

ASSUMED BREACH

WITH A

SIDE OF PHISH



```
$ 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++

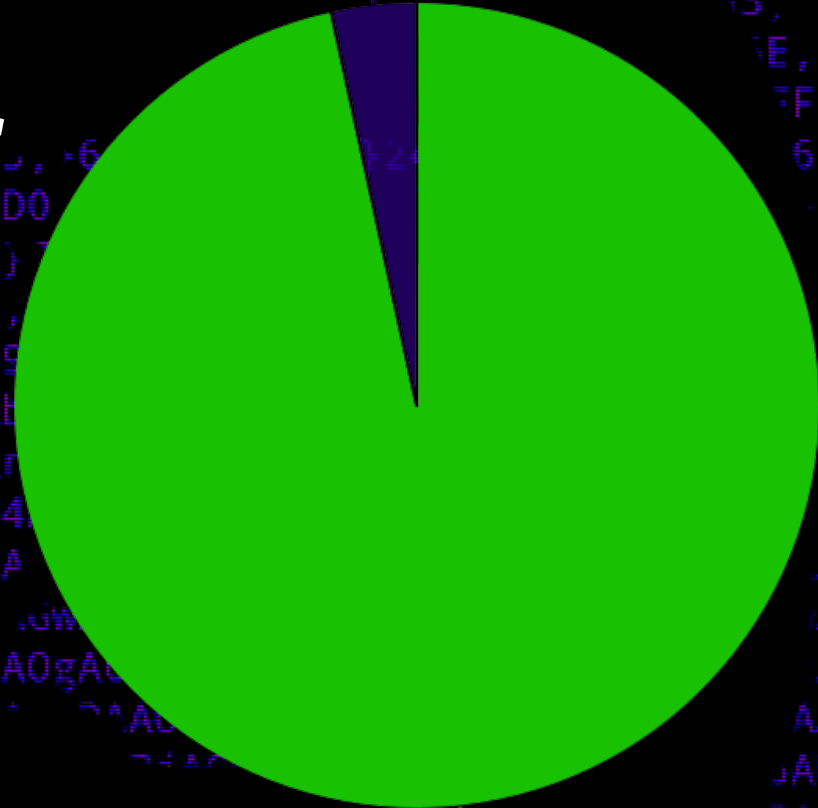
"But, we gave you access...!"



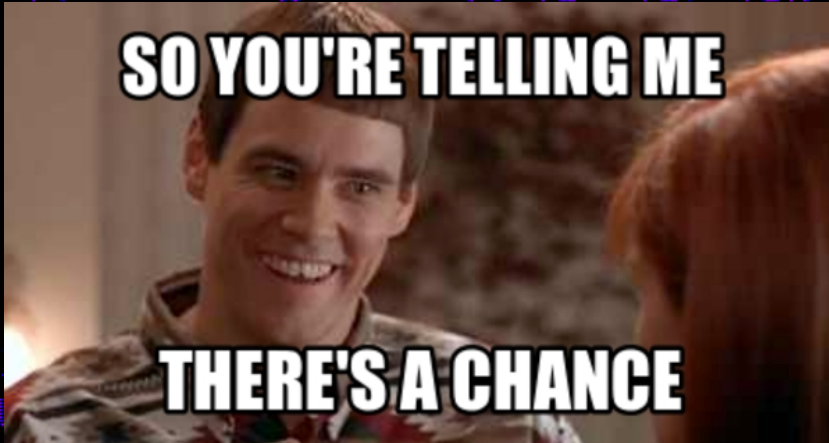
One click to Domain User

Source: 2020 Verizon DBIR

Click: 3.4 %



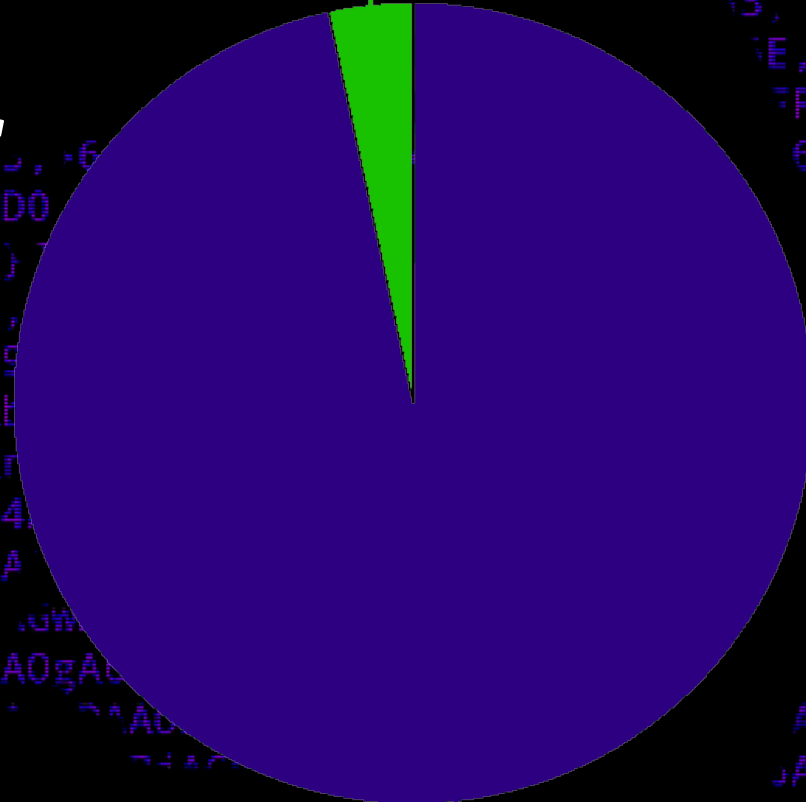
No Click: 96.6 %



One click to Domain User

Source: 2020 Verizon DBIR

Success: 3.4%



Wasting Time: 96.6%

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)

C2 Host



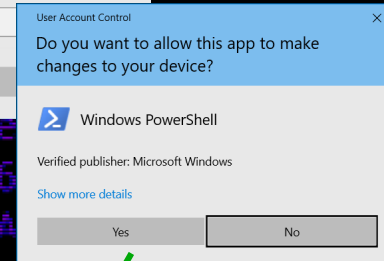
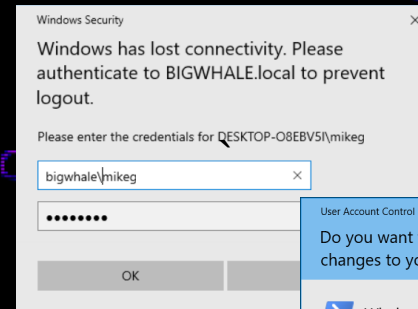
https:443

Compromised Host

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



TA0001 Initial Access 1 techniques		TA0002 Execution 2 techniques		TA0004 Privilege Escalation 1 techniques		TA0005 Defense Evasion 2 techniques		TA0006 Credential Access 1 techniques		TA0007 Discovery 5 techniques		TA0009 Collection 1 techniques		TA0011 Command and Control 1 techniques		TA0010 Exfiltration 1 techniques
T1566 Phishing (1/1)	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter (1/1)	T1059.001 PowerShell	T1548 Abuse Elevation Control Mechanism (1/1)	T1548.002 Bypass User Account Control	T1548 Abuse Elevation Control Mechanism (1/1)	T1548.002 Bypass User Account Control	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1087 Account Discovery (1/1)	T1087.002 Domain Account	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1071 Application Layer Protocol (1/1)	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel
		T1204 User Execution (1/1)	T1204.002 Malicious File			T1218 Signed Binary Proxy Execution (1/1)	T1218.005 Mshta			T1069 Permission Groups Discovery (2/2)	T1069.002 Domain Groups		T1069.001 Local Groups			

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)

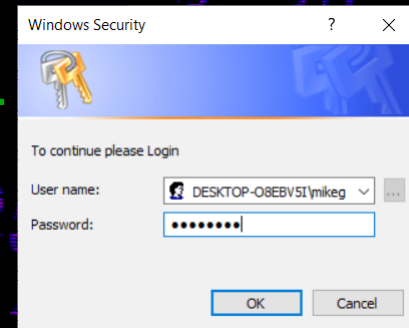
C2 Host



https:443

https:443

Compromised Host



godrop.exe	1.25	8,116 K	10,940 K	6400	
cmd.exe		2,680 K	5,440 K	15116	Windows Command Process...
conhost.exe		6,668 K	15,756 K	9472	Console Window Host
powershell.exe		45,172 K	56,028 K	16136	Windows PowerShell

https:443

TA0001
Initial Access
1 techniques

TA0002
Execution
2 techniques

TA0006
Credential Access
1 techniques

TA0009
Collection
1 techniques

TA0011
Command and Control
1 techniques

TA0010
Exfiltration
1 techniques

T1566 Phishing (1/1)	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter (1/1)	T1059.001 PowerShell	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1071 Application Layer Protocol (1/1)	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel
		T1204 User Execution (1/1)	T1204.002 Malicious File							

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

Execution plan:

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

Remote Host

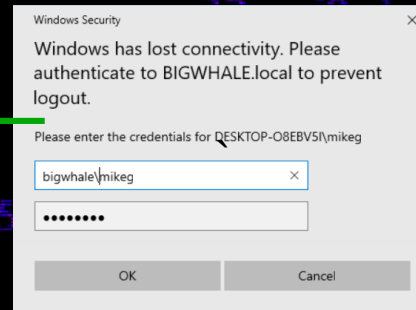


https:443

Compromised Host

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



TA0001
Initial Access
1 techniques

TA0002
Execution
2 techniques

TA0005
Defense Evasion
1 techniques

TA0006
Credential Access
1 techniques

TA0007
Discovery
3 techniques

TA0009
Collection
1 techniques

TA0010
Exfiltration
1 techniques

T1566 Phishing (1/1)	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter (1/1)	T1059.003 Windows Command Shell	T1127 Trusted Developer Utilities Proxy Execution (1/1)	T1127.001 MSBuild	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1057 Process Discovery	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1567 Exfiltration Over Web Service (0/0)
		T1204 User Execution (1/1)	T1204.002 Malicious File					T1082 System Information Discovery			
								T1033 System Owner/User Discovery			

Example #4 – VBA Macro Maldoc

Execution plan:

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

C2 Host



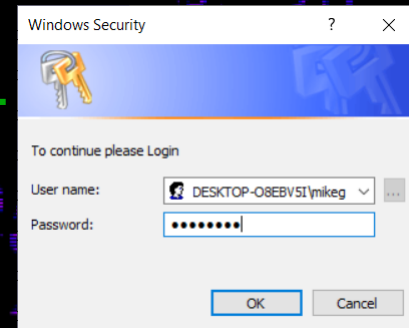
Remote Host



https:443

https:443

Compromised Host



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

TA0001
Initial Access
1 techniques

TA0002
Execution
2 techniques

TA0006
Credential Access
1 techniques

TA0009
Collection
1 techniques

TA0011
Command and Control
1 techniques

TA0010
Exfiltration
2 techniques

T1566 Phishing (1/1)	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter (2/2)	T1059.001 PowerShell	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1056 Input Capture (1/1)	T1056.002 GUI Input Capture	T1071 Application Layer Protocol (1/1)	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel
		T1204 User Execution (1/1)	T1204.002 Malicious File							T1567 Exfiltration Over Web Service (0/0)

QUESTIONS

github.com/mlgualtieri/PurpleTeamSummit2020

www.mike-gualtieri.com

@mlgualtieri

