MNEMO
NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

Agosto 2018

Reporte de Actividad de Botnets en México

DESTACADOS DEL MES

- **Banca peruana privada repele ciberataque mundial**
- **Vulnerabilidad en base de datos Oracle "CVE-2018-3110".**
- **Campaña de malware "Dark Tequila" afecta a usuarios de instituciones financieras en México.**
- Vulnerabilidad en GhostScript permite ejecución remota de comandos.

262,609 Total de eventos relacionados con servidores C&C de agosto

Direcciones IP de C&C únicas **2,716**

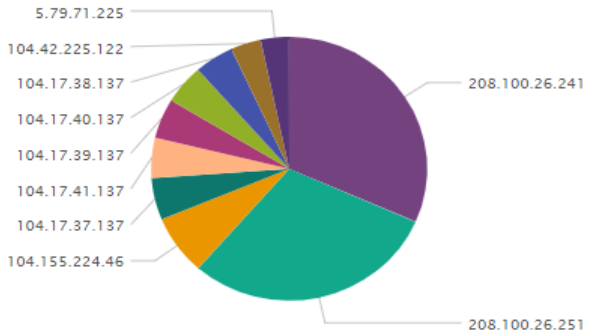
Distribución mundial de equipos C&C con afectaciones en México

Top de direcciones IP empleadas como servidores C&C

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

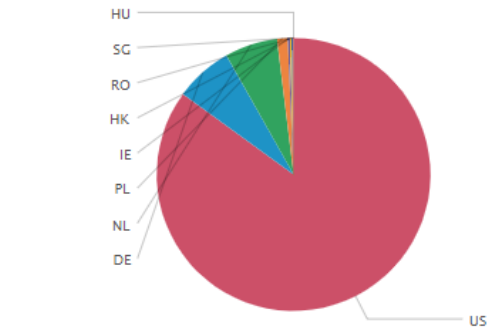
IP C&C	Eventos	%
208.100.26.241	67399	25.665152
208.100.26.251	63693	24.253929
104.155.224.46	15568	5.928205
104.17.37.137	10934	4.163604
104.17.41.137	10507	4.001005
104.17.39.137	10404	3.961783
104.17.40.137	10286	3.916850
104.17.38.137	9839	3.746635
104.42.225.122	7592	2.890990
5.79.71.225	7105	2.705543

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

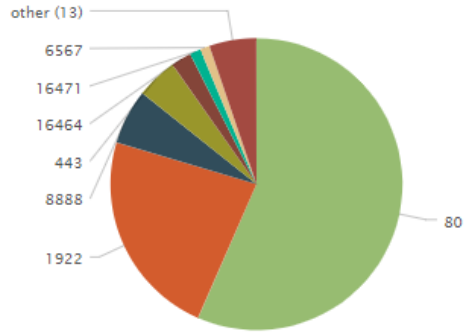


Imagen 1. Información general de los servidores C&C en México.

DESCRIPCIÓN

La actividad de Botnets que se describe se basa en 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 servidores C&C 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. 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 agosto, 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	62,576	80	US
208.100.26.241	58,837	1922	US
104.155.224.46	15,568	8888	US
104.17.37.137	10,934	80	US
104.17.41.137	10,507	80	US
104.17.39.137	10,404	80	US
104.17.40.137	10,286	80	US
104.17.38.137	9,839	80	US
104.42.225.122	7,592	80	US
5.79.71.225	6,964	80	NL
87.106.18.156	6,299	80	DE
87.106.190.153	4,147	443	DE
217.20.116.140	4,105	443	DE
208.100.26.241	2,684	6567	US
148.81.111.121	2,483	80	PL
208.100.26.241	2,335	9676	US
192.42.119.41	1,578	443	NL
46.244.21.4	1,351	7006	NL
107.170.198.33	1,184	80	US
192.42.116.41	1,059	443	NL
192.42.116.41	1,052	3720	NL
192.42.119.41	1,026	5050	NL
40.71.228.10	999	16471	US
208.100.26.241	873	4794	US
208.100.26.241	834	8948	US
5.79.71.205	678	80	NL
208.100.26.241	612	8800	US
208.100.26.241	549	9251	US
208.100.26.251	530	3444	US
192.42.119.41	523	80	NL
168.63.134.179	507	16464	HK
87.106.149.145	498	445	DE
212.227.20.93	490	80	DE
208.100.26.241	479	3618	US
85.17.164.15	469	16464	NL
85.17.31.82	451	80	NL
5.2.189.251	448	80	RO
52.169.189.46	448	16464	IE
85.17.31.122	441	80	NL
178.162.217.107	404	80	DE
68.107.207.3	400	16464	US
178.162.203.226	371	80	DE
148.81.111.121	292	65520	PL
192.42.116.41	282	80	NL
148.81.111.98	247	80	PL
168.61.86.35	223	16471	IE
174.78.129.185	184	16464	US
208.100.26.251	181	443	US
212.227.20.116	171	80	DE
163	208.100.26.241	7372	US

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

En este periodo se han identificado 92 puertos de comunicación únicos empleados por los servidores C&C, resaltando el puerto TCP 80 con una actividad del 55%. A continuación se muestra el top 10 de los puertos de comunicación utilizados con mayor frecuencia en este periodo.

Puertos	Peticiones
80	144,423
1922	58,837
8888	15,568
443	11,609
16464	5,699
16471	3,124
6567	2,684
9676	2,335
16465	1,906
7006	1,351

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 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 en 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.

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