MX

Las crónicas del DDoS

México

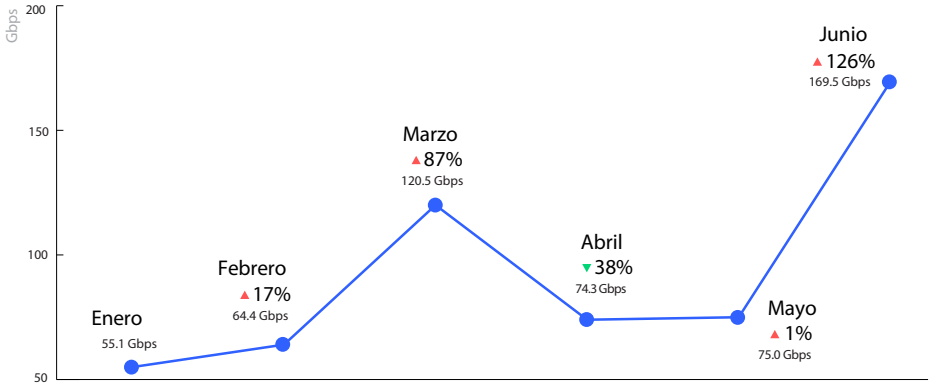
Indicadores clave del Informe de inteligencia de amenazas de NETSCOUT para el primer semestre de 2020

El 2020 se trató principalmente de "más": ataques más frecuentes, más rápidos y más complejos. Sin embargo, hubo una gran excepción: la duración del ataque, que se redujo más de un 50 por ciento a nivel mundial. También fueron más complejos, ya que los ataques con más de 15 vectores escalaron a un 126 por ciento de popularidad año tras año. Esto se suma a una mala ecuación para la defensa: duración más corta + mayor complejidad = menos tiempo para responder a escenarios de mitigación cada vez más difíciles. Esta estrategia de ataque probablemente se mantenga en el tiempo, lo que evidencia el rol esencial de una tecnología de DDoS avanzada y automatizada.

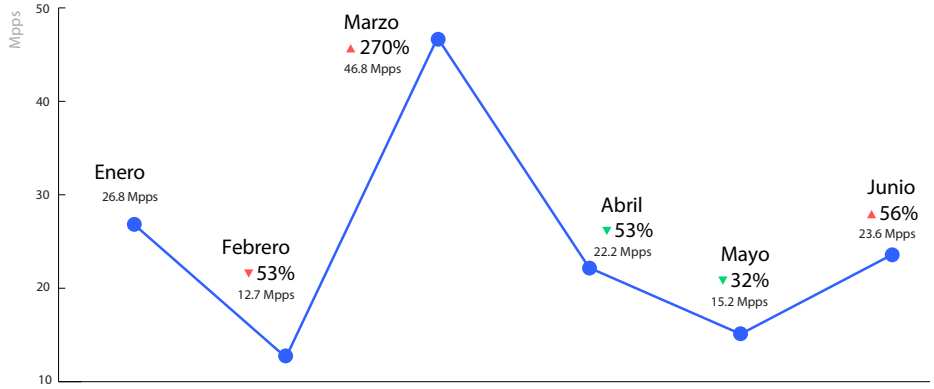
Análisis del impacto

Buscábamos comprender cuánto del tráfico que atraviesa la infraestructura de México se debe únicamente a ataques de DDoS. Para descubrirlo, creamos el coeficiente de ataques DDoS (DAC). El DAC representa la suma total del tráfico de DDoS que atraviesa cualquier región o país en un minuto. Esto nos permite identificar el tráfico de ataques DDoS que NETSCOUT observó entrando y saliendo del país en los últimos seis meses, en cualquier momento. Aquí, podemos ver claramente el enorme salto en ancho de banda y rendimiento durante marzo, el pico de la cuarentena por la pandemia.

CAMBIO EN PORCENTAJE DEL IMPACTO EN ANCHO DE BANDA



CAMBIO EN PORCENTAJE DEL IMPACTO EN RENDIMIENTO



Estadísticas de DDoS

Frecuencia de ataques	▲21%
Rendimiento máximo	▲55%
Duración promedio	▲51%

Ataque más grande

Tamaño	74.8 GBPS
Velocidad	19.9 MPPS
Duración	1,271 s
Tipos de ataques	AMPLIFICACIÓN DE NTP ICMP

Ataques por vector

Número máximo de vectores vistos en un ataque individual: **24**

Cinco principales vectores

VECTOR	N.º DE ATAQUES
ICMP	14,982
TCP SYN	13,432
TCP RST	10,854
AMPLIFICACIÓN de DNS	9,586
DNS	7,436

NETSCOUT

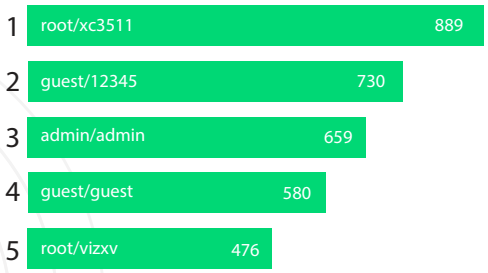
Diez principales segmentos bajo ataque

Analizamos los datos de ataques por códigos del Sistema de Clasificación de la Industria Norteamericana (NAICS), que agrupa a las empresas en 22 categorías amplias que incluyen múltiples grandes subsegmentos. La tabla de industrias a continuación muestra los sectores más atacados en 2020 ordenada por número de ataques, en comparación con el primer semestre de 2019.

CLASIFICACIÓN	SEGMENTO	FRECUENCIA	ATAQUE MÁXIMO	IMPACTO MÁXIMO	DURACIÓN PROMEDIO
1	**Telecomunicaciones**	**30,064** ▲60%	**118.9 Gbps** ▲102%	**526.5 Mpps** ▲55%	**1808.5 S** ▼28%
2	**Procesamiento de datos, alojamiento (hosting) y actividades relacionadas**	**1,185** ▲4%	**16.5 Gbps** ▲873%	**2.5 Mpps** ▲313%	**3856.6 S** ▲48%
3	**Servicios educativos**	**954** ▼28%	**5.2 Gbps** ▼80%	**0.4 Mpps** ▼91%	**4666.3 S** ▲47%
4	**Finanzas y seguros**	**387** ▼54%	**1.3 Gbps** ▼8%	**0.1 Mpps** ▼36%	**2273.4 S** ▲10%
5	**Servicios profesionales, científicos y técnicos**	**295** ▲768%	**0.3 Gbps** ▼73%	**0.03 Mpps** ▼77%	**1420.8 S** ▼56%
6	**Ejecutivo, legislativo y otro soporte gubernamental general**	**230** ▼47%	**1.7 Gbps** ▲242%	**0.8 Mpps** ▲981%	**2120.9 S** ▼12%
7	**Industrias editoriales (excepto Internet)**	**98** ▲188%	**0.7 Gbps** ▲181%	**0.1 Mpps** ▲244%	**1697.6 S** ▼3%
8	**Servicios públicos**	**83** ▼25%	**0.7 Gbps** ▼57%	**0.1 Mpps** ▼81%	**2887.8 S** ▲104%
9	**Distribuidores de materiales de construcción, equipos de jardinería y suministros**	**54** ▼70%	**0.2 Gbps** ▼51	**0.04 Mpps** ▼34%	**1806.5 S** ▼4%
10	**Bienes raíces, alquiler y arrendamiento**	**7** ▲600%	**0.1 Gbps** ▲888%	**0.02 Mpps** ▲867%	**1346.7 S** ▲9%

IoT

CINCO PRINCIPALES COMBINACIONES DE NOMBRE DE USUARIO Y CONTRASEÑA



CINCO PRINCIPALES EXPLOITS

NOMBRE DEL EXPLOIT	EDB-ID
/ctrlt/DeviceUpgrade_1 *Enrutador Huawei*	45991
/shell *MVPower DVR TV - Shell Command*	-----
/setup.cgi *Ejecucion remota de codigo Netgear*	43055
/ws/v1/cluster/apps *Hadoop YARN ResourceManager*	45025
/login.cgi *Varios dispositivos - ejecucion remota de codigo*	-----

Panorama general

En el Informe de inteligencia de amenazas de NETSCOUT para el primer semestre de 2020 encontrará la investigación más reciente acerca de tendencias y actividades del escenario de amenazas DDoS mundial.

LEA EL INFORME

NETSCOUT

SECR_020_ES-2001 10/2020