iSEC
information security inc.

Phishing Catcher

Information Security Inc.

iSEC
information security inc.

Contents

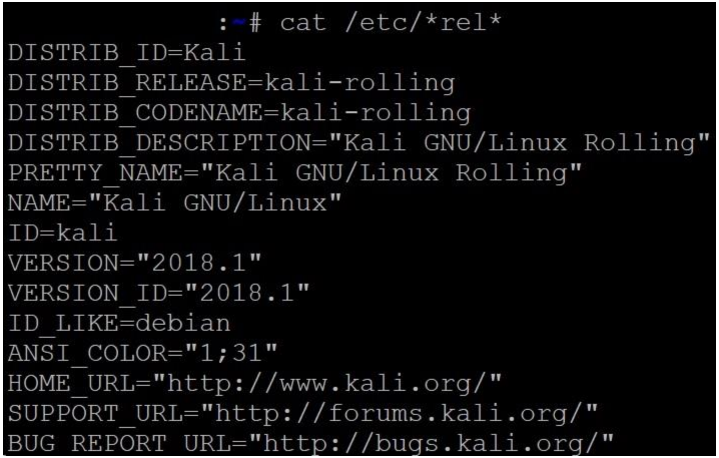
- About Phishing Catcher
- Testing Environment
- Installing Phishing Catcher
- Running Phishing Catcher
- References

About Phishing Catcher

- Catching malicious phishing domain names using certstream SSL certificates live stream

Testing Environment

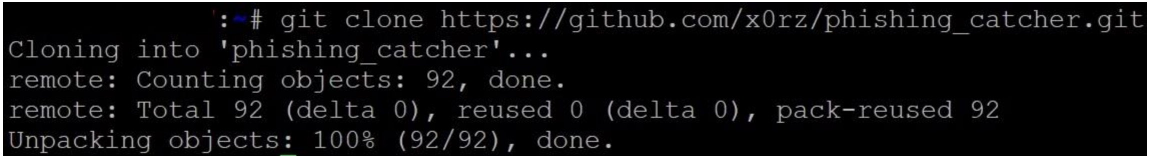
- Kali Linux 2018.1



```
:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing Phishing Catcher

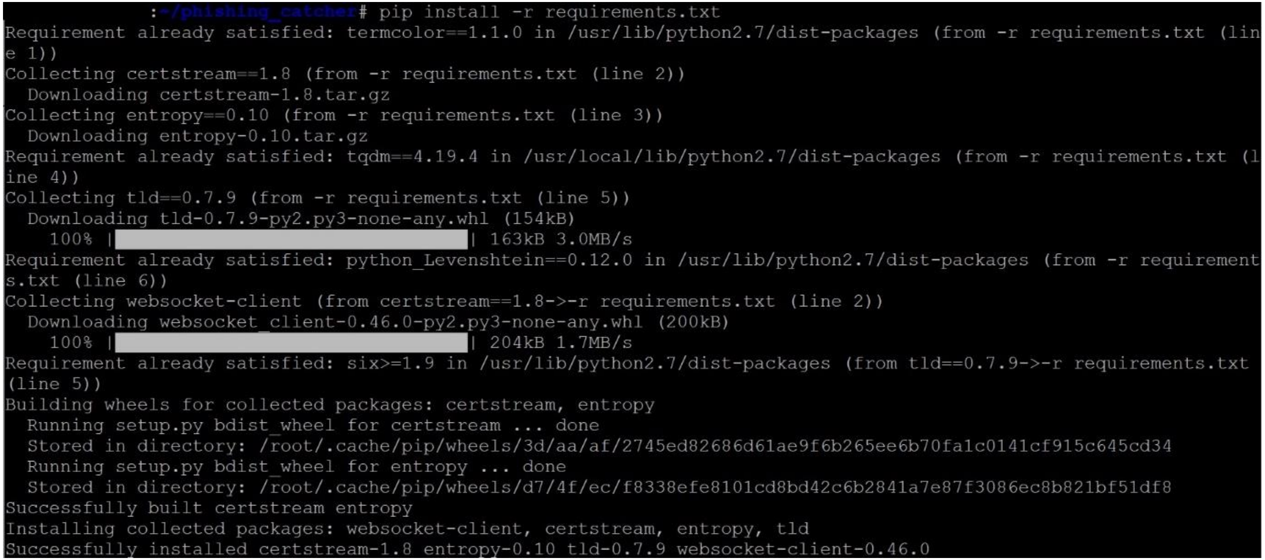
- Cloning GitHub repository



```
[redacted]:~# git clone https://github.com/x0rz/phishing_catcher.git
Cloning into 'phishing_catcher'...
remote: Counting objects: 92, done.
remote: Total 92 (delta 0), reused 0 (delta 0), pack-reused 92
Unpacking objects: 100% (92/92), done.
```

Installing Phishing Catcher

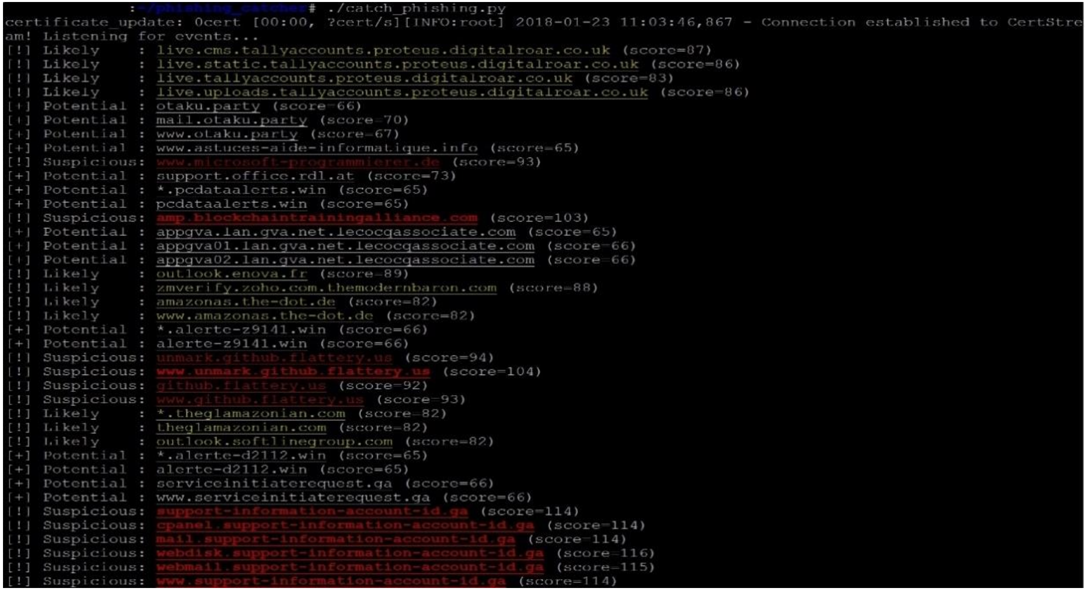
- Installing requirements



```
[redacted]:~/phishing_catcher# pip install -r requirements.txt
Requirement already satisfied: termcolor==1.1.0 in /usr/lib/python2.7/dist-packages (from -r requirements.txt (lin
e 1))
Collecting certstream==1.8 (from -r requirements.txt (line 2))
  Downloading certstream-1.8.tar.gz
Collecting entropy==0.10 (from -r requirements.txt (line 3))
  Downloading entropy-0.10.tar.gz
Requirement already satisfied: tqdm==4.19.4 in /usr/local/lib/python2.7/dist-packages (from -r requirements.txt (l
ine 4))
Collecting tld==0.7.9 (from -r requirements.txt (line 5))
  Downloading tld-0.7.9-py2.py3-none-any.whl (154kB)
    100% |████████████████████████████████| 163kB 3.0MB/s
Requirement already satisfied: python_Levenshtein==0.12.0 in /usr/lib/python2.7/dist-packages (from -r requirement
s.txt (line 6))
Collecting websocket-client (from certstream==1.8->-r requirements.txt (line 2))
  Downloading websocket_client-0.46.0-py2.py3-none-any.whl (200kB)
    100% |████████████████████████████████| 204kB 1.7MB/s
Requirement already satisfied: six>=1.9 in /usr/lib/python2.7/dist-packages (from tld==0.7.9->-r requirements.txt
(line 5))
Building wheels for collected packages: certstream, entropy
  Running setup.py bdist_wheel for certstream ... done
  Stored in directory: /root/.cache/pip/wheels/3d/aa/af/2745ed82686d61ae9f6b265ee6b70fa1c0141cf915c645cd34
  Running setup.py bdist_wheel for entropy ... done
  Stored in directory: /root/.cache/pip/wheels/d7/4f/ec/f8338efe8101cd8bd42c6b2841a7e87f3086ec8b821bf51df8
Successfully built certstream entropy
Installing collected packages: websocket-client, certstream, entropy, tld
Successfully installed certstream-1.8 entropy-0.10 tld-0.7.9 websocket-client-0.46.0
```

Running Phishing Catcher

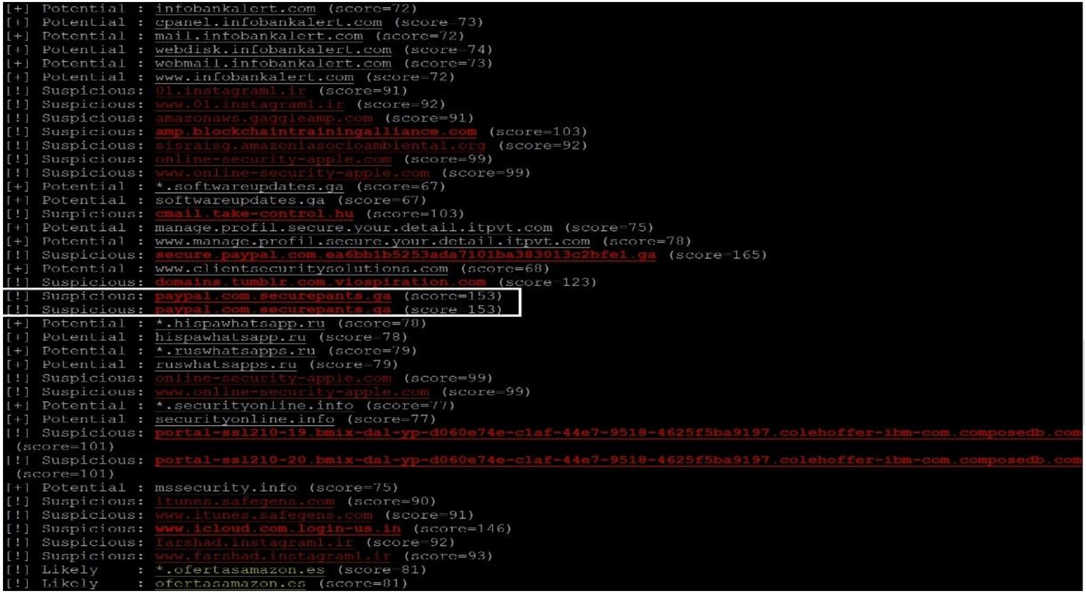
- ./catch_phishing.py



```
:~/phishing_catcher# ./catch_phishing.py
certificate_update: 0cert [00:00, ?cert/s][INFO:root] 2018-01-23 11:03:46,867 - Connection established to CertStre
am! Listening for events...
[!] Likely     : live.cms.tallyaccounts.proteus.digitalroar.co.uk (score=87)
[!] Likely     : live.static.tallyaccounts.proteus.digitalroar.co.uk (score=86)
[!] Likely     : live.tallyaccounts.proteus.digitalroar.co.uk (score=83)
[!] Likely     : live.uploads.tallyaccounts.proteus.digitalroar.co.uk (score=86)
[+] Potential  : otaku.party (score=66)
[+] Potential  : mail.otaku.party (score=70)
[+] Potential  : www.otaku.party (score=67)
[+] Potential  : www.astuces-aide-informatique.info (score=65)
[!] Suspicious: www.microsoft-programmierer.de (score=93)
[+] Potential  : support.office.rdl.at (score=73)
[+] Potential  : *.pcdataalerts.win (score=65)
[+] Potential  : pcdataalerts.win (score=65)
[!] Suspicious: amp.blockchaintrainingalliance.com (score=103)
[+] Potential  : appgva.lan.gva.net.lecocqassociate.com (score=65)
[+] Potential  : appgva01.lan.gva.net.lecocqassociate.com (score=66)
[+] Potential  : appgva02.lan.gva.net.lecocqassociate.com (score=66)
[!] Likely     : outlook.enova.fr (score=89)
[!] Likely     : zmverify.zoho.com.themodernbaron.com (score=88)
[!] Likely     : amazonas.the-dot.de (score=82)
[!] Likely     : www.amazonas.the-dot.de (score=82)
[+] Potential  : *.alerte-z9141.win (score=66)
[+] Potential  : alerte-z9141.win (score=66)
[!] Suspicious: unmark.github.flattery.us (score=94)
[!] Suspicious: www.unmark.github.flattery.us (score=104)
[!] Suspicious: github.flattery.us (score=92)
[!] Suspicious: www.github.flattery.us (score=93)
[!] Likely     : *.theglamazonian.com (score=82)
[!] Likely     : theglamazonian.com (score=82)
[!] Likely     : outlook.softlinegroup.com (score=82)
[+] Potential  : *.alerte-d2112.win (score=65)
[+] Potential  : alerte-d2112.win (score=65)
[+] Potential  : serviceinitiaterequest.ga (score=66)
[+] Potential  : www.serviceinitiaterequest.ga (score=66)
[!] Suspicious: support-information-account-id.ga (score=114)
[!] Suspicious: cpanel.support-information-account-id.ga (score=114)
[!] Suspicious: mail.support-information-account-id.ga (score=114)
[!] Suspicious: webdisk.support-information-account-id.ga (score=116)
[!] Suspicious: webmail.support-information-account-id.ga (score=115)
[!] Suspicious: www.support-information-account-id.ga (score=114)
```

Running Phishing Catcher

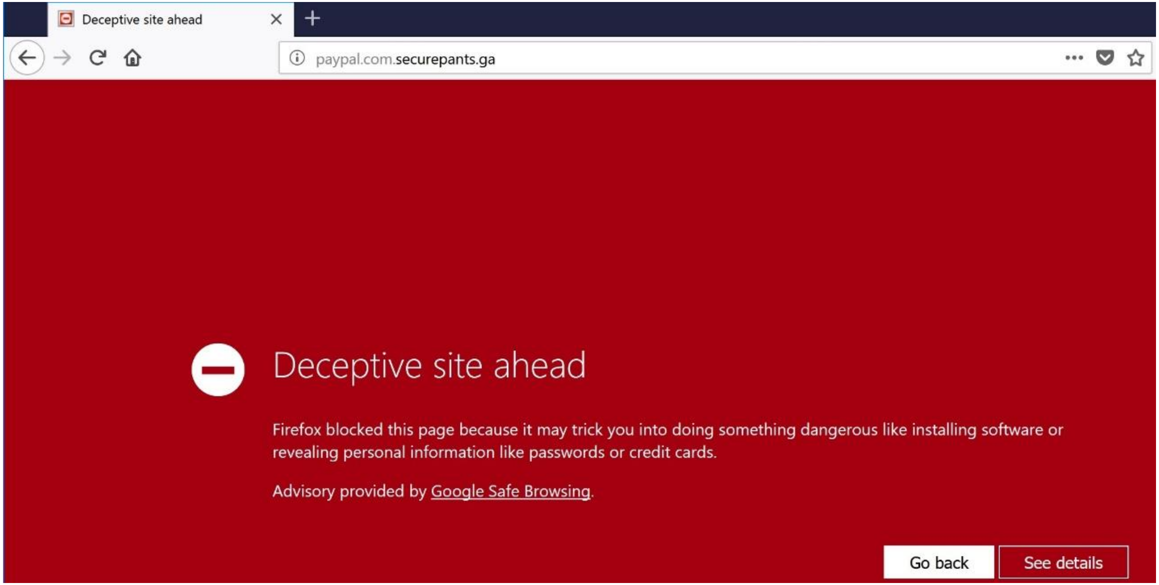
- Example phishing caught



```
[+] Potential : infobankalert.com (score=72)
[+] Potential : cpanel.infobankalert.com (score=73)
[+] Potential : mail.infobankalert.com (score=72)
[+] Potential : webdisk.infobankalert.com (score=74)
[+] Potential : webmail.infobankalert.com (score=73)
[+] Potential : www.infobankalert.com (score=72)
[!] Suspicious: 01.instagraml.ir (score=91)
[!] Suspicious: www.01.instagraml.ir (score=92)
[!] Suspicious: amazonaws.gaggleamp.com (score=91)
[!] Suspicious: amp.blockchaintrainingalliance.com (score=103)
[!] Suspicious: sisraisg.amazoniasocioambiental.org (score=92)
[!] Suspicious: online-security-apple.com (score=99)
[!] Suspicious: www.online-security-apple.com (score=99)
[+] Potential : *.softwareupdates.ga (score=67)
[+] Potential : softwareupdates.ga (score=67)
[!] Suspicious: cmail.take-control.hu (score=103)
[+] Potential : manage.profil.secure.your.detail.itpvt.com (score=75)
[+] Potential : www.manage.profil.secure.your.detail.itpvt.com (score=78)
[!] Suspicious: secure.paypal.com.ea6bb1b5253ada7101ba383013c2bfe1.ga (score=165)
[+] Potential : www.clientsecuritysolutions.com (score=68)
[!] Suspicious: domains.tumblr.com.viospiration.com (score=123)
[!] Suspicious: paypal.com.securepants.ga (score=153)
[!] Suspicious: paypal.com.securepants.ga (score=153)
[+] Potential : *.hispawhatsapp.ru (score=78)
[+] Potential : hispawhatsapp.ru (score=78)
[+] Potential : *.ruswhatsapps.ru (score=79)
[+] Potential : ruswhatsapps.ru (score=79)
[!] Suspicious: online-security-apple.com (score=99)
[!] Suspicious: www.online-security-apple.com (score=99)
[+] Potential : *.securityonline.info (score=77)
[+] Potential : securityonline.info (score=77)
[!] Suspicious: portal-ssl210-19.bmix-dal-yp-d060e74e-c1af-44e7-9518-4625f5ba9197.colehoffer-ibm-com.composedb.com
 (score=101)
[!] Suspicious: portal-ssl210-20.bmix-dal-yp-d060e74e-c1af-44e7-9518-4625f5ba9197.colehoffer-ibm-com.composedb.com
 (score=101)
[+] Potential : mssecurity.info (score=75)
[!] Suspicious: itunes.safegens.com (score=90)
[!] Suspicious: www.itunes.safegens.com (score=91)
[!] Suspicious: www.icloud.com.login-us.in (score=146)
[!] Suspicious: farshad.instagraml.ir (score=92)
[!] Suspicious: www.farshad.instagraml.ir (score=93)
[!] Likely    : *.ofertasamazon.es (score=81)
[!] Likely    : ofertasamazon.es (score=81)
```

Running Phishing Catcher

- Example phishing caught



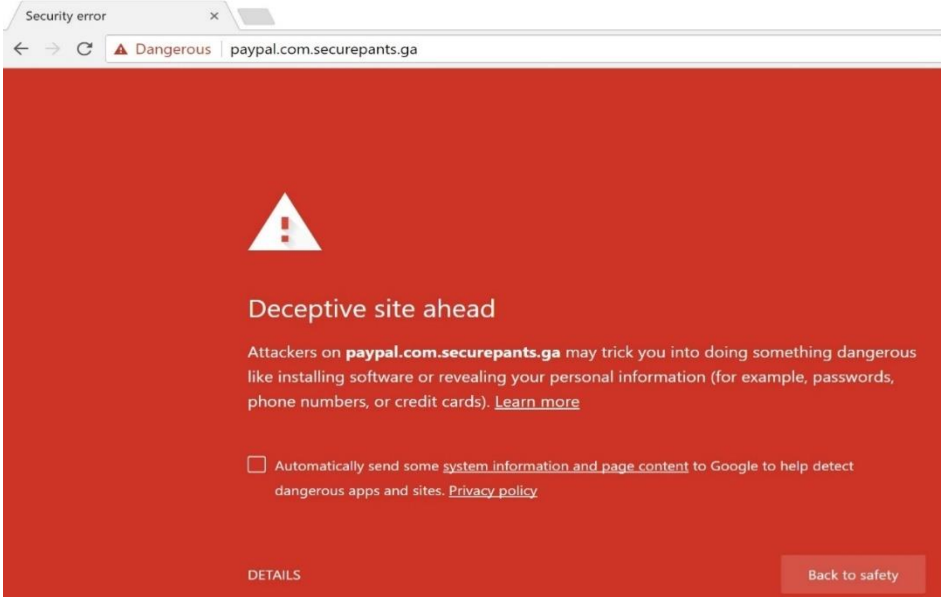
Deceptive site ahead

Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by Google Safe Browsing.

Running Phishing Catcher

- Example phishing caught



Deceptive site ahead

Attackers on **paypal.com.securepants.ga** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

References

- Certstream
https://certstream.calidog.io/

- Phishing_Catcher
https://github.com/x0rz/phishing_catcher