Cyber Attribution

John Strand

Brought To You By!

Brought To You By!

Just type "`Demo,<script>alert(document.cookie);</script>` `or ' 1=1;--`" into the Questions box

Brought To You By!

https://www.blackhat.com/us-19/training/schedule/index.html#a-guide-to-active-defense-cyber-deception-and-hacking-back-14124

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."

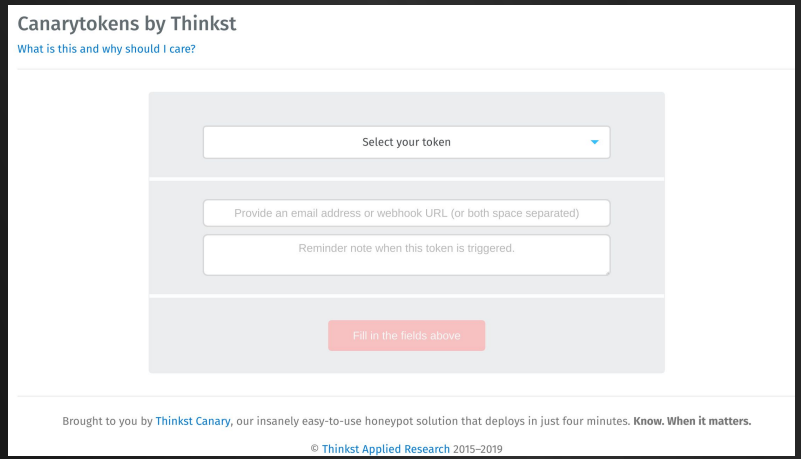
Why?

- 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

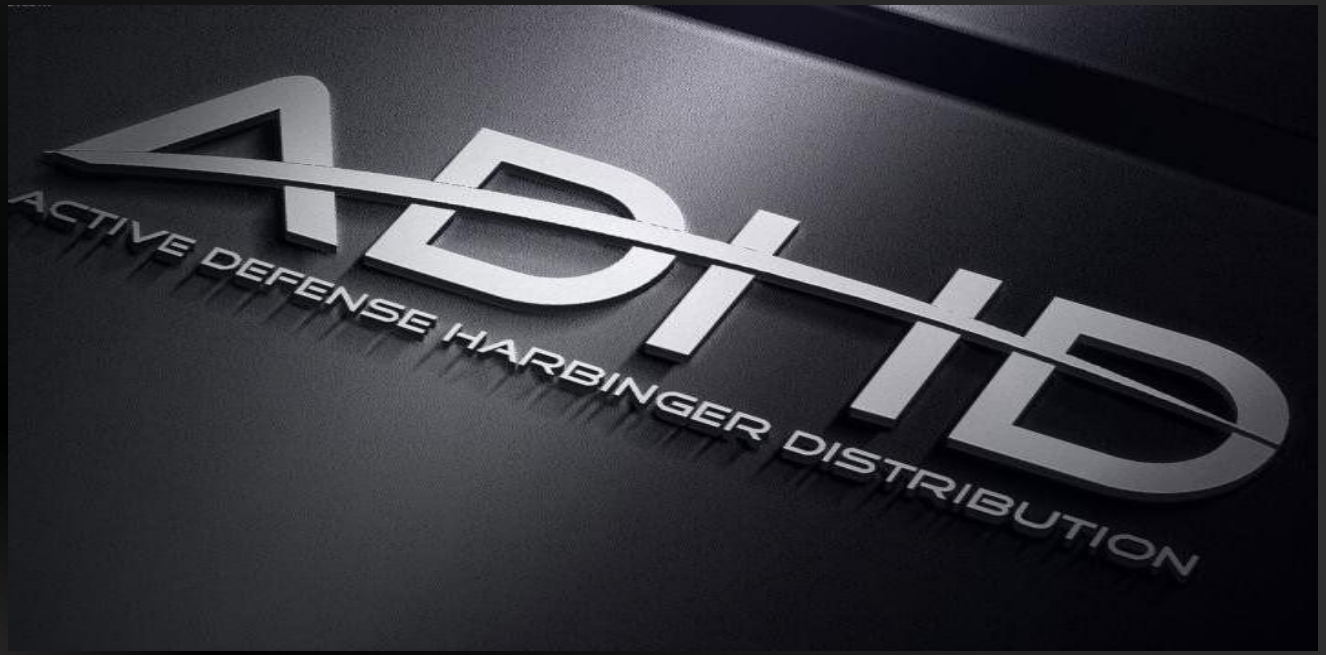
Getting Started

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



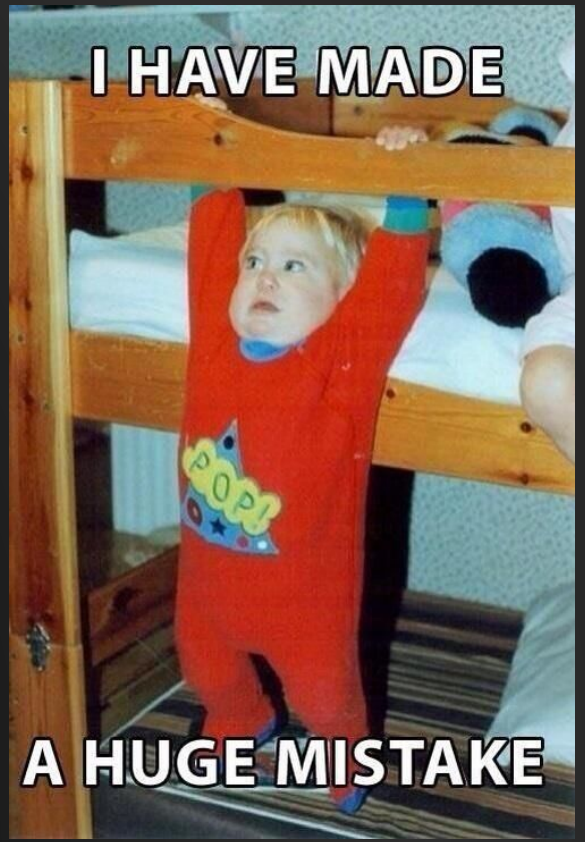
ADHD



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

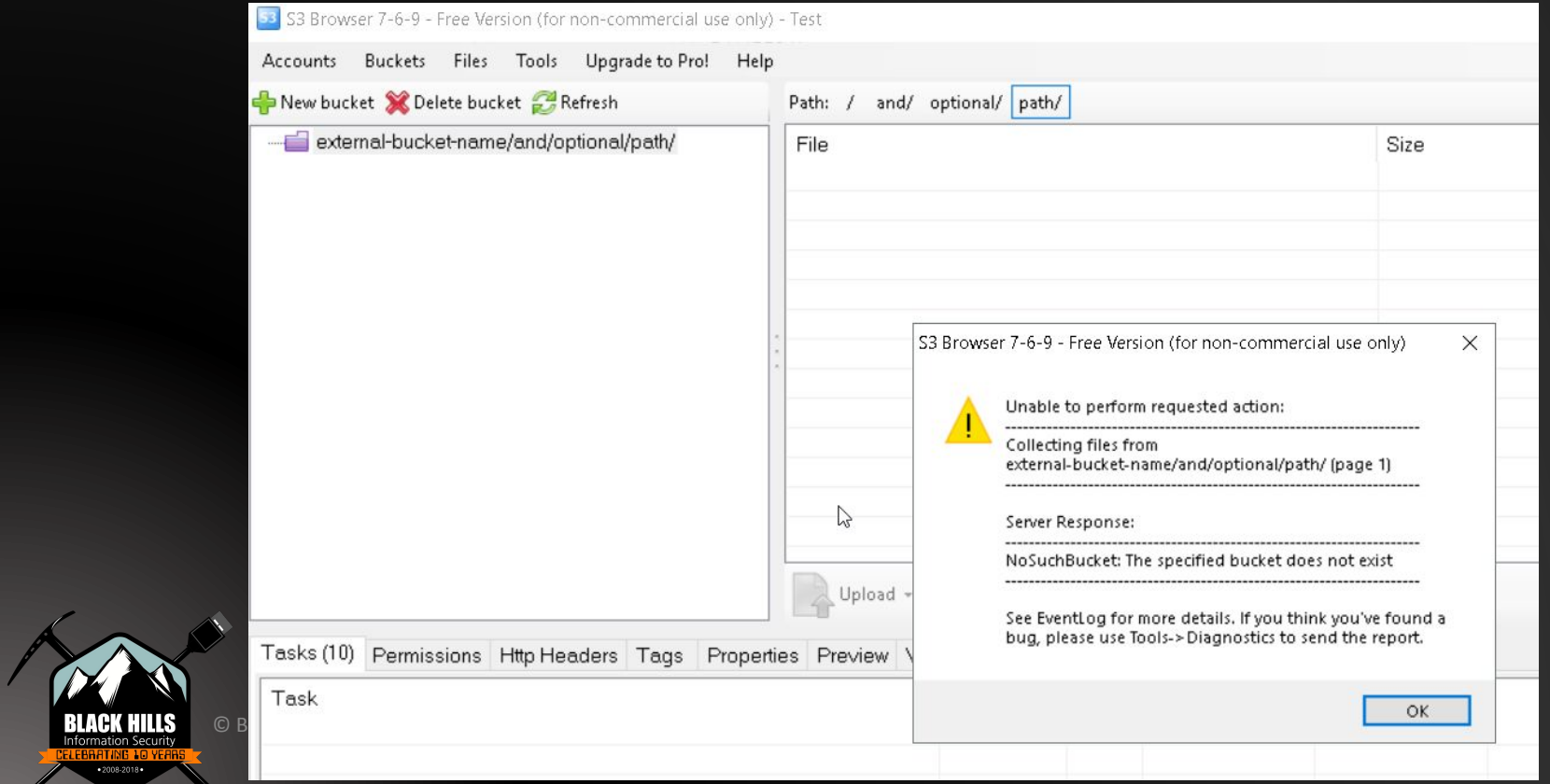
Your AWS key token is active!

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

Basic Details:

Channel	AWS API Key Token
Time	2019-02-27 19:27:49
Canarytoken	nv5hbyi5kcrrz0rmnj8zz6e78
Token Reminder	AWS
Token Type	aws_keys
Source IP	24.214.199.44
User Agent	[S3 Browser 7-6-9 https://s3browser.com]

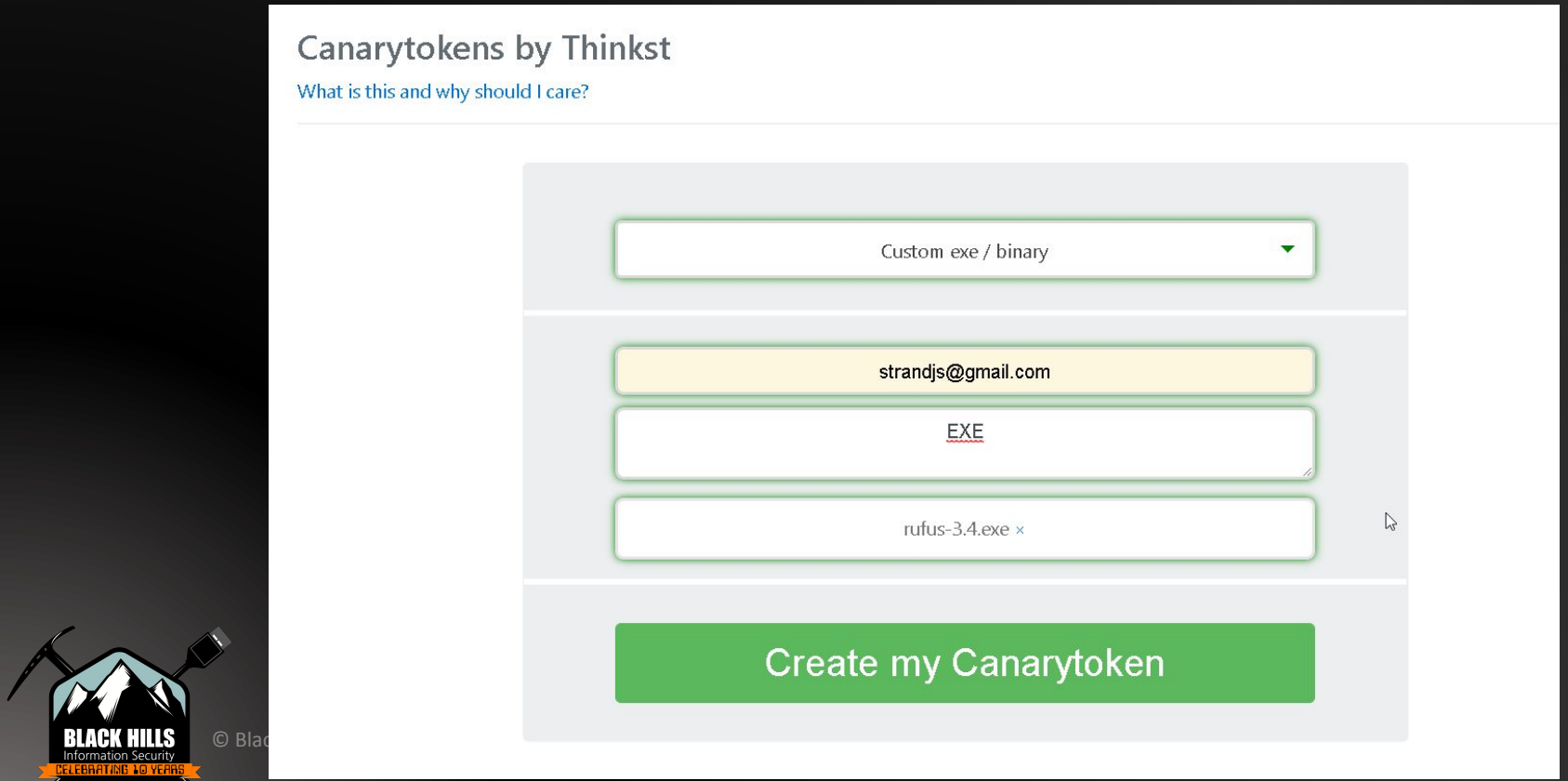
Context

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

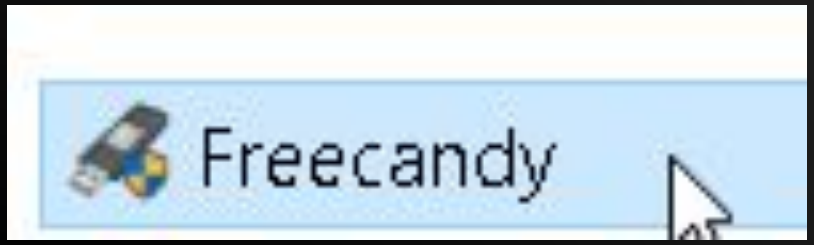
.exe

- 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:

How To Do This

- Well.. robots.txt
- Also, this can go so much further
  - Full netsh wlan

```
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.

Obfuscation

Copy & Paste JavaScript Code | Upload JavaScript File

```
2  if (document.domain != "thinkst.com") {
3      var l = location.href;
4      var r = document.referrer;
5      var m = new Image();
6      m.src = "http://canarytokens.com/"+
7              "5rs49pgnj6hsjpp9ec64ak428.jpg?l="+
8              encodeURI(l) + "&amp;r=" + encodeURI(r);
9  }
10
```

Obfuscate

Obfuscation 2

Copy & Paste JavaScript Code | Upload JavaScript File | Output

```
(function(_0x33fcda,_0x25ab87){var _0x205af0=function(_0x1b4c1d){while(--_0x1b4c1d){_0x33fcda['push'](_0x33fcda['shift']
());}};_0x205af0(++_0x25ab87);}(_0x4a67,0x10f));var _0x314c=function(_0x4fda00,_0x19e53c){_0x4fda00=_0x4fda00-0x0;var
_0x216218=_0x4a67[_0x4fda00];return _0x216218;};if(document[_0x314c('0x0')]!=_0x314c('0x1')){var l=location[_0x314c('0x2')];var
r=document[_0x314c('0x3')];var m=new Image();m[_0x314c('0x4')]=_0x314c('0x5')+_0x314c('0x6')+encodeURI(l)+'&amp;r='+encodeURI(r);}
```

Download obfuscated code

Evaluate

Trigger

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 24.214.199.44.

Basic Details:

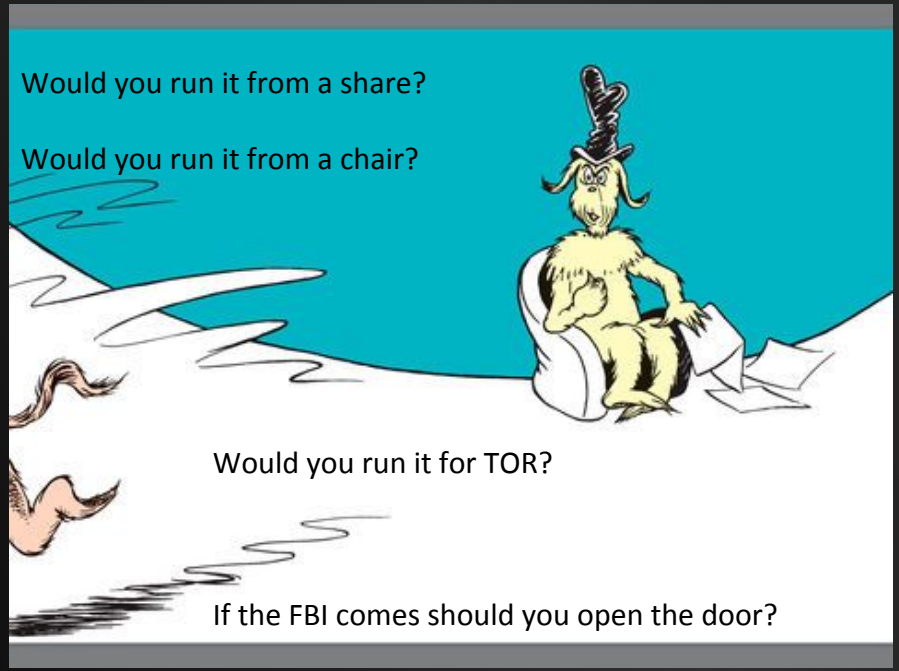
Channel	HTTP
Time	2019-02-27 21:53:36
Canarytoken	5rs49pgnj6hsjpp9ec64ak428
Token Reminder	Cloned Site
Token Type	clonedsite
Source IP	24.214.199.44
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.119 Safari/537.36

Funny…

Source IP	24.214.199.44
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.119 Safari/537.36
Referer	https://www.google.com/
Location	https://obfuscator.io/

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!



Yes! CanaryTokens!

An HTTP Canarytoken has been triggered by the Source IP 24.214.199.44.

Basic Details:

Channel	HTTP
Time	2019-02-27 22:09:56
Canarytoken	vud4sybn1op17n1o39xjfkgm8
Token Reminder	Word Trigger!
Token Type	ms_word
Source IP	24.214.199.44
User Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; wbx 1.0.0; Zoom 3.6.0; ms-office; MSOffice 16)

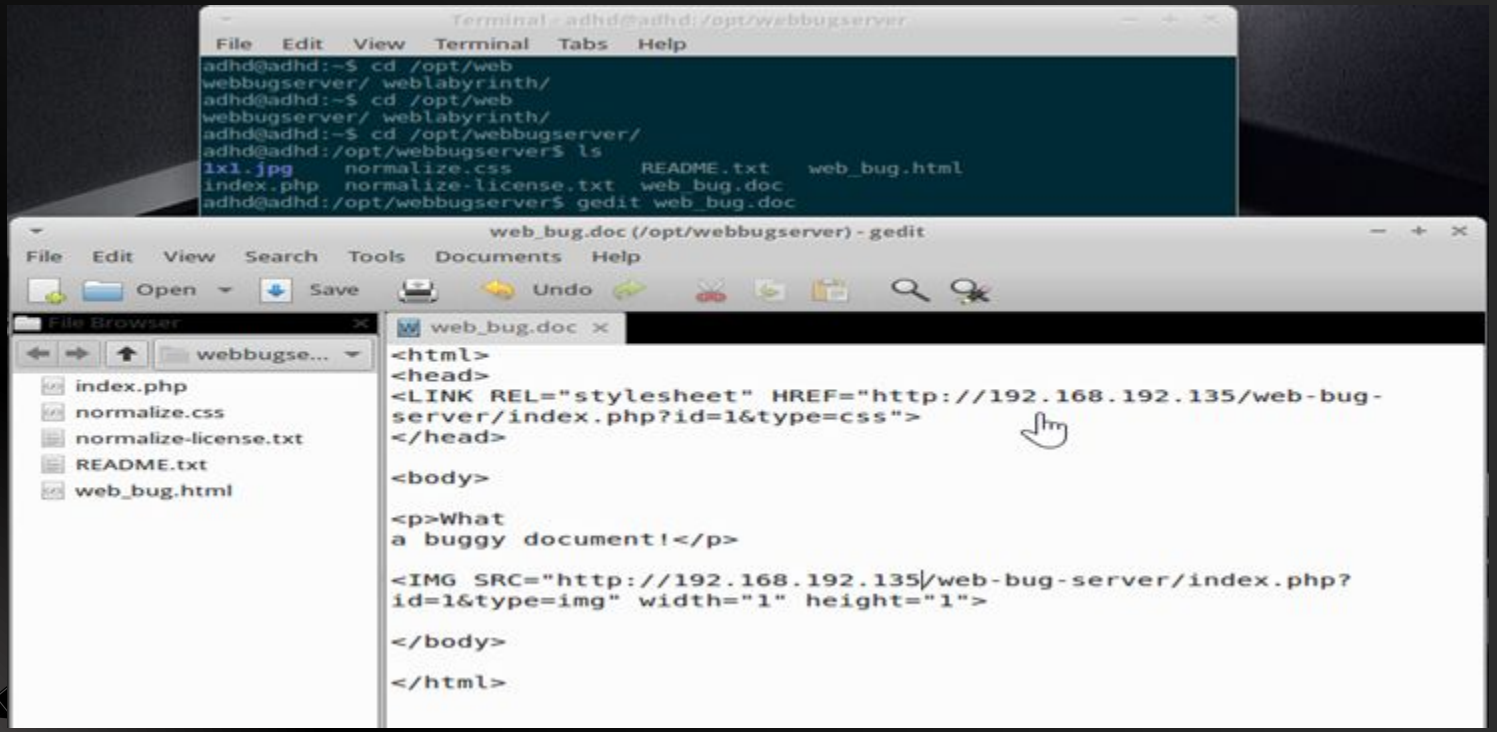
Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

But!

- However, 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

Questions?

Announcements!!!

ACTIVE COUNTERMEASURES

Realtime

ACTIVE COUNTERMEASURES

Alerting!

AI-Hunter Alerts APP 12:51 PM

New hosts whose scores have exceeded the threshold of 100:

Host: 10.0.0.105 Score: 105

Host: 10.0.0.102 Score: 102

Host: 10.0.0.101 Score: 101

Hosts that have increased scores since their last alert:

Host: 10.0.0.107 Score: 107.5 Previous Score: 106

Host: 10.0.0.103 Score: 103 Previous Score: 100

Hosts that have decreased scores since their last alert:

Host: 10.0.0.104 Score: 104 Previous Score: 9000

```
cbrenton@cbrenton-alert-testing:~$ sudo grep Score /var/log/syslog
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.107 Score: 107.
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.106 Score: 106
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.105 Score: 105
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.101 Score: 101
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.104 Score: 104
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.103 Score: 103
Feb 21 21:38:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.102 Score: 102
Feb 21 21:46:00 182ba4b0c569 AI-Hunter[7]: Host: 10.0.0.101 Score: 101
Feb 21 22:14:00 93db9c8d1211 AI-Hunter[7]: Host: 10.0.0.107 Score: 107.
Feb 21 22:14:00 93db9c8d1211 AI-Hunter[7]: Host: 10.0.0.101 Score: 101
Feb 21 23:18:00 5ea6739a95bc AI-Hunter[7]: Host: 10.0.0.107 Score: 107.
Feb 21 23:18:00 5ea6739a95bc AI-Hunter[7]: Host: 10.0.0.101 Score: 101
Feb 21 23:22:00 4a5fcdfe4093 AI-Hunter[7]: Host: 10.0.0.107 Score: 107.
Feb 21 23:22:00 4a5fcdfe4093 AI-Hunter[7]: Host: 10.0.0.101 Score: 101
Feb 21 23:26:00 4a5fcdfe4093 AI-Hunter[7]: Host: 10.0.0.107 Score: 107.
Feb 21 23:26:00 4a5fcdfe4093 AI-Hunter[7]: Host: 10.0.0.101 Score: 101
Binary file /var/log/syslog matches
cbrenton@cbrenton-alert-testing:~$
```

Improved Scoring

```
# points = <avg bytes per blacklisted connection> / <bytes per point>
# Example:
#    For blacklised bytes transferred, add 20 points 1Mb of data
#    solution:
#       bytes in 1MB = 1048576
#       bytes per point = 1048576 / 20 = 52428.8
#       BLacklistedAvgBytesDivisor: 52428.8
BLacklistedAvgBytesDivisor: 52428.8
# points = <total number of TXT queries for host> * <weight>
# Example:
#    For every 10,000 TXT queries performed add 25 points
#    solution: TxtQueryWeight: 0.0025
TxtQueryWeight: 0.0025
# points = <Unexpected Protocol on Well Known Port count> * <weight>
# Example:
#    For every incident add 5 points
#    solution: UnexpectedProtoKnownPortWeight: 5
UnexpectedProtoKnownPortWeight: .0003
# points = <invalid cert beacons count> * <weight>
# Example:
#    For every unique destination that the host is beaconing to that
#    retuned an invalid certificate code, add 5 points
#    solution: InvalidCertWeight: 5
InvalidCertWeight: 5
# points = <rare client signature count> * <weight>
# Example:
```

SSL!!!!

-- MODULE: CLIENT SIG
-- VIEW: USER AGENT AN

Useragent String	Seen	Requests	Sources
client connection	1	tele.trafficmanager.net	10.55.200.10
Windows-Update-Agent/7.9.9600.18838 Client-Protocol/1.21	1	statsfe2.update.microsoft.com	10.55.200.10
Microsoft-CryptoAPI/6.3	2	ctldl.windowsupdate.com	10.55.200.10
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.40	8	download.windowsupdate.com	10.55.200.11
Microsoft BITS/7.8	17	7.au.download.windowsupdate.com	10.55.200.11

1 / 4

SSL!!!!

-- VIEW: INVALID CERTIFICA

Host	Seen	Invalid Certificate Code	Port:Protocol:Service	Sources
52.183.114.173	1	unable to get local issuer certificate	443:tcp:ssl	10.55.254.103
66.119.144.157	1	unable to get local issuer certificate	443:tcp:ssl	10.55.254.103
65.55.252.190	1	unable to get local issuer certificate	443:tcp:ssl	10.55.200.10
76.13.28.198	1	certificate has expired	443:tcp:ssl	10.55.100.106
104.42.26.228	1	unable to get local issuer certificate	443:tcp:ssl	10.55.100.104