MNEMO
NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

Septiembre 2018

Reporte de Actividad de Botnets en México

DESTACADOS DEL MES

- Vulnerabilidad en el framework .NET permite la ejecución remota de comandos utilizando SharePoint
- Alerta CONDUSEF ante nuevos mecanismos de fraudes en terminales punto de venta
- Grupo MageCart instala skimmers digitales en distintos servicios que permiten pagos en línea
- El sitio WordPress de las Naciones Unidas expone miles de currículums

307,444 Total de eventos relacionados con servidores C&C de septiembre 2018

Direcciones IP de C&C únicas **10,873**

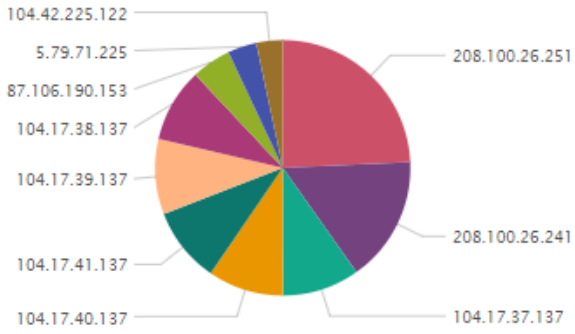
Distribución mundial de equipos C&C con afectaciones en México

Top de direcciones IP empleadas como servidores C&C

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

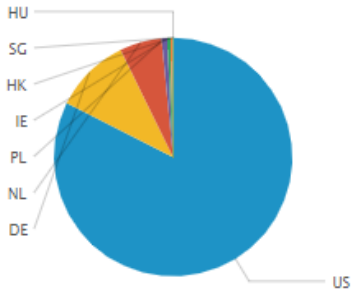
IP C&C	Eventos	%
208.100.26.251	51302	16.69
208.100.26.241	33605	10.93
104.17.37.137	20585	6.70
104.17.40.137	20236	6.58
104.17.41.137	20188	6.57
104.17.39.137	20132	6.55
104.17.38.137	19732	6.42
87.106.190.153	10517	3.42
5.79.71.225	7769	2.53
104.42.225.122	7043	2.29

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

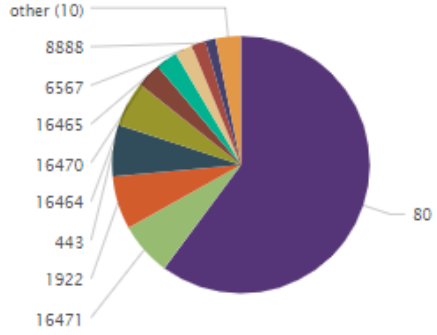


Imagen 1. Información general de los servidores C&C en México.

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 septiembre, 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
208.100.26.251	48,220	80	US
104.17.37.137	20,585	80	US
208.100.26.241	20,303	1922	US
104.17.40.137	20,236	80	US
104.17.41.137	20,188	80	US
104.17.39.137	20,132	80	US
104.17.38.137	19,732	80	US
87.106.190.153	10,499	443	DE
5.79.71.225	7,626	80	NL
104.42.225.122	7,043	80	US
87.106.18.156	6,799	80	DE
208.100.26.241	6,676	6567	US
104.155.224.46	5,407	8888	US
217.20.116.140	3,678	443	DE
46.165.254.212	2,751	443	DE
208.100.26.241	1,916	9251	US
107.170.198.33	1,759	80	US
148.81.111.121	1,710	80	PL
5.79.71.205	1,447	80	NL
46.244.21.4	1,364	7006	NL
208.100.26.241	1,225	8948	US
208.100.26.241	1,185	4794	US
192.42.119.41	1,148	443	NL
87.106.149.153	1,113	445	DE
87.106.149.145	1,092	445	DE
85.17.31.82	1,091	80	NL
212.227.20.93	1,081	80	DE
85.17.31.122	1,035	80	NL
192.42.116.41	907	3720	NL
178.162.203.226	867	80	DE
178.162.217.107	835	80	DE
168.63.134.179	828	16464	HK
52.169.189.46	771	16464	IE
208.100.26.241	746	8800	US
208.100.26.241	733	9676	US
192.42.116.41	725	443	NL
68.107.207.3	716	16464	US
85.17.164.15	690	16464	NL
74.208.153.19	657	445	US
208.100.26.251	611	3444	US
168.61.86.35	547	16471	IE
208.100.26.251	506	3123	US
40.71.228.10	465	16471	US
208.100.26.241	456	3618	US
192.42.119.41	444	80	NL
208.100.26.251	431	8916	US
212.227.20.116	425	80	DE
208.100.26.251	415	8370	US
87.106.20.192	381	445	DE
208.100.26.251	364	3775	US

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

En este periodo, se han identificado 60 puertos de comunicación únicos empleados por los servidores C&C, resaltando el puerto TCP 80 con una actividad del 60%. A continuación se muestra el top 10 de los puertos de comunicación utilizados con mayor frecuencia en este periodo.

Puertos	Peticiones
80	182,963
16471	20,356
1922	20,303
443	19,734
16464	17,236
16470	9,522
16465	8,276
6567	6,676
8888	5,407
445	3,912

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