
# Old Microsoft Had A Farm (L.O.L.B.A.S)

**with Avneet and Tas**

# Agenda

- Introduction
- A Glimpse of Threat Hunting - ATT&CK and TTP
  - Organizing the attacker methods using MITRE ATT&CK
  - What is TTP
  - ATT&CK Navigator
- Attacker Perspectives
  - What are options for attackers
  - Pros and Cons
- LOLBAS
  - Deep dive on LOLBAS
  - Real life case of LOLBAS
- LOLBAS Demo
- Outro

# Glossary

EDR – Endpoint Detection and Response

Real-time endpoint monitoring solution with detection and response capability

SIEM – Security Information And Event Management

Security solution that collect, aggregate and analyze information from various sources (e.g. Splunk or Arcsight)

AV – Anti Virus

Anti virus solution such as Windows Defender, Symantec, McAfee, etc

APT – Advanced Persistent Threat

Malicious group classified by Threat Intelligence community

DLL – Dynamic Link Library

A file extension for shared library concept by Microsoft

YARA

A signature based tool designed to help malware researchers identify and classify malware samples

SOC – Security Operations Center

Centralized unit that deals with information security issues on both organizational and technical level

C2 – Command and Control Servers

Servers controlled by attacker serving as the center of their operation, these servers can be utilized to deliver payload or to download important data collected by the malware

# The Farmers

- Not actual Farmers…
  - Mangatas Tondang (Tas) and Avneet Singh
  - (Threat) Hunters @ Bell Canada SOC

- Threat Hunting and Threat Intel
  - Threat Emulation and Detection
  - Threat Intelligence (APTs, YARA, etc)
  - Tools Development
  - Security Trainings and Presentation

- Education
  - Avneet – ISS (MEng) from Concordia University
  - Tas – ISS (BAISc) from Sheridan College


# DISCLAIMER

**This talk <u>IS NOT</u> about Farming or Farming Simulator**


**Opinions are ours and <u>DO NOT REPRESENT</u> our Employer's views**

**This presentation is for <u>EDUCATIONAL PURPOSE</u> only!**
**We are not responsible for any misuse of the information .**

a comprehensive guide to

# Yellow Stripey Things

**Carpenter Bee**
-acts like it's hot but can't actually hurt you
-has no concept of what glass is
-lives in your fence
-flies aggressively to try and scare you away

**Honeybee**
-is the bee that needs help the most
-excellent pollenator
-very friendly
-can only sting once

**Bumblebee**
-also pollenates stuff very well
-so fat it shouldn't be able to fly
-will let you pet it without getting agitated
-actually a flying panda

**Hoverfly**
-wears yellow stripey uniform to scare you
-actually can't do anything to you
-hangs out in fields
-follows you if it likes you

**Paper Wasp**
-looks scary, but will only attack if provoked
-sting hurts like hell
-will chase you if you swat at it
-has no concept of personal space

**Yellow Jacket**
-wants your food and will fight you for it
-never leaves you alone
-will sting you just for the hell of it
-is just an as

**Cicada Killer**
-looks like Satan's nightmares
-exclusively eats cicadas
-can sting you, but usually won't
-still pretty terrifying

**Dirt Dauber**
-almost never stings anything except spiders
-builds nest in the ground
-hoards spiders in said nest
-coolest looking of the wasps

# Organizing The Attackers

## Intro to ATT&CK and TTP

# MITRE ATT&CK

*https://attack.mitre.org/*

- Knowledge base of adversary tactics and techniques
- Based on real-world observations and examples
- Open source!

Created on September 2013

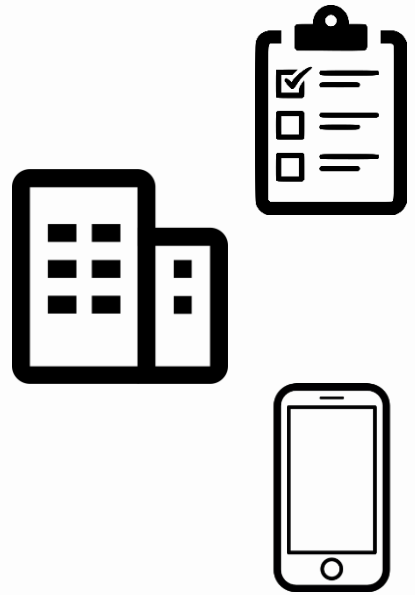
Have their own conference; MITRE ATT&CKcon

Functions:

- Track adversary behaviours (APTs, Malware, etc.)
- Common language for Defender (Blue Team)

# MITRE ATT&CK Matrices

- PRE-ATT&CK
- Enterprise
  - Operating Systems (Windows, macOS, Linux)
  - Cloud (AWS, GCP, Azure, Office 365, Azure AD, SaaS)
- Mobile
  - Android
  - iOS



# ATT&CK Enterprise Tactics

- Total 12 Enterprise Tactics

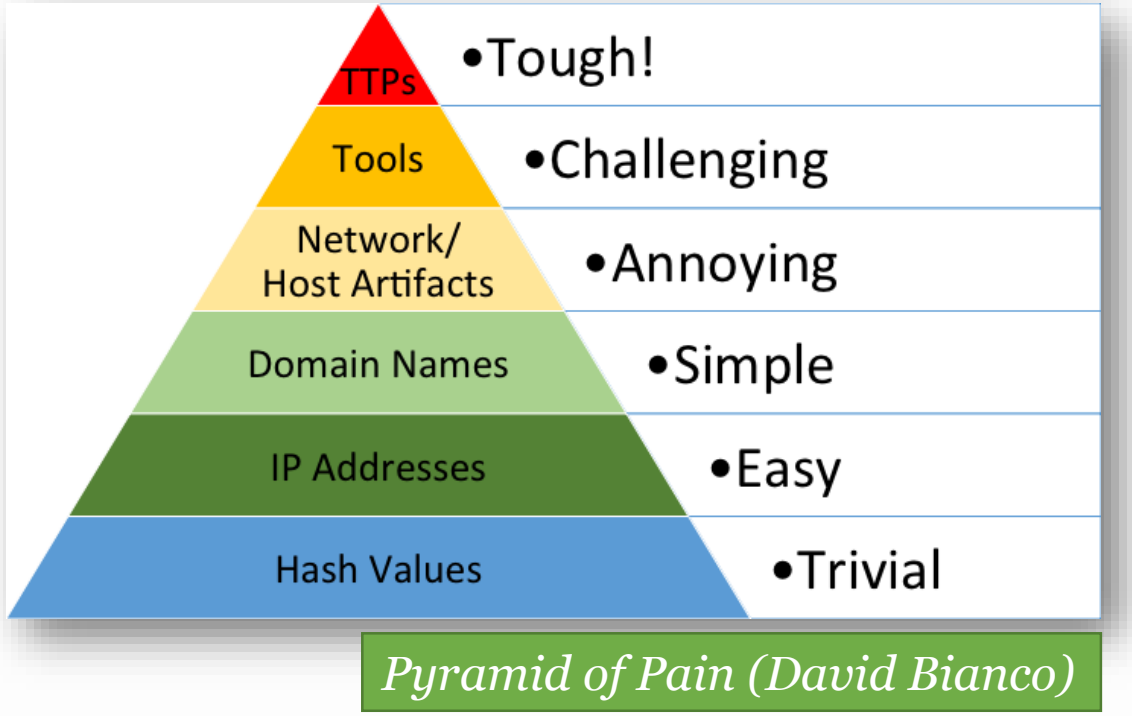
| ID | Name | Description |
|---|---|---|
| TA0001 | Initial Access | The adversary is trying to get into your network. |
| TA0002 | Execution | The adversary is trying to run malicious code. |
| TA0003 | Persistence | The adversary is trying to maintain their foothold. |
| TA0004 | Privilege Escalation | The adversary is trying to gain higher-level permissions. |
| TA0005 | Defense Evasion | The adversary is trying to avoid being detected. |
| TA0006 | Credential Access | The adversary is trying to steal account names and passwords. |
| TA0007 | Discovery | The adversary is trying to figure out your environment. |
| TA0008 | Lateral Movement | The adversary is trying to move through your environment. |
| TA0009 | Collection | The adversary is trying to gather data of interest to their goal. |
| TA0011 | Command and Control | The adversary is trying to communicate with compromised systems to control them. |
| TA0010 | Exfiltration | The adversary is trying to steal data. |
| TA0040 | Impact | The adversary is trying to manipulate, interrupt, or destroy your systems and data. |

# TTPs

Tactics, Techniques and Procedures used by adversary

## Pyramid of Pain

- Potential usefulness of intel
- Difficulty of obtaining the intel
- Resources needed by attacker to change




*Pyramid of Pain (David Bianco)*

# ATT&CK Enterprise TTPs

- Total 266 Enterprise TTPs
- TTPs can have multiple Tactics
- ID Format TXXXX

## Component Object Model and Distributed COM

Adversaries may use the Windows Component Object Model (COM) and Distributed Component Object Model (DCOM) for local code execution or to execute on remote systems as part of lateral movement.

COM is a component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces.[1] Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).[2] DCOM is transparent middleware that extends the functionality of Component Object Model (COM) [2] beyond a local computer using remote procedure call (RPC) technology.[1]

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry. [3][4][5] By default, only Administrators may remotely activate and launch COM objects through DCOM.

Adversaries may abuse COM for local command and/or payload execution. Various COM interfaces are exposed that can be abused to invoke arbitrary execution via a variety of programming languages such as C, C++, Java, and VBScript.[2] Specific COM objects also exists to directly perform functions beyond code execution, such as creating a Scheduled Task, fileless download/execution, and other adversary behaviors such as Privilege Escalation and Persistence.[1][6]

Adversaries may use DCOM for lateral movement. Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications [7] as well as other Windows objects that contain insecure methods.[8][9] DCOM can also execute macros in existing documents [10] and may also invoke Dynamic Data Exchange (DDE) execution directly through a COM created instance of a Microsoft Office application [11], bypassing the need for a malicious document.

ID: T1175
Tactic: Lateral Mo
Platform: Windo
Permissions Req
Data Sources: Po
Authentication log
monitoring, Windows Registry, Windows event logs
Supports Remote: Yes
Version: 2.0

ID: T1175

Tactic: Lateral Movement, Execution

Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Data Sources: PowerShell logs, API monitoring, Authentication logs, DLL monitoring, Packet capture, Process monitoring, Windows Registry, Windows event logs

Supports Remote: Yes

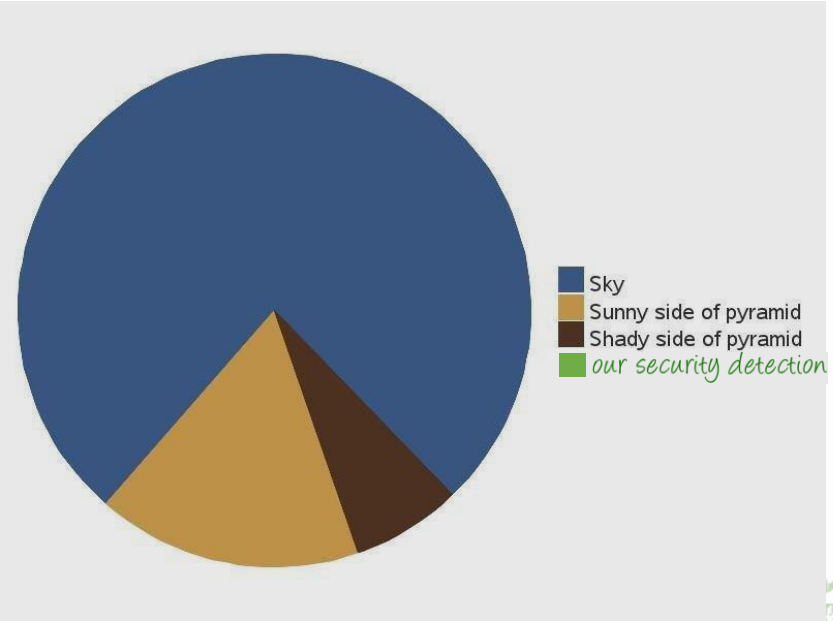
Version: 2.0

# ATT&CK Navigator Enterprise

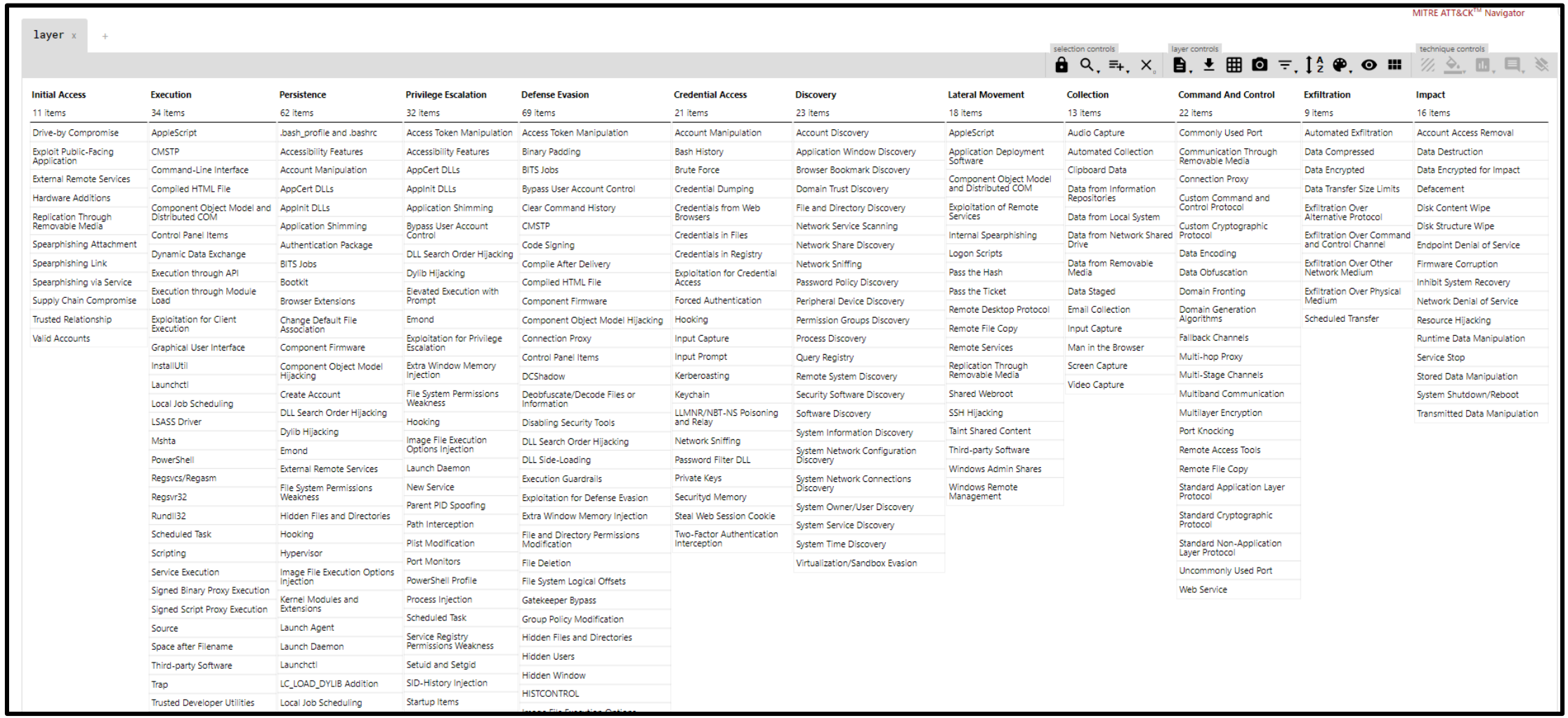
https://mitre-attack.github.io/attack-navigator/enterprise/

- Provide basic navigation and annotation of ATT&CK matrices
- Easy to look at
- Modifiable JSON file can be used to track progress

- Sample usages:
  - Defensive coverage
  - Tools (EDR, IDS, etc.) coverage
  - Red/blue team planning
  - Anything else you want to do with ATT&CK

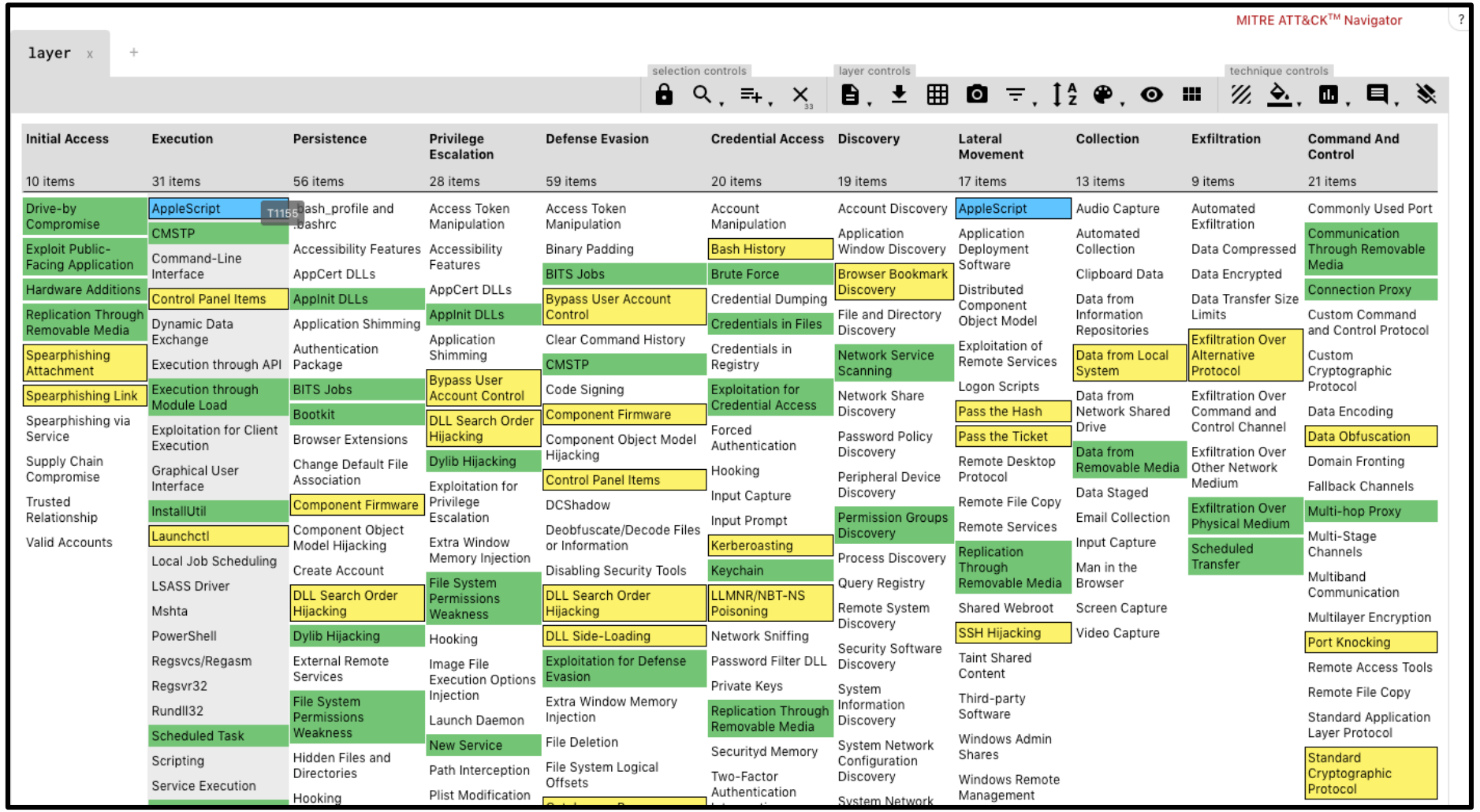


# ATT&CK Navigator Enterprise - Raw




| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 items | 34 items | 62 items | 32 items | 69 items | 21 items | 23 items | 18 items | 13 items | 22 items | 9 items | 16 items |
| 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 | Account Access Removal |
| 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 Destruction |
| 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 Encrypted for Impact |
| 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 | Defacement |
| 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 Content Wipe |
| 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 | | Hidden Window | | | | | | | |
| | Trusted Developer Utilities | | | HISTCONTROL | | | | | | | |

# ATT&CK Navigator Enterprise - Usage




## Defense Coverage

*Legends Example*

Green:

Rule Deployed

Yellow:

Dashboard Monitoring

Blue:

Planned


# Decision… Decision…

## Comparing Attack Avenues

# Attack Avenue 1 – Fileless Attack

- Don’t bring anything to the network ☺
- E.g.
  - PowerShell
    - APT28/29, Cobalt Group, Emotet
  - Malicious Macros
    - Any attack that use Word/Excel email attachment
  - Use WMI (Windows Management Instrumentation)
    - GandCrab Malware
  - Compile on the Fly (.NET, Python, etc.)
    - Ursnif Malware, Sodinokibi Ransomware

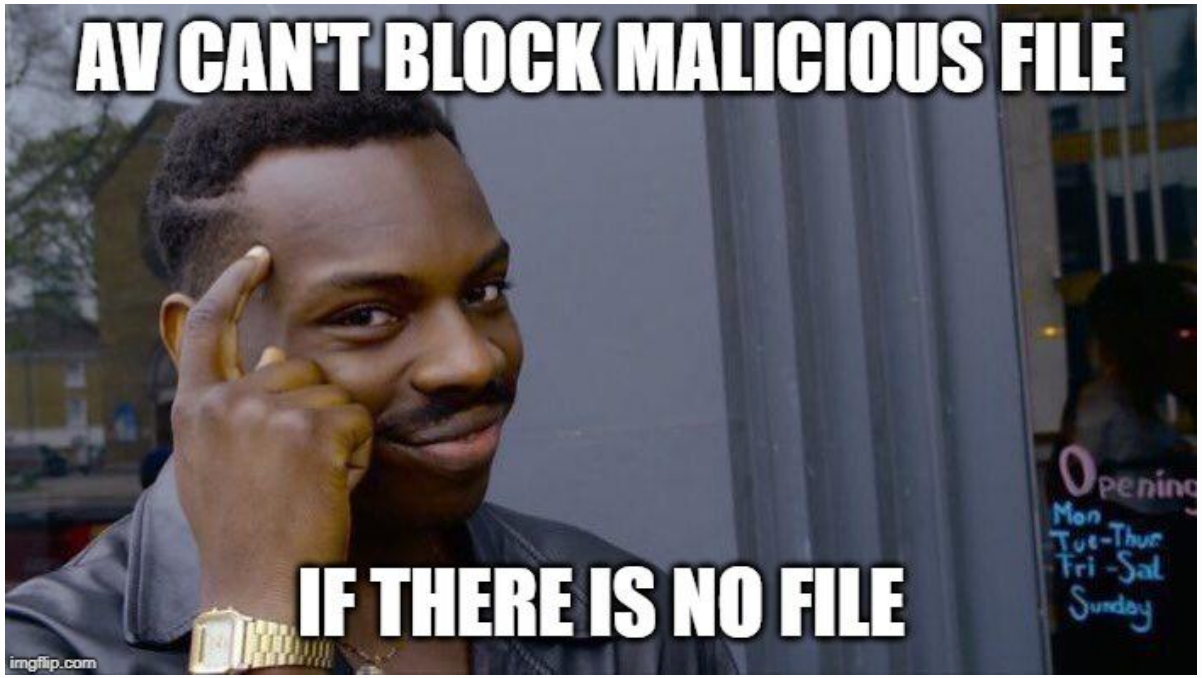
# Pros and Cons – Fileless Attack

**PROs**

- Simple
  - No need to code anything
- Stealthy
  - No file creation
  - No file download
- Bypass AV
  - AV mostly detect file based attack

**CONs**

- Limited
  - Can’t do everything you want
- Specific Target Only
  - Linux server doesn’t have PowerShell or .NET




# Attack Avenue 2 – File Drop Attack

- Bring everything to the network ☺
  - Drop Malware or supporting binaries
- E.g.
  - CosmicDuke and CosmicCar
    - Used by APT29
  - Mimikatz
    - Famous credential dumper used by APTs and Red Team
  - Miner-C
    - Crypto mining malware

# Pros and Cons – File Drop Attack

**PROs**

- Unlimited
  - Can do everything you want
- Any Targets
  - You can deploy the tools and modify the tools to follow the environment

**CONs**

- Sophisticated
  - Need to create or understand the tools
- Stealthy-NOT!
  - File creation
  - File download
- AV Detection
  - AV mostly detect file based attack


Did we miss anything?


# Yes, the main content of presentation

## Deep dive on LOLBAS

# LOLBAS


https://github.com/LOLBAS-Project/LOLBAS/

**L**iving **O**ff The **L**and **B**inaries **A**nd **S**cripts
(and also Libraries)

Also previously known as LOLBINs

- **L**iving **O**ff The **L**and **Bin**ary

LOL term coined by Christopher Campbell and Matthew Graeber

- During Derbycon 3.0 (2013)

Continued by Oddvar Moe and other security researchers

# What is LOLBAS?

A technique that abuse legitimate pre-installed Windows (Microsoft) binaries (or libraries and scripts) to perform unexpected activities that will benefit malicious actors.

**LOLBAS** ★ Star 1,340

**Living Off The Land Binaries and Scripts (and also Libraries)**

More info on the project? Click logo
Want to contribute? Go here for instructions:
https://github.com/LOLBAS-Project/LOLBAS/blob/master/CONTRIBUTING.md

If you are looking for UNIX binaries you should visit https://gtfobins.github.io/

Search among 108 binaries by name (e.g., 'MSBuild') or by function (e.g., '/execute') or by type (e.g., '#Script')

| Binary | Functions | Type |
|---|---|---|
| At.exe | Execute | Binaries |
| Atbroker.exe | Execute | Binaries |
| Bash.exe | Execute, AWL bypass | Binaries |
| Bitsadmin.exe | Alternate data streams, Download, Copy, Execute | Binaries |
| Certutil.exe | Download, Alternate data streams, Encode, Decode | Binaries |
| Cmd.exe | Alternate data streams | Binaries |
| Cmdkey.exe | Credentials | Binaries |

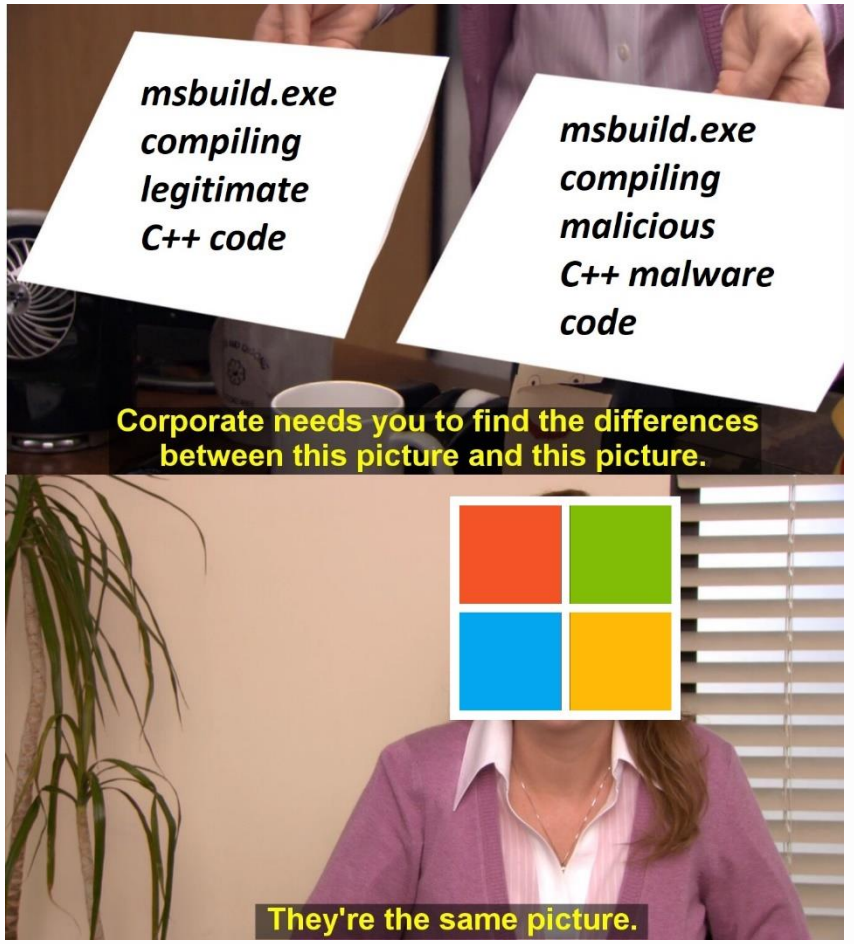
*LOLBAS Github Page*

# LOLBAS Criteria

- Be a Microsoft-signed file
  - Native to the OS or downloaded from Microsoft
- Have extra "unexpected" functionality. It is not interesting to document intended use cases.
  - Exceptions are application whitelisting bypasses
- Have functionality that would be useful to an APT or red team


# LOLBAS Functionality (1)

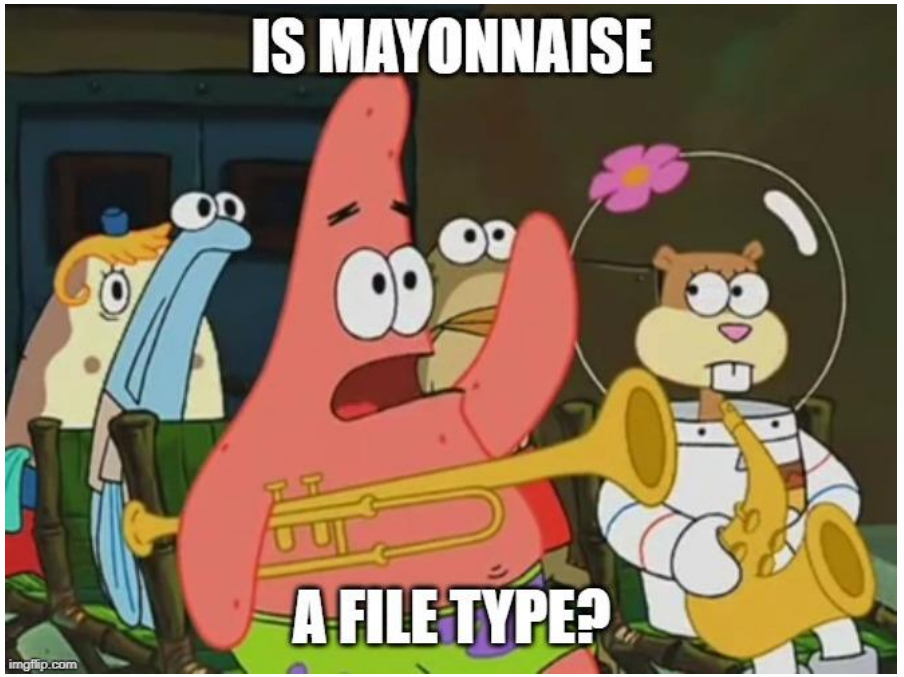
- Executing code (e.g. hh.exe)
  - Arbitrary code execution
  - Pass-through execution of other programs (unsigned) or scripts (via a LOLBin)
  - Surveillance
    - key logger, network trace
  - Log evasion/modification
- Compiling code (e.g. msbuild.exe)
- File operations (e.g. bitsadmin.exe)
  - Downloading
  - Upload
  - Copy



# LOLBAS Functionality (2)

- Persistence (e.g. regedit.exe)
  - Pass-through persistence utilizing existing LOLBin
  - Persistence (e.g. hide data in ADS, execute at logon)
- UAC bypass (e.g. Eventvwr.exe)
- Credential theft (e.g. findstr.exe)
- Dumping process memory (e.g. comsvcs.exe)
- DLL side-loading/hijacking (e.g. regsvr.exe)
  - without being relocated elsewhere in the file system.

# LOLBAS By File Type



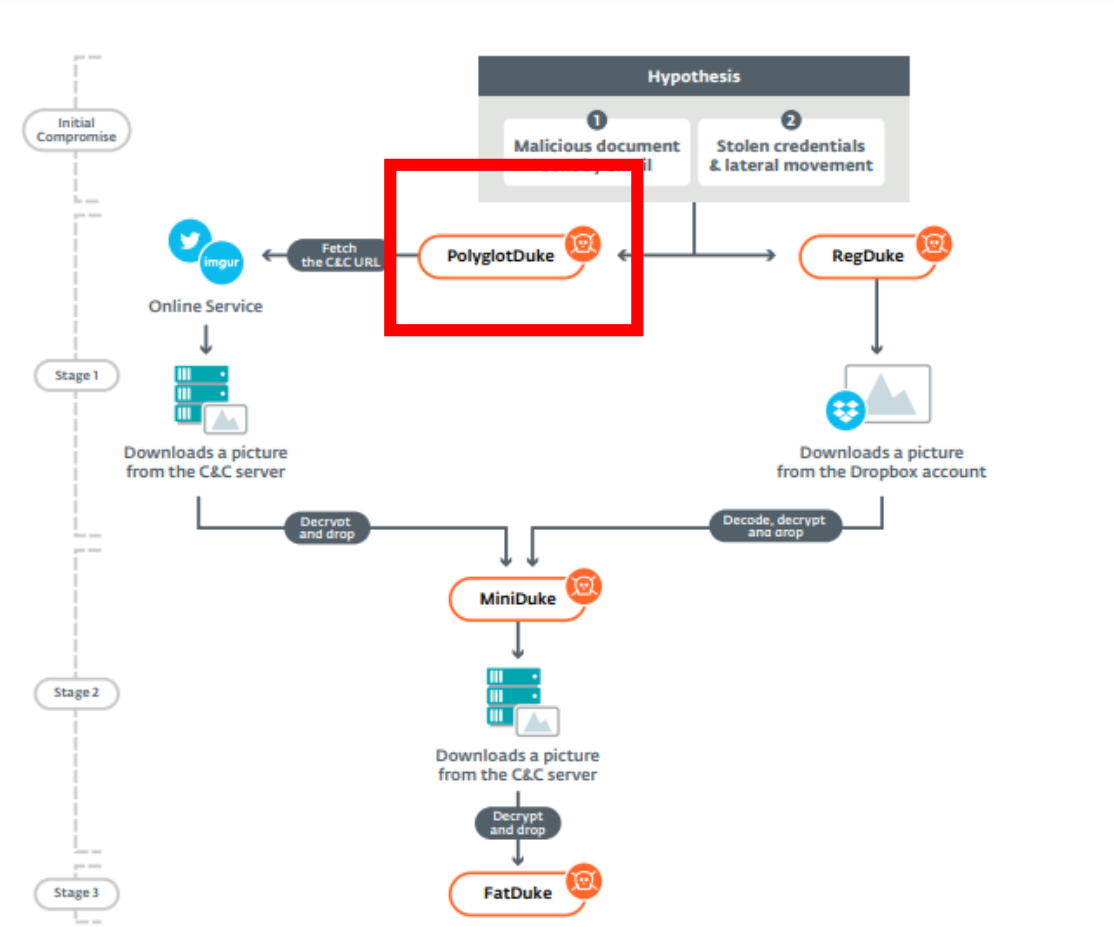

- Binaries
  - .exe files
- Libraries
  - .dll files
- Other MS Binaries
  - .exe files not installed by default
  - (e.g. MS Office Binaries, MSSQL Binaries)
- Scripts
  - .vbs, .ps1 or other scripts that can be used to perform attack functions

# Why Attacker Love LOLBAS

- Off the land!
  - No need to bring anything
  - Harvest it straight from the land
- You can do lot of stuff!
  - All the functions we mentioned above
- Signed by Microsoft!
  - So it must be legitimate ☺
- Often whitelisted by Blue Team!
  - No need to evade detection
  - Often ignored too by Analyst

# Real Life LOLBAS – APT29

- Disrupt 2016 US Election
- APT29 known to use rundll32.exe to execute their payload during Operation Ghost
  - Stage 1 - PolygotDuke Malware
  - Discovered by ESET Researcher



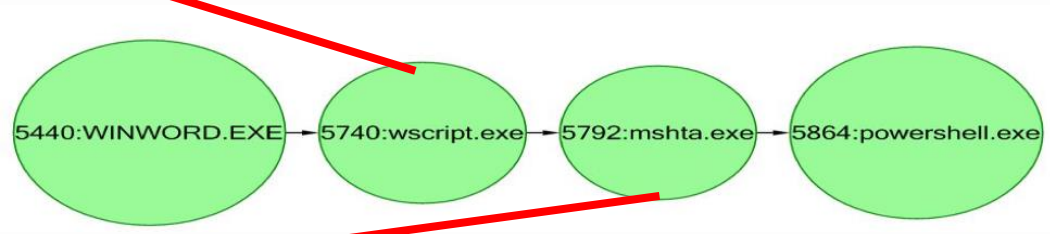

*Operation Ghost Stages (ESET)*

# Real Life LOLBAS – MuddyWater

- Iranian Threat Actor operating in Asia and Middle East
- APT29 known to use mshta.exe to execute their Wscript (.vbs) payload

Discovered by FireEye Researcher

```
{5740} C:\Windows\System32\wscript.exe  "C:\Windows\System32\WScript.exe" "C:\ProgramData\SYSTEM32SDK\ConfManagerNT.vbs"
```




```
{5792} C:\Windows\System32\mshta.exe  "C:\Windows\System32\mshta.exe" vbscript:Close(Execute("CreateObject(""WScript.Shell"").Run""powershell.exe -w 1 -exec Bypass -
nologo -noprofile -c iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((get-content C:\ProgramData\SYSTEM32SDK
\ProjectConfManagerNT.ini))));"",0 "))
```

*MuddyWater Stage 1 Campaign– Process Chain*

Nobody:

Bugs right before a demo:

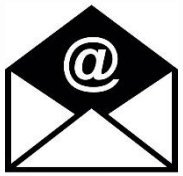

# Demo

**Did you pray to the demo God today?**

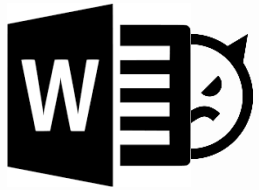
# Demo – Attack Flow

0. C2 deployed, malware campaign started

1. Victim download the malicious email attachment

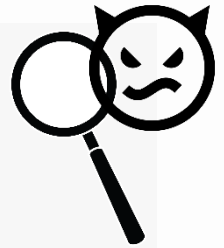


2. Victim open and run the VBS (Macro) code



3. VBS launch PowerShell process
4. PowerShell download the payload .ps1 script
5. PowerShell execute the payload

6. The script is performing data and credentials collection on the victim machine



7. The script proceed to write the data to a file in %TEMP folder
8. The script encode the data using certutil.exe

9. Ship data to C2

# Demo – TTPs Mapping

- Initial Access – using VBS (Macro)
  - Spearphishing Attachment (T1193)
- Execution – using PowerShell
  - Scripting (T1064)
  - PowerShell (T1086)
- Discovery - **using REG.EXE, SCHTASKS.EXE, WMIC.EXE (LOLBAS)**
  - Account Discovery (T1087)
  - File and Directory Discovery (T1083)
  - Query Registry (T1012)
  - System Owner/User Discovery (T1033)
  - And more…
- Defense Evasion
  - Deobfuscate/Decode Files or Information (T1140) – **using CERTUTIL.EXE(LOLBAS)**
- Command And Control
  - Data Encoding (T1132) – **using CERTUTIL.EXE(LOLBAS)**
- Persistence
  - Valid Accounts (T1078) – **using CERTUTIL.EXE(LOLBAS)**
- Privilege Escalation
  - Valid Accounts (T1078) – **using CMDKEY.EXE (LOLBAS)**

# DEMO TIME!

## PRESENTATION INTRO

## PRESENTATION OUTRO

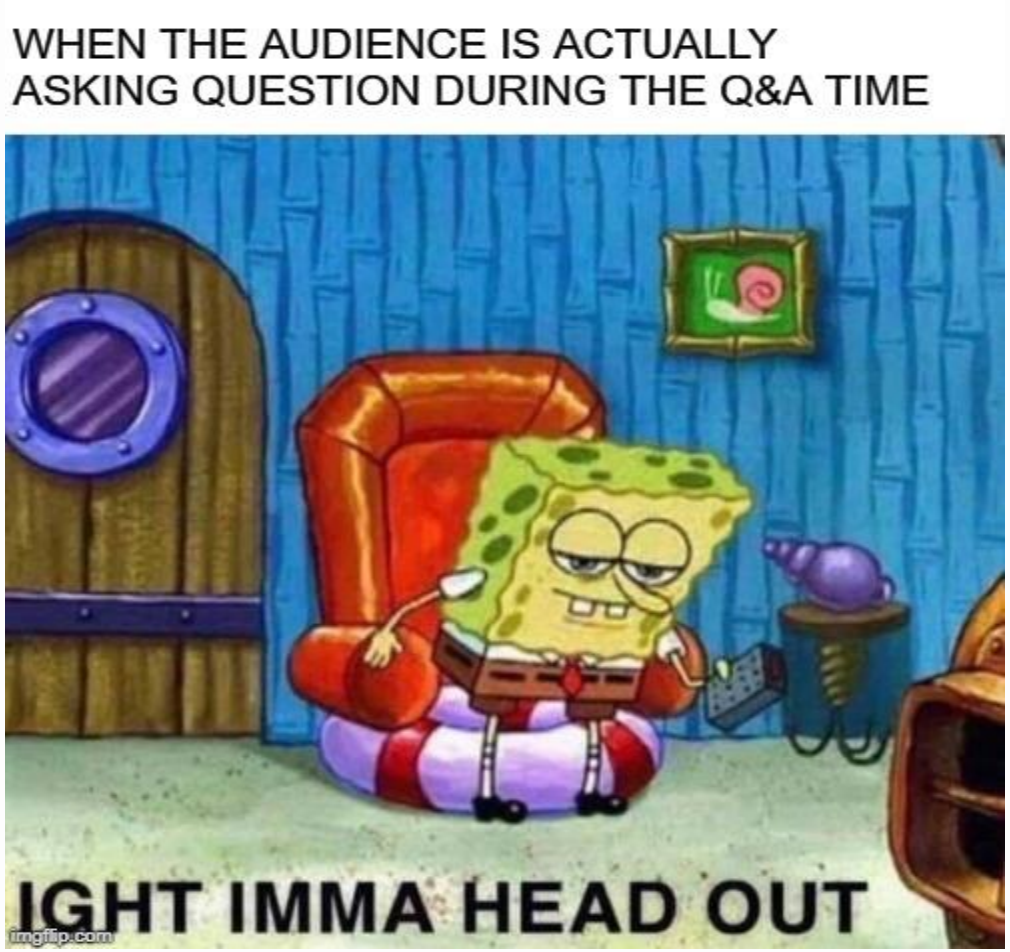
# Outro

**Recap and Q&A**

# Recap - LOLBAS

- A technique that abuse legitimate pre-installed binaries (or libraries and scripts) to perform unexpected activities that will benefit malicious actors
- Follow certain criteria and have certain file types
- Benefit of LOLBAS
  - Off the land
  - Multi function
  - Signed
  - Often whitelisted/ignored

# Question?




FAQ:

Q: Will the slide deck be available?
A: OF COURSE!

Q: Are you guys hiring co-op?
A: OF COURSE!

Q: Are you guys hiring new graduates?
A: OF COURSE!

Q: Can we buy you guys beer?
A: OF COURSE!

# Thank You!

**time to go home**

**(or Monaghan's)**


Mangatas Tondang (Tas)
twitter.com/tas_kmanager

Avneet Singh
twitter.com/13Avneet



Bell Threat Hunting Team
twitter.com/hunting_threat
medium.com/@threathuntingteam


# Reference

- Pyramid of Pain
  - http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- Operation Ghost (ESET)
  - https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/
- MuddyWater (FireEye)
  - https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html