I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Emotet es un troyano bancario modular y avanzado que funciona principalmente como descargador de otros troyanos bancarios; su fin es obtener acceso a dispositivos y espiar información privada y confidencial

Nivel de riesgo: Alto

II. ALERTA

Figura 1.- Emotet - Malware que se concibió originalmente como un troyano bancario

Emotet tiene la capacidad de engañar a los programas antivirus básicos y esconderse de ellos; una vez que infecta, el malware se propaga como un gusano informático e intenta infiltrarse en otras computadoras de la red.

Emotet pasó de ser un troyano bancario a un *dropper,* pues descarga programas maliciosos en dispositivos, en la mayoría de los casos, descargaba los siguientes programas:

- Trickster (también conocido como TrickLoader y TrickBot): troyano bancario que intenta capturar los datos de acceso a cuentas bancarias.
- Ryuk: troyano de cifrado, también conocido como criptotroyano o ransomware, cifra datos y, por lo tanto, impide que el usuario de la computadora acceda a dichos datos o a todo el sistema.

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.

III. INTRODUCCIÓN

Emotet fue diseñado originalmente como un malware bancario que intentaba colarse en un ordenador y robar información confidencial y privada. En versiones posteriores del software se añadieron los servicios de envío de spam y malware, incluidos otros troyanos bancarios.

Emotet fue identificad por primera vez por investigadores de seguridad en el 2014, cuando clientes de bancos alemanes y austriacos se vieron afectados por este troyano; Emotet había obtenido acceso a los datos de inicio de sesión de los clientes, luego el malware se propagó a nivel mundial.

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.

Emotet utiliza una serie de trucos para intentar evitar la detección y el análisis. Emotet es polimórfico, lo que significa que puede cambiar por sí mismo cada vez que se descarga y evitar la detección basada en firmas. Además, Emotet sabe si se está ejecutando dentro de una máquina virtual (virtual machine, VM) y permanecerá inactivo si detecta un entorno de sandbox.

Emotet también utiliza servidores de C&C para recibir actualizaciones. Esto funciona de la misma forma que las actualizaciones del sistema operativo en su PC y puede ocurrir sin problemas y sin ningún signo externo. Ello permite a los atacantes instalar versiones actualizadas del software, instalar malware adicional, como otros troyanos bancarios, o actuar como vertedero de información robada, como credenciales financieras, nombres de usuario y contraseñas y direcciones de correo electrónico.

En 2018, tras infectarse con Emotet, el hospital alemán Fuerstenafeldbruck tuvo que apagar 450 computadoras y desconectarse del centro de control de rescate para tratar de controlar la infección. En septiembre de 2019, el Tribunal de Apelación de Berlín se vio afectado y, en diciembre de 2019, la Universidad de Giessen. La Universidad Médica de Hannover y la administración de la ciudad de Fráncfort del Meno también fueron infectadas por Emotet.

Estos son solo algunos ejemplos de infecciones de Emotet, aunque se estima que la cantidad no revelada de empresas afectadas es mucho mayor. También se supone que muchas empresas infectadas no quisieron denunciar el problema por temor a dañar su reputación.

También es importante tener en cuenta que, si bien al principio los principales blancos de Emotet eran empresas y organizaciones, ahora el troyano apunta más a los particulares.

La Oficina Federal Alemana para la Seguridad de la Información (BSI) cree que «los desarrolladores de Emotet están subarrendando su software e infraestructura a terceros».

También recurren a malware adicional para perseguir sus propios objetivos. La BSI cree que la motivación de los delincuentes es financiera y, por lo tanto, los consideran delitos cibernéticos, no espionaje. Aun así, nadie parece tener una respuesta clara sobre quién está detrás de Emotet. Existen varios rumores con respecto a los países de origen, pero no hay pruebas fiables.

IV. VECTOR DE ATAQUE:

El principal método de distribución de Emotet es a través de malspam. Emotet saquea una lista de contactos y se envía a amigos, familiares, compañeros de trabajo y clientes. Puesto que estos correos electrónicos provienen de una cuenta de correo electrónico secuestrada, los correos electrónicos se parecen menos a spam, y los destinatarios, al sentirse seguros, tienden más a hacer clic en las direcciones URL incorrectas y descargar archivos infectados.

Si hay una red conectada, Emotet se propaga utilizando una lista de contraseñas comunes y adivina su camino hacia otros sistemas conectados en un ataque de fuerza bruta. Si la contraseña del importantísimo servidor de recursos humanos es simplemente "contraseña", entonces es probable que Emotet encuentre su camino hasta allí.

Otro método que Emotet utiliza para propagarse es a través de las vulnerabilidades EternalBlue/DoublePulsar, que fueron responsables de los ataques WannaCry y

NotPetya. Estos ataques aprovechan las vulnerabilidades de Windows que pueden permitir la instalación de malware sin interacción humana. Esta capacidad de autorreplicado, como un tipo de malware que llamamos gusano, provoca interminables dolores de cabeza a los administradores de red de todo el mundo a medida que Emotet se propaga de un sistema a otro.

La principal forma de propagación de Emotet es mediante la así llamada *recopilación de Outlook*. El troyano lee los correos electrónicos de los usuarios ya afectados y crea un contenido engañosamente real. Estos correos electrónicos parecen legítimos y personales, a diferencia de los correos spam comunes. Emotet envía estos correos electrónicos de phishing a los contactos almacenados, como amigos, familiares y compañeros de trabajo.

La mayoría de las veces, los correos electrónicos contienen un vínculo peligroso o un documento de Word infectado que se supone que el destinatario debe descargar. Siempre se muestra el nombre correcto como remitente. Por lo tanto, los destinatarios creen que es seguro: todo luce como un correo electrónico legítimo. Luego, en la mayoría de los casos, hacen clic en el vínculo peligroso o descargan el archivo adjunto infectado.

V. IMPACTO:

Todo el mundo es objetivo de Emotet. Hasta la fecha, Emotet ha afectado a particulares, empresas y entidades gubernamentales en Estados Unidos y Europa, y ha robado registros bancarios, datos financieros e incluso carteras de bitcoin.

Un ataque digno de mención de Emotet en Allentown (Pensilvania) requirió la ayuda directa del equipo de respuestas a incidentes de Microsoft para la limpieza y, al parecer, su reparación le costó a la ciudad más de 1 millón de dólares.

Ahora que Emotet se está utilizando para descargar y repartir otros troyanos bancarios, la lista de objetivos es, en potencia, aún más amplia. Las primeras

versiones de Emotet se utilizaron para atacar a clientes bancarios en Alemania. Las versiones posteriores de Emotet se dirigieron a organizaciones en Canadá, Reino Unido y Estados Unidos.

El Departamento de Seguridad Nacional de los Estados Unidos llegó a la conclusión de que Emotet es un software especialmente costoso con un enorme poder destructivo. Se estima que el costo de la limpieza es de aproximadamente un millón de dólares estadounidenses por incidente. Por ello, Arne Schoenboshm, jefe de la Oficina Federal Alemana para la Seguridad de la Información (BSI), llama a Emotet el «rey del malware».

VI. INDICADORES DE COMPROMISO

Direcciones IP asociadas a Emotet:

Ubicación (País)	Dirección IP
India	49.205.182.134
Cambodia	202.79.24.136
Turkey	78.188.106.53
France	195.144.11.124
France	195.144.11.125
Argentina	190.108.228.27
Italy	130.0.132.242
Thailand	103.253.75.46
Vietnam	112.213.89.130
Indonesia	103.85.95.5
Turkey	193.53.245.52
Singapore	139.59.107.152
Poland	51.89.36.180
Turkey	188.132.217.107
Russia	77.74.78.80
Vietnam	112.213.89.73
France	51.159.23.217

Poland	51.75.33.127
Korea, South	61.76.222.210

Ubicación (País)	Dirección IP
India	49.205.182.134

Virustotal señala:

49.205.182.134 (49.205.176.0/20)
AS 18209 (Atria Convergence Technologies pvt ltd)

IN | Last Analysis Date 16 days ago

Basic Properties

Network	49.205.176.0/20
Autonomous System Number	18209
Autonomous System Label	Atria Convergence Technologies pvt ltd
Regional Internet Registry	APNIC
Country	IN
Continent	AS

Communicating Files (759)

Scanned	Detections	Type	Name
2022-12-29	50 / 70	Win32 DLL	67c60516fc0ae02a9646bfb3d97c2fdfturns_3_add_strings_to_overlay_.exe
2023-09-28	56 / 71	Win32 DLL	00212d976969dcdcb8de96513e0a1077221cab3ce3153ae59bb3fd2f313b346b
2023-07-04	58 / 71	Win32 EXE	005720e9f897ebb44c338900c9148ec3e04806c1d55399718dbf630f8710f7ca
2023-01-02	54 / 69	Win32 DLL	016bbe3aa27e5a5b9bf4885447dcbc5dturns_4_add_strings_to_overlay_.exe
2023-05-15	45 / 70	Win32 DLL	22b76f5e627c34844736f798a7cb26b7turns_31_GAMMA_SECTIONS
2023-09-28	53 / 71	Win32 DLL	09d558427bc55ae87ffadb1d62529900turns_21_GAMMA_SECTIONS_
2023-07-17	60 / 70	Win32 DLL	VirusShare_07f06fa75bdec007587bac1dd29ddcae
2020-12-16	26 / 71	Win32 EXE	scripto.exe
2023-01-11	46 / 68	Win32 DLL	3e8b5e824babd7ab726aff8ff25ee65bturns_1_add_section_strings
2022-12-27	50 / 71	Win32 DLL	87f828175053fa004d9e4db30b1f64bfturns_2_add_strings_to_overlay_.exe

Files Referring (7)

Scanned	Detections	Type	Name
2023-06-05	0 / 59	CSV	Emotet.csv
2023-03-22	0 / 58	Text	list.txt
2021-09-23	0 / 57	Text	k00xwzTU
2021-09-23	0 / 57	C++	k09NVP33
2021-01-18	0 / 58	Pascal	1GWrJUTP
2021-01-01	0 / 60	Text	UzH3Br3m
2020-12-23	0 / 60	Pascal	ACtZbXXw

Ubicación (País)	Dirección IP
Cambodia	202.79.24.136

Virustotal señala:

202.79.24.136 (202.79.24.0/21)
AS 24492 (WiCAM Corporation Ltd.)

KH | Last Analysis Date 15 days ago

Basic Properties ⓘ

Network	202.79.24.0/21
Autonomous System Number	24492
Autonomous System Label	WiCAM Corporation Ltd.
Regional Internet Registry	APNIC
Country	KH
Continent	AS

Passive DNS Replication (1) ⓘ

Date resolved	Detections	Resolver	Domain
2023-10-11	0 / 88	VirusTotal	mynet.wicam.com.kh

Communicating Files (823) ⓘ

Scanned	Detections	Type	Name
2021-03-24	52 / 70	Win32 DLL	emotet_exe_e1_0046ee37140239885ceadab499482e1dea13fb5a39ec173dee514c338cd17bb2_2021-01-14__002205.exe_20191212_112720+0000
2021-01-15	25 / 70	Win32 DLL	emotet_exe_e1_006556912957099ee7354ea1bf229cf9b48e21d267c94e32dd66660a4f556c61_2021-01-15__042404.exe_20191212_112720+0000
2023-01-06	26 / 70	Win32 DLL	20d400d89e7cd705bf4062d56f47b15dturns_31_GAMMA_SECTIONS
2021-11-09	51 / 65	Win32 DLL	emotet_exe_e1_01a91855a7b92fd62d9e346756fed8edd747bc075062bb01f5f0a56386698a05_2020-12-21__114717._exe
2021-01-21	54 / 70	Win32 DLL	emotet_exe_e1_02465763a8aa3c2e6d328662305962f309cce88bb0b459167a81fb26ed23bada_2021-01-14__025605.exe_20191212_112720+0000
2023-01-04	51 / 69	Win32 DLL	073924abed69cc7fb804786727cca706turns_3_add_strings_to_overlay_.exe
2021-06-07	43 / 69	Win32 EXE	a9e20bcca198a5cba4ffb3dc0528828d.virus
2021-01-21	56 / 70	Win32 DLL	emotet_exe_e1_0351957d71b9d334134791c3fc76bae59571f229618c9ff4fc475f2570c31076_2021-01-15__094002.exe_20191212_112720+0000
2021-01-21	54 / 70	Win32 DLL	emotet_exe_e1_0374963686e5f756b3d543d5283b2af4318c7ba2059f30622e1b87adb7162f87_2021-01-15__174542._exe
2021-01-22	55 / 70	Win32 DLL	emotet_exe_e1_0385d8e5d4c669c541c383aaa40699f23f9ac0b465f5509377393c2e18663834_2021-01-15__094803.exe_20191212_112720+0000

• • •

Files Referring (14) ⓘ

Scanned	Detections	Type	Name
2022-05-22	1 / 66	Win32 EXE	428939
2022-05-22	1 / 66	Win32 EXE	xns6_setup.exe
2023-09-27	0 / 70	Win32 EXE	1311514
2023-06-05	0 / 59	CSV	Emotet.csv
2023-10-03	0 / 60	unknown	Posible_ref.csv
2023-05-04	0 / 58	Text	Unblocked IPs List 4-27- AW Intel Box.txt
2021-06-18	0 / 57	JavaScript	myfile.exe
2021-06-18	0 / 58	JavaScript	myfile.exe

Ubicación (País)	Dirección IP
Turkey	78.188.106.53

Virustotal señala:

78.188.106.53 (78.188.104.0/22)
AS 47331 (Turk Telekom)

TR | Last Analysis Date 4 days ago

Basic Properties

Network	78.188.104.0/22
Autonomous System Number	47331
Autonomous System Label	Turk Telekom
Regional Internet Registry	RIPE NCC
Country	TR
Continent	AS

Communicating Files (11.3 K)

Scanned	Detections	Type	Name
2020-10-25	48 / 62	Win32 EXE	Flex Box improves
2023-08-29	53 / 71	Win32 EXE	d2ec015fb417e8d140ececb7bdff9f7d.virus
2020-11-26	56 / 71	Win32 EXE	Sock
2020-11-25	58 / 70	Win32 EXE	emotet_exe_e2_008feba0a4c8f9790877cee9d00261bbea8e24c43254a604b8d956bc97bca8b0_2020-10-29__214432._exe
2020-12-31	52 / 71	Win32 EXE	ColorBoxSample
2020-10-10	56 / 70	Win32 EXE	HDF.AT Interactive Stock Chart
2020-10-30	34 / 72	Win32 EXE	emotet_exe_e2_00d22be31b04af8f95c4c63c3b1a2dec068ca8d4aa7f301071a013783a3a35e2_2020-10-29__133604.exe_20201029_141048+0000
2020-12-19	60 / 71	Win32 EXE	EffectDemo
2020-10-24	45 / 62	Win32 EXE	Flex Box improves
2020-10-22	29 / 71	Win32 EXE	379c66eb8bf1615630b411d4854fdc96.virus

Files Referring (11)

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt
2023-10-03	0 / 60	unknown	Posible_ref.csv
2023-06-05	0 / 59	CSV	Emotet.csv
2023-05-04	0 / 58	Text	Unblocked IPs List 4-27- AW Intel Box.txt
2023-03-22	0 / 58	Text	list.txt
2021-01-18	0 / 57	Text	3EvT56ak
2022-11-07	0 / 61	Text	Pmw6TbvU
2020-11-13	0 / 60	Text	Q6sutszk
2020-10-22	0 / 60	Text	IOC_IPs-Emotet
2020-10-21	0 / 55	Text	4MhJgfRi

Ubicación (País)	Dirección IP
France	195.144.11.124

Virustotal señala:

195.144.11.124 (195.144.11.0/24)
AS 35393 (CTS Computers and Telecommunications Systems SAS)

FR | Last Analysis Date 7 days ago

Basic Properties

Network	195.144.11.0/24
Autonomous System Number	35393
Autonomous System Label	CTS Computers and Telecommunications Systems SAS
Regional Internet Registry	RIPE NCC
Country	FR
Continent	EU

Communicating Files (301)

Scanned	Detections	Type	Name
2023-03-12	59 / 69	Win32 EXE	eaa1b13340ea03307f38e36598c787c8.virus
2023-08-14	20 / 59	HTML	output.19857790.txt
2022-09-08	57 / 71	Win32 EXE	Qiqaf
2022-09-17	58 / 71	Win32 EXE	Qiqaf
2022-05-22	56 / 66	Win32 EXE	zozusdigteax.exe
2022-05-27	56 / 69	Win32 EXE	tusocxuhadqo.exe
2022-05-17	47 / 68	Win32 EXE	kemfosjasese.exe
2022-08-21	51 / 71	Win32 EXE	nagymyzxaqro.exe
2023-04-17	56 / 69	Win32 EXE	makvozqaftea.exe
2023-10-03	61 / 72	Win32 EXE	2a5add1ecb04d96463f38a8992acc400.virobj

Files Referring (6)

Scanned	Detections	Type	Name
2023-02-08	1 / 59	Win32 EXE	annuweb_setup
2023-08-27	0 / 59	Python	IP.txt
2023-06-05	0 / 59	CSV	Emotet.csv
2023-03-22	0 / 58	Text	list.txt
2022-07-08	0 / 67	Win32 EXE	ANNUWEB.exe
2021-07-16	0 / 69	Win32 EXE	ANNUWEB.exe

Ubicación (País)	Dirección IP
France	195.144.11.125

Virustotal señala:

195.144.11.125 (195.144.11.0/24)
AS 35393 (CTS Computers and Telecommunications Systems SAS)

FR | Last Analysis Date 2 days ago

Basic Properties ⓘ

Network	195.144.11.0/24
Autonomous System Number	35393
Autonomous System Label	CTS Computers and Telecommunications Systems SAS
Regional Internet Registry	RIPE NCC
Country	FR
Continent	EU

Last HTTPS Certificate ⓘ

JARM Fingerprint

29d29d15d29d29d00042d42d000000038eaaf490bec8dc33757f165ce01762

Last HTTPS Certificate

```
Data:
   Version: V3
   Serial Number: 324f255fd3e090af2654883f886ca8b
   Thumbprint: 1b2c26393462ab814c77f6c6408ab8da2087138f
Signature Algorithm:
   Issuer: C=US , CN=RapidSSL Global TLS RSA4096 SHA256 2022 CA1 , O=DigiCert, Inc.
   Validity
      Not Before: 2023-01-19 00:00:00
      Not After: 2024-02-19 23:59:59
   Subject: CN=*.phpnet.org
```

Communicating Files (68)

Scanned	Detections	Type	Name
2023-03-12	59 / 69	Win32 EXE	eaa1b13340ea03307f38e36598c787c8.virus
2023-08-14	20 / 59	HTML	output.19857790.txt
2022-05-22	56 / 66	Win32 EXE	zozusdigteax.exe
2022-05-17	47 / 68	Win32 EXE	kemfosjasese.exe
2022-08-21	51 / 71	Win32 EXE	nagymyzxaqro.exe
2023-04-17	56 / 69	Win32 EXE	makvozqaftea.exe
2023-09-28	52 / 72	Win32 EXE	baxxamgozxux.exe
2023-06-05	57 / 71	Win32 EXE	mylliwillebm.exe
2023-08-08	58 / 71	Win32 EXE	kijygpizfokm.exe
2022-05-17	45 / 68	Win32 EXE	veanosudxeax.exe

Files Referring (1)

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt

Ubicación (País)	Dirección IP
Argentina	190.108.228.27

Virustotal señala:

190.108.228.27 (190.108.224.0/19)
AS 27751 (Neunet S.A.)

AR | Last Analysis Date 19 hours ago

Basic Properties

Network	190.108.224.0/19
Autonomous System Number	27751
Autonomous System Label	Neunet S.A.
Regional Internet Registry	LACNIC
Country	AR
Continent	SA

Communicating Files (9.0 K)

Scanned	Detections	Type	Name
2023-08-29	53 / 71	Win32 EXE	d2ec015fb417e8d140ececb7bdff9f7d.virus
2020-11-26	56 / 71	Win32 EXE	Sock
2020-11-25	58 / 70	Win32 EXE	emotet_exe_e2_008feba0a4c8f9790877cee9d00261bbea8e24c43254a604b8d956bc97bca8b0_2020-10-29__214432._exe
2020-12-31	52 / 71	Win32 EXE	ColorBoxSample
2022-08-02	55 / 71	Win32 EXE	00c40b772b41f51583cc133115423cef49dbb3f4a4f7d91e47fc8d40ca7ad026.exe
2020-10-30	34 / 72	Win32 EXE	emotet_exe_e2_00d22be31b04af8f95c4c63c3b1a2dec068ca8d4aa7f301071a013783a3a35e2_2020-10-29__133604.exe_20201029_141048+0000
2020-12-19	60 / 71	Win32 EXE	EffectDemo
2020-10-22	29 / 71	Win32 EXE	379c66eb8bf1615630b411d4854fdc96.virus
2020-11-10	59 / 72	Win32 EXE	FormsSpy
2020-10-26	45 / 60	Win32 EXE	EffectDemo

Files Referring (9)

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt
2023-07-23	0 / 59	Text	7cP05wY3
2023-07-12	0 / 58	Text	rUZJf9VP
2021-01-18	0 / 59	Text	Emotet malware campaign_09 Nov 2020.csv
2021-01-18	0 / 57	Text	3EvT56ak
2021-01-18	0 / 54	Text	q7P2h3TP
2022-11-07	0 / 61	Text	Pmw6TbvU
2020-10-21	0 / 55	Text	4MhJgfRi
2020-10-19	0 / 58	Text	gbCPJjSc

Ubicación (País)	Dirección IP
Italy	130.0.132.242

Virustotal señala:

130.0.132.242 (130.0.128.0/18)
AS 30722 (Vodafone Italia S.p.A.)

IT | Last Analysis Date 5 days ago

Basic Properties

Network	130.0.128.0/18
Autonomous System Number	30722
Autonomous System Label	Vodafone Italia S.p.A.
Regional Internet Registry	RIPE NCC
Country	IT
Continent	EU

Date resolved	Detections	Resolver	Domain
2021-12-29	0 / 88	VirusTotal	device-6662d6a6-99c4-41f3-8e0b-9ed014541b8d.remotewd.com

Communicating Files (9.1 K)

Scanned	Detections	Type	Name
2023-06-13	60 / 71	Win32 EXE	04741799.exe
2020-10-15	11 / 70	Win32 EXE	emotet_exe_e2_001e0fd424cc232636fa35828af46aa078111aea2680656500961731b5abd972_2020-10-15__060719_.exe
2020-10-25	48 / 62	Win32 EXE	Flex Box improves
2020-10-15	11 / 70	Win32 EXE	emotet_exe_e2_00325089a8fb94f5bf2e17ad06162ffad6e1a41b60ca906b4fc6791bae5408c4_2020-10-15__070604.exe_20201014_211813+0000
2020-10-14	11 / 71	Win32 EXE	emotet_exe_e2_003de0ff745ee56e1f3a19cad15506fa3623c998de711ff8485b103699f50ef8_2020-10-14__221130_.exe
2023-01-01	56 / 69	Win32 EXE	VirusShare_44afb34fa4867692eb55636b980dc5e2
2020-11-07	52 / 72	Win32 EXE	ColorBoxSample
2020-12-31	52 / 71	Win32 EXE	ColorBoxSample
2020-10-10	56 / 70	Win32 EXE	HDF.AT Interactive Stock Chart
2020-12-19	60 / 71	Win32 EXE	EffectDemo

Files Referring (9)

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt
2023-06-05	0 / 59	CSV	Emotet.csv
2023-10-03	0 / 60	unknown	Posible_ref.csv
2023-05-04	0 / 58	Text	Unblocked IPs List 4-27- AW Intel Box.txt
2023-03-22	0 / 58	Text	list.txt
2023-02-04	0 / 60	Text	compromised_ip_live.txt
2020-11-13	0 / 60	Text	Q6sutszk
2020-10-23	0 / 51	Text	JPK7ibHx
2020-10-19	0 / 58	Text	gbCPJjSc

Ubicación (País)	Dirección IP
Thailand	103.253.75.46

Virustotal señala:

103.253.75.46 (103.253.72.0/22)
AS 56309 (408 FI4 CATTOWER)

TH | Last Analysis Date
2 days ago

Basic Properties ⓘ

Network	103.253.72.0/22
Autonomous System Number	56309
Autonomous System Label	408 FI4 CATTOWER
Regional Internet Registry	APNIC
Country	TH
Continent	AS

Communicating Files (44) ⓘ

Scanned	Detections	Type	Name
2022-07-22	30 / 60	Windows shortcut	2022-06-07_0704.lnk
2022-06-16	27 / 57	Windows shortcut	payload_1.bin
2022-06-17	18 / 56	Windows shortcut	payload_1.bin
2022-07-22	36 / 60	Windows shortcut	payload_1.bin
2022-06-17	33 / 58	Windows shortcut	11b7b859ff92979fea85fea5a1796aff68dfa6e7f22bbb1e47a09e214aaf2429
2022-06-17	19 / 57	Windows shortcut	payload_1.bin
2022-06-17	27 / 57	Windows shortcut	payload_1.bin
2022-06-16	23 / 57	Windows shortcut	payload_1.bin
2022-06-17	19 / 57	Windows shortcut	payload_1.bin
2022-06-16	22 / 57	Windows shortcut	28a69b5f4be821633e59d9188801dcb538c85f8a7545ab07435709c01113b93f

Files Referring (3) ⓘ

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt
2023-06-05	0 / 59	CSV	Emotet.csv
2023-03-22	0 / 58	Text	list.txt

Ubicación (País)	Dirección IP
Vietnam	112.213.89.130

Virustotal señala:

112.213.89.130 (112.213.80.0/20)
AS 45544 (SUPERDATA)

VN | Last Analysis Date
2 days ago

Basic Properties ⓘ

Network	112.213.80.0/20
Autonomous System Number	45544
Autonomous System Label	SUPERDATA
Regional Internet Registry	APNIC
Country	VN
Continent	AS

Communicating Files (554) ⓘ

Scanned	Detections	Type	Name
2019-10-15	37 / 60	MS Word Document	aca1f7bf446a72de3e639678398baca0.virobj
2023-07-18	41 / 60	MS Excel Spreadsheet	unknown
2022-08-28	33 / 71	Win32 EXE	Ogeuai.exe
2019-11-01	38 / 59	MS Word Document	ZPLCMHKPRDW7Z9_AXK.doc
2021-03-09	37 / 70	Win32 EXE	71433-d2c17445ff2ef4f04ab5934a6888c7cf.exe
2023-07-18	41 / 60	MS Excel Spreadsheet	unknown
2019-10-19	39 / 61	Office Open XML Document	BL_7GOMR1AQUA9K_SZG_Oct2019.doc
2022-09-12	52 / 70	Win32 EXE	Vpvww.exe
2019-11-01	39 / 59	MS Word Document	.
2023-07-18	40 / 60	MS Excel Spreadsheet	unknown

• • •

Files Referring (3) ⓘ

Scanned	Detections	Type	Name
2023-07-17	0 / 59	Text	thanglongpt_db.sql
2022-12-24	0 / 71	Win32 DLL	eWorks.Android.dll
2020-07-02	0 / 65	Android	ed38af4ce1a6c719f71e440954eb22ee37a405d1c41e1ee4e0bdafc3d1222859

Ubicación (País)	Dirección IP
Indonesia	103.85.95.5

Virustotal señala:

103.85.95.5 (103.85.95.0/24)
AS 136077 (Universitas Islam Negeri Mataram)

ID | Last Analysis Date
4 days ago

Basic Properties ⓘ

Network	103.85.95.0/24
Autonomous System Number	136077
Autonomous System Label	Universitas Islam Negeri Mataram
Regional Internet Registry	APNIC
Country	ID
Continent	AS

Passive DNS Replication (41) ⓘ

Date resolved	Detections	Resolver	Domain
2021-12-20	0 / 88	VirusTotal	ceklulus.uinmataram.ac.id
2021-11-11	0 / 88	VirusTotal	altazkiah.uinmataram.ac.id
2021-10-24	0 / 88	VirusTotal	pubah.uinmataram.ac.id
2021-10-23	0 / 88	VirusTotal	toefl.uinmataram.ac.id
2021-07-10	0 / 88	VirusTotal	tipd.uinmataram.ac.id
2021-05-26	0 / 88	VirusTotal	lpm.uinmataram.ac.id
2021-04-30	0 / 88	VirusTotal	ppid.uinmataram.ac.id
2021-03-09	0 / 88	VirusTotal	upb.uinmataram.ac.id
2021-03-02	0 / 88	VirusTotal	rumah-jurnal.uinmataram.ac.id
2021-03-01	0 / 88	VirusTotal	karir.uinmataram.ac.id

• • •

Communicating Files (1) ⓘ

Scanned	Detections	Type	Name
2023-08-10	38 / 58	Office Open XML Spreadsheet	24f261013b2ea3c17ef7508b30b70d586796c25874ec137fcfdfdb686254656b

Files Referring (8) ⓘ

Scanned	Detections	Type	Name
2023-09-13	3 / 58	Network capture	10346484_64F55B95-0000-0020-0002-D81F00000000.pcap
2023-08-12	13 / 58	unknown	_36_Lucene84_0.tim
2022-03-10	2 / 53	XML	41f92fb571b9bf91ee3e81ba9d57bfdea3663e0b9cf75e8dea8415b403e409f6
2023-08-27	0 / 59	Python	IP.txt
2023-06-05	0 / 59	CSV	Emotet.csv
2023-06-02	0 / 59	Text	36c41ee8-747c-4fee-84e4-7d2878705b1c.tmp
2023-03-22	0 / 58	Text	list.txt
2022-04-26	0 / 58	unknown	JJpsZcvIDt.ps1

Ubicación (País)	Dirección IP
Turkey	193.53.245.52

Virustotal señala:

193.53.245.52 (193.53.245.0/24)
AS 209711 (MUV Bilisim ve Telekomunikasyon Hizmetleri Ltd. Sti.)

TR | Last Analysis Date 16 days ago

Basic Properties

Network	193.53.245.0/24
Autonomous System Number	209711
Autonomous System Label	MUV Bilisim ve Telekomunikasyon Hizmetleri Ltd. Sti.
Regional Internet Registry	RIPE NCC
Country	TR
Continent	AS

Communicating Files (208)

Scanned	Detections	Type	Name
2023-07-18	40 / 59	MS Excel Spreadsheet	022f64891d4de0dedec52021b5c9f16d415d0e68463e31404e5bd4e13fbc4de3.xls
2023-07-18	41 / 60	MS Excel Spreadsheet	message 86905672.xls
2023-05-23	41 / 60	MS Excel Spreadsheet	MAIL_11072022.xls
2023-07-18	40 / 60	MS Excel Spreadsheet	1107.xls
2023-07-18	41 / 60	MS Excel Spreadsheet	Details_1406.xls
2023-07-18	41 / 60	MS Excel Spreadsheet	DOC_814151587.xls
2022-07-12	35 / 60	MS Excel Spreadsheet	spreadsheet.xls
2023-07-18	41 / 60	MS Excel Spreadsheet	113__40.xls
2023-07-18	40 / 60	MS Excel Spreadsheet	PACK 36899.xls
2023-07-18	40 / 60	MS Excel Spreadsheet	Dokument 291.xls

Files Referring (10)

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt
2023-06-05	0 / 59	CSV	Emotet.csv
2023-03-22	0 / 58	Text	list.txt
2023-03-19	0 / 58	Text	IPS Maliciosas.txt
2022-12-06	0 / 61	Text	URL_blacklist.txt
2022-09-22	0 / 60	Text	ipsss.txt
2022-07-08	0 / 57	JavaScript	4d78c28f18f776d6df78ab06b399a548a080ceb8852f4f4b9e081817db87e6a5
2022-07-08	0 / 57	JavaScript	c1f0972e64d03f3ba8d97823c8ba3cd9464866756ba3d8272e4c9b6eda48f302
2022-07-08	0 / 57	JavaScript	f82b89f3e0fb1cb0adde4f04a9b506c6536f6795d3e92128673bea276f0b3f86
2022-07-08	0 / 57	JavaScript	58162f5ef51244440c6572ad7ce4082d147b3adbfe3b48eef9e2a4df10edeb2d

Ubicación (País)	Dirección IP
Singapore	139.59.107.152

Virustotal señala:

139.59.107.152 (139.59.0.0/17)
AS 14061 (DIGITALOCEAN-ASN)

SG | Last Analysis Date 2 days ago

Basic Properties ⓘ

Network	139.59.0.0/17
Autonomous System Number	14061
Autonomous System Label	DIGITALOCEAN-ASN
Regional Internet Registry	APNIC
Country	SG
Continent	AS

Passive DNS Replication (3) ⓘ

Date resolved	Detections	Resolver	Domain
2023-02-27	2 / 88	VirusTotal	offf.ooguy.com
2022-08-30	0 / 88	VirusTotal	offf.dynu.net
2022-07-25	1 / 88	VirusTotal	offf.kozow.com

Files Referring (37) ⓘ

Scanned	Detections	Type	Name
2023-02-13	4 / 60	PHP	block-1.php
2023-02-10	4 / 59	PHP	block-1.php
2023-02-09	3 / 60	PHP	block-1.php
2023-02-09	2 / 60	PHP	block-1.php
2023-02-09	2 / 60	PHP	block-1.php
2023-02-08	2 / 60	PHP	block-1.php
2023-02-08	2 / 60	PHP	block-1.php
2023-02-08	2 / 60	PHP	block-1.php
2022-03-20	12 / 56	TAR	b9cfe41197bf14b67219f29e7eb5ec96e0daf20febcdd134b435f3df7a63d639.file
2021-05-07	1 / 58	PHP	block-1.php

Ubicación (País)	Dirección IP
Poland	51.89.36.180

Virustotal señala:

51.89.36.180 (51.89.0.0/16)
AS 16276 (OVH SAS)

GB | Last Analysis Date
15 days ago

Basic Properties

Network	51.89.0.0/16
Autonomous System Number	16276
Autonomous System Label	OVH SAS
Regional Internet Registry	RIPE NCC
Country	GB
Continent	EU

Communicating Files (896)

Scanned	Detections	Type	Name
2022-12-29	50 / 70	Win32 DLL	67c60516fc0ae02a9646bfb3d97c2fdfturns_3_add_strings_to_overlay_.exe
2023-09-28	56 / 71	Win32 DLL	00212d976969dcdcb8de96513e0a1077221cab3ce3153ae59bb3fd2f313b346b
2023-01-02	54 / 69	Win32 DLL	016bbe3aa27e5a5b9bf4885447dcbc5dturns_4_add_strings_to_overlay_.exe
2023-05-15	45 / 70	Win32 DLL	22b76f5e627c34844736f798a7cb26b7turns_31_GAMMA_SECTIONS
2023-09-28	53 / 71	Win32 DLL	09d558427bc55ae87ffadb1d62529900turns_21_GAMMA_SECTIONS_
2023-07-17	60 / 70	Win32 DLL	VirusShare_07f06fa75bdec007587bac1dd29ddcae
2020-11-10	37 / 72	Win32 EXE	a458161036d8cf6d1ab9f71b893e2bb0.virus
2023-01-11	46 / 68	Win32 DLL	3e8b5e824babd7ab726aff8ff25ee65bturns_1_add_section_strings
2022-12-27	50 / 71	Win32 DLL	87f828175053fa004d9e4db30b1f64bfturns_2_add_strings_to_overlay_.exe
2020-12-11	52 / 70	Win32 EXE	Formula

Files Referring (9)

Scanned	Detections	Type	Name
2023-08-27	0 / 59	Python	IP.txt
2023-02-04	0 / 60	Text	compromised_ip_live.txt
2021-01-25	0 / 59	Pascal	M6PPQ1i0
2021-01-16	0 / 56	C++	b5b1d48bb77ed47458dd0c82296911b8b71c5fe8ad15553d955641c250c3b61c.js
2021-01-05	0 / 60	Text	xvnedZKQ
2021-01-18	0 / 58	Pascal	1GWrJUTP
2020-12-23	0 / 60	Pascal	ACtZbXXw
2020-12-09	0 / 60	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2020-12-08	0 / 60	C++	6848929d515850dafe396323599d5fe538469de597a6c592a26b2b7194592251.js

Ubicación (País)	Dirección IP
Turkey	188.132.217.107

Virustotal señala:

188.132.217.107 (188.132.217.0/24)
AS 42910 (PremierDC Veri Merkezi Anonim Sirketi)

TR | Last Analysis Date 10 days ago

Basic Properties ⓘ

Network	188.132.217.0/24
Autonomous System Number	42910
Autonomous System Label	PremierDC Veri Merkezi Anonim Sirketi
Regional Internet Registry	RIPE NCC
Country	TR
Continent	AS

Communicating Files (178) ⓘ

Scanned	Detections	Type	Name
2023-09-21	38 / 59	MS Excel Spreadsheet	attachment.xls
2022-12-10	43 / 62	MS Excel Spreadsheet	020b76245aae2c8b8da5a937083032601a745eb8f2deea9a087ef1e6e929b897.xls
2023-08-10	41 / 60	MS Excel Spreadsheet	027c2f010335efc0e82f1de773f2636d07cace73133db49947a8ef328a76800f.xls
2022-11-13	39 / 60	MS Excel Spreadsheet	080702bacb2fda3654e7e1d0a9f17e1be2b46a89ddc09cba556fd5bf2ab6c728.xls
2022-11-13	38 / 61	MS Excel Spreadsheet	0859b3536a6359684bbc3e2851f79d71a3c55805c5588ca328639bafe955d1ca.xls
2022-11-13	38 / 62	MS Excel Spreadsheet	0a1813895bea8e1f022b29c664d3693c740e34ef264e65f34731b9c265e94f2d.xls
2022-04-23	39 / 60	MS Excel Spreadsheet	mensaje-0104.xls
2022-04-04	19 / 60	MS Excel Spreadsheet	NOTICE-475578_xls.bin
2022-11-13	38 / 62	MS Excel Spreadsheet	0f976d8932654a0dcf750aa97b55e39b2368ae580de7d175a671c9db206e5286.xls
2022-11-13	38 / 62	MS Excel Spreadsheet	100973e2933d9b4fb53e79716d648f779ba92160ff9f144f2821bee32830b77f.xls

• • •

Files Referring (2) ⓘ

Scanned	Detections	Type	Name
2023-03-22	0 / 58	Text	list.txt
2022-05-25	0 / 56	Outlook	Quote For General Auto Spare parts (453 KB).msg

Ubicación (País)	Dirección IP
Russia	77.74.78.80

Virustotal señala:

77.74.78.80 (77.74.78.0/23)
AS 31261 (PJSC MegaFon)

RU | Last Analysis Date
22 hours ago

Basic Properties

Network	77.74.78.0/23
Autonomous System Number	31261
Autonomous System Label	PJSC MegaFon
Regional Internet Registry	RIPE NCC
Country	RU
Continent	EU

Passive DNS Replication (3)

Date resolved	Detections	Resolver	Domain
2020-03-05	0 / 88	VirusTotal	www.prospekt.org
2019-11-10	0 / 88	VirusTotal	file.litgid.org
2019-08-19	0 / 88	VirusTotal	prospekt.org

Communicating Files (64.1 K)

Scanned	Detections	Type	Name
2020-08-14	37 / 70	Win32 EXE	ListBoxCHDemo
2020-10-30	31 / 71	Win32 EXE	emotet_exe_e3_000064948fcef4b1705072bedeeac4bf079e9c63035a9a12b04c11a86cea424a_2020-10-30__053127_.exe
2023-05-22	57 / 70	Win32 EXE	ColorCoder
2020-10-23	14 / 71	Win32 EXE	emotet_exe_e3_0000e17d6d7c9d7b1bb8046cefeb464a7b41a38e33290d1aab0bf855ba9b8d23_2020-10-23__013429_.exe
2020-08-04	49 / 72	Win32 EXE	BrushTool
2020-09-21	54 / 66	Win32 EXE	WINHSTB
2020-08-25	48 / 67	Win32 EXE	TreeEditor
2020-08-11	39 / 70	Win32 EXE	FolderBrowse
2022-08-27	59 / 71	Win32 EXE	000c8ac055dc3c92b04ac95c803365a4c4bf0e7332da8cbf489ae2e8922152a2.exe
2020-10-02	60 / 70	Win32 EXE	WINHSTB

• • •

Files Referring (20)

Scanned	Detections	Type	Name
2023-11-16	0 / 60	Structured Query Language	IOC_Emotet.db
2023-10-03	0 / 60	unknown	Posible_ref.csv
2023-06-05	0 / 59	CSV	Emotet.csv
2023-05-04	0 / 58	Text	Unblocked IPs List 4-27- AW Intel Box.txt
2023-03-22	0 / 58	Text	list.txt
2021-02-05	0 / 59	Text	myfile.exe
2021-01-18	0 / 59	Text	Emotet malware campaign_09 Nov 2020.csv
2021-01-18	0 / 54	Text	q7P2h3TP

Ubicación (País)	Dirección IP
Vietnam	112.213.89.73

Virustotal señala:

112.213.89.73 (112.213.80.0/20)
AS 45544 (SUPERDATA)

VN | Last Analysis Date 2 days ago

Basic Properties

Network	112.213.80.0/20
Autonomous System Number	45544
Autonomous System Label	SUPERDATA
Regional Internet Registry	APNIC
Country	VN
Continent	AS

Communicating Files (200)

Scanned	Detections	Type	Name
2020-01-15	40 / 62	MS Word Document	4076819 20191127.doc
2020-01-06	40 / 62	MS Word Document	name
2021-10-09	14 / 61	PDF	riwodopaxeboxabifen.pdf
2021-10-08	13 / 59	PDF	1612f6b8b687fd---92829546550.pdf
-	-	file	04877ee94f46c1af224f3764ee3a452603e659fdbee3e0e1a04bfbf2cc7ad8c3
2020-09-10	41 / 62	Office Open XML Document	095cc5236f30098e9c3c9ce71aef7d97d16f534229cf8f76033280933a9b7053
2020-01-15	40 / 62	MS Word Document	5703_20191127.doc
2020-09-10	42 / 63	Office Open XML Document	0c161038a37d840ace5a445397aa2f555f581fbc52c2240c85d967ec9871bde4
2023-10-20	47 / 71	Win32 EXE	maEb.exe
2022-04-28	14 / 61	PDF	55014955878.pdf

Files Referring (5)

Scanned	Detections	Type	Name
2020-08-26	2 / 67	Win32 EXE	Tabas_PhucDat_int
2020-08-14	2 / 72	Win32 EXE	tabas_phucdat2(lop).exe
2023-08-27	0 / 59	Python	IP.txt
2022-12-24	0 / 71	Win32 EXE	Tabas_PhucDat_int
2022-06-18	0 / 67	Win32 EXE	Tabas_PhucDat_int

Ubicación (País)	Dirección IP
France	51.159.23.217

Virustotal señala:

51.159.23.217 (51.158.0.0/15)
AS 12876 (Scaleway S.a.s.)

FR | Last Analysis Date 23 hours ago

Basic Properties ⓘ

Network	51.158.0.0/15
Autonomous System Number	12876
Autonomous System Label	Scaleway S.a.s.
Regional Internet Registry	RIPE NCC
Country	FR
Continent	EU

Communicating Files (28.5 K) ⓘ

Scanned	Detections	Type	Name
2022-09-24	55 / 69	Win32 EXE	RunWinDiff
2020-09-20	56 / 68	Win32 EXE	WINHSTB
2020-09-08	58 / 69	Win32 EXE	ListBoxCHDemo
2020-10-05	54 / 70	Win32 EXE	MapEd.exe
2020-08-22	51 / 68	Win32 EXE	Pop3Monitor
2020-09-23	53 / 71	Win32 EXE	TestDigitalControl
2020-08-29	48 / 68	Win32 EXE	ListBoxCHDemo
2023-04-15	54 / 70	Win32 EXE	certutil.exe
2020-10-09	57 / 68	Win32 EXE	NetBIOS Enumerater
2020-09-25	43 / 69	Win32 EXE	NetBIOS Enumerater

• • •

Files Referring (14) ⓘ

Scanned	Detections	Type	Name
2022-05-13	1 / 58	Network capture	2020-02-07-Emotet-epoch-2-infection-with-Trickbot-gtag-mor93.pcap
2020-05-02	1 / 58	Network capture	3.pcap
2023-11-16	0 / 60	Structured Query Language	IOC_Emotet.db
2023-10-03	0 / 60	unknown	Posible_ref.csv
2023-09-13	0 / 59	Network capture	sample_traffic.pcap
2023-08-27	0 / 59	Python	IP.txt
2023-05-04	0 / 58	Text	Unblocked IPs List 4-27- AW Intel Box.txt
2023-01-07	0 / 61	Text	Quarantine_2020-11-04_14_40_28.csv
2020-09-25	0 / 62	Office Open XML Document	Malware Analysis.docx
-	-	file	dd87a1855482598062e7639b0320fa66346bdcb79cae0d94c0e0d2bedfa68ba5

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Mantenga sus dispositivos actualizados con los parches más recientes para MS Windows. Emotet puede confiar en la vulnerabilidad de Windows EternalBlue para hacer su trabajo sucio, así que no deje esa puerta trasera abierta en su red.

- Es esencial que instale lo antes posible las actualizaciones proporcionadas por los fabricantes para cerrar posibles brechas de seguridad. Esto se aplica a los sistemas operativos como Windows y macOS, así como a cualquier programa de aplicaciones, navegador, complemento del navegador, cliente de correo electrónico, programas de Office y PDF.

- No descargue archivos adjuntos sospechosos ni haga clic en un enlace que parezca sospechoso. Emotet no puede tener ese punto de apoyo inicial en su sistema o red si evita esos correos electrónicos sospechosos. Tómese tiempo para educar a sus usuarios sobre cómo detectar malspam.

- Aprenda y enseñe a sus usuarios sobre cómo crear una contraseña segura. Ya que está en ello, empiece a usar la autenticación de dos factores.

- Puede protegerse a sí mismo y a sus usuarios contra Emotet con un programa seguro de seguridad informática que incluya protección multicapa. Los productos para negocios y usuarios premium de Malwarebytes detectan y bloquean Emotet en tiempo real.

- Si su equipo está conectado a una red, aíslelo de inmediato. Una vez aislado, proceda a parchear y limpiar el sistema infectado. Pero aún no ha terminado. Debido a la forma en la que Emotet se propaga por su red, un ordenador limpio se puede volver a infectar cuando se conecta de nuevo a una red infectada. Limpie cada ordenador de su red uno a uno. Es un proceso tedioso, pero las soluciones de negocio de Malwarebytes pueden facilitarlo, aislando y desinfectando los terminales infectados y ofreciendo protección proactiva contra futuras infecciones de Emotet.

- Instale un programa completo de protección contra virus y malware, y haga que analice tu computadora regularmente en busca de vulnerabilidades. Esto te dará la mejor protección posible contra los últimos virus, spyware, etc.

- Si no está seguro de si un correo electrónico es falso, no corra ningún riesgo y póngase en contacto con el remitente. Si le pide que permita que una macro se ejecute en un archivo descargado, no lo haga bajo ninguna circunstancia y elimine el archivo de inmediato. De esta manera, no le dará a Emotet la oportunidad de entrar en su computadora.

- En caso de infección, siempre tendrá una copia de seguridad a la que recurrir y no perderá todos los datos de tu dispositivo.

- Haga que su computadora muestre las extensiones de archivos de manera predeterminada. Esto le permite detectar archivos dudosos, como «Photo123.jpg.exe», que suelen ser programas maliciosos.

En general se debe considerar las siguientes recomendaciones:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.

- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.

- Actualizar el sistema operativo de los equipos a las últimas versiones.

- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.

- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.

- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.

- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.

- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución

- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.

- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.

- Tener actualizado y utilizar, un software anti-virus

- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.

- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.

- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.

- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001/27002 en su control “Concienciación con educación y capacitación en seguridad de la información” o “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas

- Implementar un plan de respuesta a emergencias de la Organización/Institución.

- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- **Malwarebytes (2023)**. *Emotet.* https://es.malwarebytes.com/emotet/
- **Kapersky (2023).** *Emotet: La mejor manera de protegerte del troyano.* https://latam.kaspersky.com/resource-center/threats/emotet
- **Virus Total (2023).** https://www.virustotal.com/gui/home/search