

Retele de calculatoare

Introducere in securitate

Lenuta Alboaie (adria@info.uaic.ro)
Andrei Panu (andrei.panu@info.uaic.ro)

Cuprins

- Preliminarii
- Aspecte importante
- Vulnerabilitati
- Atacuri
- Prevenirea si supravietuirea
- Monitorizarea
- Testarea
- Raspunsul la incidente
- Protocoale
- Probleme specifice
- Statistici 2017-2018
- Previziuni 2019

*Multumiri:

Sabin Corneliu Buraga
Dragos Acostachioaie

Preliminarii

- Asigurarea calitatii aplicatiilor (Internet)
 - Corectitudine si robustete (*reliability*)
 - Extindere & reutilizare (*modularitate*)
 - Compatibilitate
 - Eficienta
 - Portabilitate
 - Usurinta in utilizare (*usability*)
 - Functionalitate
 - Relevanta momentului lansarii (*timeliness*)
 - Mentenabilitate
 - Reparabilitate, economie
 - **Securitate**

Preliminarii

- **Incident de securitate** = eveniment aparut in cadrul retelei, cu implicatii asupra securitatii unui calculator sau a retelei
 - Sursa: interiorul ori exteriorul retelei
- **Securitatea este procesul de mentinere a unui nivel acceptabil de risc perceptibil**
 - “*Security is a process, not an end state.*” (Mitch Kabay, 1998)
- **Cracker versus hacker**
- **Realitatea:**
 - Peste 70% din organizatii sufera de pierderi financiare datorate incidentelor de securitate
 - Cauze:
 - Virusi informatici: > 75%, Acte malitioase interne: > 40%, Actiuni malitioase externe: 25%, Erori software: 70%, Spionaj industrial: 10%

Preliminarii

- **Mituri:**

- Securitatea prin obscuritate (*security through obscurity - STO*)
 - “*bunk mentality*” security
 - Ignorarea problemelor
 - Nedocumentarea erorilor cunoscute, algoritmilor de criptare folositi
- Cracker-ii “*ascunsi*” nu pot fi detectati
- Organizarea in grupuri malefice a *crackeri*-lor
 - Deseori nu (exceptii: Cult of Dead Cow, ...)
- Software-ul de scanare de virusi ofera protectie totala
- Conexiunile internet nu pot fi detectate
- Din moment ce un fisier este sters, el se pierde pentru totdeauna

Preliminarii

- Faze ale procesului de securizare:

security audit

- Estimare a riscurilor (*assessment*)

- Activitati manageriale +
actiuni tehnice

- Protejare (*protection*)

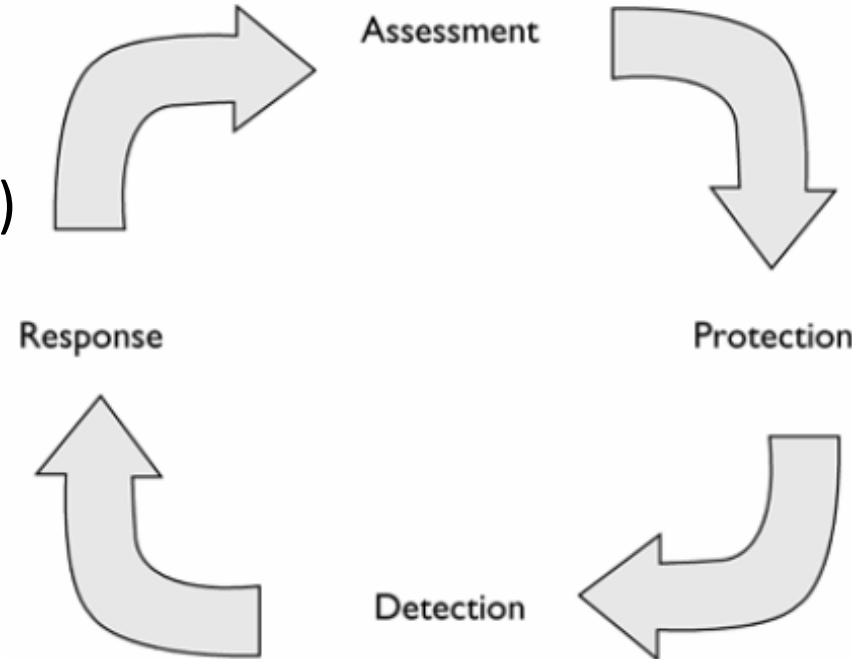
- Prevenire

- Detectare (*detection*)

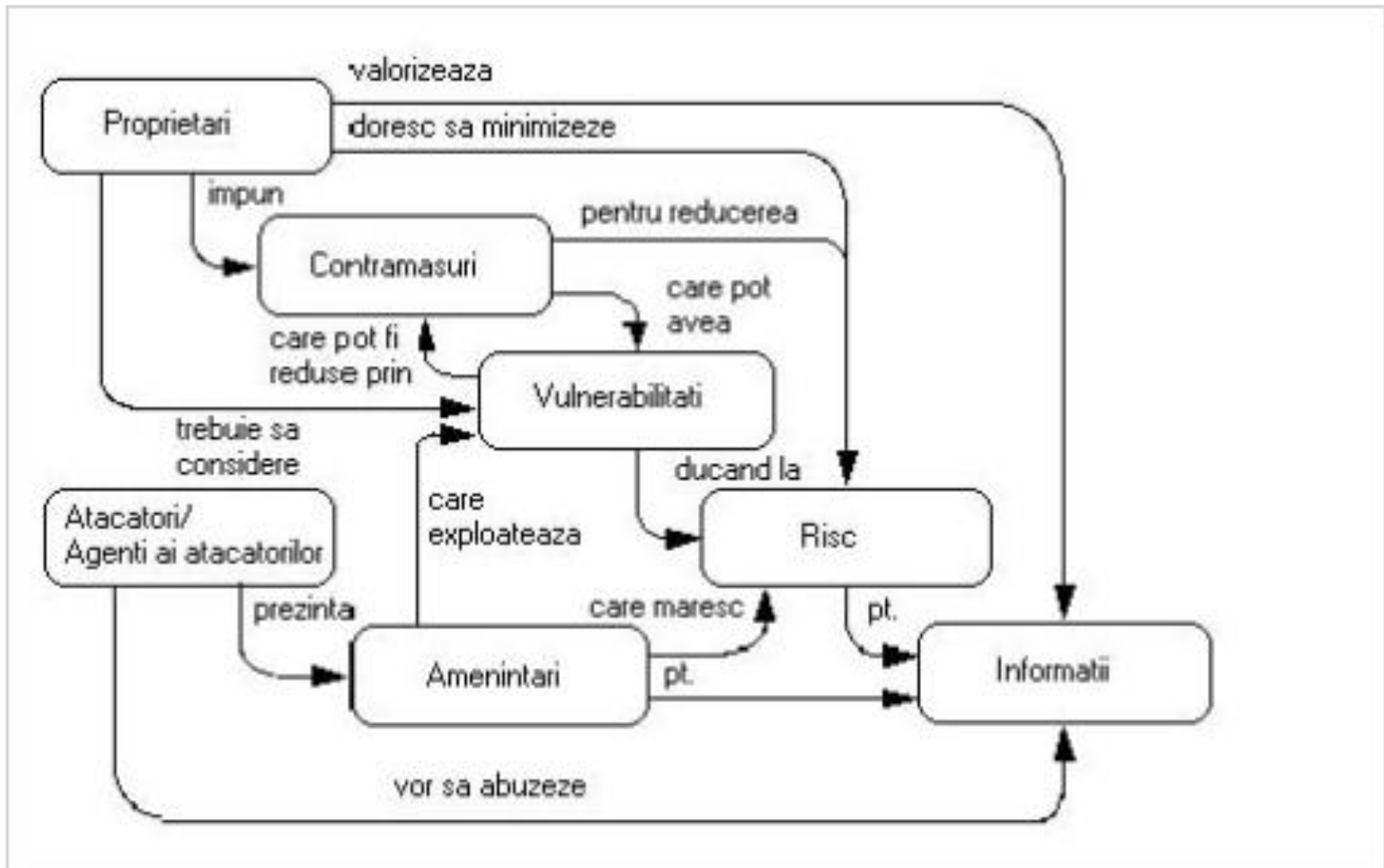
- Identificarea incidentelor (intrusions)

- Raspuns la atacuri (*response*)

- Restaurarea functionalitatii (*patch & proceed*)
- Alegerea remediilor legale (*pursue & prosecute*)



Preliminarii




<http://www.securitatea-informatica.ro/securitatea-informatica/riscurile-de-atac-asupra-securitatii-sistemelor-informationale/>

Forme de protectie

- Controlul accesului
 - Identificarea
 - Autentificarea
 - Autorizarea
 - Acces
- Confidentialitatea
- Intimitatea (*privacy*)
- Integritatea
- Disponibilitatea
- Nerepudierea

Forme de protectie

- **Controlul accesului**

- Proces prin care se ofera sau nu acces la resursa/serviciu
- Terminologie
 - Identificare
 - Exemplu: introducerea *username*
 - Autentificare – “**verify that someone is who they claim they are**”
 - Exemplu: introducerea parolei
 - Serverul ofera suport pentru autentificari de baza sau bazata pe algoritmi de tip *digest* (e.g. *script*, *bcrypt*, *SHA-2*)
 - Ex. mecanisme dedicate: Kerberos, RADIUS, TACACS+,...
 - Autorizare  Eavesdropping [RFC1510](#).
 - “**determines what a user is and is not allowed to do**”
 - Specifica actiunile (rolurile) pe care un utilizator le poate realiza
 - Exemplu: utilizatorul autorizat are dreptul sa fie logat?
 - Acces
 - Politici care definesc efectiv permisiuni sau privilegii
 - Exemplu: accesul utilizatorului la anumite date (intr-un interval orar sau doar de la un anumit IP, setari facebook – cine poate vedea o resursa?)

Forme de protectie

Controlul accesului - Modele

- Mandatory Access Control (MAC)
 - *End-user*-ul nu poate modifica/transfera controlul asupra resurselor
- Discretionary Access Control (DAC)
 - Detinatorul resursei poate acorda drepturi acesteia si altor utilizatori
 - Ex. Apple Macintosh, UNIX, Windows (User Account Control (UAC)) cer aceasta permisiune cand un soft este instalat
- Role Based Access Control (RoBAC)
 - Asigneaza permisiuni unui rol in organizatie, apoi unui utilizator i se asociaza acest rol
- Rule Based Access Control (RuBAC)
 - Asigneaza controlul in mod dinamic unui utilizator pe baza unui set de reguli. Fiecare resursa contine un set de proprietati de acces bazate pe aceste reguli.
 - Exemplu: Cineva din retea A doreste sa acceseze o resursa din retea B; RBAC include regula ca daca cineva are adresa din retea A poate accesa resursele din B;

Forme de protectie

- **Controlul accesului** – Implementari
 - Sisteme de control - la nivel hardware
 - Accesul la terminal (e.g. verificarea amprentelor, senzori *real-time anti-break*)
 - Visual event monitoring
 - Carduri de identificare
 - Identificare biometrica (e.g. recunoastere - fingerprint, iris & voice recognition)
 - Sisteme de control - la nivel software
 - Drepturi de acces (permisiuni) + liste de control al accesului (ACL – *Access Control List*)
 - Tehnici de tip SSO (*Single Sign-On*)

Forme de protectie

- **Confidentialitatea**

- Imposibilitatea unei terte entitati sa aiba acces la datele vehiculate intre doi receptori
- Solutii:
 - Conexiuni private intre cele 2 puncte terminale ale canalului de comunicatie; datele circula printr-un tunel oferit de o retea privata virtuala (VPN – *Virtual Private Network*)
 - Criptarea datelor via diverse tehnici (biblioteci specializate si/sau oferite de mediile de dezvoltare)
 - Emitatorul cripteaza mesajele
 - Receptorul decripteaza mesajele

Forme de protectie

- **Intimitatea** (*privacy*)
 - Confundata, deseori cu confidentialitatea care se aplica datelor
 - Vizeaza drepturile ce trebuie respectate privind caracterul datelor vehiculate
 - Brese:
 - Stocarea necorespunzatoare a datelor la nivel de server (*information disclosure*)
 - Atacuri de tip *phishing*
 - Configurarea necorespunzatoare a sistemelor

Forme de protectie

- **Integritatea**

- Implica detectarea incercarilor de modificare neautorizata a datelor transmise
- Solutii:
 - Algoritmi de tip *digest*
 - Semnaturi digitale


- **Disponibilitatea**

- O anumita resursa poate fi accesata la momentul oportun
- Cauze ale indisponibilitatii
 - Atacuri de refuz al serviciilor DoS (*Denial Of Service*),
Atacuri distribuite de tip DDoS (*Distributed DoS*) – (vezi slide 22)

Forme de protectie

- **Nerepudierea**

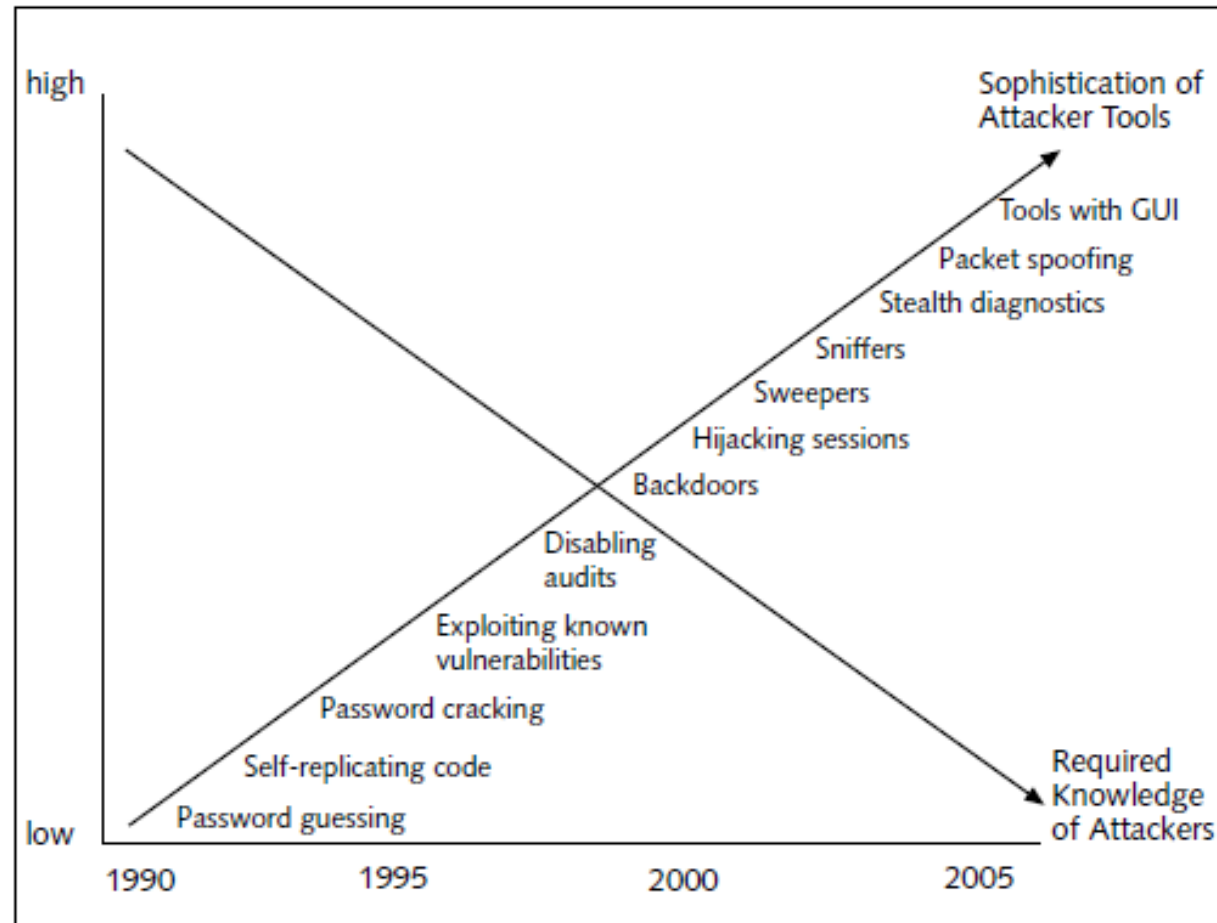
- Expeditorul mesajului nu poate afirma ca nu l-a trimis
- Solutie: certificate digitale
 - Stocheaza datele privind identitatea unei entitati detinatoare a unui secret (parola, serie a cartii de credit, certif. digital, ...)
 - Emise de o autoritate de certificare (CA – *Certification Authority*)
 - Verificate de o autoritate de inregistrare (RA – *Registration Authority*)
 - Serviciile PKI puse la dispozitie de sistem



Infrastructura
cu chei publice
(PKI - *Public*
Key
Infrastructure)

Dificultati in apararea contra unui atac

- Viteza de atac
 - “Slammer worm infected 75,000 computers in the first 11 minutes after it was released and the number of infections doubled every 8.5 seconds”
- Complexitatea atacului
- Disponibilitatea instrumentelor de atac
- Detectarea rapida a vulnerabilitatilor
- *Delay patching*
- Atacuri distribuite
- Confuzia utilizatorilor



[Security guide to network security fundamentals, Mark Ciampa]

Vulnerabilitati

- Pentru Internet, securitatea trebuie sa ia in considerare:
 - Clientul: interactiune, date personale,...
 - Datele de tranzit: securitatea rețelei, schimb de mesaje, ne-repudiere
 - Serverul: securitatea serverului (serverelor), securitatea aplicatiilor, disponibilitatea serviciilor
- **Vulnerabilitate** = slabiciune a unui sistem hardware/software care permite utilizatorilor neautorizati sa aiba acces asupra lui
 - Nici un sistem nu este 100% sigur
 - Vulnerabilitati apar si datorita proastei administrari

Vulnerabilitati

- **Riscuri asociate oamenilor**

- Depasesc jumatate din tipul de atacuri in retea
- Exemplu:
 - Atacatorul foloseste *social engineering* pentru obtinerea parolei utilizator
 - Administratorul creeaza sau configureaza incorect grupurile de utilizatori si drepturile lor de acces
 - Configurarea necorespunzatoare a programelor, serverelor si retelelor
 - *Bug*-uri existente in programe (introduse neintentionat deseori)
 - Ignorarea/nedocumentarea *bug*-urilor cunoscute
 - Lipsa suportului din partea producatorilor
 - Comoditatea sau necunoasterea problemelor de securitate de catre administrator ori de conducerea organizatiei
 - Angajati necinstiti care abuzeaza de politicile de acces
 - Pastrarea drepturilor pentru angajati care nu mai fac parte din organizatie
 -

Vulnerabilitati

- **Riscuri asociate transmisiilor si nivelului hardware**
 - Transmisia poate fi interceptata
 - *Man-in-middle attack*
 - Exemplu: un cracker capata acces asupra unui AP care ofera acces liber la WI-FI
 - Broadcast-ul realizat de un hub intr-un segment de retea poate fi vulnerabil la *sniffing*
 - Porturile serverelor neutilizate pot fi exploatare (solutie: *port scanner*)
 - Neconfigurarea corespunzatoare a routerelor poate permite utilizatorilor externi vizualizarea adreselor private
 - Neschimbarea suficient de des a parolelelor pentru routere si alte dispozitive
 - Accesul fizic la echipamentele retelei (servere, routere, sisteme intermediare,...)

Vulnerabilitati

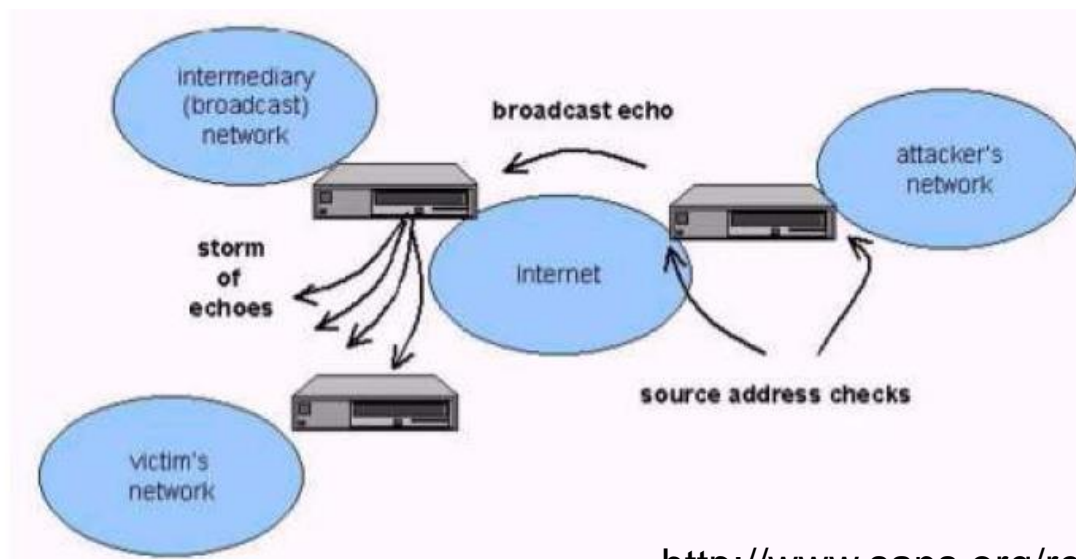
Riscuri asociate cu protocoalele si software-ul utilizat

- **Obs. Distinctia hardware vs. software este greu de facut deoarece protocoalele si nivelul hardware opereaza in tandem**
- Implementari DNS eronate
 - Vulnerabilitati BIND
- Servicii “antice” operationale
 - E.g., telnet, TFTP, ...
- Servicii/protocoale oferind date necriptate
 - FTP, SMTP, POP
- “Gauri” prezente in aplicatii (*application holes*)
 - Exemplificari: Apache, IIS, MSIE, Outlook, phpBB, ...
- Script-urile CGI (Common Gateway Interface)
- Existenta conturilor/configuratiilor implicite
- Permisuni inadecvate pentru fisiere, servicii, conturi-utilizator
- Lipsa mecanismelor de monitorizare & detectare a intrusilor
- Existenta exemplelor de configuratii, programe demonstrative ce pot fi exploatare

Vulnerabilitati

- **Riscuri asociate accesului la internet**

- Un firewall poate sa nu fie corespunzator configurat => obtinerea de adrese IP, ce vor fi utilizate pentru *IP Spoofing*
- Atac de tip *denial-of-service*: sistemul a devenit nefunctionabil deoarece este invadat cu transmisii de date
 - Atac de tip *smurf*: “flood of broadcast ping messages”



Exemplu: Atac de tip *smurf*

http://www.sans.org/reading_room/whitepapers/threats/icmp_attacks_illustrated_477?show=477.php&cat=threats

Atacuri

- Cunoasterea profilului atacatorului
- Atribute ce trebuie considerate
 - Resurse disponibile
(financiare, tehnice, pregatirea in domeniu,...)
 - Timpul alocat
(atacatorii rabdatori vor avea mai mult succes)
 - Riscul asumat – depinde de obiective
(atacul ar putea fi revendicat sau nu de *cracker*)
 - Accesul la Internet & calitatea acestuia: tip (*wireless*, conexiune satelit,...), mod de alocare al IP-ului
 - Obiectivele urmarite (recunoastere mondiala, denigrarea tinte, furt de informatii, furt de bani, ...)

Atacuri

- Niveluri de atac
 - **Oportunist** (*script kid*)
 - Scop “recreational”
 - Fara obiective/tinte clar definite
 - Se utilizeaza programe disponibile liber pentru a scana sau testa vulnerabilitati uzuale (e.g., software de scanare, *rootkits*,...)
 - Nu necesita acces in interiorul sistemului
 - Cunostinte vagi despre sistemul/organizatia tinta
 - Masuri de precautie:
 - Ziduri de protectie (*firewall*-uri)
 - Actualizarea versiunilor de programe

Atacuri

- Niveluri de atac

- **Intermediar**

- Obiectiv conturat, la nivelul organizatiei
 - Se vor efectua aceleasi actiuni ca la atacul “recreational”, dar se incearca ascunderea lor
 - Atacatorul are mai multa rabdare
 - Cunostinte tehnice mai profunde (uzual, la nivelul unui administrator de retea)
 - Probabilitate mai mare de succes, posibil efecte mai mari

- **Sofisticat**

- Obiectiv foarte bine conturat; Tinta este de cele mai multe ori o organizatie
 - Atacurile pot trece peste masurile de prevedere
 - Atacatorul va avea multa rabdare; Se investeste timp pentru colectarea de informatii despre sistemul/organizatia tinta
 - Foarte bune abilitati tehnice; Probabilitate mare de succes

Atacuri

Tip atacator	Resurse	Timp	Instrumente	Risc	Acces	Obiective
Atacator recreațional	Cunoștințe tehnice în general limitate	De obicei oportunist	Utilizează instrumente liber disponibile	Posibil să nu înțeleagă/aprecieze riscul	Extern	Recunoaștere personală, să-și dezvolte abilitățile de cracker
Angajat sau fost angajat	Depinde de abilitățile personale	Poate fi răbdător și aștepta apariția unei oportunități	Utilizează instrum. liber disponibile. Dacă a fost admin., ar putea dezvolt. singur instrumente	Înțelegere a riscului, mai ales dacă este încă angajat	Intern sau extern	Avantaje personale. Denigrarea organizației

Atacuri

Tip atacator	Resurse	Timp	Instrumente	Risc	Acces	Obiective
Activist cu motivație etică sau politică	Posibil să lucreze în echipă	Posibil răbdător, un evenim. poate însă determ. o acțiune rapidă	Utilizează instrumente liber disponibile	Nu este conștient de riscuri	Extern	Denigrarea organizației. Impresionarea opinii publice. Impresionarea instituțiilor guv.
Spion industrial	Cunoștințe avansate	Răbdător. Va încerca probabil ascunderea identității proprie	Poate modifica sau crea instrumente noi	Întelegere medie a riscului	Extern	Vânzarea inform. proprietary. Aflarea de informații despre concurență sau determinarea strategiilor organizației țintă

Atacuri

Tip atacator	Resurse	Timp	Instrumente	Risc	Acces	Obiective
Atacator la nivel național (nation-state)	Poate angaja resurse importante	Răbdător, însă informațiile dorite pot fi necesare într-un timp scurt	Ar putea dezvolta instrumente specifice dacă este mare câștigul	Întelegere medie a riscului	Extern	Accesarea de informații guvernamentale sau informațiile proprietare ale unei organizații

Atacuri

- **Tipuri de atac**

- **Accesul la nivel de utilizator**

- Atac prin acces via un cont de utilizator obisnuit sau cu privilegii superioare
 - Etape:
 - Colectarea de informatii (utilizatori, vulnerabilitati notorii, configuratii de sisteme tipice,...)
 - Exploatarea
 - Deteriorarea: acces la date importante, alterarea informatiilor, asigurarea accesului ulterior la sistem, modificarea jurnalelor de sistem
 - Solutii: eliminarea programelor, modulelor & serviciilor care nu sunt neaparat necesare, analizarea fisierelor de jurnalizare

Atacuri

- **Tipuri de atac**

- **Accesul de la distanta**

- Nu necesita acces-utilizator la sistem
 - Creeaza refuzuri de servicii prin cereri incorecte, eventual cu “caderea” serviciilor prost proiectate
 - Etape:
 - Colectarea de informatii – identificarea de servicii
 - Exploatarea – trimiterea de pachete la portul gasit
 - Deteriorarea: distrugerea unui serviciu de retea, defectarea/incetinirea (temporara) a unui serviciu sa a sistemului

Atacuri

- **Tipuri de atac**

- **Accesul de la distanta la diverse aplicatii**

- Trimiterea de date invalide aplicatiilor, nu serviciilor de retea (traficul nu este afectat)
 - Exemple: SQL injection
 - Nu necesita obtinerea unui cont de utilizator
 - Etape:
 - Colectarea de informatii – identificarea aplicatiei (e.g. server sau client Web, aplicatie de birou, sistem de stocare, solutie de mesagerie, ...)
 - Exploatarea – trimiterea continutului, direct sau indirect (e.g., via e-mail sau FTP), spre aplicatie
 - Deteriorarea
 - » Stergerea/copierea fisierelor utilizatorilor
 - » Modificarea fisierelor de configuratie

Atacuri

- Tipuri de atac

- Inocularea de programe pe calculatorul utilizatorului

- Plasarea de programe *malware* (*virusi*, spioni, cai troieni, bombe, *scareware*...) – via script-uri, plugin-uri, componente ActiveX etc. Efecte:
 - Apelarea neautorizata de programe
 - Colectarea/distrugerea de resurse
 - Lansarea de atacuri spre alte sisteme
 - Crearea de usi ascunse (*traps/backdoors*)
 - Furtul identitatii utilizatorului
 -

<http://lifehacker.com/5560443/whats-the-difference-between-viruses-trojans-worms-and-other-malware>

31

Atacuri

- Tinta

- Organizatii publice sau guvernamentale
 - Recunoastere in randul cracker-ilor
 - Captarea atentiei mass-mediei
 - Revendicari etice, politice,...
- Furnizori de Internet
 - Sabotarea activitatii
- Companii Private
 - Discreditare
 - Furt de informatii
 - Razbunare din partea fostilor angajati
- Persoane Fizice
 - Cu scop “recreational”

Atacuri

- **Moduri de atac**

- Spargerea sau penetrarea (*cracking*)

- Actiunea de descoperire a unor vulnerabilitati si de profitare de pe urma acestora
 - Acces neautorizat la sistem efectuat de *cracker*
 - Accesare, fara alta actiune – rol pasiv
 - Accesare cu alterare/distrugere a informatiilor – activ
 - Accesare cu control asupra sistemului; uneori cu creare de “usi din spate” (*backdoors*) – rol activ
 - Nu se acceseaza sistemul, ci se realizeaza actiuni distructive de refuz al serviciilor

Atacuri

- **Moduri de atac**

- *E-mail bombing*

- Trimiterea repetata a unui mesaj (de dimensiuni mari) spre o adresa e-mail a unui utilizator
 - Incetinesc traficul, umple discul
 - Unele atacuri pot folosi adrese e-mail multiple existente pe serverul tinta
 - Se poate combina cu falsificarea adresei (*e-mail spoofing*)

- *E-mail spamming*

- Trimiterea de mesaje nesolicitate (reclame)
 - Adresa expeditorului este falsa
 - Efectul atacului este accentuat daca mesajul va fi trimis pe o lista de discutii

Atacuri

- **Moduri de atac**

- **Abonarea la liste de discutii**

- “Atac” ce determina enervarea victimei, facilitat de diverse programe disponibile in Internet
 - Cauzeaza trafic inutil in retea

- **Flasificarea adresei expeditorului (*e-mail spoofing*)**

- Folosita pentru ascunderea identitatii expeditorului sau pentru determinarea utilizatorului sa raspunda la atac ori sa divulge informatii (e.g. parole)
 - Slabiciune datorata protocolului SMTP
 - Utilizatorii trebuie educati sa nu raspunda expeditorilor necunoscuti si sa nu divulge informatii confidentiale

Atacuri

- **Moduri de atac**

- *Social engineering*

- Manipularea utilizatorilor de catre un *cracker* – *phishing* (*preluarea identitatii*)
 - Tipuri: intimidare, santaj, presiune, autoritate, flatare, substitutie de persoana, vanitate etc.
 - Atacatorul colecteaza date privitoare la persoana si/sau organizatia vizata si aplica principii de persuasiune
 - <https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>

Atacuri

- **Moduri de atac**

- **Refuzul serviciilor (*Denial Of Service*)**

- Obiectiv: Degradarea calitatatii functionarii unor servicii sau dezafectarea lor
 - Modalitate: supraincarcarea serverului sau a retelei
 - Consumarea resurselor *host*-ului
 - *flood*-uri TCP SYN
 - *flood* ICMP ECHO (ping)
 - Consumarea latimii de banda
 - *flood* UDP
 - *flood* ICMP

Atacuri

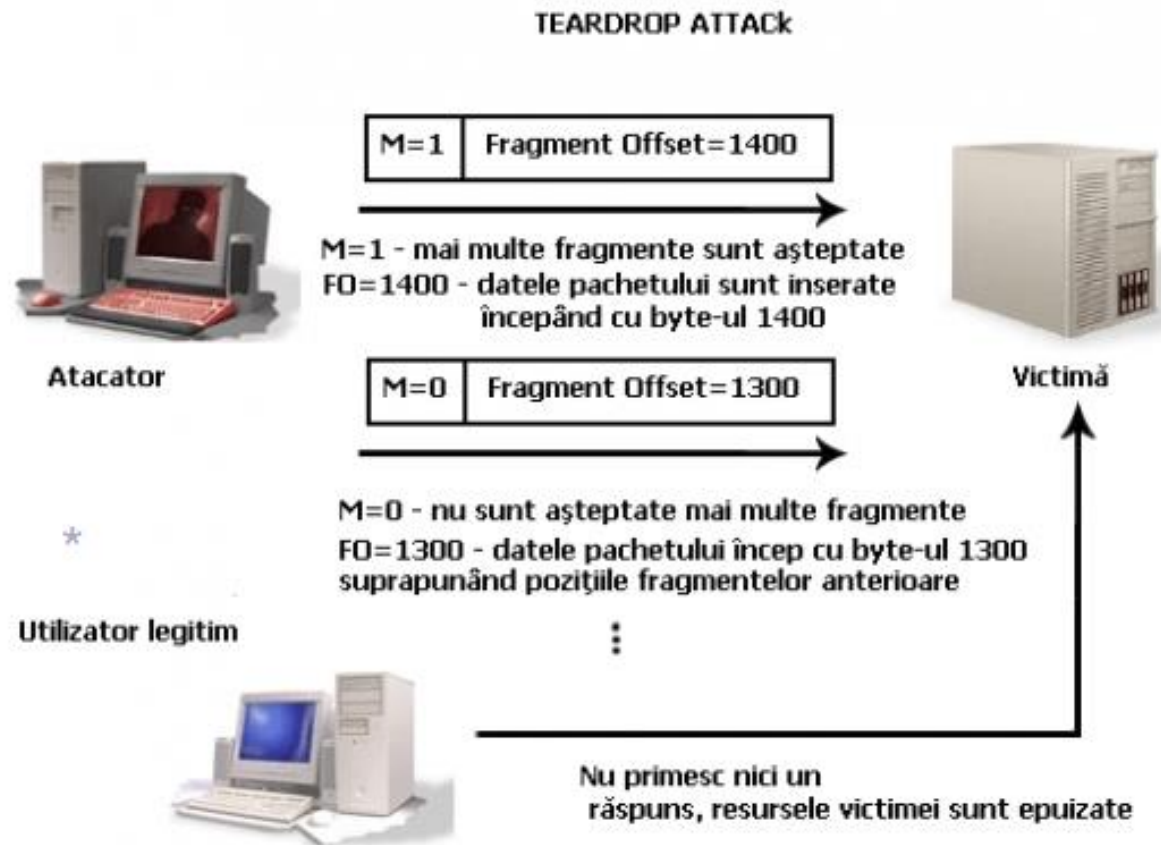
- **Moduri de atac**

- **Refuzul serviciilor (*Denial Of Service*)**

- De obicei, atacatorul isi falsifica adresa sursa (*IP spoofing*)
 - Se pot modifica porturile sursa/destinatie (pentru a trece de *firewall*-uri)
 - Exemple:
 - SYN flood – cereri multiple de realizarea a conexiunii
 - *Ping of death* – atac cu pachete ICMP mari
 - *Teardrop* – exploatarea in general a implementarilor TCP/IP care nu gestioneaza corect pachetele IP (versiunile de Windows 3.1x, Windows 95, windows NT si versiuni Linux (inainte de 2.0.32))
 - *Smurf* – atac ICMP asupra adresei de broadcast

Atacuri

- Moduri de atac
 - Teardrop



http://www.dlsit.ro/articole/106_Atacul-Teardrop

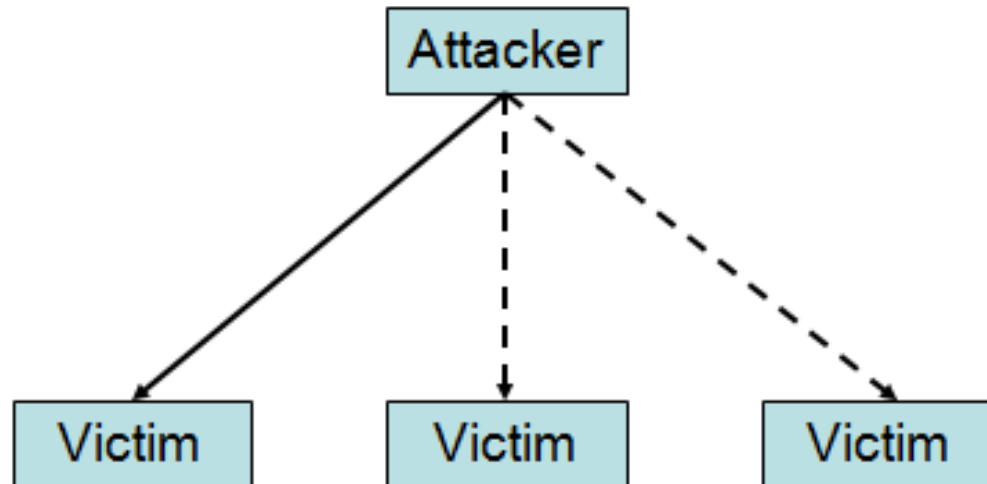
Atacuri

- Moduri de atac

- Refuzul serviciilor (*Denial Of Service*)

- DoS simplu

- De obicei, atacatorul isi falsifica adresa sursa (*IP spoofing*)
 - Usor de rezolvat

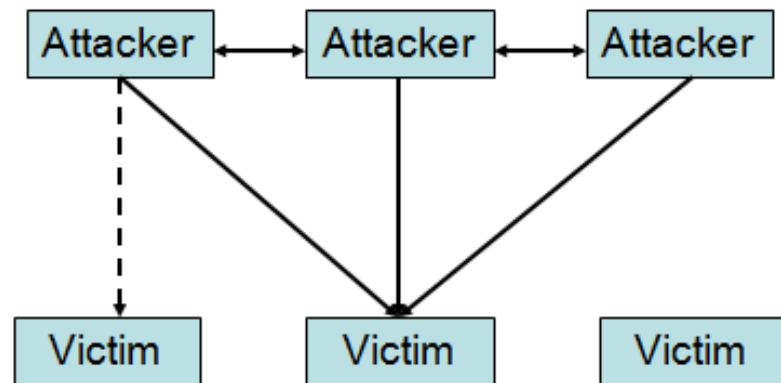


Atacuri

- Moduri de atac
 - Refuzul serviciilor (*Denial Of Service*)

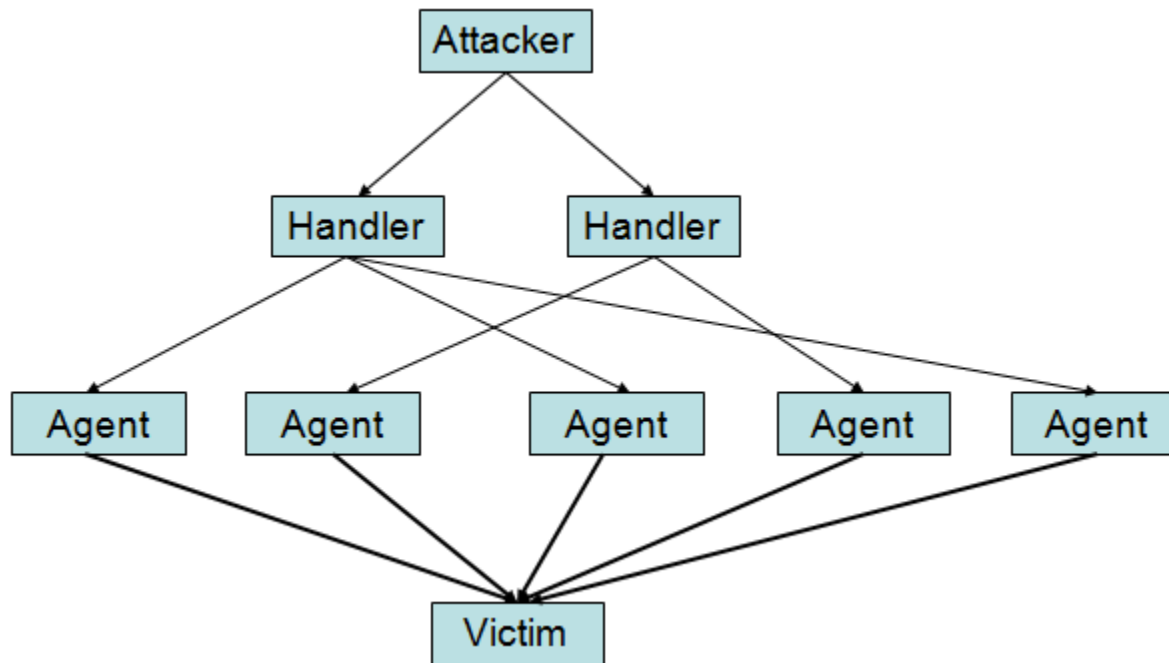
DoS coordonat

- La primul pas, este atacata o alta victima pentru a se ascunde adevaratul atac
- Atacatorul isi ascunde de obicei adresa de origine
- Greu de rezolvat



Atacuri

- Moduri de atac
 - Refuzul serviciilor (*Denial Of Service*)
DDoS (*Distributed DoS*)



Atacuri

- **Moduri de atac**

- **Refuzul serviciilor (*Denial Of Service*)**

- **DDoS (*Distributed DoS*)**

- *Handlers* – sunt de obicei serverele puternice (care ascund usor pachetele de atac)
 - *Agents* – sunt de obicei utilizatori ce au computerele infectate
 - Foarte dificil de depistat atacatorul
 - Este diferit de *FlashCrowd*

- » Slashdot Effect, Victoria Secret Webcast

- (<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.449.9815&rep=rep1&type=pdf>)

Atacuri

- **Moduri de atac**

- **Depasirea capacitatii buffer-elor (*buffer overflow*)**

- Unele programe pot aloca spatiu insuficient pentru unele date, depasirile survenite pot produce executarea de comenzi ca utilizator privilegiat (root)
 - Unele functii C – precum `gets()`, `getwd()`, `strcpy()`, `strcat()` – ofera premisele aparitiei de *buffer overflow*- uri
 - Exemple: suprascriere de cod, alterarea stivei de pointeri
 - Uzual atacul provine din interior, dar poate fi si din exterior (via un cal troian)

Atacuri

- **Moduri de atac**

- **Interceptarea rețelei (*IP sniffing*)**

- Monitorizarea datelor care circula printr-o interfata de retea
 - Se pot detecta parole transmise necriptate
 - Atacul provine din interior
 - Pentru rețele de mare viteză (peste 100M/s) unele pachete nu pot fi captate de *sniffer*
 - Software-ul interceptor trebuie supravegheat
 - Exemple: tcpdump, Wireshark (Ethereal)

Atacuri

- Moduri de atac

- Virusi

- Programe ce efectueaza operatii nedorite (distructive), cu capacitati de “multiplicare”
 - Infectarea altor programe (uzual, executabile)
 - Mai putin raspinditi in Unix/Linux, de obicei avind efect doar daca se executa sub auspicii de *root*
 - Pot genera si *e-mail bombing*
 - Remedii: utilizarea de antivirusi si porti de *e-mail*

Atacuri

- **Moduri de atac**

- **Cai troieni (*trojan horses*)**

- Programe rau intentionate “deghizate sub forma unor executabile “utile”
 - Apeleaza programe neautorizate sau sunt modificate, incluzand cod nelegitim
 - Actiuni: colectarea de informatii, distrugerea de informatii, lansarea de atacuri spre alte sisteme
 - Exemple: “vaduva neagra” (blocheaza sau corupe browsere Web)

Atacuri

- **Moduri de atac**

- **Usi ascunse (*back doors/ traps*)**

- Caz particular de cai troieni
 - Creeaza o “poarta” (e.g. utilizator, port,...) care permite accesul ulterior la calculator si/sau castigarea de privilegii

- **Viermi (*worms*)**

- Programe care se multiplica, transferandu-se pe alte gazde si efectuand (eventual) distrugerii
 - Exemplu celebru: Internet Worm (Morris Worm) (1988)
 - *fork bomb effect*

Atacuri

- **Moduri de atac**

- **Ghicirea parolelor (*password guessing*)**

- Majoritatea proceselor de autentificare folosesc parole
 - Cu cat utilizatorul trebuie sa retina mai multe parole, cu atat sistemul de protectie via parole este predispus la brese in securitate:
 - Alegerea unor parole slabe
 - Partajarea parolelor (colegi, prieteni,...)
 - Scrierea parolelor pe hartie
 - Folosirea aceleiasi parole timp indelungat, pentru mai multe aplicatii/sisteme
 - Folosirea unui program ce determina parolele prost alese (prea simple, prea scurte, cuvinte din dictionar,..)
 - Protectie prin /etc/shadow, reguli stricte de schimbarea parolelor, educarea utilizatorilor
 - Alte solutii: SSO (Single Sign On), identificare biometrica, etc.

Atacuri

- Moduri de atac

- Utilizarea tehnicilor de *reverse code-engineering*

- Analiza aplicatiilor binare fara cod-sursa accesibil (*closed –source*), pentru a se observa modul de executie la nivel scazut
 - Folosita si pentru a studia codul *malware*
 - Instrumente: editoare hexa, dezasambloare, depanatoare, monitoare de sistem,...
 - Apar probleme de legalitate

Prevenirea

- La ce nivel trebuie luate masuri de securitate?
 - Nivel fizic: inhibarea ascultarii mediilor de transmisie, interzicerea accesului fizic la server, ...
 - Nivelul legatura de date: criptarea legaturii
 - Nivelul retea: ziduri de protectie (*firewall-uri*)
 - Nivelul transport: criptarea conexiunilor (SSL – *Secure Socket Layer*, TLS – *Transport Layer Security*)
 - Nivelul aplicatiei: monitorizare si actualizarea software-ului, jurnalizare, educarea utilizatorilor, politici generale adoptate,...

Prevenirea

- Elaborarea de politici de securitate
 - Planificarea cerintelor de securitate (confidentialitate, integritate, disponibilitate,...)
 - Evidentierea riscurilor
 - Scenarii de risc
 - Analiza raportului cost-beneficii
 - Costurile prevenirii, refacerii dupa dezastru etc.
 - Stabilirea politicilor de securitate
 - Politica generala (nationala, organizationala,...)
 - Politici separate pentru diverse domenii protejate
 - Standarde & reglementari (recomandari)

Prevenirea

- **Elaborarea de politici de securitate - exemplu**
 - Gestionarea accesului (nume de cont, modul de schimbare a parolei, politica de acces din exterior,...)
 - Clasificarea utilizatorilor (grupuri, permisiuni, utilizatori speciali, utilizatori administratori,...): ACL (Access Control List)
 - Accesul la resurse (drepturi de acces la fisiere, directoare, criptarea fisierelor importante,...)
 - Monitorizarea activitatii (fisiere de jurnalizare)
 - Administrarea copiilor de siguranta (tipuri de salvari, medii de stocare, durata pastrarii, ...)

Prevenirea

- Principii de baza

- Simplificare – configurarea sistemului astfel incat sa acorde vizitatorilor cele mai scazute privilegii
 - Reducere – minimizarea ariei de actiune
 - Intarire – “never trust user input” + securizarea accesului la fisiere/aplicatii externe
 - Diversificare – utilizarea mai multor niveluri de protectie (fara *security through obscurity*)
 - Documentarea – memorarea setarilor, strategiilor si masurilor adoptate pentru securitate
- Obs. Siguranta sistemului depinde de cea mai vulnerabila componenta a acestuia

Supravietuirea

- **Supravietuirea** = capacitatea unui sistem (calculator/retea) de a-si indeplini misiunea, in timp util, in prezenta atacurilor, defectelor sau accidentelor
- **Atac** = eveniment potential distrugator provocat intentionat de persoane rau-voitoare
- **Defect** = eveniment potential distrugator cauzat de deficiente ale sistemului sau ale unui factor de care depinde sistemul (e.g., defecte hardware, bug-uri software, erori ale utilizatorilor)
- **Accident** = evenimente neprevazute (e.g. dezastre naturale, caderi de tensiune,...)
- Sistemul trebuie sa sustina macar indeplinirea functiilor vitale (*mission-critical*)
 - Identificarea serviciilor esentiale,
 - Identificarea perimetrilor de securitate majora

Supravietuirea

- **Proprietati ale sistemului:**
 - **Rezistenta la atacuri** = strategii de respingere a atacului (e.g. autentificarea utilizatorilor, *firewall*-uri, validarea obligatorie a datelor de intrare)
 - Recunoasterea atacurilor si efectelor lor = strategii pentru restaurarea informatiilor, limitarea efectelor, mentinerea/restaurarea serviciilor compromise
RAID (Redundant Array of Independent Disks),
SAN (Storage Area Network), backup-uri, cluster-e,...)
 - Adaptarea la atacuri = strategii pentru imbunatatirea nivelului de supravietuire -> invatarea din greseli

Monitorizarea

- **Monitorizarea securitatii retelei (NSM – Network Security Monitoring)** = colectarea, analiza si aprecierea indicatorilor si avertismentelor privind **detectarea** si **raspunsul** la incidente de securitate
 - **Indicator**: actiune observabila care confirma intentiile sau capacitatea de atac
 - Indicatorii generati de sistemele de detectie a intrusilor se mai numesc si **alerte** (vizind un anumit **context**)
- Observatii:
 - Detectarea este realizata (automat) de produse software
 - Analizarea implica factori umani
 - Aprecierea incidentului reprezinta un proces de luare a deciziilor

Monitorizarea: detectarea

- **Principii:**

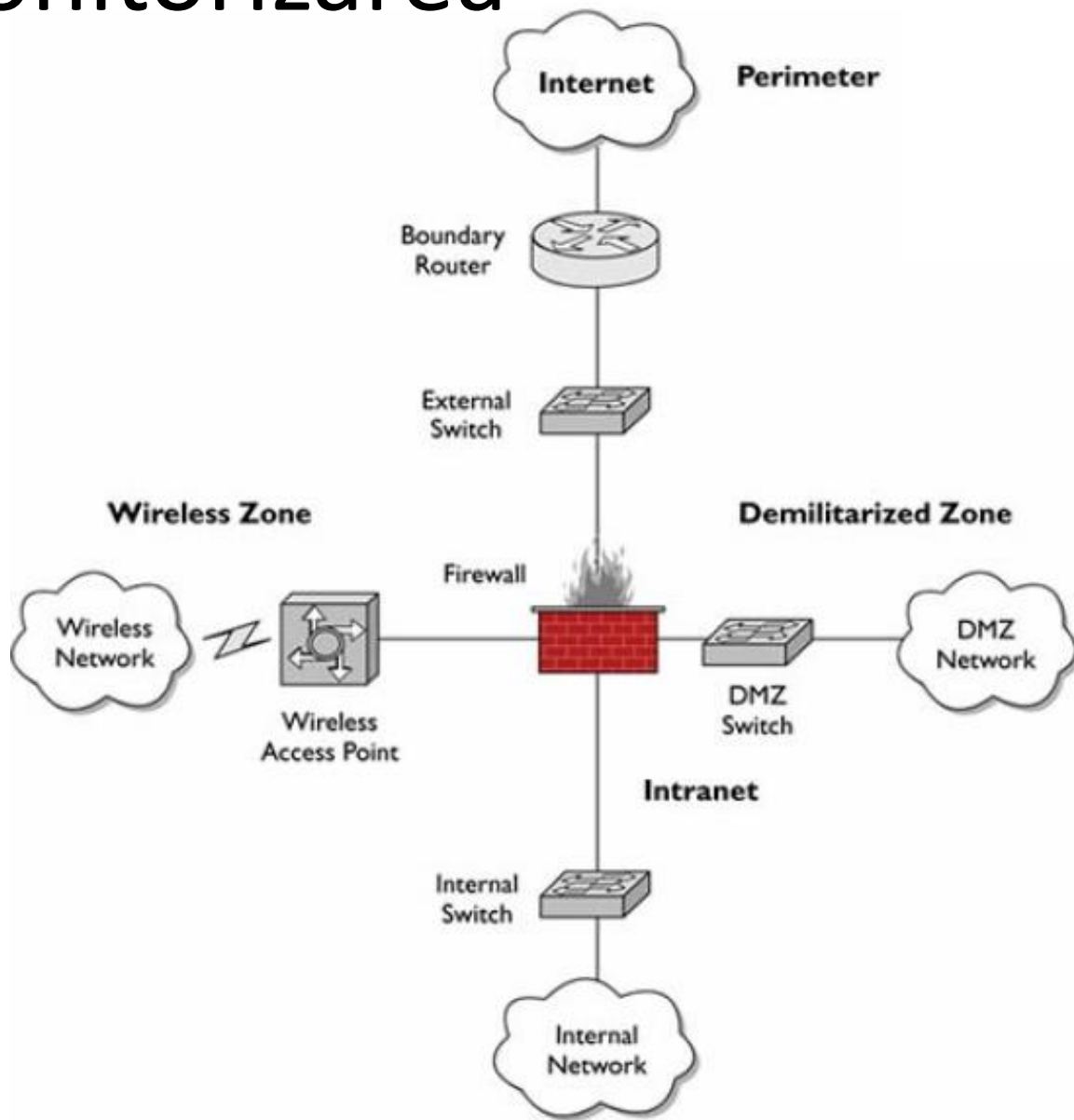
- Intrusii care comunica (direct/indirect) cu victimele pot fi detectati
- Detectia prin luare de probe (*sampling*) este superioara lipsei de detectie (nu pot fi monitorizate toate datele)
- Detectia pe baza analizei traficului este superioara lipsei detectiei

- **Obs.**

- Colectarea tuturor datelor este problematica
- Colectarea datelor poate fi efectiva daca se bazeaza pe aparitia unor evenimente
- Instrumentele de detectie trebuie sa fie optimizate si trebuie sa asigure ergonomia utilizatorului

Monitorizarea

- Divizarea rețelei in zone de interes
 - Fiecare zona poate fi tinta unor atacuri
 - DMZ separa datele sensibile de cele disponibil public



Monitorizarea

- Pot fi colectate date provenite de la:
 - *Hub-uri*, porturile *switch-urilor* (via **SPAN – Switched Port Analyzer**), *tap-uri* (*test access port* – dispozitiv de retea proiectat special pentru monitorizare), portile de filtrare (*filtering bridges*) – pentru rețele cu fir
 - Senzori între *firewall-ul* organizației și punctul de acces *wireless*, o platforma *wireless* – pentru rețele *wireless*
- Realizarea de statistici
 - La nivel de router (e.g. *CISCO accounting*)
 - La nivel de sistem de operare
 - Instrumente: *lpcad*, *ifstat*, *tcpdstat*, *MRTG* (Multi Router Traffic Grapher) etc.

Monitorizarea: identificarea

- Date (trafic de retea)
 - Normale
 - Privind HTTP, FTP, SMTP, POP3, DNS, IP, SSL/TLS etc
 - Suspicioase
 - Apar dubioase la prima vedere, dar nu cauzeaza probleme pentru corporatie, ci eventual doar utilizatorului
 - Malitioase
 - Au impact negativ asupra securitatii organizatiei

Monitorizarea: validarea

- Validarea asociaza un incident preliminar unei categorii de evenimente:
 - Acces neautorizat ca *root* (administrator)
 - Acces neautorizat la nivel de utilizator
 - Incercare de accesare neautorizata
 - Atac (D)Dos soldat cu succes
 - Violare a politicii de securitate
 - Scanare, probare, detectie
 - Infectie cu virusi

Monitorizarea: reactia

- Dupa aparitia unui incident de securitate, trebuie demarata o reactie:
 - Pe termen scurt – STIC (*SHORT-Term Incident Containment*)
 - Exemplu: inchiderea portului *switch*-ului prin care se realizeaz atacul, deconectarea fizica, introducerea unei reguli noi de filtrare a datelor etc.
 - Intrarea in stare de urgenta
 - O importanta majora o are analiza (*analyst feedback*) -> implica personal specializat

Monitorizarea

- Se poate recurge si la capcane pentru *craker*-i: *honeypots*
 - Masini-tinta special configurate pentru a observa atacurile *cracker-ilor*
 - Mai multe *honeypots* formeaza un *honeynet* (<https://www.honeynet.org>)
 - Pentru a detecta & studia noi tehnici de atac si pentru a contracara diverse incidente de securitate
 - Folosind un daemon (*honeyd*), se pot imita servicii de retea, ruland intr-un mediu virtual

Testarea

- Teste de verificare a:
 - Capacitatii de deservire a clientilor
 - Robustetei
 - Rularii in situatii extreme
- Teste referitoare la performante
- Teste specifice legate de exploatare
 - Pregatirea adecvata a exploatarii in practica (*deployment*)
 - Teste de incarcare (*load testing*)
- Teste privind opacizarea datelor (*obfuscation*)
 - Datele nu trebuie stocate in locatii predictibile
- Teste privitoare la integrarea componentelor
- Teste specifice legate de programare (de ex. lungimea parametrilor trimisi de client, a interogarilor SQL, etc)

Testarea

- Instrumentele de stresare (*stressing tools*) pot da informatii privitoare la:
 - Performanta (timp de raspuns, timp de generare a continutului etc.)
 - Scalabilitate (memoria ocupata, utilizarea discului, numarul inregistrarilor inserate, accesarea altor tipuri de resurse, ...)
 - Corectitudine (functionarea eronata a unor componente)
 - Lacune de securitate
- Metodologii de analiza a riscurilor: **DREAD** (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability), **OCTAVE** (Operationally Critical Threat Asset and Vulnerability Evaluation), **STRIDE** (Spoofing identity, Tempering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege), **OSSTMM** (Open Source Security Testing Methodology Manual) – www.ostmm.org

Testarea

- **SANS** (System Administration, Networking, and Security) :
 - Pregătire
 - Identificare
 - Controlul efectelor
 - Eradicare
 - Recuperare
 - Continuare (*follow-up*)
- Raspunsurile agresive sunt prohibite! (*hack back*)
- *Forensics* = procesul de “prindere” a cracker-ilor
 - Uzual, are loc dupa un incident de securitate
 - Implica: analiza hardware-ului (discuri, RAM,...), log-urilor etc.
 - Instrumente: WinHex, FIRE (forinsec and Incident Response Environment), ForensiX

Protocoale – exemple

- **Nivelul retea**

IPSec – RFC 2401, 2402, 2406, 2408

- Servicii oferite: controlul accesului, integritatea datelor, autentificare, confidentialitate
- Poate fi implementat in cadrul unui *router* sau *firewall*
- Nu necesita modificarea software-ului la nivel de transport/aplicatie
- Autentificarea & integritatea se precizeaza intr-un antet special: Authentication Header
- Confidentialitatea este asigurata de algoritmi de criptare via date suplimentare

ESP (*Encapsulating Security Payload*)

Protocole – exemple

- **Nivelul transport**

TLS (Transport Layer Security) – RFC8446 (TLS 1.3)

- Imbunatatire a SSL (Secure Socket Layer) creat de Netscape

SSL(Secure Sockets Layer)

- Metoda de criptare a transmisiilor TCP/IP (e.g. pagini Web, date introduse in *form-uri* web) - HTTP over Secure Sockets Layer or HTTP Secure
- Oferă servicii de securitate de baza pentru TCP
- Fiecare conexiune dintre un client si server reprezinta o sesiune (*session*)
- Starea unei sesiuni = identificator unic al sesiunii, certificat digital, metoda de compresie, metoda de cifrare (algorithm de criptare sau de tip hash), cod secret partajat de client & server
- Un mesaj are asociat un cod de autentificare: MAC (Message Authentication Code)

Protocole – exemple

- **Nivelul transport**

TLS (Transport Layer Security) – RFC8446 (TLS 1.3)

- **Alert Protocol** – mecanism care permite managementul alertelor provenite de la un punct terminal: mesaj neasteptat receptionat, eroare de decompresie, MAC incorect, certificat eronat
- **Handshake Protocol** – permite autentificarea serverului la client si vice-versa, plus negocierea algoritmilor de criptare si a cheilor; se realizeaza inainte de transmiterea efectiva a datelor

Protocoloale – exemple

- **Nivelul aplicatie**

SSH (Secure Shell)

- negociaza si stabileste o conexiune criptata intre un server si un client SSH via metode diverse de autentificare
- Implementari: ssh, PuTTY, SCP (*Secure CoPy*),...

PGP (Pretty Good Privacy) – RFC 3156

- Oferă confidențialitate & autentificarea mesajelor e-mail și a fișierelor transmise prin rețea
- Folosește o pleiadă de algoritmi de criptare
- Implementari: GPG (GNU Privacy Guard)

S/MIME – RFC 3369, 3370, 3850, 3851

- Pune la dispoziție extensii de securitate pentru MIME (Multipurpose Internet Mail Extension)

Atacuri

Mobile is growing and so are security threats.

Take a comprehensive approach to securing the mobile enterprise



By 2016 there will be over **2 billion smartphone users**¹ with over **268 billion mobile downloads** by 2017²



There are **387 new threats every minute** or more than six every second.³ **97%** of top paid **Android apps** and **87%** of top paid **iOS apps** have been hacked⁴



97% say some portion of workforce **uses mobile devices** in their job today⁵

IBM Corporation, 2015

Atacuri

- Atacuri la nivel *wireless*
 - Diminuarea semnalului
 - Capturarea pachetelor de date (*wireless sniffing*)
 - Atacuri asupra WEP (Wired Equivalent Privacy)
 - Crearea de virusi/ cod malitios
 - Folosirea resurselor retelelor wireless publice sau ale unor companii
 - *Snooping* (accesarea datelor private)
 - *Masquerading* (furt de identitate al unui dispozitiv)
 - DoS (refuz al serviciilor)

Probleme specifice

- **Sistemele wireless**
 - Necesitate: un mediu sigur (autentificare, integritate a datelor, confidentialitate, autorizare, nerepudiere)
 - Pericole – tipuri de atacuri:
 - Falsificarea identitatii (*spoofing*)
 - Interceptarea (*sniffing*)
 - Alterarea datelor (*tampering*)
 - Interferenta (*jamming*) – e.g. la Bluetooth
 - Furtul (*device theft*)

Probleme specifice

- **Sistemele wireless**

- Solutii:

- WEP (Wired Equivalent Privacy) – standard vechi inlocuit in 2003 de WPA
 - WPA (WI-FI Protected Access) – subset al 802.11i – foloseste metoda de criptare diferita (RC4 fata de AES), WPA2, WPA3
 - Protocoale de securitate WTLS (Wireless Transport Layer Security)
 - Securitatea la nivel IP: IPSec
 - Extensii de securitate in cadrul IP-ului mobil
 - Firewall-uri
 - ...

Statistici

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.

<https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf>

Statistic

Top atacuri in 2018:

- “At this year’s Security Analyst Summit we reported on Slingshot – a sophisticated cyber-espionage platform that has been used to target victims in the Middle East and Africa since 2012. We discovered this threat – which rivals Regin and ProjectSauron in its complexity – during an incident investigation. Slingshot uses an unusual (and, as far as we know, unique) attack vector: many of the victims were attacked by means of compromised MikroTik routers. The exact method for compromising the routers is not clear, but the attackers have found a way to add a malicious DLL to the device: this DLL is a downloader for other malicious files that are then stored on the router. When a system administrator logs in to configure the router, the router’s management software downloads and runs a malicious module on the administrator’s computer. Slingshot loads a number of modules on a compromised computer, but the two most notable are Cahnadr and GollumApp – which are, respectively, kernel mode and user mode modules. Together, they provide the functionality to maintain persistence, manage the file system, exfiltrate data and communicate with the C2 (command-and-control) server. The samples we looked at were marked as ‘version 6.x’, suggesting that the threat has existed for a considerable length of time. The time, skill and cost involved in creating Slingshot indicates that the group behind it is likely to be highly organized and professional, and probably state sponsored.”

<https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/>

Statistic

Top atacuri in 2018:

- “In May, researchers from Cisco Talos published the results of their research into VPNFilter, malware used to infect different brands of router – mainly in Ukraine, although affecting routers in 54 countries in total. You can read their analysis [here](#) and [here](#). Initially, they believed that the malware had infected around 500,000 routers – Linksys, MikroTik, Netgear and TP-Link networking equipment in the small office/home office (SOHO) sector, and QNAP network-attached storage (NAS) devices. However, it later became clear that the list of infected routers was much longer – 75 in total, including ASUS, D-Link, Huawei, Ubiquiti, UPVEL and ZTE. The malware is capable of bricking the infected device, executing shell commands for further manipulation, creating a TOR configuration for anonymous access to the device or configuring the router’s proxy port and proxy URL to manipulate browsing sessions. However, it also spreads into networks supported by the device, thereby extending the scope of the attack. Researchers from our Global Research and Analysis Team (GReAT) took a detailed look at the C2 mechanism used by VPNFilter. One of the interesting questions is who is behind this malware. Cisco Talos indicated that a state-sponsored or state affiliated threat actor is responsible. In its affidavit for sink-holing the C2, the FBI suggests that Sofacy (aka APT28, Pawn Storm, Sednit, STRONTIUM, and Tsar Team) is the culprit. There is some code overlap with the BlackEnergy malware used in previous attacks in Ukraine (the FBI’s affidavit makes it clear that they see BlackEnergy (aka Sandworm) as a sub-group of Sofacy).”

<https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/>

Statistic

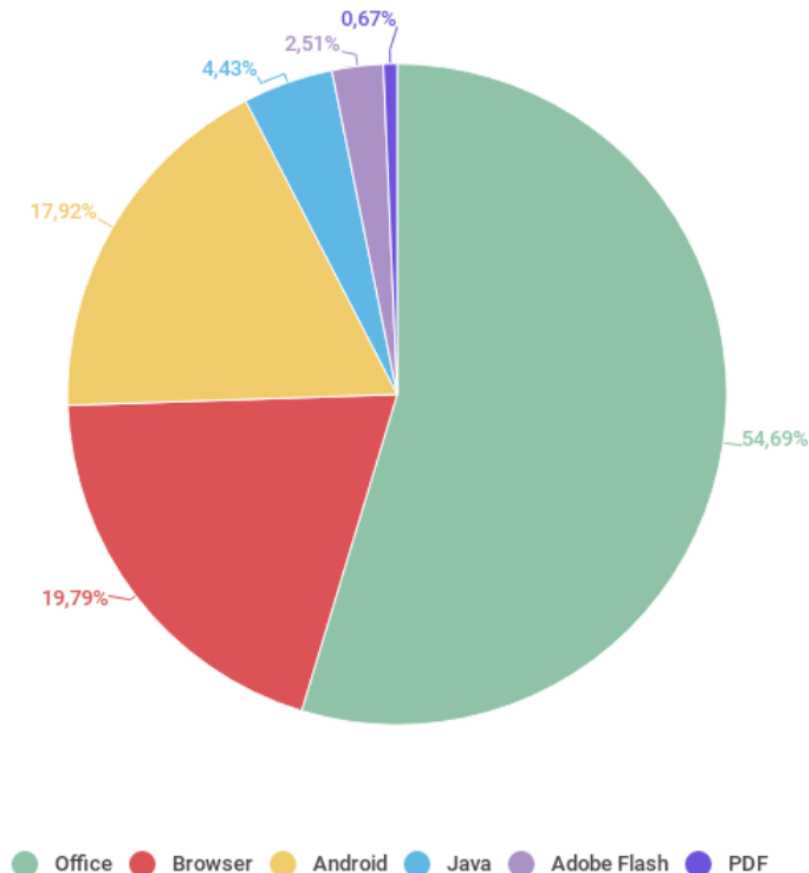
Top atacuri in 2018:

- “Early this year, two severe vulnerabilities affecting Intel CPUs were reported. Dubbed Meltdown and Spectre respectively, they both allow an attacker to read memory from any process and from its own process respectively. The vulnerabilities have been around since at least 2011. Meltdown (CVE-2017-5754) affects Intel CPUs and allows an attacker to read data from any process on the host system. While code execution is required, this can be obtained in various ways – for example, through a software bug or by visiting a malicious website that loads JavaScript code that executes the Meltdown attack. This means that all the data residing in memory (passwords, encryption keys, PINs, etc.) could be read if the vulnerability is exploited properly.”
- “The mobile APT threats segment saw three significant events: the detection of the Zoopark, BusyGasper and Skygofree cyber-espionage campaigns. Technically, all three are well-designed and similar in their primary purpose – spying on selected victims. Their main aim is to steal all available personal data from a mobile device: interception of calls, messages, geolocation, etc. There is even a function for eavesdropping via the microphone – the smartphone is used as a ‘bug’ that doesn’t even need to be hidden from an unsuspecting target.”
- ...

<https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/>

Statistici

Perioada 2018
Top aplicatii vizate de
Atacatori (inclusive
pentru
dispozitivele mobile)



*Distribution of exploits used in cyberattacks, by type of application attacked,
November 2017 – October 2018*

<https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/>

Statistici

TOP 10 most widespread encryptor families

	Name	Verdict	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	29.32
2	(generic verdict)	Trojan-Ransom.Win32.Phny	11.43
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	6.67
4	Cryakl	Trojan-Ransom.Win32.Cryakl	4.59
5	PolyRansom/VirLock	Virus.Win32.PolyRansom	2.86
6	(generic verdict)	Trojan-Ransom.Win32.Gen	2.40
7	Shade	Trojan-Ransom.Win32.Shade	2.29
8	Cerber	Trojan-Ransom.Win32.Zerber	2.20
9	Purgen/GlobelImposter	Trojan-Ransom.Win32.Purgen	1.82
10	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	1.72

Top 10 programe malitioase

* Unique users whose computers have been targeted by a specific crypto-ransomware family as a percentage of all users of Kaspersky Lab products attacked by crypto-ransomware

<https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/>

Statistici

TOP 20 malicious objects detected on user computers

For this rating, we identified the 20 most frequently detected threats on user computers in 2018. This rating does not include the Adware and Riskware classes of program.

	Verdict	%*
1	DangerousObject.Multi.Generic	32.15
2	Trojan.Script.Generic	14.46
3	Trojan.Multi.GenAutorunReg.a	5.76
4	Trojan.WinLNK.Agent.gen	4.56
5	Trojan.WinLNK.Starter.gen	3.47
6	HackTool.Win32.KMSAuto.c	3.14
7	HackTool.Win64.HackKMS.b	2.69
8	Trojan.Win32.Generic	2.56
9	Trojan.Script.Miner.gen	2.44
10	Trojan.Win32.AutoRun.gen	2.43
11	Trojan-Downloader.Script.Generic	2.33
12	Virus.Win32.Sality.gen	2.30
13	HackTool.Win32.KMSAuto.m	2.05
14	Trojan.AndroidOS.Boogr.gsh	1.96
15	Trojan.Win32.Agentb.bqyr	1.48
16	Trojan.Win32.Miner.gen	1.41
17	Trojan.Multi.GenAutorunBITS.a	1.28
18	Trojan.Multi.Babits.genw	1.19
19	Virus.Win32.Nimnul.a	1.18
20	HackTool.MSIL.KMSAuto.ba	1.13

Top 10 programe malitioase

<https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/>

Statistici

Vulnerabilitati predominante in 2017

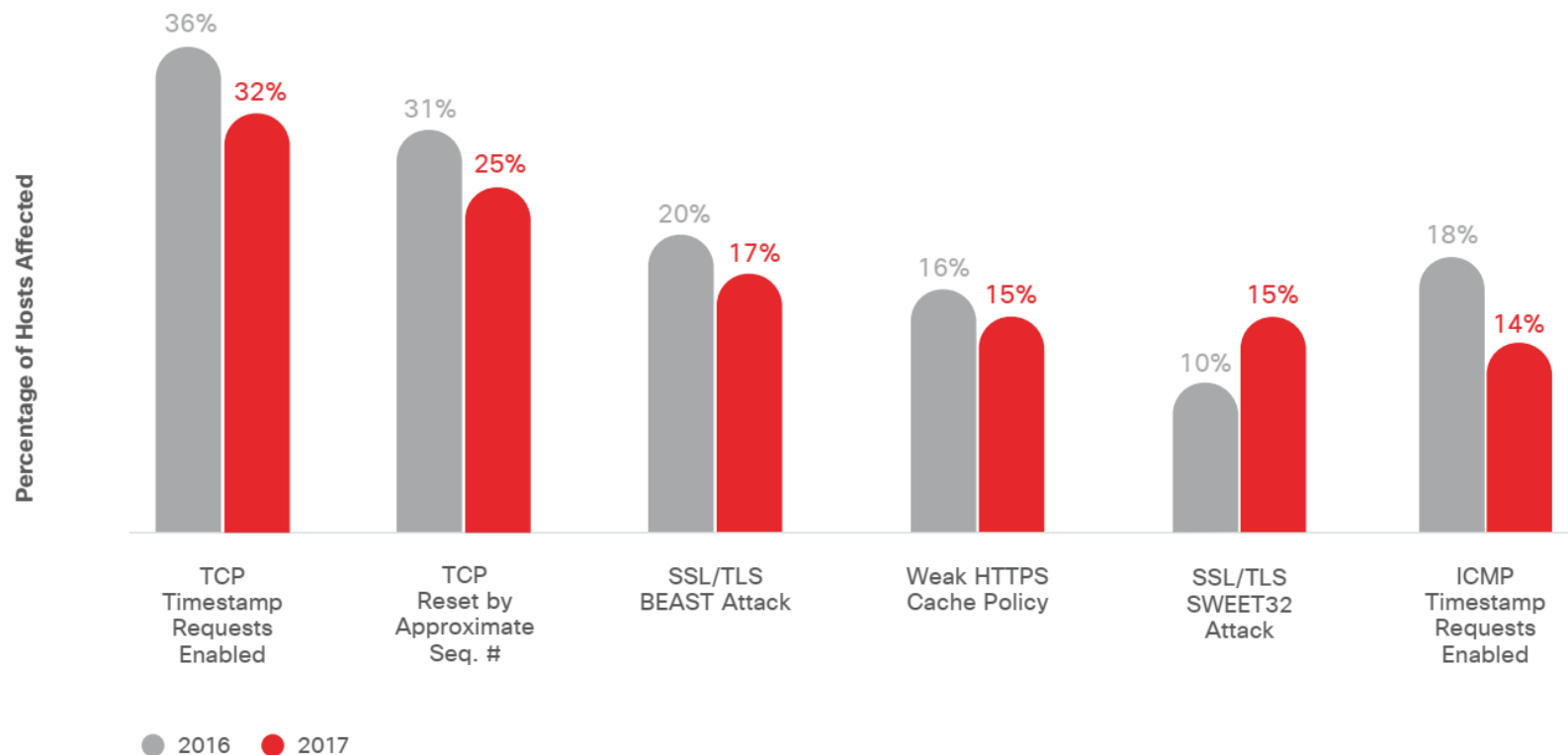
Threat Category	Jan-Sep 2016	Jan-Sep 2017	Change
CWE-119: Buffer errors	493	403	(-22%)
CWE-20: Input validation	227	268	+15%
CWE-264: Permissions, privileges and access	137	163	+18%
CWE-200: Information leak/disclosure	125	250	+100%
CWE-310: Cryptographic issues	27	17	(-37%)
CWE-78: OS Command injections	7	15	+114%
CWE-59: Link following	5	0	

Source: Cisco Security Research

<https://www.cisco.com/c/en/us/products/security/security-reports.html>

Statistici

Vulnerabilitati cu severitate scazuta, dar risc ridicat, cel mai frecvent detectate

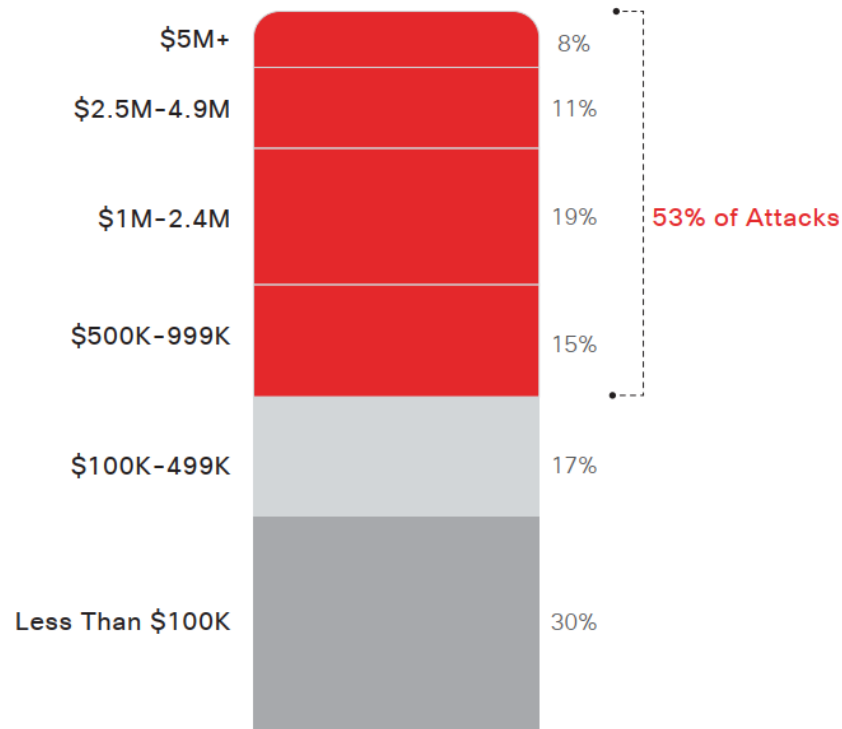


Source: SAINT Corporation

<https://www.cisco.com/c/en/us/products/security/security-reports.html>

Statistici

53% din atacuri au ca rezultat daune de peste 500.000\$



Source: Cisco 2018 Security Capabilities Benchmark Study

<https://www.cisco.com/c/en/us/products/security/security-reports.html>

Previziuni - 2019

- 1. Attackers Will Exploit Artificial Intelligence (AI) Systems and Use AI to Aid Assaults*
- 2. Defenders Will Depend Increasingly on AI to Counter Attacks and Identify Vulnerabilities*
- 3. Growing 5G Deployment and Adoption Will Begin to Expand the Attack Surface Area*
- 4. IoT-Based Events Will Move Beyond Massive DDoS Assaults to New, More Dangerous Forms of Attack*
- 5. Attackers Will Increasingly Capture Data in Transit*
- 6. Attacks that Exploit the Supply Chain Will Grow in Frequency and Impact*
- 7. Growing Security and Privacy Concerns Will Drive Increased Legislative and Regulatory Activity*

<https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond>

Rezumat

- Preliminarii
- Aspecte importante
- Vulnerabilitati
- Atacuri
- Prevenirea si supravietuirea
- Monitorizarea
- Testarea
- Raspunsul la incidente
- Protocoale
- Probleme specifice
- Statistici & Previziuni

Bibliografie

- Security guide to network security fundamentals, Mark Ciampa, 2009
- Network+ Guide to Networks, Fifth Edition, Tamara Dean, Network +, ISBN-13: 978-1-423-90245-4, 2009
- <https://www.cisco.com/c/en/us/products/security/security-reports.html>
- <https://securelist.com/statistics/>
- <https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/>
- <https://blog.checkpoint.com/2018/04/16/2018-security-report-97-companies-unprepared-cyber-attacks/>



Intrebari?

“Little by little, one travels far.”
(J. R. R. Tolkien)