Defense Evasion with Invoke-Obfuscation

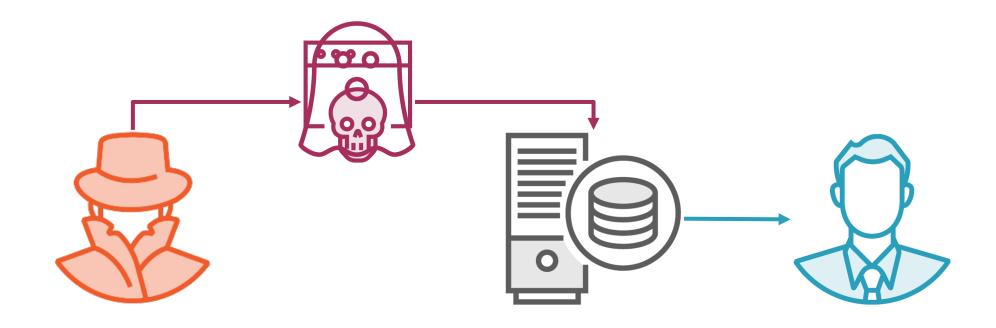


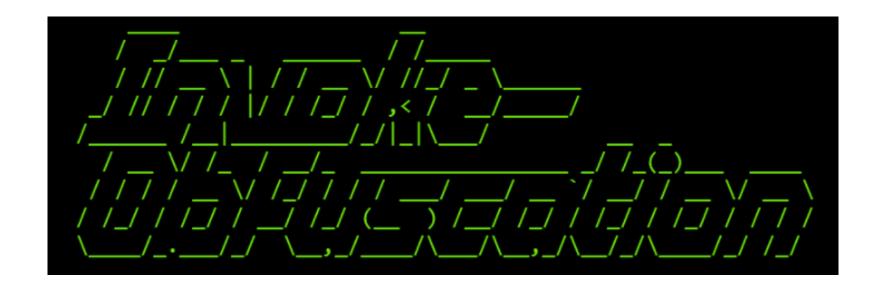
Ricardo Reimao

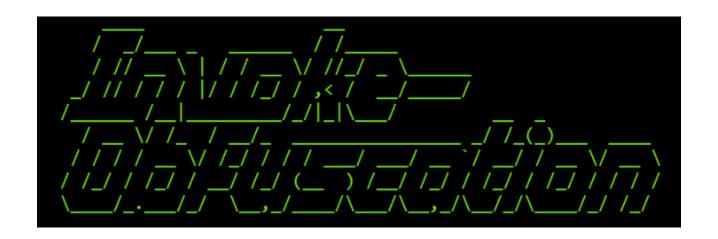
CYBER SECURITY CONSULTANT



Why Avoid Detection?







Author: Daniel Bohannon https://www.danielbohannon.com/

A PowerShell v2.0+ compatible PowerShell command and script obfuscator



Open source under Apache 2.0 License https://github.com/danielbohannon/ Invoke-Obfuscation

Supports PowerShell scripts

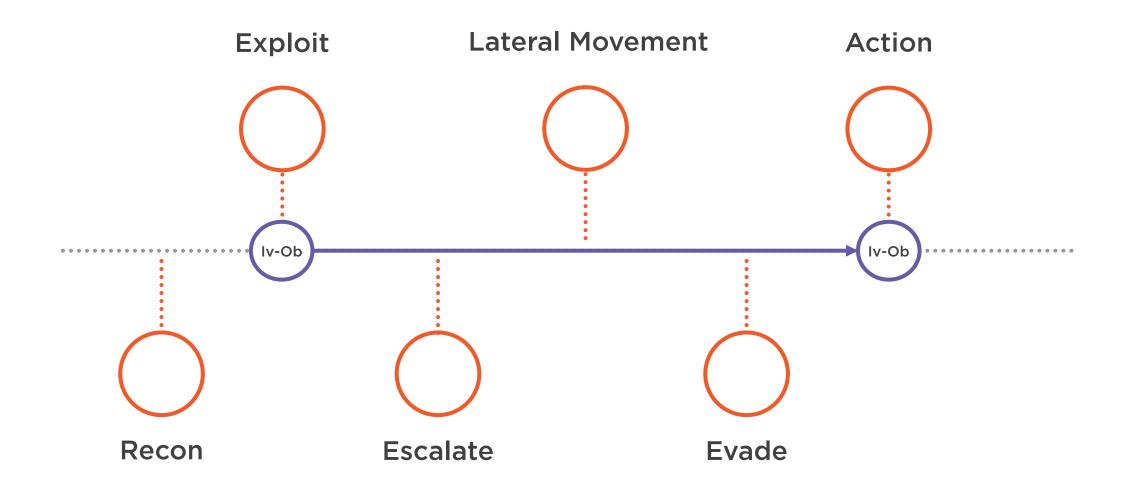
5 obfuscation methods, total of more than 20 different techniques

Runs on Windows or Linux

Easy to use and good documentation



Kill Chain





MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact



MITRE ATT&CK

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion <

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1027:

Obfuscated Files or Information

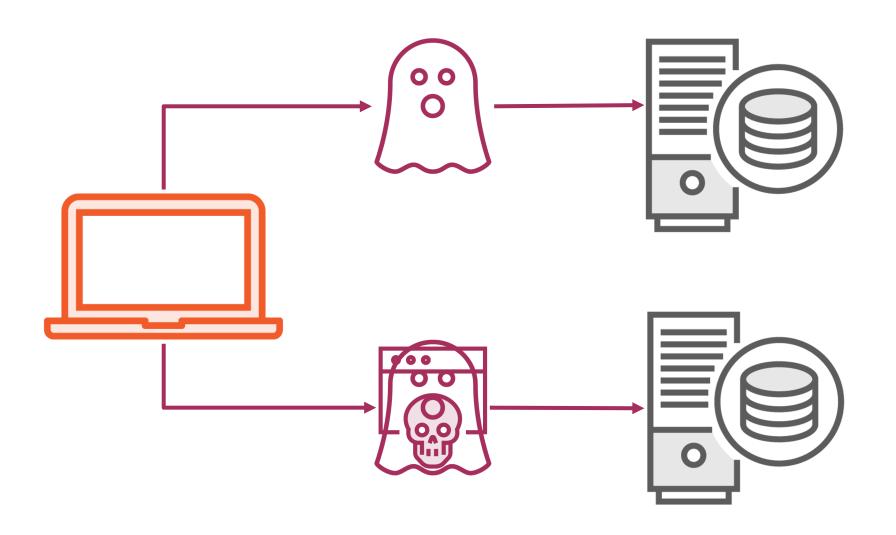
T1140:

Deobfuscate/Decode Files or Information

Tactics



Attack Explanation



Obfuscation Techniques

```
function scan ($ip, $port){
StringmapavArhamsetyspopserver";
$tring bbbver ##93e ##6021108;1.2";
$uningopoptint4944368$a,$B){
     print "IP:" + $a;
pmaptpANAME$BemEsaaasbe is:" + $servername
print "Your setbbb IP is:" + $serverIP
print "IP:" + $bbb
SmainngANdeME$pode4$aaprverIP
String aaa = "myserver";
ptrintg"bobb=comple160!1.2";
pcant$bb0N$ccc);
print info($bbb,$aaa);
print "DON3!";
```

Lab Environment



Kali Linux Version 2020.1 or superior

Alternative: Windows or any other Linux



Windows Server 2016 Windows Defender Anti-Virus

Alternative:
Any Windows/Anti-virus



Demo Place Holder

- 1. Installation Tips and Tricks
- 2. First use instructions and common usage syntax
- 3. Use of main features on live targets or in live environment



How to Increase Your Chances of Success

Write your own tools

Understand all detection mechanisms

- Anti-virus
- Host IPS/IDS
- Network detection tools
- SIEM

Replicate all detection mechanisms in your lab



Analyze logs from Windows and detection tools

Use minimum required obfuscation



More Information

Official documentation

Official GitHub

https://github.com/danielbohannon/ Invoke-Obfuscation

Daniel's talk on the tool

Hacktivity Conference, 2016 https://www.youtube.com/ watch?v=uE8IAxM_BhE

How to deobfuscate

Same author, deobfuscation tool: https://github.com/danielbohannon/
Revoke-Obfuscation

How to protect yourself

Behavior-based technologies

BlackHat, 2017 - Obfuscation detection https://www.youtube.com/ watch?v=x97ejtv56xw



Thank you!



Ricardo Reimao Cyber security consultant

