Alerta de Seguridad Informática (2CMV-00015-001)

Nivel de Riesgo: Alto

Tipo: Malware Grupo TA505

Fecha de lanzamiento original: 05 de Julio de 2019 | Última revisión 05 de Julio 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.

Ataque del Grupo TA505 nuevas familias de malware

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha observado varias campañas de phishing con el actor TA505 (nombre asignado por Proofpoint). Este grupo utiliza los troyanos bancarios Dridex y Locky ransomware y Rat. En los últimos análisis se ha observado en sus ataques otras familias de malware como FlawedGrace, FlawedAmmy y ServHelper. Según investigaciones de TredMicro estos ataques se han observado en los países como Emiratos Árabes Unidos, Arabia Saudita, India, Japón, Argentina, Filipinas y Corea del Sur. CSIRT también ha identificado campañas en Chile.

Los atacantes utilizan como vector de entrada los correos electrónicos para poder infectar los equipos, el correo electrónico que contiene archivo adjunto como Word o Excel y URL'S maliciosas. Al ser ejecutado el documento, se instala automáticamente una función macro que ejecuta un proceso y, a su vez, descarga un archivo MSI, el cual ejecuta otro ejecutable en la memoria para luego tener comunicación con server comando control.

Indicadores de Compromiso

Urls

http[:]//172.104.117.15/02[.]dat
http[:]//fakers[.]co[.]jp
http[:]//fakers[.]co[.]jp/20.06.2019_115.91.doc
http[:]//fakers[.]co[.]jp/20.06.2019_130.22.doc
http[:]//169[.]239.129.61/k1
http[:]//185[.]140.248.17/01[.]dat
http[:]//185[.]140.248.17/lt1
http[:]//carpc[.]si/OZ00488941.xls
http[:]//fakers[.]co[.]jp/20.06.2019_130.22.doc
http[:]//greenthumbsup[.]jp/20.06.2019_746.38.doc
http[:]//lancehugginsltd[.]co[.]uk/Attestation_impots.xls
http[:]//lidovemilice[.]unas[.]cz/Payment-503_Copy.xls
http[:]//medastr[.]com/docs/s.php
http[:]//nagomi-753[.]jp/20.06.2019_800.77.doc
http[:]//nanepashemet[.]com/20.06.2019_781.37.xls
http[:]//waiireme[.]com/20190706_983782.xls
http[:]//waiireme [.] com/t3

hashes (SHA256):

- 8681cd7285b83cc3174b09f3ec9a5b530bc2df2828f6e8b45efac57bd8ebeec4
- bb7930f3b5fa0079c3e5b13814642a58264845053b6a0000259592590d789d3e
- 1c3b554cc0f3a439c68fcd4918f786d94684db559e6cf71732edfabcc511f39b
- 7c0bd405ec793b1cefd6679601507ffbe9c39232b773dfcb44817ff893e43570
- e72a88c8b388ebf51bb6a43813e9d39ab12e18468c81af7e8eaa4a0903a43453
- b2ab1a485306bb25f75ad94f334ea5ad829b4d6339324575e04d3d6a18ff8b3f
- ad690ac440f04c2c65fd0ef23733233f843ceba7cea63639427733a022cd2900
- 04dc61982a30cda86e384067a014eafb2731d0e1cfe0e6d84fa169728342f44c

- 7229077c46a401744eddce418fc0ae8eac8911f601790b6fe0d5697c4c0fdf7f
- a376e884f0cb39739fa42ebe6360f5432ea83325edcedc79492e8771609f9f90
- 84c9d273bb96bc7156ac7208052f209f59dee914a18043bbe01c5d291fea9b9c
- 88d530875e304e816f1d671dc8a8c6fc553c7c888ede4a28d1b57ef7acbb8203
- 967b13a9ceb1df74b6762b7caf4584bced414e9e3b11869e13a980d65c709049
- 191a3e9abe1cedcddbf87e1401ad93d883bb144871e670c6bec839166972c5ce
- 8480e977c37d74845cd79b3f197f4f98f8572217da49e6465781669579371f3d
- 26031f6f39330fe57d15a508bf43fa2dcf3b7d40331ee3edb92d2b7f36dd53d2
- f8443efe64d7c59a18fdbebbac5f5d7124b996743829b6af9763f9403b02dcd1
- fea784dce451d4ebb7915d9dd7e4ff596f6596837dd030a4943038e2d7683aa9
- d5221fe3e9be43cf1c3f0cb5f0e3c9e953881a7a901c64e35eb3b33841e4e700
- 6dc2aef8ede6d3c32dc6164b595bfa48a55a6b647d12ffc3c522418cd08f36d0
- 6c653797bca0b191069dc7e831903ccf80ddcff5aae4e63924d31243bd549f88
- f089e28a8b2eae2e3e9ecbe78fa8d2dd3d7312857ae2a3874bb000b8c6dbdb66
- d005e2ec227c0eb5a28d9b6c61b89aba2dd8225eea65a2139aa10aaf37151af5
- 275af657efaa4b2f521b50d2855bf9ee475c97ab5af8de1dc38151c00fead536
- 45369be785d9c96e941dff4cf1ce4a7cad2adb1c94ed5a5e69c706632964f922
- a187c795435a35dd5823f74f6e28961894a70e5201502828f2e100f62c9123ad
- 4a2479569d727f1f8cad707761f412764abfc30446aac706393ff60f8d2c9671
- 98588ed38fd102048adf936453e9d2ba4be6f02a037a3f31b00ab0f8ed3af3ca
- 1b10483fe533d5f96698d5a70fe4b2e8221be75b365d49150523decaece294fb
- 0412e43c8becaccb2c7570ff5f0d913f012d0cb1cc49819cd6d3bdc285c0bb0d
- 5f8055c51ea566db33aaccca33eeae6bbb750ff1e5dd08604b0d4452f0e6dc6e
- 4fc2139adb66fca1a8e8521f390f9aac06e2d767146b8c58942c5bd82ba8c9c3
- fa6b2c2dc726e23281a0bc05880ef65c9562f80c41a763ceb8f31262fb6a177d
- 637bfe39c6e604af8cec8a54d4e6f05a79ea2d09b279ccc1fcc59b434bd89ce6
- 0f5cc1adf562b4f715e17ad08ba2aeab42abc5e6b6c5af31e46d2237ab094394
- 0fdaa02a1bcdfed33190f3b9646d6f5969ce38c59a1e3aed69218c1c4f7b3345
- 6b66d07d53c2af5b71f1cd303fa7ac8f304b36a6711cbf42a5b3f92a4a9c9383

- 6f0595aca720ab0568064f923a121311b6332c59bff558e8145133cfffc1738b
- 61efa10454c64d4109b196c37e2f1ed356f851458b96d1a699d6b851cd1105b5
- 3e56f20d3787dabeacd564641c2847f0ba2d2bbff160529d423f3508e5719dac
- 300dfa1f4ddc61567c9f9bdf38e2a3c36723350c0333019777ab778ad816a3d7
- 3270a39fa36ab84a6877a297fce077e784ff5d562227384f7e2759fd55e12d13
- 6cc9accb6b6f954b81fcec22f8229d970ce661ac72816315e2800e32261456e5
- c4963dcf6b32459740f6a3d3b4d06d9dc06f15087ca01775956df36206543301
- 98b584b31457b21d0d48fcc78093439638e15dd1705e54182d9aa4ffad014c3a
- 59af9102a921130fd1d120f6cee7fc7cdfc28292a7a4a8c24233126604aa9443
- a905838db6e6617edd9d25baaaaee9c209381d456e809081977e27c3e0b15793
- 8621fa54946096ed38aee5cbcc068c0620416a05c17328a527673e808847850d
- 3e3eb26211459eb2d8b52a2429a52e7e12d2145d7733823d7415663537a0b6ca
- f21039af47e7660bf8ef002dfcdb0c0f779210482ee1778ab7e7f51e8233e35c
- eb3792fc83cd65823bc466e7253caf12064826b058230666d2ed51542ac59275
- d0aaf465a2569abbdcbafc049be1c1a643572f4ca185058833310435bfa53358
- 52f0aaff3654110e82586d21b07c8a3de23dc9efb3f4001daf412286282315c0
- 1d72cf3dc189aaf3fd5c5118dd9811ae00178e7f04c3798b5d0a61386ae83750
- 13e9854a6dbb10e47c1c975ead8cca4591f1360ebf36d8956a8f64b654d3be86
- 2a98c5731ccdfef930bedbafe36ac04f6396c6d0218e2d13ac8818d7ca94380b
- b1f84a20ad0de42a0b0b5fe6a15bc91cdfa94ebb891d55dd1661e2bcd47b0ed0
- efd2eb9a5823e7860874ca76da492da62eb14bd6a643f663bd9caf756d33ca72
- a40426b8da80c4b6f8c1a25e2e6cdb9cf689cc19bc22d0789707b7b708eebb74
- 4c47a56bb1107228fdbdbb1ea2e81c06cf02da587c9c1f95d655b539b5d0d93b
- a8a0783c3fda32bab275587add639dfd5cb7426353d15d290a681984d15f45af
- 30d4c652343e677ad6654a9475bb2f542e01816cdd865c7e1913f86d14a1374d
- 89222cd3b62c1e8248c238a194d15cb0d0ff7c63a6b3952d67418336ff713a65
- 10f163f27391c8a9cae6676af2871604b34fbc0cff548b086cd5d1cfe1007949
- b6625c687cd73081ea738789484a0bad2196948153fc655cc9a3aeb7c331265f
- 336acec1e66e32d3a9c49c4e3ed18d5f01298aa95a2812bb1c2aa26e8b741c86

- c7f3179f33d72f0c6b98677da164cc2782e6e34defdea52e9e6ef201037f4c4a
- 654400c9b8b3013e173216e4dd77e163ab4d7a0402073be8d90bebdf8638ca45
- 659ed2c469dad1dc6c04b03a7569fce2c95ddf9c0ca39e98b976ce90cc944ec7
- d8fb098ef12be82ea8aba08fa9151c4a77b3f819f7f751854190e81fde688a14
- a14996d03910ee172d91bf94d3a3c1ef054fb834897c5df542b6bc2c6f01f254
- 8c5847b69303e10c7e83c9477cda730c2a135d1f10680635c5c2236de1dc927a
- e438038987042b012fa9d14577908803b0347a78943037a9b7932b1d0428ac6c
- ebb50213ccfb549dab01a1d43c23f8c9ee59cac794981a1118d914af4a78daa9
- 998c9438906333a841dcc4a040c5c123df39065255bf6493556a05eb280f8ea1
- 1e46bebec971784cf979153658b106a8bd38194f26230910d4d76a05bc8e8b75
- 550ff326065e9e0268dde0d50824f2718ed9bf18f806954e392e7abc02d50f3d
- bf94b27711ac9e883d8eb33eb1f214ea349f8197f90ac7192481e76e914bc069
- 8de14182d3db1a7cf02954f7711c87158a75b1942df3e11d153c2d6c199253bc
- 3b95a5413f22d059ffd33e0d006a72b289a8bd217b29507ed7e4dbca128d4ce9
- 549027f502086099542a25c31a75e6323dd833b282d5c8dd34e62d3c7782bfff
- c0b4b68afd9c243335c7c8b3e59645d0b8c9dd2edfd358f8236de5b8faf51be1
- 9f191d1ef69bb69e0b833f835b2fa0ebc7e11496bfe52003696005acc2c3594b
- 84781b14ac7468316035bad33ecccf48632d03f4a932b2098ca5214fe64c7b29
- 9a1d94768549478d726acf3f28e068b7e7bed3fc047d08e9cff16da550111291
- c9b5b1b41eb60d0b53fdfd1788e19e448539ba72eee54b28db06d28ee77de47e
- 6f420ff5cfa67d2cbe93417700d0fe433e05d7b071f98dd755fbcb51b1c0d337
- a8bb5f66eb11e191972fd4b067db35ce73317b9f3b07aea503dfbce2fbe14ea8
- 4555d0293b00a1d3e7c0da05b874a99d52e0448a5d764477f244abd0a7151a14

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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
- Actualizar los antivirus a sus últimas versiones y base de datos de protección
- Mantener campañas de educación sobre phishing a organizaciones
- No desactivar funciones de seguridad de antivirus u otro sistema de protección

Fuentes adicionales para la elaboración de este informe:

- https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south

- https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new-malware-tools-gelup-and-flowerpippi/

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob