Virtualios infrastruktūros sauga

Elektroninių nusikaltimų tyrimo aspektai virtualioje infrastruktūroje

Elektroniniai nusikaltimai

Elektroniniai nusikaltimai – tai tokios neteisėtos veikos, kuriose kompiuterinė ar programinė įranga yra nusikaltimo objektas arba įrankis.

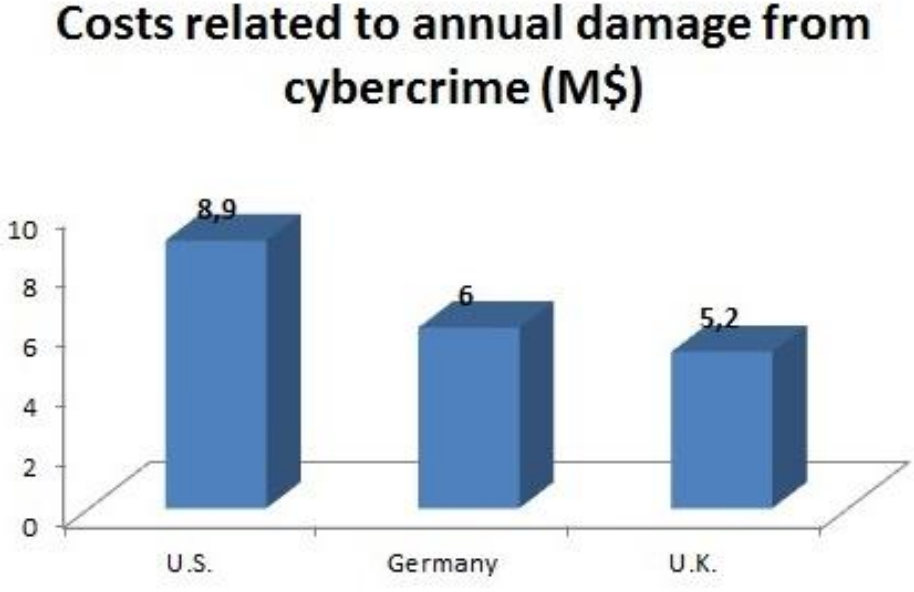
NEE sąvoka apima visą eilę nusikaltimų, tokių kaip:

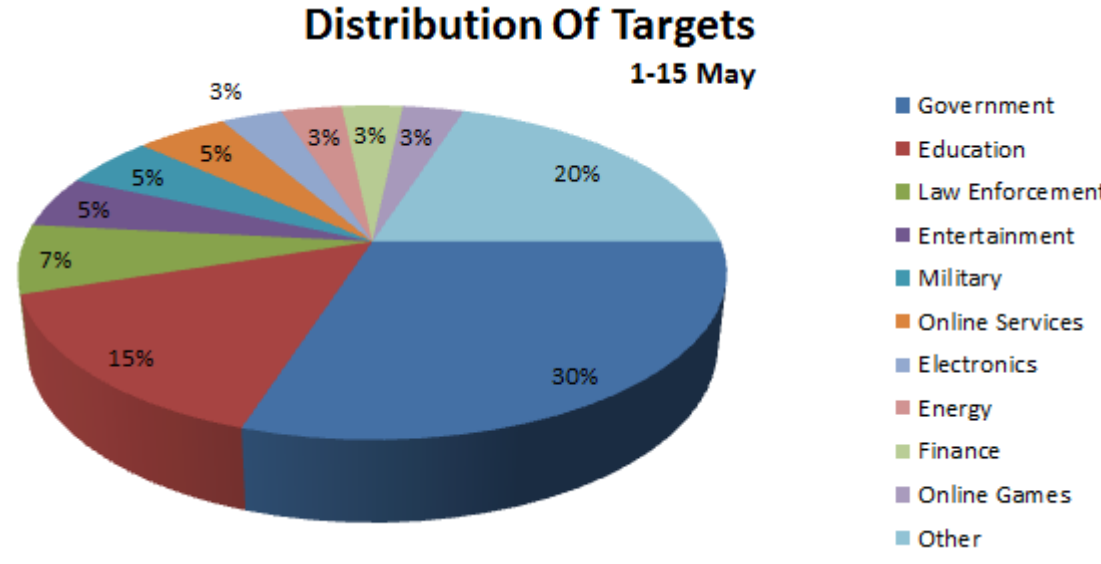
- Informacijos vagystė,
- Draudžiamos, kenksmingos informacijos kūrimas, siuntimas ir platinimas,
- Asmeninės informacijos vagystės, neteisėtas informacijos perėmimas
- Kompiuterinių resursų blokavimas,
- Autorinių teisių pažeidimas
- kiti.

Elektroniniai nusikaltimai

Statistika (*šaltinis Symantec*):

- 556 milijonų nusikaltimų per metus
- Virš 1.5 milijonų nusikaltimų per dieną





Elektroninių nusikaltimų tipai

Elektroninius nusikaltimia klasifikuojami pagal įvairius kriterijus. Panagrinėkime įvairių autorių siūlomus klasifikavimus.

D. Parker knygoje "*Crime by Computer*" pateikia tokią klasifikaciją:

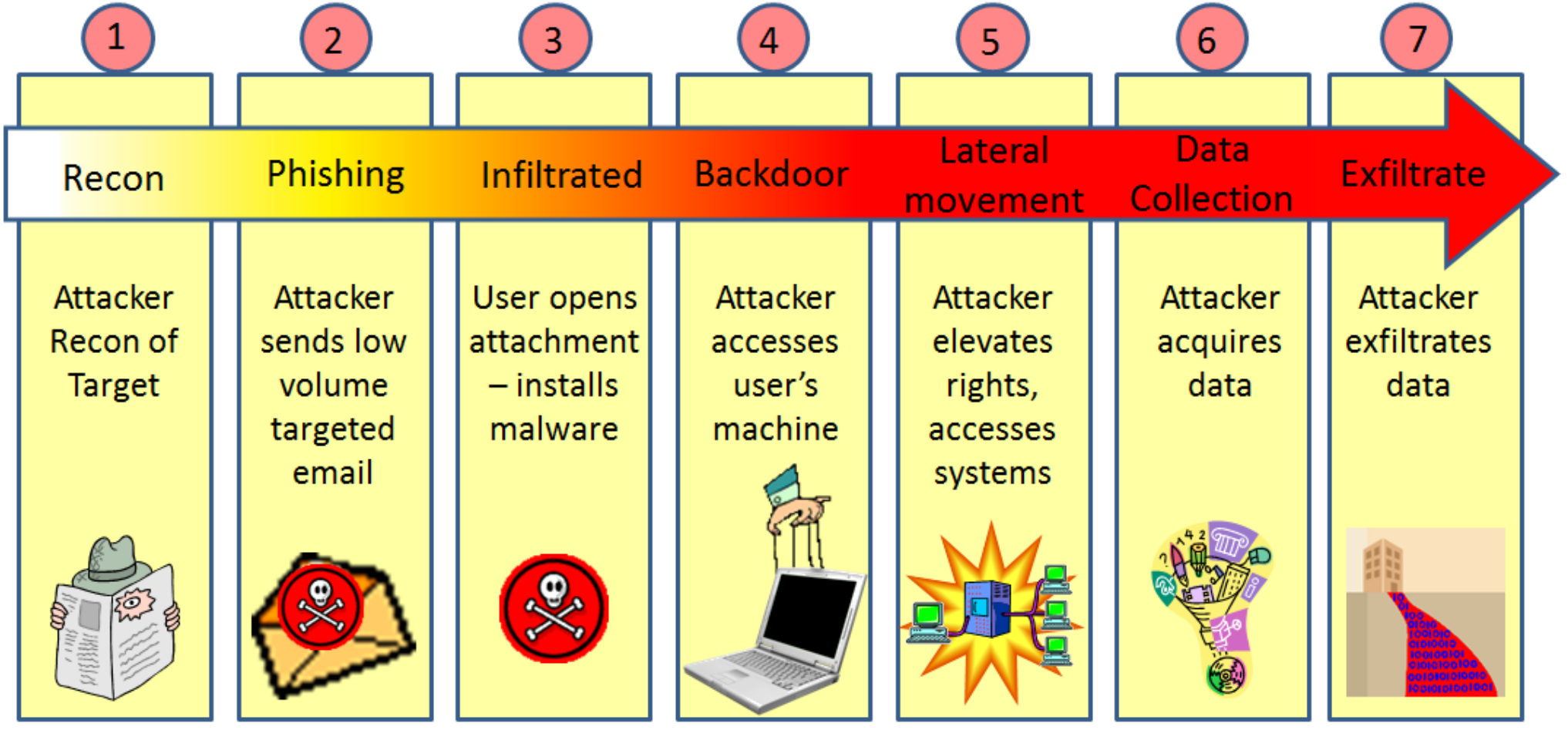
- Kompiuteris, kaip nusikaltimo taikinys.
- Kompiuteris, kaip nusikaltimo instrumentas.
- Kompiuteris, kaip nusikaltimo pagalbininkas.
- Nusikaltimai, susiję su kompiuterinės įrangos platinimu.

Elektroninių nusikaltimų tikslai

Pagrindiniai elektroninių nusikaltimų tikslai:

- Sabotažas ir destruktyvi veikla su tikslu sukompromituoti ar net sunaikinti įmonę/organizaciją
- Asmeninė, ekonominė nauda pavogiant duomenis
- Šnipinėjimas politiniais tikslai, siekiant gauti informaciją
- Įsilaužimas su tikslu, kuris vėliau panaudoti kompiuterį piktavališkiems tikslams
- Pasigyrimas ir didžiavimasis, kad sugebi įsilaužti į sistemą, apieti saugos priemones ir ribojimus.

Elektroninio nusikaltimo anotomija



Elektroninio nusikaltimo anotomija

1. Žvalgyba (recon, footprint)

Informacijos rinkimas, stebėjimas, aukos pasirinkimas

2. Skenavimas ir įsilaužimo metodo pasirinkimas (scanning)

Skenuojami prievadai, analizuojamos operacinės sistemos (versijos, atnaujinimų versijos), paleisti servisai, programinė įranga, ieškoma public SNMP.

3. Įsilaužimas (penetration, infiltration)

Sėkmingo įsilaužimo atveju paleidžiamas kenksmingas programinis kodas, renkama ir kopijuojama informacija, stengiamasi padidinti teises iki administratoriaus.

Elektroninio nusikaltimo anotomija

4. Pėdsakų naikinimas

Žurnalinių (operacinės sistemos, programų, saugos, audito) įrašų naikinimas

5. Backdoor atidarymas

Po įsilaužimo paliekama galimybė prisijungti. Naudojamas įvairius programinis kodas (pvz. root kit) arba išsaugomi prisijungimo duomenys.

6. Sistemos sutvarkymas (patching)

Po įsilaužimo kartais sutvarkoma sistema, panaikinant spragas (uždaromi portai, suintaliuojami patch ir t.t.) Taip nesudaroma galimybė kitiems laužti sistemos.

Elektroninio nusikaltimo tyrimas

Elektroninio nusikaltimo tyrimo **tikslas** yra nustatyti kas, kada, kur ir kaip buvo padaryta su kompiuteriu.

Tiriant nusikaltimą atliekami tokie pagrindiniai žingsniai

1. Nusikaltimo įkalčių išsaugojimas
2. Duomenų išgavimas iš surinktų įkalčių naudojant teisėtus metodus
3. Išgautų duomenų analizė
4. Išvadų pateikimas apie nusikaltimą, atsakant į klausimus:

   kas, kada, kaip ir kur.

Duomenų atstatymas

Virtualizacijos sluoksnis uždeda papildomus sunkumus, susijusius su duomenų atstatymus.

Galimi VM griuvimo atvejai:

- Sugadintas ESXi serveris, reikia atstatyti VM duomenis iš VMFS
- Sugadintas ESXi serveris, reikia atstatyti VM duomenis kai buvo naudojamas programinis duomenų šifravimas
- Sugadintas ESXi serveris, reikia atstatyti VM duomenis kai buvo naudojamas aparatūrinis duomenų šifravimas (TPM – trusted platform module).

Particijos/LUN atstatymas

Rekomenduojama kurti vieną failinę sistemą VMFS viename LUN. Tai supaprastina duomenų atstatymą.

Įvykus incidentui su disko particija, atstatymas apima tokius žingsnius:

1. Išsiaiškiname, kokia particija dingusi (*fdisk –l*)
2. Daromos veikiančių VM rezervinės kopijos. Net ir esant sugadintai particijai ESXi užtikrina VM veikimą, kol neperkraunama VM.
3. Sukuriama nauja particija (kartais gali reikti nurodyti pirmo ir paskutinio cilindro numerius)
4. Atstatomi duomenys iš rezervinės kopijos.

Duomenų rinkimas tyrimo metu

Duomenų surinkimas turi būti daromas laikantis galiojančių įstatymų. Surinkti duomenys gali būti pateikiami teismui, kaip įkalčiai, todėl privalo būti surinkti teisėtais būdais.

Surinkimas (angl. acquisition) susideda iš tokių aspektų:

1. Fizinės sistemos (kompiuterio, serverio) paėmimo
2. Duomenų išgavimas iš fizinės sistemos

Fiziškai paimant kompiuterį ar serverį turi būti:

- Padaroma foto nuotrauka
- Supakuojama
- Užpildoma paėmimo forma (Nr., data, aprašas, asmuo, parašas)

Duomenų išgavimas

Pagrindiniai reikalavimai:

1. Surinkti duomenys turi būti identiški duomenims, esantiems nusikaltimo įkalčiuose
2. Tyrimai negali būti daromi įkalčiais laikomuose kompiuteriuose t.y. turi būti daromos identiškos kopijos.
3. Kopijos darymo metu negalima keisti ar ištrinti duomenų įkalčiais laikomuose kompiuteriuose (read only, write - lock)
4. Kopijos teisingumas turi būti tikrinamas naudojant kontrolines sumas.
5. Įrenginys, į kurį kopijuojama turi būti tuščias ir didesnės talpos nei įkalčių kompiuterio diskas.

VM duomenų išgavimas

Duomenys, kurie turi būti išgauti tiriant VM:

- Virtualus diskas
- Atminties failai
- Metaduomenų failai

Veikiančiame VM‘e reikia nukopijuoti swap failą. Išjungus VM, swap faile duomenys trinami.

.vswp failas – tai VM swap failas iš VMFS pusės. Išjungiant VM, failas ištrinamas. Sukuriamas ir naudojamas tik viršijus vRAM.

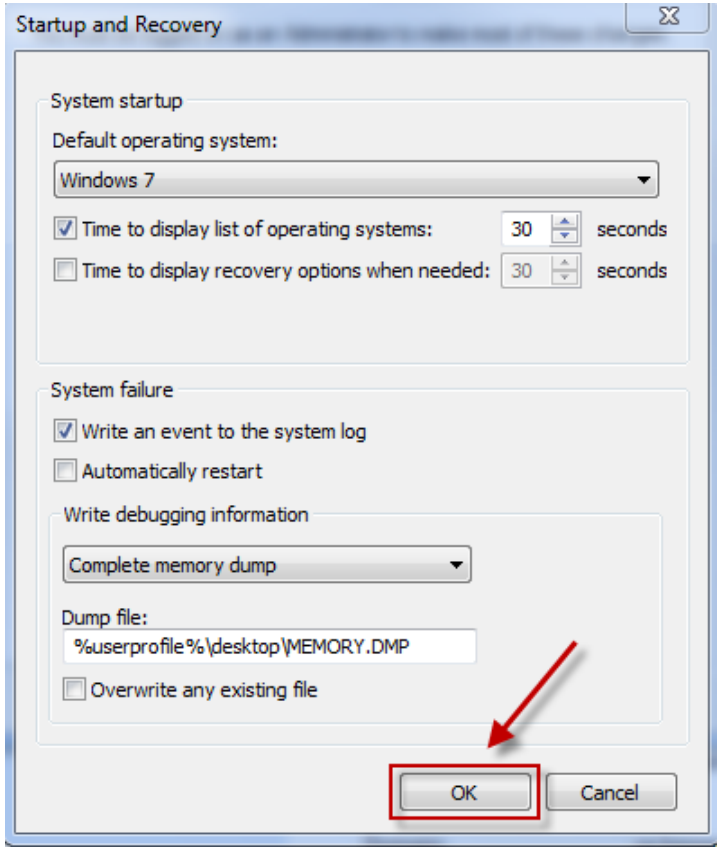
Veikiantis swap gali turėti ankstesnių įrašų dalių, nes įrašant naujus duomenis, ankstesni duomenys netrinami.

VM failų tipai

Plėtinys	Reikšmė
.log	Žurnalų failas
.nvram	RAM failas
.vmdk	VM disko failas <diskname>-<###>.vmdk
.vmem	Paging failas <snapshot_name_and_number>
.vmsd	Failas, kuriame saugoma metaduomenys apie shapshots
.vmsn	Snapshot failas <vmname>-Snapshot<###>.vmsn
.vmss	Suspenduotos VM būsenos failas
.vmtm	Konfigūracinis failas (team file)
.vmx	Pirminės konfigūracijos failas (iš Wizard)
.vmxf	Papildomas konfigūracinis failas (jei priklauso grupei - team)

VM atminties atvaizdas

Prieš išjungiant įkalčiu laikomą VM reikia atlikti jos atminties atvaizdo kopiją. Tai galima daryti iš OS pusės.



Linux

Linux OS atmintis susieta su dviem failais t.y.

/dev/mem – fizinė atmintis

/dev/kmem – virtuali atmintis

Kopijavimas atliekamas naudojant **dd** komadą.

VM atminties atvaizdai

- Fiziškai virtuali mašina ir jos konfigūracijos duomenys saugomi keliose failuose, iš kurių vienas skirtas mašinos virtualiai atminčiai.
- Norint sukurti operatyviosios atminties atvaizdą, reikia pasinaudoti vienu iš būdų:
  1. Suspenduoti virtualią mašiną ir nukopijuoti atminties failą į saugią išorinę laikmeną.
  2. Suformuoti virtualios mašinos operatyviosios atminties atvaizdą, panaudojant veikiančios sistemos būsenos kopiją.

Įrankiai

Duomenų surinkimo įrankiai:

- FTK Imager
- Encase Acquisition tool
- Linux dd komanda

Snapshot failai ir kopijos

- Snapshot failai naudojami padaryti disko būsenos atvaizdą.
- Darant kopijas atjungti VMware HA, nes priešingu atveju gali būti vykdomas duomenų atstatymas.
- Jei VMDK failai randasi shared saugykloje, tuomet turi būti naudojamos tik *read-only* teisės.
- Darant VM disko kopiją, mašina turi būti išjungta

VMFS kopija

- Norint padaryti VMFS kopija, šios failų sistemos neturi naudoti ESXi serveris.
- Visos VM, naudojančios kopijuojamą VMFS turi būti išjungtos.
- Įrenginys į kurį kopijuojama VMFS turi turėti tik read-only teises.
- Nukopijuotą VMFS galima užsimontuoti naudojant:
  - Linux‘ui skirtą **vmfs-tools paketą**
  - Windows tvarkyklę VMFS https://code.google.com/p/vmfs/
- Duomenys iš užmontuota VMFS kopijuojami su **dd** komanda
- Turint VMFS kopiją galimas ištrintų failų atstatymas
- Jei VM turėjo thin tipo zeroed diską, tokio ištrinto disko atstatymas bus probleminis.

Žurnaliniai įrašai

- **VMware.log** – failas, kuriame saugoma informacija susijusi su VM t.y. įjungimas, išjungimas, prisijungimas, įrenginių primontavimas.
- **/var/log/vmkernel** – ESXi hypervizoriaus įvykių žurnalas
- **/var/log/secure/** - prisijungimų prie ESX žurnalas, kai prisijungimai vyksta naudojant SUDO, SSH.\
- **/var/log/vmware/hostd.log** – žurnalas, kuriame registruojami vSphere kliento prisijungimai, remote CLI prisijungimai, prisijungimai prie vCenter.
- **VC žurnalai** apie prisijugimus.