air

Initial Access	Execution
11 techniques	16 techniques
Content Injection	Cloud Administration Command
Drive-by Compromise	Command and Scripting Interpreter (12)
Exploit Public-Facing Application	Container Administration Command
External Remote Services	Deploy Container
Hardware Additions	ESXi Administration Command
Phishing (4)	Exploitation for Client Execution
Replication Through Removable Media	Input Injection
Supply Chain Compromise (3)	Inter-Process Communication (3)
Trusted Relationship	Native API
Valid Accounts (4)	Scheduled Task/Job (5)
Wi-Fi Networks	Serverless Execution
	Shared Modules
	Software Deployment Tools
	System Services (3)
	User Execution (4)
	Windows Management Instrumentation

Wi-Fi Networks

Adversaries may gain initial access to target systems by connecting to wireless networks. They may accomplish this by exploiting open Wi-Fi networks used by target devices or by accessing secured Wi-Fi networks — requiring Valid Accounts — belonging to a target organization.[1][2] Establishing a connection to a Wi-Fi access point requires a certain level of proximity to both discover and maintain a stable network connection.

ID: T1200

Sub-techniques: No sub-techniques

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Version: 1.7

Created: 18 April 2018

Last Modified: 15 April 2025

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has exploited open Wi-Fi access points for initial access to target devices using the network.[2][1]
C0051	APT28 Nearest Neighbor Campaign	During APT28 Nearest Neighbor Campaign, APT28 established wireless connections to secure, enterprise Wi-Fi networks belonging to a target organization for initial access into the environment.[2]

Picture source CROWDSTRIKE

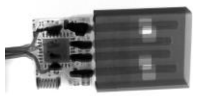
MITRE ATT&CK – over the air (částečně)

Initial Access 11 techniques	Execution 16 techniques
Content Injection	Cloud Administration Command
Drive-by Compromise	Command and Scripting Interpreter (12)
Exploit Public-Facing Application	Container Administration Command
External Remote Services	Deploy Container
Hardware Additions	ESXi Administration Command
Phishing (4)	Exploitation for Client Execution
Replication Through Removable Media	Input Injection
Supply Chain Compromise (3)	Inter-Process Communication (3)
Trusted Relationship	Native API
Valid Accounts (4)	Scheduled Task/Job (5)
Wi-Fi Networks	Serverless Execution
	Shared Modules
	Software Deployment Tools
	System Services (3)
	User Execution (4)
	Windows Management Instrumentation

Input Injection

Adversaries may simulate keystrokes on a victim's computer by various means to perform any type of action on behalf of the user, such as launching the command interpreter using keyboard shortcuts, typing an inline script to be executed, or interacting directly with a GUI-based application. These actions can be preprogrammed into adversary tooling or executed through physical devices such as Human Interface Devices (HIDs).

ID: T1674
Sub-techniques: No sub-techniques
Tactic: Execution
Platforms: Linux, Windows, macOS
Contributors: Alexey Kleymenov
Version: 1.0
Created: 27 March 2025
Last Modified: 15 April 2025



Procedure Examples

ID	Name	Description
G0046	FIN7	FIN7 has used malicious USBs to emulate keystrokes to launch PowerShell to download and execute malware from the adversary's server.[4]

ALEF

MITRE | ATT&CK®

Key-stroke Injection – Mousejack

- Mouse Jack zneužívá možnosti injektovat **nešifrovaná** stlačení kláves cílovému počítači na 2,4 GHz pásmu (nejedná se o bluetooth)
- Stlačení kláves na klávesnici je většinou šifrované, pohyby myši a stisky tlačítek **šifrované nejsou.**
- Zranitelnost spočívá v možnosti posílat **nešifrované stisky kláves**, které USB **dongl akceptuje** a provede.
- Existují i další varianty, kdy například při párování, lze díky slabému šifrovacímu algoritmu vyjednané klíče **cracknout** s možností komunikaci **odposlouchávat**, či opět stisky kláves injektovat.

Hardware

- NRF24L01+
  - Flipper Zero
  - Raspberry Pi
  - Arduino
- Nordic nRF52840 (usb dongle)
- Ubertooth One - Great Scott Gadgets
- CC1101 based
  - CC1101 standard module (10 mW output)
  - Flux capacitor - Rabbit-Labs (100 mW output, enhanced receiver capabilities)

LAB Time

Keystroke Injection

ALEF

Evil Twin útoky – obecný popis

- **Útočník nezná heslo** existující Wi-Fi sítě. Útočníkův Access Point vystupuje jako otevřené SSID, aby někoho oklamal a připojil se, nebo použije deauth (deautentizační) útok, aby uživatele odpojil a donutil k připojení k falešnému AP.
  - Útočník může nabídnout připojení k internetu a odposlouchávat provoz jako **MitM**.
  - **neodhalí heslo** skutečného SSID (klienti se automaticky nepřipojí k falešnému otevřenému SSID, pokud je to poprvé.)
- Útočník za pomoci **sociálního inženýrství**, **de-autentizačního** útoku, nebo kombinací obojího můžeš předstírat, že **skutečný AP má problém s konektivitou**.
  - Na „zlém“ AP sídlí **captive portal** (přihlašovací stránka k Wi-Fi) - která má za cíl zachytit heslo ke skutečnému AP (je potřeba zachytit handshake dříve, aby šlo ověřit, zda je zadané heslo správné).
  - Není účinné proti technicky zdatným uživatelům.
- **Útočník zná heslo** například z předchozích útoků, sociálního inženýrství, heslo je veřejně dostupné, nebo je SSID s otevřenou autentizací.
  - Útočník může pomocí **deauth** útoku odpojit uživatele, aby se připojil k falešnému AP.
  - Pokud nabídne i přístup k internetu, útočníkovo SSID vypadá legitimně a provoz lze odposlouchávat (**MitM**)
- **Kombinace Rogue Access Point** a **Evil Twin** útoku (**MitM**).
  - Útočník se stane součástí existující infrastruktury (například Access Point, AP bridge, apod.) a je fyzicky zapojený do sítě

ALEF

LAB Time

Wi-Fi Tinkering

Obrana

Obrana

Keystroke injection

- **Aktualizovat firmware** zařízení
- **Whitelisting** USB zařízení
- **Zablokování kritických tříd** USB zařízení
- **Port blocker** – kompletní blokování USB
- Použití speciálního programu pro **monitorování rychlosti psaní**
- Hledání zranitelných zařízení za pomoci **vulnerability assessment** nástroje či hledání v **lozích** operačních systémů
- **Zamezení přístupu uživatelů k příkazové řádce s vyšším oprávněním**

Evil Twin

- **Zákaz** automatického připojování
- Mandatorní použití **VPN**
- Použití **Wireless IDS**
- Implementace **WPA Enterprise** (802.1x) za pomoci **certifikátů**
- **Vzdělávání zaměstnanců**

Q&A

ALEF

Děkuji za pozornost