MNEMO

NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

JULIO 2018

Reporte de Actividad de Botnets en México

© Todos los derechos reservados. Mnemo Evolution & Integration Services

261,315 Total de eventos relacionados con servidores C&C de julio

Direcciones IP de C&C únicas **2,473**

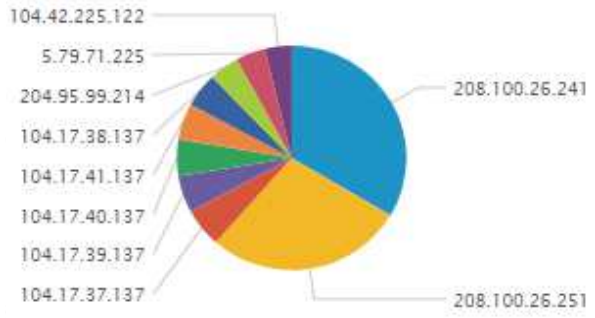
Distribución mundial de equipos C&C con afectaciones en México

Top de direcciones IP empleadas como servidores C&C

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

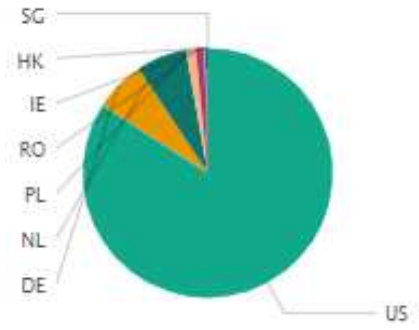
IP C&C	Eventos	%
208.100.26.241	72934	27.910376
208.100.26.251	60607	23.193081
104.17.37.137	12110	4.634254
104.17.39.137	11654	4.459752
104.17.40.137	11376	4.353367
104.17.41.137	11317	4.330789
104.17.38.137	10786	4.127585
204.95.99.214	9105	3.484301
5.79.71.225	9067	3.469759
104.42.225.122	8210	3.141802

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

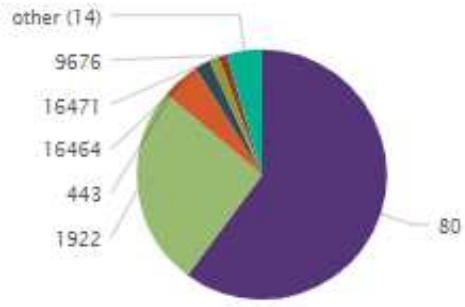


Imagen 1. Información general de los servidores C&C en México.

© Todos los derechos reservados. Mnemo Evolution & Integration Services

DESCRIPCIÓN

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

Con este reporte, MNEMO-CERT pretende aportar elementos para la ejecución de acciones concretas en beneficio de la ciberseguridad, presentando un resumen del análisis de sus fuentes de información. La información detallada está disponible para los suscriptores de sus servicios.

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

IP de C&C	Peticiones	Puerto Destino	Ubicación
208.100.26.241	65,004	1922	US
208.100.26.251	59,134	80	US
104.17.37.137	12,109	80	US
104.17.39.137	11,654	80	US
104.17.40.137	11,376	80	US
104.17.41.137	11,317	80	US
104.17.38.137	10,786	80	US
204.95.99.214	9,105		US
5.79.71.225	8,904	80	NL
104.42.225.122	8,210	80	US
217.20.116.140	4,687	443	DE
87.106.190.153	4,618	443	DE
87.106.18.156	4,432	80	DE
208.100.26.241	2,997	9676	US
5.2.189.251	2,884	80	RO
148.81.111.121	2,417	80	PL
107.170.198.33	1,961	80	US
192.42.119.41	1,465	443	NL
46.244.21.4	1,314	7006	NL
208.100.26.241	1,531	7006	NL
208.100.26.241	1,527	7372	US
192.42.116.41	1,494	80	NL
40.71.228.10	1,304	16464	NL
208.100.26.241	1,288	16464	IE
5.79.71.205	80	16464	NL
85.17.31.122	80	4794	NL
208.100.26.251	3,444	80	US
85.17.31.82	80	3444	NL
68.107.207.3	16,464	80	US
192.42.116.41	3,720	8948	NL
208.100.26.241	8,800	3618	US
192.42.119.41	80	80	NL
178.162.217.107	80	80	DE
87.106.149.145	445	16471	DE
178.162.203.226	80	80	DE
208.100.26.241	9,251	80	US
168.63.134.179	16,464	9251	HK
208.100.26.241	3,618	8800	US
85.17.164.15	16,464	80	NL
52.169.189.46	16,464	445	IE
208.100.26.241	7,372	16471	US
148.81.111.99	80	3720	PL
192.42.116.41	80	16464	NL
212.227.20.93	80	80	DE
148.81.111.121	65,520	65520	PL
148.81.111.98	80	3123	PL
208.100.26.251	443	445	US
168.61.86.35	16,471	6567	IE
174.78.129.185	16,464	80	US
208.100.26.251	81	80	US

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

En este periodo se han identificado 74 puertos de comunicación únicos empleados por los servidores C&C, resaltando el puerto TCP 80 con una actividad del 58%. A continuación se muestra el top 10 de los puertos de comunicación utilizados con mayor frecuencia en este periodo.

Puertos	Peticiones
80	150,882
1922	65,004
443	12,531
16464	5,110
16471	3,020
9676	2,997
16465	1,686
7006	1,314
6567	1,193
8948	1,056

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

© Todos los derechos reservados. Mnemo Evolution & Integration Services

RECOMENDACIONES

Las direcciones IP de los servidores C&C en conjunto con los puertos utilizados por los bots para establecer las comunicaciones presentadas en este reporte representan Indicadores de Compromiso (IOCs), los cuales deben ser tratados de manera adecuada, para que apoyen las fases de identificación y contención, lo que permitirá en consecuencia determinar su valor y evitar cualquier afectación no deseada. 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.
- Si detecta equipos con actividad maliciosa en su infraestructura, solicite el apoyo de un equipo de respuesta a incidentes de ciberseguridad.

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 a perjudicar la integridad, confidencialidad y disponibilidad de la información contenida en él. A continuación se listan algunas de las actividades a las que se encuentran expuestas 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 a través del análisis de la información proveniente 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 que definan las actividades necesarias para atender y solucionar los hallazgos contenidos en los reportes emitidos.

© Todos los derechos reservados. Mnemo Evolution & Integration Services

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