Curs 5-6

Evoluția aplicațiilor malware.
Exemple.

Arhitectura unui virus (clasic) și ciclul său de viață

2 module:
- cod de multiplicare;
- codul dăunător;

2 (sau 3) perioade în durata de viață a unui virus:
- perioada de incubație (execuția codului de multiplicare);
- perioada de activare (execuția codului dăunător);
- auto shutdown (la unii viruși).

Activarea se face de obicei:
- la scurgerea unui interval de timp fix de la infectarea sistemului;
- la o anumita data fixa;
- la anumite date cu un anumit pattern (ex. zilele de vineri 13);
- în cazul viermilor după detectarea infectării a unui anumit număr de alte sisteme;
- în cazul calculatoarelor zombie din rețele botnet la primirea unei comenzi de la botmaster;
- în cazul ransomware, după criptarea unui anumit număr de fișiere.

Acțiuni întreprinse de codul dăunător

- inofensive (afișarea de mesaje) ;
- distructive software: ștergerea de fișiere, criptarea fișierelor, distrugerea tabelei de partiții;
- consumatoare de resurse: încetinirea sistemului, ocuparea lățimii de banda în Internet, atacuri de tip DDOS;
- destructive hardware: distrugerea BIOS-ului calculatorului (vezi CIH), uzarea unor sectoare ale hardisk-ului prin scrieri repetate și continue ale acelorași sectoare

Mutații ale virușilor

- Viruși polimorfi:
  - infectează un fișier cu o copie criptată a virusului;
  - cheia de decriptare e de fiecare data alta, aleasă aleator;
  - codul virusului se schimbă, detecția devine mai dificilă;
  - virusul conține un modul de decriptare a codului său care nu este criptat, detecția se poate face pe baza acestui modul, însă multe executabile și vendori de programe adopta metoda criptări pentru a descuraja tehnicile de dezasamblare și reverse engineering;
- Viruși metamorfici:
  - se rescriu de fiecare dată folosind noi instrucțiuni, însă păstrează algoritmul de bază implementat de virus același;
  - mecanisme de rescriere: folosirea aleatoare de instrucțiuni NOP, schimbarea regiștrilor folosiți, rearanjarea ordinii instrucțiunilor independente;
  - "code integration": imbricarea aleatoare a instrucțiunilor virusului cu instrucțiunile executabilului infectat.
- Variante ale unui virus rescrise de terți

Viruși bazați pe instrucțiuni de virtualizare

- Doar în teorie, nu s-a descoperit existența unui asemenea virus;
- Proiectul "Blue Pill", Joanna Rutkowska, cercetător antivirus polonez;
- Presupun folosirea de către virus a instrucțiunilor de virtualizare oferite de procesoarele noi pentru un mai bun suport a mașinilor virtuale și a se “ascunde” sub sistemul de operare (sistemul de operare devine o mașină virtuală, iar virusul un soft de virtualizare);
- Se bazează pe ideea ca un antivirus instalat în cadrul unei mașini virtuale nu poate detecta infecția sistemului de operare gazdă.

Idee de disertație (pentru cei interesați): În ce măsura un bug într-un soft de

Sisteme antivirus

- 1988 - Lista de discuții prin e-mail despre diferiți viruși și metode de dezinfectare a sistemelor infectate. Printre membri acestei liste s-au numărat John McAfee și Eugene Kaspersky.
- Primii antiviruși doar scanau;
- Checksum ale fișierelor pentru o scanare rapidă și a detecta eventuale modificări ale acestora de către viruși;
- În cadrul sistemelor de operare monotasking: antiviruși TSR (Terminate and Stay Resident);
- Odată cu dezvoltarea sistemelor de operare multitasking, antiviruși ca procese separate
- În prezent oferă soluții complete de protecție: antivirus, antimalware, (privacy protection) antispyware, antiadware, firewall, linkscanner, antiphishing.

Tipuri

- Standalone (calculatoare personale);
- Pentru servere, mailserver-e, router-e, firewall-uri, etc;

Industria antivirus & virușii

- Acuzații nedovedite de creare de viruși pentru a avea piață pentru sistemele antivirus;
- Exagerării în media și online asupra impactului și a gradului de periculozitate a unui anumit virus, de asemenea tot pentru a-și dezvolta piața.

Metode de scanare:

Evoluția numărului de viruși existenți

- 2007 (conform Symantec):
  - 711.000 noi viruși, o creștere de 468% fata de 2006;
- 2010 (conform G Data SecurityLabs):
  - peste 2.000.000 noi virusi in 2010, cu o creștere de 50% față de 2009;
- 2015 (conform CNN Tech)
  - 300.000.000 forme de malware

Facts:

- providerii de soluții antivirus exagerează pentru a-și vinde mai bine produsele;
- mulți viruși creați în trecut nu mai reprezintă un pericol pentru sistemele de operare și arhitecturile actuale (spre

Primii viruși

- Elk Cloner, 1981, Rich Skrenta (15 ani) - virus de boot infecta calculatoarele Apple II;
- Brain, 1986, primul virus care afecta calculatoarele IBM-PC compatibile ce rulau MS-DOS (scris de frații Basit and Amjad Farooq Alvi, Pakistan) - scris inițial pentru detectarea versiunilor de software piratat;
- Whale, 1990 primul virus polimorfic

Viruși Celebri – CIH (1998)

- Cel mai cunosc virus care "defecta" hardware un sistem prin coruperea BIOS-ului sistemului;
- Creat în Taiwan în 1998, dar programat să se activeze un an mai târziu;
- Inițial plasat într-un update de firmware pentru unități optice Yamaha; mai târziu calculatoare personale IBM fiind livrate spre retailer-i gata infectate;
- Autorul Chen Ing Hau (de la inițialele sale și numele virusului) nu a fost pus sub acuzare niciodată (constituția și legile Taiwaneze din anul 2000 nu incriminau sub nici o formă acțiunile sale), legi privind criminalitate informatică fiind adoptate in Taiwan abia în 2003 (urmare a epidemiei provocate de acest virus);

Viruși Celebri - Morris worm (1998)

- 1988 – primul vierme cu replicare automată;
- Infecta sistemele UNIX bazându-se pe diferite vulnerabilități ale acestora;
- Scris de Robert Tappan Morris, student la Cornell University și lansat din cadrul rețelei MIT; condamnat la 400 de ore în folosul comunității si 10.000$ amenda;
- Cofondator a Viaweb, vândută pentru 48 de milioane de dolari $ și devenită ulterior Yahoo! Store;

Virușii Celebri – Melisa (1999)

- Primul macrovirus răspândit pe scară largă în Internet, 1999;
- Deși se dorea inofensiv, a dus la blocarea serverelor de mail din Internet datorita supra-încărcării acestora;
- Răspândit inițial prin intermediul unui fișier ce conținea parole de acces la site-uri cu conținut pentru adulți;
- Creat de David Smith care deși a fost condamnat la 10 ani de închisoare, a ispășit doar 20 de luni și a primit o amenda de 5000$. Mai târziu, a ajutat FBI-ul

Viruși Celebri - I Love You (2000)

- 4 mai 2000 (fișier vbs transmis prin e-mail numit LOVE-LETTER-FOR-YOU.TXT.vbs, extensia .vbs nu era afișata de către Windows);
- în 9 zile 50 de milioane de calculatoare infectate;
- daune estimate la 5.5 miliarde $;
- a afectat rețelele pentagonului, CIA, parlamentului Britanic;
- Sursa: doi studenți filipinezi
  - neacuzați in final, în lipsa legislației filipineze în domeniu;
  - legea adoptată în iulie 2000 la 2 luni de la lansarea

Viruși Celebri – Nimda (2001)

- primul vierme multi-vector cu răspândire pe mai multe canale;
- infecta toate versiunile de Windows de la 95 la XP, atât orientate desktop cât și server;
- folosea cinci mecanisme diferite de propagare:
  - prin e-mail;
  - prin directoare partajate în rețea neprotejate;
  - navigarea pe site-uri compromise;
  - exploatarea unor vulnerabilități prezente în IIS 4.0 și IIS 5.0;
  - prin intermediul unor backdoor-uri lăsate anterior de alți virușii.

Viruși Celebri – MyDoom (2004)

- Apărut în 26 ianuarie 2004, cel mai celebru vierme din toate timpurile, răspândidu-se prin e-mail dar și prin intermediul rețelelor P2P;
- Transforma sistemul infectat într-un sistem zombie, plasat sub controlul unui Bot Master;
- Sisteme infectate au fost folosite pentru a trimite spam-uri dar și in atacul de tip DDOS împotriva Sco;
- Virusul nu permitea sistemelor infectate să acceseze site-uri și domenii ale principalelor companii antivirus;
- În primele 24 de ore de la apariție era răspunzător de 10% din traficul e-mail din Internet;
- La o zi de la apariție, Sco a oferit o recompensă de 250.000$ pentru prinderea autorului virusului;
- La două zile de la prima apariție apare o noua versiune, cu un atac identic de tip DDOS asupra Microsoft. Microsoft oferă și ei o recompensă similară. MyDoom este răspunzător de 20% din traficul e-mail din Internet;
- La 6 luni de la apariție, o variantă (clonă a virusului) atacă Google, paralizând

Santy, primul "webworm" cunoscut în Internet (2004)

- se baza pe o vulnerabilitate din cadrul phpBB (open source bulletin board software);
- folosea Google pentru a găsi noi sisteme vulnerabile și a se răspândi în Internet;
- în trei ore de la lansare s-a răspândit pe tot globul, în 24 de ore a afectat între 30.000 și 40.000 de sisteme;
- Google a filtrat, într-un final, search query-ul folosit de vierme pentru a localiza noi sisteme vulnerabile;
- un update (patch) exista deja la momentul lansării viermelui;
- printre primii viermi pentru care a fost lansat în Internet un anti-worm.

Viruși Celebri - RavMonE (2006)

- celebru mai degrabă faptului că un număr limitat de iPod-uri Video de la Apple au ieșit din fabrică în 2006 virusate cu acest virus;
- demonstrează că aplicațiile malware se pot răspândi și pe canale “oficiale”, soft legitim, lanțuri de furnizori hardware și softwar

Conficker (2008)

- exploata diverse vulnerabilități în procese server de pe sistemele de operare Microsoft;
- a infectat între 9 și 15 milioane de sisteme rulând Windows;
- dezactivează update-urile Windows și blochează anumite cereri DNS;
- nu provoacă daune foarte mari pentru că creatorii săi (din spațiul exsovietic) l-au abandonat după ce infecția s-a răspândit mai mult decât au crezut inițial și pentru a nu atrage atenția asupra lor.

CryptoLocker (2013)

- printre primele aplicații de tip ransomware care criptau datele utilizatorilor și cereau o „recompensă” pentru decriptarea lor;
- infecția cu CryptoLocker a început în toamna lui 2013 odată cu creșterea prețului Bitcoin (criptomonedele începeau să fie populare);
- distribuit prin intermediul unor troieni, e-mailuri infectate și a unei rețele botnet;
- cripta fișierele folosind criptografie cu cheie publică/ chete privată – cheia privată era deținută doar pe server-ele atacatorilor;
- s-a estimat că criminalii cibernetici au reușit să obțină in jur de 3 milioane $ de la cei ce au plătit recompensa;
- în final sa reușit destructurarea rețelei botnet prin intermediul căreia se distribuia/opera CryptoLocker-ul, recuperându-se o bază

Mirai (2016)

- Malware ce infecta IoT device-uri precum router-e personale și camere IP;
- Se bazează pe faptul ca deseori astfel de echipamente nu sunt actualizate („updatate”) de utilizatori, sau suportul cu update-uri de securitate din partea producătorilor este inexistent;
- Exploata inclusiv faptul că multe echipamente aveau datele de conectare (nume de utilizator / parolă) implicite;
- Codul să sursă este open source disponibil pe GitHub, fiind preluat și de alte aplicații malware ulterioare;
- În jur de 380.000 de device-uri infectate care în principal erau folosite pentru atacuri DDOS (Distributed Denial of Service);
- S-a estimat că un astfel de atac atingea între 620Gbit/s și 1 Tbit/s.

WannaCry (2017)

- Cel mai celebru ransomware din toate timpurile (poate și datorită numelui);
- A afectat i🤦usiv calculatoare doamnelor secretare de la noi de la facultate;
- Afecta calculatoarele cu Windows și cererea de asemenea o răscumpărare în Bitcoin pentru decriptarea fișierelor
- A fost construit pe baza unui exploit „scurs” denumit EternalBlue dezvoltat de NSA (National Security Agency din SUA) ce exploata o vulnerabilitate din Windows;
- La data propagării acestui malware, exista un update (patch de securitate de la Microsoft) care nu era instalat pe multe calculatoare;
- Deși nu afecta direct calculatoarele cu Windows XP, Microsoft a oferit patch-uri de securitate și pentru Windows XP deși acest sistem de operare nu mai primea suport din 2014;
- Originar din Coreea de Nord.

Viruși pentru dispozitive mobile

- Primul malware pentru dispozitive mobile: 2004, realizat de creatorii unui joc numit Mosquito pentru a raporta prin SMS copiile piratate ale jocului (SMS-ul era trimis fără înștiințarea utilizatorului);
- Cabir, dezvoltat în 2004, destinat să atace telefoanele cu Symbian Seria 60 și să se multiplice prin Bluetooth - proof of concept;
- Commwarrior-A, 2005, ținta tot telefoanele cu Symbian Seria 60, se răspandește prin mesaje MMS;
- 2010: Trojan-SMS.AndroidOS.FakePlayer.a, descoperit de laboratoarele Kaspersky, infectează telefoanele cu Android și trimite mesaje SMS la numere cu suprataxă;
- Hummingbad, februarie 2016, 50.000 mobile infectate, afișa 20 de milioane de reclame lunar și genera lunar venituri de 300.000 dolari.

- În prezent, datorită asemănării sistemelor de operare mobile cu cele desktop (iOS, Android ~ kernel linux): vulnerabilități standard ale sistemelor de operare, afectate de aceleași forme de malware, cele mai întâlnite: troieni, adware, spyware, ransomware.
- Principalele cauze: OS neactualizat (bug-uri kernel, bug-uri în diverse servicii sau aplicații client), lipsa suport și update-uri firmware producător, iOS jailbreak, root access Android

Virusul de test Eicar

- Dezvoltat de European Institute for Computer Antivirus Research;
- Util pentru detectarea bunei funcționalitatea a sistemelor antivirus;
- "X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*";
- Executabil valid com.

Bibliografie

- *Timeline of computer viruses and worms** http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms
- Jeremy Paquette, *A History of Viruses* http://www.symantec.com/connect/articles/history-viruses
- Justin Pot, *A History of Computer Viruses & The Worst Ones of Today,* http://www.makeuseof.com/tag/history-computer-viruses-worst-today-case-wondering