Uvod u analizu zlonamjernih programa (malware-a)

Veleučilište Velika Gorica - 07.06.2022

Uvod u analizu malwarea

- Što su virusi i malware (zlonamjerni programi)
- Uradi sam
  - Potrebna znanja
  - Vrste analize
    - Ručna analiza
    - Automatska analiza
  - Alati za analizu
- Primjeri napada

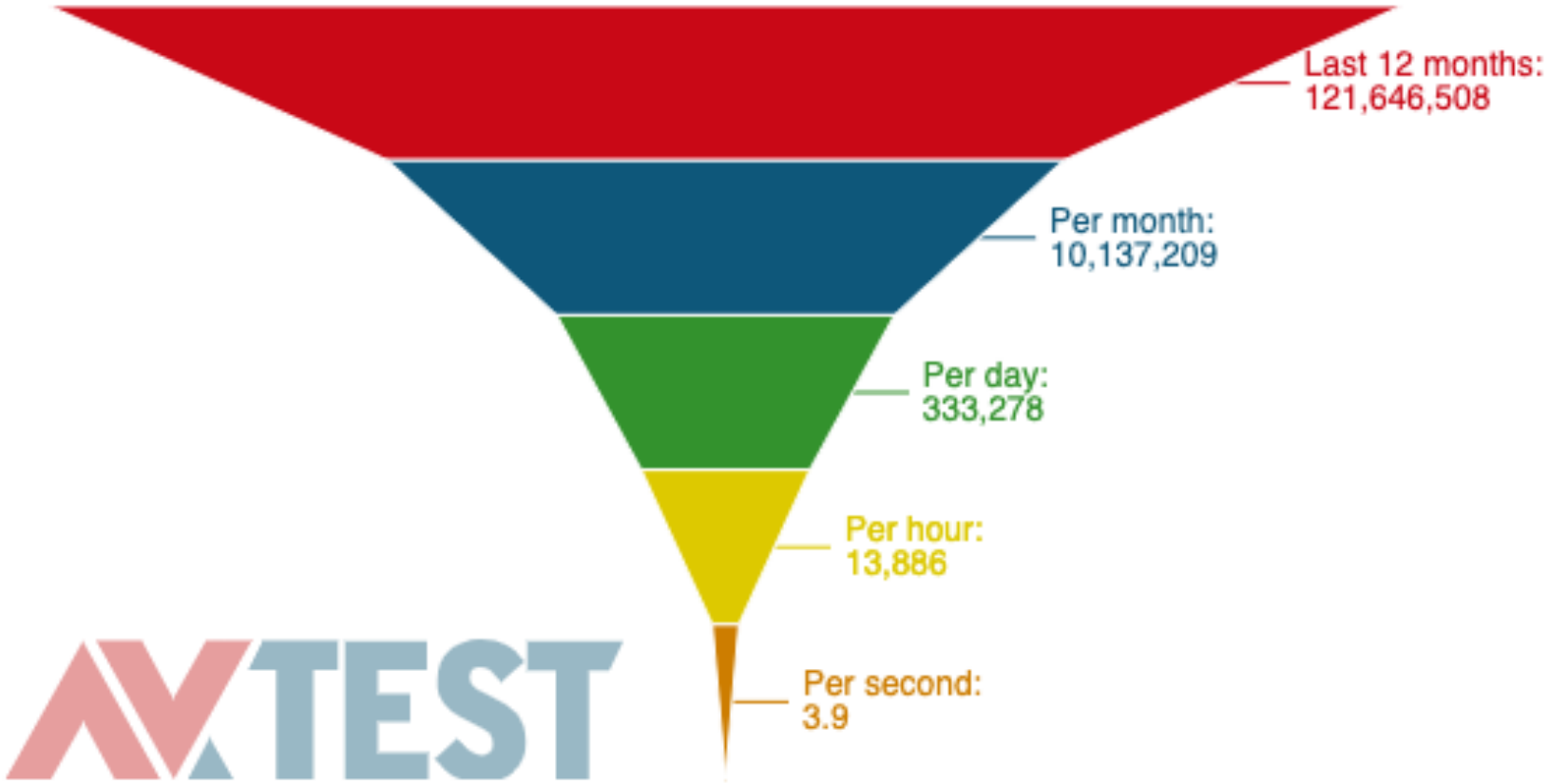
Definicija virusa

- Što su virusi i malware (zlonamjerni programi)
- Ne postoji jedna definicija
  - Virusi
  - Crvi
  - Trojanci
  - Potencijalno neželjeni programi

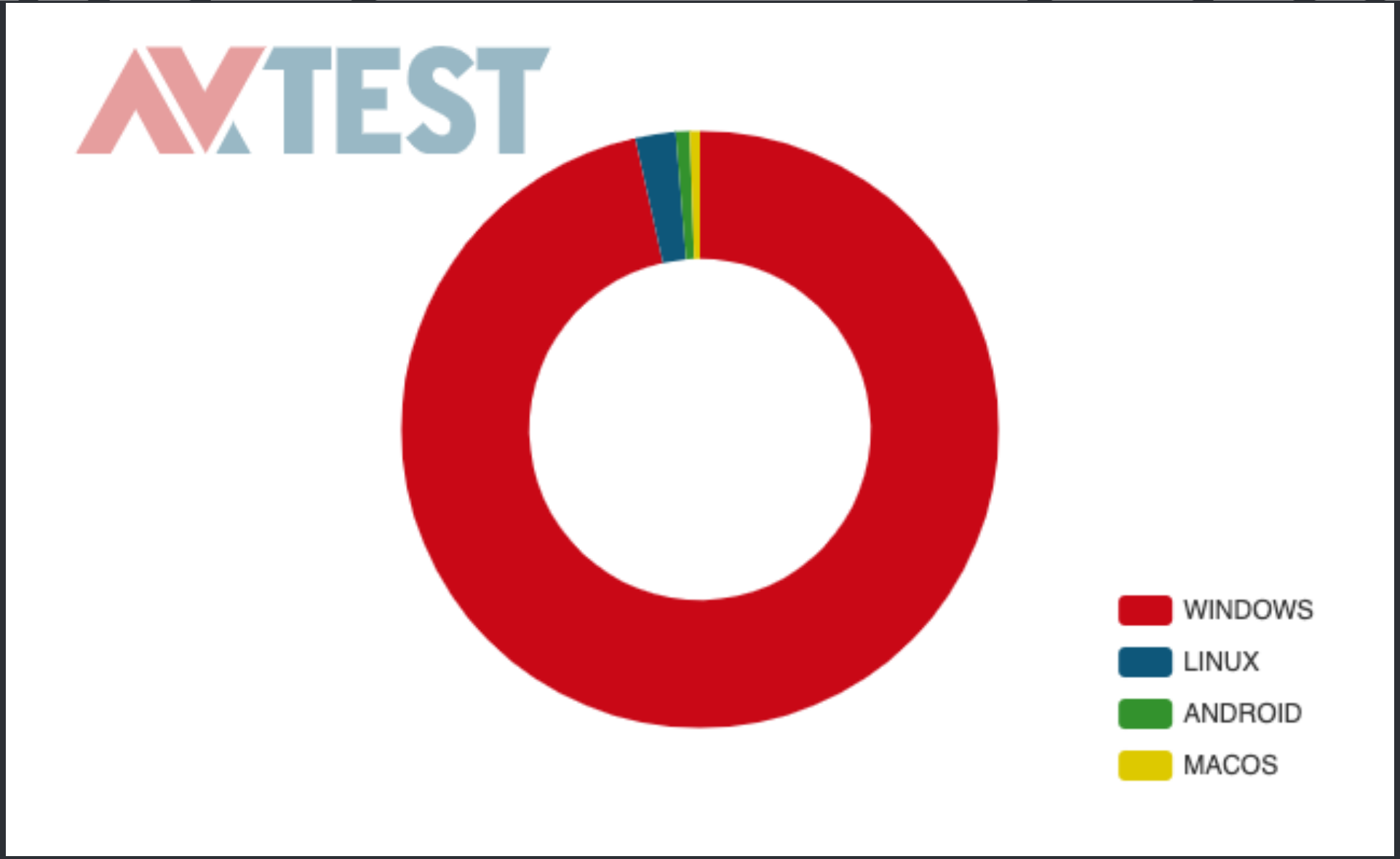
Najčešće prijetnje

- Ransomware
- Kradljivci podataka (stealers)
- Alati za daljinski pristup (RATs)
- Living off the land (sistemski i alati višestruke funkcije)

Statistika – novi malware



Statistika – po operativnom sustavu



Najčešći ciljevi

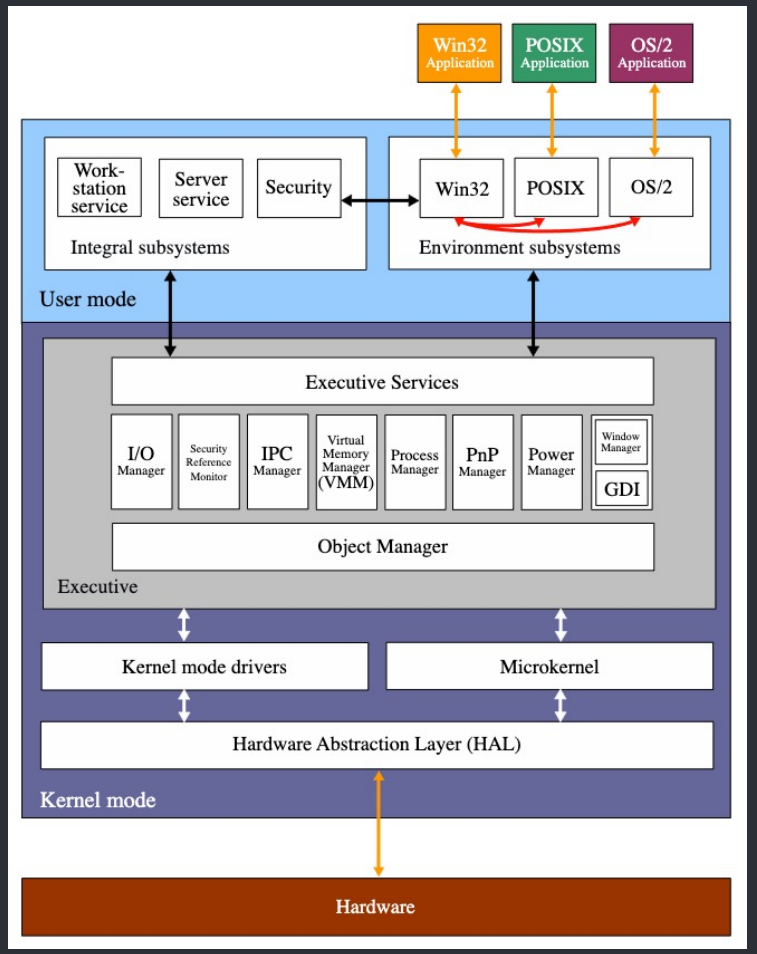
- Ekonomski
  - Izravna zarada
  - Krađa i prodaja podataka (ucjena)
  - Industrijska špijunaža
- Politički
  - Špijunaža
  - Destrukcija i ometanje funkcioniranja infrastrukture
- Za zabavu/dokazivanje znanja

Najčešći načini upada (vektori)

- Email + web
- Ranjivosti
- Besplatni (krekirani) programi na P2P mrežama
- Društvene mreže

Potrebna znanja

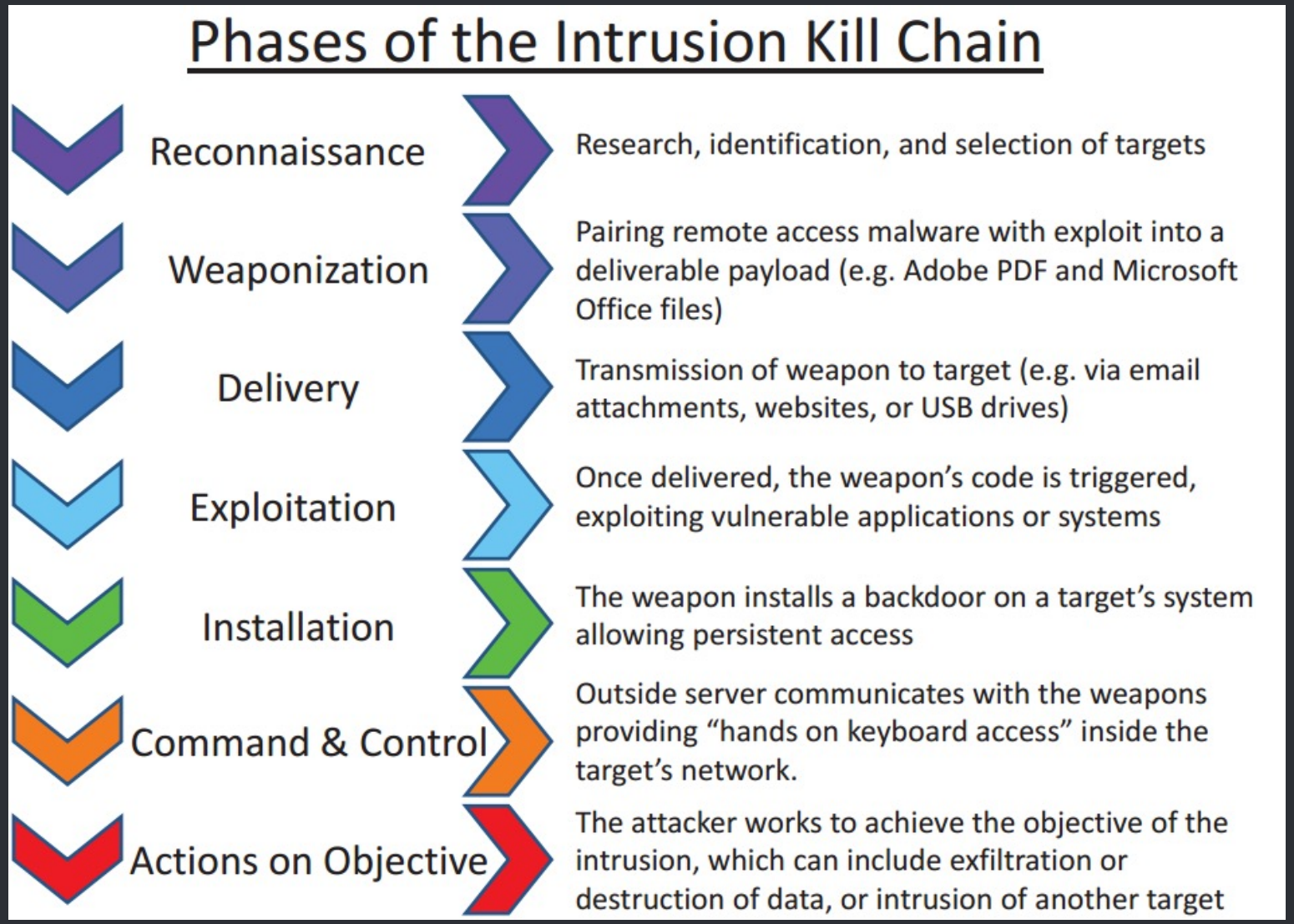
- Arhitektura Windowsa (BIOS, EFI, API, Boot process, memorija, Registry, File system)



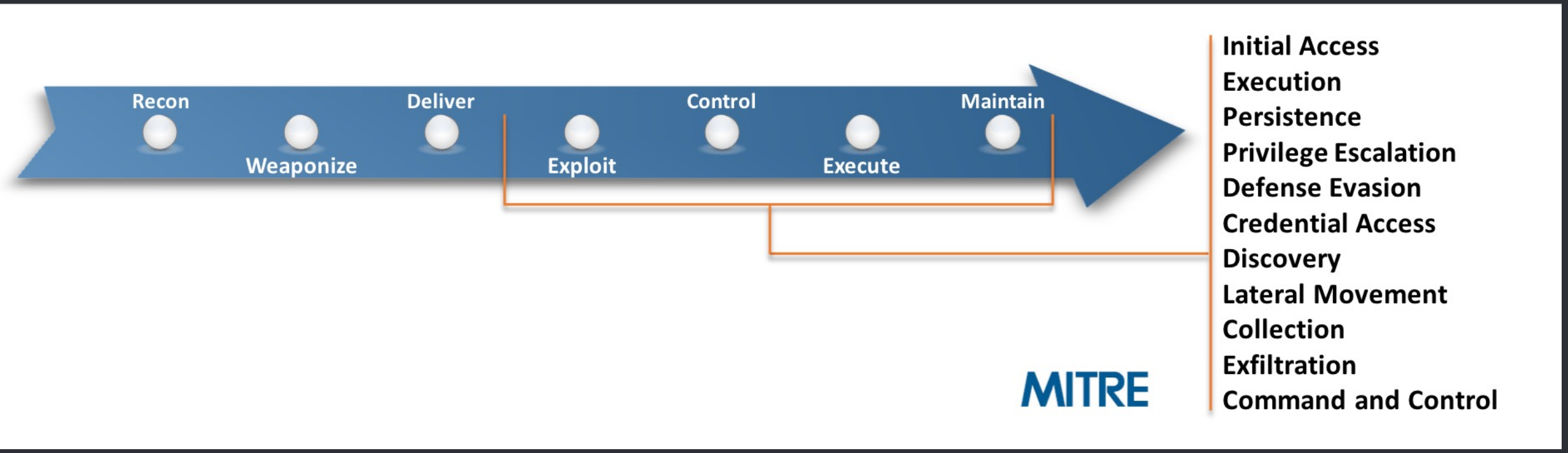
Potrebna znanja

- x64 (x86) assembler (i ARM, idealno) – na razini ABI
- Javascript, Visual Basic, Powershell
- Poznavanje formata datoteka (PE exe, OLE2 doc, PDF, Flash, RTF)
- Tipično ponašanje inficiranog sustava
- Barem jedan skriptni jezik (Python najpopularniji)
- Puno strpljenja i upornosti!!!

Lanac napada malware programa - killchain



ATT&CK okvir



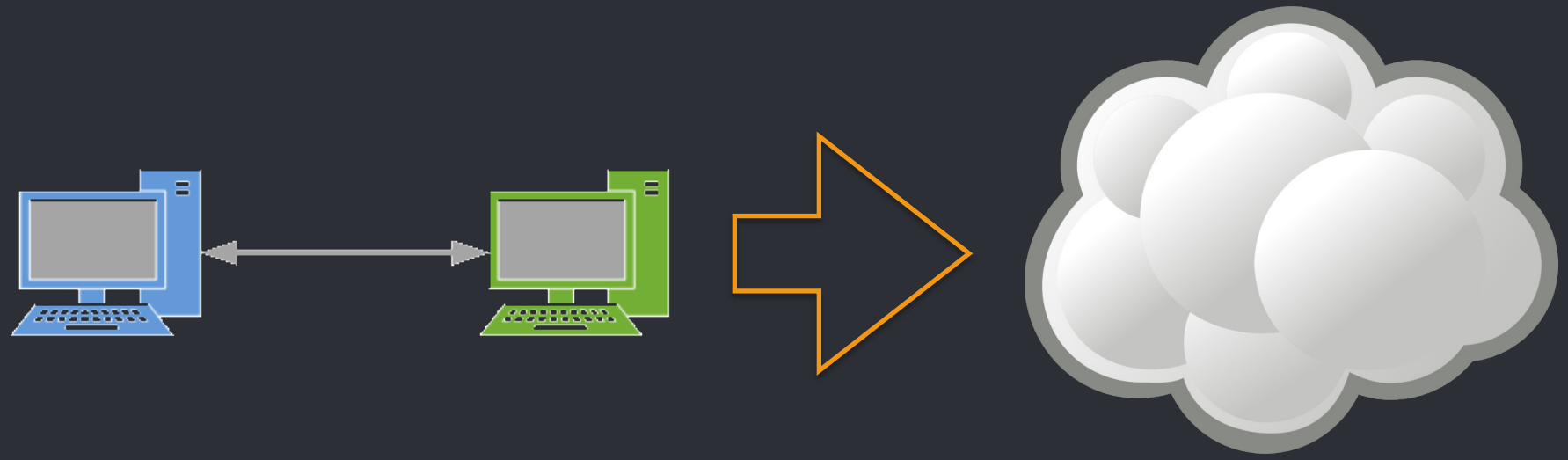
https://attack.mitre.org/wiki/Main_Page

Vrste i cilj analize

- Statička
- Dinamička
  - Ručna
  - Automatska

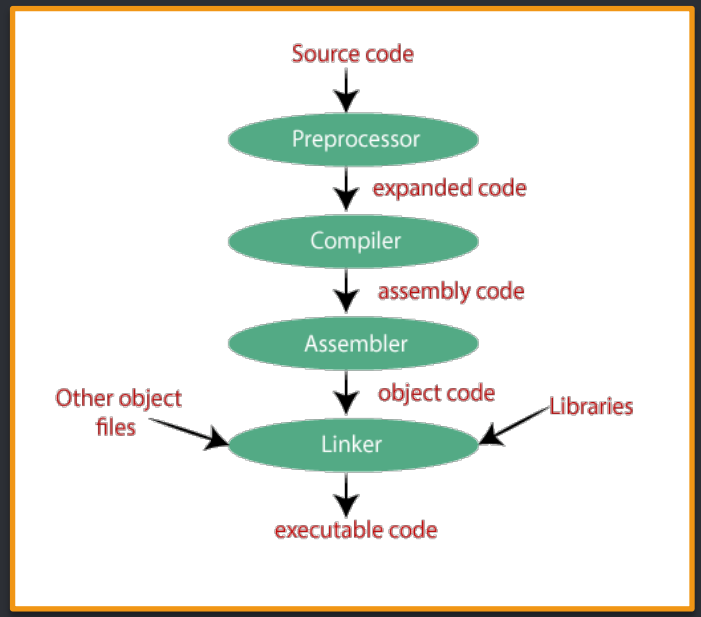
Okruženje za ručnu analizu

- Virtualni stroj(evi)
- Mrežna veza na VPN ili TOR



Alati - desktop

- Disasembleri i dekompajleri
  - IDAPro (free)
  - Ghidra
  - Radare
  - ilspy, dotPeek, dnSpy
- Debuggeri, API spies
  - OllyDbg (Immunity debugger)
  - x64dbg
  - WinDbg
  - Rohitab API monitor
  - sysmon
- Za analizu izmjena na sustavu
  - Sysinternals tools (process explorer, process monitor, autoruns, strings)
  - Process hacker
  - Hijack this, regshot
- Mrežni alati
  - Wireshark (tcpdump)
  - inetsim
  - Burp



Alati - desktop

- Anti rootkit alati
  - GMER
- Alati za analizu (statičku)
  - PEStudio, CFFExplorer
  - Ole tools, PDF tools (Didier Stevens), Cerbero Suite
  - HxD (hex editor)
- Antivirusni alati za samostalnu detekciju
  - Yara!!!
  - clam-av
- Alati za čišćenje računala
  - Kaspersky rescue disk
  - Sophos Hitman Pro

Alati – online i paketi

- Online sustavi
  - Virustotal
  - Hybrid analysis
  - Any.run
  - Joe sandbox
  - Hatching Triage
- Distribucije i kolekcije
  - Flare VM (Fireeye)
  - Remnux
  - Kali Linux
- Automatska analiza i klasifikacija
  - Cuckoo sandbox
  - Viper
- Virtualizacija
  - Virtualbox
  - Qemu (KVM)

Informacije o zlonamjernim programima

- Online analize/članci
  - Malpedia
  - Kaspersky securelist blog
  - Eset research
  - Microsoft Malware Protection blog
  - Sophos blog
  - Talos Intelligence

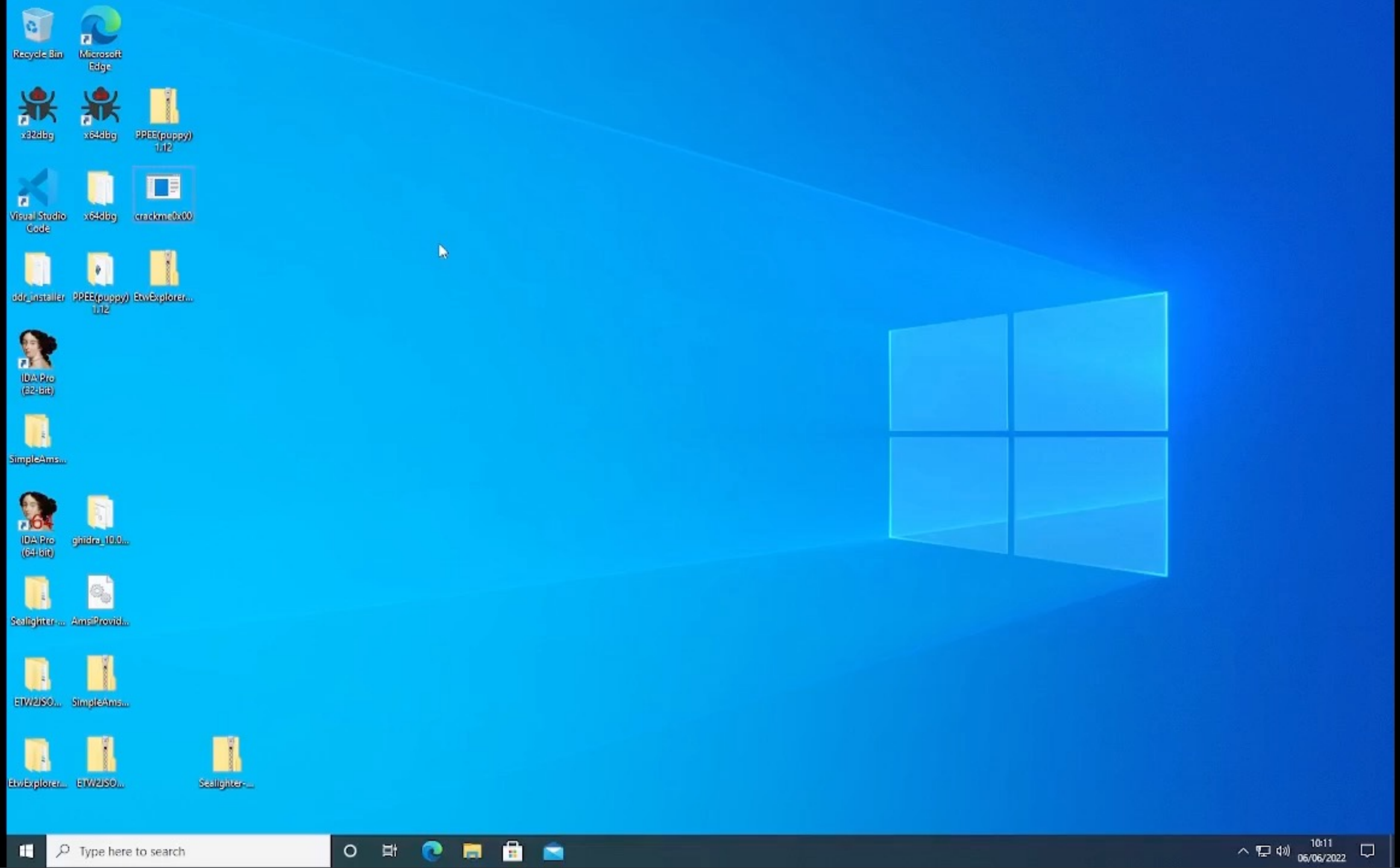
- Izvori uzoraka
  - Vxunderground
  - Malware bazaar (abuse.ch)
  - theZoo - A Live Malware Repository - na Githubu
  - virusshare.com
  - Vlastiti izvori poput računala ili honeypota

Primjer

- Analizirajte sami

https://github.com/Maijin/radare2-workshop-2015/blob/master/IOLI-crackme/bin-win32/crackme0x00.exe

1. CFF Explorer (PE Explorer, PPEE)
2. VirusTotal
3. Any.run
4. Ghidra
5. x32dbg/Ghidra debugger


Recycle Bin
Microsoft Edge
x32dbg
x64dbg
PPEE(puppy) 1.12
Visual Studio Code
x64dbg
crackme0x00
ddr_installer
PPEE(puppy) 1.12
EtwExplorer...
IDA Pro (32-bit)
SimpleAms...
IDA Pro (64-bit)
ghidra_10.0...
Sealighter-...
AmsiProvid...
ETW2JSO...
SimpleAms...
EtwExplorer...
ETW2JSO...
Sealighter-...
Type here to search
10:11
06/06/2022

Kamo dalje?

- https://github.com/corkami/pics/tree/master/binary
- https://malwareunicorn.org/workshops/re101.html
- https://malwareunicorn.org/workshops/re102.html

- Analizirajte https://github.com/Maijin/radare2-workshop-2015/blob/master/IOLI-crackme/bin-win32/crackme0x01.exe

Pitanja i odgovori