A Proactive Approach to Hunting for Phishing Websites

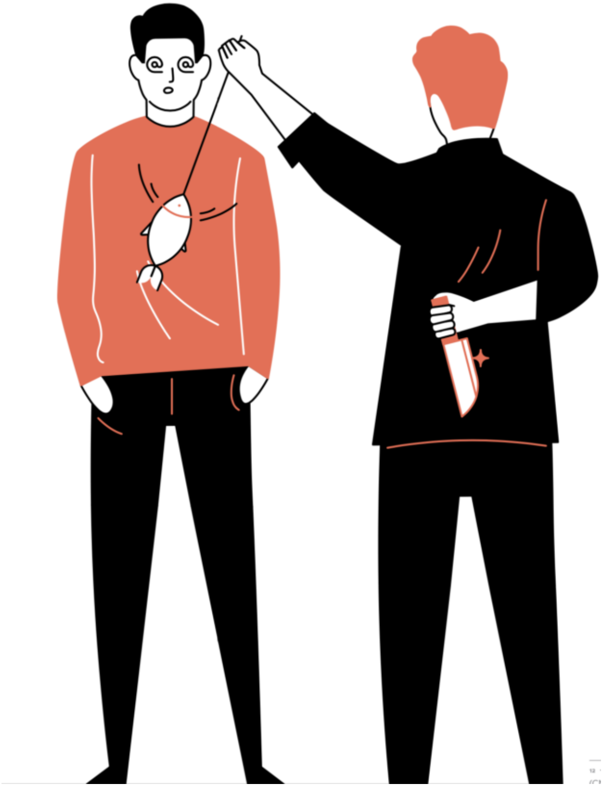
douglas_mun@csa.gov.sg

30 Sep 2019

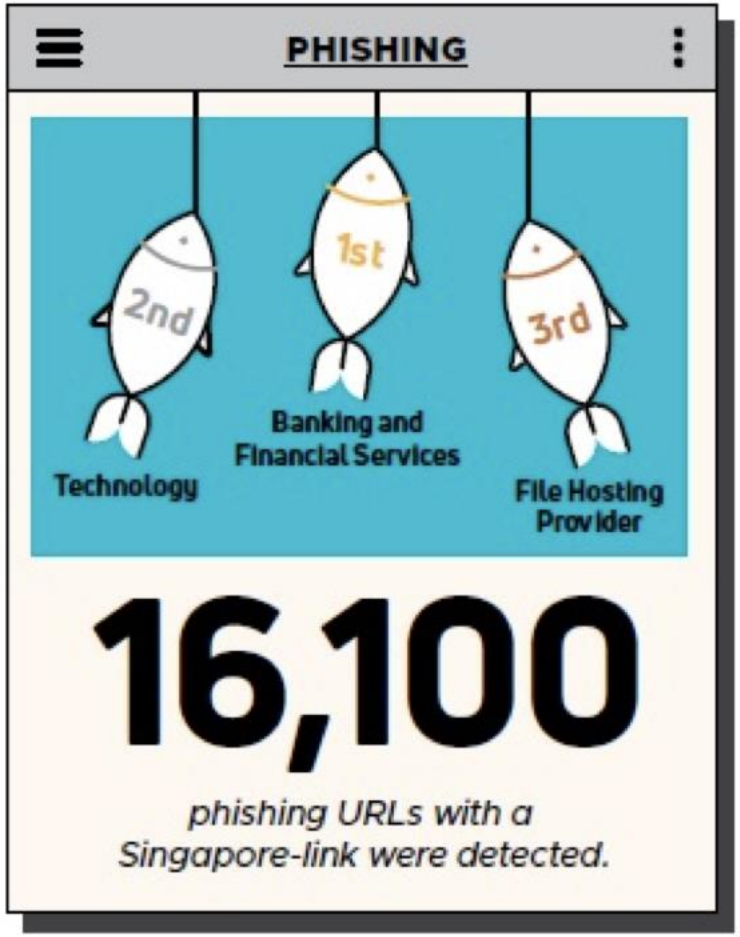
TLP: GREEN

Agenda

- Singapore's Cyber Landscape (Phishing)
- The Ever-Evolving Phishing Tactics
- Look into the increasing Phishing problem
- Proactive vs Reactive Hunt for Phishing Websites
- Proactive Hunting via DNS Zone Files
- Proactive Hunting via Certificate Transparency Log



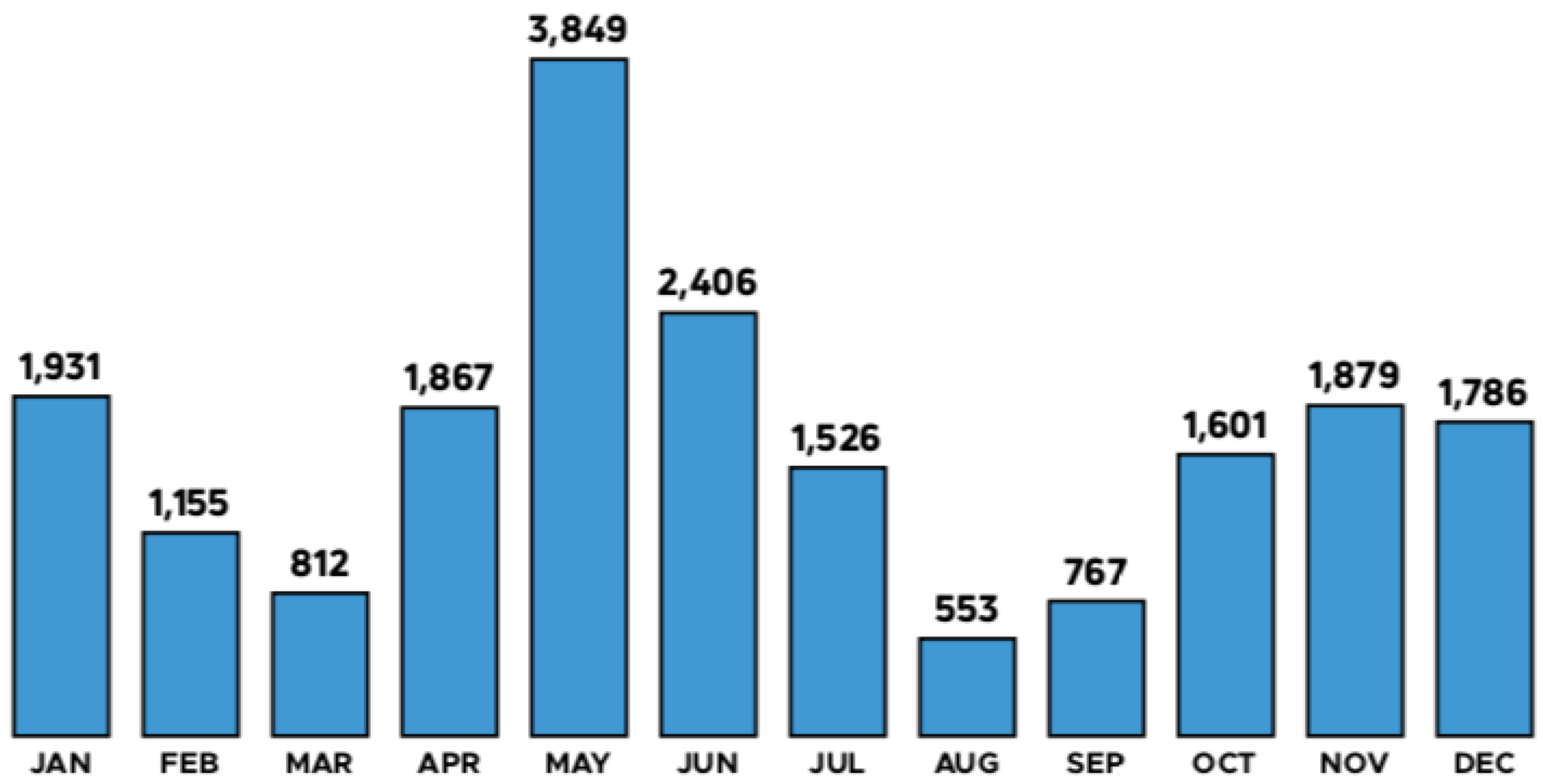
Phishing URLs with a Singapore-Link



16,100

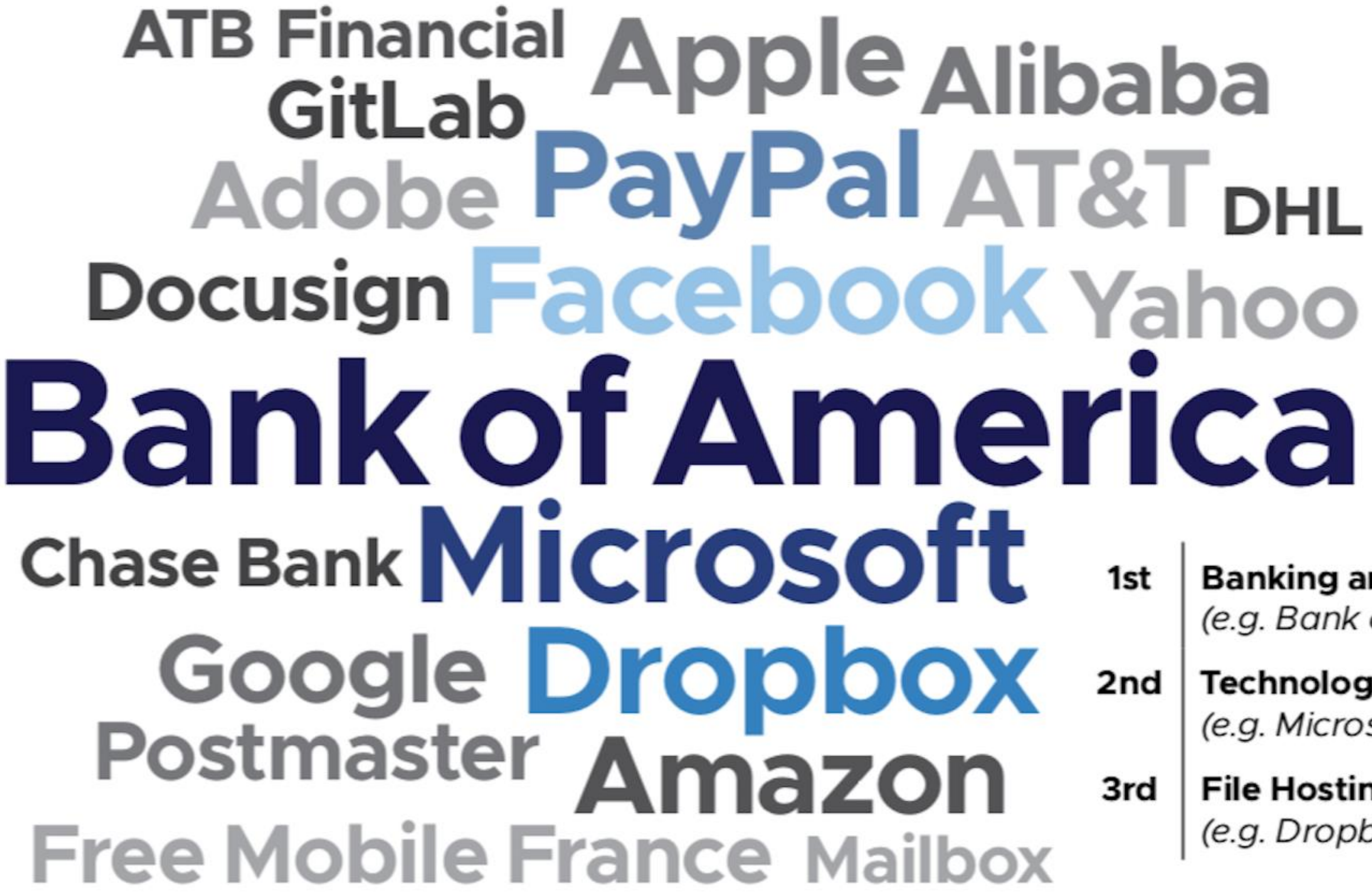
phishing URLs with a Singapore-link were detected.

NUMBER OF PHISHING URLS WITH A SINGAPORE-LINK OBSERVED IN 2018



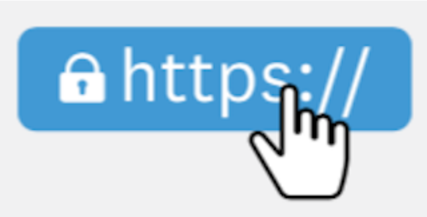
source: https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018

COMMONLY SPOOFED ORGANISATIONS IN 2018



1st	**Banking and Financial Services** *(e.g. Bank of America)*
2nd	**Technology** *(e.g. Microsoft)*
3rd	**File Hosting Services** *(e.g. Dropbox)*

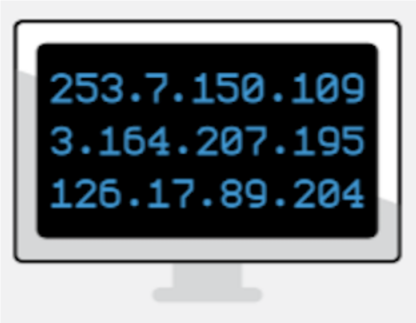
The Ever-Evolving Phishing Tactics



TAKING ADVANTAGE OF "HTTPS"

2,450 URLs using "HTTPS" in 2018, more than tenfold jump from 2017.

Using "HTTPS" – rather than "HTTP" – lures victims into a **false sense of security**, by having them believe that they were transacting on a secure website.



USE OF DYNAMIC DOMAIN NAME SYSTEM SERVICES (DDNS) SERVICES

210 URLs using DDNS in 2018, three times more than in 2017.

Such services enable malicious URL and IP address constantly to **evade blocking**.

LEVERAGING GENERIC TOP LEVEL DOMAINS (TLD)

Domains such as ".com" (8,100 URLs) and ".club" (700 URLs) were commonly abused.

Some TLD are cheap or even **free**. They **lack regulation**, allowing threat actors to constantly create new malicious URLs.

Look into the Increasing Phishing Problem

- Phishing attacks are **increasing in quantity worldwide**, affecting individuals and corporations

- Phishing **impacts people life**. Victims faced theft of identity, exposure of confidential data and even compromised of an entire corporate network. Some lost their entire life savings through a phishing scam

- Phishing **tactics are ever-evolving**, cyber-defenders play a difficult catch up game

- To better combat phishing and scams, a **more proactive approach** is needed to reduce the current time of taking down phishing websites from days to hours

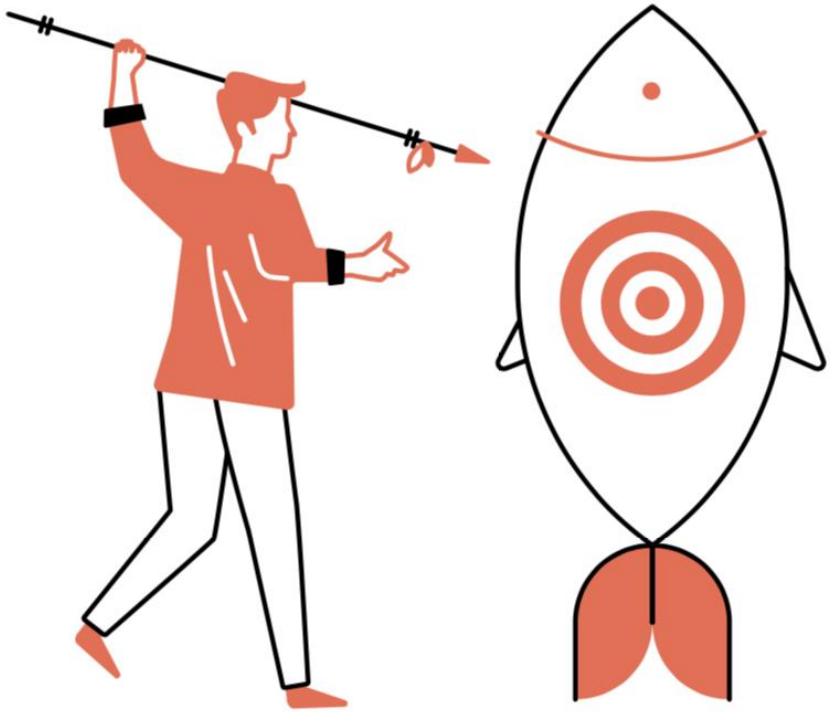
Proactive vs Reactive Hunt for Phishing Websites

- **Proactive**
  - Hunt for newly created suspicious websites
  - Raise take-down before phishing attacks made their impact

- **Reactive**
  - Depend on phishing alerts from member of the public and third parties anti-phishing feeds
  - Commonly available feeds are:

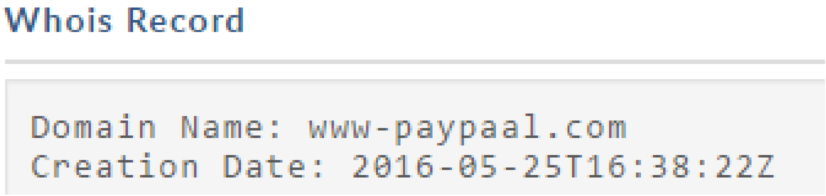
    PhishTank OpenPhish NETCRAFT

  - Detection is **reactive and laggard**. Alert and feed received are might be outdated



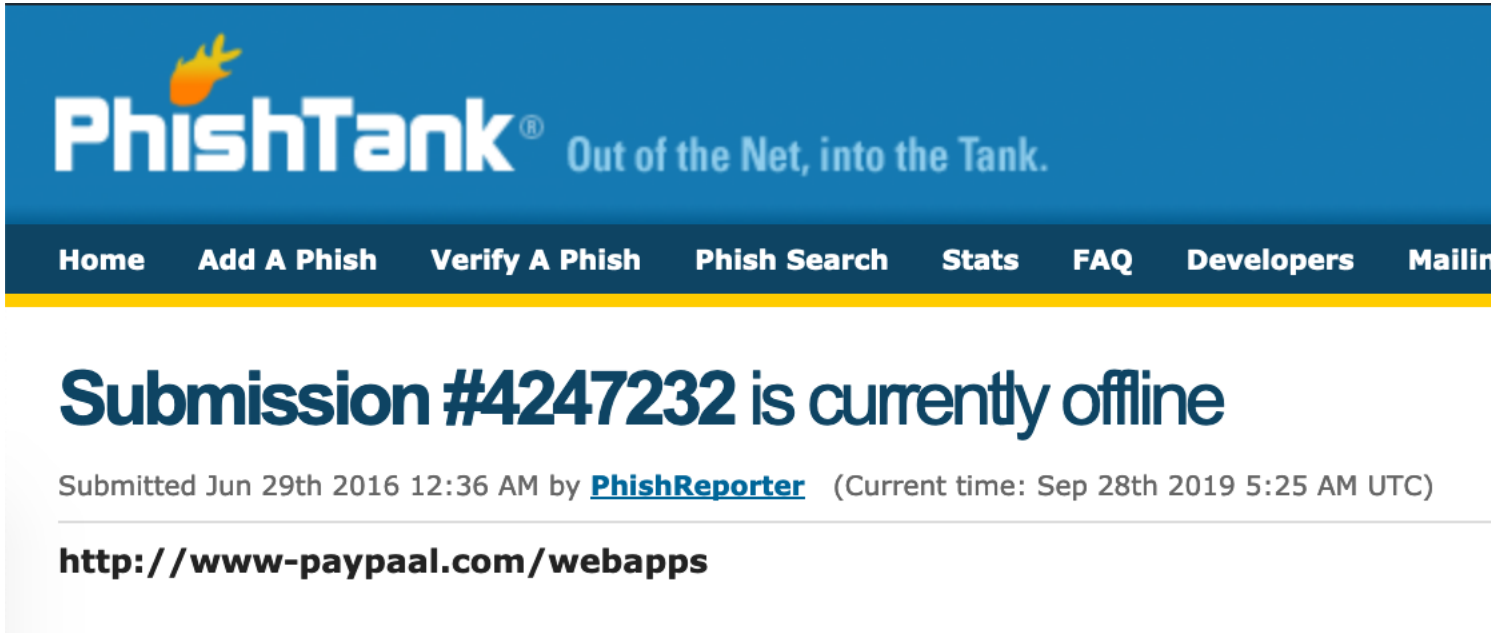
Reactive Example - PhishTank

- Phishing domain www-paypaal.com was registered on 25th May, but it was submitted to PhishTank **35 days later** on 29th June



Whois Record

```
Domain Name: www-paypaal.com
Creation Date: 2016-05-25T16:38:22Z
```



Submission #4247232 is currently offline

Submitted Jun 29th 2016 12:36 AM by PhishReporter (Current time: Sep 28th 2019 5:25 AM UTC)

http://www-paypaal.com/webapps

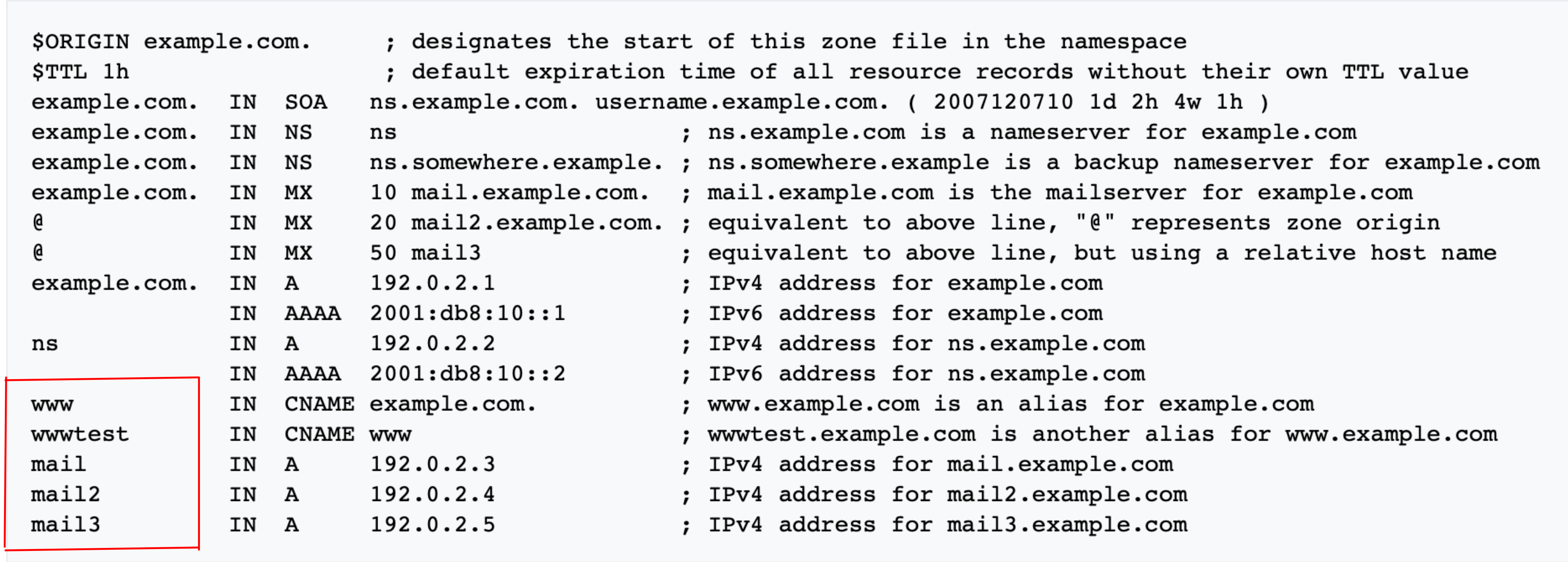
DNS Zone Files

```
01110010 01110011 01110000 01100001 01100011
01100101 01100001 01101110 01100100 01110011
01100101 01110100 01101111 01100111 01100101
01001100 01100101 01110100 01110101 01110011
01110011 01101001 01101110 01100111 01100001
01100011 01111001 01100010 01100101 01110010
01100101 01110011 01100001 01100110 01100101
01100101 01100011 01110101 01110010 01100101
01110100 01101000 01100101 01110010 01001100
01101011 01100101 01100101 01110000 01110011
```

What are DNS Zone Files

- A Domain Name System (DNS) zone file is a **text file** that describes a DNS zone. In this case, the DNS zone we refer to is a Top Level Domain (TLD) i.e. .com .club .top

- An example of a zone file for the domain example.com is the following:



```
$ORIGIN example.com.      ; designates the start of this zone file in the namespace
$TTL 1h                   ; default expiration time of all resource records without their own TTL value
example.com.  IN  SOA   ns.example.com. username.example.com. ( 2007120710 1d 2h 4w 1h )
example.com.  IN  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  IN  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver for example.com
example.com.  IN  MX    10 mail.example.com.  ; mail.example.com is the mailserver for example.com
@             IN  MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@             IN  MX    50 mail3              ; equivalent to above line, but using a relative host name
example.com.  IN  A     192.0.2.1             ; IPv4 address for example.com
              IN  AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            IN  A     192.0.2.2             ; IPv4 address for ns.example.com
              IN  AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           IN  CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       IN  CNAME www                   ; wwwtest.example.com is another alias for www.example.com
mail          IN  A     192.0.2.3             ; IPv4 address for mail.example.com
mail2         IN  A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         IN  A     192.0.2.5             ; IPv4 address for mail3.example.com
```

How to obtain Zone Files for Proactive Hunting

- Obtain TLD Zone Files from ICANN Registries to detect domains registration
  - https://czds.icann.org/en
  - https://www.verisign.com/en_US/channel-resources/domain-registry-products/zone-file/index.xhtml

- Utilise available Whois Registrant details to conduct further investigation
  - https://community.riskiq.com
  - https://whois.domaintools.com
  - https://domainbigdata.com

Using Zone Files for Proactive Hunting

- VeriSign Global Registry Services is the ICANN assigned registry operator for the Top-Level Domain (TLD) **.com**

- To date, there are more than 156 million registered **.com** domains (Sep 2019)

- We focused our effort on **.com** sites as this TLD domains are more susceptible to phishing abuses

- **Our Method**
  1. Download the zone file from VeriSign ftp site
  2. Select out newly registered but highly suspicious domains
  3. Verify if highly suspicious domains are hosting phishing sites
  4. File take down report if it is a phishing site exists

1. **Download .COM zone file, verify its md5 checksum**

```
ftp://rz.verisign-grs.com/com.zone.gz  &  ftp://rz.verisign-grs.com/com.zone.gz.md5
cat com.zone.gz.md5  & md5 com.zone.gz
```

2. **Extracts domain names from the zone file**

```
awk '{print $1}' com.zone.26690 > com.zone.1
sort -u com.zone.1 > com.zone.2
egrep '^[A-Z0-9]([A-Z0-9\-]{0,61}[A-Z0-9])?$' com.zone.2 > com.zone.3
awk '{print $1".COM"}' com.zone.3 > com.zone.4
```

3. **Filter out newly created or updated domains**

```
diff /old/com.zone.4 /new/com.zone.4 > diff1.txt
grep '>' diff1.txt > diff2.txt
sed 's,> ,,' diff2.txt > diff3.txt
```

4. **Search for domain that matches your brand**

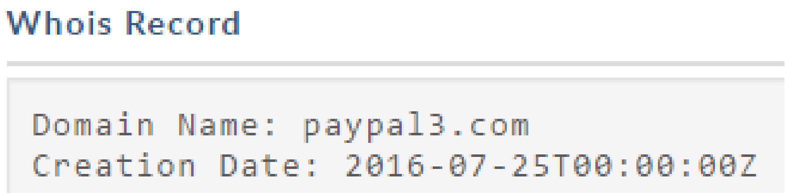
```
grep ^PAY.*PAL diff3.txt > list1.txt   (or ) create a search.txt
for domain in $(cat search.txt) ; do grep $domain diff3.txt >> list1.txt ; done
```

5. **Probe for active domain/website** *(usually HTTP CODE 200 OK) Open websites on default browser for visual check.*

```
for url in $(cat list1.txt) ; do curl --max-time 6 -sL -w "%{http_code} %{url_effective}\\n" "$url" -o /dev/null; done >
list2.txt
grep "^200" list2.txt > list3.txt
sed 's,200 ,,' list3.txt > list4.txt
for url in $(cat list4.txt) ; do open $url ; done
```

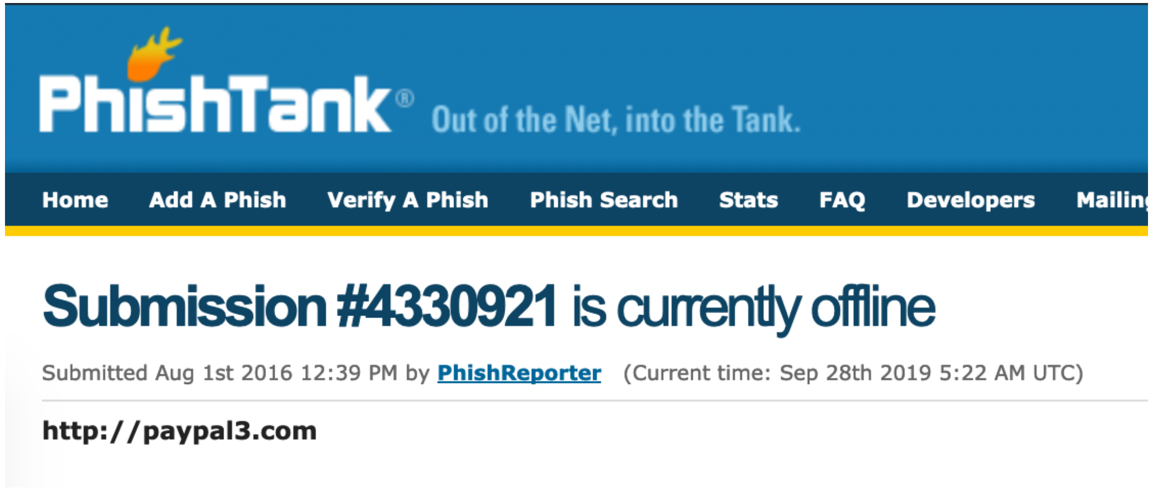
Proactive Example - DNS Zone File

- Phishing domain paypal3.com was created on 25th July, SingCERT detected it using Zone file two days later on 27th July. Someone submitted to PhishTank on 1st Aug



Whois Record

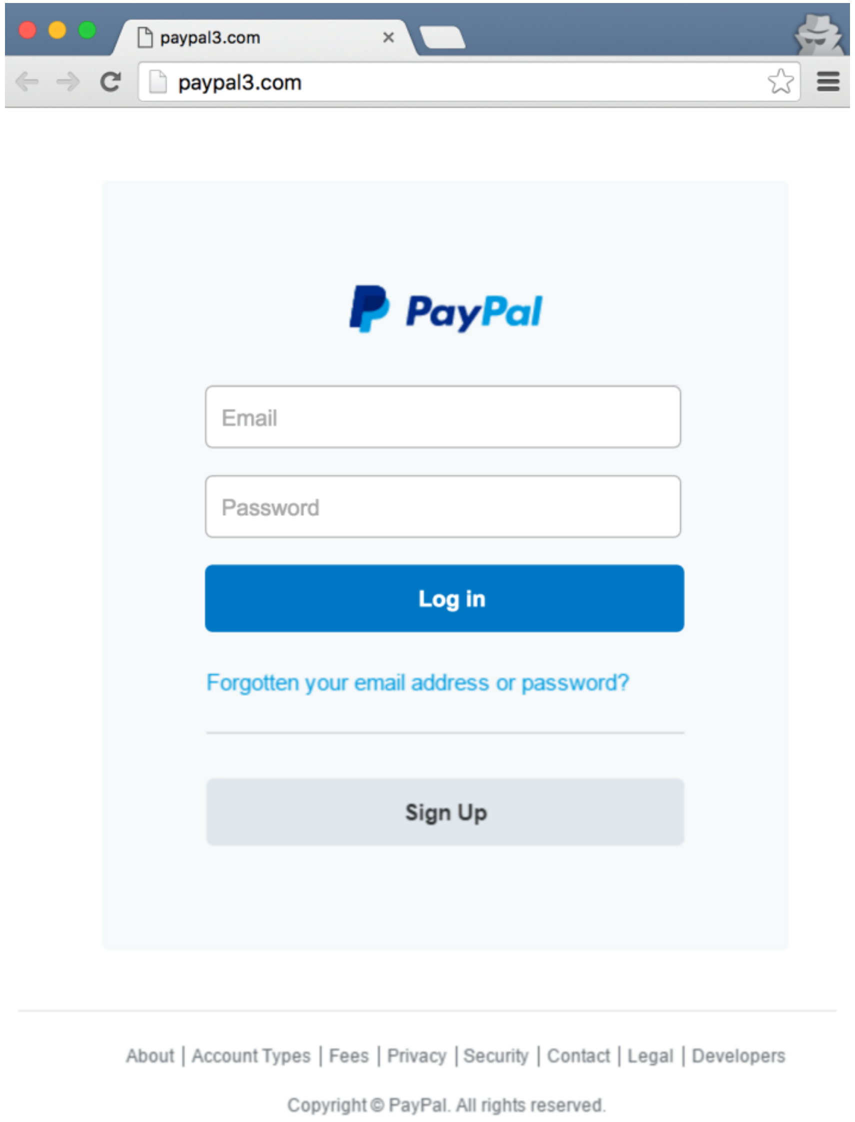
```
Domain Name: paypal3.com
Creation Date: 2016-07-25T00:00:00Z
```



Submission #4330921 is currently offline

Submitted Aug 1st 2016 12:39 PM by PhishReporter (Current time: Sep 28th 2019 5:22 AM UTC)

http://paypal3.com

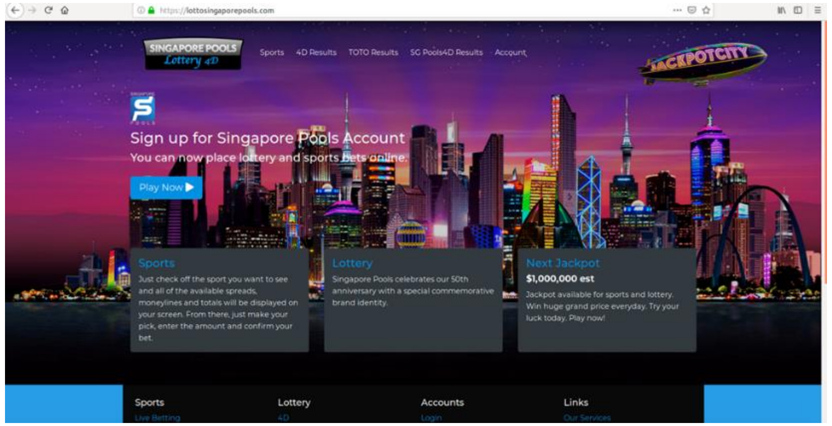


paypal3.com
paypal3.com
PayPal
Email
Password
Log in
Forgotten your email address or password?
Sign Up
About | Account Types | Fees | Privacy | Security | Contact | Legal | Developers
Copyright © PayPal. All rights reserved.

More Proactive Example - DNS Zone File

- On first run using zone file, SingCERT detected **three** fake SingaporePools phishing websites targeting Singaporeans to sign up for an online betting account

- All three fakes websites were taken offline on the next business day



https://lottosingaporepools.com

Sign up for Singapore Pools Account

You can now place lottery and sports bets online.

Sports

Just check off the sport you want to see and all of the available spreads, moneylines and totals will be displayed on your screen. From there, just make your pick, enter the amount and confirm your bet.

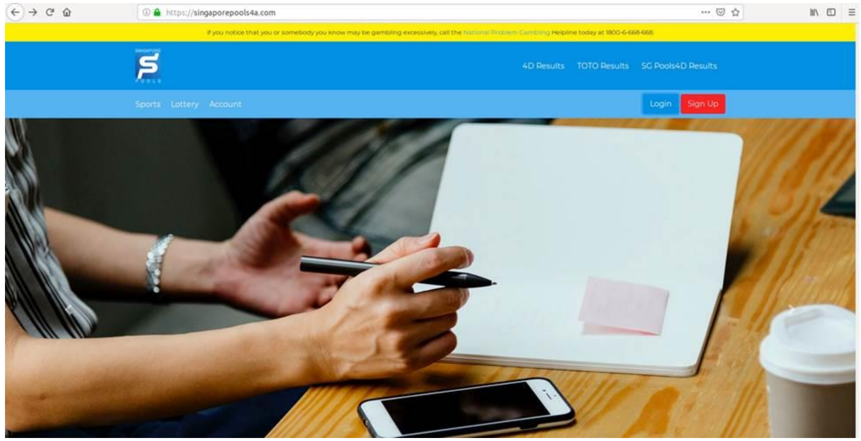
Lottery

Singapore Pools celebrates our 50th anniversary with a special commemorative brand identity.

Next Jackpot

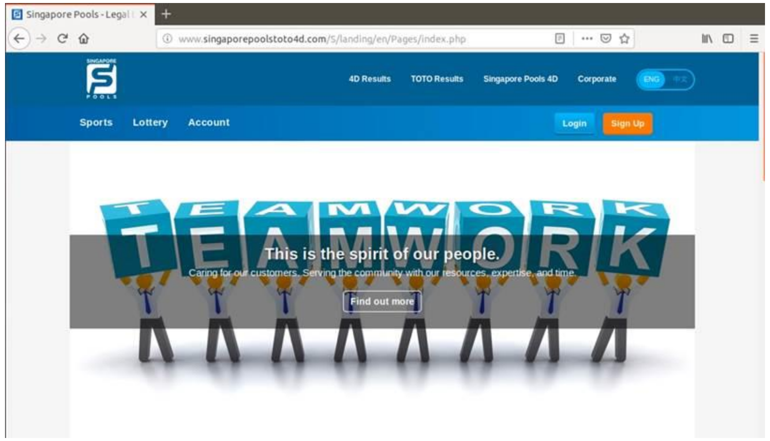
$1,000,000 est

Jackpot available for sports and lottery. Win huge grand price everyday. Try your luck today. Play now!



https://singaporepools4a.com

If you notice that you or somebody you know may be gambling excessively, call the National Problem Gambling Helpline today at 1800-6-668-668.



Singapore Pools - Legal

www.singaporepoolstoto4d.com/S/landing/en/Pages/index.php

This is the spirit of our people.

Caring for our customers. Serving the community with our resources, expertise, and time.

Certificate Transparency Logs

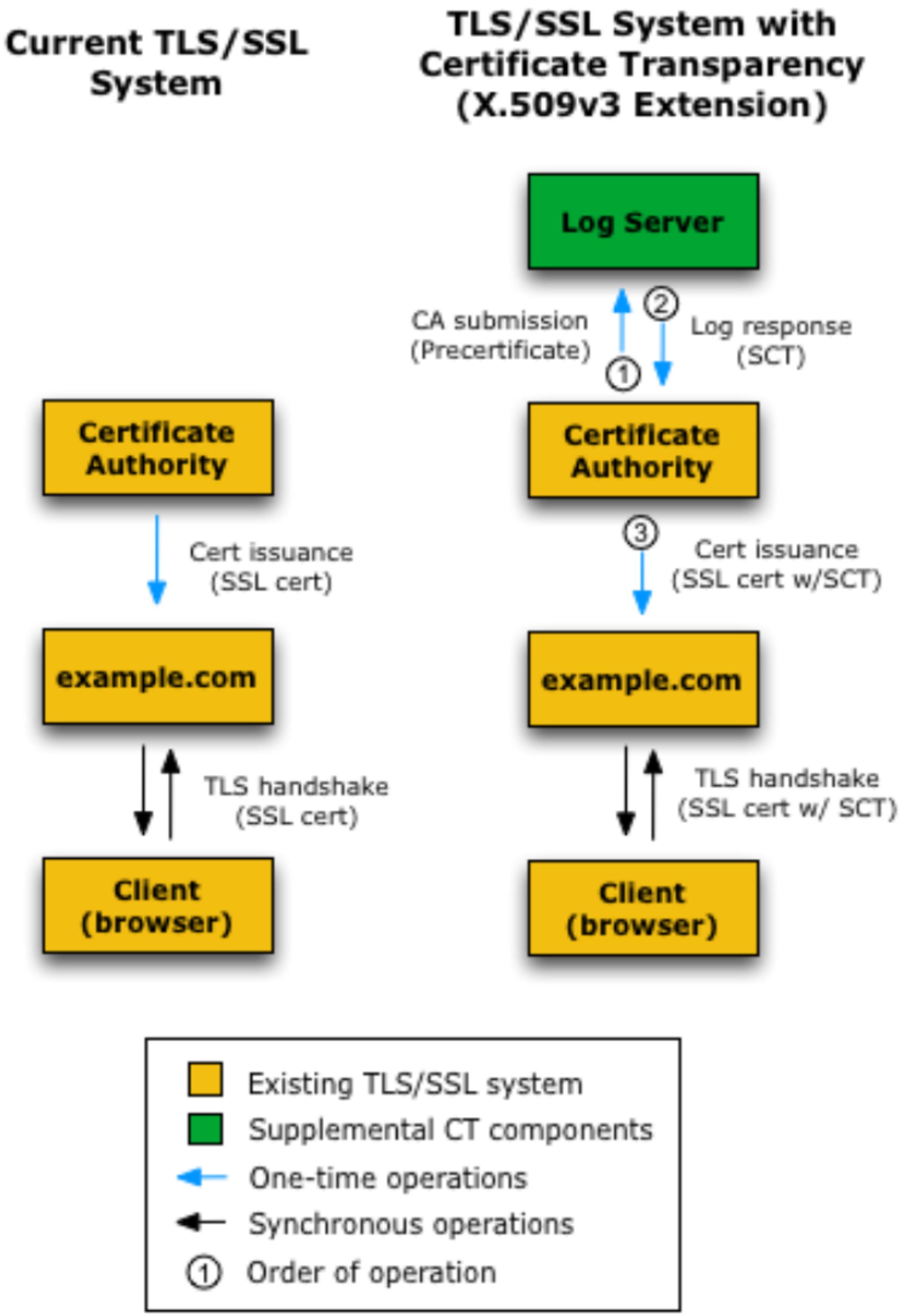
Certificate Transparency (CT)

- **Certificate Transparency** (CT) adds three new functional components to the current SSL certificate system: (i) Certificate logs, (ii) Certificate monitors and (iii) Certificate auditors

- **Certificate Log** is a simple network service that maintains a record of SSL certificates with three important qualities: (i) append-only, (ii) cryptographically assured and (iii) publicly auditable

- **Contributors**: Google, Cloudflare, DigiCert, Certly, Sectigo/Comodo, WoSign, Venafi, CNNIC, StartCom

source: http://www.certificate-transparency.org/how-ct-works
https://developers.facebook.com/docs/certificate-transparency

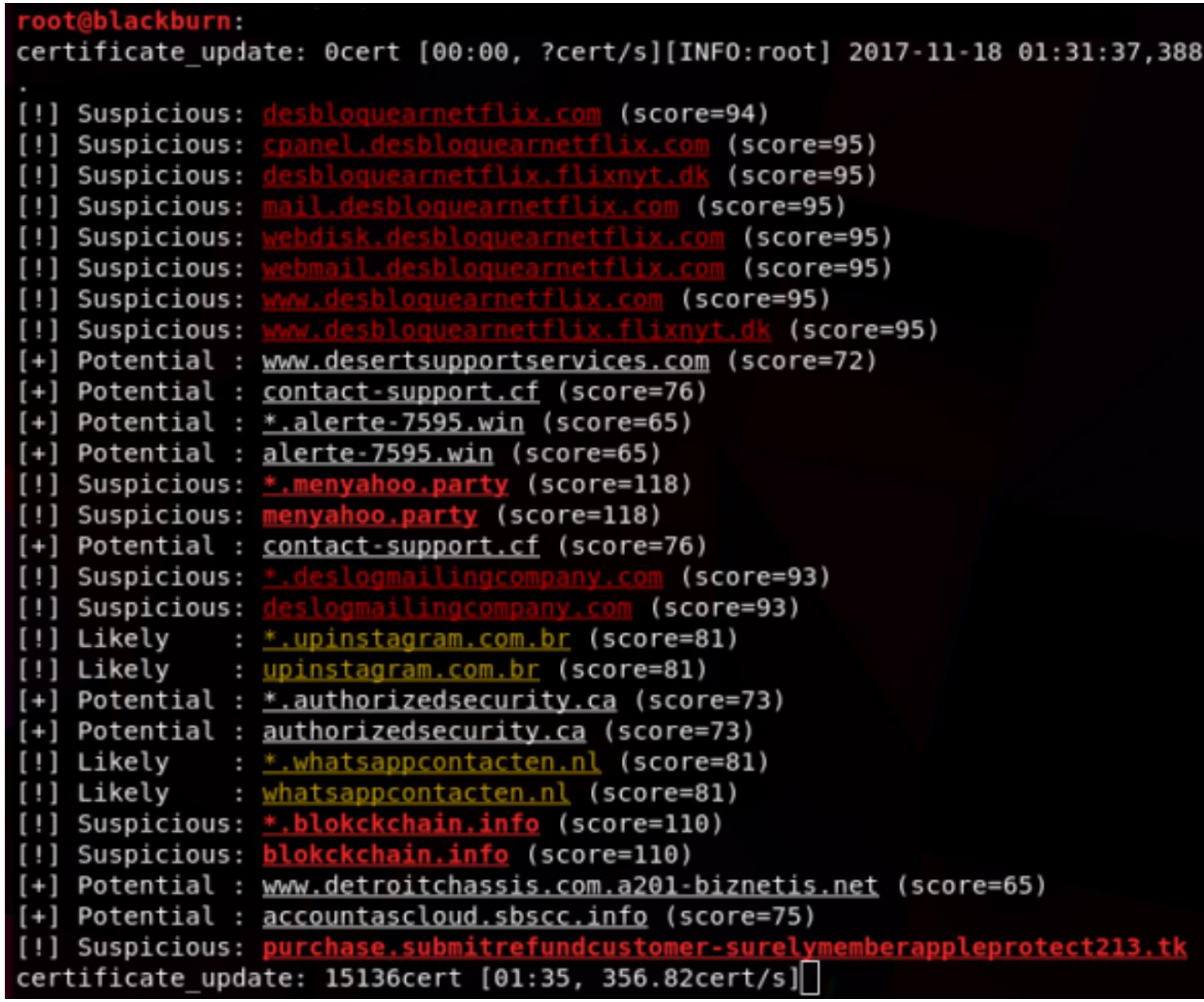


Using CertStream for Proactive Hunting

- **CertStream** is a python script that provides real-time feed from the Certificate Transparency Log networks

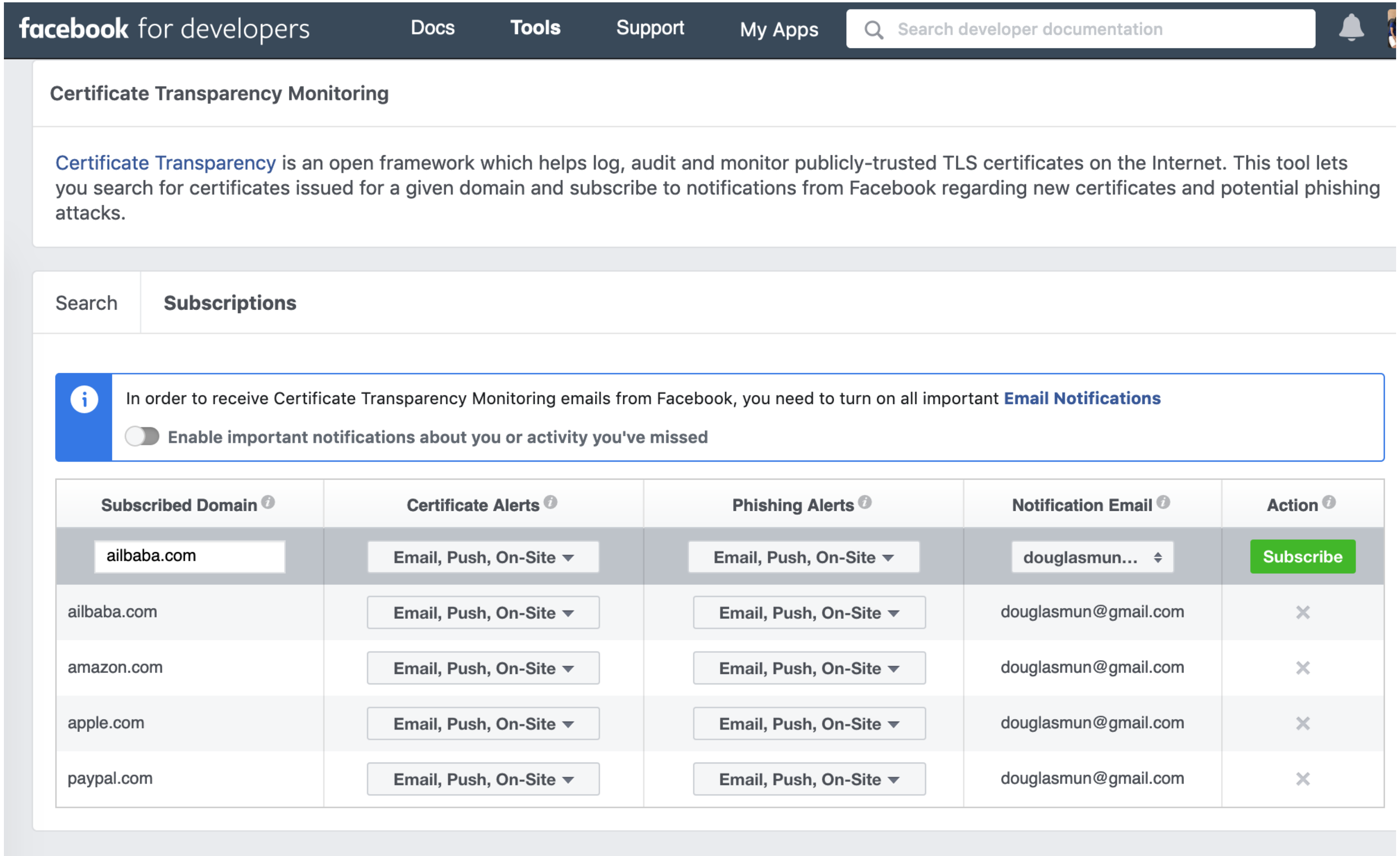
- It observes newly issued and existing renewed certificates and give a phishing risk rating (i.e. Potential, Likely, Suspicious)

- **Our Method**
  1. Run CertStream to hunt for suspicious SSL certificate issued to websites
  2. Verify if suspicious URLs are phishing sites
  3. Report for take down if it is a phishing site



```
root@blackburn:
certificate_update: 0cert [00:00, ?cert/s][INFO:root] 2017-11-18 01:31:37,388
.
[!] Suspicious: desbloquearnetflix.com (score=94)
[!] Suspicious: cpanel.desbloquearnetflix.com (score=95)
[!] Suspicious: desbloquearnetflix.flixnyt.dk (score=95)
[!] Suspicious: mail.desbloquearnetflix.com (score=95)
[!] Suspicious: webdisk.desbloquearnetflix.com (score=95)
[!] Suspicious: webmail.desbloquearnetflix.com (score=95)
[!] Suspicious: www.desbloquearnetflix.com (score=95)
[!] Suspicious: www.desbloquearnetflix.flixnyt.dk (score=95)
[+] Potential : www.desertsupportservices.com (score=72)
[+] Potential : contact-support.cf (score=76)
[+] Potential : *.alerte-7595.win (score=65)
[+] Potential : alerte-7595.win (score=65)
[!] Suspicious: *.menyahoo.party (score=118)
[!] Suspicious: menyahoo.party (score=118)
[+] Potential : contact-support.cf (score=76)
[!] Suspicious: *.deslogmailingcompany.com (score=93)
[!] Suspicious: deslogmailingcompany.com (score=93)
[!] Likely     : *.upinstagram.com.br (score=81)
[!] Likely     : upinstagram.com.br (score=81)
[+] Potential : *.authorizedsecurity.ca (score=73)
[+] Potential : authorizedsecurity.ca (score=73)
[!] Likely     : *.whatsappcontacten.nl (score=81)
[!] Likely     : whatsappcontacten.nl (score=81)
[!] Suspicious: *.blokckchain.info (score=110)
[!] Suspicious: blokckchain.info (score=110)
[+] Potential : www.detroitchassis.com.a201-biznetis.net (score=65)
[+] Potential : accountascloud.sbscc.info (score=75)
[!] Suspicious: purchase.submitrefundcustomer-surelymemberappleprotect213.tk
certificate_update: 15136cert [01:35, 356.82cert/s]
```

Using Facebook CT for Proactive Hunting



Certificate Transparency Monitoring

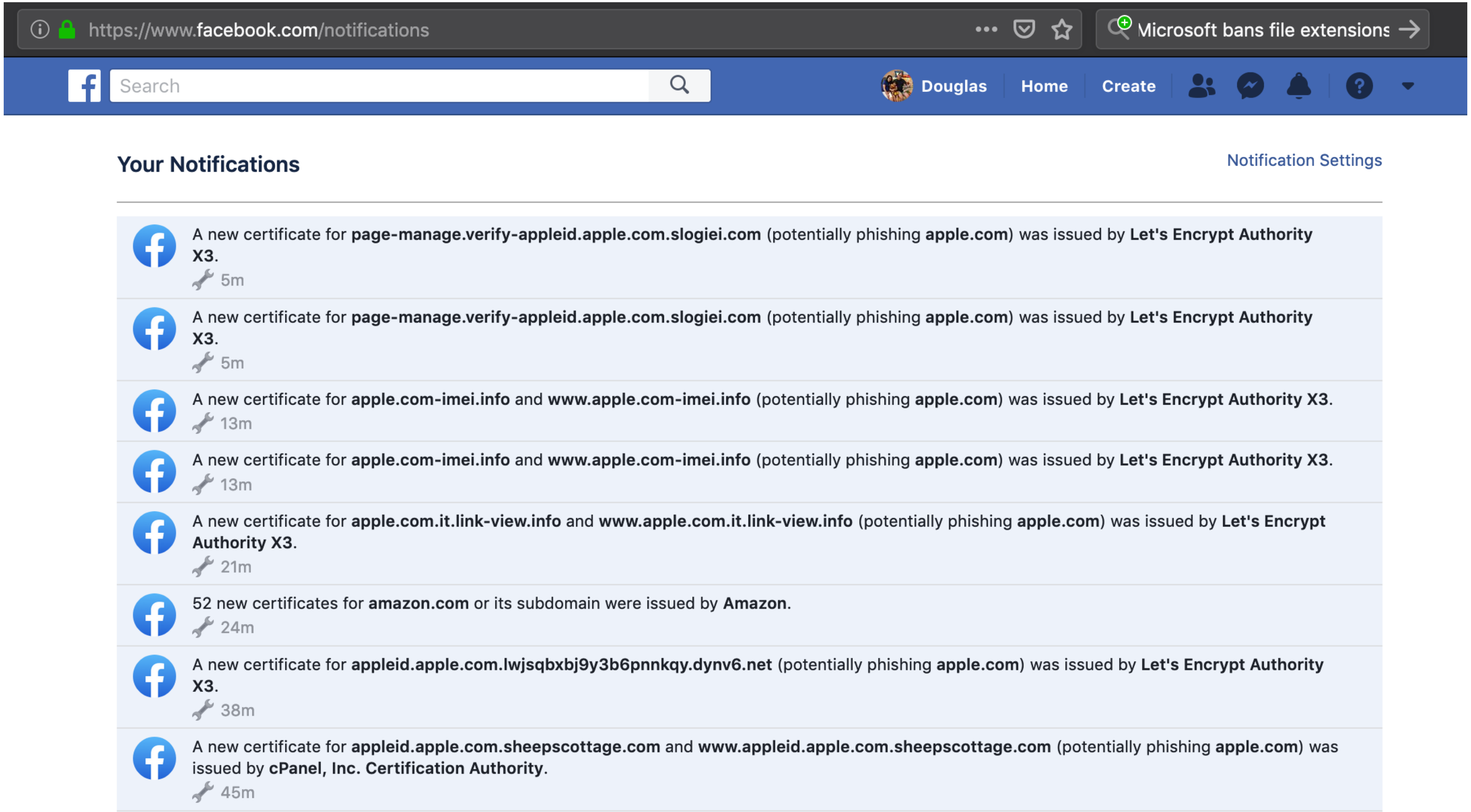
Certificate Transparency is an open framework which helps log, audit and monitor publicly-trusted TLS certificates on the Internet. This tool lets you search for certificates issued for a given domain and subscribe to notifications from Facebook regarding new certificates and potential phishing attacks.

In order to receive Certificate Transparency Monitoring emails from Facebook, you need to turn on all important **Email Notifications**

Enable important notifications about you or activity you've missed

Subscribed Domain	Certificate Alerts	Phishing Alerts	Notification Email	Action
ailbaba.com	Email, Push, On-Site	Email, Push, On-Site	douglasmun...	Subscribe
ailbaba.com	Email, Push, On-Site	Email, Push, On-Site	douglasmun@gmail.com	✕
amazon.com	Email, Push, On-Site	Email, Push, On-Site	douglasmun@gmail.com	✕
apple.com	Email, Push, On-Site	Email, Push, On-Site	douglasmun@gmail.com	✕
paypal.com	Email, Push, On-Site	Email, Push, On-Site	douglasmun@gmail.com	✕

Proactive Example - Certificate Transparency Logs



https://www.facebook.com/notifications
Microsoft bans file extensions
Search
Douglas
Home
Create

Your Notifications

Notification Settings

A new certificate for **page-manage.verify-appleid.apple.com.slogiei.com** (potentially phishing **apple.com**) was issued by **Let's Encrypt Authority X3**.
5m

A new certificate for **page-manage.verify-appleid.apple.com.slogiei.com** (potentially phishing **apple.com**) was issued by **Let's Encrypt Authority X3**.
5m

A new certificate for **apple.com-imei.info** and **www.apple.com-imei.info** (potentially phishing **apple.com**) was issued by **Let's Encrypt Authority X3**.
13m

A new certificate for **apple.com-imei.info** and **www.apple.com-imei.info** (potentially phishing **apple.com**) was issued by **Let's Encrypt Authority X3**.
13m

A new certificate for **apple.com.it.link-view.info** and **www.apple.com.it.link-view.info** (potentially phishing **apple.com**) was issued by **Let's Encrypt Authority X3**.
21m

52 new certificates for **amazon.com** or its subdomain were issued by **Amazon**.
24m

A new certificate for **appleid.apple.com.lwjsqbxbj9y3b6pnnkqy.dynv6.net** (potentially phishing **apple.com**) was issued by **Let's Encrypt Authority X3**.
38m

A new certificate for **appleid.apple.com.sheepscottage.com** and **www.appleid.apple.com.sheepscottage.com** (potentially phishing **apple.com**) was issued by **cPanel, Inc. Certification Authority**.
45m

Thank You!