

We're all Script Kiddies

Side A: Domains for Evil

Who am I?

David E. Switzer

- **Experience:** 20+ Years .. Blah Blah.. Train industry, cable industry, and the ISP industry. Choo-Choo.
- **Interests:** Whispers in the dark and connecting the dots (802.[11|15.1|15.4, metadata, and other things not related).
- **Cert roll call:** GSE #136, G[CIH|PEN|AWN|CIA|SEC] (SANS-whore), CISSP, ITILv3 and CPR*.
- **Job:** Red Team Operator @ ReliaQuest in Tampa, FL

** = CPR certification is expired*

Fun Fact

Glossophobia is the fear of public speaking.
From the Greek γλῶσσα glōssa, meaning tongue,
and φόβος phobos, fear or dread.

... no reason ...

Now on to the questionable use of found
graphics!

Red Teaming

- I'm part of a red team.
- We sell “continuous red teaming services”, which means we try to hack our customers constantly.
- With enough time, we have a 100% success rate.

... Let's investigate that last one a bit ...

How we get in.

- Hardware Analysis / Reversing



How we get in.

- USBs / Public Machines



How we get in.

- Physical / B&E



Hi Ian and Jonathan!

So what is our most successful method?



Shocker.

Phishing.. gets boring.

Sure there is the initial thrill, but this gets boring...
quickly.

How can we take some pain out of this, and speed
things up?

How to detect Evil Domains?

This started with a fun discussion on noticing evil with an engineer on our blue team.

(Hi Casey!)

What do evil domains “look” like?

Evil Domain Detection?

- The proposed idea of detecting evil domains:
 - **Categorization** – What do the various web-proxy/scanning companies say it is? Bluecoat, etc.
 - **TLD** – “.com” or even “.net” are seen as less likely to host evil than a “.at” domain *
 - **Age** – Was this domain created last week, or has it been around?

** = No, this isn't a domain-fronting talk, we've played with that too ;)*

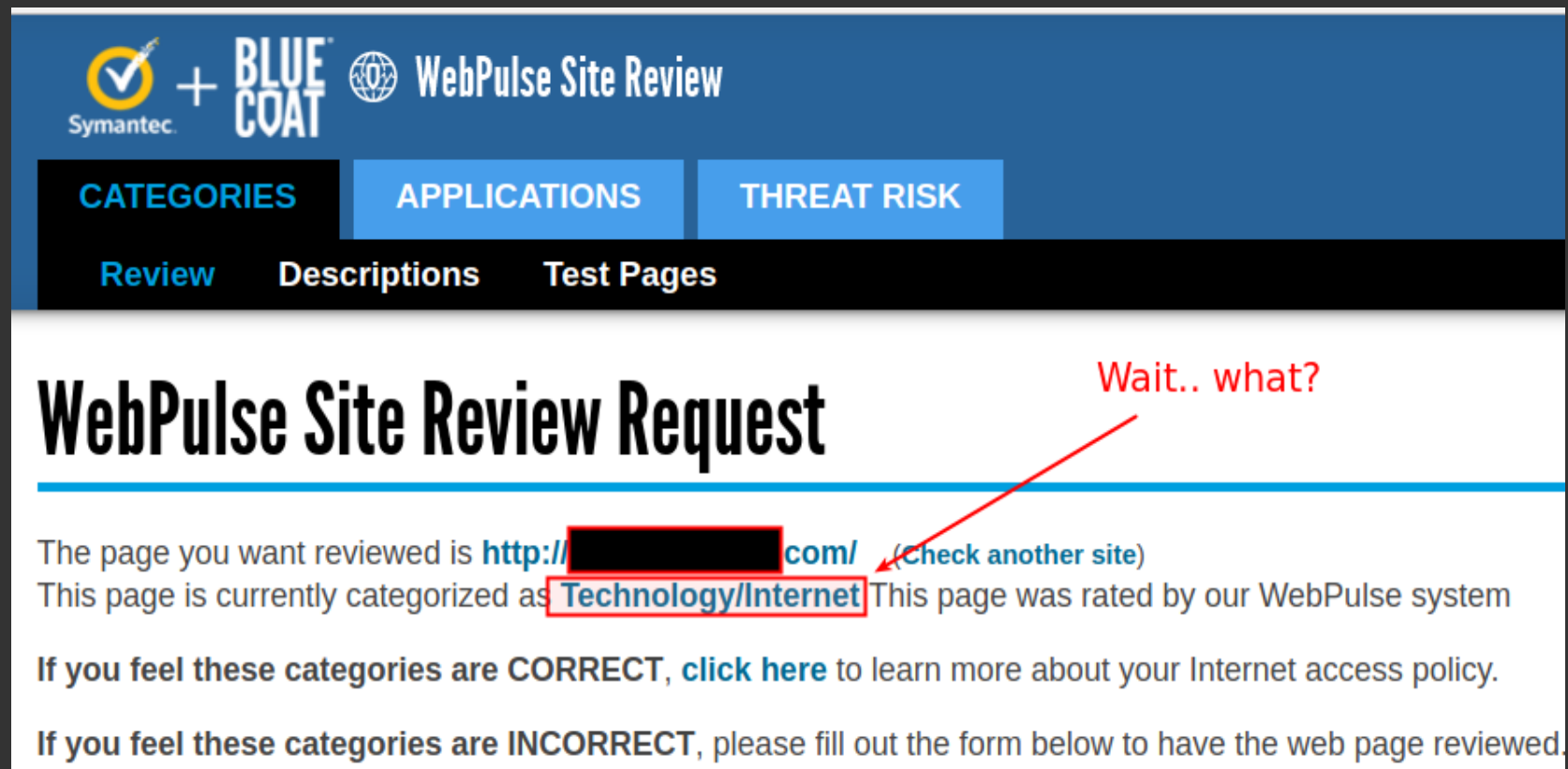
So I was curious.



- Picked a domain that was purchased for an engagement/client.
- TLD Check? It's a .com.
- Age Check? Six months old, that's good.

```
Domain Name: [REDACTED]  
Registrar: 101DOMAIN, INC.  
Sponsoring Registrar IANA ID: 1011  
Whois Server: whois.101domain.com  
Referral URL: http://101domain.com  
Name Server: NS1.101DOMAIN.COM  
Name Server: NS2.101DOMAIN.COM  
Name Server: NS5.101DOMAIN.COM  
Status: clientTransferProhibited https  
  
Updated Date: 14-sep-2016  
Creation Date: 14-sep-2016  
Expiration Date: 14-sep-2017
```

So I was curious.

- Picked a domain that was purchased for an engagement/client.
- **Categorization?** .. I've never used this domain ..



 +  WebPulse Site Review

CATEGORIES APPLICATIONS THREAT RISK

Review Descriptions Test Pages

WebPulse Site Review Request

The page you want reviewed is [http://\[REDACTED\].com/](http://[REDACTED].com/) [\(Check another site\)](#)

This page is currently categorized as **Technology/Internet** This page was rated by our WebPulse system

If you feel these categories are CORRECT, [click here](#) to learn more about your Internet access policy.

If you feel these categories are INCORRECT, please fill out the form below to have the web page reviewed.

Now I'm super curious.

- How is a domain that was purchased, and never touched.. categorized as “tech/internet” ?
- Bluecoat crawled the “park” page, and it was keywordy enough to get ranked.

The screenshot shows the 101domain.com website. At the top left is the 101domain.com logo. At the top right is the phone number 877.983.6624 and the international number ++1.760.444.8674. Below the header, there's a section titled "Featuring the future site for:" followed by a redacted domain name ".com". To the right of this is a yellow button with a right arrow and the text "LOGIN TO MANAGE DOMAINS / HOSTING", and below it, a yellow button with the text "LOGIN". Below the domain name, it says "Do any of the following, and more, when you Log-in to Manage Your Domains:" followed by a list of services: Renew Domains, Edit Administrative Contact, Domain Help Support, Edit DNS Servers, Forward Domain, and Access Hosting Management. At the bottom, there are four service boxes: "SSL Security" with logos for Symantec, GeoTrust, and RapidSSL; "Email Hosting" with the text "All Unlimited! All The Time!" and a "MORE INFO" link; "HIGH SECURITY DNS SERVICES WITH ANYCAST" with a "CLICK HERE FOR MORE INFO" link; and "Corporate Brand Protection" with the text "Protect what you've built." and an image of a hand holding a tree.

101domain.com

877.983.6624
International: ++1.760.444.8674

Featuring the future site for:

.com

Do any of the following, and more, when you Log-in to Manage Your Domains:

- Renew Domains
- Edit Administrative Contact
- Domain Help Support
- Edit DNS Servers
- Forward Domain
- Access Hosting Management

SSL Security
Symantec. GeoTrust
RapidSSL. thawte

Email Hosting
All Unlimited!
All The Time!
MORE INFO

HIGH SECURITY
DNS SERVICES
WITH
ANYCAST
CLICK HERE FOR MORE INFO

Corporate Brand
Protection
Protect what
you've built.

This site parked courtesy of 101domain.com, The Leader in International Domain Registration

Let's review.

- **Age? CHECK!**
- **Lovable, trustworthy TLD? CHECK!**
- **Categorized with a web proxy service? CHECK!**

So we're good!

So what? A parked domain.

- Amusing, but so what? An old domain I bought a while ago.
- Anyone who went to this page would see it was parked, so it looks very suspect.

How can we do this in a more believable way, that's not that "labor" intensive?

Aging domains. Or go “vintage” ?

In many ways, buying the domains yourself and let them age is the best way to go.



We're in a hurry, so let's be hipsters and go “vintage”.

Roll the dice, go “vintage”.



Domains are deleted and expire daily.

Domain reputation services aren't checking every domain every day.

* Yes, that is a real banner for a real site.
No, we didn't use it.

Finding Expired Domains

- Manually digging around for domains to use seems like work. Let's not do that.
- Enter: <https://ExpiredDomains.Net>

Total Domains: 204,912,268	Deleted Domains: 193,185,848
----------------------------	------------------------------

Expired Domains.net
Expired Domain Name Search Engine

Finding Expired Domains

- Sign up for an account – it's free and allows better searching/filtering.

The screenshot shows a domain search interface with several filter panels. Red boxes highlight specific settings, and red arrows point from a common point at the bottom to each of these settings.

Domain Name Settings

- ☒ no Numbers
- ☐ no Characters
- ☐ no Hyphens
- ☒ no consecutive Hyphens
- ☐ only Numbers
- ☐ only Characters
- ☐ no Adult Names

Length: min [] max []

Hyphens: min [] max []

Vowels: min [] max []

Consonants: min [] max []

Characters: min [] max []

Numbers: min [] max []

SimilarWeb Top Country

United-States

Common SEO

- ☐ only with Dmoz Entry
- ☐ only with SimilarWeb Rank
- ☐ only with Alexa Rank
- ☐ only with Quantcast Rank

Backlinks: min [] max []

ACR: min [] max []

Alexa: min [] max []

WBY: - min - [] - max - []

ABY: - min - [] - max - []

SimilarWeb

Global Rank: min [] max []

Traffic Countries: min [] max []

Top Country Rank: min [] max []

Top Country Share: min [] max []

Listing Settings

- ☐ only new last 12 hours
- ☒ only new last 24 hours
- ☐ only new last 7 days
- ☐ only new last 30 days

Add Date

End Date

Named Ending

Ends in days

max Price

Listing Type

Price

- ☐ only Watchlist
- ☐ only available Domains

Registrar

Domains per Page

Let's pick something plain.
And recent.


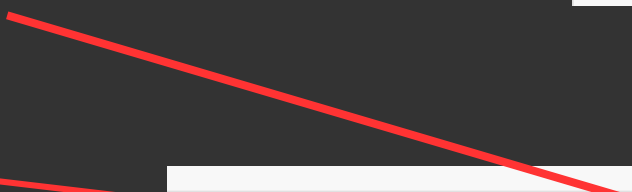
Finding Expired Domains








Interesting information to review and sort by:

- Domain “Birth Date”
- Status
- When domain was dropped
- 12 mo Google search average



<u>LE</u>	<u>BL</u>	<u>DP</u>	<u>WBY</u>	<u>ABY</u>	<u>ACR</u>
13	19	3	2016	2008	56
11	0	0	2016	2005	7
12	0	0	2015	2013	13
16	26	5	2016	2007	43
10	0	0	2016	2013	2
21	0	0	2014	2014	4
12	2	0	2005	2005	79



<u>SG</u>	<u>CO</u>	<u>CPC</u> ▲	<u>Dropped</u>	<u>Status</u>	<u>RL</u>
1.6 K	3	7.29 USD	Yesterday 18:32	available	
450.0 K	8	4.93 USD	Yesterday 18:38	available	
480	4	2.76 USD	Yesterday 18:55	available	
320	12	2.26 USD	Yesterday 19:01	available	
4.1 M	0	2.05 USD	Yesterday 18:36	available	
30	54	1.90 USD	Yesterday 18:56	available	
3.6 K	46	1.74 USD	Yesterday 18:32	available	

Personal Internet Rule

“Wait Long Enough, Someone Will Code It For You.”

Started to contemplate coding something to automate the domain discovery, and ran across “DomainHunter” by Joe Vest (@joevest) & Andrew Chiles (@andrewchiles).

*** Limit your searching, Bluecoat’ll start requiring Captchas*

```
switzerd@isthisreal:/usr/local/src/domainhunter$ ./domainhunter.py -h
usage: domainhunter.py [-h] [-q QUERY] [-c] [-r MAXRESULTS] [-w MAXWIDTH]
                        [-f FILE]

Checks expired domains, bluecoat categorization, and Archive.org history to
determine good candidates for C2 and phishing domains

optional arguments:
  -h, --help                show this help message and exit
  -q QUERY, --query QUERY   Optional keyword used to refine search results
  -c, --check                Perform slow reputation checks
  -r MAXRESULTS, --maxresults MAXRESULTS
                            Number of results to return when querying latest
                            expired/deleted domains (min. 100)
  -w MAXWIDTH, --maxwidth MAXWIDTH
                            Width of text table
  -f FILE, --file FILE      Input file containing potential domain names to check
                            (1 per line)
```

<https://github.com/minisllc/domainhunter>

Tree Service

To stay Bside:Orlando themed, we searched for the word “Orlando”.

We found a keeper!

treeserviceorlando .net

10.99 USD / 1 Year

10.99 USD

☒ Keep my personal information [private](#). **RECOMMENDED**

5.99 USD

ICANN Fee ([what is this?](#))


0.18 USD

Enter coupon code

APPLY

Subtotal:17.16 USD

Total:17.16 USD

Continue 

Content?

Why add content you've created to make the domain look real.

Someone else already did that for you!



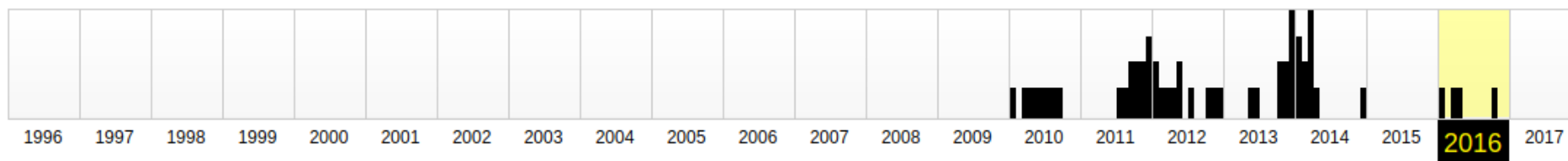
<http://treeserviceorlando.net>

BROWSE HISTORY

<http://treeserviceorlando.net>

Saved **55 times** between [January 29, 2010](#) and [October 10, 2016](#).

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



JAN

FEB

MAR

APR

							1	2								1	2	3	4	5	6								1	2
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Content?

Perfect!


→ ↻ ⓘ https://web.archive.org/web/20121107182523/http://www.treeserviceorlando.net/ ☆ gU

Apps GUITAR WORK infosec IDEAS 102.5 SharkLasers R REGEXTst http://188.25.175 » Other bookmarks


INTERNET ARCHIVE
WayBackMachine
55 captures
29 Jan 10 - 10 Oct 16

http://www.treeserviceorlando.net/ Go

JUL NOV DEC
2011 7 2012 2013
Close X Help ?



Orlando Tree Removal Service


 **Arboriculture News**

There are current no articles for this topic or there's a problem with this feed. Please check your settings.

[Orlando Tree Removal](#)
[Orlando Tree Company](#)
[Orlando Tree Service](#)
[Orlando Tree Trimming](#)

Tree Service in Orlando

Having a reliable **tree service in Orlando** provider can help in addressing your tree-related concerns. Problems with trees are everywhere. There are trees that are needed to be cut down, trimmed or removed from their very roots. Tree problems should be forwarded to tree service companies to avoid or minimize the potential of encountering property damage or accidents which are by themselves dangerous for anyone. You can lose a part of your precious house along with other properties such as vehicles, your garden or other trees. Not only that, it can also cause problem for your neighbor's property which would only lead to your loss. You might end up in court being sued for damaging the properties of others. You also risk your and others



Tips for “borrowing” Content

Want this url:

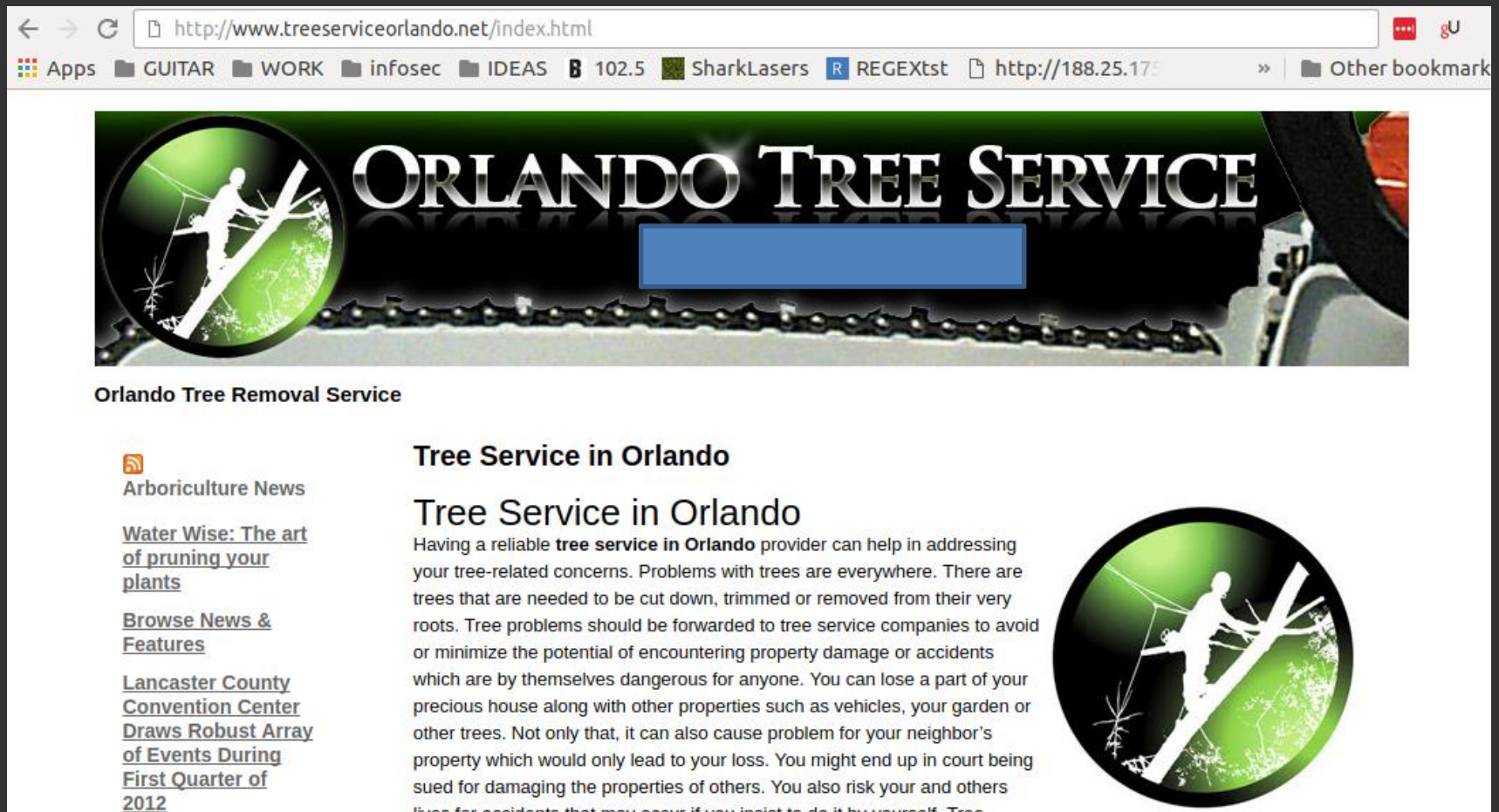
<https://web.archive.org/web/20121107182523/http://www.treeserviceorlando.net>
but without the WebArchive toolbar?

Add “id_” 

https://web.archive.org/web/20121107182523id_/http://www.treeserviceorlando.net

BUT BE SURE TO DOWNLOAD THE FIRST ONE TOO – WebArchive doesn’t supply
jpgs or style sheets when you add “id_” in some cases, but you can add those later.

Content in place.



So what else can we do to make this seem more believable?

“Let’s Encrypt”? Why not?

Let’s Encrypt makes it very easy!



Automatically enable HTTPS on your website with EFF's Certbot, deploying [Let's Encrypt](#) certificates.

I'm using Apache on Ubuntu 16.10 (yakkety)

Apache on Ubuntu 16.10 (yakkety)

automated advanced

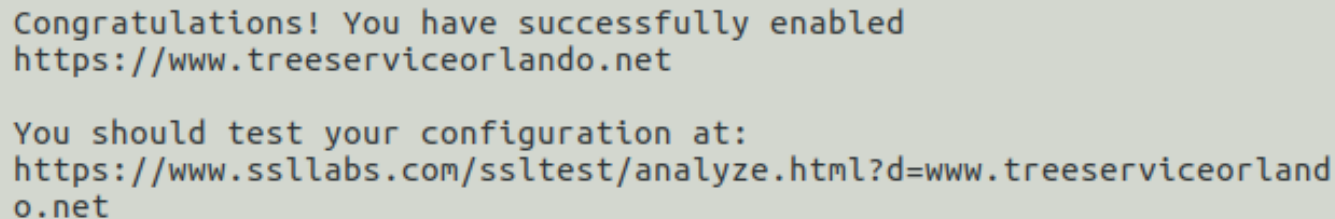
Install

On Ubuntu systems, the Certbot team maintains a PPA. Once you add it to your list of repositories all you'll need to do is apt-get the following packages.

```
$ sudo add-apt-repository ppa:certbot/certbot
$ sudo apt-get update
$ sudo apt-get install python-certbot-apache
```

“Lets Encrypt” ? Why not!

“certbot –apache”, hit enter a few times, and ta-da!
It even sets your Apache configuration.



```
Congratulations! You have successfully enabled
https://www.treeserviceorlando.net

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=www.treeserviceorlando.net
```

< OK >

“Lets Encrypt” ? Why not!

Neato, I’m secure!



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.treeserviceorlando.net](#)

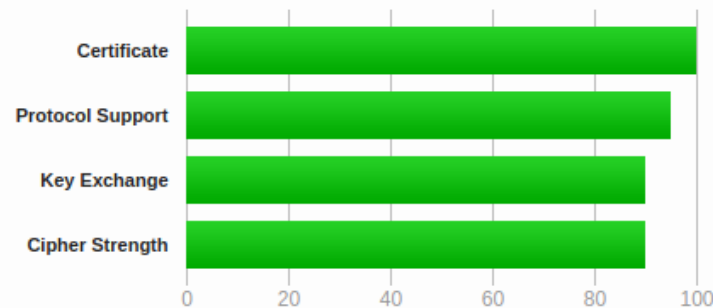
SSL Report: [www.treeserviceorlando.net](#)

Assessed on: Mon, 03 Apr 2017 23:25:16 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Everything is in place – let's review!

- **Categorization** – Yep! Bluecoat thinks it's a vehicle related site.
- **TLD** – Yep! .net, warm and fuzzy!
- **Bonus, SSL Cert!**
- **Age** – .. Oh yeah ..

Age?

Typed “domain age history” into Google, clicked “I’m Feeling Lucky”:

<http://www.webconfs.com/web-tools/domain-age-tool>

Domain Age Tool

No.	Domain Name	Age
1	treeserviceorlando.net	7 years 2 months old

```
switzerd@isthisreal:~$ date
vie abr  7 18:36:33 EDT 2017
switzerd@isthisreal:~$ whois treeserviceorlando.net | grep -i Creation
Creation Date: 2017-04-03T02:04:28Z
switzerd@isthisreal:~$
```

Nearly four days later, the old results are still showing for age.

End of Side A

Side B: Gatos Guardianes

You can keep your watch dogs.

<https://github.com/violentlydave/GatosGuardianes>



GUARD CAT

Waves you on.

Gatos Guardianes



The heros of Watch Dogs hack lots of things with just their phones.
That's totally fantasy... *right?*

NetHunter



The Offensive Security/Kali team jammed Kali onto phones. Most of your tools – now at your finger tips.

It's totally possible now... *right?*

Back to Reality



Typing on a phone sucks enough when typing regular words/sentences, let alone command line tools with flags/switches.

That's what scripts are for.

Let's further embrace our inner script kiddie, and automate some tasks, shall we?



Scripts – Wireless/802.11x

autox.sh = sniff for probes, then try to cross reference 'em for bluetooth names

quickprobegrab.sh = quick pcap grab of probes in an area for later dissecting/discovery

mdk3me.sh = spew out wifi-ssids (from test file, can be used to send out messages)

karmacheck.py = spew out random wifi probes to fill up logs if tracking is happening, or help detect a karma/pineapple attack

mdkdowngradetest.sh = test downgrades on wifi

nmapme.sh = nmap -sP local network

paper-- = scripts to detect HP printers w/ wireless direct on, and do stuff

Scripts - Bluetooth

eddystonebeacon.sh = generate eddystone URL beacon (wip – facebook beacons soon)

find_bt_hciname.sh = check for bluetooth addy (mac+1) via wifi mac

Scripts – Local Exploit / Video

mubix-lock.sh / linklocal-mubix-lock.sh = variations on sniffing locked Windows boxen

dropkick.sh = Detect and deauth wireless cameras

Scripts – Voice/VOIP

callsomeonesaysomething.sh = Call someone, spew voice-synth message.

ringmybell.sh = Call a number constantly.

asterisk minimal install = Minimal install that'll work on NetHunter on a Nexus5, supporting the above scripts.

Thanks for Listening

Questions/Suggestions/Additions/fixes?:
github.com/violentlydave // @violentlydave
Email in the code on Github.. Barely obfuscated.

- Thanks to the red team (Jonathan, Damian, Ian and Col Burger) and Joe.
- Thanks to some recent customers for providing interesting problems that lead to interesting ideas.
- Thanks for just dealing w/ me through the tests, interviews, papers and prepping for talks: my awesome wife, **Jaci**.