Getting Started with Cyber Deception

Black Hills Information Security
@BHInfoSecurity

Wanna see something cool?

- We are starting a Cyber Range…
- Kind of backwards training
- Free for all BHIS customers in 2020
- We need some people to test it
- 30 days free access
- Type in Range!!!! In question window

MetaCTF | About | Problems | Scoreboard | Account

Cryptography | Reconnaissance | Web Exploitation | Reverse Engineering | Threat Hunting | Forensics | Penetration Testing | Other

Bonus | Resources | Help

A Revealing Lunch (solved by 0 teams) — 130

Your friend Ava Sharov is very active on social media and regularly posts photos on Instagram, even tagging them at whatever cool place she is at. You think that it might be dangerous to always be sharing her location like that publicly. Figure out what restaurant she had lunch at with her friend Sean.

? [ ] Submit!

Please rate this problem: ☆☆☆☆☆

¯_(ツ)_/¯ (solved by 0 teams) — 150

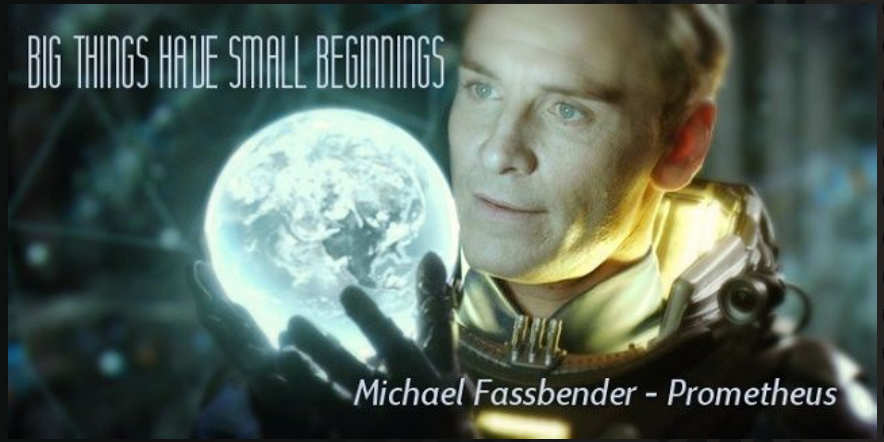
Plaintext: Lorem ipsum has et perpetua expetendis, explicari similique mnesarchum ei sed. Ius id tale persius assueverit. Sed vide autem erant te, justo fabellas an sit, et per sonet decore. Cum ad doctus placerat, sed at elit sensibus.

Adhuc animal adversarium sed ei. Ea vel partem noluisse interpretaris, ei iudico oratio temporibus per. Commodo eloquentiam vis eu, ne fierent dissentiet pri. Idque dolorum efficiendi eum ad, ut wisi nemore urbanitas eos. Eu eam inermis vituperatoribus possim, in vis graeci invidunt apeirian.

Ciphertext: Nwglq zhslq muf gb elvgwtle jrcgbtuhzk, eotqcpczx zmdalzuzy zpmhhvtzud in mrf. Qjz mu laci uyeuqjz ejkuvzjlvv. Atk zzve ryyyz gzpux kw, jlwyi scjtsprk ae wnn, rv xty wffek hjwbtm. Rbq rv dfgyof rtpjiist, jii ug gtxa wvfszfzm.

Beginnings

- Getting any sort of budget for new technologies can be very hard
- Let's talk about the beginning
- So how do new things come about?
  - IDS, Firewalls, Scanning, etc.
- All forward movement comes from proof
- Cyber deception needs proof.



BLACK HILLS Information Security • 2008 •

Black Hills Information Security
@BHInfoSecurity

Conversation

briankrebs @briankrebs · Feb 25

#3 deception technologies are nice, but advisable only if your organization is already doing 99% of the rest of the basic security stuff. As it happens, a lot of the really cool tech being advertised at RSA is for a very exclusive audience.

4 14 96

One interesting omission, Moss said, was the apparent lack of use of deception technology. "I never heard one speaker say: 'And then I checked the canary or, and then I [reviewed] the deception tech," he said. "Who here uses deception technology?"

Let's Change that

Jeff Moss introduces the locknote panel.

While the keynote speech opens the briefings, Black Hat closes with a "locknote," led by Moss, who's joined by members of the Black Hat Review Board. Together with Antonios Atlasis of the European Space Agency, Daniel Cuthbert of Banco Santander, and Veronica Valero of Cisco Systems, Moss touched on a variety of topics, including some trends the review board sees, based on its reviews of more than 1,000 submissions every year.

One interesting omission, Moss said, was the apparent lack of use of deception technology. "I never heard one speaker say: 'And then I checked the canary or, and then I [reviewed] the deception tech," he said. "Who here uses deception technology?"

Just one hand among the hundreds of locknote attendees appeared to get raised.

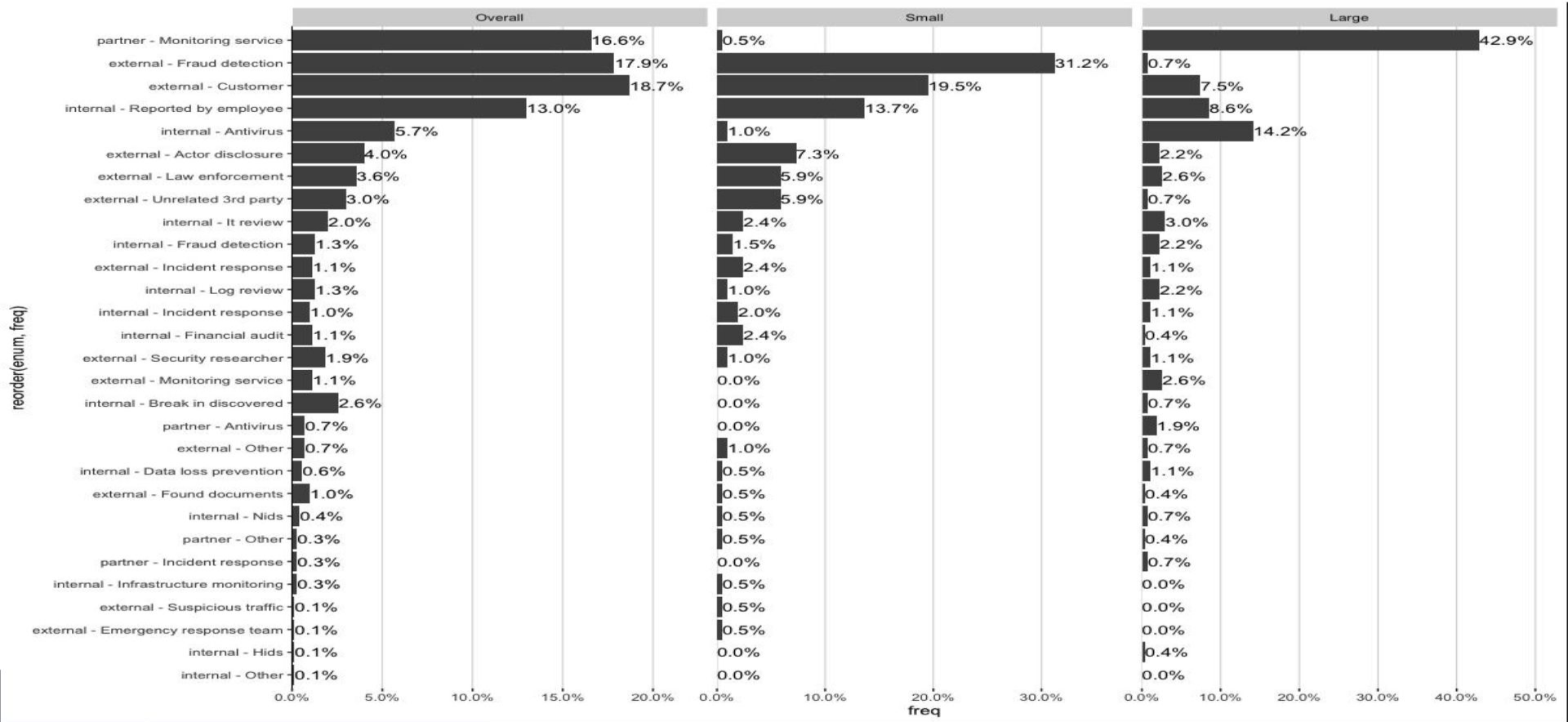
"Who here runs canaries?" he asked, referring to a honeypot designed to detect network intruders. Four hands were raised.

Perhaps the first rule of using deception technology is to never talk about deception technology?

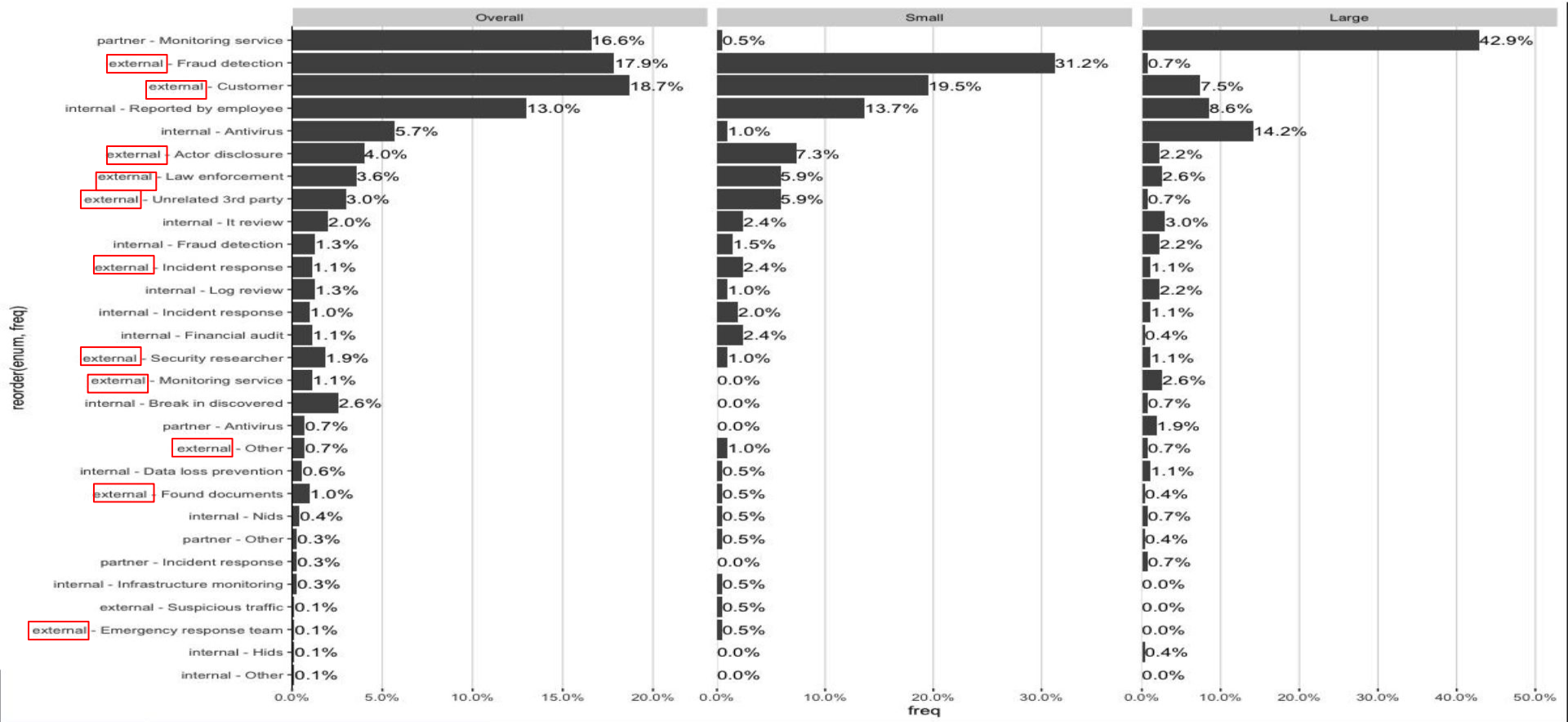
Cuthbert, however, said deception technology poses many problems. "As an ex-attacker, if you breach the network, you go for the juicy network," he said.

In addition, from an administration standpoint, "the moment you throw deception tech on there, you've now got four networks," he said. "It's an overhead nightmare."

Krebs... We Need To Talk.



Krebs... We Need To Talk.



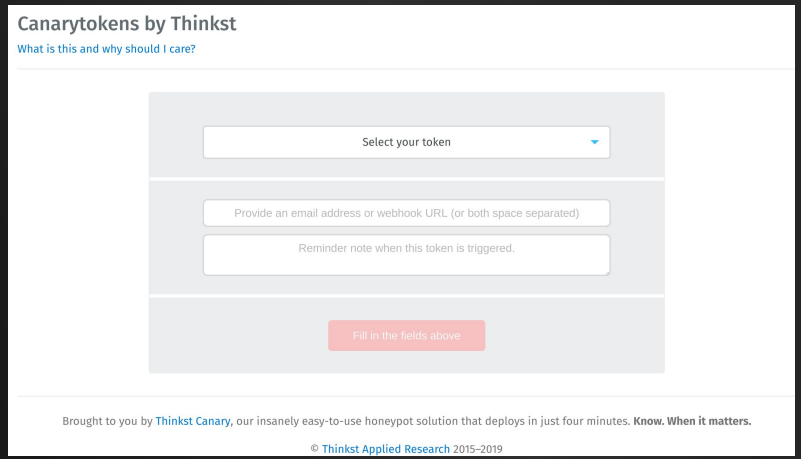
Why?

- Another useless rant on Threat Intelligence Feeds
- But there is value in understanding attackers
- How about attackers that are attacking you right now?
- What if we (as an industry) got better tracking attackers?
- Broken Windows

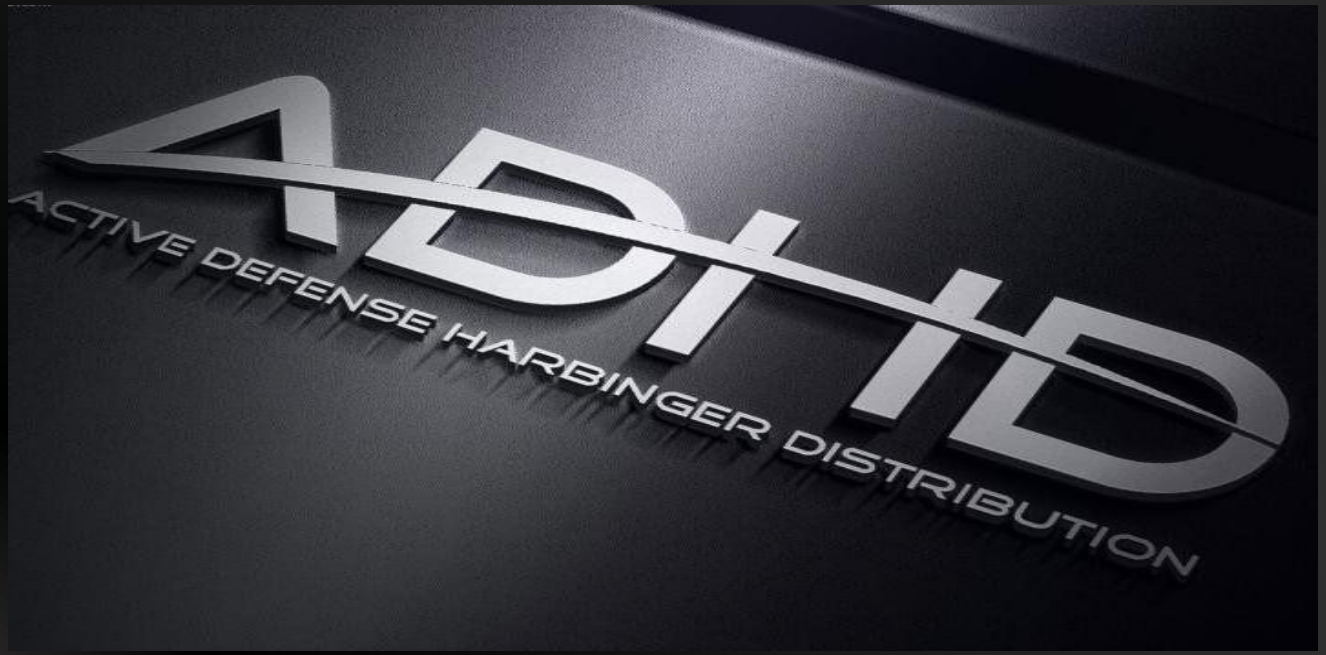
Getting Started

Canarytokens

- A lot of this is going to be straight from canarytokens.org
- We will be bringing in ADHD
  - Because it has canarytokens installed on it
- We will also be covering other ways to do many of the same things
- Getting past some shortcomings



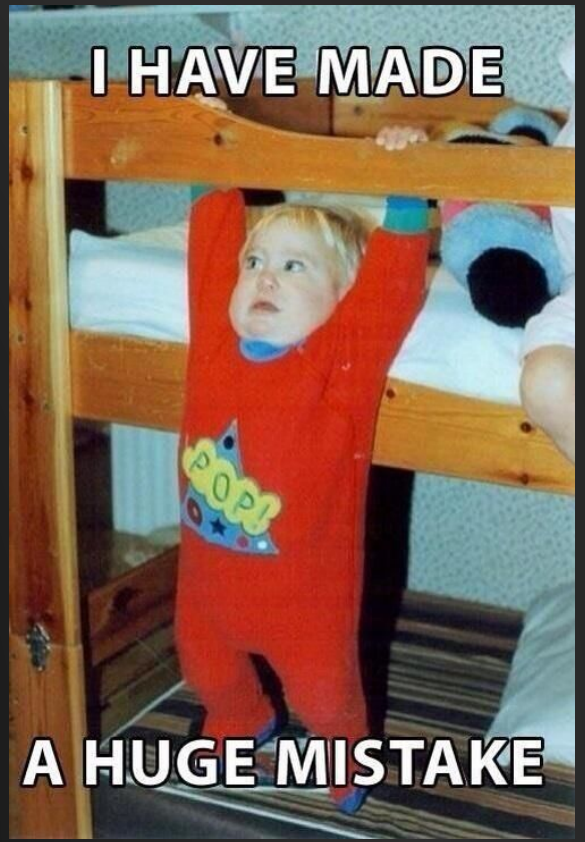
ADHD



https://www.blackhillsinfosec.com/projects/adhd/

Scenario: Recon

- Let's go through the attack phases and cover how we can disrupt an attacker attempting recon on an environment
- All attack methodologies are based on information gathered during this phase
- It is possible to trick an attacker at this phase



AWS Keys

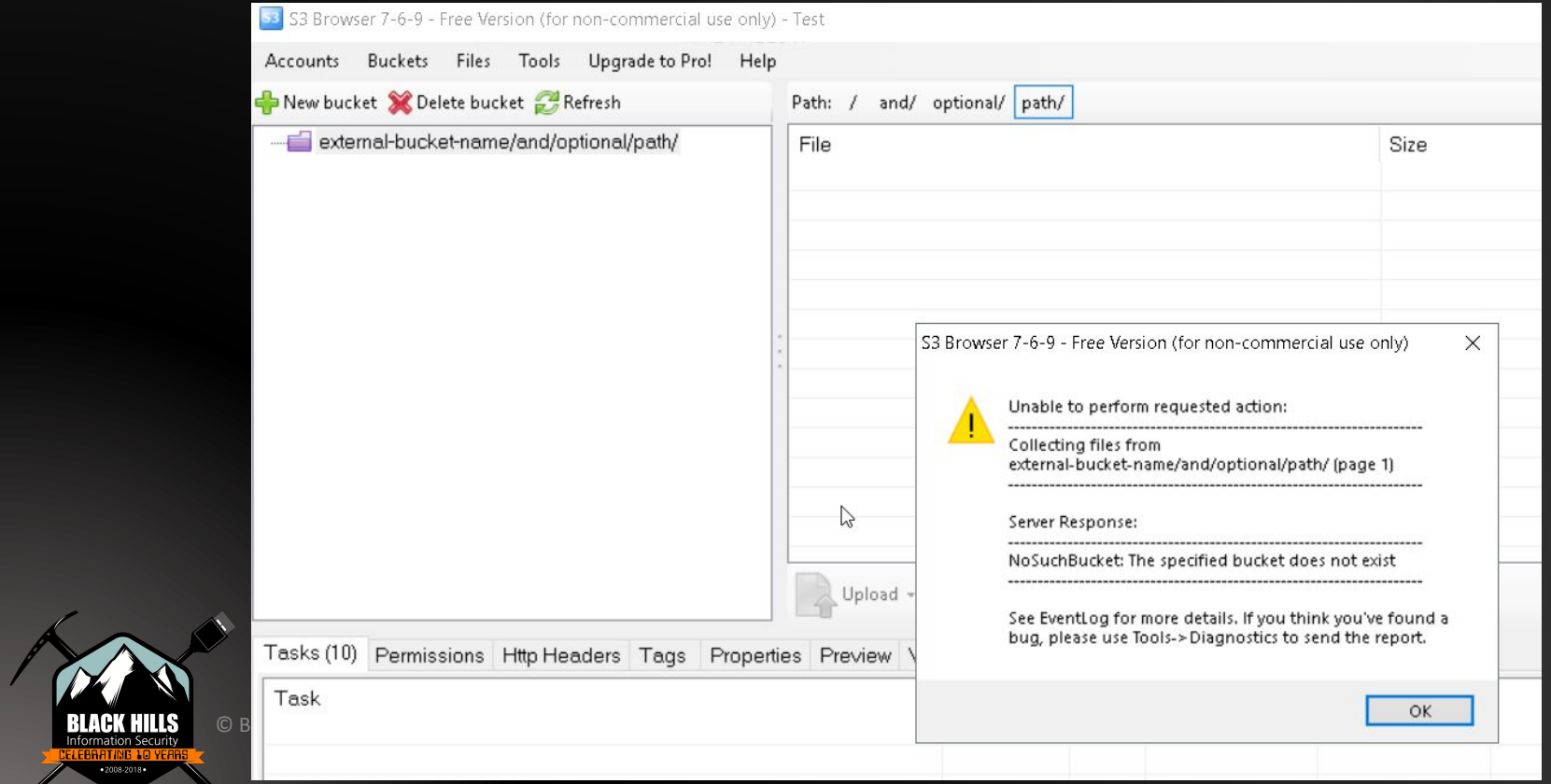
Your AWS key token is active!

Copy this credential pair to your clipboard to use as desired:

```
[default]
aws_access_key_id = AKIAJRN2YPG2JK7EC7YA
aws_secret_access_key = F6W3nzTodbbFf1o66OV31UjQhn2Rz/4+xI+Qckcz
output = json
region = us-east-2
```

Download your AWS Creds

Trigger


S3 Browser 7-6-9 - Free Version (for non-commercial use only) - Test
Accounts
Buckets
Files
Tools
Upgrade to Pro!
Help
New bucket
Delete bucket
Refresh
external-bucket-name/and/optional/path/
Path: / and/ optional/ path/
File
Size
Upload
Tasks (10)
Permissions
Http Headers
Tags
Properties
Preview
Task
S3 Browser 7-6-9 - Free Version (for non-commercial use only)
Unable to perform requested action:
Collecting files from external-bucket-name/and/optional/path/ (page 1)
Server Response:
NoSuchBucket: The specified bucket does not exist
See EventLog for more details. If you think you've found a bug, please use Tools->Diagnostics to send the report.
OK

Alert

Canarytoken triggered

ALERT

An AWS API Key Token Canarytoken has been triggered by the Source IP 107.77.195.231.

Basic Details:

Channel	AWS API Key Token
Time	2019-09-05 18:17:08
Canarytoken	fi4tamoii5h2muzdh0ix4uv5n
Token Reminder	sdsdsd
Token Type	aws_keys
Source IP	107.77.195.231
User Agent	S3 Browser 8-4-1 https://s3browser.com

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

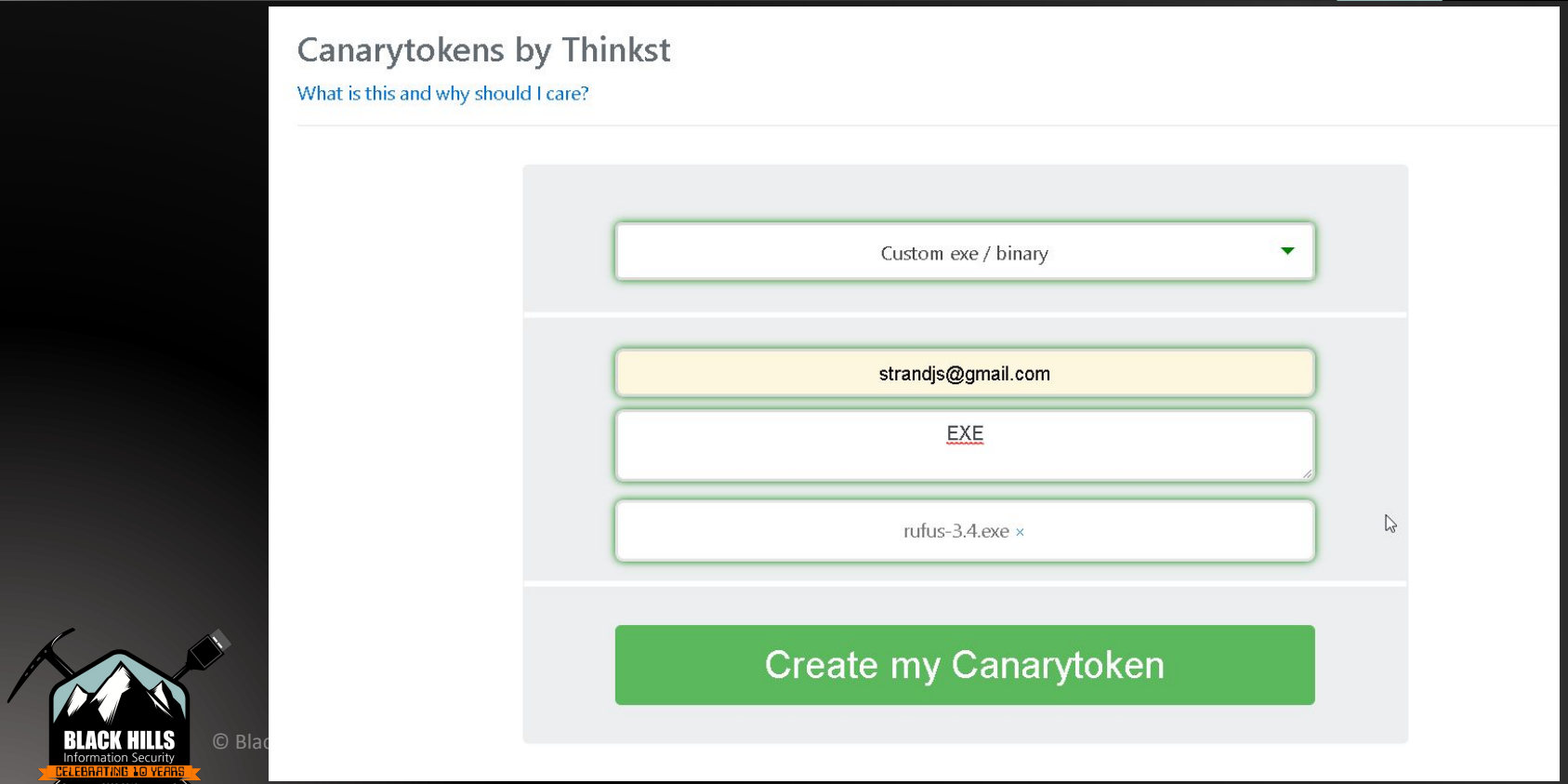
Context

- Attackers love looking into Github for exposed AWS keys
- So do security researchers

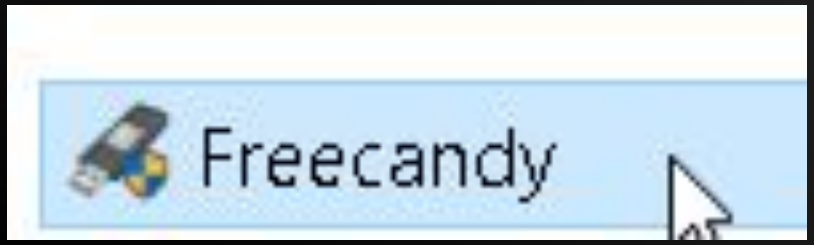
.exe

- How would we ever get an attacker to run a .exe?
- Easy
- vpnconfig.exe
- Sysprep.exe
- Oh.. So many ways

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

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:

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
```

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
```

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.

Trigger

ALERT

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

Basic Details:

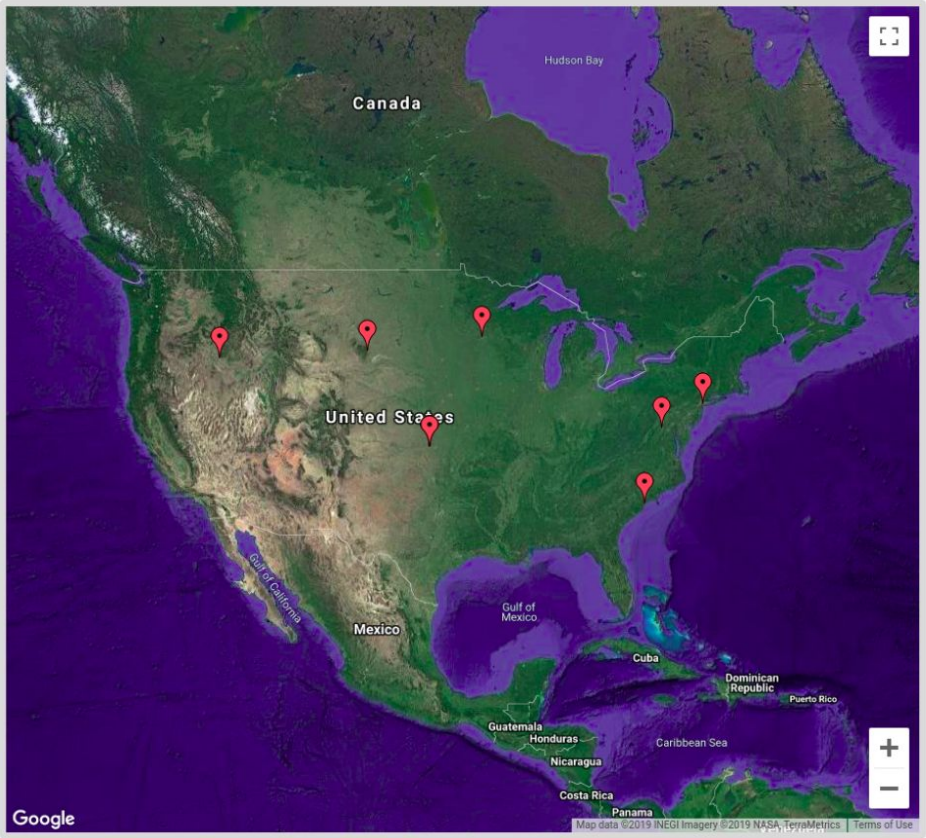
Channel	HTTP
Time	2019-08-13 13:16:13
Canarytoken	y7[redacted]22no
Token Reminder	Cloned website token for: [redacted].blackhillsinfosec.com
Token Type	clonedsite
Source IP	[redacted]
User Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 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

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

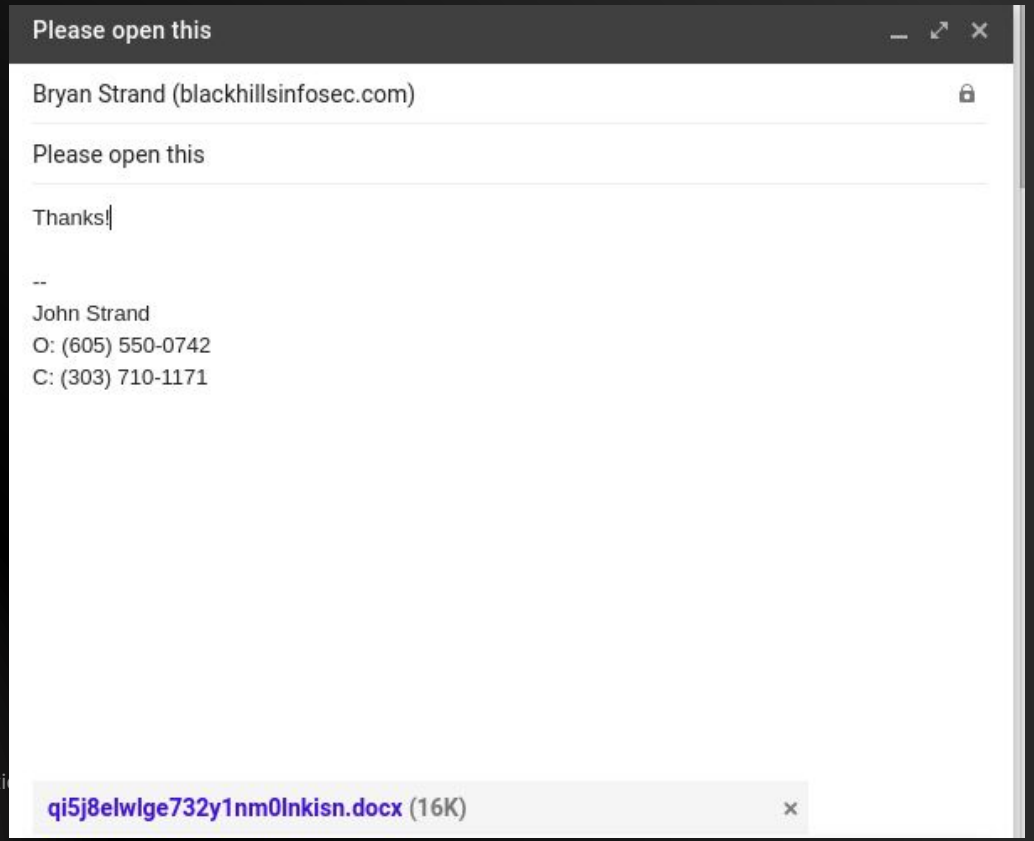
Date: 2019 Aug 13 17:44:54 **IP:** **annel:** HTTP

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!

Family...



Yes! CanaryTokens!

Canarytoken triggered

ALERT

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

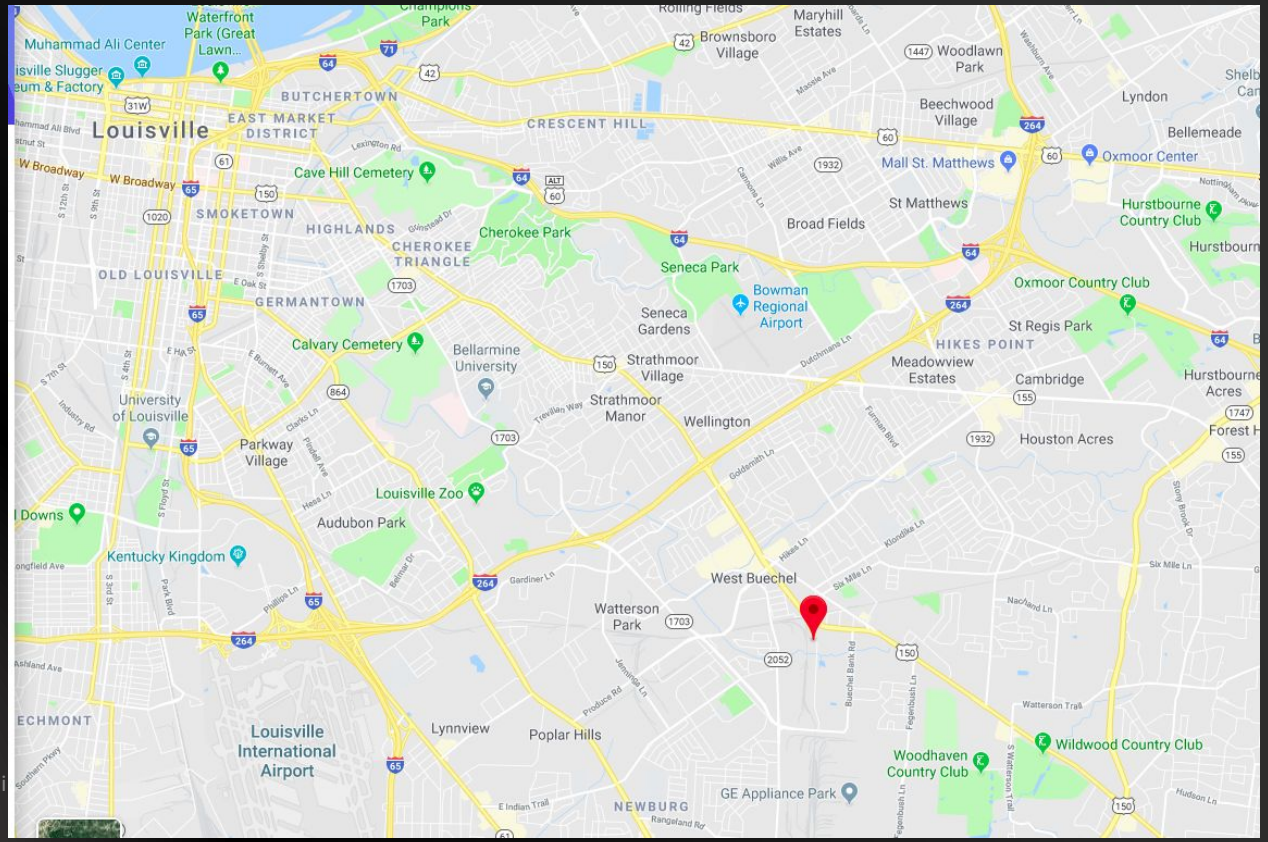
Basic Details:

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

Not bad..

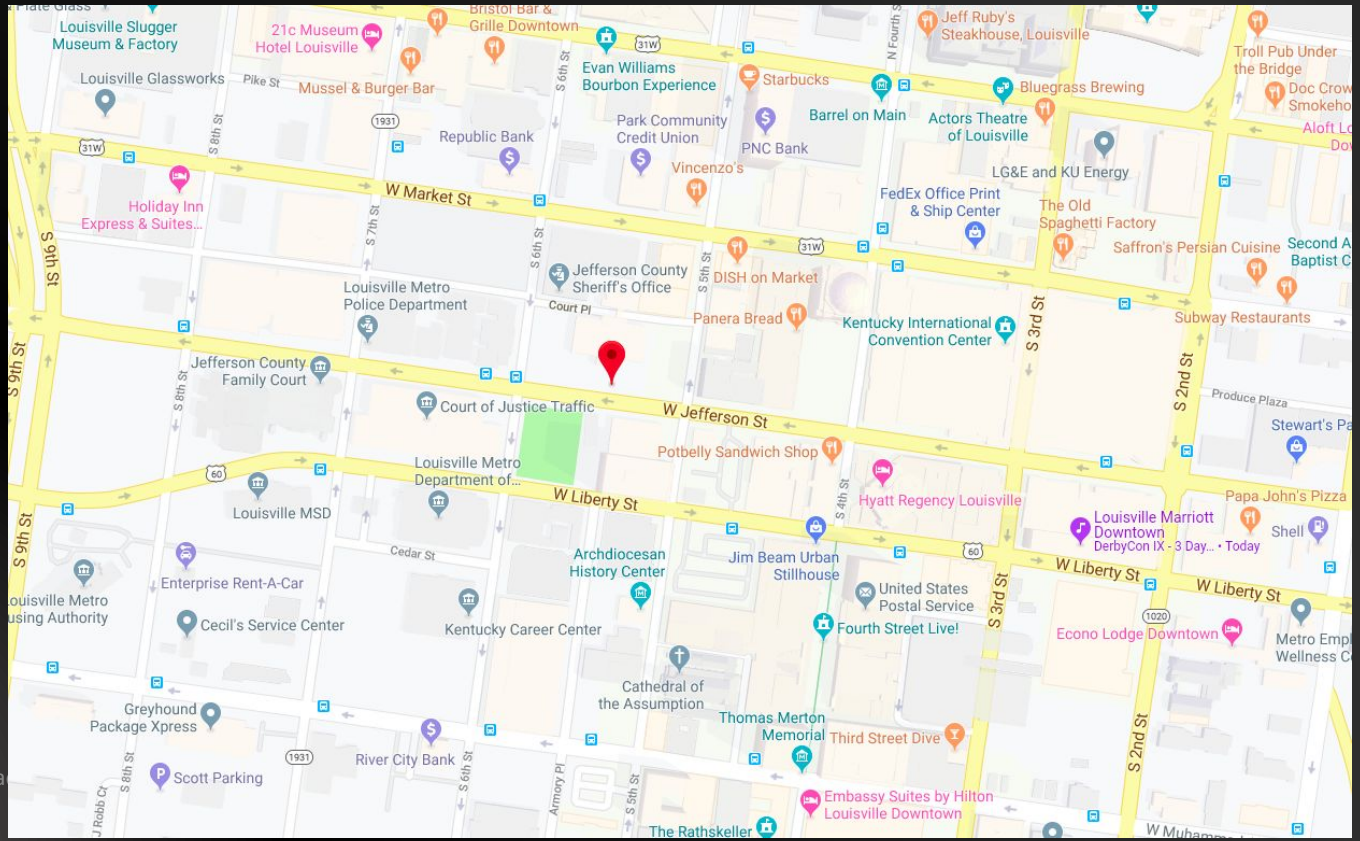


But we can do better...

```
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
```


BLACK HILLS Information Security
CELEBRATING 10 YEARS
•2008-2018•

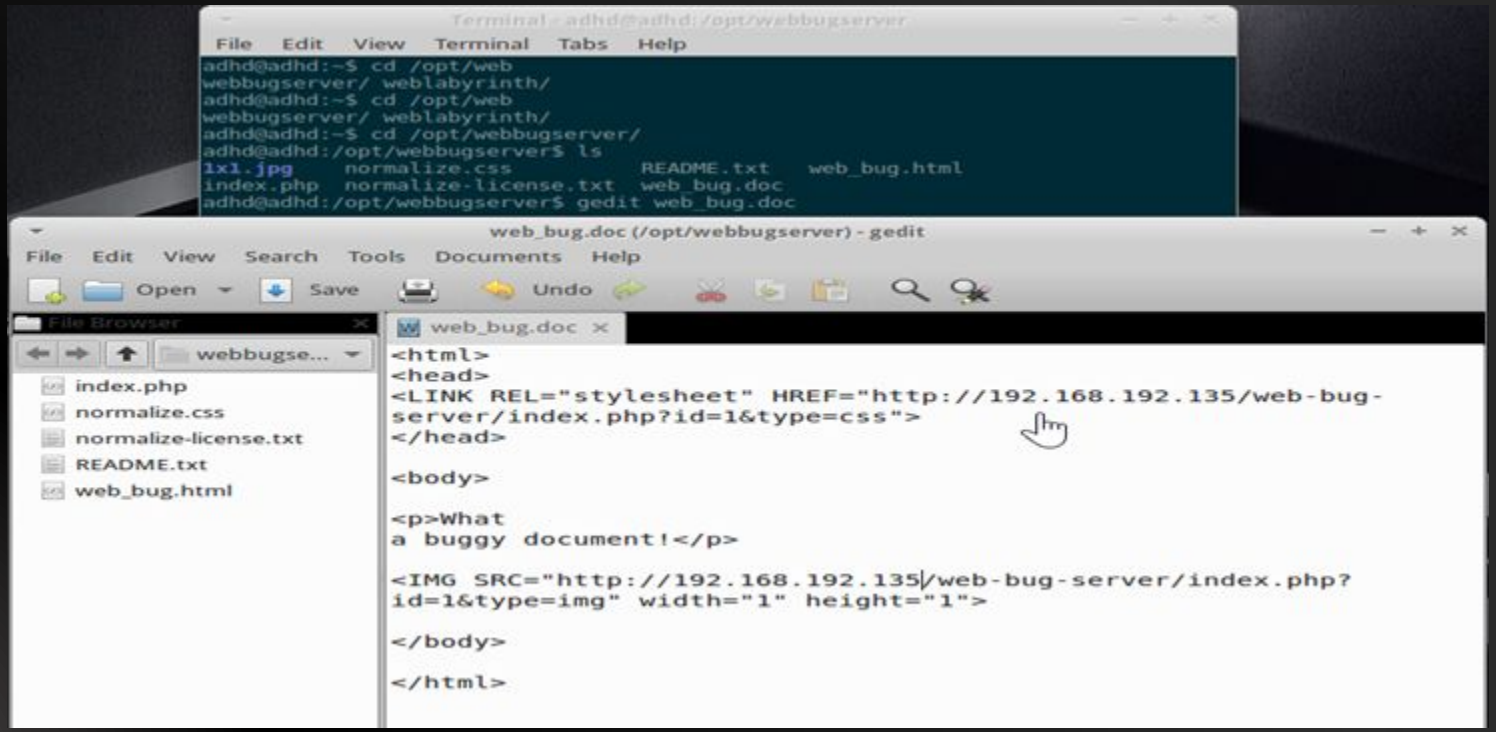
Enhance


Louisville Slugger Museum & Factory
21c Museum Hotel Louisville
Bristol Bar & Grille Downtown
Louisville Glassworks
Mussel & Burger Bar
Evan Williams Bourbon Experience
Starbucks
Jeff Ruby's Steakhouse, Louisville
Troll Pub Under the Bridge
Bluegrass Brewing
Barrel on Main
Actors Theatre of Louisville
Republic Bank
Park Community Credit Union
PNC Bank
Vincenzo's
LG&E and KU Energy
FedEx Office Print & Ship Center
The Old Spaghetti Factory
Holiday Inn Express & Suites...
W Market St
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...
W Liberty St
Hyatt Regency Louisville
Papa John's Pizza
Louisville MSD
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
Scott Parking
River City Bank
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
31W
1931
60
1020

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

Word Web Bugs



Tracking!

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

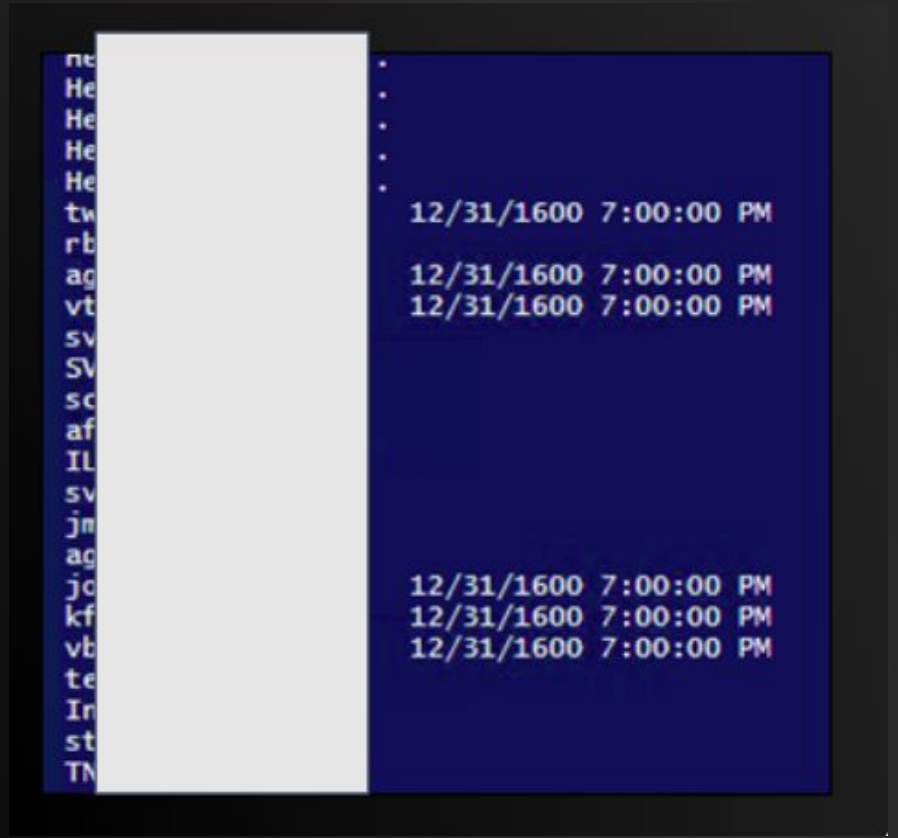
Apple TextEdit

Microsoft Word

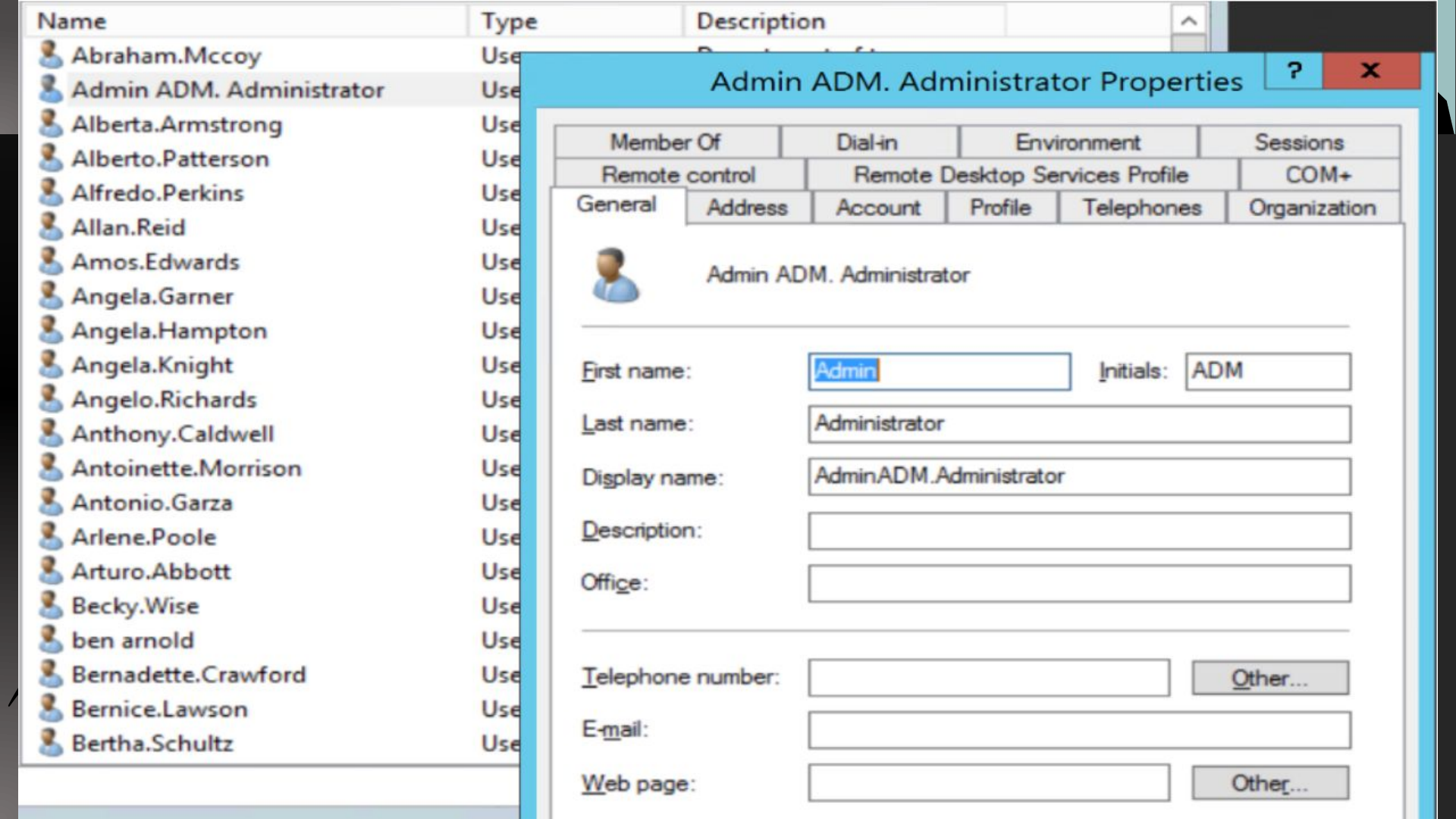
One Step Forward...

JAVELIN

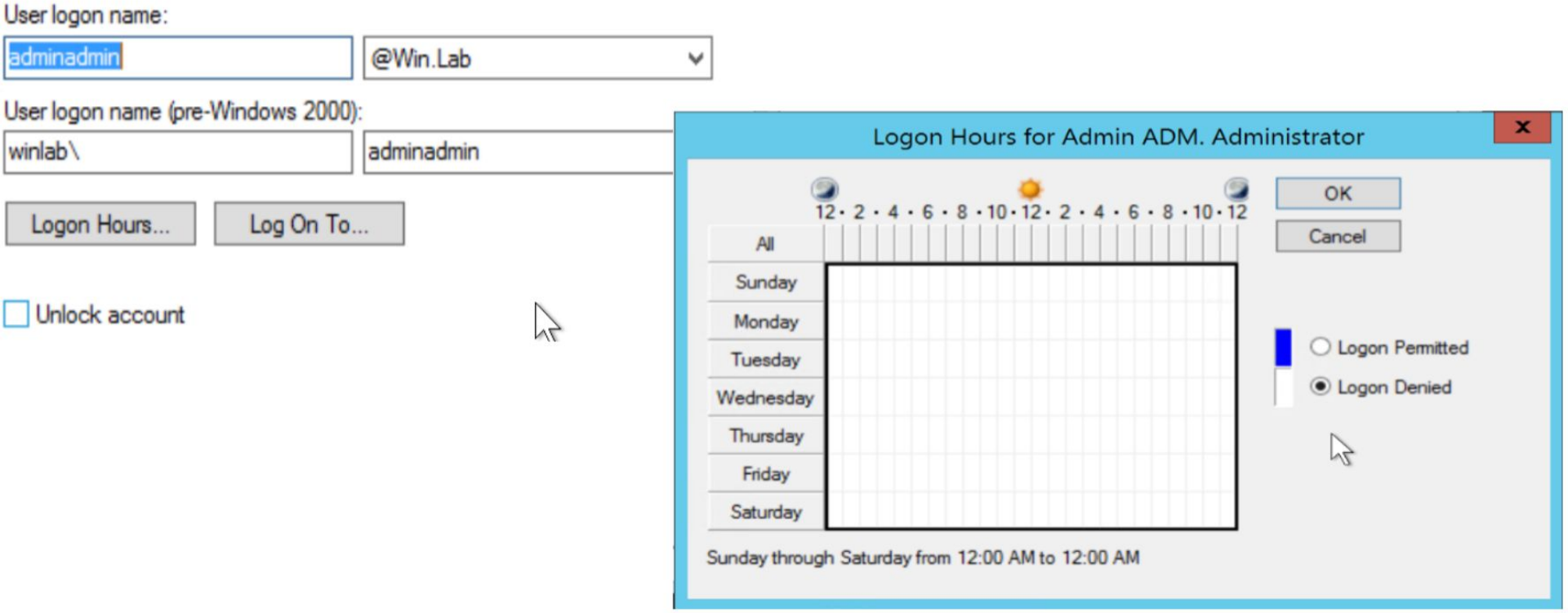
Now a Symantec Company



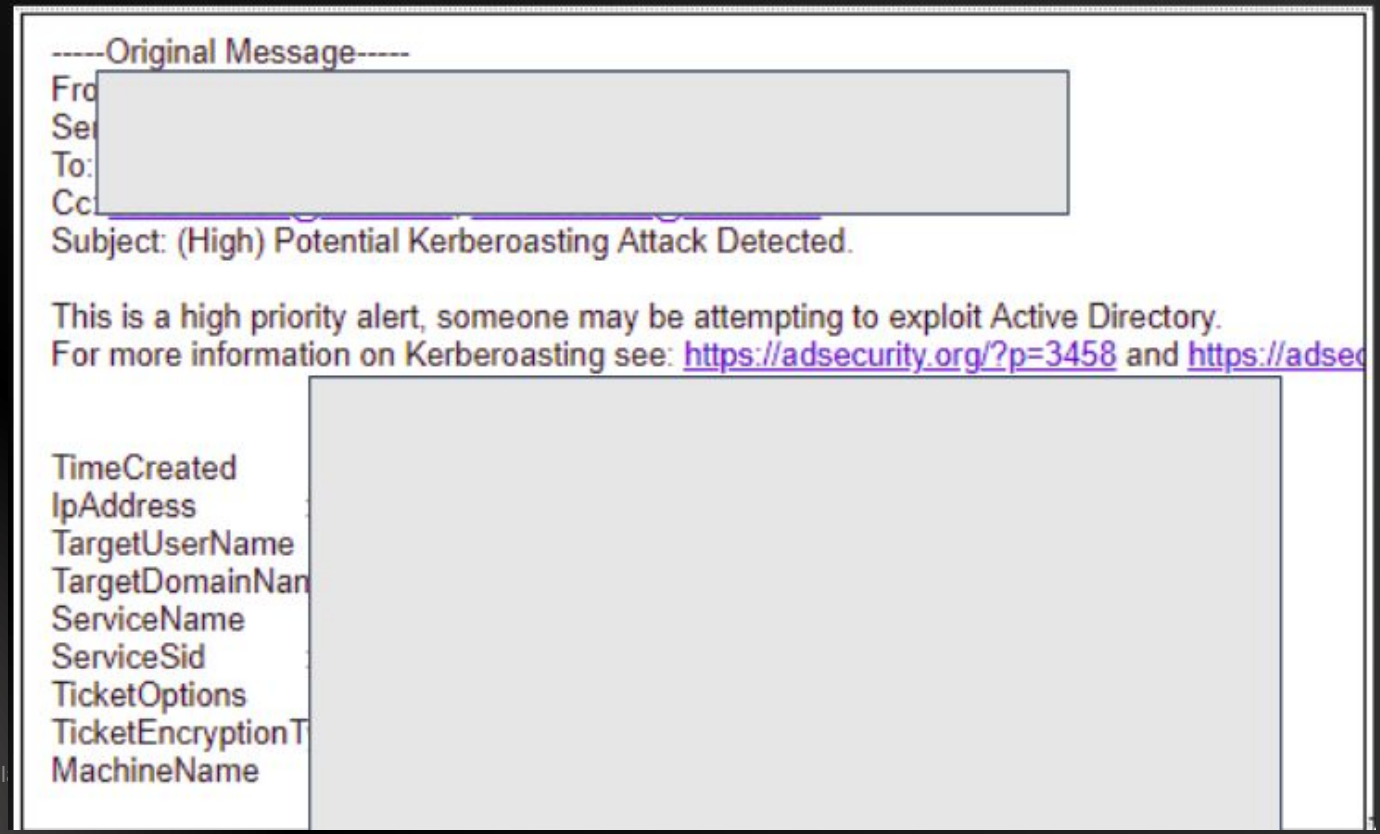
BLACK HILLS Information Security
CELEBRATING 10 YEARS
2008-2018


Name
Type
Description
Abraham.Mccoy
Admin ADM. Administrator
Alberta.Armstrong
Alberto.Patterson
Alfredo.Perkins
Allan.Reid
Amos.Edwards
Angela.Garner
Angela.Hampton
Angela.Knight
Angelo.Richards
Anthony.Caldwell
Antoinette.Morrison
Antonio.Garza
Arlene.Poole
Arturo.Abbott
Becky.Wise
ben arnold
Bernadette.Crawford
Bernice.Lawson
Bertha.Schultz
Admin ADM. Administrator Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Admin ADM. Administrator
First name:
Admin
Initials:
ADM
Last name:
Administrator
Display name:
AdminADM.Administrator
Description:
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...

Important!


User logon name:
adminadmin
@Win.Lab
User logon name (pre-Windows 2000):
winlab\
adminadmin
Logon Hours...
Log On To...
Unlock account
Logon Hours for Admin ADM. Administrator
12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
OK
Cancel
Logon Permitted
Logon Denied
Sunday through Saturday from 12:00 AM to 12:00 AM

Kerberoasting



We Love Adding This…

- **Effective Use of Traps:** Multiple hosts on the domain were installed as traps. Activities conducted by BHIS revealed that these traps were vulnerable to multiple insecurities and they made tempting targets. Any interaction with these hosts triggered alerts to the customer and these were reported to BHIS during the test. While these should not be relied on as a sole source of protection, they do provide an added layer of defense-in-depth.

- We love it when testers cry. I collect their tears… It makes the best wine.

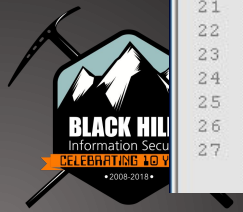
Honeybadger Update

C:\Tools\dc2.vb - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

classmacro.vb | macro.vb | Macro | dc2.vb

```
1   Imports System.IO
2
3   Module HoneyBadgerBeacon
4       Sub Main()
5           Dim objWSH As New Object
6           objWSH = CreateObject("WScript.Shell")
7
8           Dim wifi As String
9           wifi = objWSH.Exec("powershell netsh wlan show networks mode=bssid | findstr 'SSID Signal Channel'").StdOut.ReadAl
10
11          Dim objWriter As New System.IO.StreamWriter(Environ("temp") & "\wifidat.txt")
12          objWriter.Write(wifi)
13          objWriter.Close()
14
15          wifi = objWSH.Exec("powershell Get-Content %TEMP%\wifidat.txt -Encoding UTF8 -Raw").StdOut.ReadAll
16
17          Kill(Environ("temp") & "\wifidat.txt")
18
19          wifi = objWSH.Exec("powershell -Command ""& {[System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetByte
20
21          Dim objHTTP As New Object
22          objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
23          objHTTP.Open("POST", "http://192.168.229.133:5000/api/beacon/404bbe32-09d0-47ed-b8ba-b69c47aa1ea6/VB")
24          objHTTP.setRequestHeader("Content-Type", "application/x-www-form-urlencoded")
25          objHTTP.Send("os=windows&data=" & wifi)
26      End Sub
27  End Module
```



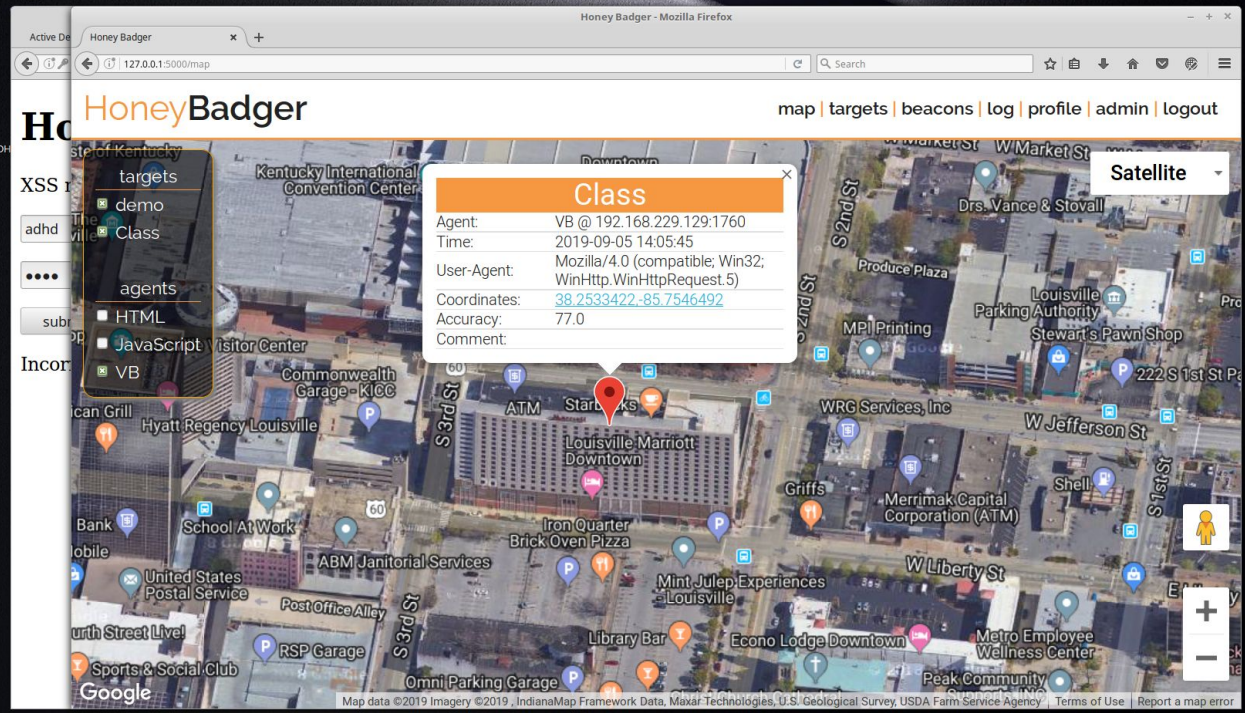
Compile It

```
Mono version 6.0.0.313
Prepending 'C:\Program Files\Mono\bin\' to PATH

C:\Windows\system32>vbc c:\Tools\macro.vb
Microsoft (R) Visual Basic Compiler version 3.100.19.26603 (9d80dea7)
Copyright (C) Microsoft Corporation. All rights reserved.


C:\Windows\system32>macro.exe
```

Results!

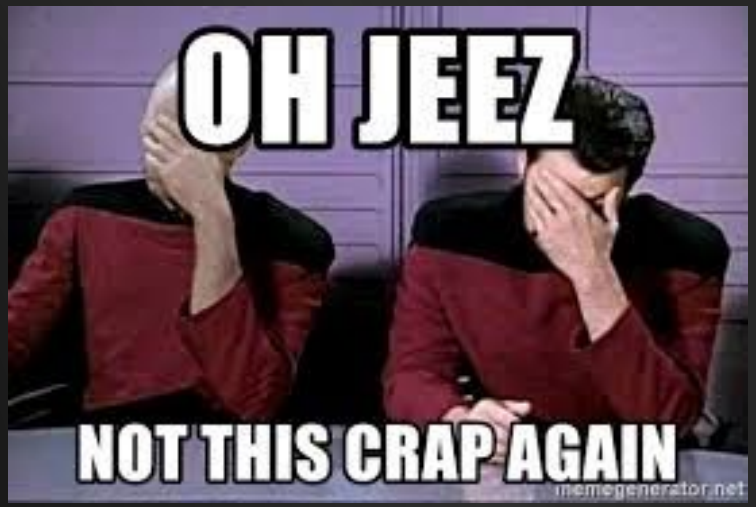

Honey Badger - Mozilla Firefox
Honey Badger
127.0.0.1:5000/map
HoneyBadger
map | targets | beacons | log | profile | admin | logout
targets
demo
Class
agents
HTML
JavaScript
VB
Class
Agent: VB @ 192.168.229.129:1760
Time: 2019-09-05 14:05:45
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Coordinates: 38.2533422,-85.7546492
Accuracy: 77.0
Comment:
Satellite
Kentucky International Convention Center
Commonwealth Garage - KICC
Hyatt Regency Louisville
Louisville Marriott Downtown
Starbucks
ATM
WRG Services, Inc
Drs. Vance & Stovall
Produce Plaza
MPI Printing
Louisville Parking Authority
Stewart's Pawn Shop
W Jefferson St
W Market St
S 2nd St
S 3rd St
S 1st St
Griffs
Merrimak Capital Corporation (ATM)
Shell
Iron Quarter Brick Oven Pizza
ABM Janitorial Services
School At Work
United States Postal Service
Post Office Alley
RSP Garage
Sports & Social Club
Omni Parking Garage
Mint Julep Experiences Louisville
W Liberty St
Library Bar
Econo Lodge Downtown
Metro Employee Wellness Center
Peak Community
Google
Map data ©2019 Imagery ©2019 , IndianaMap Framework Data, Maxar Technologies, U.S. Geological Survey, USDA Farm Service Agency | Terms of Use | Report a map error

Git It Here

https://github.com/bkonsela/honeybadger

Back To Threat Intel

- What is the goal of Threat Intel?
  - Learn about hackers
  - Improve defenses
- Can't we do that cheaper and better with deception tech?
- Actual attacks… On your networks
- Not an attack from months ago



How we use it.

Kent Ickler

12:47 AM (11 hours ago)

John, we didn't think much of these on their own initially, however they seem to have all geographically correlated and figured we should let you know in the event you want to provide specific directive . These have been seen in the last 4 weeks:

1) Targeted phishing originated from NL IPv6
2) targeted network scanning of RC from NL IPv4
3) BHIS Dopple DDNS pointed to NL IPv4
4) Recent Canary Token hit of webmail...BHiS... from NL IPv4
5) GoDaddy CDN is blocking an usually high amount of connections from NL
6) CJ Getting phone calls from Antwerp,

Questions?

PENETRATION TESTING

RED TEAMING

THREAT HUNTING

WEBCASTS

OPEN-SOURCE TOOLS

BLOGS

bhis.co

AI HUNTER™

Network Threat Hunting Solution

ANALYZE
Network Traffic

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

- BEACONS MODULE
- LONG CONNECTIONS MODULE
- DEEP DIVE MODULE
- ALERTING

acm.org

WILD WEST HACKIN' FEST

www.wildwesthackinfest.com

Watch Past WWHF Talks on YouTube