Alerta de seguridad informática	2CMV20-00042-01
Clase de alerta	Fraude
Tipo de incidente	Phishing- Malware Emotet
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Enero de 2019
Última revisión	15 de Enero de 2019

NOTIFICACIÓN

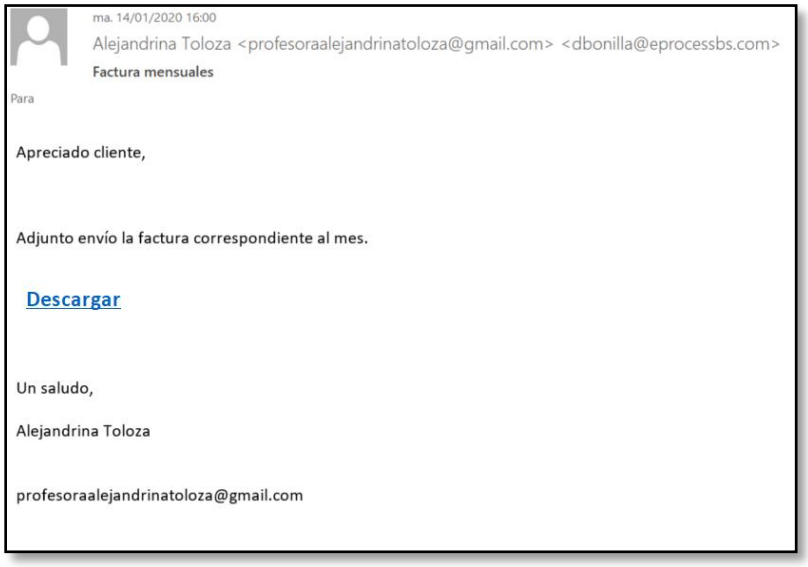
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con malware Emotet.

La campaña consiste en el envío de un correo cuyo mensaje hace alusión a una factura que se adjunta en el documento, sin indicar otros detalles. El objetivo es incentivar al receptor del correo para que seleccione el enlace. Al hacerlo se realiza la descarga de un archivo doc, el que una vez abierto desencadena una infección del malware comunicándose con otras URLs y servidores comando y control.

Imagen de Correo



Indicadores de compromisos

Sender
ferdiansyah@airpower[.]co.id
dbonilla@eprocessbs[.]com

Servidor Smtp
110[.]4[.]43[.]201 [spfilter-4[.]mschosting[.]com]
198[.]71[.]225[.]49 [a2nlsmtp01-05[.]prod[.]iad2[.]secureserver[.]net]

Url's Inicial:
http://asciidev.com[.]ar/mestiz[.]old/closed_disk/open_profile/5r7n1ez6n095l_8638708w3s0/

Descarga Documento:
Archivo : Untitled.doc
MD5 : 22fe3b70f2a0e5ef3f3bffa0f16ea916

Url Documento:
http[:]//fxkoppa[.]com/wp-admin/y2d4SsG
http[:]//mustuncelik[.]com/wp-admin/D3QY3136405
http[:]//www[.]forgefitlife[.]com/article/Ycan6NV2n6
http[:[//fabulousladies[.]info/8c8c022d0dd1523db4008ba9cf0d936e/ALPLsSy7p
http[:]//www[.]tiswinetrail[.]com/ifjza/enLL737

IOC Archivos de las URL
462dd8bb74e23e7d9b1ffb0689c5dd72

Comunicación C&C

51.77.113.100:7080
178.250.54.208:8080
45.55.82.2:8080
70.184.69.146:80
186.177.165.196:443
139.47.135.215: 80

IOC de Documentos relacionados SHA-256

ac14a7b6c8cb7923ee95db3a0468c0f19d1ce99cbe1d6ed5b0d130394bbde40b
de8bb6d0a58ccd3c237c42b39168d8ccee518c95f47c5d51dc97a19ea5b62d83
397a6c2bd325e0e53ff62af0b490f32b859e2f339ee3c49f69763225a70c3300
52c25ebb2e5ee3f2fc6b15e6559b883ba03bee153096e8e734c1087404268f7c
5273d76ad6441f4caba48d3a526da24b2b1903e1f28f56783def840b0bc445d6
d4101775c4d158f606095b84ac9df745a10e8df2a807b52caffb4c241cec10d7
53b1e4419026f8b3d712d63cffe8ecb677efb19b505082a2d9d0e6be6e83ecad
2510d4d55185c8ef165652f81739893cd7c04abf26113711856326a6ee9b8712
1461579364bf395ed7f04ba02b8a3feff767dac05703d0e8167db712038b927a
acc560ed1da89d2d60fb212db283c25d810aa6be0649f0cb7d356d26a7d7e907
bd6605dcc7f2dc1ed917ea678ea319a2f28dff1aeaeca1145de532a6d6729e11
879cf2433e705c1f05b900d9de1410e4cb1cdfada5a3a8616bca7f5ee8df7d53
fd3ff178db3097837f2ff687a0396dc9fdb4ebca0ed9701ea6bc50b0dec126a7
8b1d21b726bb50672c55bd728500228c64eb0140e70ec010631a63aa922ace30
3b8bc312e4c903c76b0c2dc2501b54801119b64775ebc98d569a10d3d1c8557c
0627097329fd133924f2784e6c4d9849d2b27b534aa4d8445e45c99a5d9622d4
55a90290c86c29608fd69aa880215b403ad936559b022c7b51117cd2a4e65f78
0cb8014d674cfe0b26052c265db5c5372765bbcce07a8873c7464156a4094645
a6b95df0d3361c12b0d7136227185ae8eeb0e0a7e8e3d1f555c96ff750bc7d58
498ba73b01d20bf622b233b774f02d1f612e4ac63f2a7147e50219cd2ca14a12
0fb50b5b206f00dd7262c5c93442db0ceae46f68721a7ed6f20c651af7bdd5a6
a829433d3680dde004e1188cb58af731f9b6ee1bb481af27a8f1dd24f6dc7510
b3832a3c4ae2d9be6a35c3ab9a728c2bff26fc14b864397741e6f1707b39e60e
faf25c52b64cbd04813d0328f5fe8ef887510d3b037f5d8db31b64526d3d3864
b249fd914ab266b32431e9802d894d43d117ad52e33be2f2491571008e6bdfef
e8c9580155c9cb3f8d8dab592e0201fbddd287e2fc24b70817f8bda493227e03
8242d37d4b31aabd27e87dfe62d4228c1b8fb2a272b120e24a1ef4d403547a8e
ef44b441fbba8e01cc787b846617ca105b50c5952a920fb7da70a4b3e3b31fbc
7f0f9632dd3dd3431dc47b5f7d5153de3bff25c7a17a619d6aff896d6e1e8068
e4a2fb5287ef2620ece2c90499b31d9b32d278abb562a7510cda42a965c2101e
b092928f774c770c21f0679ddf5994c6caca1795cf03bc84c1f181dfa8763a49
0c7825c80066650f70b7c1f56d287aae552fc2da9e2312e59df2543dbe55637a
7892b2b70752b1d2ea7e1130decbd5d193738e9de5683b058c1124aa6b8ad1f9
285f500998c7cffde0ed4c2898adaef16fef8f6679b2be40b697b4b6ade4495d
39bfeeabcf77b494d068ef3ac49576ebf99b16723fa1facf76e5b0b1752d99b4
b7c8a3e40105bd185fc5919dedc336a0f6c9a193ba36312490ca17aa2bb7d45e
c41155d2e8ce4ee09707a46b488e2bb2c03c051f64b3808a3e817e092902ca74

c66a18d443e024ac3f3f883c877343d82034dd3921c440b6483a88c60744e1c4
cc8fa601502880142e1c8612c271c5cc3f67807e972f3d813de99d3e12753a2e
7134c9d6237c6c981c13243360b5dfadf3709a3e52dd35e0c012850be32728e1
70a281040bf3f8d73c928eaf9bdc87e46a7387c9c4c236ccace12c5e9c55275a
ae4e6d36da90fe64bd8ef9703f9d6a61b93ab85453bb82c4e32d4bdef03e58c2
e645e5776b51f2c1ba8470db85b6badb937d35e2ad9366648ed9d4d62a77aa83
78735b699dc38bc91622fc2d0af4e6c2ee35989c4c31b1d2c8eb322c3d6ee39f
3a8a3b9858dbfaf6f6cb10e3a83470fb905871f61392e6bc8e3b31d091feaf5b
563a16757ae16bec1fd6952e8a57f005b0f52b4a5a95c71832c13e0228b3b51e
be40fbca15fec859b02c6b2a00b5cbdf8bda163521dffe036218d68dfe3f873e
ea5c9f7aac7989138196adfefe9b17d6b199ccbdcc76dbe93c4868d01df0c291
ddbd858ccc5362a0a6e6dbc2238ada1a79e1662e9f57beca3c8465cfb02d9430
ca2a635d82ac8a1279fb28d623336f851d520808d8ef30beb337ecfa0da26676
1d582853970da099ed41422a2f291fa2dccd5198b3017c168e4b700e5eaf7747
ac605dcda5c8653eb8b0437d6a161072253a981bf83a5611f7159316234bc9dd
6b78461e615852e383331a94abd73d16e11343be38e2cf23b74c57b3ec935327
63665d74c67914af0867a9cf3992a2f449b5e7722b62a924c5c9e61ca5615478
e39e188e3378f5c54f58a0f76f3a194372be94ffb4d4311a937c08a577b36e89
2e08996c6b2e945284298d12fa32aa2f9095d766e0b2e67f6f3b8e07ee541810
874a2092657b77033a7fb9677611920554961576l7b4db2272ca648fdeab1c06
e5e20816cdc86a953545ba6f6f83002794c133f92310988908a2e1ff634e1321
065493b240622fcf41ac821bac22caaeb283f6381f54dff213967797a7734600
b20588703ba75100bf3bca60339373b1493dc9cdfe320a6758c8b0f58671b95a
f049f771bdb9501f9bf0f2d6381914b4e4432c33778a4cb021e8e17eb05d0b5e
2a51a98de304c6a08d4418244985666b44e6066d0f94b888332164023efbafd6
eb486687c693b22b5bb67f13930ef5bbf2c794f3cc2199a659637c61398a6c29
41b1b931a506b54e225476fe1f5f9c849d632992642ce221f466e93bb666c841
09aaf59e8836f2b712c0394624b450ec5c3034c050c3c1aede62c93d43d4839e
85ebdcfd63f8661688778f89d0c7cc1638d26b8beb04ce71b650cccd0fe83069
fbaf39e19e8f1c3ae81e10de723b0faea6e2e77095a2af1ee9aad08666d02440
b3e54de9eb83f7893c5f002fe0b7f461cf72f0bcae7e43a68c07e2163f7ce82c

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.15 19:57:57 -03'00'