Вступ до аналізу шкідливого програмного забезпечення

курс лекцій

Ільїн Микола Іванович

2021 рік

Про автора

- к.т.н., зав. лабораторії технічної інформаційної безпеки
  - https://infosec.kpi.ua/ua/about.html
- CTO KievInfoSecurity LLC
  - тестування на проникнення, дослідження та розробка систем активного захисту
  - дослідження шкідливого програмного забезпечення, аналіз інцидентів
  - тренінги з технічної інформаційної безпеки
- засновник та лідер CTF команди dcua
  - https://defcon.org.ua
  - ТОП-10 2013-2019 рр. за версією CTFtime.org
  - команда чемпіон світу у 2016 році

Зміст

Лекція 1: Вступ, огляд інструментів та середовища аналізу

У лекції

Introduction and analysis environment setup

- Правові питання дослідження та використання ШПЗ
- Налаштування середовища аналізу
- Налаштування інструментів аналізу
- Операційна безпека при досліджені ШПЗ
- ЛР 1

Діюче законодавство України

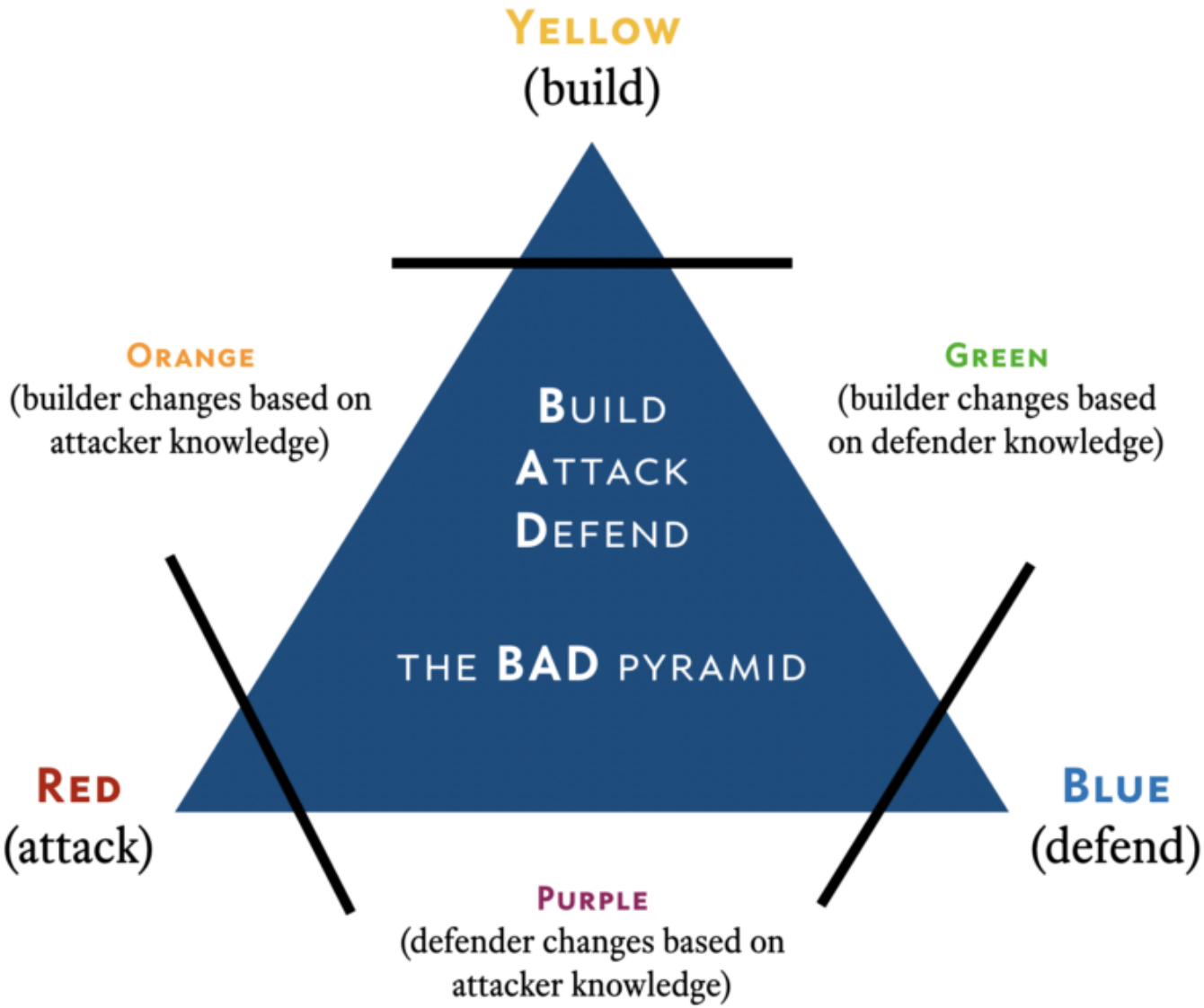
- Кримінальний кодекс України
  - Розділ XVI: кримінальні правопорушення у сфері використання ЕОМ, мереж
  - Ст. 361 незаконне втручання (також 376-1 втручання в документообіг суду)
  - Ст. 361-1 створення шкідливих програмних та технічних засобів (також ст. 359 СТЗ отримання інформації)
  - Ст. 361-2 розповсюдження інформації з обмеженим доступом
  - Ст. 363-1 DoS (також ст. 360 пошкодження телекомунікаційної мережі)
- Закон про оперативно-розшукову діяльність
  - Ст. 8 п. 18, 20 негласне зняття інформації

Легальне застосування технологій ШПЗ

- Правоохоронні органи, громадська безпека, державна та приватна розвідувальна спільнота
- Приклади застосувань
  - ISS World Europe – https://www.issworldtraining.com
  - 2021 Program Agenda: NSO Group, FinFisher, Memento Labs (former Hacking Team), CANDIRU, ...
- Private companies in nation-state offensive cyber operations
  - https://xorl.wordpress.com/offensive-security-private-companies-inventory
- https://citizenlab.ca/tag/spyware

- ... `¯\_(owo)_/¯`

Застосування ШПЗ та захист



Ізоляція небезпечного коду

- Віртуалізація
  - Типи гіпервізорів: 1 (ESXi, Proxmox VE), 2 (VMWare Workstation, VirtualBox)
  - Віртуалізація робочого столу, процесору, мережі, диску
- Відновлення стану системи
  - Засоби антивіртуалізації та антиемуляції у ШПЗ
- Застосування віртуалізації для динамічного аналізу
  - VMWare Workstation/Player
  - Oracle VirtualBox

Налаштування системи віртуалізації

TIME FOR A LIVE DEMO

- Налаштування віртуальної машини
  - Обмеження ресурсів (оперативна пам'ять, диск)
  - Мережевий інтерфейс
  - Збереження стану

Цільова система для досліджень

- Windows VMs
  - Microsoft Edge Developer
  - Windows 7, 8.1 x86
  - Windows 10 x64
  - Безкоштовні з обмеженням у часі
- ISO образи Windows
  - Microsoft Software Download
  - Windows 11, 10, 8.1, 7 x86/x64
  - Вимагає інсталяції, пробні версії без активації

Засоби аналізу

- Windows 10/11 development environment VM
  - SDK, Visual Studio, WSL з Ubuntu
  - Безкоштовна з обмеженням у часі
- FLARE VM
  - Інсталюється у існуючу Windows VM
- REMnux
  - OVA або у існуючу Ubuntu VM
- Kali
  - VM або live USB

Засоби аналізу та цільові системи

TIME FOR A LIVE DEMO

- Налаштування віртуальних машин
  - FLARE VM
  - REMnux
  - Kali
- Анонімізація мережевих комунікацій

Кошенятко після лекції CRDF_RE

Лекція 2: Основи програмування для аналізу ШПЗ

У лекції

Programming basics for malware analysis

- Основи мов програмування
  - Bash
  - Python 2 та 3
  - C#
  - Visual Basic for Applications
  - Powershell
- MITRE ATT&CK T1059: Command and Scripting Interpreter
- Приклади реалізації компонентів ШПЗ
- ЛР 2

Основні елементи мов програмування на прикладах

- Реалізація зворотного з'єднання з доступом до оболонки
- Reverse Shell Cheatsheet
  - https://github.com/swisskyrepo/PayloadsAllTheThings
  - Bash TCP, UDP, OpenSSL
  - C, C#
  - Python
  - Powershell
- Reverse Shell Generator
  - https://www.revshells.com
  - https://github.com/0dayCTF/reverse-shell-generator/blob/main/js/data.js

Bash

- T1059.004 – Command and Scripting Interpreter: Unix Shell
  - https://attack.mitre.org/techniques/T1059/004/
  - Windows Command Shell – https://attack.mitre.org/techniques/T1059/003/
- Приклад: закріплення FinSpy у Linux
  - https://securelist.com/finspy-unseen-findings/104322/
  - Linux Infection / Installer, Initial Loader

- Додаткові матеріали
  - Bash One-Liners – https://catonmat.net/books
  - Bash Reference Manual – https://www.gnu.org/software/bash/manual/bash.html

Python

- T1059.006 – Command and Scripting Interpreter: Python
  - https://attack.mitre.org/techniques/T1059/006/
- Приклад: Python for Offensive PenTest
  - https://github.com/PacktPublishing/Python-for-Offensive-PenTest
- Приклад: Ninja – C2 server for stealth red team operations
  - https://github.com/ahmedkhlief/Ninja/

C#

- Defense Evasion
  - T1027.004 – Obfuscated Files or Information: Compile After Delivery
  - T1127.001 – Trusted Developer Utilities Proxy Execution: MSBuild
- Приклад: Offensive C#
  - https://github.com/matterpreter/OffensiveCSharp
  - PowerSharpPack – https://github.com/S3cur3Th1sSh1t/PowerSharpPack
  - SharpKatz – https://github.com/b4rtik/SharpKatz, SharpKatz/Win32/Syscall.cs
- Приклад: AsyncRAT-C#
  - https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp

Visual Basic for Applications

- T1059.005 – Command and Scripting Interpreter: Visual Basic
  - https://attack.mitre.org/techniques/T1059/005/
- Приклад: macro_pack
  - https://github.com/sevagas/macro_pack

Powershell

- T1059.001 – Command and Scripting Interpreter: PowerShell
  - https://attack.mitre.org/techniques/T1059/001/
- Приклад: обхід Mark of the Web у ISO навантаженні Nobelium
  - https://www.scythe.io/library/threat-thursday-evading-defenses-with-iso-files-like-nobelium
  - https://gist.github.com/mgraeber-rc/a780834c983bc0d53121c39c276bd9f3

Кошенятко після лекції CRDF_RE

Лекція 3: Вступ до статичного аналізу ШПЗ

У лекції

Basic static analysis

- Визначення типу файлу на основі сигнатурного аналізу
- Аналіз неструктурованих даних
- Аналіз виконуваних файлів Windows (Portable Executable)
- Аналіз документів Microsoft Office (OLE2, OOXML)
- ЛР 3

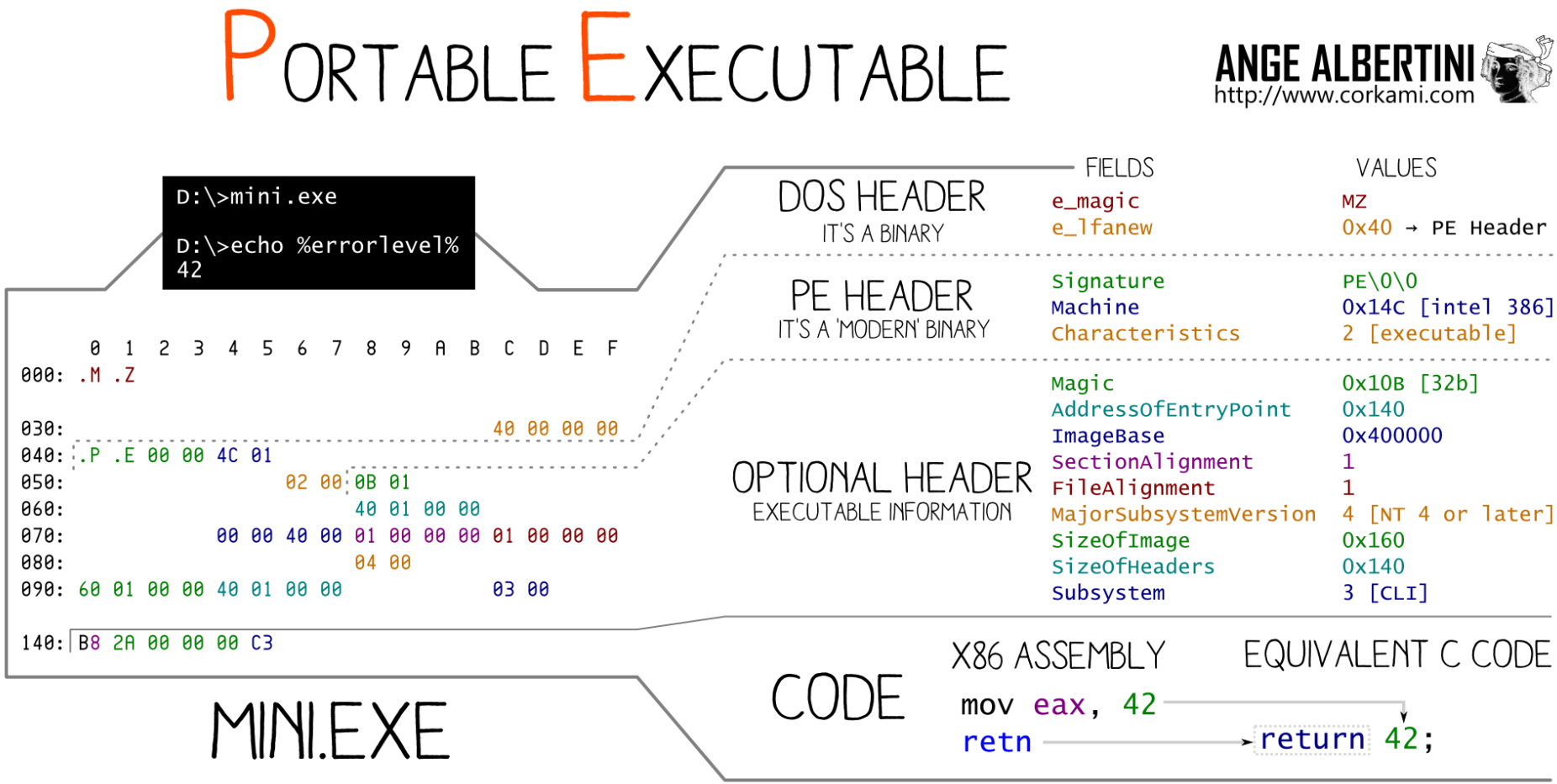
Визначення типу файлу

- Пошук сигнатур відомих форматів
  - file/libmagic
- Аналіз виконуваних файлів
  - Визначення компілятору, лінкеру і версій
  - Пакувальник, протектор виконуваних файлів
  - Використані бібліотеки та функції: криптоалгоритми, алгоритми стиснення даних
- Засоби аналізу
  - PEiD, TrID, DIE, Exeinfo PE
  - Вбудовані засоби PeStudio, PE-bear
  - Розширення IDA FindCrypt/FindCrypt2, findcrypt-yara
  - Розширення FindCrypt-Ghidra

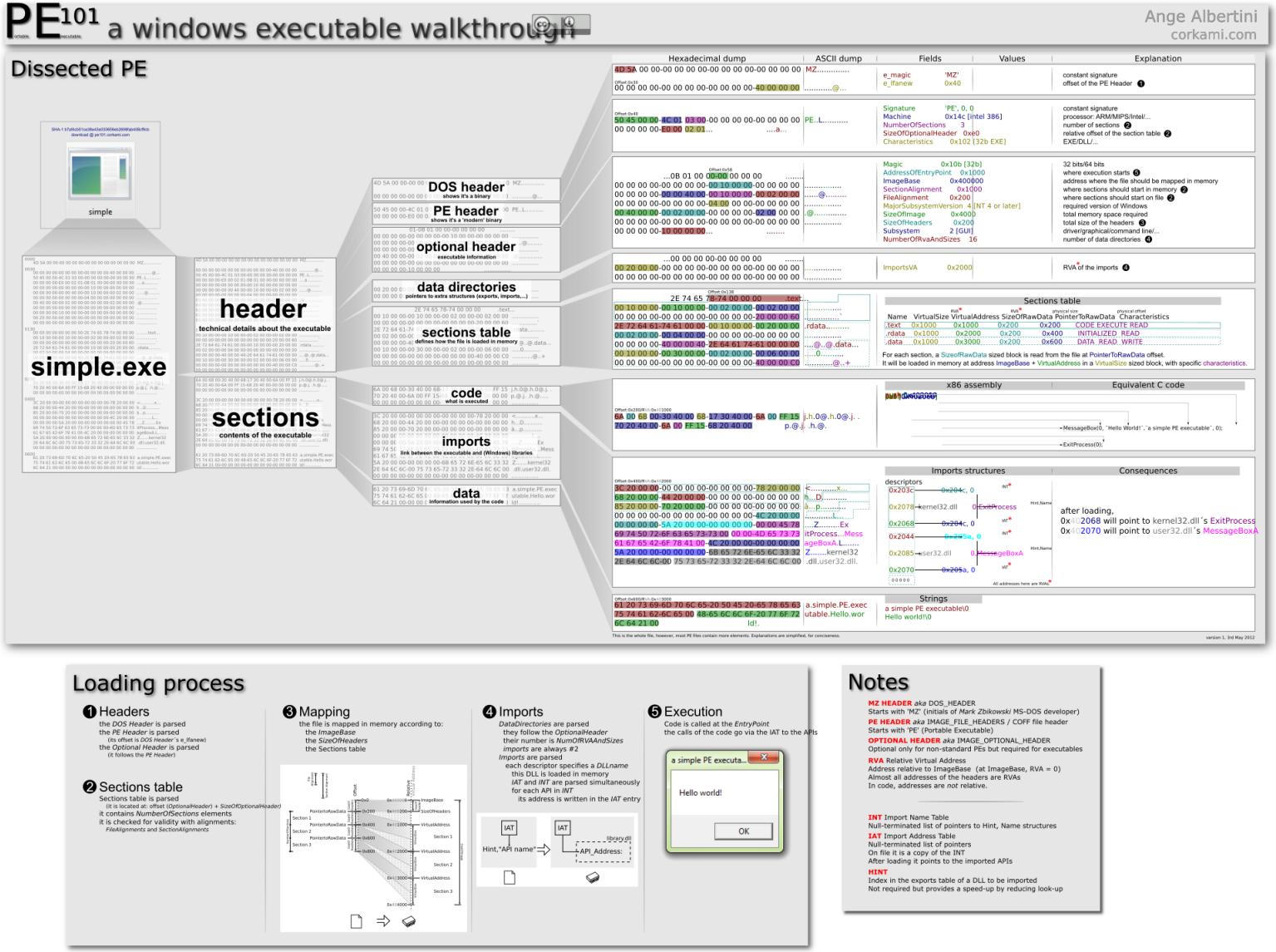
Аналіз неструктурованих даних

- Пошук відомих форматів у потокових даних
  - Зліпок пам'яті, диску
  - Вбудовані файли та архіви у виконуваних файлах
- Засоби аналізу
  - foremost
  - binwalk -e
  - bulk_extractor
- Розробка інструментів аналізу
  - Hachoir – https://hachoir.readthedocs.io
  - hachoir.parser, hachoir-metadata
  - hachoir.editor

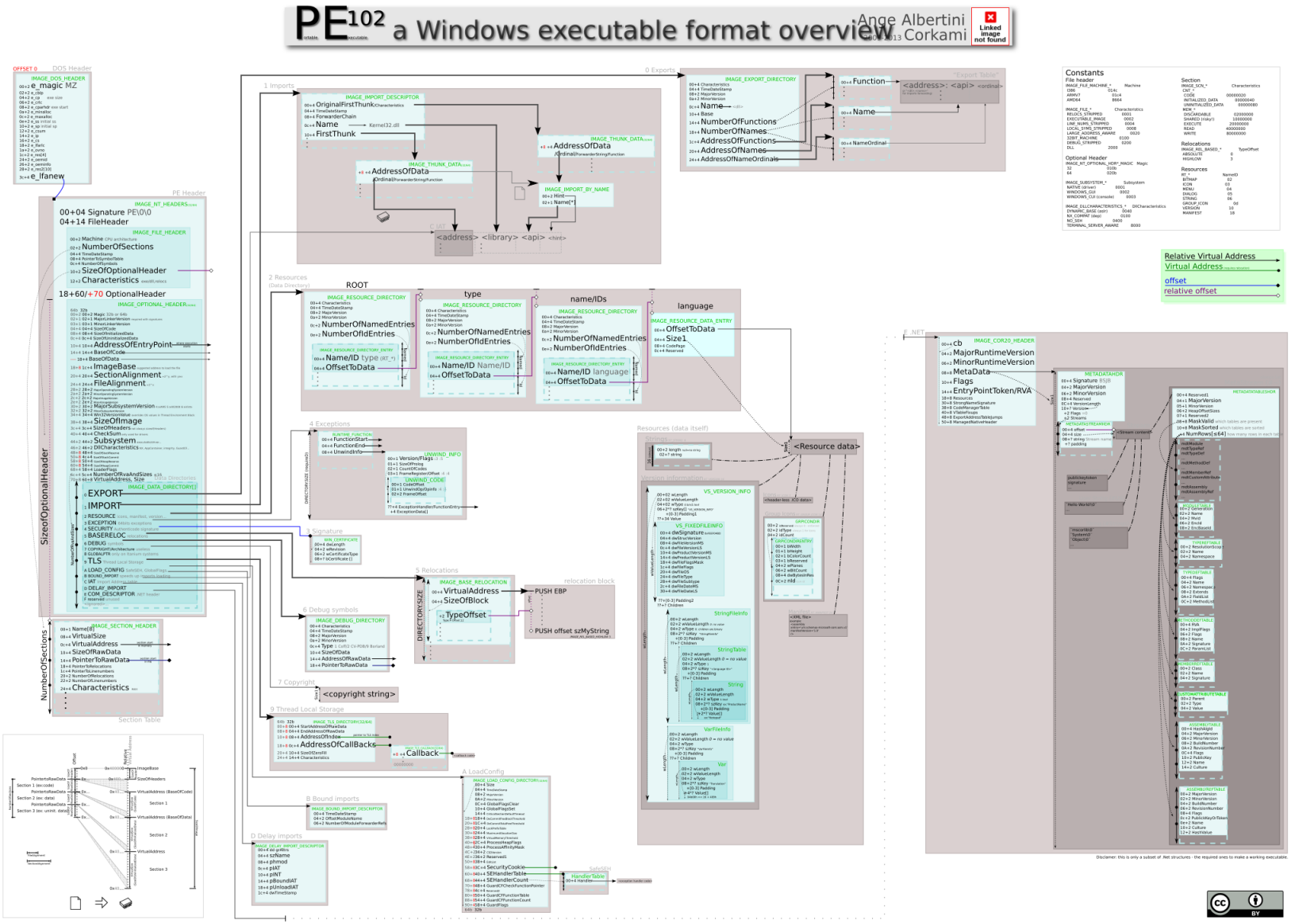
PE – https://github.com/corkami/pics



PE 101 – https://github.com/corkami/pics



PE 102 – https://github.com/corkami/pics



Ознаки ШПЗ та аналіз виконуваних файлів

- Візуалізація PE
  - PE Tree – https://github.com/blackberry/pe_tree
  - pev – https://github.com/merces/pev
- Евристики PeStudio
  - MalAPI – https://malapi.io
- Евристики capa
  - https://github.com/mandiant/capa-rules
- Аналіз спотворених файлів у PE-bear
  - bearparser, https://hshrzd.wordpress.com/pe-bear
- Розробка інструментів аналізу
  - pefile, LIEF
- Приклад: мітки часу у заголовках PE
  - https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps

Аналіз документів Microsoft Office

- Формати файлів
  - DOC, XLS, PPT: Microsoft OLE2 (Compound File Binary Format, Compound Document format, Composite Document File V2)
  - DOCX, XLSX, PPTX: Office Open XML (OOXML)
- Специфікація форматів
  - MS-CFB: Compound File Binary File Format
  - ECMA-376, ISO/IEC 29500:2008
- Ознаки ШПЗ
  - python-oletools oleid, olevba
- Розробка інструментів аналізу
  - Apache Tikka, POI
  - olefile, python-oletools
  - openmcdf

Кошенятко після лекції CRDF_RE

Лекція 4: Основи статичного аналізу ШПЗ

У лекції

Intermediate static analysis

- Дизасемблювання та декомпіляція для статичного аналізу ШПЗ
  - Hex Rays IDA Pro
  - NSA Ghidra SRE
- Дизасемблювання VBA p-code
- ЛР 3

Статичний аналіз з IDA Pro

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у IDA Free/Educational

Статичний аналіз з Ghidra

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у Ghidra

Статичний аналіз проміжного коду VBA

TIME FOR A LIVE DEMO

- VBA p-code disassembler
  - https://github.com/bontchev/pcodedmp
  - VBA5 (Office 97), VBA6 (Office 2000-2009), VBA7 (Office 2010+)
- Приклад: EvilClippy
  - https://github.com/outflanknl/EvilClippy

Кошенятко після лекції CRDF_RE

Лекція 5: Вступ до динамічного аналізу ШПЗ

У лекції

Basic dynamic analysis

- Використання пісочниць для аналізу ШПЗ
- Поведінковий аналіз з Sysinternals Suite
- Онлайн севріси аналізу ШПЗ
- ЛР 4

Додаткові матеріали

1. Malware Reverse Engineering Handbook
   - https://ccdcoe.org/library/publications/malware-reverse-engineering-handbook

Технології ізоляція ШПЗ у Windows

- Windows Sandbox
  - Microsoft Defender Application Guard (WDAG)
  - https://github.com/LloydLabs/wsb-detect
- Sandboxie
  - https://github.com/sandboxie-plus
- Емулятори на прикладі Windows Defender
  - https://github.com/0xAlexei/WindowsDefenderTools
  - https://github.com/hfiref0x/WDExtract
- Проблеми емуляції Windows x86
  - ISA https://github.com/trailofbits/mishegos
  - (bdshemu) https://github.com/bitdefender/bddisasm
  - WinAPI https://github.com/jackullrich/Windows-API-Fuzzer
  - (AVLeak)

Windows Sandbox

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у WSB

Динамічний аналіз ШПЗ з Sysinternals Suite

- Sysinternals Suite
  - https://aka.ms/sysinternals
  - https://live.sysinternals.com
- Аналіз процесів
  - Process Explorer
  - Process Monitor
  - AutoRuns
- Аналіз безпеки
  - Sysmon
- Пісочниці на базі утиліт Sysinternals
  - https://github.com/Rurik/Noriben

Sysinternals Suite

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у Noriben

Онлайн севріси аналізу ШПЗ

- Cuckoo Sandbox
  - https://github.com/cuckoosandbox
  - https://cuckoo.cert.ee
- ANY.RUN - Interactive Online Malware Sandbox
  - https://any.run/features
  - https://app.any.run
- Hybrid Analysis
  - CrowdStrike Falcon Sandbox
  - https://www.hybrid-analysis.com
- VirusTotal
  - https://www.virustotal.com
  - https://twitter.com/RedDrip7/status/1293128696035815425
  - Аналоги https://virustest.gov.ru
- Агрегація даних
  - https://github.com/Neo23x0/munin

Cuckoo Sandbox

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у Cuckoo Sandbox

Кошенятко після лекції CRDF_RE

Лекція 6: Основи динамічного аналізу ШПЗ

У лекції

Intermediate dynamic analysis

- Застосування налагоджувача для динамічного аналізу ШПЗ
  - x64dbg
  - WinDbg, WinDbgX
- ЛР 4, 8

Додаткові матеріали

1. Windows Malware Analysis training (volume 1)
   - https://github.com/hasherezade/malware_training_vol1

Динамічний аналіз з x64dbg

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у x64dbg

Динамічний аналіз з WinDbgX

TIME FOR A LIVE DEMO

- Аналіз виконуваного файлу ШПЗ у WinDbgX

Динамічний аналіз на рівні ядра Windows

TIME FOR A LIVE DEMO

- Аналіз маскування процесів у ШПЗ на рівні ядра
- Аналіз структури EPROCESS з `windbg -kl`

Кошенятко після лекції CRDF_RE

Лекція 7: Аналіз пам'яті систем з активним ШПЗ

У лекції

Memory forensics in malware analysis

- Отримання зліпку пам'яті системи (memory dump)
- Отримання зліпку процесу (process dump)
- Аналіз зліпків пам'яті з Volatility Framework
- ЛР 5, 6

Отримання зліпку пам'яті цільової систем

- FTK Imager
  - https://www.exterro.com/ftk-imager
- The Pmem Suite
  - WinPmem, OSXPmem, LinPmem
  - WinXP - Win 10, x86 + x64
  - https://winpmem.velocidex.com
- Приклад DMA атак: Inception
  - https://github.com/carmaa/inception

Отримання зліпку пам'яті процесу

- Sysinternals ProcDump
  - https://docs.microsoft.com/en-us/sysinternals/downloads/procdump
  - Аналоги https://github.com/glmcdona/Process-Dump
- Win32 MiniDumpWriteDump API
  - https://car.mitre.org/analytics/CAR-2020-05-001
- T1003.001 – OS Credential Dumping: LSASS Memory
  - mimikatz sekurlsa::minidump

Аналіз зліпку пам'яті

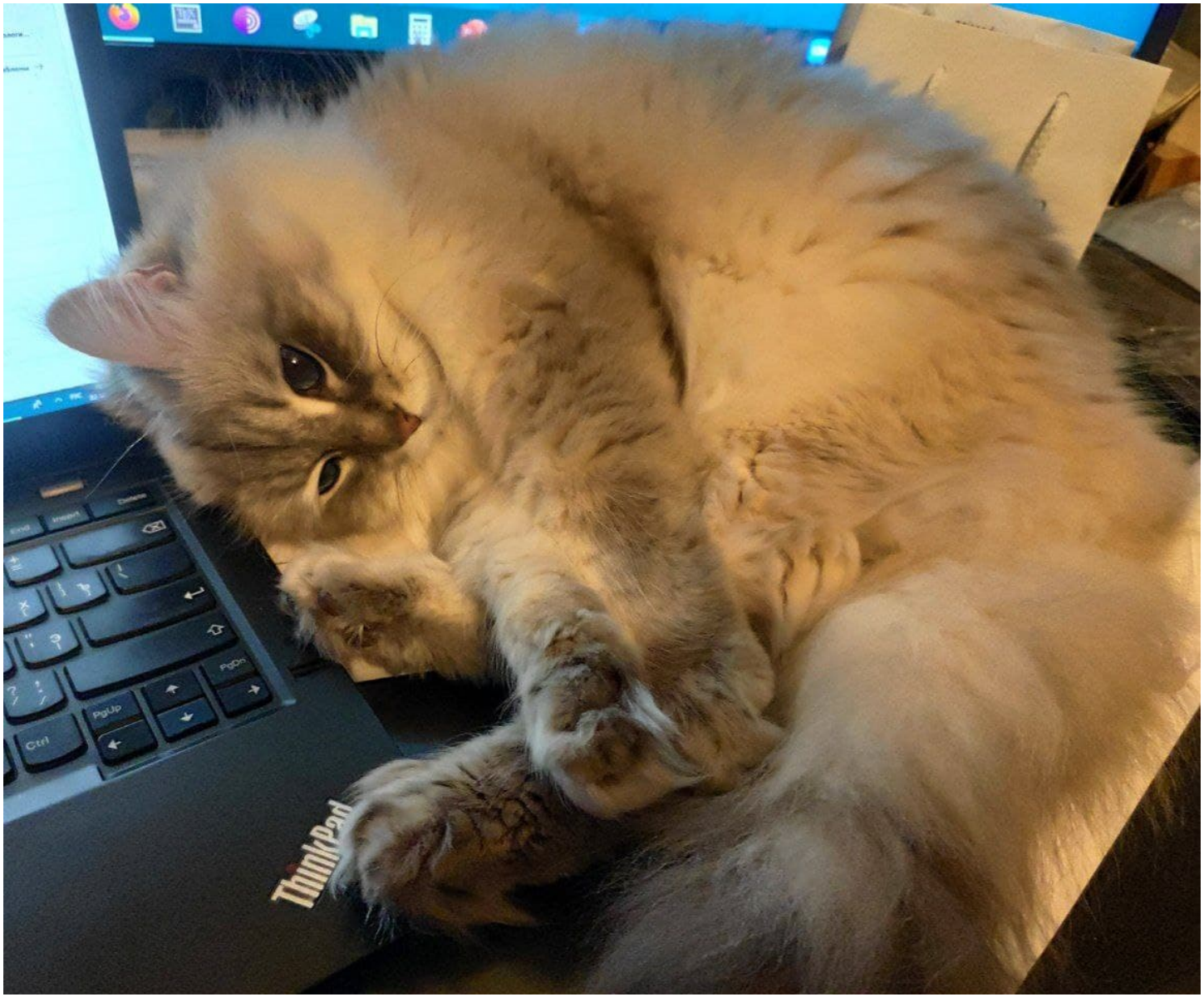
- Volatility Framework
  - https://www.volatilityfoundation.org
- FireEye Redline
  - https://www.fireeye.com/services/freeware/redline.html
- Розробка інструментів аналізу: Malduck
  - https://github.com/CERT-Polska/malduck
  - Memory model objects

Аналіз зліпку пам'яті з Volatility

TIME FOR A LIVE DEMO

- Аналіз зліпку пам'яті системи Windows 10 з активним ШПЗ
- Плагіни Volatility 2, 3

Кошенятко після лекції CRDF_RE



Лекція 8: Аналіз загроз

У лекції

Technical threat intelligence

- Ознаки компрометації (Indicators of Compromise, IoC)
- Обмін інформацією про загрози з MISP
- Аналіз цільової системи
- ЛР 6, 7

Вступ до YARA

- YARA
  - Пошук та класифікація ШПЗ
  - https://virustotal.github.io/yara
  - yextend
  - https://github.com/InQuest/awesome-yara
- Сигнатури YARA
  - https://yara.readthedocs.io/en/stable/writingrules.html
  - Текстові рядки (nocase, wide)
  - Бінарні дані (hexadecimal string, base64, xor)
  - Регулярні вирази
  - Умови (at, довжина, entrypoint, логічні вирази)
  - Ітератори
  - Модулі (pe, dotnet, hash, math, magic)
  - https://github.com/Neo23x0/yarGen

Приклади YARA

TIME FOR A LIVE DEMO

- Приклади сигнатур YARA
- IDDQD - Godmode YARA Rule
  https://gist.github.com/Neo23x0/f1bb645a4f715cb499150c5a14d82b44
- https://github.com/Neo23x0/signature-base

Вступ до MISP

- Обмін інформацією про загрози з MISP
  - https://www.misp-project.org
  - Моделі даних ознак компрометації (IoC)
  - Класифікація з автоматичною кореляцією IoC
  - Розповсюдження IoC у реальному часі
  - API (в т.ч. Python), підтримка STIX 2.0, OpenIOC
  - Автоматичне створеня правил IDS (Snort, Suricata, Zeek)
- Моделі даних
  - MISP Core Format
  - https://www.misp-project.org/datamodels
  - https://github.com/MISP/misp-taxonomies

Приклади MISP

TIME FOR A LIVE DEMO

- MISP default feeds

Аналіз цільової системи

- Сигнатури YARA

```
yara [OPTION]... RULES_FILE... FILE | DIR | PID
```

- Інші IoC
  - https://github.com/Neo23x0/Loki
  - https://www.nextron-systems.com/thor-lite
  - https://github.com/spyre-project/spyre

- Аналіз загроз в корпоративному середовищі
  - Security Onion 2 Linux
  - Security Onion Console Network, Host Visibility
  - TheHive Security Incident Response Platform
  - https://docs.securityonion.net

Приклади аналізу цільової системи

TIME FOR A LIVE DEMO

- Аналіз індикаторів скомпрометованої системи Windows 10

Кошенятко після лекції CRDF_RE

Дякуємо за увагу!

Telegram	@mykola_ilin
Threema	2SS7EYDB
Email	m.ilin@kpi.ua
PGP	B88F 30B6 E01F B518 9891 F8D1 2CD2 D192 CC69 26A6

Кошенята в кінці лекцій з https://t.me/cats_cats