MNEMO
NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

Noviembre 2018

Reporte de Actividad de Botnets en México

DESTACADOS DEL MES

- ICANN/LACNIC: primera rotación de las claves criptográficas en la zona raíz de Internet (DNSSEC).
- Investigador revela vulnerabilidad de día cero de VirtualBox.
- HTTP/QUIC será renombrado como HTTP/3.
- Los datos de 500 millones de clientes de varias cadenas hoteleras, han sido vulnerados.
- El valor del mercado de las criptomonedas cae un 58% en 2018.

257,701 Total de eventos relacionados con servidores C&C de Noviembre 2018

Direcciones IP de C&C únicas **10,174**

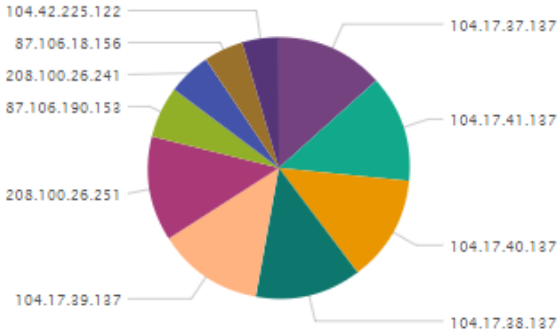
Distribución mundial de equipos C&C con afectaciones en México

Top de direcciones IP empleadas como servidores C&C

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

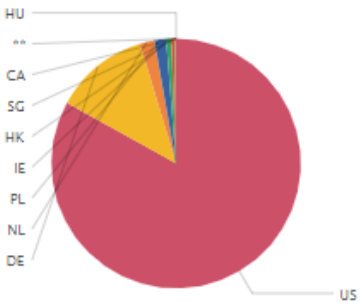
IP C&C	Eventos	%
104.17.37.137	23775	9.23
104.17.41.137	23542	9.14
104.17.40.137	23386	9.07
104.17.38.137	23301	9.04
104.17.39.137	23279	9.03
208.100.26.251	23078	8.96
87.106.190.153	11299	4.38
208.100.26.241	9515	3.69
87.106.18.156	8693	3.37
104.42.225.122	8046	3.12

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

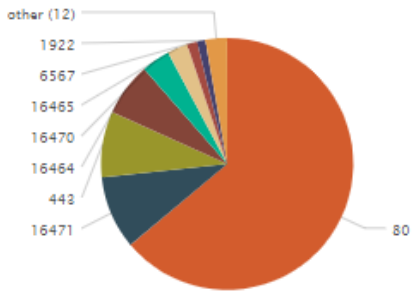


Imagen 1. Información general de los servidores C&C en México.

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 noviembre, 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	23,775	80	US
104.17.41.137	23,542	80	US
104.17.40.137	23,386	80	US
104.17.38.137	23,301	80	US
104.17.39.137	23,279	80	US
208.100.26.251	21,505	80	US
87.106.190.153	11,289	443	DE
87.106.18.156	8,693	80	DE
104.42.225.122	8,046	80	US
46.165.254.212	4,422	443	DE
217.20.116.140	3,361	443	DE
208.100.26.241	3,361	6567	US
148.81.111.121	2,749	80	PL
208.100.26.241	2,711	1922	US
168.63.134.179	1,206	16464	HK
46.244.21.4	1,150	7006	NL
212.227.20.93	1,130	80	DE
52.169.189.46	1,081	16464	IE
192.42.119.41	1,078	443	NL
208.100.26.241	1,071	9251	US
208.100.26.241	1,031	8948	US
148.81.111.121	706	65520	PL
192.42.119.41	656	80	NL
168.61.86.35	573	16471	IE
107.170.198.33	544	80	US
192.42.116.41	532	443	NL
40.71.228.10	517	16471	US
212.227.20.116	492	80	DE
192.42.116.41	488	3720	NL
208.100.26.241	427	4794	US
68.107.207.3	372	16464	US
208.100.26.251	358	3444	US
192.42.119.41	340	5050	NL
208.100.26.241	296	8800	US
208.100.26.251	290	3123	US
208.100.26.241	288	3618	US
148.81.111.98	258	80	PL
70.184.12.133	248	16464	US
192.42.116.41	240	80	NL
208.100.26.251	229	8370	US
87.106.18.141	223	80	DE
208.100.26.251	202	8916	US
208.100.26.251	189	3775	US
192.42.116.41	176	5050	NL
74.208.64.145	169	445	US
74.208.64.191	168	445	US
208.100.26.251	168	4410	US
168.63.254.209	167	16465	SG
208.100.26.241	166	7372	US
70.160.172.104	143	16471	US

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

En este periodo de mes, se han identificado 46 puertos de comunicación únicos empleados por los servidores C&C, resaltando el puerto TCP 80 con una actividad del 63%. A continuación se muestra el top 10 de los puertos de comunicación utilizados con mayor frecuencia en este periodo.

Puertos	Peticiones
80	163,269
16471	23,979
443	21,603
16464	17,417
16470	9,357
16465	6,654
6567	3,361
1922	2,711
7006	1,150
9251	1,071

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