Proyecto Final
Primera entrega

Detalles:

Para la elaboración del presente informe, han sido analizadas las siguientes fuentes de información:

- Informe de estatus de situación actual
- Muestra de malware entregado por el equipo de soporte técnico de Corporación LexCorp

Análisis de Malware

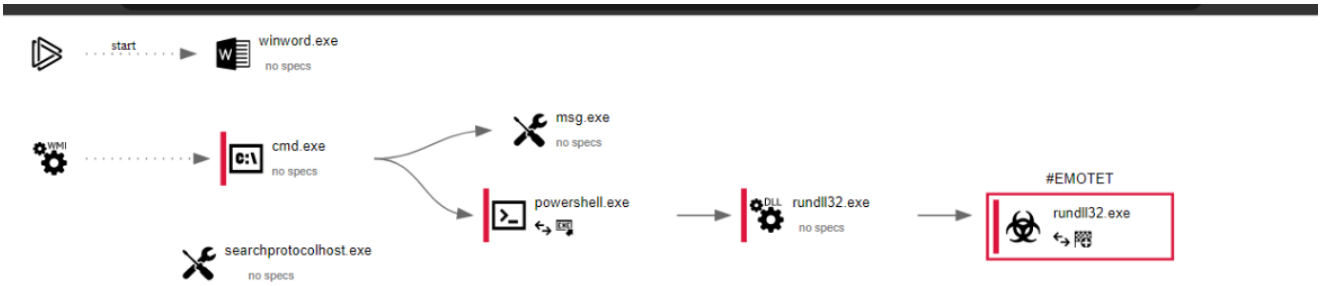
Emotet es un 'malware' que se distribuye a través de archivos adjuntos en correos electrónicos y tiene por objetivo obtener los contactos del usuario para propagarse y realizar fraude bancario mediante credenciales.

Este es un tipo de virus conocido.

Muestra analizada con Any.run

Nombre de la muestra	1word.doc
Fecha del análisis	01/03/2023, 06:24:26
OS utilizado para análisis	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
MD5	349d13ca99ab03869548d75b99e5a1d0

Comportamiento



Información Estática encontrada

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

File info: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: white Groves Face to face Credit Card Account Investment Account West Virginia pixel Buckinghamshire, Author: Jeanne Perrin, Template: Normal.dotm, Last Saved By: Benjamin Philippe, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Mon Jan 4 18:59:00 2021, Last Saved Time/Date: Mon Jan 4 18:59:00 2021, Number of Pages: 1, Number of Words: 2435, Number of Characters: 13886, Security: 8

MD5:

5CC5E8213D3BBB6A1AA3319DC6917E46

SHA1:

CDA98DDBBC5CEC76D432E5E417C7CA8F7BD88B67

SHA256:

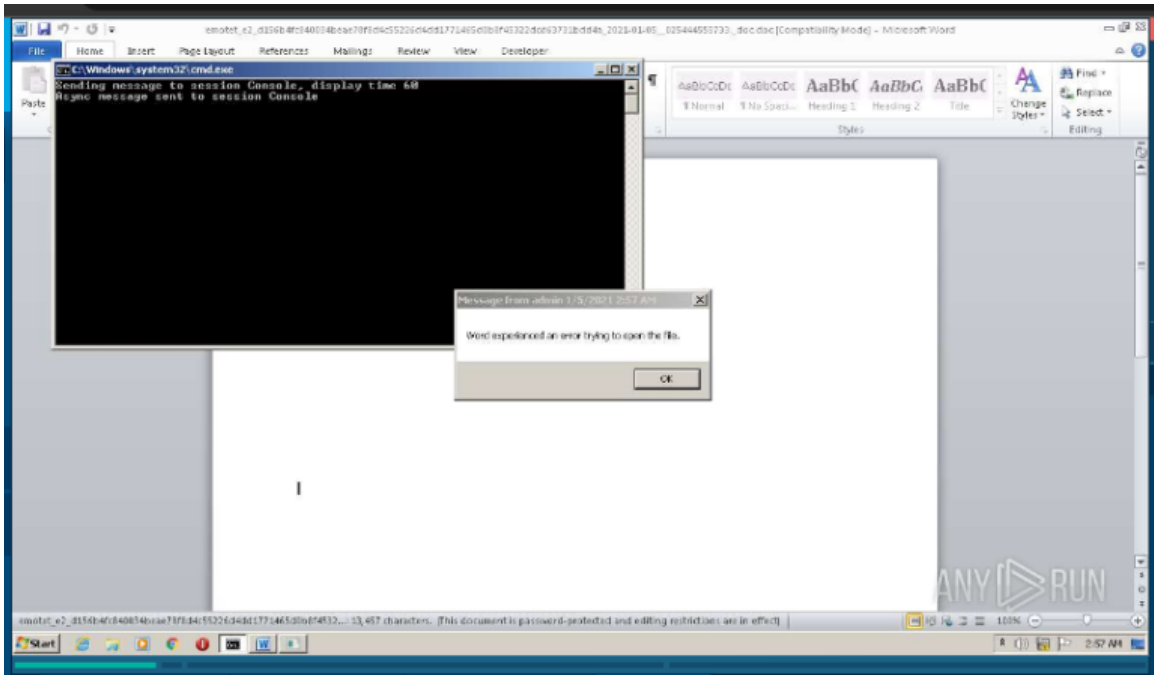
D156B4FC840034BEAE78F8D4C55226D4DD1771465D0B8F45322DCD63731BDD4A

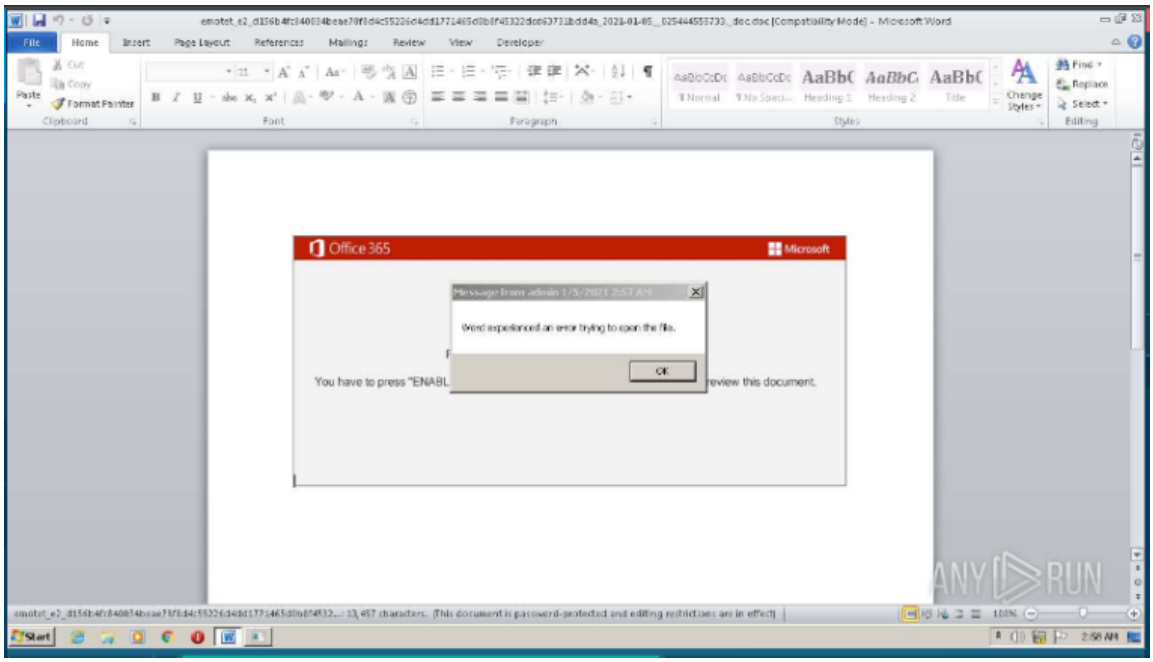
SSDEEP:

3072:XYgB99ufstRUUKSns8T0OJSHUgteMJ8qMD7g2R5:ogB99ufsfgIf0pL2L

1.0.0.0

Screenshot de la simulación





Eventos asociados

PID	Process	Filename	Type
2472	**WINWORD.EXE**	**C:\Users\admin\AppData\Local\Temp\CVR99D.tmp**	**—**
		MD5:— **SHA256:—**	

2472	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$otet_e2_d156b4fc840034beae78f8d4c55226d4dd1771465d0b8f45322dcd63731bdd4a_2021-01-05__025444555733._doc.doc	
		MD5:41F198BC634D35DB73595098C6CE8D6E	SHA256:E1A3D739B4698412857F8A761488D447668BDC49A6BA6C2A82711A43EE85AB31
2472	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
		MD5:CB902F751BC5C3AABBD2084FA54153CA	SHA256:A1D1E46D18126A4C74A25E419474F0C0DC75F00944B4AFC0749C3C394DE6C2E2
1392	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms	
		MD5:3EEC306A4042DDE8A76D075A9281AF0D	SHA256:1AC0444CA13F67716A12A7A7F78AA5E4FA7F3D62B2B7C991E416F463C1011D78
1392	powershell.exe	C:\Users\admin\Gh4952x\Ouda02n\E75Y.dll	
		MD5:F55D67388EF01E345A5CAD89A3FAA953	SHA256:17D200F8540FC9707EA405E6C15BD4A06D21F02928611FF976B981A7DDBCB58A
1392	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\I9YONBLXXWWA6W5I67GQ.temp	
		MD5:3EEC306A4042DDE8A76D075A9281AF0D	SHA256:1AC0444CA13F67716A12A7A7F78AA5E4FA7F3D62B2B7C991E416F463C1011D78

HTTP Request

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1392	powershell.exe	GET	200	103.237.147.16:80	http://etbnaman.com/wp-admin/V0Sv/	VN		190 Kb	
2564	rundll32.exe	POST	200	90.160.138.175:80	http://90.160.138.175/a3ek89s/vESqjs6qd0y85/			3.77 Kb	

DNS requests

Domain	IP	Reputation
etbnaman.com	**103.237.147.16**	

Amenazas

PID	Process	Class	Message
1392	powershell.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
1392	powershell.exe	A Network Trojan was detected	AV INFO Suspicious EXE download from WordPress folder
1392	powershell.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
1392	powershell.exe	Misc activity	ET INFO EXE - Served Attached HTTP
1392	powershell.exe	Misc activity	ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)
2564	rundll32.exe	A Network Trojan was detected	AV TROJAN Emotet Second Stage CnC Request

1 ETPRO signatures available at the full report

Conclusiones

Comportamiento del Malware: Evasion / Loader
Nombre general: Emotet
Tipo de malware: Troyano

Información sobre Emotet

Es un troyano que se propaga principalmente a través de correos electrónicos de spam (malspam). La infección puede llegar a través de archivos de órdenes maliciosos, archivos de documentos habilitados para macros o enlaces maliciosos. Los correos electrónicos de Emotet pueden contener imágenes de marcas conocidas diseñadas para que parezcan un correo electrónico legítimo. Emotet puede intentar persuadir a los usuarios para que hagan clic en los archivos maliciosos utilizando un lenguaje tentador sobre "Su factura", "Información de pago" o posiblemente un próximo envío de empresas de mensajería muy conocidas.

Emotet ha pasado por algunas repeticiones. Las primeras versiones llegaron como un archivo JavaScript malicioso. Las versiones posteriores evolucionaron para utilizar documentos habilitados para macros para recuperar la carga de virus de los servidores de comando y control (C&C) ejecutados por los atacantes.