Introducere în Securitatea cibernetică

Silviu-Laurențiu Vasile
Laurențiu-Vasile Crețu

Laborator de finanțe inovative,
6 martie 2025

CUPRINS

- Context
- Scurt istoric incidente cibernetice
- Amenințări Cibernetice în domeniul financiar
- *Phishing. Ransomware. DDos*
- *OpenSSL* - generare certificat, chei de autentificare
- *Practice* (temă)
- Concluzii

Context

- Informația stocată, prelucrată, manipulată, (re)interpretată reprezintă un avantaj decisiv în cadrul competiției din diferite domenii esențiale ale economiei
  - Conform *Cybersecurity Ventures* vor fi stocate 200 de zettabytes de date până în 2025, echivalentul a un trilion de gigabytes sau 10^{21} bytes (1.000.000.000.000.000.000.000). Aceste date au o valoare imensă și vor continua să fie o țintă pentru infractorii cibernetici.
- O sursă care asigură creșterea criminalității cibernetice, într-o asemenea măsură încât poate destabiliza economiile, este reprezentată de faptul că infractorii cibernetici nu mai au nevoie de cunoștințe tehnice avansate pentru a lansa atacuri.
  - malware-ul este disponibil pentru achiziție prin intermediul dark web-ului, prin servicii ilegale care vând kituri *Ransomware-as-a-Service* (RaaS) ce includ chiar asistență pentru clienți, suport tehnic și garanții de returnare a banilor.

Context

- Potrivit World Economic Forum criminalitatea cibernetică a crescut atât de mult încât poate fi descrisă acum ca a treia cea mai mare economie din lume, după SUA și China. Criminalitatea cibernetică generează mult mai mulți bani decât traficul ilegal de droguri, contrabanda și traficul de persoane la un loc.

- Se estimează că în 2023 criminalitatea cibernetică a generat 8 trilioane de dolari și că ar putea ajunge la aproximativ 10,5 trilioane de dolari până în 2025 (*link*). Un singur atac de tip *ransomware* sau o serie de atacuri cibernetice pot costa foarte mult afacerile și economia

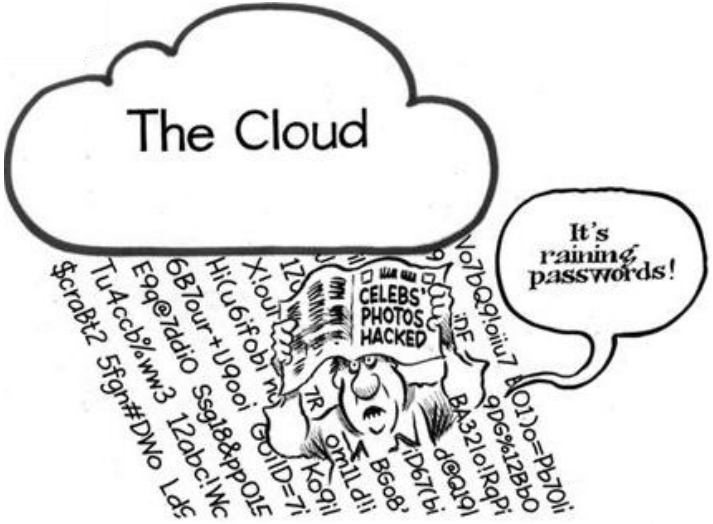
  - Atacul ransomware WannaCry din 2017 a paralizat companii din întreaga lume, inclusiv instituții de sănătate și firme de tehnologie. A afectat peste 200.000 de computere din mai mult de 100 de țări și a cauzat pierderi estimate la 8 miliarde de dolari în doar patru zile.

- Cronologia incidentelor cibernetice în care au fost implicate instituțiile financiare (*link*)

Breșe de securitate în Europa

- **British Airways (iunie 2018 – septembrie 2018) – sunt compromise datele personale a 500k de clienți** (Hackerii au avut acces la site-ul web și aplicația mobilă, interceptând datele sensibile ale clienților în timpul procesului de rezervare; numele, adresele, detaliile cardurilor de credit și informațiile de călătorie ale clienților au fost expuse; breșa a deteriorat semnificativ reputația companiei, ducând la o amendă de 20 de milioane de lire sterline în temeiul GDPR)
- **European Central Bank (iulie 2014) – sunt compromise 20k de adrese de email împreună cu date de contact, ulterior in 2018 este victima unui atac de tip malware**
- **PrivatBank – iulie 2014 în urma unui atac cibernetic sunt expuse 40M de înregistrări cu date persoanle pe un site public**
- **Warsaw Stock Exchange (octombrie 2014) – 30k de conturi (username, email, parole) sunt compromise în urma unui atac ISIS care face ca site-ul bursei sa nu mai fie valabil mai multe ore**
- **COSMOTE Mobile Telecommunications (septembrie 2020) – datele a 4.8M de clienti sunt expuse**
- **Binance (octombrie 2022) – sunt furate aproximativ $570M**

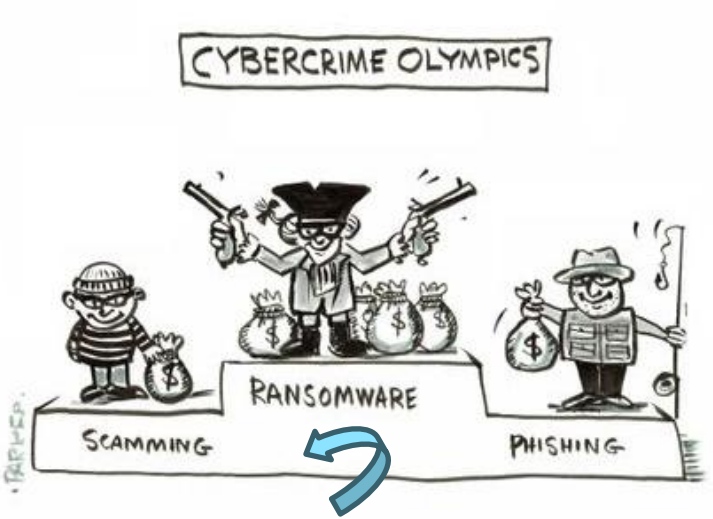
Breșe de securitate în România



- 29.04.2022: *"Astăzi dimineaţă, accesarea site-urilor **gov.ro**, **mapn.ro** si **politiadefrontiera.ro**, **cfrcalatori.ro** si a site-ului unei instituţii financiare a fost afectată de o serie de atacuri cibernetice de tip DDOS (distributed denial of service)" – **link***
- 7.03.2022: *"During this night, Rompetrol faced a complex cyber-attack. We are in constant contact with the National Directorate of Cyber Security (DNSC) and fully involved to resolve the situation. To protect the data, the company has temporarily suspended the operation of the websites and the Fill&Go service, both for the fleets and for the private customers..." – **link***
- 20.02.2023: *"Compania Tarom informează că în cursul zilei de astăzi a avut loc un incident de securitate izolat, în urma căruia au fost afectate mai multe fişiere de către un virus de tip ransomware. Menţionam că toate cursele au fost operate conform planului de zbor, iar din cauza acestui incident nu au fost afectate operaţiunile de zbor sau sistemul de rezervări al companiei" – **link***

Amenințări Cibernetice în domeniul financiar

- Conform VMware, prima jumătate a anului 2020 a înregistrat o creștere de 238% ale atacurilor cibernetice care vizau instituțiile financiare
- Conform IBM **costul mediu** al unei breșe de securitate în sectorul financiar în 2023 este de 5,17 milioane de dolari (Statista – 5.90M/'23, 6.08M/'24, G-AVG -4.88M/'24)
- În 2025, pe măsură ce tehnologia continuă să evolueze, sectorul financiar va rămâne o țintă majoră pentru atacuri cibernetice. Inovațiile tehnologice, cum ar fi tehnologiile de blockchain, plățile digitale și inteligența artificială, aduc noi riscuri și vulnerabilități.
- Pe baza acestor statistici, dacă activezi în sectorul serviciilor financiare, există o șansă foarte mare să devii, la un moment dat, victima unui atac cibernetic foarte costisitor.



Cele mai comune amenințări cibernetice în domeniul financiar

- Phishing
- Ransomware
- SQL Injections (SQLi)
- Cross-Site Scripting (XSS)
- DDoS Attacks
- Local File Inclusion (LFI)
- OGNL (*Object Graph Navigation Language*) Java Injection

Phishing

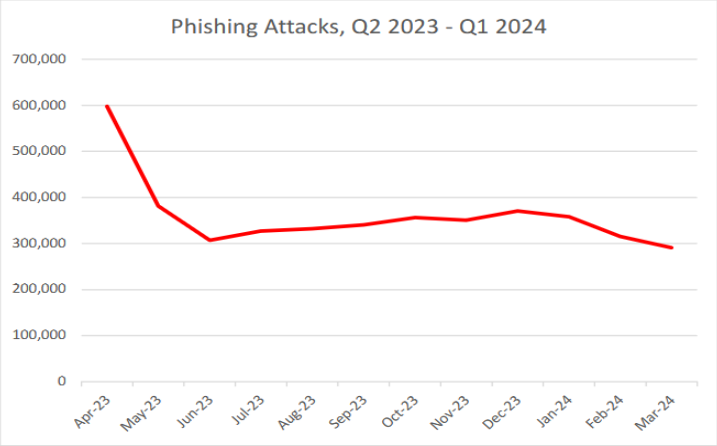
- **Phishing**, variantă de **inginerie socială**, este o metodă de păcălire a utilizatorilor pentru a divulga datele de autentificare, cu scopul de a obține acces la o rețea internă
- Cea mai comună formă de phishing este **phishing-ul prin e-mail**, în care un e-mail ce pare a fi o comunicare legitimă este trimis victimelor
- Interacționarea cu oricare dintre linkurile sau atașamentele infectate din e-mailurile de tip phishing poate declanșa instalarea de malware în sistemul informatic țintă sau poate încărca o pagină web falsă care colectează datele de autentificare
- Pentru destinatarul neavizat, aceste e-mailuri înșelătoare par foarte convingătoare, mai ales atunci când sunt prezentate cu un **sentiment de urgență**
- Template-uri pentru astfel de mesaje: link

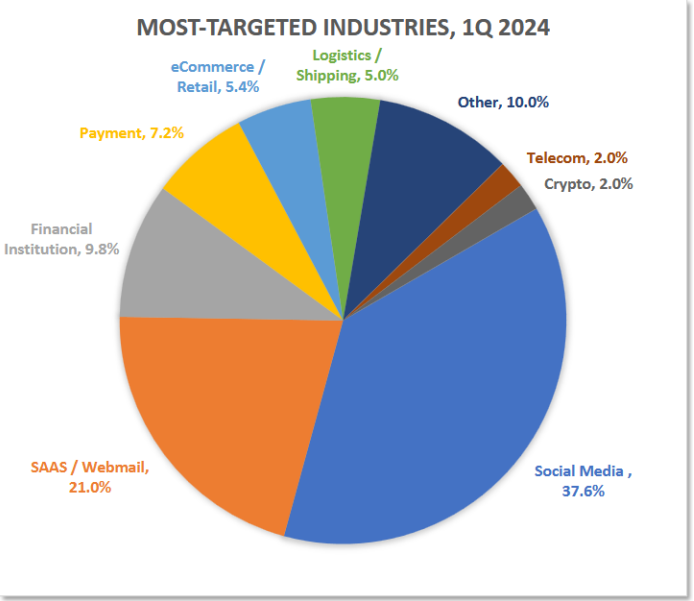
Phishing

- Se estimează că peste 90% dintre atacurile cibernetice reușite încep cu un atac de tip phishing, iar această rată de conversie nefericită afectează grav industria financiară

- În primele șase luni ale anului 2021, atacurile de tip *phishing* în sectorul financiar au crescut cu 22% față de aceeași perioadă din 2020. Atacurile care vizează aplicațiile financiare au înregistrat o creștere de 38% în aceeași perioadă.

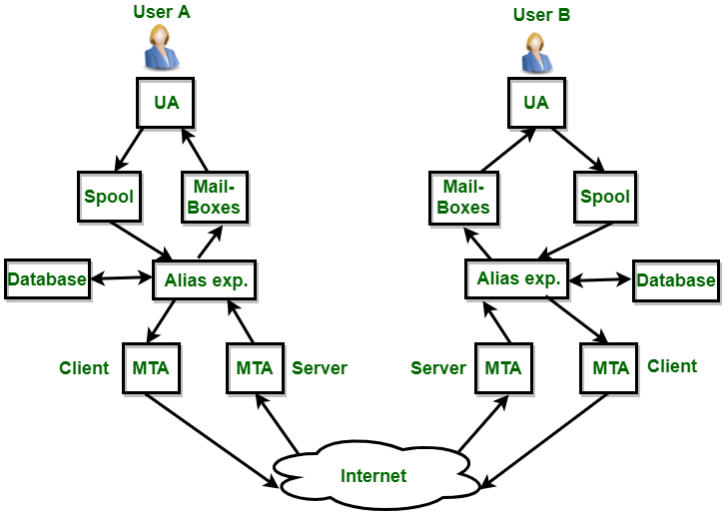
- Phishing Activity Trends Report '24





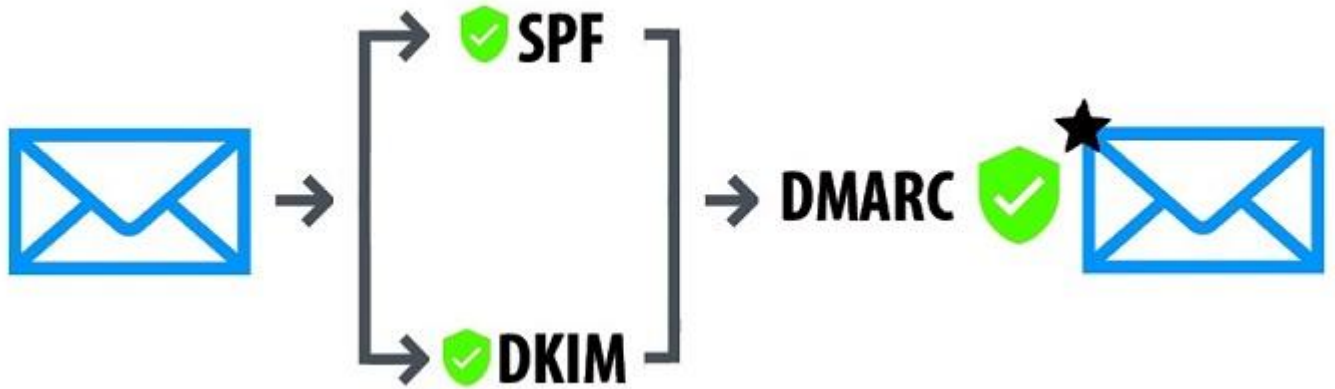
Phishing - Ce este un email?

- Un pachet/obiect transmis între 2 adrese IP!!!
- O structură cu o serie de proprietăți: *header*, *titular*, *destinatar*, *adresa IP server sursa*, *adresa IP server destinatie* etc;
- Tehnic pot fi transmite mesaje în "*numele*" altor persoane?
  - https://bit.ly/3TaBsoj



Verificare email

- https://mxtoolbox.com/NetworkTools.aspx



Verificare email

- Mail –> show original

Reminder Seminar

Inbox ×

Elena

to [redacted]

Stimați colegi,

Marți, , va avea loc seminarul în sala , etaj 4, sala nr. 4331.

Speaker:

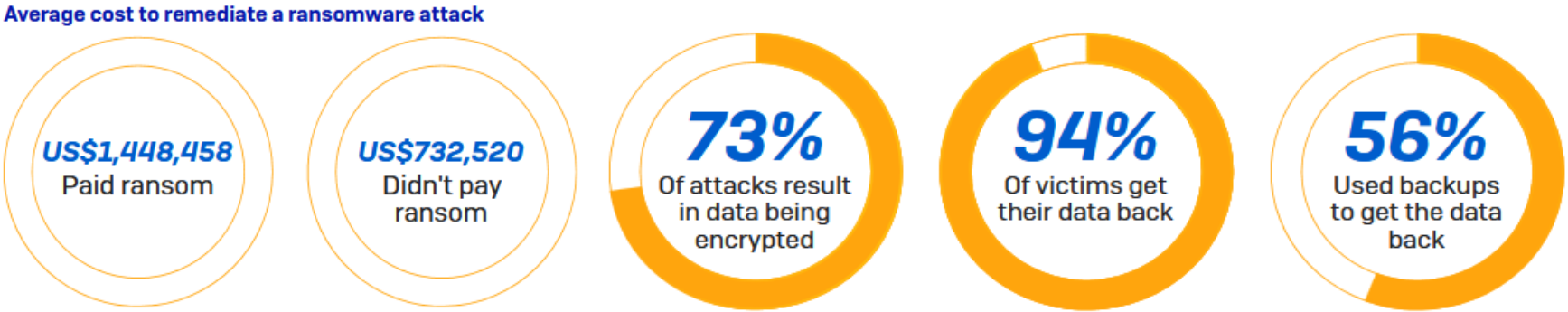
Titlul: Securitatea activităților desfășurate în mediul online (Abstract https:// =846)

Verificare email

```
Delivered-To: vslsilviu
Received: by 2002:a05:6
        Mon,    Mar 202
X-Received: by 2002:a17
        Mon,    Mar 202
ARC-Seal: i=1; a=rsa-sha256; t=1678700609; cv=none;
        d=google.com; s=arc-20160816;
        b=ye3SigDGpqcggSEzgXWmTJSZPBMpkVSzSaoblMoNuySX3fAJdPB9Jn86x/j1hRkZrK
         auOt+1cKyCYLer0KkDIiKbuuWusXHpOvhmt90WJH/IiXtxpH/EGuZRHehDMVtwVApKpU
         fsXntlXYS3TNLjrAdDIRNIdXx8JPr5qNifcrXadSNCoxOCzHo9Q63X1R9bsufSwv5lkd
         OsIwaGEwIfypWOT9aAURaw+7rVdIfQ/F7tddQzlhptCGK869O9tSAlbUKtLwv6lztqjn
         kq4/IC144tf7X1uV2xGsDNpFJZiVNUbDnAuLwjUsqX698b+qPcmgbEONOTuNTxjc1nZD
         /rsQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:in-reply-to:references:mime-version
         :dkim-signature;
        bh=od5AetWuVcdNN64sPpeO9zQoUefUbjoZi5fapWJ5GXE=;
        b=YSHiTmPuufXJoMUhWnMrx75Y1INZ2M6Dok3lcoS7wJxKYSsxBIIHsdp2jpo33smZjb
         j/0OUSUEgC/u2XvlM9SONCcbPwU2IxEHoAslASCkQZ7z3ldhcKSPmh/cl5sgSa8A0kD/
         PSmf8QEHUrckOBTwX/00dbJ4MAk8aw0B3IXu8S4l5MAHhW0wF5XGhTosZepLMpcvqkiR
         bEUaGGWsPQG4WfaIeyKtDdAm3OgTy6SH8RMbWT91bdctBETLBAchC+SdrDA33MAEI6oB
         aPeOyPI/xwKxCdwsZsrv9VXWVrLUgkNlVVYMbQaxxdf+X9/2LflAkwoE/NQTT3DWPBRc
         HShA==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=5QSmdq1t;
       spf=pass (google.com: domain of          sa@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=          a@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <          !sa@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id p8-20020a170906b20800b00925d98803f7sor1644174ejz.66.2023.03.13.02.43.28
        (Google Transport Security);
        Mon,
Received-SPF: pass (google.com: domain of          sa@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=5QSmdq1t;
       spf=pass (google.com: domain of                designates 209.85.220.41 as permitted sender) smtp.mailfrom=!          .com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20210112; t=1678700608;
        h=to:subject:message-id:date:from:in-reply-to:references:mime-version
         :from:to:cc:subject:date:message-id:reply-to;
        bh=od5AetWuVcdNN64sPpeO9zQoUefUbjoZi5fapWJ5GXE=;
        b=SQSmdq1tkpDamNZqp6sluyE3rTOrYwf0Wie0+ATbxmXBEjHbzJDHv+1Cn9s/bPb9PM
         GIdF+U2SYIRt+B4x5w9/jvGjiJX7fxaikjcOrsYbQttOaO9rI9Gn4lNRhdQydxvjrG7m
         2bIxENALbbif1ih21GyMdaAx+qCYQuCilbBs7wd9RgfaSeH1cOS7yTDTpZoPw2fZ4fCd
         RaDp0Zcu7Pa7D9f0LrTAil2De3BXtL9kYNnHefdhBmISHqcDYDqIDxX5c8X/wpgfA4rD
         5y9Zp1URIi61h9PFckzDXrqR9ovwSonNn2+8E6JEPHwVfYVBxfSLyERoAc6rU+/kO2Ao
         tpsQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20210112; t=1678700608;
        h=to:subject:message-id:date:from:in-reply-to:references:mime-version
```

Ransomware

- **Ransomware** și **Ransomware-as-a-Service** reprezintă un alt risc cibernetic critic pentru serviciile financiare. În timpul unui atac de tip ransomware atacatorii blochează accesul victimelor la computerele lor prin criptarea informației cu malware
- Daunele pot fi inversate doar dacă se plătește o răscumpărare ?! (raport)
- Atacatorii folosesc mai multe metode pentru a pune presiune pe victime să plătească răscumpărarea. Cea mai populară metodă este publicarea treptată a unor porțiuni tot mai mari de date sensibile capturate pe web până când este plătită răscumpărarea
- Astfel de tactici sunt foarte eficiente împotriva instituțiilor financiare, deoarece reglementările stricte impun politici speciale în fața atacurilor cibernetice și a divulgării de date personale



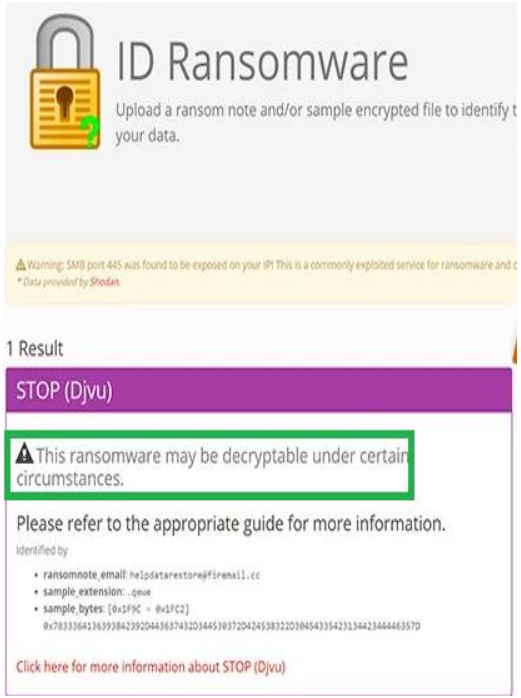
Ransomware

- **Cele mai cunoscute tipuri:**

- ✓ **Sodinkokibi** –> *How to remove*
- ✓ **Conti V2** –> *How to remove*
- ✓ **Lockbit** –> *How to remove*
- ✓ **Clop** –> *How to remove*
- ✓ **Egregor** –> *How to remove*
- ✓ **Avaddon** –> *How to remove*
- ✓ **Ryuk** –> *How to remove*
- ✓ **Darkside** –> *How to remove*
- ✓ **SunCrypt** –> *How to remove*
- ✓ **Netwalker** –> *How to remove*
- ✓ **Phobos** –> *How to remove*

Ransomware

- Una dintre cele mai simple și rapide modalități pentru a identifica o infecție ransomware este utilizarea site-ului web ID Ransomware:



ID Ransomware

- Acest serviciu detectează în prezent **1159** de tipuri diferite de ransomware.
- O listă parțiala (A-C) a ceea ce este detectat în prezent**:**

AAC, ABCLocker, Abyss Locker, ACCDFISA v2.0, AdamLocker, Adhubllka, Admin Locker, AES_KEY_GEN_ASSIST, AES-Matrix, AES-NI, AES256-06, AESMew, Afrodita, AgeLocker, Akira, Ako / MedusaReborn, Al-Namrood, Al-Namrood 2.0, ALC, Alcatraz, Alfa, Allcry, Alma Locker, Alpha, AMBA, Amnesia, Amnesia2, Anatova, AnDROid, AngryDuck, Annabelle 2.1, AnteFrigus, Anubi, Anubis, AnubisCrypt, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ApolloLocker, ARCrypter (Chile Locker), AresCrypt, Argus, Aris Locker, Armage, ArmaLocky, Arsium, ASN1 Encoder, AstraLocker, Ataware, Atchbo, Aurora, AutoLocky, AutoWannaCryV2, Avaddon, AVCrypt, Avest, AvosLocker, AWT, AxCrypter, aZaZeL, Azov Wiper, B2DR, Babaxed, Babuk, BabyDuck, BadBlock, BadEncript, BadRabbit, Bagli Wiper, Bam!, BananaCrypt, BandarChor, Banks1, BarakaTeam, Bart, Bart v2.0, Basilisque Locker, BasnEncrypter, BB Ransomware, Beast, BeijingCrypt, BetaSup, BianLian, BigBobRoss, BigLock, Bisamware, Bisquilla, BitCrypt, BitCrypt 2.0, BitCryptor, BitKangoroo, Bitpaymer / DoppelPaymer, BitPyLock, Bitshifter, BitStak, BKRansomware, Black Basta, Black Buy, Black Claw, Black Feather, Black Shades, BlackByte, BlackCat (ALPHV), BlackHeart, BlackHunt, BlackKingdom, BlackMatter, Blackout, BlackRuby, BlackSuit, Blind, Blind 2, Blocatto, BlockFile12, Blooper, Blue Blackmail, BlueSky, Bonsoir, BoooamCrypt, Booyah, BrainCrypt, Brazilian Ransomware, Brick, BrickR, BrightNight, BTCamant, BTCWare, BTCWare Aleta, BTCWare Gryphon, BTCWare Master, BTCWare PayDay, Bubble, Bucbi, Bud, Bug, BugWare, BuyUnlockCode, c0hen Locker, C3rb3r, Cactus, Cancer, Cassetto, CatB, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberImposter, CerberTear, Chaos, CheckMail7, Checkmate, Cheers, Chekyshka, ChernoLocker, ChiChi, Chimera, ChinaJm, ChinaYunLong, ChineseRarypt, CHIP, Cicada3301, CiphBit, ClicoCrypter, Clop, Clouded, CmdRansomware, CNHelp, CobraLocker, CockBlocker, Coin Locker, CoinVault, Combo13 Wiper, Comet, Comrade Circle, Conficker, Consciousness, Conti, CoronaVirus, CorruptCrypt, Cossy, Coverton, Cr1ptT0r Ransomware, CradleCore, CreamPie, Creeper, Crimson, Cripton, Cripton7zp, Cry128, Cry36, Cry9, Cryakl, CryCryptor, CryFile, CryLocker, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt0r, Crypt12, Crypt32, Crypt38, Crypt3r / Ghost / Cring, CryptConsole, CryptConsole3, CryptFuck, CryptGh0st, CryptInfinite, CryptoApp, CryptoDarkRubix, CryptoDefense, CryptoDevil, CryptoFinancial, CryptoFortress, CryptoGod, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLockerEU, CryptoLocky, CryptoLuck, CryptoMix, CryptoMix Revenge, CryptoMix Wallet, CryptON, Crypton, CryptoPatronum, CryptoPokemon, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, CryptoViki, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, Crystal, CSP Ransomware, CTB-Faker, CTB-Locker, Cuba, CXK-NMSL, CyberVolk, Cyborg, Cyrat

Atacuri de tip DDoS

- Atacurile de tip **DDoS** (*Distributed Denial of Service*) reprezintă o amenințare cibernetică populară împotriva serviciilor financiare, sunt utilizate metode foarte diverse, este inclusă infrastructura IT, conturile clienților, portalurile de plăți etc.

- Impactul atacurilor DDoS este mai profund pentru entitățile financiare

- În timpul unui atac cybernetic de tip Ddos haosul rezultat poate fi exploatat în două moduri diferite:

  - ✓ **Sunt lansate atacuri cibernetice suplimentare** în timp ce echipele de securitate sunt distrase de atacul DDoS (pregătește terenul pentru atacuri mai tehnice!)

  - ✓ **Este cerută o sumă de bani pentru a opri atacul DDoS**

- Atacurile care au vizat identificarea unor date de autentificare prin intermediul unui scenariu de tip DDOS au fost printre cele mai comune 2 tipuri în domeniul portalurilor de plată online

- Real-time DDoS Attack Map: **link**

- Live Cyber Threat Map: **link**

Cum îmi generez o parolă/certificat digital

- **Resursă: *https://github.com/laurentiucretu68/ase-cybersecurity***

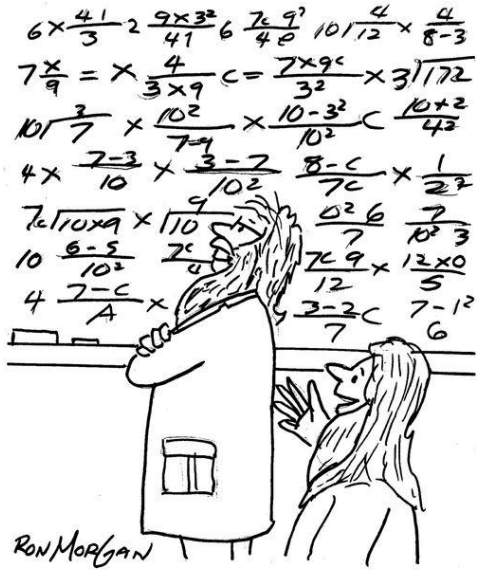
- ***OpenSSL*** este o librărie *open-source* utilizată pentru criptarea și comunicarea securizată pe rețea. Acronimul SSL vine de la *Secure Socket Layer*, un protocol criptografic care asigură confidențialitatea și integritatea datelor transmise între două părți (un client și un server)

- ***OpenSSL*** oferă o gamă largă de funcționalități, precum:

✓ Criptare simetrică
✓ Criptare asimetrică
✓ Generarea de chei și certificate digitale

- Idee cadou luna martie (**link**): ***stick USB Kingston IronKey D300S***

- **Temă**: Criptarea/decriptarea simetrică a unui mesaj/fișier



"You've done it - you've come up with the perfect password."

Concluzii

- Autentificare, transmis date => strict criptat/https
- Verificati certificatele utilizate pentru criptarea traficului
- Plata on-line doar prin intermediul unor operatori recunoscuti, poate carduri dedicate/ speciale (plata in 2 pasi);
- Nu accesati link-uri, atasamente ale unor mail-uri care nu par legitime
- Verificati detaliile (mesajul original) pentru mesajele neașteptate/suspecte
- Incercati utilizarea unei solutii care cripteaza traficul (VPN)
- Evitati conectarea la retele publice
- Limitati utilizarea retelelor wireless

Vă mulțumesc!