ACTOR DEL MES

Tendencias | Operaciones | Noticias | APTs

Nota de la redacción

Durante estos días tan duros que estamos viviendo y bajo una situación nunca antes vista queremos desearos lo mejor y esperamos que estéis bien tod@s. Para intentar amenizar la cuarentena desde Derecho de la Red hemos pensado qué puede interesaros el siguiente formato, que englobará toda la información sobre los tres actores que hemos analizado hasta ahora.

Así, a modo de informe, siempre podréis tener la información disponible para vuestra visualización, estudio o consulta de manera gratuita.

De cara a futuras publicaciones vamos a realizar una colaboración con otras comunidades. Intentando así traeros un contenido de mayor calidad tanto en estas publicaciones como en los reportes mensuales.

Estos cambios se irán introduciendo poco a poco.

¡Muchas gracias por tanto! Y recordad, sin vosotros lectores, no somos nadie ;)

Agradecimientos a Julio San José, por su inestimable ayuda y apoyo durante todos estos proyectos y los que vendrán.

Os compartimos nuestros canales oficiales en un acto de spam del sano :P

- Canal principal: https://t.me/DerechodelaRed
- Canal CTI: https://t.me/cti_espana
- Canal información COVID19: https://t.me/CORONAV1RU

Lazarus Group

Actor del 24 de noviembre de 2019, Luis Diago de Aguilar.

Presentación

Este es quizás uno de los actores más famosos. Supuestamente se encuentra bajo financiación del gobierno de **Corea del Norte**.

Empezó a actuar sobre 2009 más o menos, según la fuente en la que nos fijemos y, el grupo, se divide luego a su vez en varios subgrupos:

- **BlueNorOff**
- **APT38** (un actor muy relevante y destacado)
- **AndAriel**

Se les relaciona con ataques a compañías como: **Sony Pictures**, **Samsung**, **SWIFT** e **instituciones financieras**, entre otros objetivos.

Operaciones

Durante la realización de este artículo hemos encontrado una serie de informes sobre estas operaciones, os los dejamos junto a la lista de operaciones. Sinceramente, son unos **informes imprescindibles**.

- Operación Troy 2009
  - https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
- Ten Days of Rain 2013
  - https://www.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf
- Sony 2014
- Operación Blockbuster 2016
  - https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf

- Ataques con **WannaCry** 2017
  - https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
- Ataques contra entidades financieras 2017
  - https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/
  - https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/
- GhostSecret 2018
  - https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/
- También se les ha visto actuando sobre 2019

Malware asociado

A este grupo se le atribuyen, entre otros, los siguientes **malwares**, algunos de ellos vistos en el apartado anterior:

- **Tdrop**: con afectación a Windows 7. En el marco de la Operación Troy.
- **Tdrop2**
- **Destrover**: con varios objetivos, entre ellos Sony. En el marco de la operación Blockbuster.
- **FALLCHILL**: Operación GhostSecret, con objetivos como el FBI o defensa.
- **Volgmer**: Operación GhostSecret. Contra el gobierno de EEUU.
- **Wcry** (WanaCrypt0r, WanaCrypt0r 2.0, WanaCryptor, WannaCry, WannaCry 2.0, WannaCryptor, Wannacrypt).
- **HANGMAN**
- **SpaSpe**

Virus Total

Vamos a dejaros algunas referencias a Lazarus que hemos podido encontrar en VT de los últimos 30 días que se atribuyen a este actor:

- https://www.virustotal.com/en/file/18f0ad8c58558d6eb8129f32cbc2905d0b63822185506b7c3bca49d423d837c7/analysis/
- https://www.virustotal.com/gui/file/a7ff0dfc2456baa80e6291619e0ca480cc8f071f42845eb8316483e077947339/detection
- https://www.virustotal.com/gui/file/ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d/detection
- https://www.virustotal.com/gui/file/9a78bbc6d05a7e67e1abfa4ecbc275fb20fbe0b06f73f9a524ba656101e7841e/detection

Podríamos seguir añadiendo una lista enorme, es por ello por lo que hemos puesto solo los más recientes que hemos encontrado.

IOCs

Ahora vamos a poner una lista de algunos de los indicadores de compromiso en este caso del WannaCry:

8A4D2BAA8CF519C7A9B91F414A0A9D8BA2B9E96D21D9E77DA7B34ED849830A36	mks.exe
CA8DC152DC93EC526E505CF2A173A635562FFBF55507E3980F7DC6D508F0F258	hptasks.exe
2A99BCB5D21588E0A43F56AADA4E2F386791E0F757126B2773D943D7CBF47195	ENTASKLOADER.EXE. Creates forti.exe
3C86FC0A93299A0D0843C7D7FF1A137A9E799F8F2858D3D30F964E3C12C28C9E	forti.exe
92b0f4517fb22535d262a7f17d19f7c21820a011bfe1f72a2ec9fbffbdc7e3e0	javaupdate.exe, creates g.exe
3C86FC0A93299A0D0843C7D7FF1A137A9E799F8F2858D3D30F964E3C12C28C9E	g.exe
91146EE63782A2061701DB3229320C161352EE2BC4059CCC3123A33114774D66	svchost.exe, Creates lsasvs.exe
A7EA1852D7E73EF91EFB5EC9E26B4C482CA642D7BC2BDB6F36AB72B2691BA05A	lsasvs.exe, Creates 50793105.exe
7F8166589023CD62AE55A59F5FCA60705090D17562B7F526359A3753EB74EA2F	50793105.exe, Creates taskhcst.exe
043E0D0D8B8CDA56851F5B853F244F677BD1FD50F869075EF7BA1110771F70C2	taskhcst.exe, WannaCry
92B0F4517FB22535D262A7F17D19F7C21820A011BFE1F72A2EC9FBFFBDC7E3E0	armsvc.exe, javaupdate.exe
524F8F0F8C31A89DF46A77C7A30AF5D2A1DC7525B08BFAFBED98748C3D8A3F1C	jusched.exe
41E9D6C3374FD0E78853E945B567F9309446084E05FD013805C70A6A8205CD70	msinj32.exe
436195BD6786BAAE8980BDFED1D7D7DBCCCB7D5085E79EBDCC43E22D8BAE08A8	goyqsvc.dll
9F177A6FB4EA5AF876EF8A0BF954E37544917D9AABA04680A29303F24CA5C72C	exldcmgmt.dll
AE8E9FF2DC0EC82B6BAE7C4D978E3FEAC93353CB3CD903E15873D31E30749150	oledbg32.dll
FC079CEFA19378A0F186E3E3BF90BDEA19AB717B61A88BF20A70D357BF1DB6B8	bitssvcs.dll
2BA20E39FF90E36086044D02329D43A8F7AE6A7663EB1198B91A95EA556CF563	00bebc12.exe

Más hashes de malware

02f75c2b47b1733f1889d6bbc026157c
06cd99f0f9f152655469156059a8ea25
07e13b985c79ef10802e75aadfac6408

09a77c0cb8137df82efc0de5c7fee46e
0abdaebbdbd5e6507e6db15f628d6fd7
16a278d0ec24458c8e47672529835117
17bc6f5b672b7e128cd5df51cdf10d37
198760a270a19091582a5bd841fbaec0
1bfbc0c9e0d9ceb5c3f4f6ced6bcfeae
1d0e79feb6d7ed23eb1bf7f257ce4fee
268dca9ad0dcb4d95f95a80ec621924f
2963cd266e54bd136a966bf491507bbf
2de01aac95f8703163da7633993fb447
2ef2703cfc9f6858ad9527588198b1b6
3b1dfeb298d0fb27c31944907d900c1d
459593079763f4ae74986070f47452cf
474f08fb4a0b8c9e1b88349098de10b1
579e45a09dc2370c71515bd0870b2078
5d0ffbc8389f27b0649696f0ef5b3cfe
5ebfe9a9ab9c2c4b200508ae5d91f067
5fbfeec97e967325af49fa4f65bb2265
6eec1de7708020a25ee38a0822a59e88
7413f08e12f7a4b48342a4b530c8b785
8387ceba0c020a650e1add75d24967f2
85d316590edfb4212049c4490db08c4b
949e1e35e09b25fca3927d3878d72bf4
954f50301207c52e7616cc490b8b4d3c
9d1db33d89ce9d44354dcba9ebba4c2d
ad5485fac7fed74d112799600edb2fbf
b135a56b0486eb4c85e304e636996ba1
b9be8d53542f5b4abad4687a891b1c03
bbd703f0d6b1cad4ff8f3d2ee3cc073c
c1364bbf63b3617b25b58209e4529d8c
c635e0aa816ba5fe6500ca9ecf34bd06
cb65d885f4799dbdf80af2214ecdc5fa
ce6e55abfe1e7767531eaf1036a5db3d
e29fe3c181ac9ddbb242688b151f3310
e62a52073fd7bfd251efca9906580839
f5e0f57684e9da7ef96dd459b554fded
fde55de117cc611826db0983bc054624

bfb39f486372a509f307cde3361795a2f9f759cbeb4cac07562dcbaebc070364

No verificados pero que podrían ser de Lazarus:

3cc9d9a12f3b884582e5c4daf7d83c4a510172a836de90b87439388e3cde3682
93a01fbbdd63943c151679d037d32b1d82a55d66c6cb93c40ff63f2b770e5ca9
a0664ac662802905329ec6ab3b3ae843f191e6555b707f305f8f5a0599ca3f68
c5c1ca4382f397481174914b1931e851a9c61f029e6b3eb8a65c9e92ddf7aa4c

Recursos extras

Queremos compartir algo más de información relativa a Lazarus. Durante la documentación para este artículo hemos encontrado una web dedicada entera a la **OpBlockbuster**, y cómo tiene varios informes excelentes. Por ello queremos compartiros el recurso:

https://operationblockbuster.com/resources/

Y antes de irnos vamos a dejar aún más recursos para los que quieran profundizar más en el tema:

- https://github.com/649/APT38-DYEPACK
- https://github.com/fboldewin/FastCashMalwareDissected/
- https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/dtrack_lazarus_group.md
- https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.DarkComet
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180231/LazarusUnderTheHood_PDF_final_for_securelist.pdf
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
- https://marcoramilli.com/2019/11/04/is-lazarus-apt38-targeting-critical-infrastructures/

Grim Spider

Actor del 16 de diciembre de 2019, Luis Diago de Aguilar.

Presentación

Grim Spider es un grupo "**eCrime**", es decir, es un grupo cibercriminal. Se dice que este grupo es de origen Ruso y que lleva operando con el ransomware Ryuk desde agosto del 2018. Sus objetivos son grandes organizaciones, multinacionales... y su **modus operandi** consiste en la infección de las mismas para obtener a cambio un beneficio económico. Por ello atacan a grandes entidades, "cuanto más grande, más pasta" ¿no?

Este malware aprovecha el acceso a la red para difundir otro tipo de programas maliciosos (**Emotet** y **TrickBot**) y así robar credenciales de inicio de sesión. Por ello es por lo que se asocia a **Grim Spider** con **Wizard Spider**.

Wizard Spider es el grupo que se encuentra tras Trickbot. Es ruso también y es asociado a **Grim Spider** y **Lunar Spider**. Lo único que podemos saber es que hay pruebas que los relacionan, por sus formas de actuación y colaboración, pero todo son suposiciones basadas en los indicios obtenidos tras los análisis de los ataques.

Os dejamos con un enlace que habla sobre esta relación:

https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/.

Uno de sus últimos ataques con éxito conocidos hasta la fecha ha sido el de **Prosegur**:

Desde Derecho de la Red queremos decir:

Este tipo de ataques a grandes empresas está siendo la orden del día. Empresas como **Everis**, **Prosegur** y **Vodafone** (sin confirmar a fecha de publicación la causa) han sufrido grandes incidentes de seguridad. Nos descartamos que puedan darse más ataques de este tipo.

Operaciones

Operation Pick-Six:

- https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/campaigns-details.operation-pick-six.html
- https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

Malware Asociado

Como ya es costumbre, vamos a hablar sobre los malwares asociados. Ya os adelantamos que son especialistas en ransomware...

- Ryuk Ransom
- LockerGoga Ransom
- Spider Ransom
- Hermes Ransom
- TrickBot

Os dejamos una comparativa entre Ryuk y Hermes realizada por Check Point: https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/

Virus Total

Vamos a dejaros algunas referencias que hemos encontrado de este grupo en los últimos 30 días en VT relacionadas con este actor:

- https://www.virustotal.com/gui/file/3b37696309e8ff7dd21717ff9edfcfab3840e62236b49a1cf6f470ee9074faf8/detection

- https://www.virustotal.com/gui/file/d27d318e35c5a625f2f29128dea3982dede23c96292056c6c2d18a73b82f946b/detection
- https://www.virustotal.com/gui/file/d8ae763ad133268fd0ff364879789da77ce86df814138f2de14c9e4a28f83eed/detection
- https://www.virustotal.com/gui/file/60662418c48f9f1af895ae947e97b0a362ade157ff0241fe1384fe7414ff329e/detection
- https://www.virustotal.com/gui/file/2398629b4f48e0397178c6f05864e02fc668fad660cac2ca771ee9e8a63f3577/detection
- https://www.virustotal.com/gui/file/f30d6979658c78d379d8a1b6dc0d91a8202fa6c32d4c1d9f61fec4317614f389/detection
- https://www.virustotal.com/gui/file/46ebde10ec3b6dd30a7ea16182a11be7f89c6615983dd90633222bd2cb71c96c/detection

Cómo podríamos seguir añadiendo una lista enorme, es por ello por lo que hemos puesto solo los más recientes que hemos encontrado.

IOCs

Vamos a ver algunos indicadores de compromiso.

031dd207c8276bcc5b41825f0a3e31b0
0f9931210bde86753d0f4a9abc5611fd
12597de0e709e44442418e89721b9140
32ea267296c8694c0b5f5baeacf34b0e
395d52f738eb75852fe501df13231c8d
39b7c130f1a02665fd72d65f4f9cb634
3c5575ce80e0847360cd2306c64b51a0
46d781620afc536afa25381504059612
4ec86a35f6982e6545b771376a6f65bb
73e7ddd6b49cdaa982ea8cb578f3af15
8452d52034d3b2cb612dbc59ed609163
8c099a15a19b6e5b29a3794abf8a5878
9d3fdb1e370c0ee6315b4625ecf2ac55
d2f9335a305440d91702c803b6d046b6
34187a34d0a3c5d63016c26346371b54
5ac0f050f93f86e69026faea1fbb4450

c0202cf6aeab8437c638533d14563d35
d348f536e214a47655af387408b4fca5
958c594909933d4c82e93c22850194aa
86c314bc2dc37ba84f7364acd5108c2b
29340643ca2e6677c19e1d3bf351d654
cb0c1248d3899358a375888bb4e8f3fe
1354ac0d5be0c8d03f4e3aba78d2223e
5ac0f050f93f86e69026faea1fbb4450

74654957ba3c9f1ce8bb513954b9deea68a5a82217806977a1247fb342db109f
7dc3fc208c41c946ac8238405fce25e04f0c2a7a9e1d2701986217bd2445487a

Recursos extras

Información relativa a este actor, informes, análisis de malware relativo a este actor...

- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4183-ccn-cert-id-23-19-emotet/file.html
- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4189-ccn-cert-id-24-19-trickbot/file.html
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ryuk-exploring-the-human-connection/
- https://github.com/advanced-threat-research/Yara-Rules/
- https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf
- https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/

Helix Kitten

Actor del 16 de enero de 2020, Luis Diago de Aguilar.

Presentación

Este actor que es de **origen iraní** (por si no quedaba claro...) y se le relaciona con un largo historial de operaciones de ciber espionaje. Se calcula que lleva activo desde **2014** (a pesar de que se dice que se creó sobre el 2004) y sus objetivos están muy relacionados con los intereses del gobierno de Irán.

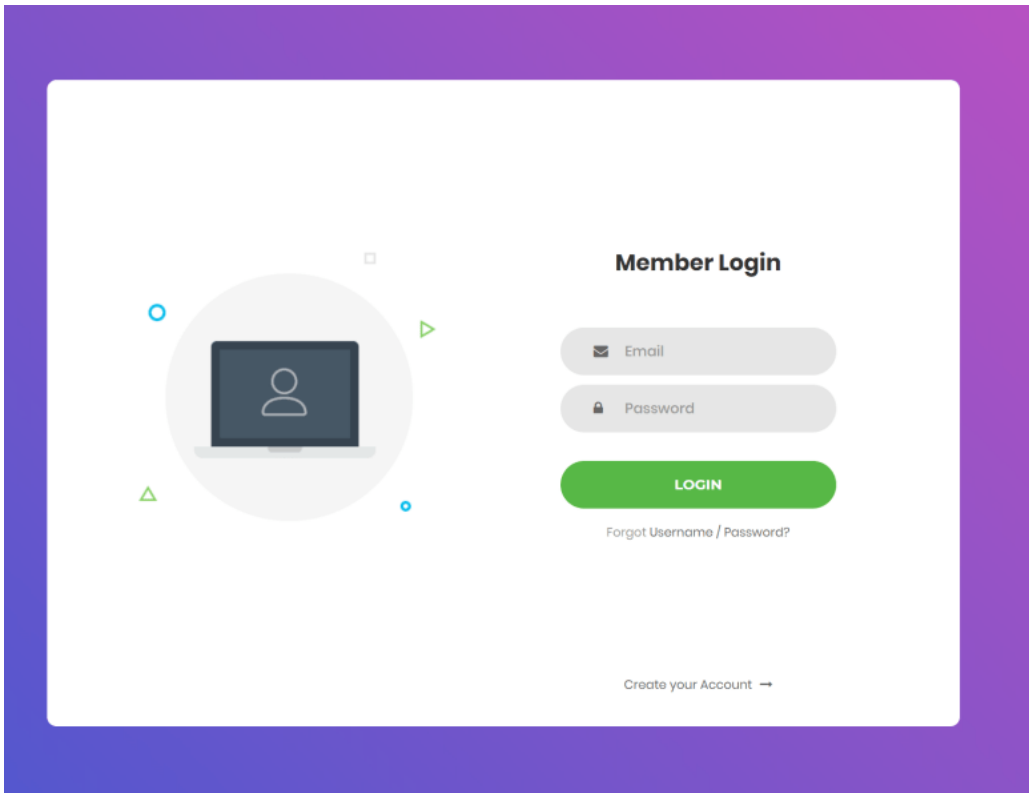
Algunos de los nombres que se le dan son APT34 OilRig, Cobalt Gypsy, Twisted Kitten, entre otros.

El **primer artículo** en el que se hace referencia a este actor data del 11 de Septiembre del 2014. Os dejamos el enlace: http://www.nationmultimedia.com/opinion/Energy-competition-in-South-China-Sea-A-front-burn-30243078.html.

Su ultima acción conocida a fecha de escribir este artículo sería el siguiente: https://www.secrss.com/articles/16441.

Foto extraída del artículo referido

Durante este mes hemos tenido **acceso a varias de sus herramientas**, algunas antiguas, y hemos podido ver algunos de sus paneles usados en algunas de sus operaciones. Adjuntamos foto del **panel**.



Panel de acceso para controlar el malware

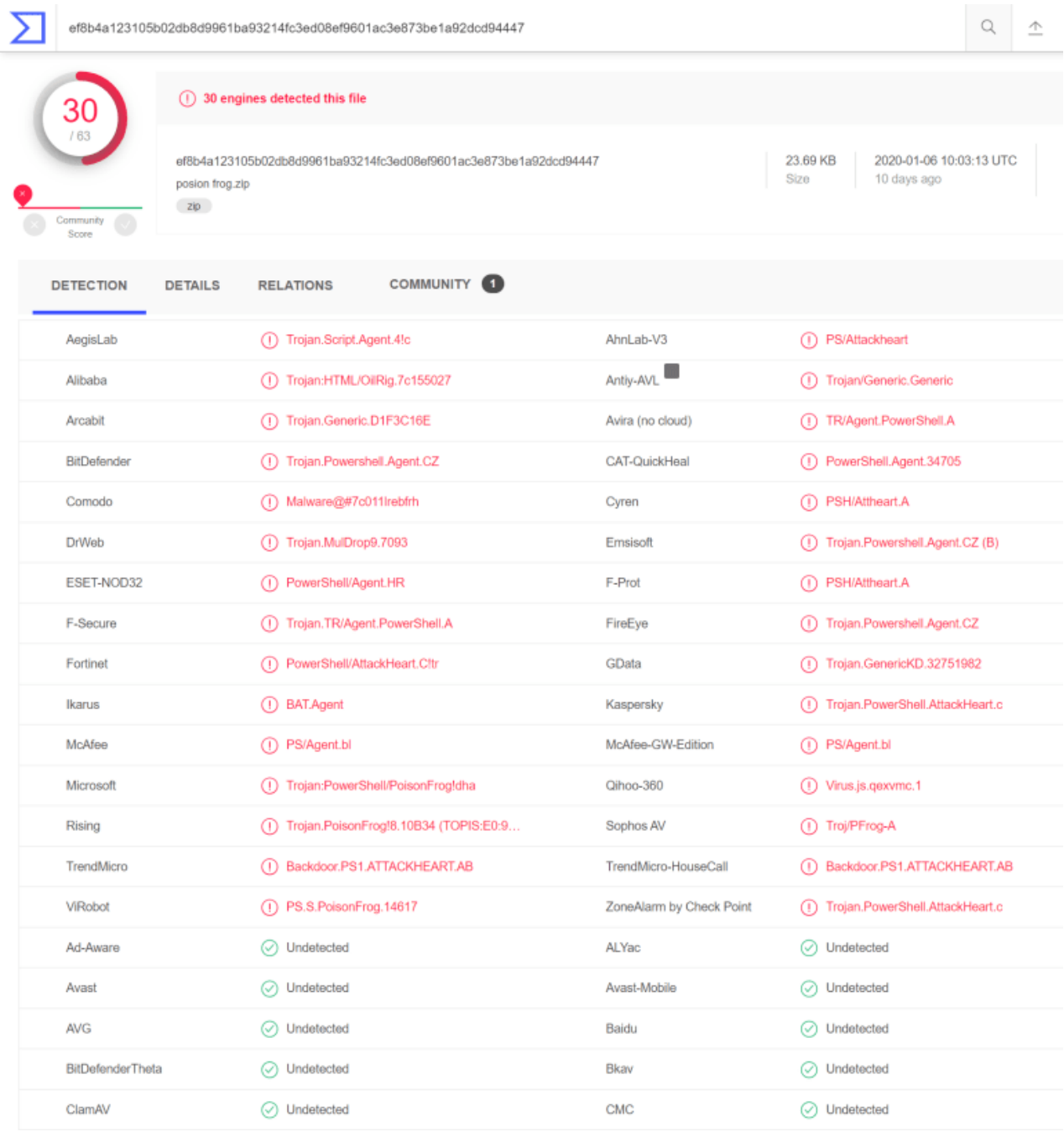
Durante las averiguaciones tuvimos acceso a instrucciones de uso a la hora de **ocultar las direcciones IPs** o sobre como **redireccionar los DNS**. También se incluían **instrucciones para realizar DDoS** y una lista de servidores comprometidos con sus paneles para poder acceder a ellos en caso de ser necesario.

Incluso conseguimos unos ejemplos de **Posion Frog**, casualmente al tiempo que una empresa muy conocida del sector que por cierto, según VT aún no detecta como malicioso el archivo. Desde nuestro **nivel noob reversing** hemos detectado que hay dos ficheros (esa era fácil), uno del cliente y otro del servidor. El del servidor incluye las vistas necesarias para controlar todo por interfaz. Incluye instrucciones de uso muy detalladas... en otras palabras, cualquiera puede usarlo.

Por otro lado se han dejado unas credenciales de configuración...

Finalmente comprobamos el hash: 4b92597fc4004ab673e8ba506ed9dceb.

Al buscar en virus total nos llevó efectivamente al zip de **Posion**.



Se subió a VT un día después de nuestra detección

Y tras este pequeño análisis de los noob analistas de malware pasamos a lo que nos atañe (nota: en el apartado IOCs os dejamos una **lista de shells** que sacamos del análisis del archivo anterior).

Operaciones

Sus operaciones se basan en objetivos financieros, energéticos, de telecomunicaciones e industrias químicas. Infraestructuras críticas cobre todo.

Sus operaciones más conocidas son:

- **xHunt**. Ataques a organizaciones de envío y transporte de Kuwait: https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/
- **Magic Hound**. Ataques con objetivos sauditas: https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/
- **ShadowHammer**. Inyectaban una puerta trasera en una actualización preinstalada en los ordenadores ASUS: https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/herramienta-asus-infectada-operacion-shadowhammer

Malware Asociado

Este grupo de caracteriza por hacer uso de las **macros en Microsoft Excel**, **exploits y payloads en PowerShell** y el uso de la **ingeniería social** para ganar acceso a los objetivos.

Algunos serían:

- **PowDesk**. En PowerShell. Para más información os dejamos un análisis muy detallado: https://www.clearskysec.com/powdesk-apt34/
- **Tonedeaf**. Distribuido por LinkedIn. Más info aquí: https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
- **Glimpse Infection Payload**: https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
- **Poison Frog**: https://ironnet.com/blog/chirp-of-the-poisonfrog/

Destacamos el dato de que en algunos casos **usaban LinkedIn para propagar malware**.

Virus Total

Vamos a dejaros algunas referencias a este actor que hemos podido encontrar en VT de los últimos 30 días. Algunos de ellos aún no son detectados por antivirus actuales.

- https://www.virustotal.com/gui/file/9b09e4a06c8c3770783c751e1193bcd80fd86dc93e0f04d35ec1c108a3e1d8b3/detection
- https://www.virustotal.com/gui/file/10499057d09fb7382cfdbd622536f798e342fb4e418284f5e2bb1f0e17638585/detection
- https://www.virustotal.com/gui/file/b3e44bdb3fa18f3dd1c5ab062dd6a88b3a60928eaf04ac0204b4b0c5a899d456/detection
- https://www.virustotal.com/gui/file/beccb0de25063a2e3cde6797715afb2619fef8da93d173507dac2a0829051e88/detection
- https://www.virustotal.com/gui/file/7d14524b6d7bcb68d1c8a364ebf991669e2078d8c857293ad4cc66dfdfb79b2d/detection
- https://www.virustotal.com/gui/file/3046608570015e2a97192aeedf9d5311c85fb4d83bda4c8e400305adfd304930/detection
- https://www.virustotal.com/gui/file/307928b8b4f86fbc4f805c99dc987f3561ca5e57af5e7a7fcba1f0d6347b1cae/detection
- https://www.virustotal.com/gui/file/2564817f40c0246784bdd14ad3c7f627e4483f067d0526ae0463f321e0e76233/detection
- https://www.virustotal.com/gui/file/0f20995d431abce885b8bd7dec1013cc1ef7c73886029c67df53101ea330436c/detection
- https://www.virustotal.com/gui/file/084086b4975e21887e1e433a2a9ab580671e93f59b392ea19ba2d9f7b21d3aa2/detection
- https://www.virustotal.com/gui/file/390afa26ccfbdb81f82c4f7179967890f1cbc815244ee630d1afffb42d634fcc/detection

IOCs

Vamos ahora con unos cuantos IOCS:

c21074f340665935e6afe2a972c8d1ab517954e2dd05cc73e5ff0e8df587b99d

ea139a73f8ec75ea60dfa87027c7c3ef4ed61b45e1acb5d1650cc54e658984ba

da2abdc951e4b2272fea5c8989debd22e26350bab4b4219104bccec5b8a7ff5a

0d3ae682868cb3ff069ec52e1ffc5ef765453fd78e47b6366d96aebb09afd8ab

f0ecc4388f0d84501499711681a64a74c5d95e0bb6a2174cbe3744bd5a456396

860f4cd44371a180a99bc16526f54f8b051c420a3df334d05d569d0cdadac3d2

b42b1186211633c2d47f3d815f0371ba234fee2ed0f26e487badc58e1ab81061

4beee6e7aa244335e161fdc05296ea100090c2114b4ff2e782e3ee3e1f936fdf

5e0e09c9860b293c4c9a2382a7392963adc54d6a23440abb9a2d89c50f8fd305

3161f9087d89a2d036ea32741d5a006c6bb279d36ff8d1acde63f2e354f8c502

b6c159cad5a867895fd41c103455cebd361fc32d047b573321280b1451bf151c

6a7537f2cedbf453114cfba086e4746e698713777fb4fa4fc8964247dde741ed

16d87fbd8667677da1af5433b6d797438f8dc0ab565fb40ecb29f83f148888cd

92bc7d04445cf67aa7ddf15792cd62778d2d774d06616d1986f4c389b3d463f5

86d3409c908f667dd298b6a7e1e17652bb29af73e7daed4a5e945fbdf742e9f4

c3a8f5176351e87d28f45e58c79bb6646bb5d94ade7a24c6556514c860004143

a390365ddfcce146a8fa8435022f19b9a1be29f2b11a049cb660ec53f36beb06

d2ffc757a12817e4b58b3d58d71da951b177dedd3f65ca41fad04a03fc63fac6

79c9894b50cde62b182bd1560060c5c2bf5a1cef2b8afdffc4766e8c55ff6932

2f7f3582504fbce349a6991fbb3b5f9577c5c014b6ce889b80d51977fa6fb31a

8c2e4aa8d73ad2e48d70dfa18abea62769c7bef59c8c1607720f4f6162413f75

abe8e86b787998a07411ee24f3f3d8a79e37c6da539650ceed566b081f968c26

9e4d2e983f8a807f741f8873e6fa5d222dc6f3b358ccfc3a6c700398b342f656

e57f77cc3d117923ec01aa0e044edc11b1042e57993ca7f74d971630893ca263

ca6e823dedd6ca5fada2b1fa63d0acb288027f5a3cdd2c60dcace3c424c5ced0

eaaecabb439c81e522d9f5681fdb047ee62381e763f0d9646e68cd507479ba5a

1c3e527e496c4b0594a403d6d582bc6db3029d27369720d0d5122f862b10d8f1

29a659fb0ef0262e4de0dc3c6a140677b6ddee13c1819b791bd280be0547e309

218fac3d0639c0d762fcf71685bcf6b64c33d1533df03b4cf223d9b07ca1e3c2

e5b643cb6ec30d0d0b458e3f2800609f260a5f15c4ac66faf4ebf384f7976df6

71e584e7e1fb3cf2689f549192fe3a82fd4cd8ee7c42c15d736ebad47b028087

388b26e22f75a723ce69ad820b61dd8b75e260d3c61d74ff21d2073c56ea565d

33ee8a57e142e752a9c8960c4f38b5d3ff82bf17ec060e4114f5b15d22aa902e

5469facc266d5582bd387d69032a91c8fff373213b66a2f0852666e72bcdc1da

528714aaaa4a083e72599c32c18aa146db503eee80da236b20aea11aa43bdf62

66d24a529308d8ab7b27ddd43a6c2db84107b831257efb664044ec4437f9487b

cfce4827106c79a81eef6d3a0618c90bf5f15936036873573db76bed7e8a0864

68db2b363a88b061cc9063535f3920673f1f08d985b14cb52b898ced6c0f8964

e837f6b814c09900726dac2cf55f41babf361152875ba2a765a34ee5cc496087

f912d40de9fe9a726448c1d84dfba2d4941f57210b2dbc035f5d34d68e8ac143

af0ae0fa877f921d198239b7c722e12d14b2aa32fdfadaa37b47f558ae366de9

6d1a50ca3e80442fa3e2caca86c166ed60bef32c2d0af7352cd227303cdec031

Algunos hosts del malware

service.chrome-up[.]date

www3.chrome-up[.]date

www7.chrome-up[.]date

timezone[.]live

service1.chrome-up[.]date

104.238.184[.]252

www5.chrome-up[.]date

servicesystem.serveirc[.]com

45.76.128[.]165

139.59.46[.]154

104.218.120[.]128

89.107.62[.]39

69.87.223[.]26

analytics-google[.]org

89.107.60[.]11

www3.chrome-up[.]date

www.microsoftsubsystem.com-adm[.]in

www1.chrome-up[.]date

Shells sacadas de los análisis del archivo de la amenaza

Address,Site name,Country/region
https://202.183.235.31/owa/auth/signout.aspx,rtarf.mi.th,Thailand
https://202.183.235.4/owa/auth/signout.aspx,rtarf.mi.th,Thailand
https://122.146.71.136/owa/auth/error3.aspx,mail.taifo.com.tw,Taiwan
https://59.124.43.229/owa/auth/error0.aspx,tgpf.org.tw,Taiwan
https://202.134.62.169/owa/auth/signin.aspx,rshe13.com{outlook},Commercial
https://202.164.27.206/owa/auth/signout.aspx,wmail.hkcsl.com,Commercial
https://213.14.218.51/owa/auth/logon.aspx,botas.gov.tr{outlook},Turkey
https://88.255.182.69/owa/auth/getidtoken.aspx,mail.gulsanholding.com.tr,Turkey
https://95.0.139.4/owa/auth/logon.aspx,.nvi.gov.tr{outlook},Turkey
https://1.202.179.13/owa/auth/error1.aspx,mail.cecep.cn,China
https://1.202.179.14/owa/auth/error1.aspx,mail.cecep.cn,China
https://114.255.190.1/owa/auth/error1.aspx,mail.generali-china.cn,China
https://180.166.27.217/owa/auth/error3.aspx,exchange.bestv.com.cn,China
https://180.169.13.230/owa/auth/error1.aspx,bdo.com.cn,China
https://210.22.172.26/owa/auth/error1.aspx,lswebext.sdec.com.cn,China
https://221.5.148.230/owa/auth/outlook.aspx,mail.swsc.com.cn,China
https://222.178.70.8/owa/auth/outlook.aspx,mail.swsc.com.cn,China
https://222.66.8.76/owa/auth/error1.aspx,lswebext.sdec.com.cn,China
https://58.210.216.113/owa/auth/error1.aspx,mail.neway.com.cn,China

https://60.247.31.237/owa/auth/error3.aspx,crccre.cn,China
https://60.247.31.237/owa/auth/logoff.aspx,crccre.cn,China
https://202.104.127.218/owa/auth/error1.aspx,mail.aisidi.com,services
https://202.104.127.218/owa/auth/exppw.aspx,mail.aisidi.com,services
https://132.68.32.165/owa/auth/logout.aspx,CSEX.csf.technion.ac.il,Israel
https://132.68.32.165/owa/auth/signout.aspx,CSEX.csf.technion.ac.il,Israel
https://209.88.89.35/owa/auth/logout.aspx,mail.netone.co.zw,Zimbabwe
https://114.198.235.22/owa/auth/login.aspx,mail.its.ws,Samoa
https://114.198.237.3/owa/auth/login.aspx,mail.its.ws,Samoa
https://185.10.115.199/owa/auth/logout.aspx,sstc.com.sa,Saudi Arabia
https://195.88.204.17/owa/auth/logout.aspx,saptco.com.sa,Saudi Arabia
https://46.235.95.125/owa/auth/signin.aspx,safari.com.sa,Saudi Arabia
https://51.211.184.170/owa/auth/owaauth.aspx,uqu.edu.sa,Saudi Arabia
https://91.195.89.155/owa/auth/signin.aspx,moe.gov.sa,Saudi Arabia
https://82.178.124.59/owa/auth/gettokenid.aspx,admincourt.gov.om,Oman
https://83.244.91.132/owa/auth/logon.aspx,mail.hbtf.com.ps{outlook},Palestine
https://195.12.113.50/owa/auth/error3.aspx,MAIL.M.GOV.KZ,Kazakhstan
https://78.100.87.199/owa/auth/logon.aspx,ashghal.gov.qa{outlook},Qatar
https://110.74.202.90/owa/auth/errorff.aspx,mail.fmis.mef.gov.kh,Cambodia
https://211.238.138.68/owa/auth/error1.aspx,mailexchange.blueside.co.kr,North Korea
https://168.63.221.220/owa/auth/error3.aspx,mail.tc-gaming.co,Colombia
https://213.189.82.221/owa/auth/errorff.aspx,cait.gov.kw,Kuwait
https://205.177.180.161/owa/auth/erroref.aspx,ogero.gov.lb,Lebanon
https://77.42.251.125/owa/auth/logout.aspx,{ul.edu.lb},Lebanon
https://202.175.114.11/owa/auth/error1.aspx,webmail.netcraft.com.mo,Macau
https://202.175.31.141/owa/auth/error3.aspx,exchange.must.edu.mo,Macau
https://213.131.83.73/owa/auth/error4.aspx,ad.gov.eg{shell},Egypt
https://187.174.201.179/owa/auth/error1.aspx,correo.cns.gob.mx,Mexico
https://200.33.162.13/owa/auth/error3.aspx,sre.gob.mx,Mexico
https://202.70.34.68/owa/auth/error0.aspx,mfa.gov.mn,Myanmar
https://202.70.34.68/owa/auth/error1.aspx,mifa.gov.mn,Myanmar

https://197.253.14.10/owa/auth/logout.aspx,mail.mfaforum.gov.ng,Nigeria

https://41.203.90.221/owa/auth/logout.aspx,mail.mfaforum.gov.ng,Nigeria

http://www.abudhabiairport.ae/english/resources.aspx,www.abudhabiairport.ae,United Arab Emirates

https://mailkw.agility.com/owa/auth/RedirSuiteService.aspx,mailkw.agility.com,Kwait

http://www.ajfd.gov.ae/_layouts/workpage.aspx,www.ajfd.gov.ae,United Arab Emirates

https://mail.alfuttaim.ae/owa/auth/change_password.aspx,mail.alfuttaim.ae,United Arab Emirates

https://mail.alraidah.com.sa/owa/auth/GetLoginToken.aspx,mail.alraidah.com.sa,Saudi Arabia

http://www.alraidah.com.sa/_layouts/WrkSetlan.aspx,www.alraidah.com.sa,Saudi Arabia

https://webmail.alsalam.aero/owa/auth/EventClass.aspx,webmail.alsalam.aero,Saudi Arabia

https://webmail.bix.bh/owa/auth/Timeoutctl.aspx,webmail.bix.bh,Bahrain

https://webmail.bix.bh/owa/auth/EventClass.aspx,webmail.bix.bh,Bahrain

https://webmail.bix.bh/ecp/auth/EventClass.aspx,webmail.bix.bh,Bahrain

https://webmail.citc.gov.sa/owa/auth/timeout.aspx,webmail.citc.gov.sa,Saudi Arabia

https://mail.cma.org.sa/owa/auth/signin.aspx,mail.cma.org.sa,Saudi Arabia

https://mail.dallah-hospital.com/owa/auth/getidtokens.aspx,mail.dallah-hospital.com,Saudi Arabia

https://webmail.dha.gov.ae/owa/auth/outlookservice.aspx,webmail.dha.gov.ae,United Arab Emirates

https://webmail.dnrd.ae/owa/auth/getidtoken.aspx,webmail.dnrd.ae,United Arab Emirates

http://dnrd.ae:8080/_layouts/WrkStatLog.aspx,dnrd.ae,United Arab Emirates

https://www.dns.jo/statistic.aspx,www.dns.jo,Jordan

https://webmail.dsc.gov.ae/owa/auth/outlooklogonservice.aspx,webmail.dsc.gov.ae,United Arab Emirates

https://e-albania.al/dptaktkonstatim.aspx,e-albania.al,Albania

https://owa.e-albania.al/owa/auth/outlookdn.aspx,owa.e-albania.al,Albania

https://webmail.eminsco.com/owa/auth/outlookfilles.aspx,webmail.eminsco.com,United Arab Emirates

https://webmail.eminsco.com/owa/auth/OutlookCName.aspx,webmail.eminsco.com,United Arab Emirates

https://webmail.emiratesid.ae/owa/auth/RedirSuiteService.aspx,webmail.emiratesid.ae,United Arab Emirates

https://mailarchive.emiratesid.ae/EnterpriseVault/js/jquery.aspx,mailarchive.emiratesid.ae,United Arab Emirates

https://webmail.emiratesid.ae/owa/auth/handlerservice.aspx,webmail.emiratesid.ae,United Arab Emirates

http://staging.forus.jo/_layouts/explainedit.aspx,staging.forus.jo,Jordan

https://government.ae/tax.aspx,government.ae,United Arab Emirates

https://formerst.gulfair.com/GFSTMSSSPR/webform.aspx,formerst.gulfair.com,Bahrain

https://webmail.ictfund.gov.ae/owa/auth/owaauth.aspx,webmail.ictfund.gov.ae,United Arab Emirates

https://jaf.mil.jo/ShowContents.aspx,jaf.mil.jo,Jordan

http://www.marubi.gov.al/aspx/viewpercthesaurus.aspx,www.marubi.gov.al,Albania

https://mail.mindware.ae/owa/auth/outlooktoken.aspx,mail.mindware.ae,United Arab Emirates

https://mail.mis.com.sa/owa/auth/Redirect.aspx,mail.mis.com.sa,Saudi Arabia

https://webmail.moe.gov.sa/owa/auth/redireservice.aspx,webmail.moe.gov.sa,Saudi Arabia

https://webmail.moe.gov.sa/owa/auth/redirectcache.aspx,webmail.moe.gov.sa,Saudi Arabia

https://gis.moei.gov.ae/petrol.aspx,gis.moei.gov.ae,United Arab Emirates

https://gis.moenr.gov.ae/petrol.aspx,gis.moenr.gov.ae,United Arab Emirates

https://m.murasalaty.moenr.gov.ae/signproces.aspx,m.murasalaty.moenr.gov.ae,United Arab Emirates

https://mail.mofa.gov.iq/owa/auth/RedirSuiteService.aspx,mail.mofa.gov.iq,Iraq

http://ictinfo.moict.gov.jo/DI7Web/libraries/aspx/RegStructures.aspx,ictinfo.moict.gov.jo,Jordan

http://www.mpwh.gov.jo/_layouts/CreateAdAccounts.aspx,www.mpwh.gov.jo,Jordan

https://mail.mygov.ae/owa/auth/owalogin.aspx,mail.mygov.ae,United Arab Emirates

https://ksa.olayan.net/owa/auth/signin.aspx,ksa.olayan.net,Saudi Arabia

https://mail.omantourism.gov.om/owa/auth/GetTokenId.aspx,mail.omantourism.gov.om,Oman

https://email.omnix-group.com/owa/auth/signon.aspx,email.omnix-group.com,United Arab Emirates

https://mail.orange-jtg.jo/OWA/auth/signin.aspx,mail.orange-jtg.jo,Jordan

http://fwx1.petra.gov.jo/SEDCOWebServer/global.aspx,fwx1.petra.gov.jo,Jordan

http://fwx1.petranews.gov.jo/SEDCOWebServer/content/rtl/QualityControl.aspx,fwx1.petranews.gov.jo,Jordan

https://webmail.presflt.ae/owa/auth/logontimeout.aspx,webmail.presflt.ae,United Arab Emirates

https://webmail.qchem.com/OWA/auth/RedirectCache.aspx,webmail.qchem.com,Qatar

https://meet.saudiairlines.com/ClientResourceHandler.aspx,meet.saudiairlines.com,Saudi Arabia

https://mail.soc.mil.ae/owa/auth/expirepw.aspx,mail.soc.mil.ae,United Arab Emirates

https://email.ssc.gov.jo/owa/auth/signin.aspx,email.ssc.gov.jo,Jordan

https://mail.sts.com.jo/owa/auth/signout.aspx,mail.sts.com.jo,Jordan

http://www.sts.com.jo/_layouts/15/moveresults.aspx,www.sts.com.jo,Jordan

https://mail.tameen.ae/owa/auth/outlooklogon.aspx,mail.tameen.ae,United Arab Emirates

https://webmail.tra.gov.ae/owa/auth/outlookdn.aspx,webmail.tra.gov.ae,United Arab Emirates

http://bulksms.umniah.com/gmgweb/MSGTypesValid.aspx,bulksms.umniah.com,Jordan

https://evserver.umniah.com/index.aspx,evserver.umniah.com,Jordan

https://email.umniah.com/owa/auth/redirSuite.aspx,email.umniah.com,Jordan

https://webmail.gov.jo/owa/auth/getidtokens.aspx,webmail.gov.jo,Jordan

https://www.tra.gov.ae/signin.aspx,www.tra.gov.ae,United Arab Emirates

https://www.zakatfund.gov.ae/zfp/web/tofollowup.aspx,www.zakatfund.gov.ae,United Arab Emirates

https://mail.zayed.org.ae/owa/auth/espw.aspx,mail.zayed.org.ae,United Arab Emirates

https://mail.primus.com.jo/owa/auth/getidtoken.aspx,mail.primus.com.jo,Jordan

Recursos Extras

- https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
- https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
- https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram