VII Venice AppSec

In collaborazione con

Venezia, Università Ca’ Foscari
3 Ottobre 2019
Mariano Graziano

Fishing phishing attempts
- Technical Leader in Cisco Talos
- PhD in System Security (Eurecom)
- Binary/Malware Analysis, Memory forensics, Automation
Why phishing?
Phishing

- 1996 the first time the term “phishing” is used online
- Users have an online life and more and more credentials
1996 the first time the term “phishing” is used online

Users have an online life and more and more credentials
Phishing

- 1996 the first time the term “phishing” is used online
- Users have an online life and more and more credentials

Banking apps

Electricity/Energy

Music (Spotify/Deezer, etc)

Gym

Console
Phishing

- 1996 the first time the term “phishing” is used online
- Users have an online life and more and more credentials
- Years of research and many products but it is still an open problem
Phishing evolution

Quality

Massive

Targeted

t
Phishing evolution

Quality

Massive

Low quality

High quality

Targeted

t
Phishing evolution

Means
- SMS
- IM apps
- Documents
- Compromised websites
- Registered websites
- Emails
- Social networks
Phishing evolution

Complexity

- Anti-analysis tricks
- Homograph attacks
- Twitter campaigns
- DNS/BGP hijacking

$t$
Phishing evolution

**Complexity**

- Anti-analysis tricks
- Homograph attacks
- Twitter campaigns
- DNS/BGP hijacking

- icloud.com
- paypal.org
Phishing evolution

Hacker Hijacks DNS Server of MyEtherWallet to Steal $160,000

By Catalin Cimpanu

DNS Poisoning or BGP Hijacking Suspected Behind Trezor Wallet Phishing Incident

By Catalin Cimpanu

The team behind the Trezor multi-cryptocurrency wallet service has discovered a phishing attack against some of its users that took place over the weekend.

The Trezor team says "signs point toward DNS poisoning or BGP hijacking" as the means attackers hijacked legitimate traffic meant for the official wallet.trezor.io domain but redirected these users to a malicious server hosting a fake website. An investigation is still underway to determine the exact cause.

A hacker (or group of hackers) has hijacked the DNS servers of MyEtherWallet.com, a web-based Ether wallet service.

Users accessing the site were redirected to a fake version of the website. Those who logged in had their wallet private keys stolen, which the attacker used to empty accounts.
Phishing evolution

**Categories**

- Basic Credential phishing
- Credential phishing with 2FA
- Spear phishing
- OAuth phishing
Phishing evolution

**Protocol**

HTTP

HTTPS
Phishing evolution

https://letsencrypt.org/stats/ -- via Firefox Telemetry
Credential phishing

Impersonate a legitimate website to steal user’s credentials

**phishing**

/ˈfiʃhɪŋ/

noun

the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

"an email that is likely a phishing scam"

Phishing - Wikipedia

[https://en.wikipedia.org/wiki/Phishing](https://en.wikipedia.org/wiki/Phishing)

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
Credential phishing

Impersonate a legitimate website to steal user’s credentials

What is phishing?

Credentials phishing (or “Password-Stealing Phishing”) consists in the creation of a website that imitates the login prompt of a given online service, such as Gmail or Facebook, with the objective of luring a victim into visiting the malicious page and entering their username and passwords, thereby transmitting these credentials to the attackers.

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Credential phishing
Credential phishing

[Image] A phishing email or website designed to look like a legitimate PayPal login page, prompting the user to enter their email or mobile number and password. The URL is indicated as 'paypal.login.ufence.click', which is a dangerous link.
Credential phishing

original

fake
Credential phishing

original

1 form

fake

2 forms
Credential phishing

1 form

```html
<form action="/signin" method="post" class="proceed maskable" autocomplete="off" name="login"autocomplete="off" novalidate>
    Email or mobile number
    Next
</form>
```

2 forms

```html
<form action="post.php" method="post" class="" autocomplete="off" name="login"autocomplete="off" novalidate>
    Email or mobile number
    Password
    Log In
    or
    
</form>
```
Credential phishing

REQUIREMENTS:

• Web server:
  • Self hosted
  • Free/Paid
  • Compromised

• Phishing kit

• Distribution:
  • Emails, Social media, etc..
Phishing kit

- Kit to deploy a phishing website
- It may contain “filters” to avoid detection
Phishing kit

• How do they steal credentials?
Phishing kit

- How do they steal credentials?

```php
<?php if(isset($_GET['error'])){ if ($_GET['error'] == "true") { echo "
<form class="form-signin" style="padding:16px;" id="fr1m" name="login_form" method="post" action="loginNext.php">
</form>
</div>
<br /></"; }
```
Phishing kit

• How do they steal credentials?
Phishing kit

- How do they steal credentials?

```php
$user_agent = $_SERVER['HTTP_USER_AGENT'];
$browser = $_SERVER['HTTP_ACCEPT_LANGUAGE'];
$SESSION['_browser'] = $browser;
$subject = "PayPal Login True - [ "._SESSION['cntname'] . " / "._SESSION['_IP']." ] ";
$headers = "MIME-Version: 1.0 "; "\n"
$headers .= "Content-type:text/html; charset=UTF-8 "; "\n"
$headers .= "From: Yeni T/Login <Tlogging@mailfahad.com>";
$message = "

ą
ę
ł
ń
ó
ś
ż
`
```
Phishing kit

• How do they avoid detection?
Phishing kit

- How do they avoid detection? .htaccess
Phishing kit

- How do they avoid detection? .htaccess
Phishing kit

- How do they avoid detection? .htaccess

```plaintext
125 deny from shadowserver.org
126 deny from datasift.com
127 deny from ebay.com
128 deny from internetbs.net
129 deny from apple.com
130 deny from env=stealthed
131 deny from firefox.com
132 deny from google.com
133 deny from paypal.com
134 deny from datasift.com
135 deny from google-cache.google.co.jp
136 deny from google-cache.google.com
137 deny from googlecache.google.com
138 deny from googlecache.google.co.jp
139 deny from mozorg.dynect.mozilla.net
140 deny from www.mozilla.org.cdn.cloudflare.net
141 deny from log-334788911.us-east-1.elb.amazonaws.com
142 deny from avast.com.edgekey.net
```
**Phishing kit**

- How do they avoid detection? .htaccess

```
```

```
RewriteRule .* - [F,L]
```
Phishing kit

- How do they avoid detection? php
Phishing kit

- How do they avoid detection? VPN?
Hunting

- What can we hunt?
  - Phishing kits
  - New domains
Hunting

- What can we hunt?
  - Phishing kits

![Directory Listing](image-url)
Hunting

- What can we hunt?
  - Phishing kits

[Image of web browser displaying the directory of www.plankstoere.xyz]

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>PayPal Checker - Madhacker</td>
<td>17-May-2019 22:48</td>
<td>-</td>
</tr>
<tr>
<td>paypal</td>
<td>17-May-2019 22:54</td>
<td>-</td>
</tr>
<tr>
<td>paypal.zip</td>
<td>17-May-2019 22:54</td>
<td>1960k</td>
</tr>
<tr>
<td>index</td>
<td>17-May-2019 22:02</td>
<td>348k</td>
</tr>
</tbody>
</table>

Proudly Served by LiteSpeed Web Server at www.plankstoere.xyz Port 80

https://twitter.com/nullcookies/status/1141144897174560768
Hunting

- What can we hunt?
  - Phishing kits
Hunting

• Phishing kits:

  • StalkPhish - The Phishing kits stalker, harvesting phishing kits for investigations by tAd
  • Miteru - An experimental phishing kit detection tool by ninoseki
  • Phish-collect - Python script to hunt phishing kits by duolabs
Hunting

- Phishing kits:

- StalkPhish - The Phishing kits stalker, harvesting phishing kits for investigations by tAd

**OSINT modules:**
- urlscan.io search API
- urlquery.net search web crawler
- Phishtank free OSINT feed (with or without API key)
- Openphish free OSINT feed
- PhishStats search API

**tools/download.py:**
```
rhtml = requests.get(siteURL, headers=user_agent, proxies=proxies, allow_redirects=True, timeout=(5, 12), verify=False)
Ziplst += [siteURL + '/' + tag['href'] for tag in thmlatag if '.zip' in tag.text]
```
Hunting

- Phishing kits:

- StalkPhish - The Phishing kits stalker, harvesting phishing kits for investigations by tAd

**config/example:**

```
[SEARCH]
# External source keywords to search for (keywords separated by a comma)
search = whatever,you,want
```
Hunting

• Phishing kits:

• StalkPhish - The Phishing kits stalker, harvesting phishing kits for investigations by tAd

config/example:
[SEARCH]
# External source keywords to search for (keywords separated by a comma)
search = whatever,you,want

http_proxy = socks5h://
Hunting

- Phishing kits:

- StalkPhish - The Phishing kits stalker, harvesting phishing kits for investigations by tAd

```
config/example:
[SEARCH]
# External source keywords to search for (keywords separated by a comma)
search = whatever,you,want

http_proxy = socks5h://

# StalkPhish's default user-agent (don't remove):
http_UA = Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.91 Safari/537.36
# Use a HTTP user-agents file to use for phishing kits HTTP Get informations
UAfile =
```
Hunting

- Phishing kits:

- StalkPhish - The Phishing kits stalker, harvesting phishing kits for investigations by tAd

```
config/example:
[SEARCH]
# External source keywords to search for (keywords separated by a comma)
search = whatever,you,want

http_proxy = socks5h://

# StalkPhish's default user-agent (don't remove):
http_UA = Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.91 Safari/537.36
# Use a HTTP user-agents file to use for phishing kits HTTP Get informations
UAfile =
```
Hunting

Complete paypal spamming phishing and cashing out pack

Price: $ 50 / 0.005880 BTC / 0.879458 LTC / 0.860659 XMR / 0.277534 ETH

Complete paypal spamming phishing and cashing out pack

Price: $ 50
Transaction type: Escrow
Payment method: Bitcoin, Litecoin, Monero, Ethereum
Ships From: Not Specified
Category: PayPal
Stock Remaining: 9999

In this pack you will find everything you need to make paypal spamming and phishing and then cashout the money in the accounts you will get.

- The pack contains:
- A big and fresh mail list
- Many well designed letters to send to your victims with adress, copyright, logos...

Paypal scamper
- A list of good and free host servers for the scamperages
- Mailers
- Phishing tutorials
- And cashout tutorials

http://silkroadjuwsx3nq.onion/?listing=kmpvFoTgYfKUaq2f8T6qKtpMrM6o5RO12zd5G6afamz2QrXO9S3JAf1NacdtrTj
Hunting

• What can we hunt?
  • New domains (CTL, Passive DNS, etc)
Hunting

Certificate Transparency Logs (CTL):

- 3 goals:
  - Certificate for a domain always visible to the owner of that domain
  - Provide an open and monitoring system to detect malicious or mistakenly issued certs
  - Protect users from malicious certificates

https://www.certificate-transparency.org/how-ct-works
Certificate Transparency Logs (CTL):

- Certificate Authorities (CAs) logs all the certificates they have issued to open CT log servers
- There was no easy way to detect a cert issued by a compromised CA/mistake
- Users/companies/researchers can inspect these logs and find suspicious entries
- Browsers require CT proof to have the green padlock (starting with EV certificates in 2015)
- CT logs cannot be deleted and modified in any way
- We can extract domains by parsing the logs:
  - Common Name (CN) field
  - Subject Alternative Name (SAN) field (optional)

https://www.certificate-transparency.org/how-ct-works
Hunting

- **CTL:**

Certificate Transparency è un framework aperto che aiuta a registrare, controllare e monitorare tutti i certificati TLS pubblicamente attendibili su Internet. Questo strumento ti consente di cercare i certificati emessi per un dato dominio e di attivare la ricezione delle notifiche da Facebook relative ai nuovi certificati e ai potenziali attacchi di phishing.

<table>
<thead>
<tr>
<th>Domini</th>
<th>Oggetto</th>
<th>Emittente</th>
<th>Validità</th>
<th>Certificato</th>
</tr>
</thead>
</table>
Hunting

- **CTL:**
  - `certstream` library

```python
import certstream

HOT_KEYWORDS = ['whatever', 'bla']

def filter_domain(domain):
    for hk in HOT_KEYWORDS:
        if hk in domain:
            print('%s,%s' % (hk, domain))

def callback(message, context):
    if message['message_type'] == 'heartbeat':
        return

    if message['message_type'] == 'certificate_update':
        all_domains = message['data']['leaf_cert']['all_domains']
        for d in all_domains:
            domain = str(d)
            filter_domain(domain.lower())

def main():
    certstream.listen_for_events(callback, url='wss://certstream.calidog.io/')

main()
```
Hunting

Domain: icloud.support-verify.us

icloud.support-verify.us
191.101.42.166 🇺🇸

URL: http://icloud.support-verify.us/
Submission: On September 14 via api (September 14th 2018, 5:57:50 pm) from CA 🇨🇦

Summary

This website contacted 1 IPs in 1 countries across 1 domains to perform 1 HTTP transactions. The main IP is 191.101.42.166, located in Lincoln, United States and belongs to ILSERVER-RU-NET, UA. The main domain is icloud.support-verify.us.

The main domain was scanned 3 times on urlscan.io

Verdict: Unknown

Google Safe Browsing: Malicious (Current Verdict)

Additional live information
Certificates: 6 TLS cert observed from 2018-09-14 to 2019-03-10

Domain & IP information

<table>
<thead>
<tr>
<th>IP/ASNs</th>
<th>IP Detail</th>
<th>(Sub)Domains</th>
<th>Domain Tree</th>
<th>Links</th>
<th>Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
<td>AS Autonomous System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>191.101.42.166 🇺🇸</td>
<td></td>
<td>44812 (IPSERVER-RU-NET)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stats

1 Requests
0 Ad-blocked
0 Malicious
0% HTTPS
0% IPv6
1 Domains
1 Subdomains
1 IPs
1 Countries
0 KB Transfer
Hunting

Domain: icloud.support-verify.us

> whois support-verify.us | grep -i gmail
Registrant Email: amine.mehdi27@gmail.com
Admin Email: amine.mehdi27@gmail.com
Tech Email: amine.mehdi27@gmail.com
Registrant Email: amine.mehdi27@gmail.com
Admin Email: amine.mehdi27@gmail.com
Tech Email: amine.mehdi27@gmail.com
Report for:
Email amine.mehdi27@gmail.com

In our dataset we observed 5 unique domains:

- appleid.verifylocation.us
- apple.support-verify.us
- icloud.support-verify.us
- icloud.com.iosmap.us
- icloud.iosmap.us
Hunting

Report for:
Email amine.mehdi27@gmail.co

**Umbrella observed 37 domains:**

- ac-id.us
- alertfound.com
- apple-location.online
- apple-url.us
- ccdmsa.us
- cclickme.us
- devicesfound-apple.com
- devicesfound-ios.com
- findmyiphone-ios.com
- findmyiphone-location-tracking.com
- findmyiphone-location-tracking.com
- findmyiphone-map-location.com
- findmyiphone-track-location.com
- icloud-inc.website
- idlocation.us
- inc-support.us
- iosfind.us
- iosfound.us
- ioslocated.us
### Hunting

**Subdomains**
7 unique subdomains for support-verify.us

<table>
<thead>
<tr>
<th>Farsight observed 7 subdomains:</th>
</tr>
</thead>
<tbody>
<tr>
<td>support-verify.us</td>
</tr>
<tr>
<td>mail.support-verify.us</td>
</tr>
<tr>
<td>icloud.support-verify.us</td>
</tr>
<tr>
<td>lcloud.support-verify.us</td>
</tr>
<tr>
<td>appleid.support-verify.us</td>
</tr>
<tr>
<td>apple.support-verify.us</td>
</tr>
<tr>
<td><a href="http://www.support-verify.us">www.support-verify.us</a></td>
</tr>
</tbody>
</table>
Hunting

Do you remember this?

---

**Index of .U**

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Netflix.zip</td>
<td>2018-07-02 14:25</td>
<td>270K</td>
<td></td>
</tr>
<tr>
<td>cgi-bin/</td>
<td>2018-07-02 14:23</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Hunting

index.php
Login
  billing.php
  complete.php
  crypt.php
  css
    a.css
    b.css
    c.css
    include27e6.css
    include2e3a.css
    include616d.css
    include659e.css
    include6b80.css
    includefba4.css
    index.php
    z.css
  email.php
  finish.php
  hok.js
  hostname_check.php
  htaccess
  img
    done.png
    index.php
    login-daredevil-1500x1000.2.jpg
    mtcon2013.tec
    Thumbs.db
    index.php
    payment.php
    r1.php
    r2.php
    success.php
    Netflix.zip
Hunting

What can we fingerprint?

> sha256sum Login/img/login-daredevil-1500x1000.2.jpg
2fe58973af7207f53c1b315444103f8262b3e4d58c67c7770c68b852a5a8bceb
Login/img/login-daredevil-1500x1000.2.jpg
What can we fingerprint?

> sha256sum Login/hok.js
847c86ae982abe9180233276125b930b4a1b6f1bd12649b0c07535c1e984def
8 Login/hok.js

> head Login/hok.js

```javascript
var Aes = {}; // Aes namespace
/**
 * AES Cipher function: encrypt 'input' state with Rijndael algorithm
 */
```

/* AES implementation in JavaScript (c) Chris Veness 2005-2011 */
/* - see http://csrc.nist.gov/publications/PubsFIPS.html#197 */
/* - */
Hunting

About urlscan.io

A sandbox for the web

urlscan.io is a service to scan and analyse websites. When a URL is submitted to urlscan.io, an automated process will browse to the URL like a regular user and record the activity that this page navigation creates. This includes the domains and IPs contacted, the resources (JavaScript, CSS, etc) requested from those domains, as well as additional information about the page itself. urlscan.io will take a screenshot of the page, record the DOM content, JavaScript global variables, cookies created by the page, and a myriad of other observations.

Finally, urlscan.io will query external services to determine whether a page is malicious. It will also try to detect some common malicious practices, such as CryptoJacking.

The original idea behind urlscan.io was to allow even inexperienced users to get a look at what a particular website is requesting in the background. Since it was started in December 2016, urlscan.io has become a widely-used tool for security professionals and amateurs to investigate possibly malicious pages, such as phishing attempts or pages impersonating known brands.

You can contact us at info@urlscan.io. You can also use the GPG key DC9F5A9CDC7D90BE9CB7F5847D68F659926988F9 to encrypt your mail.
Hunting

URLScan.io query:

hash:(2fe58973af7207f53c1b315444103f8262b3e4d58c67c7770c68b852a5a8bceb) AND
hash:(847c86ae982abe9180233276125b930b4a1b6f1bd12649b0c07535c1e984def8)
## Hunting

Search for domains, IPs, filenames, hashes, ASNs

<table>
<thead>
<tr>
<th>#</th>
<th>URL</th>
<th>Submitted</th>
<th>Size</th>
<th>IPs</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>URL: ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe...</td>
<td>2 days ago</td>
<td>204 KB</td>
<td>6</td>
<td>phishTank</td>
</tr>
<tr>
<td>2</td>
<td>URL: ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe...</td>
<td>2 days ago</td>
<td>204 KB</td>
<td>6</td>
<td>phishTank</td>
</tr>
<tr>
<td>3</td>
<td>URL: ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe...</td>
<td>2 days ago</td>
<td>204 KB</td>
<td>6</td>
<td>phishTank</td>
</tr>
<tr>
<td>4</td>
<td>URL: aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcd491569c179623</td>
<td>4 days ago</td>
<td>284 KB</td>
<td>6</td>
<td>phishTank</td>
</tr>
<tr>
<td>5</td>
<td>URL: aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcd491569c179623</td>
<td>5 days ago</td>
<td>284 KB</td>
<td>6</td>
<td>opmPhish</td>
</tr>
<tr>
<td>6</td>
<td>URL: aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcd491569c179623</td>
<td>5 days ago</td>
<td>284 KB</td>
<td>6</td>
<td>opmPhish</td>
</tr>
<tr>
<td>7</td>
<td>URL: help.uniteacad.com/public/11/1f27578beb50335a9aabafbec/</td>
<td>9 days ago</td>
<td>283 KB</td>
<td>6</td>
<td>phishTank</td>
</tr>
<tr>
<td>8</td>
<td>URL: help.uniteacad.com/public/11/cfa23d43fbbe0a703ce68b2b/</td>
<td>9 days ago</td>
<td>283 KB</td>
<td>6</td>
<td>phishTank</td>
</tr>
</tbody>
</table>
DOMANDE?

magrazia@cisco.com
@emd3l
Evento realizzato grazie agli Sponsor e Sostenitori di ISACA VENICE CHAPTER

Sponsor Platinum

Sponsor Platinum

Sponsor Platinum

con il patrocinio di:

con il patrocinio di: