APT - C36
Phishing

26 de Febrero del 2019
CONFIDENCIAL

ATAQUE CIBERNÉTICO

NIVEL DE ALERTA: Muy crítica.

PHISHING

El phishing es un ataque que tiene como finalidad la suplantación de la identidad de una persona, entidad u organización. Este es un modelo de abuso informático que usa la ingeniería social para adquirir información confidencial de forma fraudulenta.

Desde A3sec se implementa este boletin debido a la cantidad de ataques tipo PHISHING que se han generado en el 2018 y 2019 a nivel mundial y nacional, con el fin de sensibilizar y capacitar a los usuarios.

Los atacantes utilizan principalmente vulnerabilidades de Microsoft Office para adquirir información confidencial de forma fraudulenta, se vale de CVE's como:

CVE-2018-0819

La herramienta Microsoft Office 2016 para Mac le permite a un atacante enviar un archivo adjunto de correo electrónico especialmente diseñado a un conjunto de usuarios en un intento de realizar un ataque Phishing, debido que en la herramienta Outlook para Mac detalla direcciones de correo electrónico codificadas.

CVE-2017-11882

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1 y Microsoft Office 2016 le permite a un atacante que ejecute código arbitrario en el contexto del usuario actual al no manejar adecuadamente los objetos en la memoria, también conocido como " Vulnerabilidad de corrupción de memoria en Microsoft Office ". Este ID de CVE es único de CVE-2017-11884.

y entre otros CVE referentes al tipo de ataque PHISHING como:

- CVE-2018-1654
- CVE-2018-12241
- CVE-2018-11067

- CVE-2018-15403
- CVE-2018-1704
- CVE-2018-1736
- CVE-2016-8609
- CVE-2018-5385
- CVE-2017-16652

PRODUCTOS AFECTADOS

- Sistemas operativos que cuenten con Microsoft Office

DESCRIPCIÓN DEL ATAQUE

Desde abril de 2018, se ha ejecutado un conjunto de ataques dirigidos contra instituciones del gobierno colombiano , así como importantes corporaciones en el sector financiero, la industria petrolera, la fabricación profesional, etc.

Los atacantes apuntan a la plataforma Windows y apuntan a instituciones gubernamentales y grandes empresas en Colombia.

el primer intento de ataque Phishing se detectó en abril del 2018 y desde ahí se han evidenciado numerosos correos maliciosos de este tipo. Los atacantes realizan un proceso llamado la pesca submarina el cual hace referencia a el envío de un archivo RAR protegido con contraseña para no ser detectados por la seguridad que tiene el servidor de correo. la contraseña se detalla en el cuerpo del mensaje del correo electrónico donde al abrir el archivo se identifica que es un documento tipo DOC basado en macros MHTML, lo que puede facilitar la implementación del movimiento lateral de seguimiento.

el atacante se centra en la inteligencia a nivel estratégico y también puede tener motivaciones para robar la inteligencia de negocios y las propiedades intelectuales.

Desde CSVD se han venido analizando correos de diferentes clientes para identificar los ataques Phishing y se identifica que la mayoría de documentos adjuntos tienen la siguiente presentación:

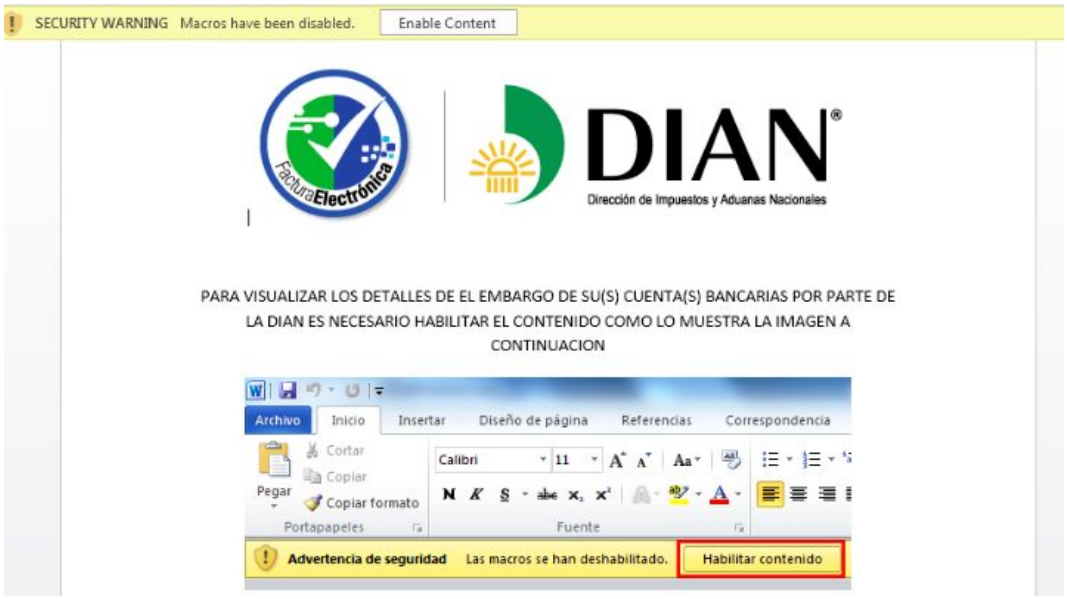


Imagen 1. suplantación de la DIAN.

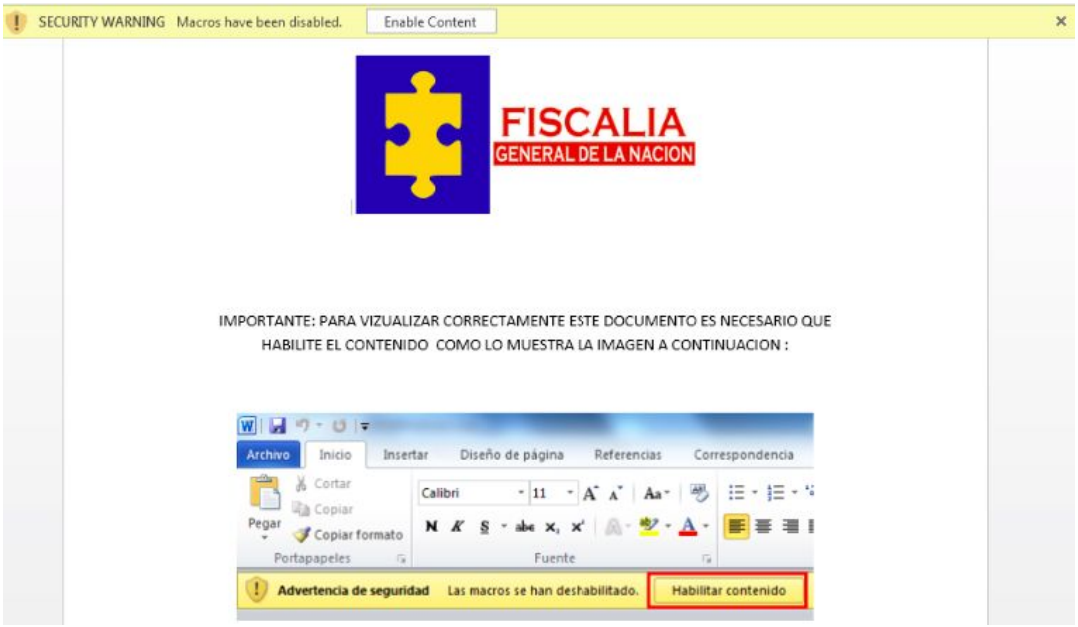


Imagen 2. suplantación de la fiscalía nacional colombiana.

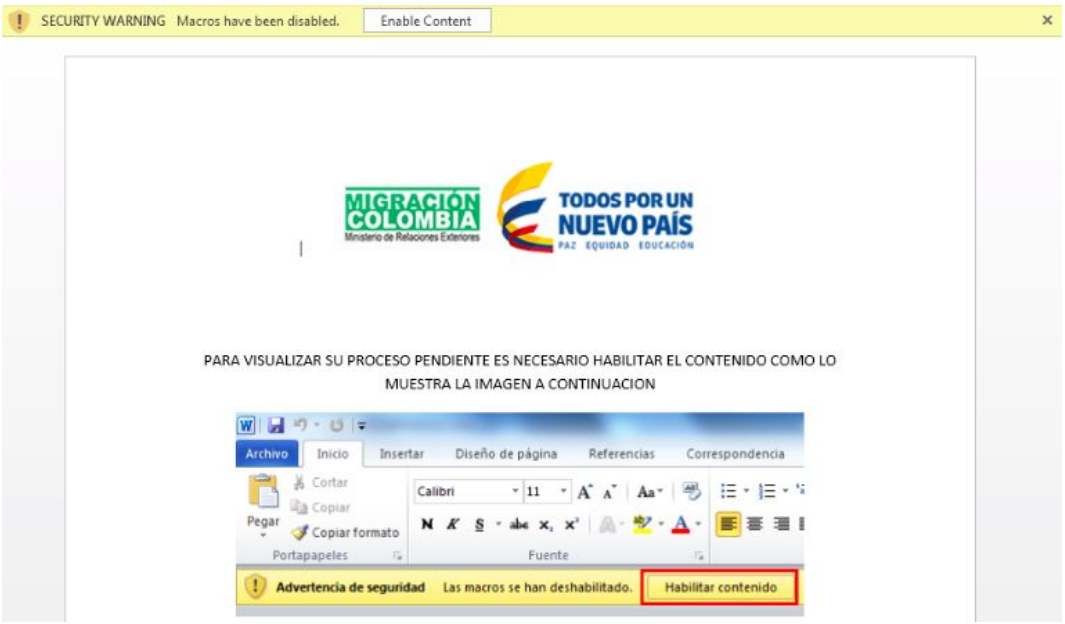


Imagen 3. suplantación de la migración colombiana.

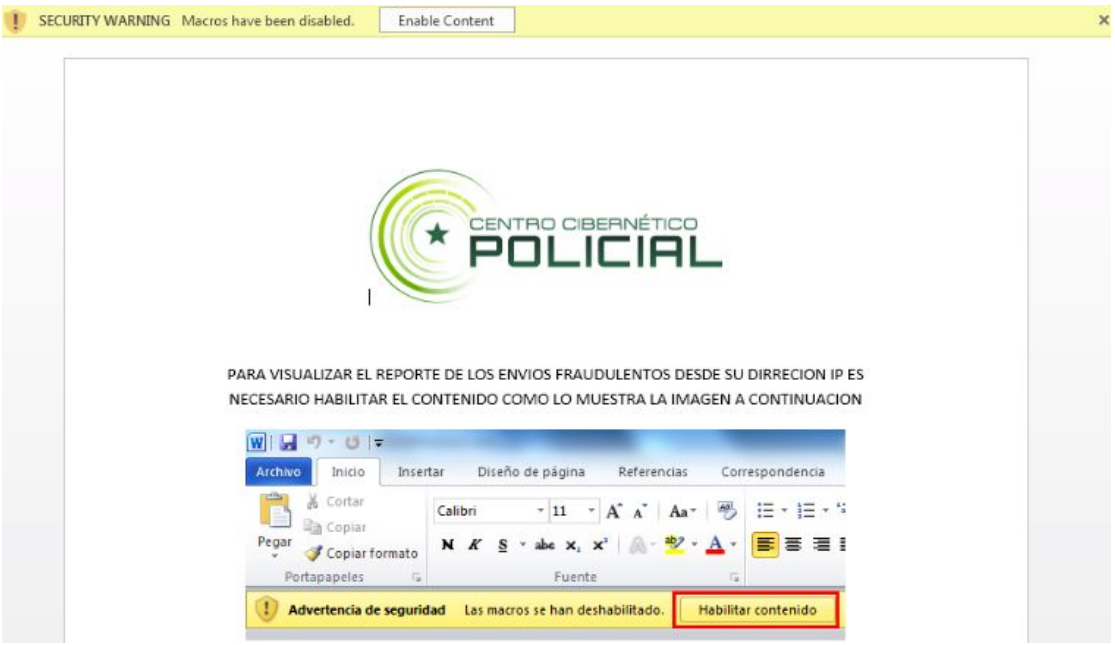


Imagen 4. suplantación del centro cibernético policial colombiano.

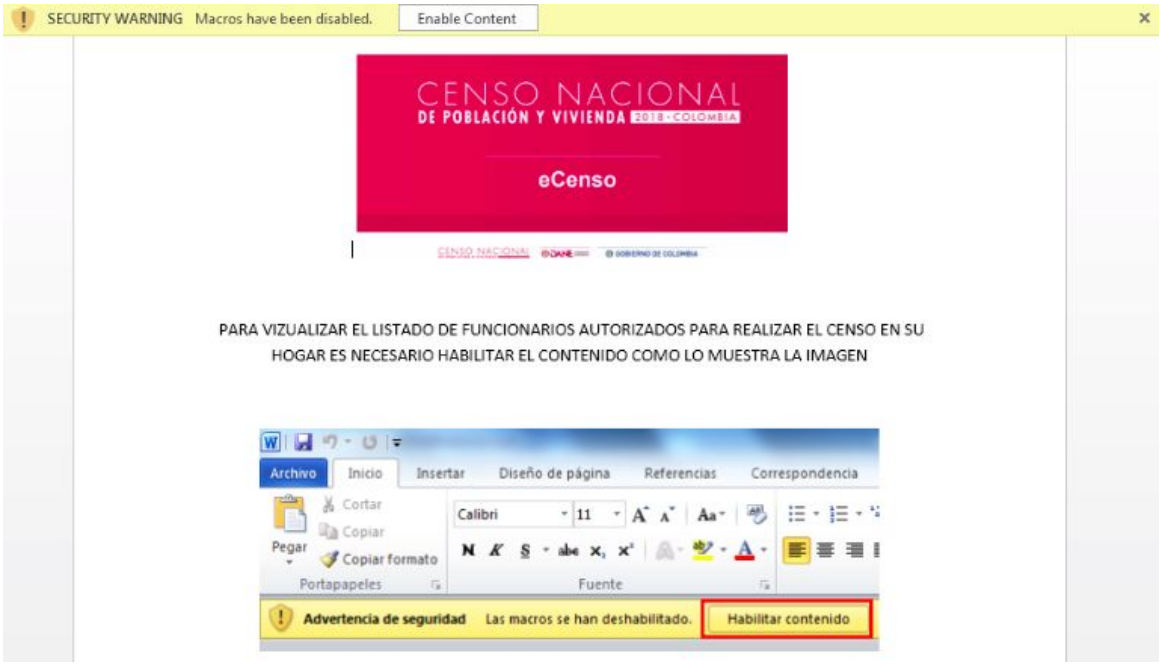


Imagen 5. suplantación del censo nacional colombiano.

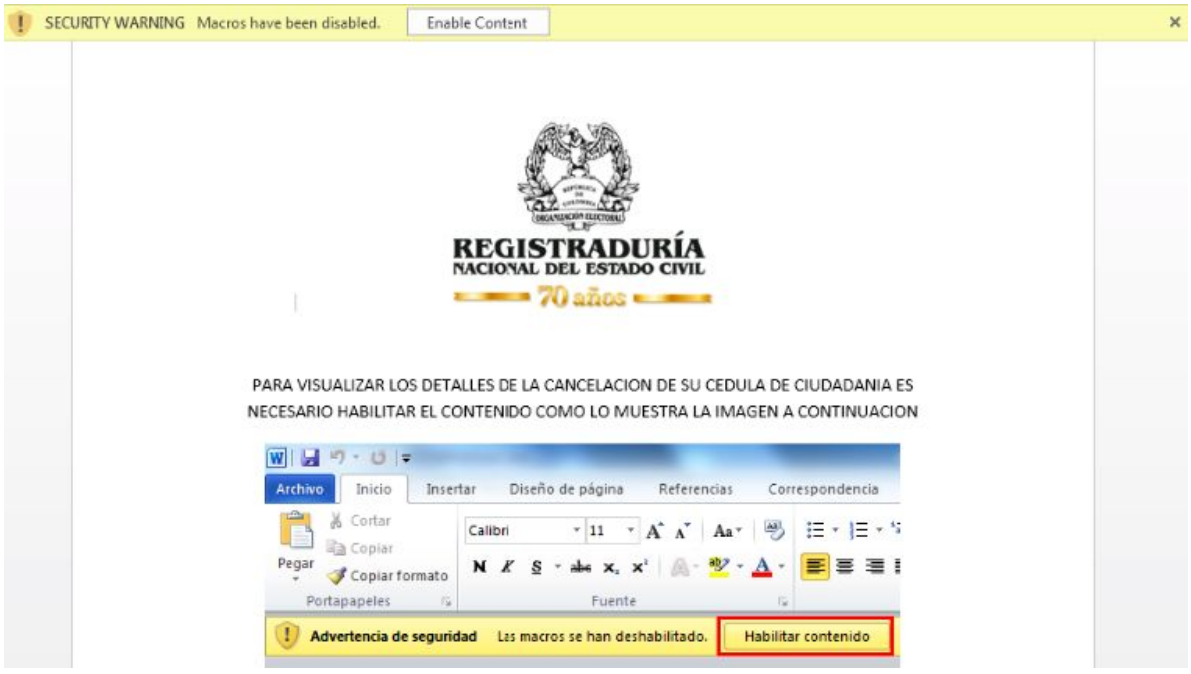


Imagen 6. suplantación de la registraduría colombiana..

La zona horaria desde donde realizan los ataque es UTC -4 el cual está relacionada algún país de América del Sur.

A continuación se relacionan los Indicadores de compromiso para el ataque APT-C-36 y otros ataques Phishing.

INDICADORES DE COMPROMISO

Tabla 1. IOC

Tipo	Indicador de compromiso	Nombre del archivo
Documento	0c97d7f6a1835a3fe64c1c625ea109ed	Registraduria Nacional - Notificacion cancelación cedula de ciudadania.doc
Documento	16d3f85f03c72337338875a437f017b4	estado de cuenta.doc
Documento	27a9ca89aaa7cef1ccb12ddefa7350af	455be8a4210b84f0e93dd96f7a0eec4ef9816d47c11e28cf7104647330a03f6d.bin
Documento	3a255e93b193ce654a5b1c05178f7e3b	estado de cuenta.doc
Documento	3be90f2bb307ce1f57d5285dee6b15bc	Reporte Datacredito.doc
Documento	3de286896c8eb68a21a6dcf7dae8ec97	registraduría Nacional del Estado Civil -Proceso iniciado.doc
Documento	46665f9b602201f86eef6b39df618c4a	Orden de comparación N \ xc2 \ xb0 5098.doc
Documento	476657db56e3199d9b56b580ea13ddc0	Reporte Negativo como codeudor.doc
Documento	4bbfc852774dd0a13ebe6541413160bb	listado de funcionarios autorizados para el censo nacional 2018.doc
Documento	51591a026b0962572605da4f8ecc7b1f	Orden de comparación multa detallada.doc
Documento	66f332ee6b6e6c63f4f94eed6fb32805	Código Tarjeta Éxito Regalo.doc
Documento	688b7c8278aad4a0cc36b2af7960f32c	fotos.doc
Documento	7fb75146bf6fba03df81bf933a7eb97d	Dian su deuda a la fecha.doc
Documento	91cd02997b7a9b0db23f9f6377315333	crédito solicitado.doc
Documento	9a9167abad9fcab18e02ef411922a7c3	comparendo electronico.doc

Documento	a91157a792de47d435df66cccd825b3f	C: \ Users \ kenneth.ubeda \ Desktop \ Migración colombia proceso pendiente 509876.doc
Documento	b4ab56d5feef2a35071cc70c40e03382	Reporte fraude desde su dirección ip.doc
Documento	b6691f01e6c270e6ff3bde0ad9d01fff	Dian Embargo Prima de Navidad.doc
Documento	cbbd2b9a9dc854d9e58a15f350012cb6	IMPORTANTE IMPORTANT.doc
Documento	cf906422ad12fed1c64cf0a021e0f764	Migración colombia Proceso pendiente.doc - copia.nono.txt
Documento	e3050e63631ccdf69322dc89bf715667	Citación Fiscalia general de la Nación Proceso 305351T.doc
Documento	ea5b820b061ff01c8da527033063a905	Fiscalia proceso 305351T.doc
Documento	eb2ea99918d39b90534db3986806bf0c	Proceso Pendiente Migracion Colombia (2) .doc
Documento	ecccdbb43f60c629ef034b1f401c7fee	Dian Embargo Bancario
Documento	ee5531fb614697a70c38a9c8f6891ed6	BoardingPass.doc
Documento	fd436dc13e043122236915d7b03782a5	texto.doc
Documento	bf95e540fd6e155a36b27ad04e7c8369	Migracion colombia Proceso pendiente.mht
Documento	ce589e5e6f09b603097f215b0fb3b738	estado de cuenta.mht

Tabla 2. IOC

Tipo	Indicador de compromiso
MD5s	0915566735968b4ea5f5dadbf7d585cc
MD5s	0a4c0d8994ab45e5e6968463333429e8
MD5s	0e874e8859c3084f7df5fdfdce4cf5e2
MD5s	1733079217ac6b8f1699b91abfb5d578
MD5s	19d4a9aee1841e3aee35e115fe81b6ab
MD5s	1bc52faf563eeda4207272d8c57f27cb
MD5s	20c57c5efa39d963d3a1470c5b1e0b36
MD5s	2d52f51831bb09c03ef6d4237df554f3

MD5s	30ecfee4ae0ae72cf645c716bef840a0
MD5s	3155a8d95873411cb8930b992c357ec4
MD5s	3205464645148d393eac89d085b49afe
MD5s	352c40f10055b5c8c7e1e11a5d3d5034
MD5s	42f6f0345d197c20aa749db1b65ee55e
MD5s	4354cb04d0ac36dab76606c326bcb187
MD5s	43c58adee9cb4ef968bfc14816a4762b
MD5s	4daacd7f717e567e25afd46cbf0250c0
MD5s	4e7251029eb4069ba4bf6605ee30a610
MD5s	50064c54922a98dc1182c481e5af6dd4
MD5s	519ece9d56d4475f0b1287c0d22ebfc2
MD5s	53774d4cbd044b26ed09909c7f4d32b3
MD5s	5be9be1914b4f420728a39fdb060415e
MD5s	5dee0ff120717a6123f1e9c05b5bdbc2
MD5s	60daac2b50cb0a8ugs6060d1c288cae2
MD5s	6d1e586fbbb5e1f9fbcc31ff2fbe3c8c
MD5s	763fe5a0f9f4f90bdc0e563518469566
MD5s	7a2d4c22005397950bcd4659dd8ec249
MD5s	7b69e3aaba970c25b40fad29a564a0cf
MD5s	8518ad447419a4e30b7d19c62953ccaf
MD5s	8ec736a9a718877b32f113b4c917a97a
MD5s	940d7a7b6f364fbcb95a3a77eb2f44b4
MD5s	9b3250409072ce5b4e4bc467f29102d2
MD5s	9db2ac3c28cb34ae54508fab90a0fde7
MD5s	a1c29db682177b252d7298fed0c18ebe
MD5s	a3f0468657e66c72f67b7867b4c03b0f
MD5s	a7cc22a454d392a89b62d779f5b0c724
MD5s	aaf04ac5d630081210a8199680dd2d4f
MD5s	ac1988382e3bcb734b60908efa80d3a5
MD5s	ad2c940af4c10f43a4bdb6f88a447c85

MD5s	afb80e29c0883fbff96de4f06d7c3aca
MD5s	b0ed1d7b16dcc5456b8cf2b5f76707d6
MD5s	b3be31800a8fe329f7d73171dd9d8fe2
MD5s	b5887fc368cc6c6f490b4a8a4d8cc469
MD5s	b9d9083f182d696341a54a4f3a17271f
MD5s	c654ad00856161108b90c5d0f2afbda1
MD5s	ccf912e3887cae5195d35437e92280c4
MD5s	d0cd207ae63850be7d0f5f9bea798fda
MD5s	df91ac31038dda3824b7258c65009808
MD5s	e2771285fe692ee131cbc072e1e9c85d
MD5s	e2f9aabb2e7969efd71694e749093c8b
MD5s	e3dad905cecdcf49aa503c001c82940d
MD5s	e4461c579fb394c41b431b1268aadf22
MD5s	e770a4fbada35417fb5f021353c22d55
MD5s	e7d8f836ddba549a5e94ad09086be126
MD5s	e9e4ded00a733fdee91ee142436242f4
MD5s	edef2170607979246d33753792967dcf
MD5s	ef9f19525e7862fb71175c0bbfe74247
MD5s	f1e85e3876ddb88acd07e97c417191f4
MD5s	f2776ed4189f9c85c66dd78a94c13ca2
MD5s	f2d81d242785ee17e7af2725562e5eae
MD5s	f3d22437fae14bcd3918d00f17362aad
MD5s	f7eb9a41fb41fa7e5b992a75879c71e7
MD5s	f90fcf64000e8d378eec8a3965cff10a
Dominio	ceoempresarialsas.com
Dominio	ceosas.linkpc.net
Dominio	ceoseguros.com
Dominio	diangovcomuiscia.com
Dominio	ismaboli.com
Dominio	medicosco.publicvm.com

Dominio	mentes.publicvm.com
URL	http://ceoempresarialsas.com/js/d.jpg
URL	http://ceoseguros.com/css/c.jpg
URL	http://ceoseguros.com/css/d.jpg
URL	http://diangovcomuiscia.com/media/a.jpg
URL	http://dianmuiscaingreso.com/css/w.jpg
URL	http://dianportalcomco.com/bin/w.jpg
URL	http://ismaboli.com/dir/i.jpg
URL	http://ismaboli.com/js/i.jpg

Tabla 3. IOC

Tipo	Indicador de compromiso	Contraseña
Archivos RAR MD5s	censonacionaldepoblacion2018307421e68dd993c4a8bb9e3d5e6c066946ro	592C9B2947CA31916167386EDD0A4936
Archivos RAR MD5s	documentoadjuntodian876e68dd993c4a8bb9e3d5e6c066946deudaseptiembre	A355597A4DD13B3F882DB243D47D57EE
Archivos RAR MD5s	procesofiscalia30535120180821e68dd993c4a8bb9e3d5e6c066946se	77FEC4FA8E24D580C4A3E8E58C76A297
Archivos RAR MD5s	migracioncolombia	0E6533DDE4D850BB7254A5F3B152A623
Archivos RAR MD5s	credito	F486CDF5EF6A1992E6806B677A59B22A
Archivos RAR MD5s	421e68dd993c4a8bb9e3d5e6c066946r	FECB2BB53F4B51715BE5CC95CFB8546F
Archivos RAR MD5s	centrociberneticoenviosipfraude876e68dd993c4a8bb9e3d5e6c066946octubre	19487E0CBFDB687538C15E1E45F9B805
Archivos RAR MD5s	fiscaliadocumentos421e68dd993c4a8bb9e3d5e6c066946agosto	99B258E9E06158CFA17EE235A280773A
Archivos RAR MD5s	20180709registraduria421e68dd993c4a8bb9e3d5e6c066946r	B6E43837F79015FD0E05C4F4B2F30FA5

RECOMENDACIONES

Técnicas

- Ejecutar fullscan de la estación de trabajo del usuario al que le llegó el correo electrónico, descartando posible instalación de software en una segunda instancia.

- A todo archivo que venga anexado a correos de dudosa procedencia realizar previamente una prueba de malware antes de ejecutarlo o abrirlo, estas pruebas se pueden hacer en Virus total con la siguiente direccion web: https://www.virustotal.com/es/

Gestión

- Ejecutar cambios de contraseña periódicos de los correos corporativos; si es posible crear una política de expiración de contraseñas.

- Prestar atención a el remitente del mensaje y al aspecto del mensaje; si nunca ha recibido correos electrónicos de dicho remitente y el asunto del mensaje puede que no tenga relación con su funciones en la organización, posiblemente no será legítimo.

- NO hacer uso de la cuenta corporativa para recibir información diferente al ámbito estrictamente laboral, de lo contrario se estaría comprometiendo las cuentas de correo corporativo de los demás colaboradores y facilitando una posible distribución de malware, phishing, spam.

- Realizar jornadas de sensibilización, relacionadas con el buen uso de los recursos que ofrece la compañía, y fortalezcan los conceptos básicos de seguridad de la información.

ACCIONES TOMADAS POR EL CSVD

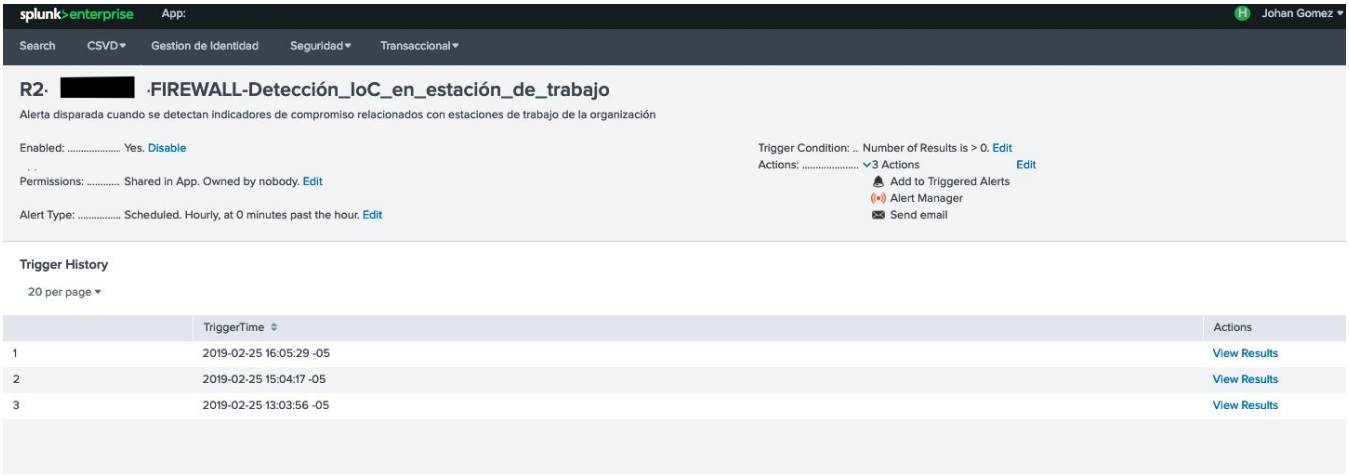
Desde el csvd se realizan las siguientes acciones:

- Actualizar la base de datos de los indicadores de compromiso donde se detallan los dominios, URL, hash y posibles archivos maliciosos mencionados en la sección de (IOC)

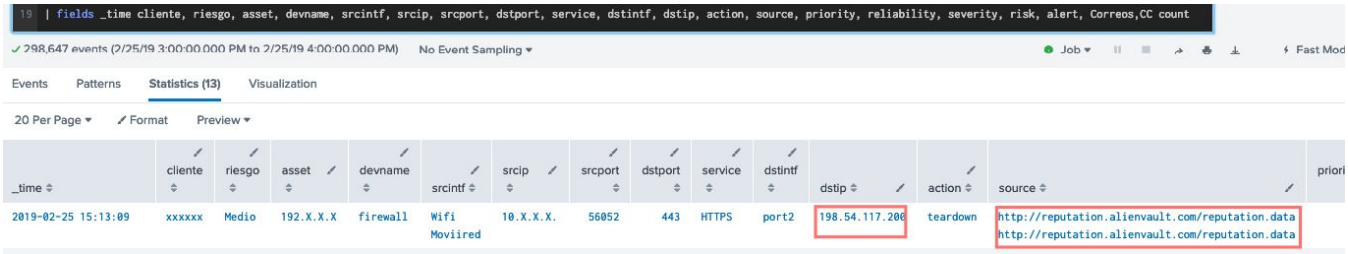
reputacion

entity	type	direction	source	notes	date
212.7.220.13	IPv4	inbound	http://www.projecthoneypot.org/list_of_ips.php?rss=1		2018-03-19
151.106.4.113	IPv4	inbound	http://www.projecthoneypot.org/list_of_ips.php?rss=1		2018-03-19
146.185.223.197	IPv4	inbound	http://www.projecthoneypot.org/list_of_ips.php?rss=1		2018-03-19
212.7.220.14	IPv4	inbound	http://www.projecthoneypot.org/list_of_ips.php?rss=1		2018-03-19
212.7.219.198	IPv4	inbound	http://www.projecthoneypot.org/list_of_ips.php?rss=1		2018-03-19

- Realizar un filtro y una alerta a través de la herramienta Splunk para identificar los IOC desde la base de datos anteriormente nombrada.



- Reportar a los clientes que se le identifique tráfico desde o hacia alguno de los indicadores de compromiso relacionados, para que así realicen un plan de acción frente a este ataque.



REFERENCIAS

https://otx.alienvault.com/pulse/5b9319c69116e533bfe27246/related
https://otx.alienvault.com/pulse/5c6aed104866631cac8227b1
https://ti.360.net/uploads/2019/02/18/dde2665fc91bd4f9f67a9c43fbb59db2.png
https://otx.alienvault.com/pulse/5c73bcb52d99fb13b55e2e6c
https://otx.alienvault.com/pulse/5c7309dde3e36621a07a3f20
https://otx.alienvault.com/pulse/5c72579e1a83e435c55f00ae
https://otx.alienvault.com/pulse/5c707e1e99222a092bbb98a4

A3Sec España C/ Aravaca, 6, 2do Piso, 28040 **Madrid, España** **T**.+34 915330978	**A3Sec México** Shakespeare 30, Piso 2. CP. 11590, **CDMX, México** **T.**+52 55 7822 8093	**A3Sec Colombia** Carrera 49A # 94-76 Ofc. 304, Castellana **Bogotá DC, Colombia** **T.**+57 1 3099533	**A3Sec USA** 1401 Brickell Ave # 320, FL 33131, **Miami, USA** **T.**+1 7865569032