
	<h1>INGENIERÍA DE SISTEMAS</h1>	 INICIAL APELLIDO PATERNO
	<h2>AUDITORIA DE SISTEMAS</h2>	
<h3>EXAMEN SEGUNDO PARCIAL</h3>		
NOMBRES	APELLIDO PATERNO	APELLIDO MATERNO
EDSON JAVIER	PACO	LIMACHI
CI.	CEL.	FECHA
5972576	73734591	15/06/2023

TABLA DE CONTENIDO

LABORATORIO 6	2
Indicaciones	2
Preparación de herramienta	2
Proceso de descarga de archivos para la auditoria.....	3
Documento 01.....	4
Proceso de auditorio del archivo descargado.....	4
Análisis de los resultados extraídos del documento junto a la herramienta.....	6
Documento 2 (.doc)	8
Proceso de descarga del archivo.....	8
Proceso de auditoria del archivo descargado	9
Análisis de los resultados extraídos del documento junto a la herramienta.....	11
Documento 3(.docx)	13
Proceso de descarga del archivo.....	13
Proceso de auditoría del archivo descargado	14
Análisis de los resultados extraídos del documento junto a la herramienta.....	16

PREGUNTA DE EXAMEN (LABORATORIO 6)

68	PACO	LIMACHI	EDSON JAVIER	5972576	200028567	6
----	------	---------	--------------	---------	-----------	---

LABORATORIO 6

INDICACIONES

(Auditoria de Malware en Documentos Word, Excel PDF, PowerPoint, etc.). Para este laboratorio debe **realizar paso a paso y con capturas de pantalla de todo el procedimiento realizado** en función de los siguientes puntos:

• Del siguiente sitio web <https://github.com/jstrosch/malware-samples> puede descargar los siguientes **tipos de archivos (3 opciones dadas)**, de los cuales debe elegir 2 muestras para la realización de su examen (A su elección):

• Tipo Microsoft Word.

• Tipo Microsoft Excel.

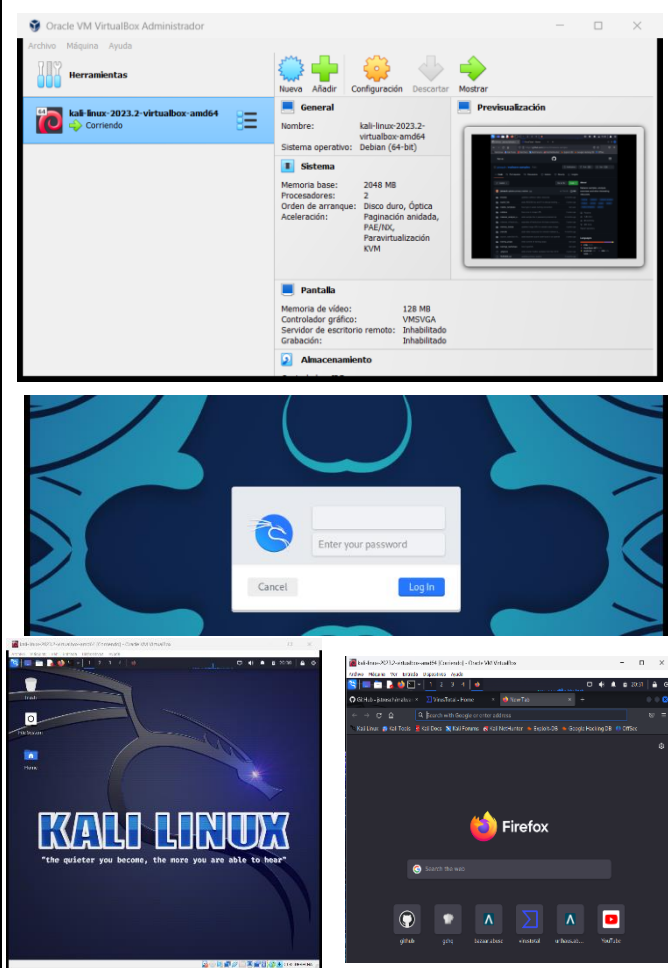
• Tipo aplicación, ejecutable.

• Posteriormente debe analizar de manera exhaustiva con las herramientas vistas los resultados obtenidos (Exploit, reglas Yara, Visual Basic, entre otros...)

• A mayor cantidad de análisis de los resultados obtenidos, mayor la asignación de la nota.

Nota. Si los archivos que eligió NO contienen mucha información en cuanto a resultados, debe buscar otros que si contengan una gran cantidad de información de malware.

Empiezo de auditoria y analisis

CAPTURAS	EXPLICACION
	<h3>PREPARACIÓN DE HERRAMIENTA</h3> <ol style="list-style-type: none">1. Primeramente realizamos s la previa instalación de la maquina virtual y el software para realizar virtualización el cual es VIRTUAL-BOX2. El sistema operativo usado es la distribución de LINUX que es KALI LINUX.3. Esta maquina fue descargada desde su pagina oficial de Kali y solo se debe realizar configuración de red después todo viene ya configurado ya que es una plantilla pre diseñada listo para el uso4. Como vemos en la imagen damos a iniciar la maquina virtual5. Una ves iniciada la maquina nos pedirá las credenciales6. Las cuales son USUARIO : Kali PASSWORD: Kali7. Estas credenciales ya están configuradas por defecto si se desea se puede cambiar pero por el momento no es recomendable8. Como podemos apreciar en las imágenes mostramos la pantalla inicial de Kali9. Procedemos a abrir el navegador y hacer pruebas de conexión a internet

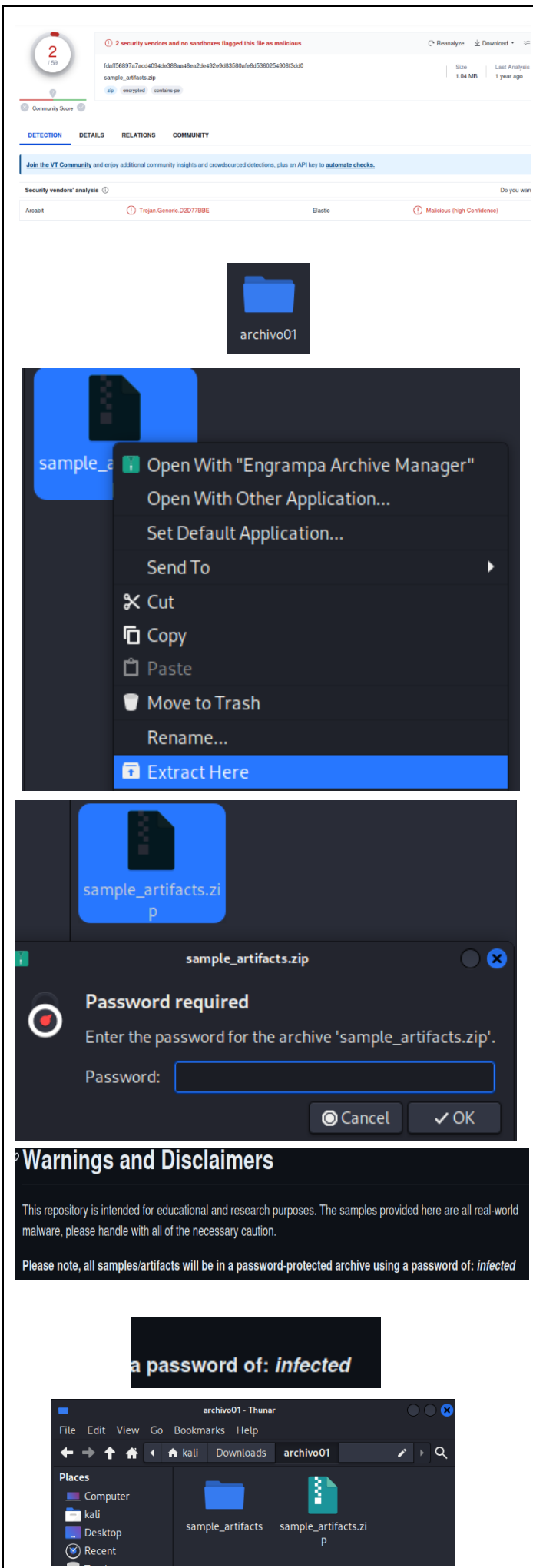
10. Esto se puede realizar desde la terminal realizando un **ping 8.8.8.8**

11. Con esta verificación de la conexión a internet por la maquina finalizamos la preparación del ambiente de trabajo

NOTA: se realiza el trabajo en una maquina virtual por ser un entorno controlado y no corremos el riesgo de infectar las maquina host anfitrión con malware en el momento de la auditoria

PROCESO DE DESCARGA DE ARCHIVOS PARA LA AUDITORIA

- Una vez realizado el proceso de comprobación de conexión a la red
- Procedemos a abrir el navegador
- Ingresamos al siguiente repositorio de GIT HUB
(<https://github.com/jstrosch/malware-samples>)
- En este repositorio se encuentran ejemplos de malware
- Nos dirigimos a la opción que nos dice
- SUMMARY OF SAMPLES**
- Procedemos a realizar la búsqueda de los archivos
- En la imagen podemos ver un archivo encontrado ese realizaremos la descarga
- Damos clic y nos redirecciona a la raíz del repositorio
- Podemos ver sus archivos pero el que nos interesa
- Es el que tiene extensión .zip
- Ingresamos a esa carpeta y nos redirecciona a la pagina donde podemos realizar la descarga
- Damos clic a la opción descargar
- Podemos apreciar que procede a realizar la descarga



15. Ingresamos de igual manera a la herramienta virtual llamada **VIRUSTOTAL** para ver el tipo de malware encontrado por su antivirus

16. En la imagen podemos apreciar que la herramienta nos indica que se encontró alertas de malware

DOCUMENTO 01

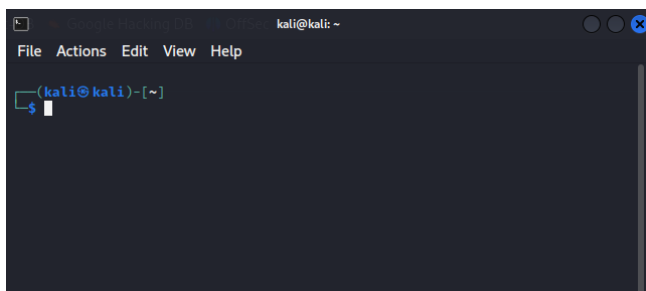
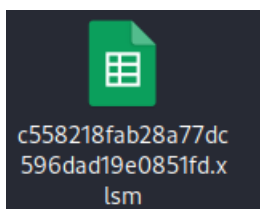
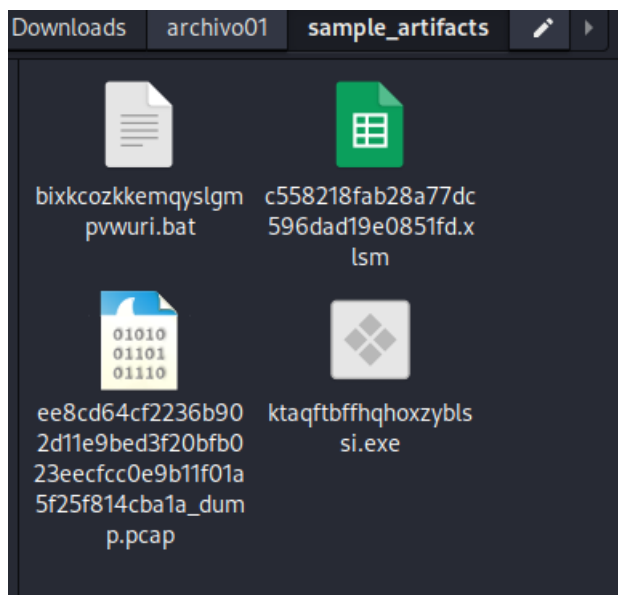
PROCESO DE AUDITORIO DEL ARCHIVO DESCARGADO

1. Ingresamos al archivo donde realizamos la descarga
2. Podemos ver el archivo descargado damos clic derecho
3. Damos a la opción de **EXTRACT HERE**
4. Esto es para realizar la descompresión del archivo .zip

5. Para el mismo nos pide ingresar una contraseña
6. Donde podemos encontrar la contraseña se encuentra en el mismo repositorio

7. En este sector podemos ver la contraseña

8. La contraseña es : **infected**



```
(kali@kali)-[~]
$ sudo pip3 install quicksand
Collecting quicksand
  Downloading quicksand-2.0.13-py3-none-any.whl (34 kB)
Collecting pdfreader
  Downloading pdfreader-0.1.12.tar.gz (2.9 MB)
    2.9/2.9 MB 4.1 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting oletools
  Downloading oletools-0.60.1-py2.py3-none-any.whl (977 kB)
    977.2/977.2 kB 5.1 MB/s eta 0:00:00
Requirement already satisfied: cryptography in /usr/lib/python3/dist-packages
(from quicksand) (38.0.4)
Collecting zipfile38
  Downloading zipfile38-0.0.3.tar.gz (22 kB)
  Preparing metadata (setup.py) ... done
Collecting msocryptcrypto-tool
  Downloading msocryptcrypto-tool-5.0.1-py3-none-any.whl (34 kB)
Requirement already satisfied: olefile in /usr/lib/python3/dist-packages (from
quicksand) (0.46)
Requirement already satisfied: yara-python in /usr/lib/python3/dist-packages
(from quicksand) (4.2.0)
Collecting pyparsing<3, >=2.1.0
  Downloading pyparsing-2.4.7-py2.py3-none-any.whl (67 kB)
    67.8/67.8 kB 16.0 MB/s eta 0:00:00
```

```
(kali@kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
archivo01 archivo02 archivo03 archivo04
(kali@kali)-[~/Downloads]
$ cd archivo01
(kali@kali)-[~/Downloads/archivo01]
$ ls
sample_artifacts sample_artifacts.zip
(kali@kali)-[~/Downloads/archivo01]
$ cd sample_artifacts
(kali@kali)-[~/Downloads/archivo01/sample_artifacts]
$ ls
bixkcozkkemqyslgm pwwuri.bat
c558218fab28a77dc 596dad19e0851fd.x lsm
ee8cd64cf2236b90 2d11e9bed3f20bfb0 23eecfcc0e9b11f01a 5f25f814cba1a_dump.pcap
ktaqftbfffhoxzybls si.exe
```

9. Podemos ver como se realiza la extracción de los documentos s

10. Ingresamos a la carpeta y podemos ver los archivos encontrados

11. De todos los archivos el que mas nos interesa es el archivo Excel .xlsm

12. Visto en la imagen

13. Una vez realiza la extracción de los archivos

14. Abrimos la terminal de la herramienta

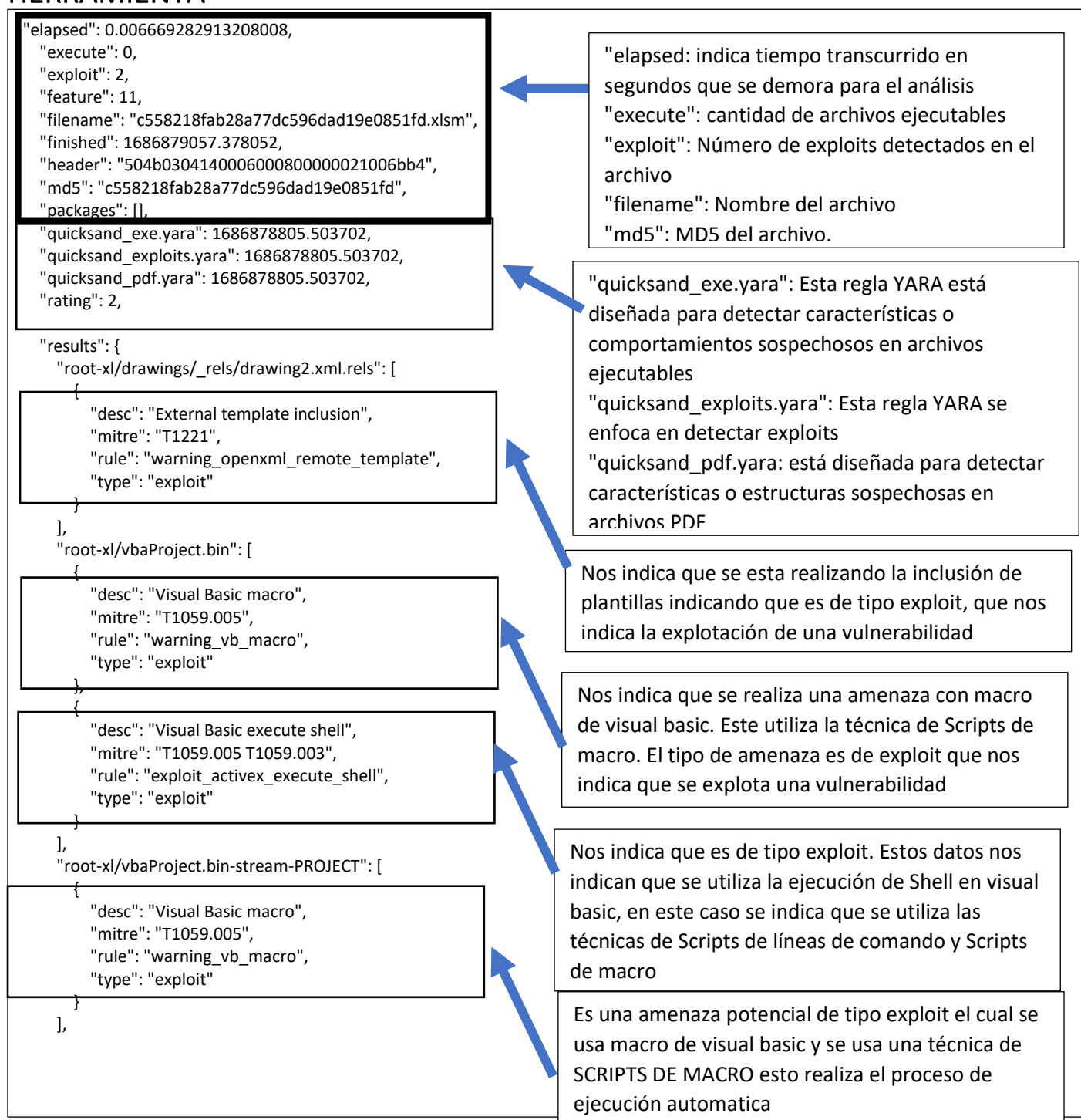
15. Procedemos a instalar la herramienta **quicksand**
Para el proceso de instalación se debe realizar La ejecución del comando
Sudo pip3 install quicksand

16. Ingresamos a la carpeta donde se encuentra los archivos

```
(kali@kali)-[~/Downloads/archivo01/sample_artifacts]
$ quicksand c558218fab28a77dc596dad19e0851fd.xlsm
{
  "elapsed": 0.007746458053588867,
  "execute": 0,
  "exploit": 2,
  "feature": 11,
  "filename": "c558218fab28a77dc596dad19e0851fd.xlsm",
  "finished": 1686878921.1254756,
  "header": "504b0304140006000800000021006bb4",
  "md5": "c558218fab28a77dc596dad19e0851fd",
  "packages": [],
  "quicksand_exe.yara": 1686878805.503702,
  "quicksand_exploits.yara": 1686878805.503702,
  "quicksand_pdf.yara": 1686878805.503702,
  "rating": 2,
  "results": {
    "root-xl/drawings/_rels/drawing2.xml.rels": [
      {
        "desc": "External template inclusion",
        "mitre": "T1221",
        "rule": "warning_openxml_remote_template",
        "type": "exploit"
      }
    ],
    "root-xl/vbaProject.bin": [
      {
        "desc": "Visual Basic macro",
        "mitre": "T1059.005",
        "rule": "warning_vb_macro",
        "type": "exploit"
      },
      {
        "desc": "Visual Basic execute shell",
        "mitre": "T1059.005 T1059.003",
        "rule": "exploit_activex_execute_shell",
        "type": "exploit"
      }
    ],
    "root-xl/vbaProject.bin-stream-PROJECT": [
      {
        "desc": "Visual Basic macro",
        "mitre": "T1059.005",
        "rule": "warning_vb_macro",
        "type": "exploit"
      }
    ]
  }
}
```

17. Esto se realiza mediante comandos en la terminal
18. Una vez ingresado en la carpeta donde se encuentra el documento **.xlsm**
19. Procedemos con la extracción de datos mediante la herramienta
20. Damos inicio a la herramienta con el siguiente comando
Quicksand "nombre del archivo". "la extensión del archivo"

ANÁLISIS DE LOS RESULTADOS EXTRAÍDOS DEL DOCUMENTO JUNTO A LA HERRAMIENTA



```

"root-xl/vbaProject.bin-stream-VBA-Learn more": [
  {
    "desc": "Visual Basic macro",
    "mitre": "T1059.005",
    "rule": "warning_vb_macro",
    "type": "exploit"
  }
],
"root-xl/vbaProject.bin-stream-VBA-Start": [
  {
    "desc": "Visual Basic macro",
    "mitre": "T1059.005",
    "rule": "warning_vb_macro",
    "type": "exploit"
  }
],
"root-xl/worksheets/_rels/sheet2.xml.rels": [
  {
    "desc": "External template inclusion",
    "mitre": "T1221",
    "rule": "warning_openxml_remote_template",
    "type": "exploit"
  }
]
},
"risk": "risk of exploit",
"score": 37,
"sha1": "f9fb21d7ca217bd86b833b416629681c9bd8934b",
"sha256": "8d15fadf25887c2c974e521914bb7cba762a8f03b17a2bc8198e9fb94d45a5",
"sha512": "7d737a4a46a5fda63bc1b11f891f6f0288a9b03569ad92136c4566b427df679db4c45fc",
"size": 75009,
"started": 1686879057.3713827,
"structhash": "a3bc1dfb774be969869ec3781555960c",
"structhash_elements": 48,
"structhash_version": "1.0.3",
"structure": "openxml:root,mso:root-[Content_Types].xml,mso:root-_rels/.rels,mso:root-xl/_rels/workbook.xml.rels,mso:root-xl/workbook.xml,mso:root-xl/worksheets/sheet1.xml,mso:root-xl/worksheets/sheet2.xml,mso:root-xl/worksheets/sheet3.xml,mso:root-xl/theme/theme1.xml,mso:root-xl/styles.xml,mso:root-xl/sharedStrings.xml,mso:root-xl/drawings/drawing1.xml,data:root-xl/media/image1.png,mso:root-xl/drawings/drawing2.xml,data:root-xl/media/image2.PNG,data:root-xl/media/image3.png,mso:root-xl/media/image4.png,data:root-xl/media/image5.png,mso:root-xl/media/image6.svg,ole:root-xl/vbaProject.bin,stream-PROJECT,stream-PROJECTwm,stream-VBA-Learn more,stream-VBA-Start,stream-VBA-ThisWorkbook,stream-VBA-Workbook,stream-VBA-_VBA_PROJECT,stream-VBA-__SRP_0,stream-VBA-__SRP_1,stream-VBA-__SRP_2,stream-VBA-__SRP_3,stream-VBA-dir,mso:root-xl/worksheets/_rels/sheet1.xml.rels,mso:root-xl/worksheets/_rels/sheet2.xml.rels,mso:root-xl/drawings/_rels/drawing1.xml.rels,mso:root-xl/drawings/_rels/drawing2.xml.rels,mso:root-customXml/item1.xml,mso:root-customXml/item3.xml,mso:root-customXml/itemProps3.xml,mso:root-docProps/core.xml,mso:root-docProps/app.xml,mso:root-docProps/custom.xml,mso:root-customXml/itemProps1.xml,mso:root-customXml/itemProps2.xml,mso:root-customXml/_rels/item1.xml.rels,mso:root-customXml/_rels/item2.xml.rels,mso:root-customXml/_rels/item3.xml.rels,mso:root-customXml/item2.xml",
"struzzy": "HiEglijkcOnFEGNGkIxbKeaDDLDDFEFGHdeqsENNvCDOPQr",
"type": "openxml",
"version": "2.0.12",
"warning": 11

```

Nos indica de igual manera que se utiliza macros en visual basic y el numero de técnica nos indica que es de **SCRIPTS DE MACRO** el cual es encargado de realizar acciones de manera automática y el tipo de amenaza es exploit

Esta amenaza nos indica que existe una extracción de plantillas y la inclusión de las mismas el punto XML nos indica que se puede realizar la inclusión de plantillas remotas

Nos indica que existe una potencial manera de explotación de vulnerabilidades

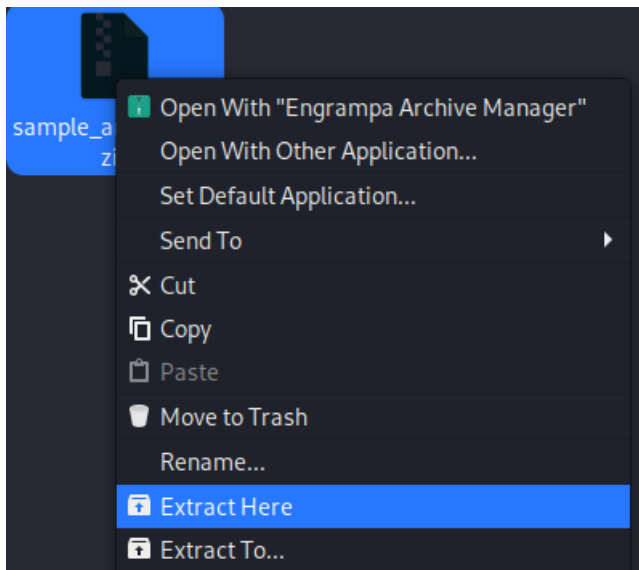
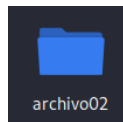
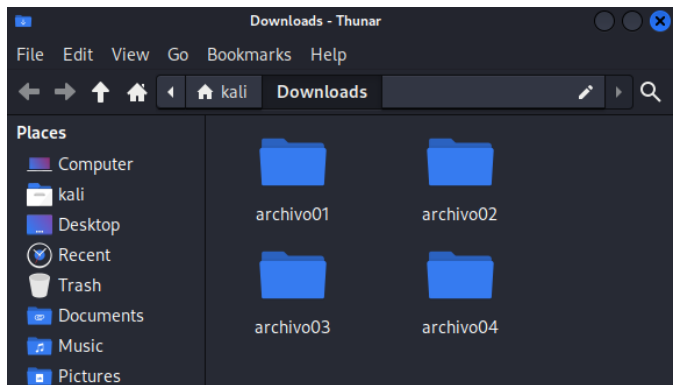
Y el numero de 37 indica el valor de la vulnerabilidad calificada

DOCUMENTO 2 (.DOC)

<div data-bbox="108 226 753 479"><p>-> Training PCAPs</p><h3>Summary of Samples</h3><ul style="list-style-type: none">2023-02-17: YouTube Video: OneNote Malware Trends - Investigating Script Execution that Leads to QuakBot2023-02-07: YouTube Video: A .NET Downloader and an Open Directory - Unraveling the Encrypted Payload That Leads to CryptBot2023-02-04: YouTube Video Series: Investigating NullMixer - Identifying Packing Techniques, Identifying and Unraveling ASPack, and Investigating Network Traffic with Suricata and Evebox2023-01-23: YouTube Video: OneNote Malware - Tips and Tricks for Investigating OneNote Malware Used to Deliver AsyncRAT2023-01-12: YouTube Video: Suricata Getting Started with Detect-It-Easy</div> <div data-bbox="108 499 782 566"><ul style="list-style-type: none">2021-11-13: Word Document uses Packager Shell Object to Execute VBScript, Run Powershell to Download AgentTesla</div> <div data-bbox="108 589 782 790"><p><> Code Pull requests Discussions Actions Security Insights</p><p>master malware-samples / maldocs / agenttesla / 2021 / November / Go to file</p><p>Josh Stroschein adds word doc that downloads agenttesla on Nov 25, 2021 History</p><p>... </p><p>README.md adds word doc that downloads agenttesla 2 years ago</p><p>sample_artifacts.zip adds word doc that downloads agenttesla 2 years ago</p></div> <div data-bbox="108 806 774 862"><p>sample_artifacts.zip adds word doc that downloads agenttesla</p></div> <div data-bbox="108 873 774 1124"><p>jstrosch / malware-samples Public Notifications Fork 201 Star 1.2k</p><p><> Code Pull requests Discussions Actions Security Insights</p><p>master malware-samples / maldocs / agenttesla / 2021 / November / sample_artifacts.zip Go to file ...</p><p>Josh Stroschein adds word doc that downloads agenttesla Latest commit 291f1f9 on Nov 25, 2021 History</p><p>0 contributors</p><p>2.53 MB Download</p></div> <div data-bbox="300 1142 525 1256"><p>Download</p></div> <div data-bbox="188 1272 668 1379"><p>sample_artifacts(1).zip Completed — 2.5 MB</p></div> <div data-bbox="108 1391 753 1886"><p>VIRUSTOTAL</p><p>FILE URL SEARCH</p><p>Choose file</p><p>2 / 57</p><p>2 security vendors and no sandboxes flagged this file as malicious</p><p>72980c770a4b53db49704f4452707b473a6d1c811290231462647a56a</p><p>Size 2.53 MB Last Analysis Date 11 months ago ZIP</p><p>Community Score</p><p>DETECTION DETAILS RELATIONS COMMUNITY</p><p>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</p><p>Security vendors' analysis</p><p>Do you want to automate checks?</p><p>Elastic Malicious (High Confidence) NAVIO Antivirus Exploit-Kit-Heuristic-rl-danbp</p></div>	<h2>PROCESO DE DESCARGA DEL ARCHIVO</h2> <ol style="list-style-type: none">Nos dirigimos a la opción que nos diceSUMMARY OF SAMPLESProcedemos a realizar la búsqueda de los archivosEn la imagen podemos ver un archivo encontrado ese realizaremos la descargaDamos clic y nos redirecciona a la raíz del repositorioPodemos ver sus archivos, pero el que nos interesaEs el que tiene extensión .zipIngresamos a esa carpeta y nos redirecciona a la pagina donde podemos realizar la descargaDamos clic a la opción descargarPodemos apreciar que procede a realizar la descargaIngresamos de igual manera a la herramienta virtual llamada VIRUSTOTAL para ver el tipo de malware encontrado por su antivirusEn la imagen podemos apreciar que la herramienta nos indica que se encontró alertas de malware
---	--

PROCESO DE AUDITORIA DEL ARCHIVO DESCARGADO

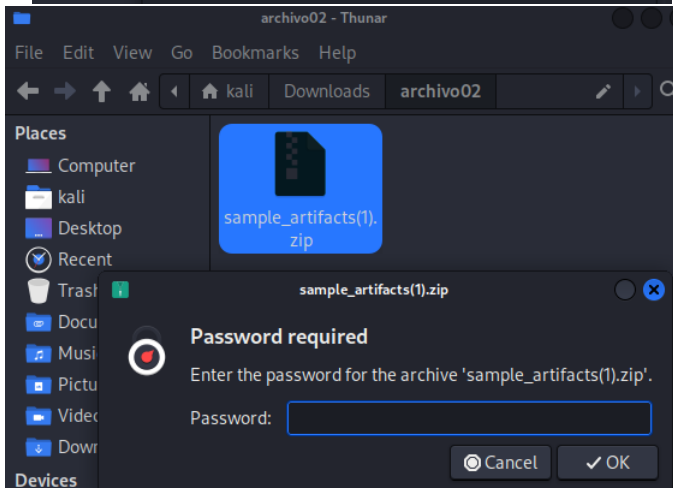
13. Ingresamos al archivo donde realizamos la descarga



14. Podemos ver el archivo descargado damos clic derecho

15. Damos a la opción de **EXTRACT HERE**

16. Esto es para realizar la descompresión del archivo .zip



17. Para el mismo nos pide ingresar una contraseña

18. Donde podemos encontrar la contraseña se encuentra en el mismo repositorio

Warnings and Disclaimers

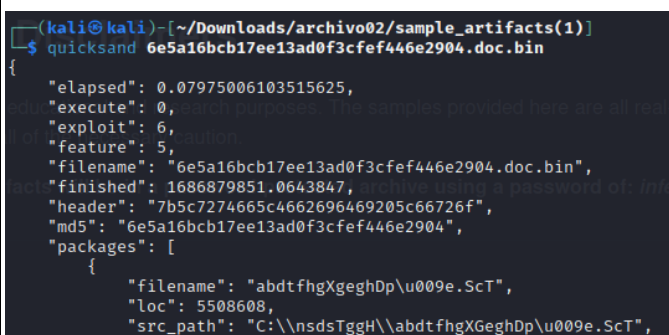
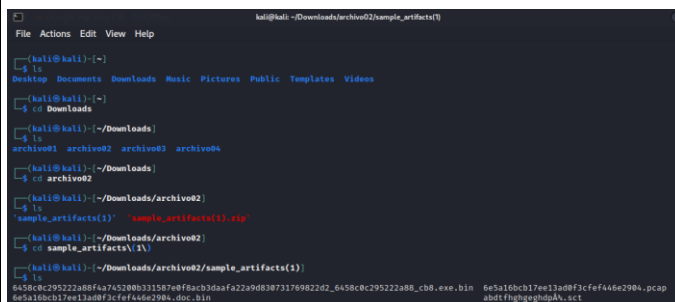
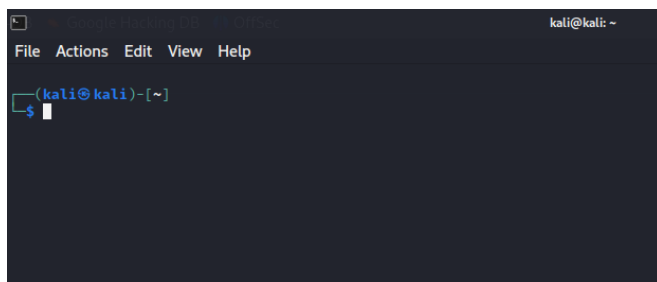
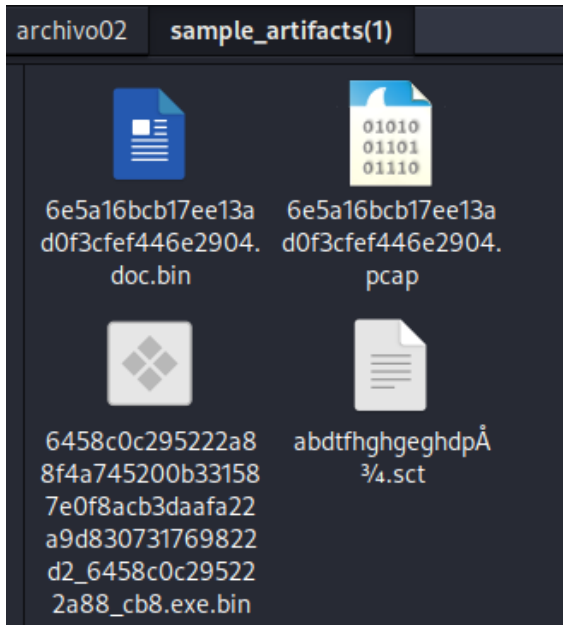
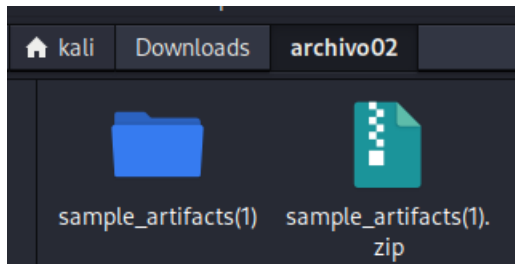
This repository is intended for educational and research purposes. The samples provided here are all real-world malware, please handle with all of the necessary caution.

Please note, all samples/artifacts will be in a password-protected archive using a password of: *infected*

19. En este sector podemos ver la contraseña

a password of: *infected*

20. La contraseña es : **infected**



21. Podemos ver como se realiza la extracción de los documentos.

22. Ingresamos a la carpeta y podemos ver los archivos encontrados

23. De todos los archivos el que mas nos interesa es el archivo Excel **.doc**

24. Visto en la imagen

25. Una ves realiza la extracción de los archivos

26. Abrimos la terminal de la herramienta

27. Procedemos a instalar la herramienta **quicksand**

28. Ingresamos a la carpeta donde se encuentra los archivos

29. Esto se realiza mediante comandos en la terminal

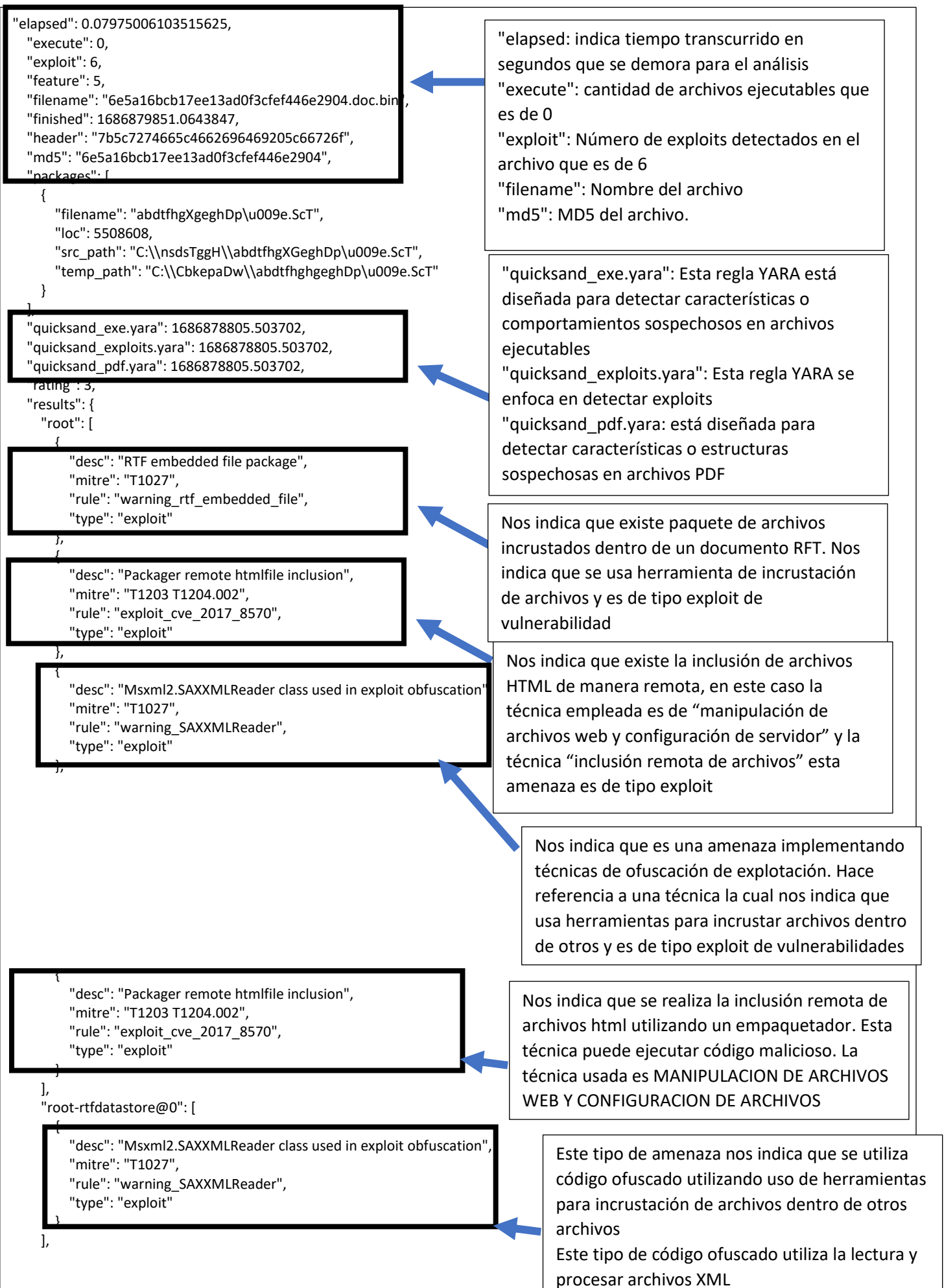
30. Una ves ingresado en la carpeta donde se encuentra el documento **.doc**

31. Procedemos con la extracción de datos mediante la herramienta

32. Damos inicio a la herramienta con el siguiente comando

Quicksand “nombre del archivo”. “la extensión del archivo”

ANÁLISIS DE LOS RESULTADOS EXTRAÍDOS DEL DOCUMENTO JUNTO A LA HERRAMIENTA



```
{
  "desc": "update RTF object may load malicious content",
  "mitre": "T1027",
  "rule": "warning_rtf_objupdate",
  "type": "exploit"
},
"root-rtfcls@5708647_00000300-0000-0000-C000-000000000046": [
  {
    "desc": "Office OLE2Link unsafe content such as remote risky content",
    "mitre": "T1027 T1204.002",
    "rule": "warning_ole2link_embedded",
    "type": "exploit"
  },
  {
    "risk": "high risk of exploit",
    "score": 46,
    "sha1": "be860a6fc0a27f2fb775ec6bf73b32c8551ac1b5",
    "sha256": "b615de9997243c8fbef6fbc8f9e3890c22faa2adc6b3b849540ecff25b7d806a",
    "sha512": "6569308878a01edc508340e007bc78040c8a16c5fafcd2515f39afe2eb91185335c97f54086098832afa3636d9772bfeac2df233cbe04465cfa79a547220f5e",
    "size": 5896558,
    "started": 1686879850.9846346,
    "strcthash": "e3e4528f5d9dad416cf396cb6120c2a4",
    "strcthash_elements": 12,
    "strcthash_version": "1.0.3",
    "structure": "rtf:root,rtfdatastore@0,ole0,hexobj,abdtfhgXgeghDp\u0009e.ScT,rtfpkg@5508608,hexobj,rtfobjole@5708647,ole:root-rtfobjole@5708647,stream-\u0001OLE,stream-\u0003LinkInfo,stream-\u0003ObjInfo",
    "struzzy": "kheqXUqaRsMB",
    "type": "rtf",
    "version": "2.0.12",
    "warning": 5
  }
]
```

PROCESO DE DESCARGA DEL ARCHIVO

- Nos dirigimos a la opción que nos dice
- SUMMARY OF SAMPLES**
- Procedemos a realizar la búsqueda de los archivos
- En la imagen podemos ver un archivo encontrado ese realizaremos la descarga
- Damos clic y nos redirecciona a la raíz del repositorio
- Podemos ver sus archivos pero el que nos interesa
- Es el que tiene extensión .zip
- Ingresamos a esa carpeta y nos redirecciona a la pagina donde podemos realizar la descarga
- Damos clic a la opción descargar
- Podemos apreciar que procede a realizar la descarga
- Ingresamos de igual manera a la herramienta virtual llamada **VIRUSTOTAL** para ver el tipo de malware encontrado por su antivirus
- En la imagen podemos apreciar que la herramienta nos indica que se encontró alertas de malware

→ Training PCAPs

Summary of Samples

- 2023-02-17: YouTube Video: OneNote Malware Trends - Investigating Script Execution that Leads to QuakBot
- 2023-02-07: YouTube Video: A .NET Downloader and an Open Directory - Unraveling the Encrypted Payload That Leads to CryptBot
- 2023-02-04: YouTube Video Series: Investigating NullMixer - Identifying Packing Techniques, Identifying and Unraveling ASPack, and Investigating Network Traffic with Suricata and Evebox
- 2023-01-23: YouTube Video: OneNote Malware - Tips and Tricks for Investigating OneNote Malware Used to Deliver AsyncRAT
- 2023-01-12: YouTube Video: Seven-Gaming Started with Detect-It-Easy
- 2021-04-20: Word Document Uses Template Injection that downloads an RTF Document, Exploits CVE-2017-11882 to Drop Nanocore

jsroch / malware-samples (Public)

Code Pull requests Discussions Actions Security Insights

master malware-samples / maldocs / nanocore / 2021 / April /

Go to file

Josh Strochein adds maldoc that uses template injection to download RTF, exploit CVE... on Apr 21, 2021 History

..

README.md adds maldoc that uses template injection to download RTF, exploit CVE... 2 years ago

artifacts.zip adds maldoc that uses template injection to download RTF, exploit CVE... 2 years ago

artifacts.zip adds maldoc t

https://github.com/jsroch/malware-samples/blob/master/maldocs/nanocore/2021/April/artifacts.zip

Sign up

jsroch / malware-samples (Public)

Code Pull requests Discussions Actions Security Insights

master malware-samples / maldocs / nanocore / 2021 / April / artifacts.zip

Go to file ...

Josh Strochein adds maldoc that uses template injection to download ... Latest commit fa2339e on Apr 21, 2021 History

0 contributors

2.25 MB Download

View raw

(Sorry about that, but we can't show files that are this big right now.)

Download

artifacts.zip Completed — 2.3 MB

VIRUSTOTAL

Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

Choose file

2 / 5

2 security vendors and no sandboxes flagged this file as malicious

01a6b5774d99787173a5eac8ba079a2a32544d06a73303016a3981ca7962 artifacts.zip

Size: 2.25 MB Last Analysis Date: 11 months ago ZIP

DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

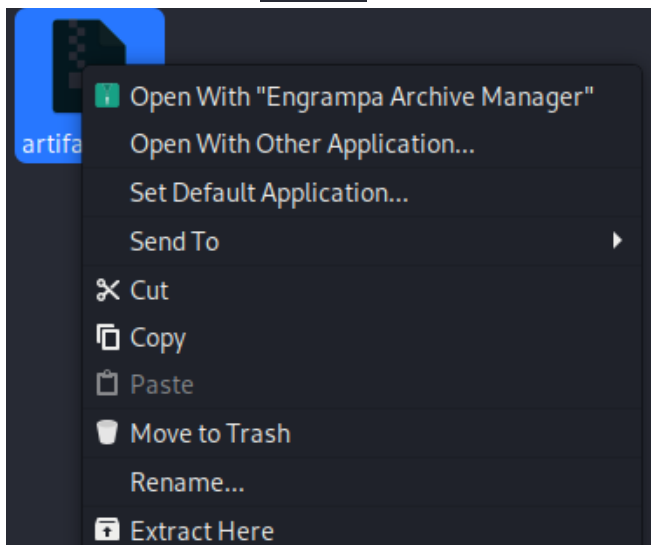
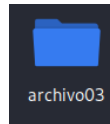
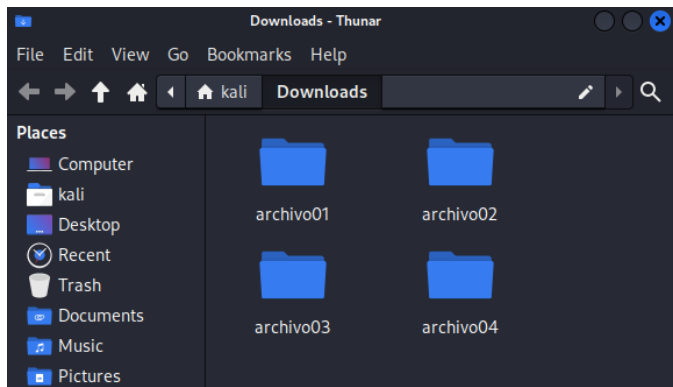
Security vendors' analysis

Do you want to automate checks?

Elastic Malicious (High Confidence) NANO-Antivirus Exploit.FBI.Herzliot-RT-010p

PROCESO DE AUDITORÍA DEL ARCHIVO DESCARGADO

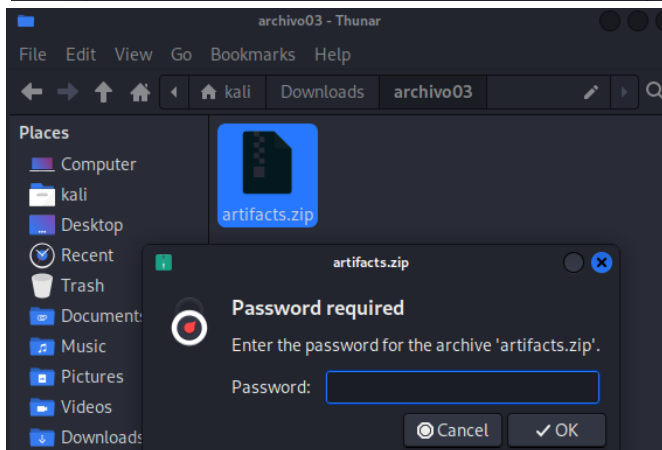
13. Ingresamos al archivo donde realizamos la descarga



14. Podemos ver el archivo descargado damos clic derecho

15. Damos a la opción de **EXTRACT HERE**

16. Esto es para realizar la descompresión del archivo .zip



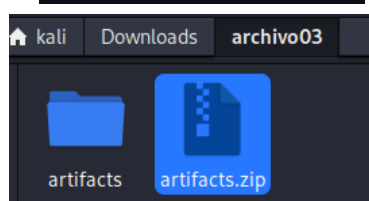
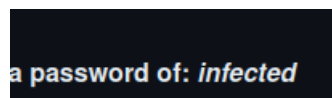
17. Para el mismo nos pide ingresar una contraseña

18. Donde podemos encontrar la contraseña se encuentra en el mismo repositorio

Warnings and Disclaimers

This repository is intended for educational and research purposes. The samples provided here are all real-world malware, please handle with all of the necessary caution.

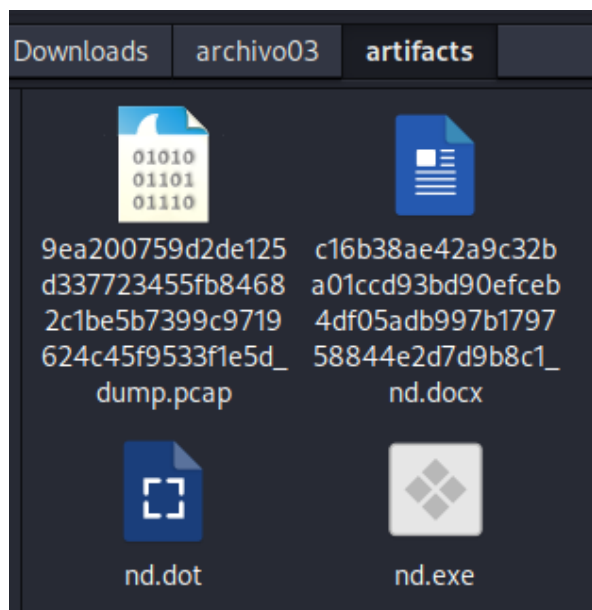
Please note, all samples/artifacts will be in a password-protected archive using a password of: *infected*



19. En este sector podemos ver la contraseña

20. La contraseña es : **infected**

21. Podemos ver como se realiza la extracción de los documentos



```
(kali@kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
archivo01 archivo02 archivo03 archivo04
(kali@kali)-[~/Downloads]
$ cd archivo03
(kali@kali)-[~/Downloads/archivo03]
$ ls
artifacts artifacts.zip
(kali@kali)-[~/Downloads/archivo03]
$ cd artifacts
(kali@kali)-[~/Downloads/archivo03/artifacts]
$ ls
9ea200759d2de125d337723455fb84682c1be5b7399c9719624c45f9533f1e5d_dump.pcap nd.dot
c16b38ae42a9c32ba01ccd93bd90efceb4df05adb997b179758844e2d7d9b8c1_nd.docx nd.exe

(kali@kali)-[~/Downloads/archivo03/artifacts]
$ quicksand c16b38ae42a9c32ba01ccd93bd90efceb4df05adb997b179758844e2d7d9b8c1_nd.docx
{
  "elapsed": 0.001924753189086914,
  "execute": 0,
  "exploit": 0,
  "feature": 1,
  "filename": "c16b38ae42a9c32ba01ccd93bd90efceb4df05adb997b179758844e2d7d9b8c1_nd.docx",
  "finished": 1686880491.4508915,
  "header": "504b03041400060008000002100ddfc",
  "md5": "0fa0fc8e801d4228a50ec62e2f4d7396",
  "packages": [],
  "quicksand_exe.yara": 1686878805.503702,
  "quicksand_exploits.yara": 1686878805.503702,
  "quicksand_payload.yara": 1686878805.503702
}
```

22. Ingresamos a la carpeta y podemos ver los archivos encontrados
23. De todos los archivos el que mas nos interesa es el archivo Excel **.docx**

24. Visto en la imagen

25. Una vez realiza la extracción de los archivos
26. Abrimos la terminal de la herramienta

27. Procedemos a instalar la herramienta **quicksand**
28. Ingresamos a la carpeta donde se encuentra los archivos
29. Esto se realiza mediante comandos en la terminal
30. Una vez ingresado en la carpeta donde se encuentra el documento **.docx**
31. Procedemos con la extracción de datos mediante la herramienta
32. Damos inicio a la herramienta con el siguiente comando

Quicksand "nombre del archivo". "la extensión del archivo"

ANÁLISIS DE LOS RESULTADOS EXTRAÍDOS DEL DOCUMENTO JUNTO A LA HERRAMIENTA

```
"elapsed": 0.001924753189086914,
"execute": 0,
"exploit": 0,
"feature": 1,
"filename": "c16b38ae42a9c32ba01ccd93bd90efceb4df05adb997b179758844e2d7d9b8c1_nd.docx",
"finished": 1686880491.4508915,
"header": "504b03041400060008000002100ddfc",
"md5": "0fa0fc8e801d4228a50ec62e2f4d7396",
"packages": [],
"quicksand_exe.yara": 1686878805.503702,
"quicksand_exploits.yara": 1686878805.503702,
"quicksand_pdf.yara": 1686878805.503702,
"rating": 2,
"results": {
  "root-word/_rels/webSettings.xml.rels": [
    {
      "desc": "External template inclusion",
      "mitre": "T1221",
      "rule": "warning_openxml_remote_template",
      "type": "exploit"
    }
  ]
},
"risk": "high risk active content",
"score": 5,
"sha1": "f263339ab10d01dc983cedbb82fa84e9bf5baf79",
"sha256": "c16b38ae42a9c32ba01ccd93bd90efceb4df05adb997b179758844e2d7d9b8c1",
"sha512": "0c26839e4a8e37499b33354290da31b4647f997fc1e45774ba9d69cb765f710f5db3ada184f1bd20e30cf6782850a4550e701ecef06aacdf3bd19ec40b4b019",
"size": 10329,
"started": 1686880491.4489667,
"structhash": "1e19960a96a584925dfe48b02d1a089d",
"structhash_elements": 13,
"structhash_version": "1.0.3",
"structure": "openxml:root,mso:root-[Content_Types].xml,mso:root-_rels/.rels,mso:root-word/_rels/document.xml.rels,mso:root-word/document.xml,mso:root-word/theme/theme1.xml,mso:root-word/settings.xml,mso:root-word/fontTable.xml,mso:root-word/_rels/webSettings.xml.rels,mso:root-docProps/app.xml,mso:root-word/styles.xml,mso:root-docProps/core.xml,mso:root-word/webSettings.xml",
"struzzy": "HiEZBkTNRNWnt",
"type": "openxml",
"version": "2.0.12",
"warning": 1
```

"quicksand_exe.yara": Esta regla YARA está diseñada para detectar características o comportamientos sospechosos en archivos ejecutables

"quicksand_exploits.yara": Esta regla YARA se enfoca en detectar exploits

"quicksand_pdf.yara": está diseñada para detectar características o estructuras sospechosas en archivos PDF

Nos indica que se realiza una inclusión externa de plantillas usando la técnica de "uso de plantillas para incrustar contenido o código" en este caso se realiza la inyección de malware