Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°037	Fecha: 12-02-2024
		Página: 4 de 23

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Análisis técnico realizado a archivo ejecutable		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

Mediante correo electrónico proveniente de la DIVINDAT se informa que al realizar sus actividades lograron identificar que actores de amenazas vienen compartiendo a través de correos electrónicos un archivo adjunto que al parecer podría ser un tipo de malware. Por tal motivo y en prevención de víctimas potenciales solicitan el análisis forense y la obtención de los IoC.

2. **DETALLES:**

A. Se procede a realizar el análisis de un archivo ejecutable, con los siguientes detalles:

Datos del Archivo	
Nombre	3da8b112675a563df0c4239dc627bdf604d8b4c58616107c17ffeab5fe596ff3.exe
Nombre Original	SecuriteInfo.com.exe yotarazpug.exe
Tipo	Ejecutable
Tamaño	0.25 MB
Extensión	exe

B. Se obtuvieron los siguientes códigos hash, que permitirán generar las reglas para los sistemas de detección de amenazas o intrusos:

Hash Obtenidos	
md5	ca4c0cc996735dc70322e716af1ad5f8
sha-1	c16a3df96079a7c03cd15937788430e3ad5e7b8a
sha256	3da8b112675a563df0c4239dc627bdf604d8b4c58616107c17ffeab5fe596ff3
Vhash	025046655d6555z12z5cdz41z2025z71z87z
Authentihash	60f7e74e5986a98b64cf0d8b546b72be25754d1893373c1e9b1802426a33a9bd
Imphash	f472c59f9e1a0db2f918cd2d2bb7f320
Rich PE header hash	6f28dd1f0c5f1d88370b8464f0af23c6
SSDEEP	6144:pJ/Zh+n3dMvrqkTJTYfF6CgGDODBwrl0zXe2xuVCV:pR+3dMvrqkTJTY fF6CgGDODB5emuVC
TLSH	T18E447B11B1C0C432D6772C3306A4D6B18D7E78701DA69A9F67C90A7 ACF346D0E629B6F
File type	Win32 EXE
Compilador	PE32 Compiler: EP:Microsoft Visual C/C++ (2017 v.15.5-6) [EXE32] Compiler: Microsoft Visual C/C++ (19.36.32824) [C++] Linker: Microsoft Linker (14.36.32824) Tool: Visual Studio (2022 version 17.6)

C. Obtención de direcciones IP de conexión al comando y control:

- 192.229.211.108:80 (TCP)
- 20.42.65.92:443 (TCP)
- 20.99.133.109:443 (TCP)
- 20.99.186.246:443 (TCP)
- 23.216.147.64:443 (TCP)
- 23.216.147.74:80 (TCP)
- 23.216.147.78:80 (TCP)

D. Después de realizar diferentes pruebas con el archivo, éste fue clasificado como malicioso, el mismo que realiza diferentes acciones cuando toma el control de un equipo, como se grafica en la imagen:

Del análisis del archivo ejecutable con nombre **3da8b112675a563df0c4239dc627bdf604d8b4c58616107c17ffeab5fe596ff3.exe**, se advierte que es considerado como malicioso, en razón a que realiza conexiones TCP a una serie de direcciones IP, generando la extracción de datos de los equipos infectados.

3. RECOMENDACIÓN:

- Compartir los indicadores de compromiso a fin de evitar posibles víctimas de este malware.

Fuente de Información:	Análisis Forense Digital

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°037	Fecha: 12-02-2024
		Página: 6 de 23

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Análisis técnico realizado a archivo Java Script		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

Mediante correo electrónico proveniente de la DIVINDAT se informa que al realizar sus actividades lograron identificar que actores de amenazas vienen compartiendo a través de correos electrónicos un archivo adjunto que al parecer podría ser un tipo de malware. Por tal motivo y en prevención de víctimas potenciales solicitan el análisis forense y la obtención de los IoC.

2. **DETALLES:**

A. Se procede a realizar el análisis de un archivo ejecutable, con los siguientes detalles:

Datos del Archivo	
Nombre	14ff76924ff2f4102e06ba9f9109311e296c3d07bf5fc0cd888c93b69b545394.js
Nombre Original	INVOICE_1877_1553532450.js malicious_41570.js 14ff76924ff2f4102e06ba9f9109311e296c3d07bf5fc0cd888c93b69b545394.vbs 14ff76924ff2f4102e06ba9f9109311e296c3d07bf5fc0cd888c93b69b545394.js
Tipo	Java Script
Tamaño	5.3 MB
Extensión	js

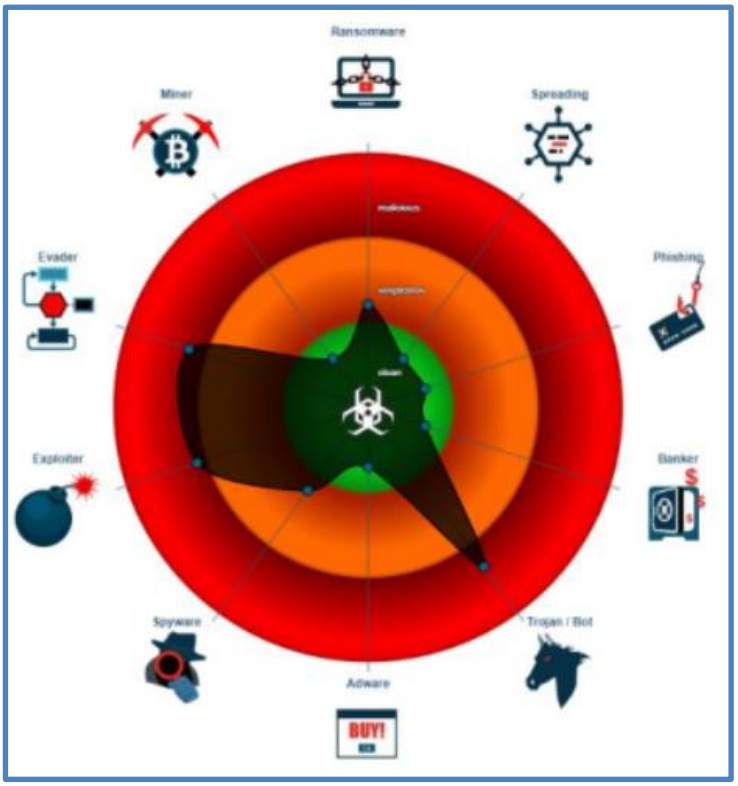
B. Se obtuvieron los siguientes códigos hash, que permitirán generar las reglas para los sistemas de detección de amenazas o intrusos:

Hash Obtenidos	
md5	34bcdbd3855b4a4354f3cd03e608440a
sha-1	6a8bf0531a981e6f567782801c5cfc0ef9f01a91
sha256	14ff76924ff2f4102e06ba9f9109311e296c3d07bf5fc0cd888c93b69b545394
Vhash	105ff404f2a6f24657f35ebbb9f292ab
SSDEEP	24576:LioNDFYpmVzSyuXqoeJxJNK2Q9bAnWdvgTABkeW+3khCxsOwy2W HM+sJE9qP4e2g:r2map+5wnVBK3UbUt
TLSH	T1E746F9E476E077D30FB5690DB7CE80B23D64B857F0EDAD86128D0D1 E928035999BBDA0
File type	JavaScript

C. Obtención de direcciones IP de conexión al comando y control:

- 193.109.85.77/server.php
- 1.1.1.1:53
- 20.101.57.9:123

D. Después de realizar diferentes pruebas con el archivo, éste fue clasificado como malicioso, el mismo que realiza diferentes acciones cuando toma el control de un equipo, como se grafica en la imagen:



Del análisis del archivo ejecutable con nombre **14ff76924ff2f4102e06ba9f9109311e296c3d07bf5fc0cd888c93b69b545394.js**, se advierte que es considerado como malicioso, en razón a que realiza conexiones a diferentes direcciones IP, posibilitando el ingreso de otros archivos, por lo que es considerado un troyano, y por el tipo de comportamiento que éste posee como: Ejecución, Persistencia, Escalada de privilegios y Evasión de defensas.

3. RECOMENDACIÓN:

- Compartir los indicadores de compromiso a fin de evitar posibles víctimas de este malware.

Fuente de Información:	Análisis Forense Digital

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Análisis técnico realizado a archivo de documento de Excel – Microsoft Office		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

Mediante correo electrónico proveniente de la DIVINDAT se informa que al realizar sus actividades lograron identificar que actores de amenazas vienen compartiendo a través de correos electrónicos un archivo adjunto que al parecer podría ser un tipo de malware. Por tal motivo y en prevención de víctimas potenciales solicitan el análisis forense y la obtención de los IoC.

2. **DETALLES:**

A. Se procede a realizar el análisis de un archivo ejecutable, con los siguientes detalles:

Datos del Archivo	
Nombre	3d8a60463219bf3008e509aed8a505043d3e76e7110d5dbe9a245a26e957330e.xls
Nombre Original	3d8a60463219bf3008e509aed8a505043d3e76e7110d5dbe9a245a26e957330e.xls Enquire 2455.xls 1.xls 5c8b305236ca208eea43945d2771a401.file
Tipo	MS Excel
Tamaño	0.49 MB
Extensión	xls

B. Se obtuvieron los siguientes códigos hash, que permitirán generar las reglas para los sistemas de detección de amenazas o intrusos:

Hash Obtenidos	
md5	5c8b305236ca208eea43945d2771a401
sha-1	f73eff1d83d88158f32ab062c8279b8209dff82f
sha256	3d8a60463219bf3008e509aed8a505043d3e76e7110d5dbe9a245a26e957330e
Vhash	13c58281c7aa6f14ba8de31ef84a79f7
SSDEEP	12288:pSNtBC6uEkpQpozwjTqCfgb+W6xZsVPg0vik:Ow6srWWCfgKWNVPJ
TLSH	T17DB4235530D7DB6BC0D760704EEA80DB1607BC02A742F97735ACB7A E197A740C8B2A27
File type	MS Excel Spreadsheet

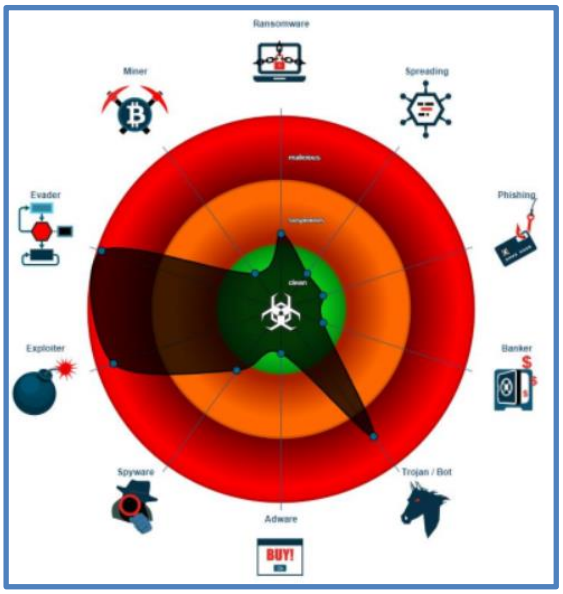
C. Obtención de direcciones IP de conexión al comando y control:

- www.fino-shop.store/he09/
- clhear.com
- maythunguyen.com
- xiongmaoaijia.com
- kembangzadsloh.xyz

- speedwagner.com
- 360bedroom.com
- campereurorg.top
- cwxg2.site
- mcdlibre.live
- globigprimecompanylimited.com
- 1707102023-stripe.com
- xhfj5.site
- mugiwaranousopp.xyz
- texmasco.com
- sc9999.net
- lite.team
- 8xb898.com
- cibecuetowing.top
- mgplatinemlak.xyz
- southwestharborkeyword.top
- mil840.vip
- mygovindexhtml.online
- pepecasinofun.online
- lindalilly.com
- 4da8.com
- gladespringtowing.top
- tinblaster.net
- jpedwardscoaching.com
- toursardegna.net
- ngocchiluong.com
- darringtontowing.top
- oiuajh.xyz
- nighvideos.com
- 15868.mom
- blueblaze.app
- escachifollad.store
- credclub.shop
- digitalfreedomhub.com
- onemobileal.com
- obqk8.site
- kelownainsulationservices.com
- skywatchnewsstores.com
- neu-de-update.com
- streamart.live
- popla9001.com
- theundraftd.com
- claims.scot
- bonk-token.com
- iwoulddye4u.com
- tenderherbschool.com
- thegoodbeautypodcast.com
- nahanttowing.top

- moneyshift.store
- relaxify.cloud
- wjr3x0d.shop
- churchsec.net
- chromadentalclinic.com
- kadeonline.com
- frank-cazino.com
- desixair.com
- cftd4o5.com
- ipodenergy.com
- kravingsbykiersten.com
- richmondvilletowing.top

D. Después de realizar diferentes pruebas con el archivo, éste fue clasificado como malicioso, el mismo que realiza diferentes acciones cuando toma el control de un equipo, como se grafica en la imagen:



Del análisis del archivo ejecutable con nombre **3d8a60463219bf3008e509aed8a505043d3e76e7110d5dbe9a245a26e957330e.xls**, se advierte que es considerado como malicioso, en razón a que realiza conexiones a diferentes direcciones Url, posibilitando el ingreso de otros archivos, por lo que es considerado un troyano, y por el tipo de comportamiento que éste posee como: Persistencia.

3. RECOMENDACIÓN:

- Compartir los indicadores de compromiso a fin de evitar posibles víctimas de este malware.

Fuente de Información:	Análisis Forense Digital

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Análisis técnico realizado a una extensión asociada con Microsoft PowerPoint – Microsoft Office.		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

Mediante correo electrónico proveniente de la DIVINDAT se informa que al realizar sus actividades lograron identificar que actores de amenazas vienen compartiendo a través de correos electrónicos un archivo adjunto que al parecer podría ser un tipo de malware. Por tal motivo y en prevención de víctimas potenciales solicitan el análisis forense y la obtención de los IoC.

2. **DETALLES:**

A. Se procede a realizar el análisis de un archivo ejecutable, con los siguientes detalles:

Datos del Archivo	
Nombre	18cdd23ad044b247dd5e24623746cc01a6f813c26c241d9f8925289adec606d5.ppam
Nombre Original	Detalhes_Reserva.ppam 18cdd23ad044b247dd5e24623746cc01a6f813c26c241d9f8925289 adec606d5.ppam
Tipo	Microsoft PowerPoint 2007+
Tamaño	0.01 MB
Extensión	ppam

B. Se obtuvieron los siguientes códigos hash, que permitirán generar las reglas para los sistemas de detección de amenazas o intrusos:

Hash Obtenidos	
md5	b37bdaaf0080a29e0a242ba0a257a977
sha-1	c1f206db9929dfd08d5b53dfe1e47d67b5821539
sha256	18cdd23ad044b247dd5e24623746cc01a6f813c26c241d9f8925289adec606d5
Vhash	32a56078b6667acbb9542f6005c26bb7
SSDEEP	192:xrXP/Gimwb0CPXzf6408ojuzA5W4yzD9a6XB:dXPnJXzQTuzAo4moY
TLSH	T10B22BF66D80F5BD3C6239D3582072FB6955CA00A70CE5B5AE8 449A0918F11CF0E9BDCE
File type	Office Open XML Presentation

C. Obtención de direcciones IP de conexión al comando y control:

- https://pt.textbin.net/download/rcd5ihynxw
- marcelotatuape.ddns.net:333
- 199.101.134.238
- 148.72.177.212
- 23.88.14.37

- 199.101.133.72
- 104.21.6.247

D. Después de realizar diferentes pruebas con el archivo, éste fue clasificado como malicioso, el mismo que realiza diferentes acciones cuando toma el control de un equipo, como se grafica en la imagen:

Del análisis del archivo ejecutable con nombre **18cdd23ad044b247dd5e24623746cc01a6f813c26c241d9f8925289adec606d5.ppam**, se evidencia que el contenido del archivo deriva de las variantes de los malware NJRAT y REVENGERAT, por ese motivo es considerado como malicioso; además, realiza conexiones a diferentes direcciones Url e IPs, posibilitando el ingreso de otros archivos, por lo que es considerado un troyano de acceso remoto (RAT).

3. RECOMENDACIÓN:

- Compartir los indicadores de compromiso a fin de evitar posibles víctimas de este malware.

Fuente de Información:	Análisis Forense Digital