MNEMO
NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

Diciembre 2018

Reporte de Actividad de Botnets en México

DESTACADOS DEL MES

- Una botnet de más de 20 mil sitios de WordPress, está atacando a otros sitios.
- Atacantes comprometen 100 millones de datos de usuarios de la plataforma Quora.
- Atacantes logran infectar 415 mil routers para minar criptomonedas.
- Anonymous inicia la campaña #OpIcarus 2.0 contra instituciones financieras a nivel mundial.

235,293 Total de eventos relacionados con servidores C&C de Diciembre 2018

Direcciones IP de C&C únicas **10,305**

Distribución mundial de equipos C&C con afectaciones en México

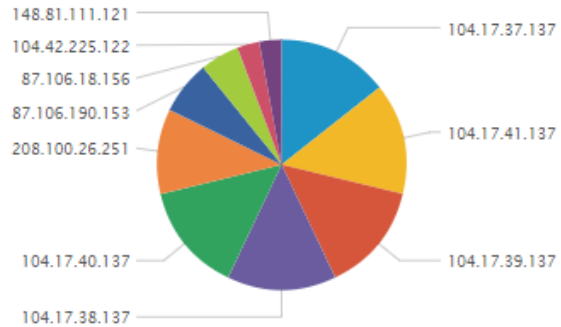
País	Diciembre
Estados Unidos	10,063
Alemania	135
Desconocido	39
Polonia	38
Países Bajos	16
Irlanda	4
Hong Kong	4
Singapur	3
Hungría	2
Canadá	1

Top de direcciones IP empleadas como servidores C&C

Detalle de peticiones Top 10 de direcciones IP de C&C

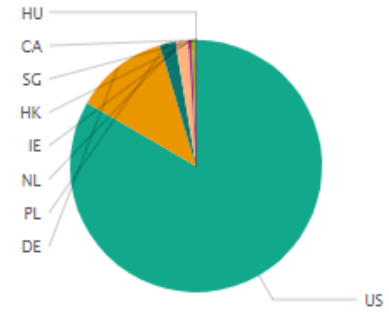
IP C&C	Eventos	%
104.17.37.137	21800	9.27
104.17.41.137	21750	9.24
104.17.39.137	21448	9.12
104.17.38.137	21444	9.11
104.17.40.137	21405	9.10
208.100.26.251	16670	7.08
87.106.190.153	10527	4.47
87.106.18.156	7650	3.25
104.42.225.122	4372	1.86
148.81.111.121	4366	1.86

Top 10 de direcciones IP de C&C



US País con mayor actividad

Ubicaciones por país



80 Puerto de comunicación utilizado con mayor actividad por los C&C

Puertos de comunicación

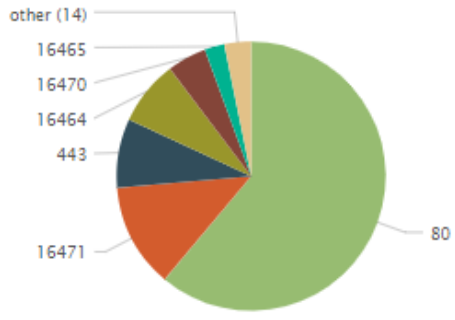


Imagen 1. Información general de los servidores C&C en México.

DESCRIPCIÓN

La actividad de Botnets que se describe está basada en el análisis de los intentos de conexión realizados por bots a servidores de Comando y Control (C&C). Los bots son equipos comprometidos con algún tipo de malware instalado que permite que sean controlados de manera remota a través de los servidores de C&C, los cuales son utilizados por usuarios mal intencionados para enviar instrucciones a los equipos comprometidos.

Con este reporte, MNEMO-CERT aporta elementos para la ejecución de acciones concretas en beneficio de la ciberseguridad, presentando un resumen del análisis de sus fuentes de información. Los datos detallados se encuentran disponibles para los suscriptores de nuestros servicios.

En la siguiente tabla, se presentan las direcciones IP de los 50 servidores de C&C con mayor actividad en el mes de diciembre, el número de eventos en el que estuvieron implicados, puerto de comunicación del C&C y su ubicación a nivel país.

IP de C&C	Peticiones	Puerto Destino	Ubicación
104.17.37.137	21,800	80	US
104.17.41.137	21,750	80	US
104.17.39.137	21,448	80	US
104.17.38.137	21,444	80	US
104.17.40.137	21,405	80	US
208.100.26.251	15,571	80	US
87.106.190.153	10,514	443	DE
87.106.18.156	7,650	80	DE
104.42.225.122	4,372	80	US
46.165.254.212	4,245	443	DE
148.81.111.121	3,518	80	PL
217.20.116.140	2,925	443	DE
208.100.26.241	1,307	1922	US
212.227.20.93	1,176	80	DE
70.184.12.133	1,104	16464	US
46.244.21.4	1,099	7006	NL
208.100.26.241	967	6567	US
148.81.111.121	848	65520	PL
107.170.198.33	798	80	US
52.169.189.46	790	16464	IE
168.63.134.179	785	16464	HK
68.107.207.3	725	16464	US
192.42.119.41	724	443	NL
208.100.26.241	716	9251	US
208.100.26.241	620	8948	US
192.42.116.41	551	443	NL
192.42.119.41	535	80	NL
208.100.26.241	395	4794	US
168.61.86.35	323	16471	IE
192.42.116.41	283	3720	NL
192.42.119.41	275	5050	NL
40.71.228.10	272	16471	US
208.100.26.251	218	3444	US
148.81.111.98	199	80	PL
137.116.128.103	196	16464	SG
208.100.26.251	189	8370	US
104.40.6.5	186	16464	US
104.41.132.71	183	16464	US
208.100.26.251	180	3123	US
192.42.116.41	177	80	NL
212.227.20.116	171	80	DE
208.100.26.251	157	8916	US
70.160.145.58	154	16471	US
70.160.43.176	152	16471	US
70.160.44.138	151	16471	US
208.100.26.251	146	3775	US
70.160.139.96	137	16471	US
208.100.26.241	129	8800	US
87.106.18.141	128	80	DE
70.171.124.250	126	16471	US

Tabla 1. Top 50 de direcciones IP empleadas como C&C.

En este periodo de mes, se han identificado 41 puertos de comunicación únicos empleados por los servidores C&C, resaltando el puerto TCP 80 con una actividad del 61%. A continuación se muestra el top 10 de los puertos de comunicación utilizados con mayor frecuencia en este periodo.

Puertos	Peticiones
80	143,284
16471	29,349
443	19,406
16464	18,250
16470	11,063
16465	5,577
1922	1,307
7006	1,099
6567	967
65520	848

Tabla 2. Top 10 de los puertos más utilizados por los servidores C&C.

RECOMENDACIONES

Las direcciones IP de los servidores C&C en conjunto con los puertos utilizados por los bots para establecer las comunicaciones y que son presentadas en este reporte, representan Indicadores de Compromiso (IOCs), los cuales deben apoyar las fases de identificación y contención de actividad maliciosa, que permitirá reducir cualquier afectación al respecto. Una vez que se han madurado los IOCs se recomienda realizar algunas de las siguientes actividades:

- Generar listas negras que eviten comunicación hacia los equipos C&C.
- Identificar equipos en su infraestructura que presenten comunicación con los C&C listados.
- Implementar dispositivos de seguridad que permitan identificar y bloquear peticiones maliciosas hacia o desde los equipos de su infraestructura (IDS, IPS, gestores de contenido, AV, EndPoint, firewall, DLP, por mencionar algunos).
- Verificar la eficacia de los controles de ciberseguridad implementados.
- Implementar procedimientos para la identificación y gestión de vulnerabilidades en la infraestructura de TI.
- Implementar campañas de información y planes de concientización de la seguridad de la información dentro su organización.
- Gestionar el apoyo de un equipo de respuesta a incidentes de ciberseguridad, si detectan equipos con actividad maliciosa en su infraestructura.

Por otro lado, debe tenerse en cuenta que cuando un host ha sido comprometido y es controlado desde un servidor de C&C, éste podría recibir instrucciones orientadas en perjudicar la integridad, confidencialidad y disponibilidad de la información contenida en él. A continuación se listan algunas de las actividades de uso malintencionado de los equipos comprometidos (bots):

- Robo de información confidencial del equipo infectado.
- Envío de correo Spam.
- Publicación de software ilegal, pornografía, repositorios malintencionados por mencionar algunos.
- Generación de ataques de Negación de Servicio Distribuido (DDoS).
- Publicación de sitios fraudulentos (Phishing).
- Propagación de ataques hacia otros equipos de la red.

MNEMO-CERT realiza el monitoreo continuo de las vulnerabilidades y actividad maliciosa que se presenta en la infraestructura tecnológica del país, con el fin de generar información de inteligencia, derivado de efectuar un análisis de los datos provenientes de distintas fuentes. Esta actividad permite notificar de manera oportuna, a los responsables de los activos tecnológicos afectados, inscritos en los servicios de MNEMO-CERT, para establecer las actividades necesarias que permitan atender y solucionar los hallazgos contenidos en los reportes emitidos.

MNEMO

NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

Si desea conocer mayor detalle de este reporte o de algún tema/servicio de ciberseguridad, puede contactarnos a través de los siguientes medios:

/MNEMOCERT

@MNEMOCERT

cert.mnemo.com