

SOC146 - Phishing Mail Detected - Excel 4.0 Macros



Contenido


Descripción.....	3
Detalles de la alerta	3
Análisis	3
Correo electrónico entrante:.....	4
Análisis de registros de dominio.....	5
Análisis del contenido	7
Iroto1.dll.....	8
Iroto.dll	9
Research-1646684671.xls	9
Respuesta	13
Conclusiones	13

Descripción

El 13 de junio de 2021, a las 14:13, se recibió una alerta sobre un email de phishing que contenía un archivo de Excel sospechoso con macros maliciosas. Las posibles consecuencias de abrir este archivo incluyen la ejecución de código malicioso que puede comprometer la seguridad del sistema, el robo de información personal o confidencial, y la propagación de malware a otros dispositivos de la red.

Contexto: Las macros en Excel pueden ser utilizadas para automatizar tareas, pero también pueden ser aprovechadas por atacantes para ejecutar código malicioso sin el conocimiento del usuario. La identificación y el análisis de estas amenazas son cruciales para mantener la seguridad de la red y los datos corporativos.

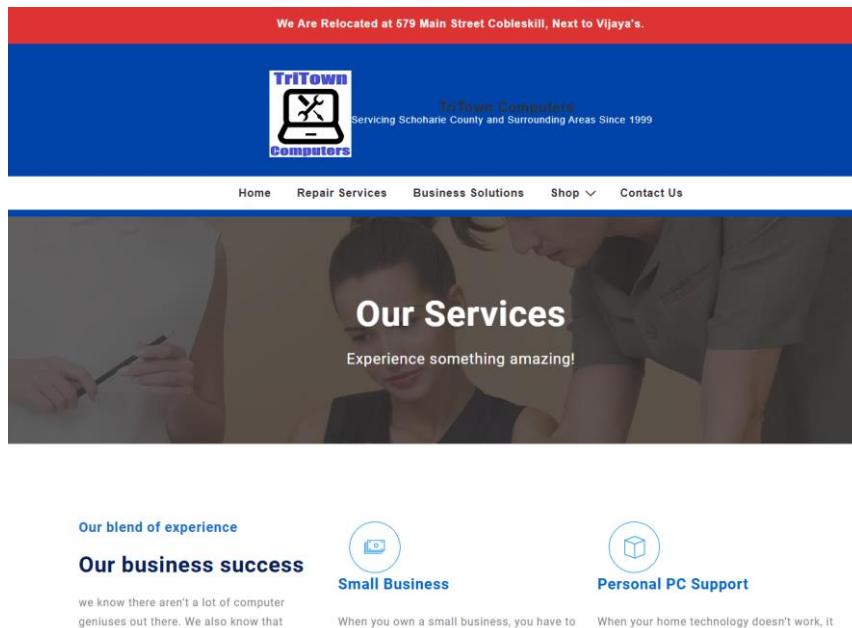
Detalles de la alerta

SEVERITY	DATE	RULE NAME	EVENTID	TYPE
High	Jun, 13, 2021, 02:13 PM	★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros	93	Exchange
This alert has been re-investigated				
★ This alert was generated from a real phishing attack.				
EventID :		93		
Event Time :		Jun, 13, 2021, 02:13 PM		
Rule :		SOC146 - Phishing Mail Detected - Excel 4.0 Macros		
Level :		Security Analyst		
SMTP Address :		24.213.228.54		
Source Address :		trenton@tritowncomputers.com		
Destination Address :		lars@letsdefend.io		
E-mail Subject :		RE: Meeting Notes		
Device Action :		Allowed		
Show Hint 				

- **ID de evento:** 93
- **Tiempo del evento:** 13 de junio de 2021, 14:13
- **Type:** Exchange
- **Subtype:** Phishing (Malicious Attachment)
- **Regla:** SOC146 - Correo de phishing detectado - Macros de Excel 4.0
- **Dirección SMTP:** 24.213.228.54
- **Dirección de la fuente:** trenton@tritowncomputers.com
- **Dirección de destino:** lars@letsdefend.io
- **Asunto del correo electrónico:** RE: Notas de la reunión.
- **Acción del dispositivo:** Permitido.

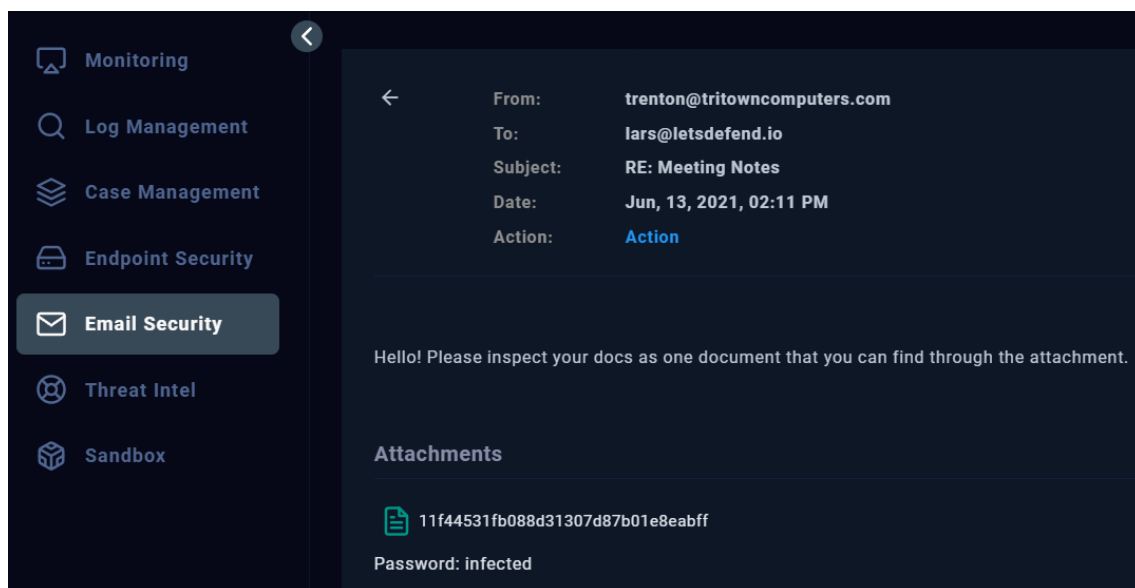
Análisis

Antes de comenzar el análisis, debemos tener un contexto del dominio involucrado por lo que haremos una búsqueda en internet. [TriTown Computers](#)



Nos encontramos frente a empresa que brinda servicios y venta de computadoras en Estados Unidos, Nueva York. Esto lo hacemos para poder identificar si tanto el asunto como cuerpo y adjuntos tienen relación con el remitente.

Correo electrónico entrante:



¿Cuándo fue enviado? **Jun, 13, 2021, 02:11 PM.**

¿Cuál es la dirección SMTP del correo electrónico? **24.213.228.54.**

¿Cuál es la dirección del remitente? **trenton@tritowncomputers.com.**

¿Cuál es la dirección del destinatario? **lars@letsdefend.io.**

¿El contenido del correo es sospechoso? **El nombre del archivo adjunto es sospechoso, el cuerpo del mensaje parece genérico, no tiene firma.**

Análisis de registros de dominio

Utilizando las herramientas de: [Network Tools: DNS,IP,Email \(mxtoolbox.com\)](https://mxtoolbox.com)

Lo primero que realicé fue verificar si el dominio tiene un registro **SPF** (Sender Policy Framework) que indique qué servidores de correo están autorizados a enviar correo en nombre de ese dominio.

spf:tritowncomputers.com				Find Problems	Solve Email Delivery Problems	spf
	Test	Result				
✖	SPF Record Published	No SPF Record found		More Info		

En este caso vemos que no tiene registros SPF lo que ya nos estaría dando un indicio que nos encontramos frente a una posible suplantación de identidad por parte de un atacante hacia la empresa.

Lo próximo es buscar los registros **MX**.

mx:tritowncomputers.com				Find Problems	Solve Email Delivery Problems	mx
Pref	Hostname	IP Address	TTL			
0	mail.tritowncomputers.com	108.179.232.57 Network Solutions, LLC (AS19871)	4 hrs	Blacklist Check	SMTP Test	
	Test	Result				
✖	DMARC Record Published	No DMARC Record found		More Info		
⚠	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled		More Info		
✔	DNS Record Published	DNS Record found				

```
(kali㉿kali)-[~]
$ nslookup -type=MX tritowncomputers.com

Server:          186.130.128.250
Address:         186.130.128.250#53

Non-authoritative answer:
tritowncomputers.com mail exchanger = 0 mail.tritowncomputers.com.

Authoritative answers can be found from:

(kali㉿kali)-[~]
$ nslookup mail.tritowncomputers.com
Server:          186.130.128.250
Address:         186.130.128.250#53

Non-authoritative answer:
Name:   mail.tritowncomputers.com
Address: 108.179.232.57
```

Probamos conexión con la dirección obtenida (108[.]179[.]232[.]57) - Esto se suele hacer cuando los registros MX nos devuelven muchos servidores y debemos saber cuál opera.

smtp.mail.tntowncomputers.com

Monitor This

Solve Email Delivery Problems

SMTP

220-gator4243.hostgator.com ESMTP Exim 4.96.2 #2 Mon, 29 Jul 2024 19:41:13 -0500
220-We do not authorize the use of this system to transport unsolicited,
220-and/or bulk e-mail.

Test	Result
SMTP Reverse DNS Match	Reverse DNS does not contain the hostname
SMTP Connection Time	5.316 seconds - Warning on Connection time
SMTP Transaction Time	11.089 seconds - Not good on Transaction Time
SMTP Valid Hostname	OK - Reverse DNS is a valid Hostname
SMTP Banner Check	OK - Reverse DNS matches SMTP Banner
SMTP TLS	OK - Supports TLS
SMTP Open Relay	OK - Not an open relay

Session Transcript

Connecting to 108.179.232.57

220-gator4243.hostgator.com ESMTP Exim 4.96.2 #2 Mon, 29 Jul 2024 19:41:13 -0500
220-We do not authorize the use of this system to transport unsolicited,
220-and/or bulk e-mail. (5.316 ms)
EHLO keeper-us-east-1d.metroline.com
220-gator4243.hostgator.com Hello keeper-us-east-1d.metroline.com
(11.089.56.113)
250-PIPELINING
250-8BITMIME
250-STARTTLS
250-PIPECONNECT
250-STARTS PLAIN LOGIN
250-STARTTLS
250 HELP (114 ms)
MAIL FROM: keeper-us-east-1d.metroline.com
250 OK (113 ms)
RCPT TO: user@metrolinecamping.com
250-Please run an SMTP authentication in your mail client, or login to the
250-IMAP/POP3 server before sending your message.
250-keeper-us-east-1d.metroline.com (108.179.232.57) 27432 (a not permitted to
250-relay through this server without authentication. 11037 ms)
LookingServer: 11028ms

Site Setup

Feedback

Help text

Transcript

Reported by metroline.com on 7/29/2024 at 7:41:09 PM. Just for you.

Análisis del contenido

Descomprimos el archivo adjunto en el correo electrónico recibido.

```
(kali㉿kali)-[~/Downloads]
$ ls
11f44531fb088d31307d87b01e8eabff.zip

(kali㉿kali)-[~/Downloads]
$ 7z x 11f44531fb088d31307d87b01e8eabff.zip

7-Zip 24.07 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-06-19
64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 109381 bytes (107 KiB)

Extracting archive: 11f44531fb088d31307d87b01e8eabff.zip
--
Path = 11f44531fb088d31307d87b01e8eabff.zip
Type = zip
Physical Size = 109381

Enter password (will not be echoed):
Everything is Ok

Folders: 1
Files: 3
Size:      1554006
Compressed: 109381

(kali㉿kali)-[~/Downloads]
$ ls
11f44531fb088d31307d87b01e8eabff  11f44531fb088d31307d87b01e8eabff.zip

(kali㉿kali)-[~/Downloads]
$ cd 11f44531fb088d31307d87b01e8eabff

(kali㉿kali)-[~/Downloads/11f44531fb088d31307d87b01e8eabff]
$ ls
iroto1.dll  iroto.dll  research-1646684671.xls
```

Obtenemos los hashes de los archivos.

```
(kali㉿kali)-[~/Downloads/11f44531fb088d31307d87b01e8eabff]
$ sha256sum iroto1.dll
e05c717b43f7e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b  iroto1.dll

(kali㉿kali)-[~/Downloads/11f44531fb088d31307d87b01e8eabff]
$ sha256sum iroto.dll
055b9e9af987aec9ba7adb0eef947f39b516a213d663cc52a71c7f0af146a946  iroto.dll

(kali㉿kali)-[~/Downloads/11f44531fb088d31307d87b01e8eabff]
$ sha256sum research-1646684671.xls
1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820  research-1646684671.xls
```

Analizamos los hashes con herramientas como **virustotal**

Iroto1.dll

12
/ 74

Community Score

12/74 security vendors flagged this file as malicious

e05c717b437e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b

iroto1.dll

Size
434.52 KB

Last Analysis Date
2 months ago

Reanalyze Similar More

pedll detect-debug-environment overlay checks-user-input

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY12+

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

Contacted IP addresses (1)

IP	Detections	Autonomous System	Country
204.79.197.203	0 / 93	8068	US

Execution Parents (4)

Scanned	Detections	Type	Name
2024-07-22	9 / 68	ZIP	11f44531fb088d31307d87b01e8eabff.zip
2024-02-28	36 / 62	ZIP	11f44531fb088d31307d87b01e8eabff.zip
2023-04-30	36 / 63	ZIP	11f44531fb088d31307d87b01e8eabff 2.zip
2024-01-20	35 / 62	ZIP	11f44531fb088d31307d87b01e8eabff (extract.me).zip

Resultado malicioso con relación a un .zip con el mismo nombre que anteriormente descomprimimos y conectado a la siguiente IP 204.[.] 79.[.]197.[.]203

AbuseIPDB » 204.79.197.203

Check an IP Address, Domain Name, or Subnet
e.g. 190.175.75.66, microsoft.com, or 5.188.10.0/24

192.229.2

204.79.197.203 was found in our database!

This IP was reported 74 times. Confidence of Abuse is 23%: ?

23%

ISP

Microsoft Corporation

Usage Type

Data Center/Web Hosting/Transit

Hostname(s)

a-0003.a-msedge.net

Domain Name

microsoft.com

Country

United States of America

City

Redmond, Washington

IP info including ISP, Usage Type, and Location provided by IP2Location.
Updated monthly.

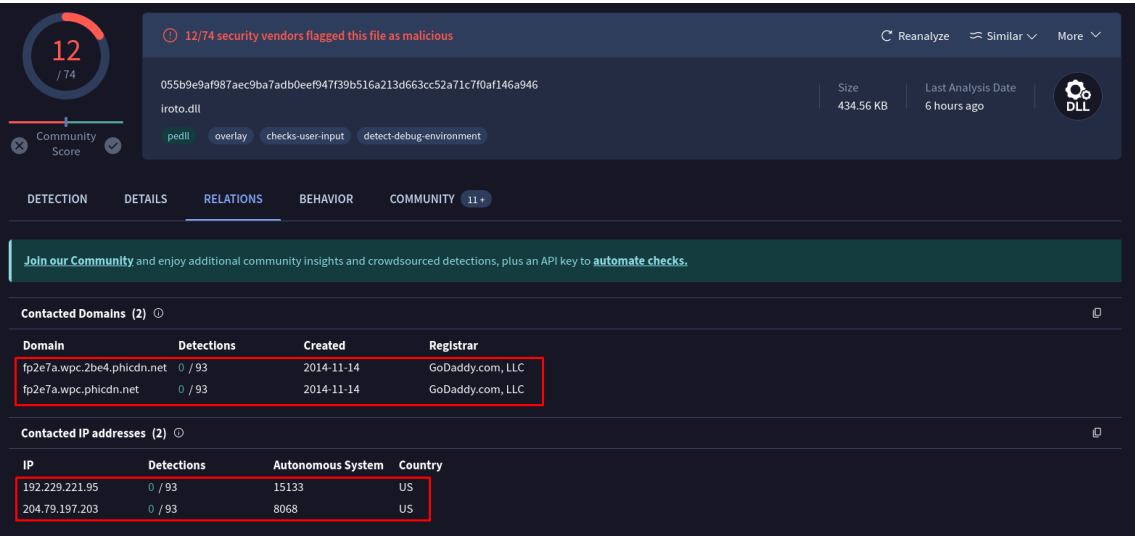
REPORT 204.79.197.203

WHOIS 204.79.197.203

Rodríguez, Facundo Iván

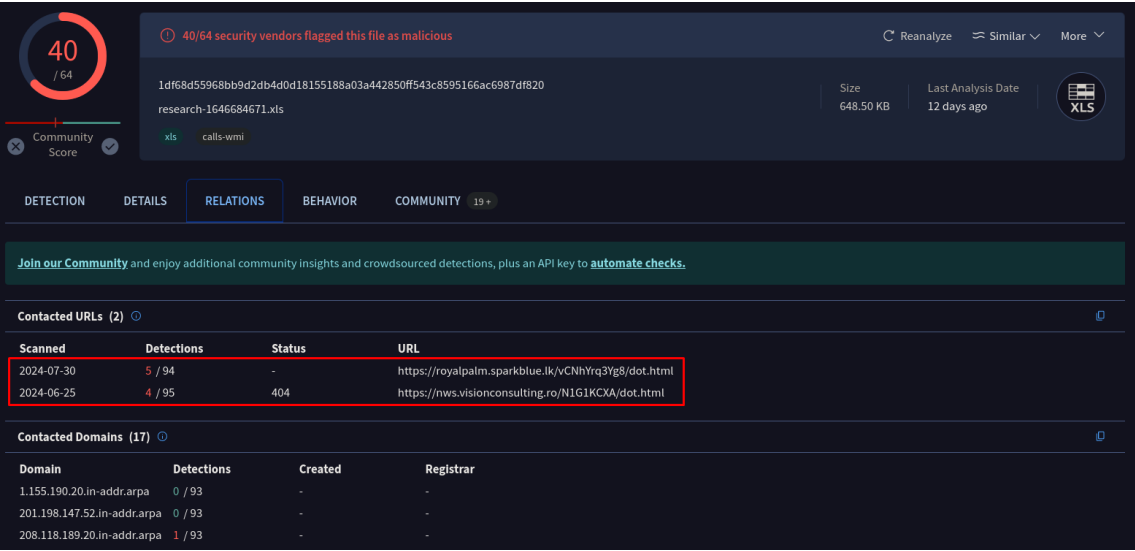
8

Iroto.dll



Resultado malicioso con relación a un .zip con el mismo nombre que anteriormente descomprimimos, conectado a las siguientes IPs 204[.] 79[.]197[.]203 - 192[.]229[.]221[.]95 y los siguientes dominios fp2e7a.wpc.phicdn.net - fp2e7a.wpc.2be4.phicdn.net.

Research-1646684671.xls



Resultado malicioso con relación los siguientes dominios hxxps://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html - hxxps://nws.visionconsulting.ro/N1G1KCXA/dot.html

Se emplea la utilización de 2 herramientas para el análisis del archivo .xls.

- Quicksand
- Olevba

Quicksand:

```
(kali@kali)~[~/Downloads/11f44531fb088d31307d87b01e8eabff]
$ sudo quicksand research-1646684671
{
  "elapsed": 0.05229830741882324,
  "execute": 0,
  "exploit": 0,
  "feature": 2,
  "filename": "research-1646684671",
  "finished": 1722471334.4478724,
  "header": "d0cf11e0a1b11ae10000000000000000",
  "md5": "b775cd8be83696ca37b2fe00bcb40574",
  "ole_author": "",
  "ole_company": "",
  "ole_create_time": "2015-06-05 18:17:20",
  "ole_last_saved_by": "Amanda",
  "ole_last_saved_time": "2021-06-13 09:24:55",
  "packages": [],
  "quicksand_exe.yara": 1722466625.175004,
  "quicksand_exploits.yara": 1722466625.175004,
  "quicksand_pdf.yara": 1722466625.175004,
  "rating": 1,
  "results": {
    "root": [
      {
        "desc": "Excel 4.0 macro",
        "mitre": "T1059.005",
        "rule": "warning_excel_macro",
        "type": "exploit"
      }
    ],
    "root-stream-\u0005DocumentSummaryInformation": [
      {
        "desc": "Excel 4.0 macro",
        "mitre": "T1059.005",
        "rule": "warning_excel_macro",
        "type": "exploit"
      }
    ]
  },
  "risk": "risky active content",
  "score": 2,
  "sha1": "60c8a9fdf2b24f8fb4913d4745a8557df5ff8e07",
  "sha256": "1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820",
  "sha512": "5ad4da8582bec3cc545e322cad2e356f59c4bfa5fe4ca90c0e781dd0e63a7aefbcc27b4045583232e4fdccffbc2bceb832b8d8e9ec3c070cf4b6559ca3c99a72",
  "size": 664064,
  "started": 1722471334.395574,
  "structhash": "a6352d901a438b8e3d076eddbed70553",
  "structhash_elements": 4,
  "structhash_version": "1.0.3",
  "structure": "ole:root,stream-\u0005DocumentSummaryInformation,stream-\u0005SummaryInformation,stream-Book",
  "struzy": "vjka",
  "type": "ole",
  "version": "2.0.12",
  "warning": 2
}
```

Como resultado se detectan 2 ejecuciones de macros que podríamos relacionarlo con los .dll analizados anteriormente.

Olevba:

```
' RAW EXCEL4/XLM MACRO FORMULAS:
' SHEET: Doc2, Macrosheet
' CELL:B041      , =LEFT("LdecvsbgvrsxLxrgxg",1.0), L
' CELL:BH68      , None
' CELL:BH79      , None
' CELL:B056      , None
' CELL:BK37      , None
' CELL:BG29      , None
' CELL:BI80      , None
' CELL:BQ41      , None
' CELL:BI33      , None
' CELL:BK67      , None
' CELL:BR33      , None
' CELL:BR44      , None
' CELL:BN36      , None
' CELL:BH71      , None
' CELL:B037      , None
' CELL:B048      , None
' CELL:BK29      , None
' CELL:BL30      , None
' CELL:BI74      , None
' CELL:BN55      , None
' CELL:BJ75      , None
' CELL:BQ52      , None
' CELL:BM33      , None
' CELL:B067      , None
' CELL:BI25      , None
' CELL:BI36      , None
' CELL:BR36      , None
' CELL:BG68      , None
```

CELL:B036	, None	, nws.visionconsulting.ro/N1G1KCXA/dot.html
CELL:BG37	, None	, eg
CELL:BH78	, None	, LM
CELL:BL29	, None	, LM
CELL:BR51	, None	,
CELL:BN43	, None	,
CELL:BQ40	, None	,
CELL:BM32	, None	,
CELL:B055	, None	,
CELL:BI24	, None	, ..\irotto.dll
CELL:BG67	, None	,
CELL:BA18	, FullEvaluation	, FORMULA(Doc2B036:B036,Doc3AY13:AY13)
CELL:BA19	, FullEvaluation	, FORMULA("UDoc3AY16:AY16Doc2BL32:BL32Doc2BJ31:BJ31Doc2BL31:BL31Doc2BL34:BL34Doc2BJ32:BJ32eA",Doc3AY11:AY11)
CELL:BA20	, FullEvaluation	, FORMULA(Doc2B041:B041,Doc3AY17:AY17)
CELL:BA21	, FullEvaluation	, FORMULA(Doc2B037:B037,Doc3AY14:AY14)
CELL:BA25	, FullEvaluation	, FORMULA("Doc2BM28:BM28Doc2BM29:BM29Doc2BM30:BM30B",Doc3AY11:AY12)
CELL:BA26	, FullEvaluation	, BG16()
CELL:BG17	, PartialEvaluation	, =WORKBOOK.HIDE("Doc2",1)
CELL:BG18	, PartialEvaluation	, =WORKBOOK.HIDE("Doc3",1)
CELL:BG19	, PartialEvaluation	, =WORKBOOK.HIDE("Doc4",1)

Type	Keyword	Description
Suspicious	EXEC	May run an executable file or a system command using Excel 4 Macros (XLM/XLF)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	irotto1.dll	Executable file name
IOC	irotto.dll	Executable file name
Hex String	tRcHg!1	74526348672131
Suspicious	XLM macro	XLM macro found. It may contain malicious code

Podemos ver la ubicación donde se encuentran urls analizadas anteriormente y los .dll, además de los IOC y contenido sospechoso detectado por la herramienta.

Lo próximo a realizar es analizar si se logró una conexión a un servidor de command and control (C2) para esto vamos a tomar las 2 urls que encontramos al analizar el .xls

hxxps://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html -
hxxps://nws.visionconsulting.ro/N1G1KCXA/dot.html

Ambas al analizarlas son detectadas como maliciosas categorizadas como malware, por lo que podríamos confirmar de posibles servidores C2. Veremos si la víctima tuvo conexión con los mismos.

Utilizando el endpoint que nos brinda la página de Lestdefend buscamos al usuario "Lars" y nos aparece un usuario llamado "LarsPRD" por lo que accedemos a él y copiamos su dirección IP (172.16.17.57).

La misma la buscamos en los logs para ver eventos.

Source Address contains "172.16.17.57"

All Time

Q

2 events (before Jun, 13, 2021, 11:20 AM)

< 1 >

> Show Fields

Event

Jun, 13, 2021, 02:20 PM

source_address=172.16.17.57 source_port=43633 destination_address=188.213.19.81 destination_port=443 raw_log: {Request URL: 'https://nws.visioncons...

Jun, 13, 2021, 02:20 PM

source_address=172.16.17.57 source_port=45235 destination_address=192.232.219.67 destination_port=443 raw_log: {Request URL: 'https://royalpalm.spa...

Event

source_port

43633

destination_address

188.213.19.81

destination_port

443

time

Jun, 13, 2021, 02:20 PM

Raw Log

Request URL

https://nws.visionconsulting.ro/N1G1KCXA/dot.html

Request Method

GET

Device Action

Allowed

Process

excel.exe

Parent Process

explorer.exe

Parent Process MD5

8b88ebbb05a0e56b7dcc708498c02b3e

Event

source_port

45235

destination_address

192.232.219.67

destination_port

443

time

Jun, 13, 2021, 02:20 PM

Raw Log

Request URL

https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html

Request Method

GET

Device Action

Allowed

Process

excel.exe

Parent Process

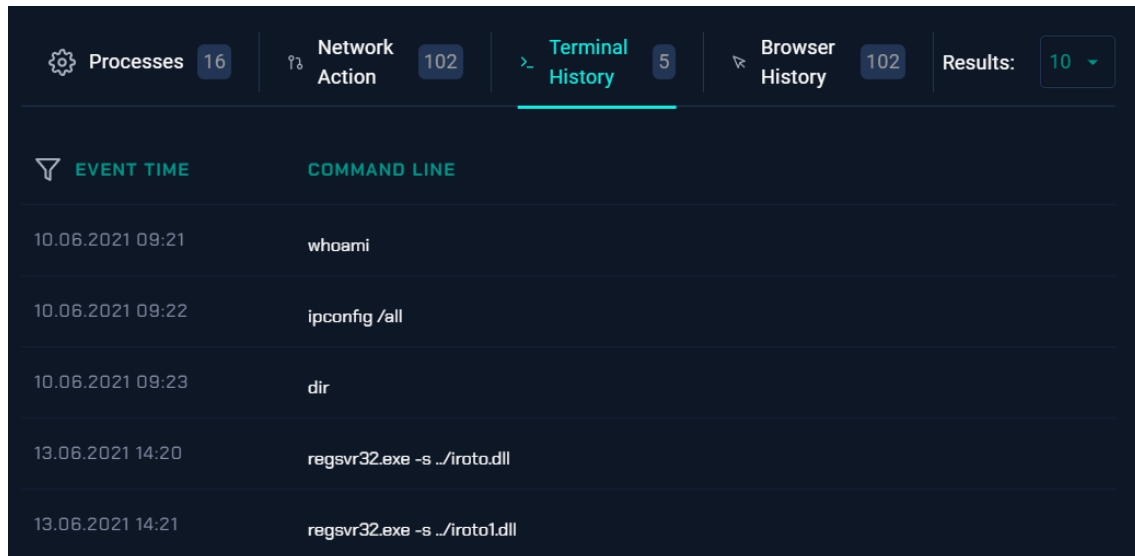
explorer.exe

Parent Process MD5

8b88ebbb05a0e56b7dcc708498c02b3e

Al ver que se tuvo comunicación con estas IPs verificamos en el Endpoint Security la lista de comandos ejecutados.

Encontramos que se ejecutó el comando regsvr32 (es una herramienta de la línea de comandos del sistema operativo Microsoft Windows que sirve para registrar y quitar bibliotecas de enlace dinámico (DLL) y controles ActiveX del registro de Windows).



EVENT TIME	COMMAND LINE
10.06.2021 09:21	whoami
10.06.2021 09:22	ipconfig /all
10.06.2021 09:23	dir
13.06.2021 14:20	regsvr32.exe -s ./iroto.dll
13.06.2021 14:21	regsvr32.exe -s ./iroto1.dll

Respuesta

1. Aislar la máquina afectada para evitar movimiento lateral.
2. Se recomienda plan de capacitación de concienciación sobre phishing para los usuarios.
3. Eliminación del correo recibido de la casilla del usuario involucrado.

Conclusiones

Se determinó que el correo electrónico recibido efectivamente era phishing con un adjunto que contenía macros maliciosas, que el usuario ejecuta tal archivo lo que conlleva a la ejecución 2 URLs C2. Cuando se examina el historial de CMD de LarsPRD, se observa que se ejecuta el comando regsvr32, que se incluye en las macros de Excel (lo que permitiría la ejecución de los 2 .dll maliciosos encontrados). Las acciones tomadas incluyeron la eliminación del correo, el aislamiento de la máquina.

Recomendaciones:

- Mejorar las políticas de seguridad de correo electrónico.
- Implementar autenticación multifactor (MFA).
- Realizar simulacros de phishing periódicamente.
- Monitorear constantemente los sistemas en busca de comportamientos sospechosos.