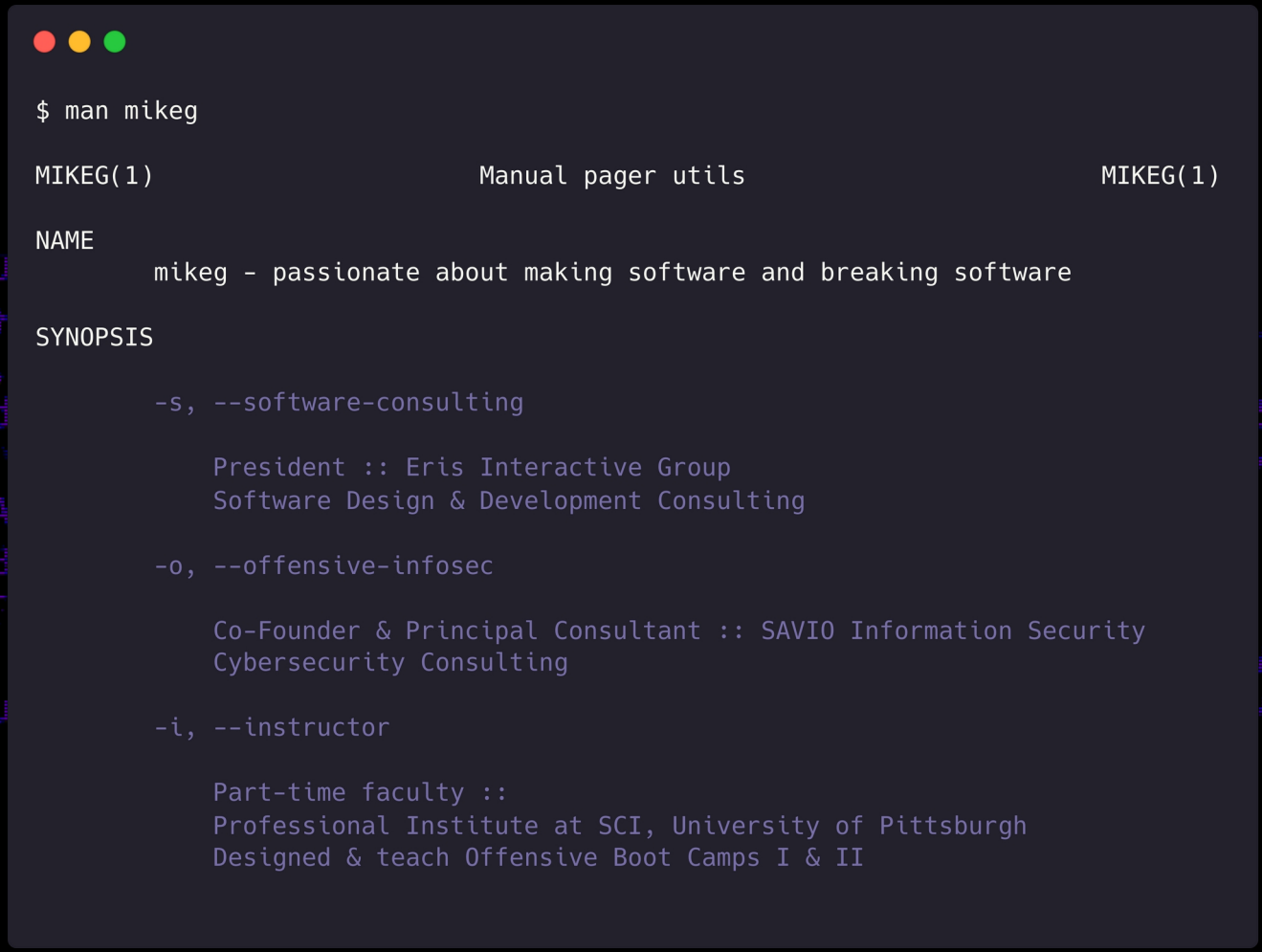

ASSUMED BREACH
WITH A
SIDE OF PHISH
[2020 Purple Team Summit]
[Mike Gualtieri]


$ man mikeg
MIKEG(1) Manual pager utils MIKEG(1)
NAME
mikeg - passionate about making software and breaking software
SYNOPSIS
-s, --software-consulting
President :: Eris Interactive Group
Software Design & Development Consulting
-o, --offensive-infosec
Co-Founder & Principal Consultant :: SAVIO Information Security
Cybersecurity Consulting
-i, --instructor
Part-time faculty ::
Professional Institute at SCI, University of Pittsburgh
Designed & teach Offensive Boot Camps I & II

The Assumed Breach Penetration Testing Advantage

```
> time--
  > cost--
    > value++
```

[2020 Purple Team Summit]

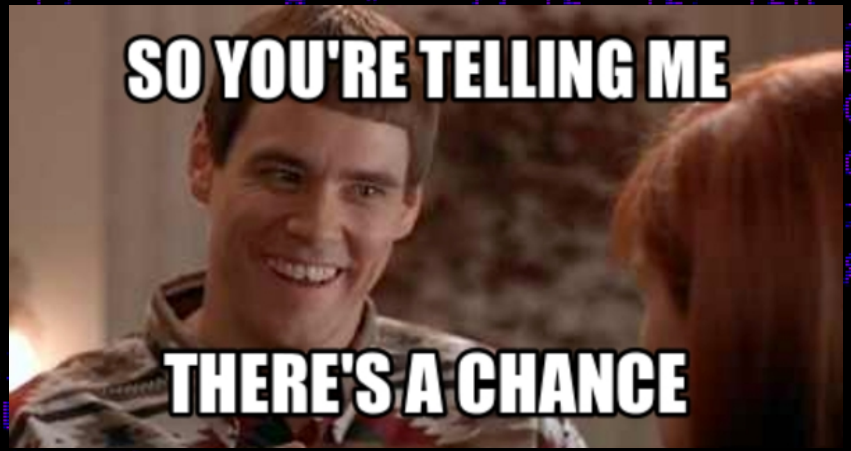
[Mike Gualtieri]

"But, we gave you access..."

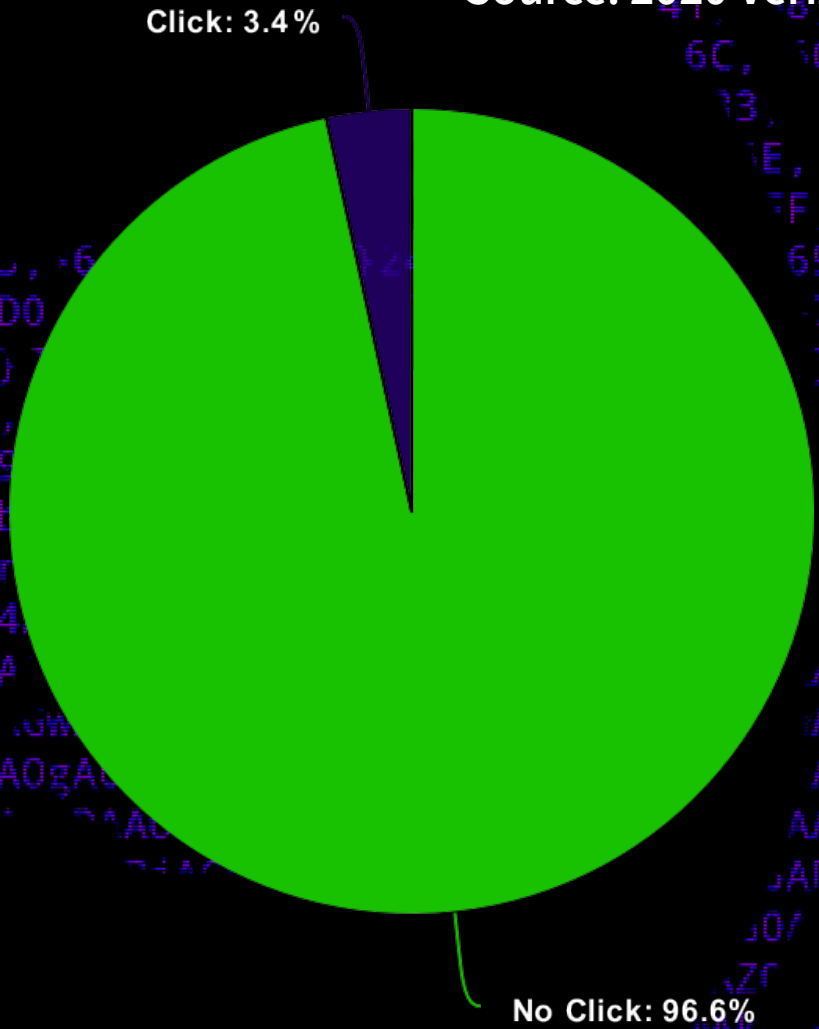
[2020 Purple Team Summit]

[Mike Gualtieri]

One click to Domain User



Source: 2020 Verizon DBIR

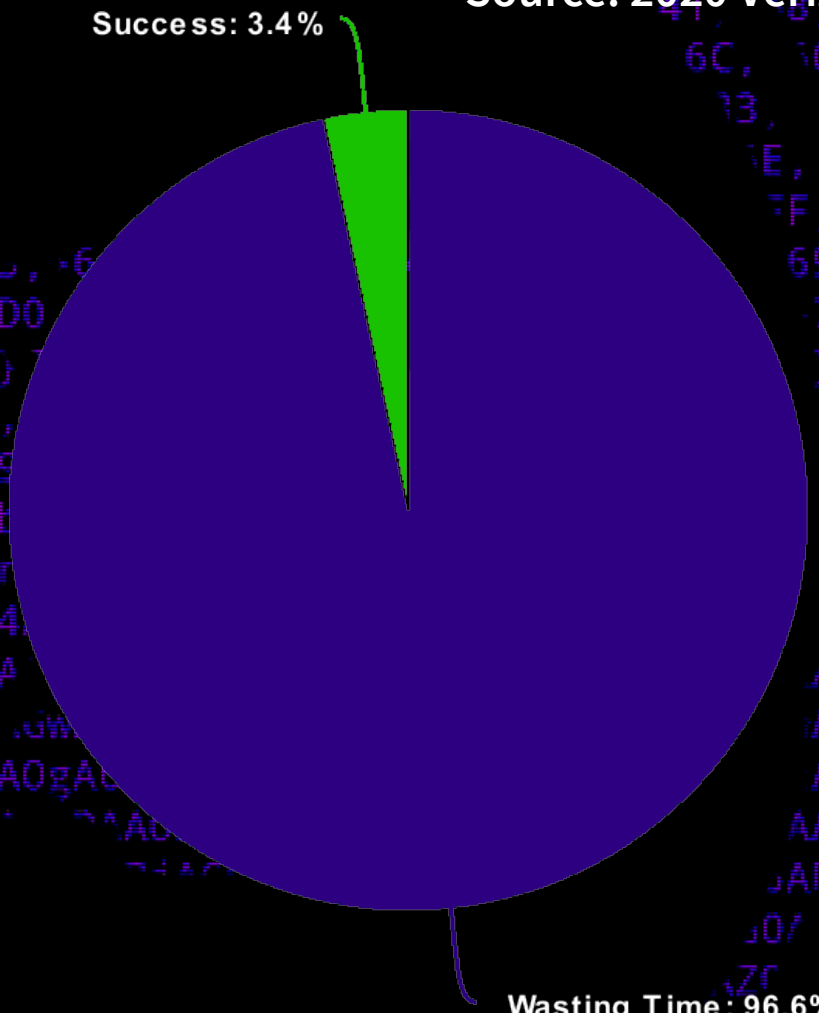


[2020 Purple Team Summit]

[Mike Gualtieri]

One click to Domain User

Source: 2020 Verizon DBIR



[2020 Purple Team Summit]

[Mike Gualtieri]

Closing the loop with phishing simulation

Goals:

> Situational Awareness

> Gather Credentials

> Setting up a C2 Channel

METHODOLOGY

> Use open source offensive tools (OST)
> Modify to bypass expected defenses
> Don't overthink things
> Customize it!

Situational Awareness

```
Net / cmd.exe
Wmic
Powershell / Upsh
C# / .NET API
C2 Modules
Key logger
Clipboard stealing
Disabling Antivirus
```

Gather Credentials

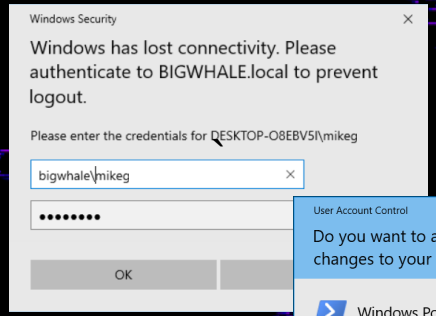
```
CredPhisher
Invoke-LoginPrompt
SharpLocker
```

C2 Channel

```
Empire
SILENTTRINITY
Meterpreter
C2 Matrix
  (pick your poison)
```

Example #1 – Empire Enum; Privesc; CredPhisher

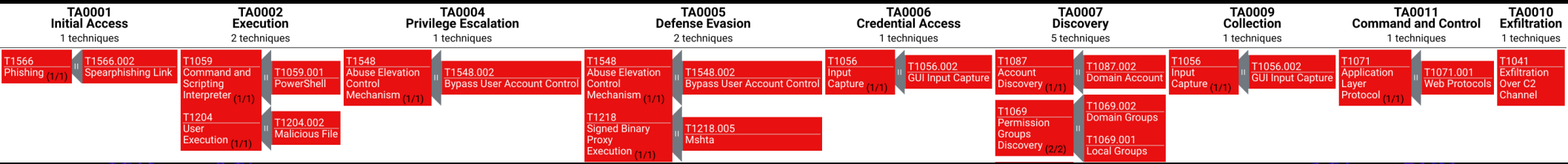
```
Execution plan:
1) Custom HTA dropper (MSHTA.exe)
2) Download Empire stage0 > C:\Users\Public
3) Execute stage0; Clean up dropped files
4) empire> execute 'net' enumeration
5) empire> bypassuac privesc/ask (custom)
6) empire> execute CredPhisher (custom)
```



MSHTA.exe

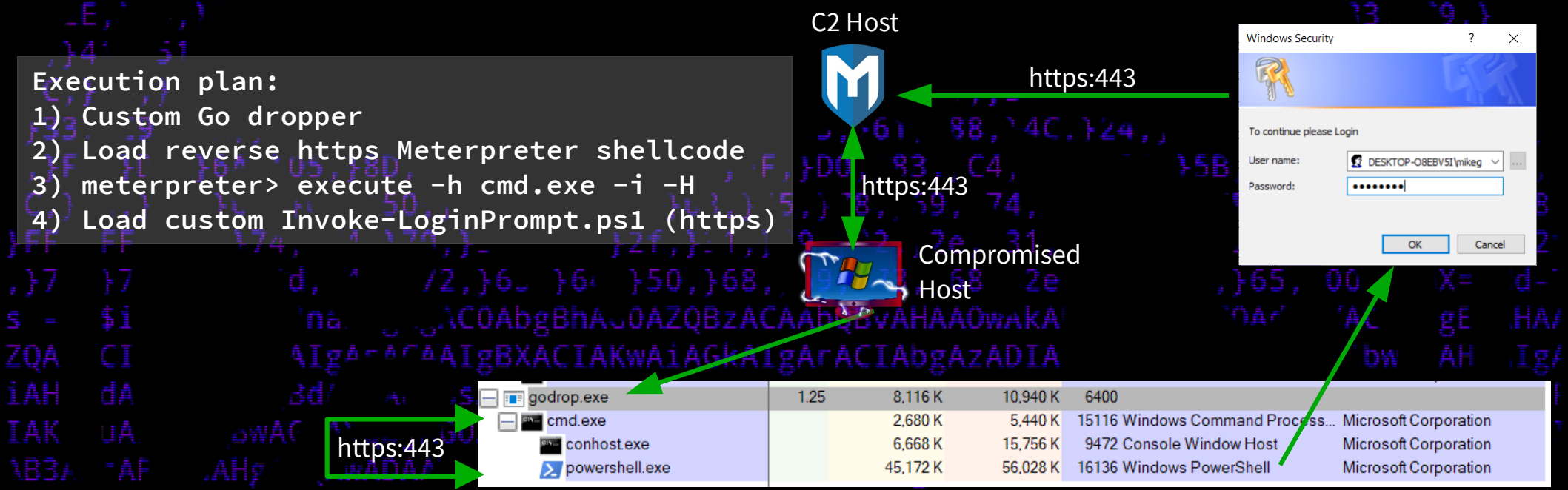
empire.ps1

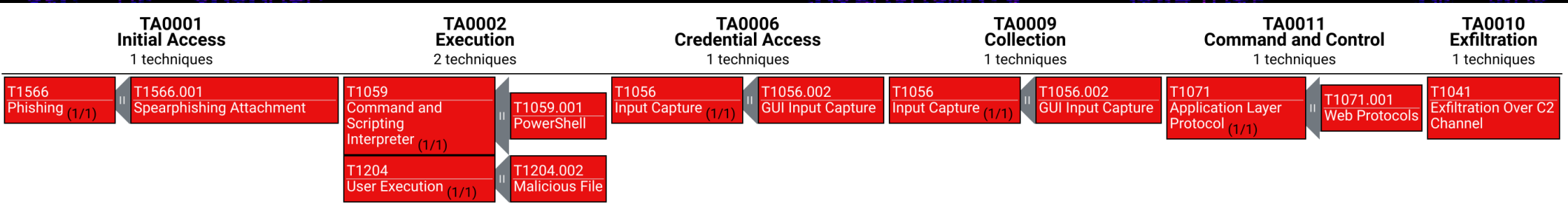
cmd.exe	2,676 K	5,056 K	12564 Windows Command Process...	Microsoft Corporation
conhost.exe	6,520 K	12,224 K	18884 Console Window Host	Microsoft Corporation
cmd.exe	2,580 K	5,240 K	2696 Windows Command Process...	Microsoft Corporation
powershell.exe	36,504 K	39,896 K	17492 Windows PowerShell	Microsoft Corporation
powershell.exe	51,616 K	63,936 K	16240 Windows PowerShell	Microsoft Corporation



Example #2 – Meterpreter Credential Theft

```
Execution plan:
1) Custom Go dropper
2) Load reverse https Meterpreter shellcode
3) meterpreter> execute -h cmd.exe -i -H
4) Load custom Invoke-LoginPrompt.ps1 (https)
```

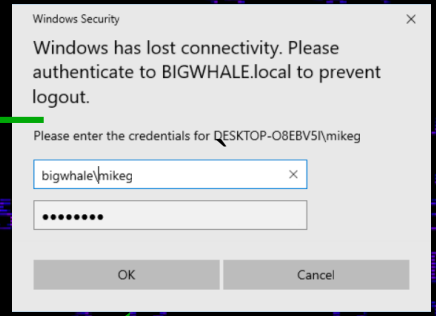




Example #3 – MSBuild, C#, .NET Assembly

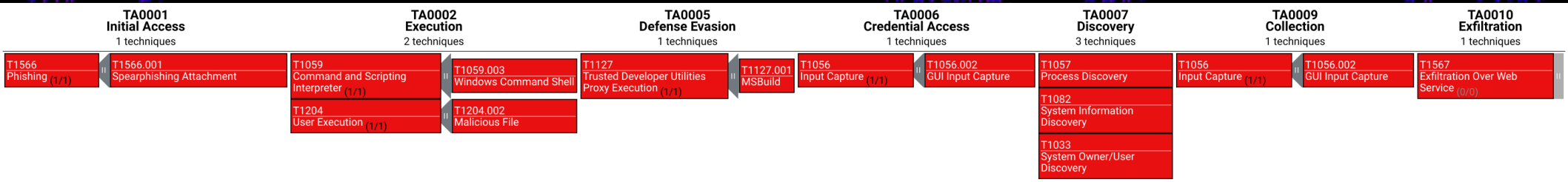
```
Execution plan:
1) Execution through MSBuild
2) C# .NET API enumeration
3) Custom CredPhisher loaded as assembly
```

https:443



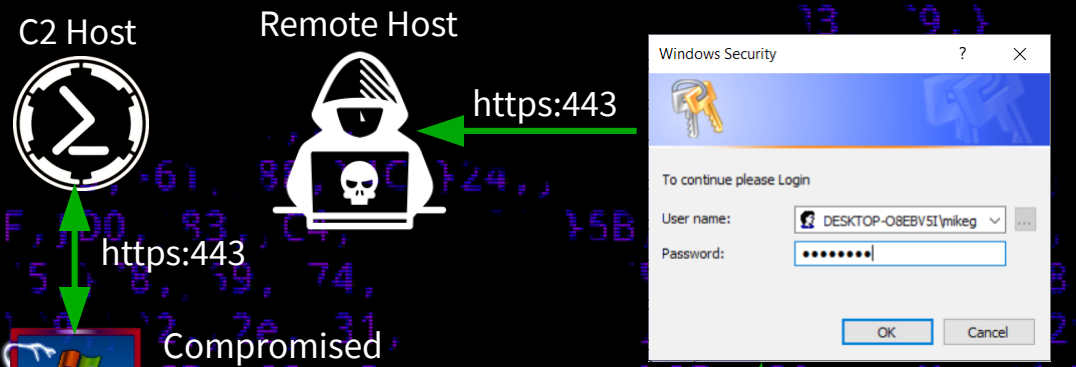
Any dropper or none!

cmd.exe	2,344 K	4,480 K	3728 Windows Command Process...	Microsoft Corporation
conhost.exe	7,428 K	22,264 K	18708 Console Window Host	Microsoft Corporation
MSBuild.exe	39,084 K	74,088 K	4076 MSBuild.exe	Microsoft Corporation

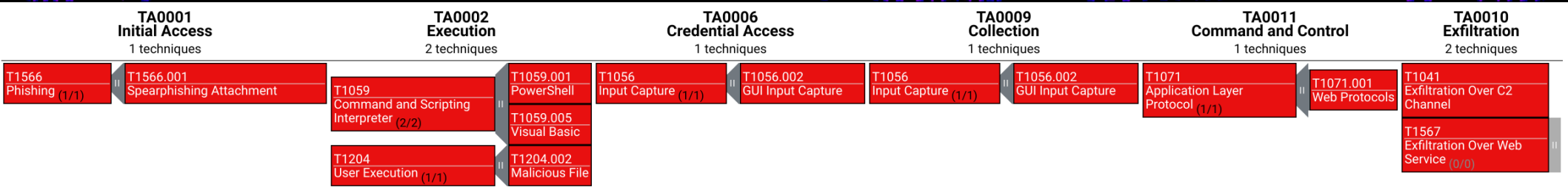


Example #4 – VBA Macro Maldoc

```
Execution plan:
1) Execution through VBA macro
2) Load custom Invoke-LoginPrompt (https)
3) Launch Empire agent
```



swriter.exe		748 K	3,756 K	12156 LibreOffice Writer	The Document Foundation
soffice.exe		1,180 K	5,272 K	13732 LibreOffice	The Document Foundation
soffice.bin	0.13	566,988 K	670,352 K	9756 LibreOffice	The Document Foundation
powershell.exe	0.01	61,328 K	106,824 K	5776 Windows PowerShell	Microsoft Corporation
conhost.exe		3,172 K	9,124 K	13564 Console Window Host	Microsoft Corporation
powershell.exe		50,836 K	55,952 K	12396 Windows PowerShell	Microsoft Corporation
conhost.exe	< 0.01	3,264 K	9,248 K	9136 Console Window Host	Microsoft Corporation
powershell.exe	0.13	99,000 K	113,452 K	1644 Windows PowerShell	Microsoft Corporation



QUESTIONS

github.com/mlgualtieri/PurpleTeamSummit2020

www.mike-gualtieri.com

@mlgualtieri