Email Security: Phishing

Alex Stan

$whoami

- Master Degree: FMI SLA
- Past job: Security Analyst @SecureWorks
- Current job: Application Security Analyst @Adobe

Agenda

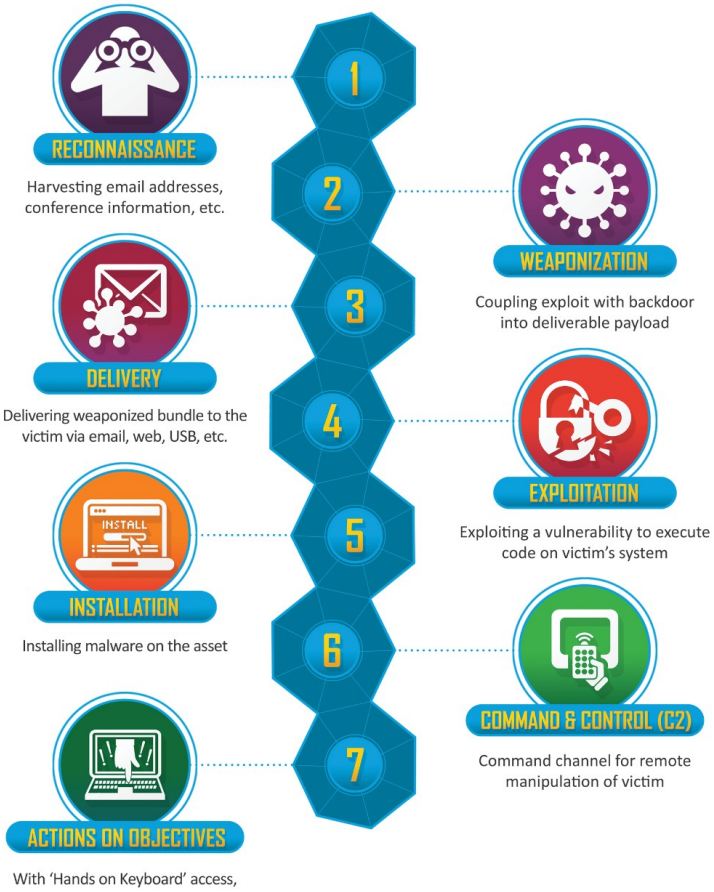
1. Motivatie: Cyber Kill Chain, CVSS
2. Tipuri de phishing
3. Tool-uri de atac - The Harvester
4. Email spoofing
5. Protectii: SPF, DKIM, DMARC
6. Phishing la nivel enterprise (SOC, Threat Intelligence, PhishStats)
7. Recomandari, resurse, directii viitoare

Phishing: Motivatie

- *"91% of breaches starting with phishing emails" – Cofense*
- *Se situeaza la etapa de **Delivery** din **Cyber Kill Chain***

Ref: https://cofense.com

Cyber Kill Chain



Ref: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Phishing: Motivatie #2 CVSS

- CVSS = **Common Vulnerability Scoring System**
- Oricarei vulnerabilitati ii se atribuie un scor ce reflecta severitatea
- User-Interaction este o componenta CVSS

CVSS: User Interaction

Base Score	8.0 (High)

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

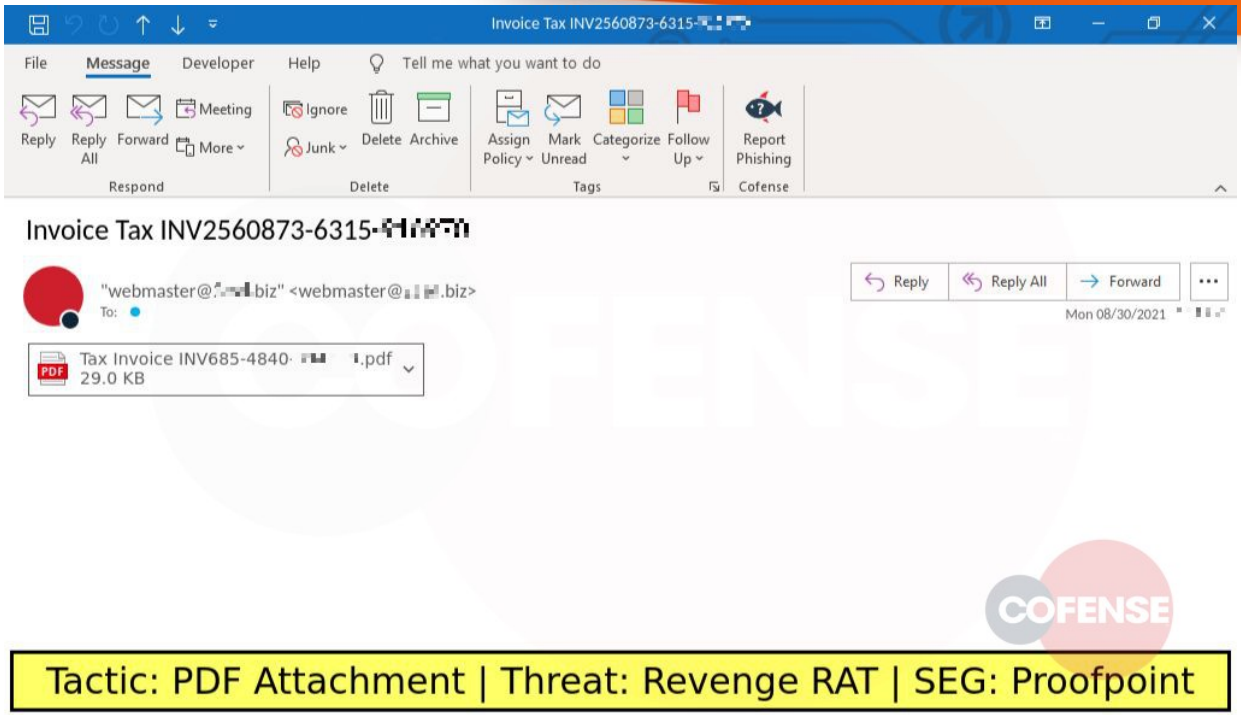
None (N) | Low (L) | High (H)

Ref: https://www.first.org/cvss/calculator/3.1

Diverse tipuri de phishing

- Categorii in functie de:
  - Tactici
  - Tematica
  - Tehnici
  - Destinatar

Exemple: #1

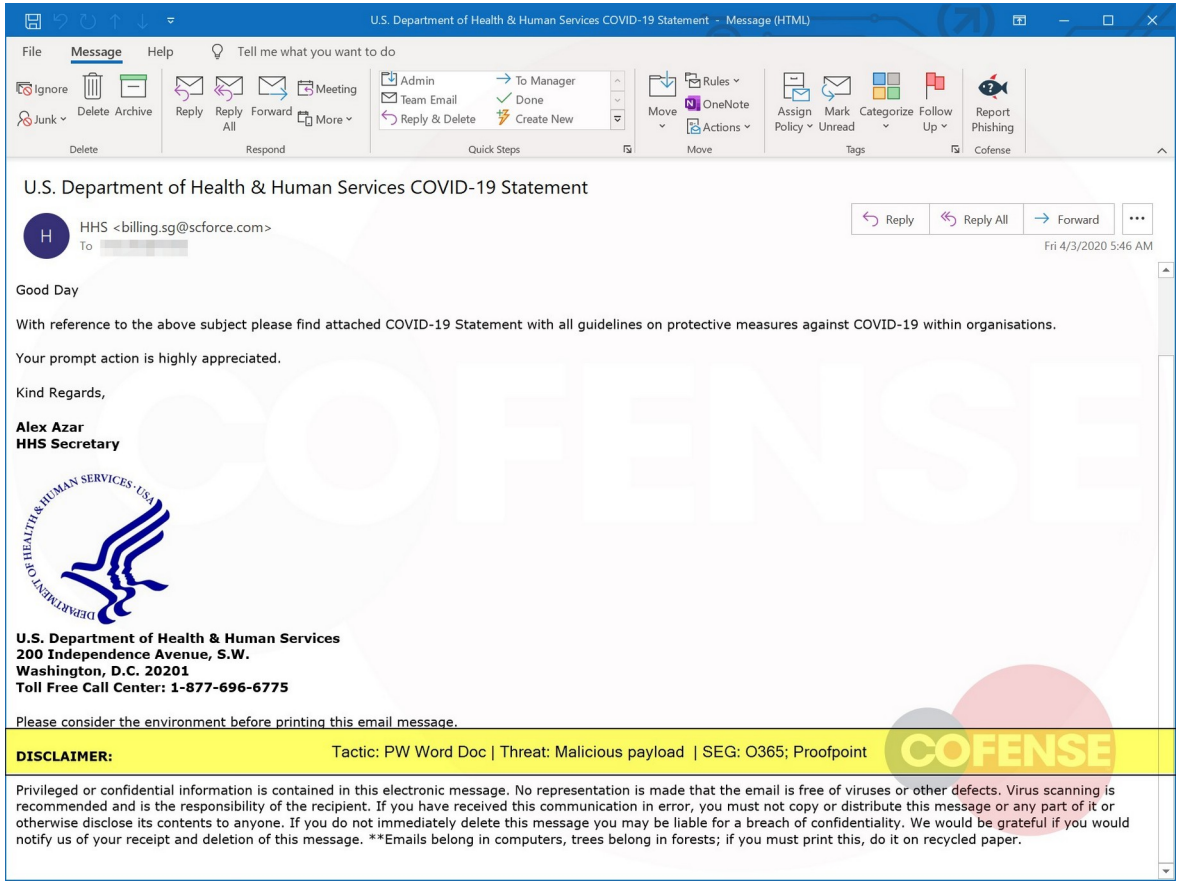


Tactic: PDF Attachment | Threat: Revenge RAT | SEG: Proofpoint

Ref:https://cofense.com/real-phishing-examples-and-threats/

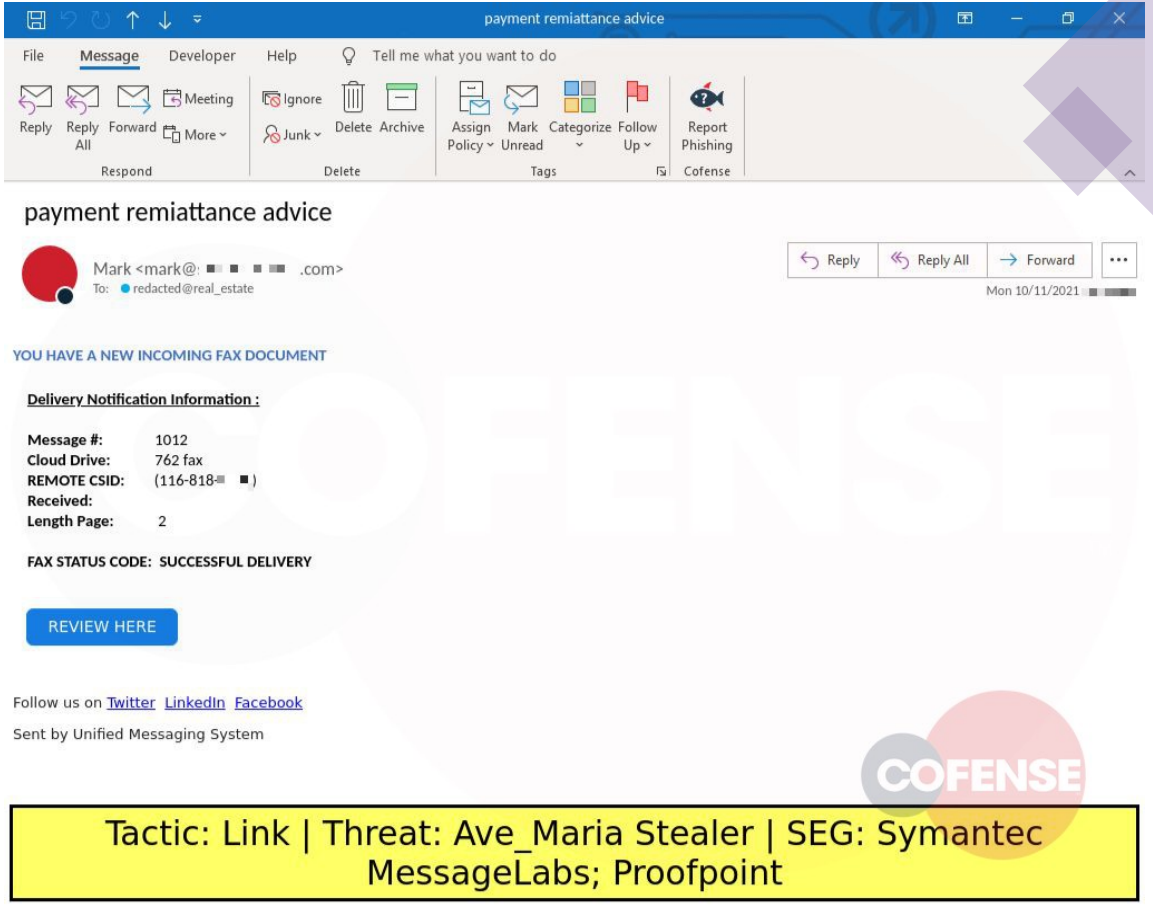
Exemple: #2

- Ref:https://cofense.com/real-phishing-examples-and-threats/



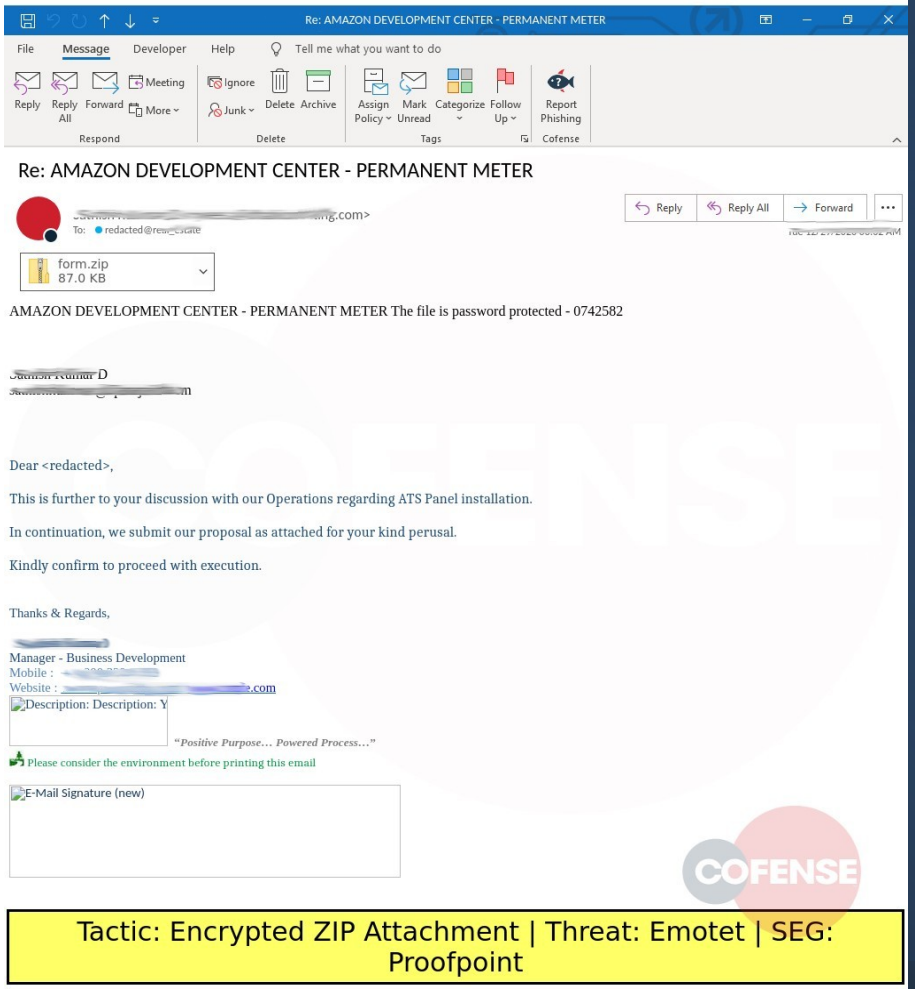
Exemple: #3

•Ref:https://cofense.com/real-phishing-examples-and-threats/



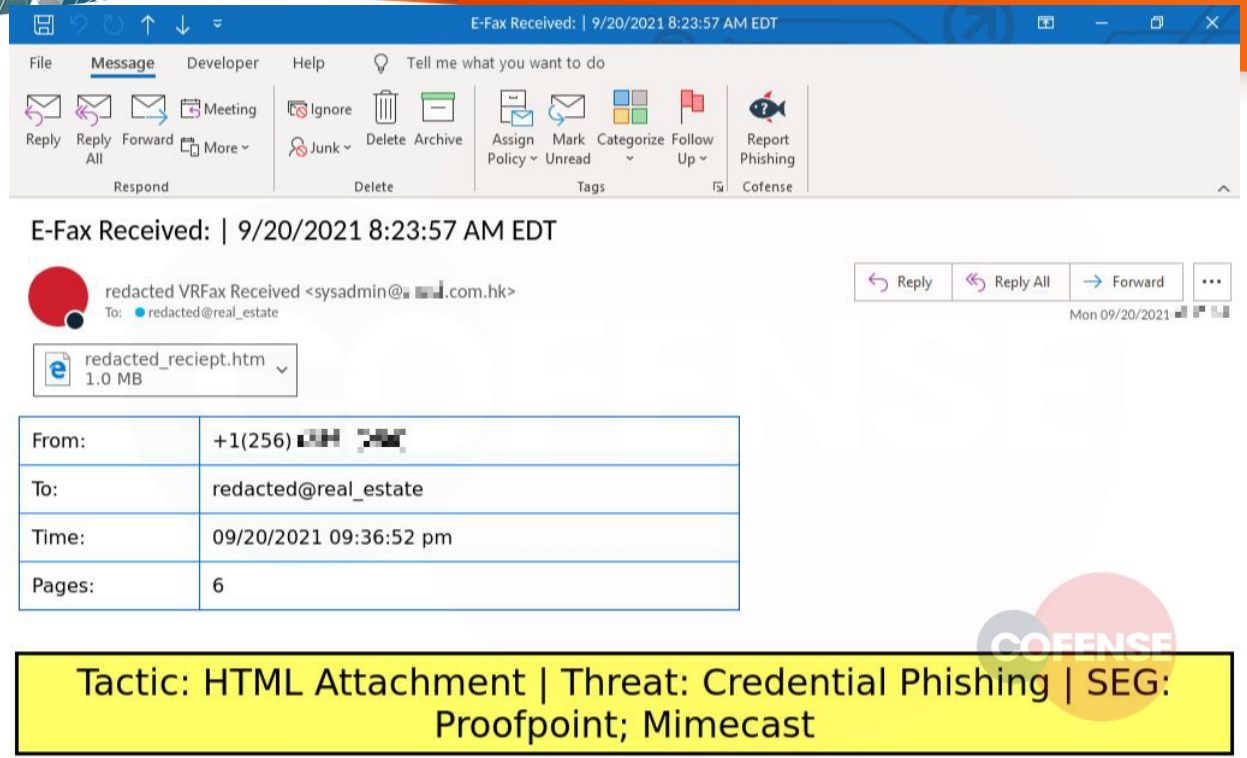
Exemple: #4

- Ref: https://cofense.com/real-phishing-examples-and-threats/



Tactic: Encrypted ZIP Attachment | Threat: Emotet | SEG: Proofpoint

Exemple: #5



Ref:https://cofense.com/real-phishing-examples-and-threats/

Efectuarea unui atac

- Diverse tool-uri:
  - Social Engineering Toolkit
  - The Harvester
  - Recon-ng
  - PHPMailer
  - Online Spoofing Tools

```
root@kali:/# theharvester

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

  ************************************************************************
*                                                                        *
* | |_| |_  ___   /\ /\__ _ _ ____   _____  ___| |_ ___ _ __           *
* | __| '_ \ / _ \ / //_/ _` | '__\ \ / / _ \/ __| __/ _ \ '__|         *
* | |_| | | |  __// __ \ (_| | |   \ V /  __/\__ \ ||  __/ |            *
*  \__|_| |_|\___| \/ \/\__,_|_|    \_/ \___||___/\__\___|_|            *
*                                                                        *
* TheHarvester Ver. 3.0.0                                                *
* Coded by Christian Martorella                                          *
* Edge-Security Research                                                 *
* cmartorella@edge-security.com                                          *
************************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all

       -s: start in result number X (default: 0)
       -v: verify host name via dns resolution and search for virtual hosts
       -f: save the results into an HTML and XML file (both)
       -n: perform a DNS reverse query on all ranges discovered
       -c: perform a DNS brute force for the domain name
       -t: perform a DNS TLD expansion discovery
       -e: use this DNS server
       -p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
       -l: limit the number of results to work with(bing goes from 50 to 50 results,
           google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```

The Harvester: Recon tool

Kali Linux: https://www.kali.org/get-kali/#kali-platforms

Email spoofing

- Structura unui email - 2 componente:
  - Envelope / P1 Header
  - Header and Body / P2 Header

Email spoofing

- P1 header:
  - MAIL FROM: user@domeniu.com
  - RCPT TO: user2@domeniu2.com
- P2 header:
  - FROM: user@altdomeniu.com
  - TO: user2@domeniu2.com

Protectii

- SPF: (Sender Policy Framework)
- DKIM: (DomainKeys Identified Mail)
- DMARC (Domain-based Message Authentication Reporting and Conformance)

Exemplu protectii

```
Authentication-Results: spf=pass (sender IP is 54.240.11.150)
 smtp.mailfrom=amazonses.com; s.unibuc.ro; dkim=pass (signature was verified)
 header.d=amazonses.com;s.unibuc.ro; dmarc=none action=none
 header.from=netacad.com;compauth=pass reason=102
Received-SPF: Pass (protection.outlook.com: domain of amazonses.com designates
 54.240.11.150 as permitted sender) receiver=protection.outlook.com;
 client-ip=54.240.11.150; helo=a11-150.smtp-out.amazonses.com;
```

Spoofed email

Hop↓	Submitting host	Receiving host
1		emkei.cz (Postfix, from userid 33)
2	emkei.cz (101.99.94.155)	HE1EUR04FT063.mail.protection.outlook.com (10.152.27.52)
3	HE1EUR04FT063.eop-eur04.prod.protection.outlook.com (2603:10a6:209:8c:cafe::9d)	AM6PR10CA0106.outlook.office365.com (2603:10a6:209:8c::47)
4	AM6PR10CA0106.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:209:8c::47)	AM9PR03MB6979.eurprd03.prod.outlook.com (2603:10a6:20b:285::8)
5	AM9PR03MB6979.eurprd03.prod.outlook.com (2603:10a6:20b:285::8)	VI1PR03MB4287.eurprd03.prod.outlook.com

Tool: https://mha.azurewebsites.net

Phishing la nivel enterprise

- Campanii de phishing
- **SOC** – Security Operations Center
- Echipa de **incident-response** pentru mitigare

Actiuni de mitigare in SOC

- Blocarea sender-ilor in **Security Email Gateway** (SEG)
- Blocarea url-urilor/domeniilor in IPS, AV, EDR
- Blocarea hash-urilor corespunzatoare atasamentelor
- Resetarea credentialelor compromise
- Reimage la host-uri infectate (sau analiza de tip forensics)

Threat Intelligence

- **Threat intelligence** (TI) - informarea in legatura cu ultimile amenintari si motivatii ale atacatorilor

- Vrem sa aflam trend-uri si statistici despre phishing pentru a ne apara mai bine

PhishStats

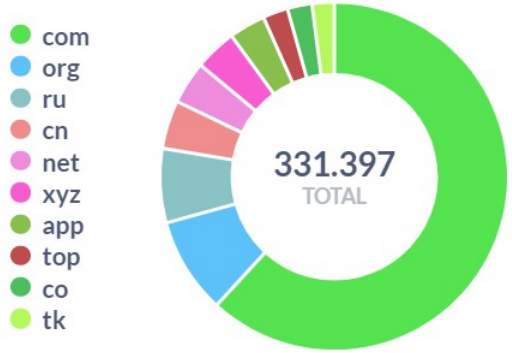
Top 50 Titles - Current Year

Count	title
7.251	WhatsApp Group Invite
5.099	Log into Facebook
4.909	Undangan Grup Whatsapp
3.839	Facebook
3.774	Suspected phishing site | Cloudflare
3.213	Sign in to your account
3.208	Sign in
3.137	Amazon 27th anniversary celebration !
2.574	Verification | Royal Mail Group Ltd
2.356	Amazonサインイン
2.117	Этот домен припаркован компанией Timewe
2.024	Netflix
1.986	Login

Top 10 IPs - Search

Count	IP
15.325	198.54.115.30 | NAMECHEAP-NET, US
14.109	199.188.201.33 | NAMECHEAP-NET, US
7.624	199.34.228.53 | WEEBLY, US
7.424	199.34.228.54 | WEEBLY, US
5.809	87.251.76.135 | HOSTKEY-AS HOSTKEY B.V., NL
4.783	151.101.65.195 | FASTLY, US
4.730	151.101.1.195 | FASTLY, US
3.669	185.30.164.4 | FNXTEC FNX Tecnologia LTDA, NL
3.344	74.220.219.183 | UNIFIEDLAYER-AS-1, US
2.813	5.57.226.202 | SERVIHOSTING-AS ServiHosting Networks S.L., ES

Top 10 TLDs - Current Year



Ref: https://phishstats.info

Resurse/directii viitoare

- Cofense: https://cofense.com
- SANS: https://www.sans.org/emea/
- INE: https://ine.com
- Security Blue Team: https://www.securityblue.team
- TryHackMe: https://tryhackme.com
- HackTheBox: https://www.hackthebox.eu

Recomandari certificari

- GIAC: https://www.giac.org (GCIH, GCFA, GREM, GNFA etc.)
- Offensive Security: https://www.offensive-security.com (OSCP, OSWE, OSED etc.)
- eLearnSecurity: https://elearnsecurity.com (eJPT, eCPPT, eWPT, eCTHP etc.)

Multumesc
Q&A

Contact
Linkedin: https://www.linkedin.com
/in/alex-stan-2a3366139/