Reporte de Actividad de Botnets en México

Abril

04/05/2018

I. Resumen

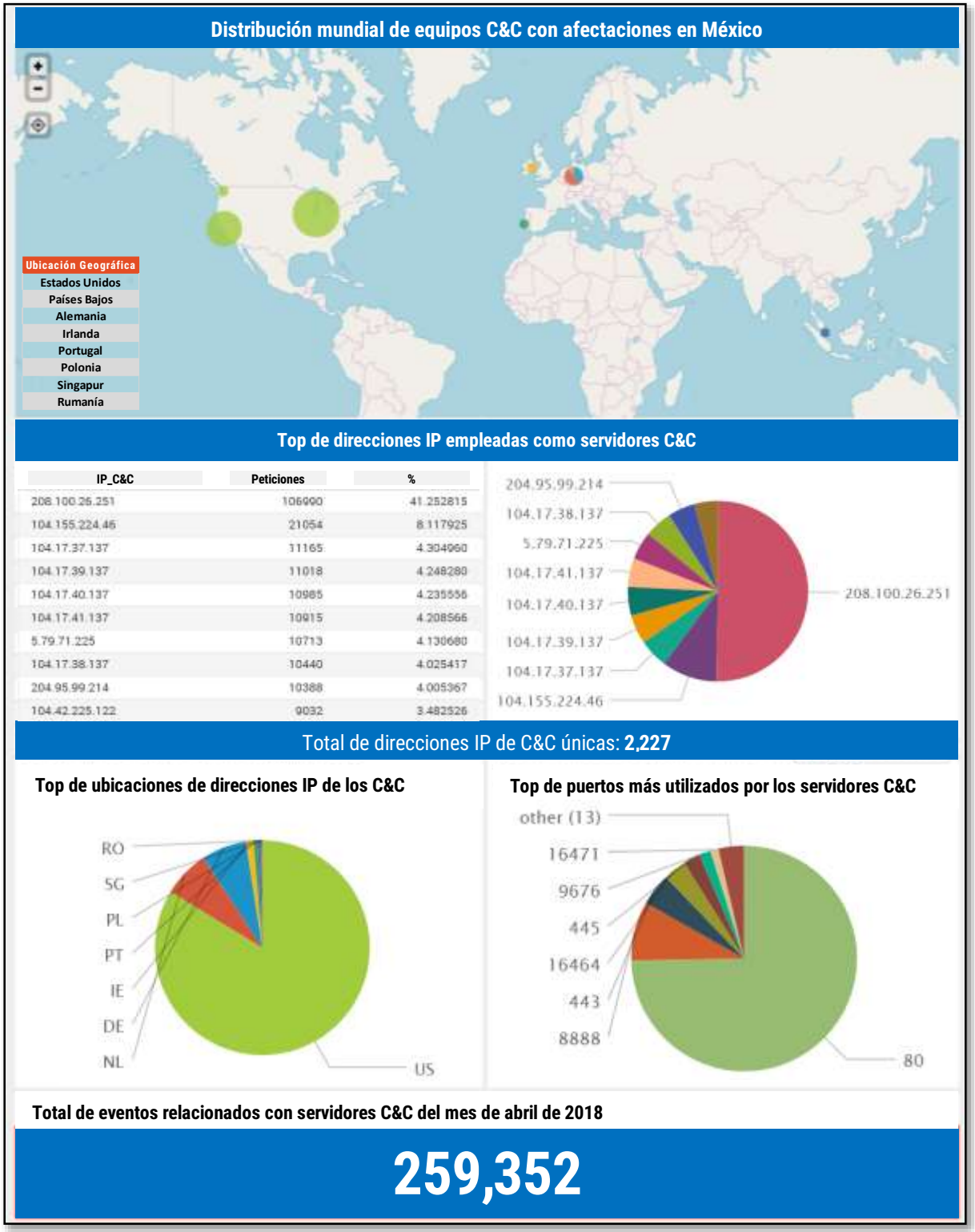

Imagen 1. Información general de los servidores C&C en México.

II. Descripción

El equipo de Respuesta a Incidentes de Ciberseguridad MNEMO-CERT identificó en el mes de abril de 2018 equipos en redes de México, utilizados para operar redes comprometidas de manera remota que son controladas por equipos de Comando y Control (C&C), de los cuales el 83.7% corresponde a direcciones IP ubicadas en Estados Unidos, 7% en Países Bajos, 6.8% en Alemania, 1.1% en Irlanda, 0.6% en Portugal, equivalentes a un total de [2,227] direcciones IP de servidores C&C.

A continuación se muestra un resumen del top 50 de las direcciones IP empleadas como C&C.

Peticiones	IP de C&C	Puerto Destino	Ubicación
102,676	208.100.26.251	80	US
21,046	104.155.224.46	8888	US
11,165	104.17.37.137	80	US
11,018	104.17.39.137	80	US
10,985	104.17.40.137	80	US
10,915	104.17.41.137	80	US
10,581	5.79.71.225	80	NL
10,440	104.17.38.137	80	US
10,388	204.95.99.214		US
9,032	104.42.225.122	80	US
5,634	217.20.116.140	443	DE
5,132	87.106.190.153	443	DE
3,001	208.100.26.251	9676	US
1,977	74.208.153.9	445	US
1,803	52.169.189.46	16464	IE
1,778	85.17.164.15	16464	NL
1,495	87.106.20.192	445	DE
1,420	5.79.71.205	80	NL
1,383	46.244.21.4	7006	NL
1,358	74.208.164.167	445	US
1,228	107.170.198.33	80	US
1,178	168.61.86.35	16471	IE
1,121	195.22.4.21	3720	PT
1,008	208.100.26.241	9676	US
928	148.81.111.121	80	PL
633	178.162.217.107	80	DE
587	85.17.31.122	80	NL
579	178.162.203.226	80	DE
569	68.107.207.3	16464	US
558	195.22.4.21	80	PT
557	85.17.31.82	80	NL
549	192.42.116.41	3720	NL
532	208.100.26.251	3444	US
476	87.106.149.145	445	DE
359	168.63.254.209	16465	SG
304	87.106.18.141	80	DE
290	212.227.20.93	80	DE
285	192.42.116.41	8000	NL
285	174.78.129.185	16464	US
247	208.100.26.251	443	US
237	192.42.116.41	80	NL
216	87.106.253.18	445	DE
183	87.106.18.112	80	DE
166	84.16.241.199	23	DE
163	174.71.176.74	16464	US
160	192.42.119.41	80	NL
158	108.175.9.190	445	US
154	213.165.83.176	23	DE
144	84.16.241.195	23	DE
142	46.244.21.6	23	NL

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

En este periodo se han identificado 44 puertos de comunicación únicos empleados por los servidores C&C, resaltando el puerto TCP 80 con una actividad del 72%. A continuación se muestra el top 10 de los puertos de comunicación utilizados con mayor frecuencia.

Peticiones	Puertos más utilizados
185,601	80
21,046	8888
11,603	443
8,068	16464
6,137	445
4,009	9676
2,865	16471
1,971	16465
1,692	23
1,670	3720

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

III. Recomendaciones

- 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, entre otros).

- 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.

Es importante mencionar que cuando un host es comprometido y es controlado desde un C&C, es susceptible de recibir instrucciones que podrían perjudicar la integridad, confidencialidad y disponibilidad de la información contenida en él. Algunas de las instrucciones que puede recibir el equipo infectado (bot) son las siguientes:

- 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 es una empresa especializada en servicios de ciberseguridad y seguridad de la información.

Sitio web: https://cert.mnemo.com
Facebook: MnemoCERT
Twitter: @mnemocert