Curs 2-3

Aplicații malware.
Clasificarea aplicațiilor malware
Evoluția aplicațiilor malware

Prefață

- 1944, John von Neumann, seminarii cu titlul: *Theory of Self-reproducing Automata* (doar în teorie).
- Primii viruși au apărut abia 40 de ani mai târziu.

Aplicații malware

- Viruși
- Viermi
- Troieni
- Rootkit-uri
- Spyware
- Adware
- Dialer-e
- Retele botnet & Zombies
- Phishing & Social engineering
- Scareware
- APT
- Crypto-ransomwar

Virușii informatici

- Definiție: program care se replică fără știința utilizatorului și infectează sistem după sistem, transmiterea de la un sistem la altul făcându-se print intermediul unui **vector de transmitere**. Printre vectorii uzuali de transmitere: mediile de stocare (floppy disk-uri în anii 80 si 90, memorii USB în prezent) dar și rețelele de calculatoare odată cu dezvoltarea exponențială a acestora.
- Definiția a fost dată de Fred Cohen, profesor la Universitatea de Sud California într-o lucrare denumită: *Computer Viruses - Theory and Experiments* (1984).
- În prezent, sub denumirea de virus informatic sunt catalogate toate categoriile de programe malware precum programele adware și

Viermi

- Au apărut odată cu dezvoltarea rețelelor de calculatoare și a rețelei Internet.
- Exploatează de obicei procese server vulnerabile.
- Se replică din sistem în sistem (un vierme infectează un sistem, în timp ce virus infecta un fișier).
- Spre deosebire de un virus, un vierme (codul său) rezida în

Troieni

- Aplicații malware care pretind ca fac ceva dar de fapt fac altceva.
- Exemple: aplicațiile de tipul keygen folosite pentru înregistra unele softuri piratate.
- Este recomandată rularea aplicațiilor de proveniență îndoielnică într-o mașină virtuală

Rootkit-uri

Folosite de atacatori pentru:

- a-și ascunde urmele în cadrul unui sistem a cărui securitate a fost penetrată (sistem „spart”);
- oferirea unei “portițe” de acces mai facil pe viitor a atacatorului asupra sistemului - **backdoor**.

Un backdoor poate oferi atacatorului:

- port alternativ deschis de un proces pentru a oferi conectivitate oricând atacatorului;
- proces care rulează local periodic printr-un mecanism oferit de sistemul de operare (cron pe Linux, scheduled task în Windows) care face callback (conexiune inversă) la un server

Ascunderea urmelor atacatorului prin intermediul unui rootkit

Pentru a ascunde urmele atacatorului (fișierele create de atacator, procesele rulate), un rootkit se integrează in cadrul sistemului de operare prin două modalități:

- În așa numitul user space (nivel aplicație) prin suprascrierea comenzilor uzuale ale sistemului de operare, gen: ls, ps, netstat pentru a ascunde fișierele/procese create de atacator, inclusiv fișierele propriu-zise ale rootkit-ului;
- În așa numitul kernel space (la nivelul nucleului sistemului de operare) prin redirectarea anumitor apeluri sistem oferite de sistemul de operare respectiv, astfel de redirectări având impact direct asupra aplicațiilor de la nivel aplicație care afișează utilizatorului aceste resurse (fișiere, procese)

Spyware & Adware

- Populare odată cu dezvoltarea rețelei Internet și comportamentul utilizatorilor de a petrece cât mai mult timp "online"
- Se instalează fără un acord explicit al utilizatorului, fie ca aplicații 3rd party
- Uneori vin sub forma unor aplicați asemănătoare troienilor (dar mai puțin dăunătoare), gen free screensavers, free smileys with sound, toolbar-uri, etc.
- Urmăresc activitatea utilizatorului pentru ai crea un profil
- Rulează în background, analizează

Motive de clasificarea a lor ca aplicații malware:

- încărcarea și încetinirea sistemului (majoritatea fiind aplicații standalone);
- îngrijorări legate de aspecte ce țin de user privacy - (intimitatea sau poate un termen mai bun în limba romana confidențialitatea datelor

Dialer-e

- aplicații malware la modă la sfârșitul anilor 90 începutul anilor 2000 când lumea se conecta la Internet prin intermediul unui modem folosind conexiuni dial-up
- calculatoarele infectate sunau prin intermediul unui modem la un număr cu suprataxă
- ținând cont de popularitatea conexiunilor dial-up în acea perioadă, astfel de aplicații erau și ele destul de populare
- principala motivație: financiară
- au revenit la moda în prezent odată cu

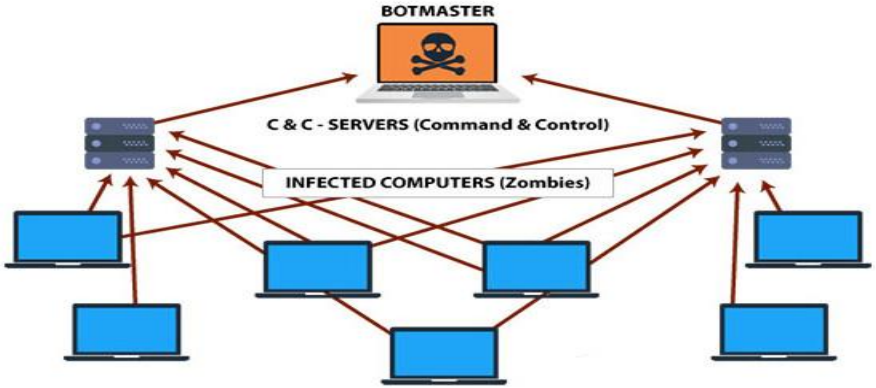
Rețelele botnet & calculatoarele zombii

Botnet

- calculatoare infectate cu diferite aplicații malware aflate sub controlul aceleiași organizații sau individ (bot herder sau botmaster).

Zombie

- calculator infectat ce face parte dintr-un botnet.



Scopuri: în principal financiare

- Trimiterea de spam-uri
- Flood & DDOS

Rețele botnet (exemple)

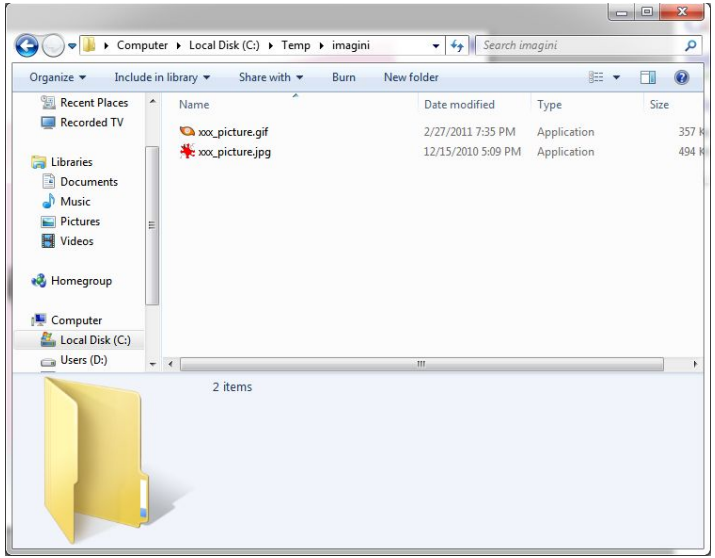
Data	Nume	Număr de calculatoare zombie controlate	Capacitate
2016	Mirai	380,000	Device-uri IoT Linux (camere IP sau routere)
2013	Chameleon	120,000	6 million $/lunar afișarea de reclame
2009	BredoLab	30,000,000	3.6 miliarde spam-uri / zi
2008	Mariposa	12,000,000	NA
NA	Conficker	10,500,000	10 miliarde spam-uri / zi
2007	Cutwail	1,500,000	74 miliarde spam-uri / zi
NA	Grum	560,000	39.9 miliarde spam-uri / zi
2007	Srizbi	450,000	60 miliarde spam-uri / zi
2006	Rustock	150,000	30 miliarde spam-uri / zi

Phishing & Social Engineering

- Tehnicile de Social Engineering constau în manipularea și inducerea în eroare a utilizatorilor mai puțin instruiți, avizați și necunoscători din punct de vedere tehnic.
- Tehnicile de phishing (care presupun de obicei clonarea site-ului unei instituții bancare) se bazează tot pe neatenția sau lipsa discernământului utilizatorului de a detecta site-ul contrafăcut - uneori reproducerea este atât de fidelă încât nu se poate face diferența vizual între site-ul original și clonă, existând alte elemente care pot sugera însă diferența (URL-ul din

Folosirea unor tehnici de tip "social engineering" de către viruși

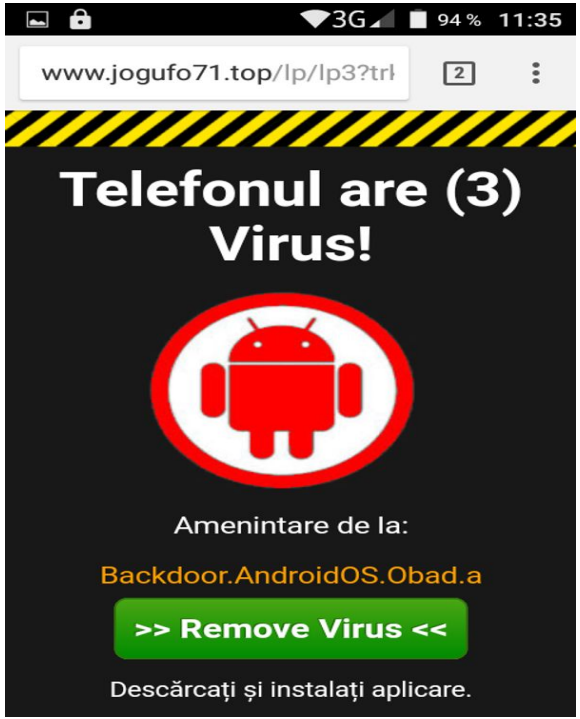
Inducerea în eroare a utilizatorilor mai puțin instruiți. Exemple:



- Ascunderea implicită a extensiei de către Windows pentru fișierele " înregistrate" (extensii care au asociate un program care să deschidă fișierele cu aceasta extensie). Exemple:
  - fisier.txt.vbs,
  - xxx_picture.jpg.exe
- Folosirea extensiei .com în numele unui "virus dropper" care mimează un URL: www.exemple.com (remarcați extensia ".com" a unui fișier cu numele "www.example");
- Pentru virușii transmisibili prin e-mail, un calculator odată infectat, trimite e-mailuri automat tuturor contactelor

Scareware

- nu sunt aplicații malware în adevăratul sens al cuvântului , se bazează pe lipsa de cunoștințe și neștiința utilizatorului de rând pentru al "speria" (tot o tehnică de social engineering)
- exemple: pagini web ce imitau look and feel-ul unei ferestre a sistemului de operare - simulau prin intermediul unei animații o scanare a calculatorului (utilizatorii de rând nu știu că o fereastră de browser nu le poate accesa sistemul de fișiere local)
- mai nou prezente inclusiv pe dispozitive mobile
- motivație financiară: forțarea utilizatorului să plătească fără să fie cazul pentru o devirusare inexistentă sau forțarea acestuia



APT – Advanced Persistent Threat

- cea mai avansată forma de aplicații malware, folosite in general in scopuri precum culegerea de informații, spionaj, etc.
- in spate la un APT sta un actor statal sau un grup de atacatori sprijinit/sponsorizat de un actor statal
- spre deosebire de alte aplicații malware care infectează la întâmplare sistem după sistem, un APT target-ează un anumit sistem sau o anumita rețea, fiind deseori create / customizate pentru sistemul sau rețeaua target-ată
- greu de detectat, unul din scopurile unui APT este să rămână cat mai mult timp ascuns pentru a facilita culegerea de informații pentru o perioada mai lunga de timp
- pentru a și atinge scopurile, creatorii unui APT pot afecta / penetra inclusiv lanțul de producție a unor dispozitive hardware sau aplicații software – adică un echipament sau soft de încredere să

Crypto-ransomware

Aplicațiile malware de tip Crypto-ransomware combină mai multe aspecte /paradigme:

- Criptografia asimetrică cu cheie publică / cheie privată pentru criptarea fișierelor utilizatorului – cheile private de decriptare fiind doar în posesia atacatorului;
- Vulnerabilități cunoscute / proaspăt descoperite pentru a se propaga prin diverse canale (în special e-mail, dar și linkuri distribuite spre malware-ul găzduit pe diverse site-uri sparte);
- Cer răscumpărare pentru decriptarea fișierelor (neexistând nicio garanție în acest sens), veniturile obținute în urma unei campanii ransomware fiind de ordinul milioanelor de dolari în criptomonede (pentru a face plățile de răscumpărare greu de urmărit, dacă nu imposibil);

Motivație

De ce sunt create aplicații malware?

- primele forme de malware din teribilism;
- predispoziția psihologică a unora de a face rău;
- motivație financiară (monetizare): trimiterea de spam-uri contra cost, culegerea de date bancare/personale care să fie valorificate, răscumpărări Crypto-ransomware;
- spionaj, culegerea de informații (cyber weapons).

Viruși vs. Viermi

Virușii:

- se atașează unei gazde: sector de boot, fișier executabil, e-mail;
- un virus în accepțiunea clasică a termenului nu poate exista de sine stătător, el trebuie să se "lipească" de gazda pe care o infectează (fișier executabil, sector de boot);
- gazda infectată este transmisă din sistem in sistem prin intermediul vectorului de transmisie (discheta, stick-ul USB, rețeaua Internet);
- presupun intervenția utilizatorului uman pentru execuție: introducerea dischetei în calculator, execuția unui fișier, deschiderea unui atașament

Viermi:

- se multiplică automat prin intermediul unei rețele de calculatoare, fără intervenție umană;
- nu au nevoie de o gazdă (de fapt gazda e întregul sistem infectat), codul acestora putând fi memorat în mai multe fișiere;
- se bazează pe vulnerabilități întâlnite în cadrul serviciilor/daemon-ilor/proceselor server sau a stivei TCP/IP a sistemului țintă.

Ușor de confundat ca termeni deoarece:

- propagarea prin e-mail a anumitor viruși, e-mailuri transmise tot prin intermediul rețelei Internet;
- caracterul hibrid virus / vierme a anumitor programe malware;

Viruși macro pentru fișiere Microsoft Office

- Limbaj Macro: limbaj built-in în cadrul unei aplicații software pentru a permite customizarea sau automatizarea anumitor acțiuni întreprinse în cadrul aplicației de către utilizator;
- În cadrul pachetului Microsoft Office, se permite scrierea de instrucțiuni macro care să fie încorporate în cadrul documentelor și executate la deschiderea acestora;
- Exploatează un nou tip de gazdă / mediu de transmisie, utilizatorii nu mai trebuie să partajeze medii de stocare sau diferite programe (jocuri) ci documente: mediu propice de răspândire – rețele Enterprise cu un flux ridicat al documentelor între departamente;
- Independente de sistemul de operare, spre exemplu macrovirușii care infectează documente Microsoft Office (Word și Excel) pot afecta atât sisteme Windows cât și MacOS.
- Primul macrovirus: WM.Concept aparut în 1995.

Evoluția limbajelor în care au fost / sunt scriși virușii

- primii viruși - în limbaj de asamblare;
- virușii macro - limbaje de scripting (Visual Basic for Applications);
- viermi stand-alone scriși în orice limbaj / multiple limbaje de programare;
- limbaje diferite, tehnologii diferite, platforme diferite și multiple în cazul aplicațiilor malware

Evoluția metodelor de execuție

- viruși de boot infectau sectorul de boot al dischetelor și se executau odată cu încărcarea sistemului de operare - primele calculatoare personale din anii '80 boot-au de pe dischete, hardisk-urile nefiind populare
- infectau la început fișierele executabile .com și .exe și se executau odată cu aceste executabile
- viruși rezidenți în memorie datorită caracterului monotasking ale primelor sisteme de operare. Pentru a rămâne rezidenți în memorie, aceștia redirectau diferite rutine de tratare a întreruperilor / apeluri sistem și se executau odată cu execuția rutinei / apelului sistem redirectat
- odată cu dezvoltarea sistemelor de operare multitasking și apariția viermilor, aceștia puteau executa diferite module ca procese independente, pornite la start-up prin diverse mecanisme, execuția de taskuri automate (cron pe Linux sau

Evoluția metodelor de replicare/execuție

- Sisteme de operare monotasking, execuția codului virusului avea loc prin 2 mecanisme:
  - Odată cu execuția unui fișier infectat codul virusului rulând la începutul rulării executabilului;
  - Rămânerea rezidentă în memorie și redirectarea unor apeluri sistem / întreruperi care se execută la apariția unor evenimente.
- In cadrul sistemelor de operare multitasking, replicarea este facilitată de faptul că virusul in sine poate instanția procese separate care să ruleze in paralel.
- In cadrul sistemele de operare multiutilizator (utilizatori diferiți cu privilegii diferite), este nevoie de exploatarea unor **vulnerabilități locale** pentru a duce la **escaladare de privilegii**

Evoluția vectorilor de transmitere a virușilor

- dischete – mediul propice atât pentru virușii de boot cât și pentru virușii ce infectau fișiere executabile - în anii 80, 90 dischetele erau și principala formă de file sharing, programe (în special jocuri) infectate;
- sisteme BBS - Bulletin Board System - primele mecanisme de file sharing folosite pe scară largă;
- odată cu dezvoltarea rețelei Internet apariția viermilor (viruși "stand-alone"):
  - exploatau diferite vulnerabilități întâlnite în cadrul serviciilor/daemon-ilor/proceselor server sau a stivei TCP/IP a sistemului țintă;
  - transmisibili prin e-mail;
  - linkuri transmise prin mesageria instant;

Bibliografie

- John von Neumann, *Theory of self-reproducing automata*, http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf
- Fred Cohen, *Computer Viruses - Theory and Experiments*, https://www.profsandhu.com/cs5323_s18/cohen-1987.pdf
- *Computer virus** http://en.wikipedia.org/wiki/Computer_virus