**DDOS WEAPONS & ATTACK VECTORS**

Attacks grow each year as the cyber landscape changes. A10 Networks tracked nearly 800,000 WS-Discovery sources for exposed IoT devices. China hosts nearly a quarter of observed DDoS botnet agents.

**ATTACK VECTORS**
- With the top ASNs where they connect.
- The top countries hosting DDoS weapons align closely

**TOP COUNTRIES WHERE DO ATTACKS ORIGINATE?**
- China 24%
- Brazil 9%
- Iran 6%
- Taiwan 4%
- Thailand 4%

**MALWARE DROPPERS**
- MALWARE DROPPERS
- Top malware drone source
  - Claro S.A.

**TOP ASNS**
- Top reflected amplifier source
  - Guangdong Mobile Communication Co. Ltd.
- Top malware drone source
  - Claro S.A.

**TOP IOT PORT SEARCHES**
- TCP PORT #
  - 8080
  - 5555
  - 2323
  - 60001
- UDP PORT #
  - 69
  - 53
  - 5353
  - 520

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- SSDP and SNMP remain the top sources for DDoS attacks, but
- but attacking drones are most often seen in Brazil.
- China hosts nearly a quarter of observed DDoS botnet agents

**WHERE DO BOTNETS LIVE?**
- 1. Brazil 9%
- 2. China 24%
- 3. Iran 6%
- 4. Taiwan 4%
- 5. Thailand 4%

**OTHER 53%**
- 6. South Korea
- 5. Hashemite Kingdom of Jordan
- 4. Romania
- 3. Argentina
- 2. Hong Kong

**ATTACKS’ FAVORITE PORTS**
- Malware family leads the pack so far.
- Launch amplified reflection DDoS attacks.
- Top protocols and countries of origin

**ATTACKS: TARGETS OF choice**
- Brand of choice for weaponized WS-Discovery
- Attackers are flocking to internet-exposed IoT devices

**ATTACKERS' FAVORITE PORTS**
- Top reflected amplification
- Top ASNs
- Worms and botnets thrive on

**DISARMING DDOS**
- Sophisticated DDoS threat intelligence, real-time threat detection,
- and automated signature extraction can help protect your
- organization against even the largest DDoS attacks.

**TRENDS**
- Top ports scanned for fresh TCP and UDP services to exploit.
- Over 800,000 DDoS weapons in Q4 2019.
- With reflected amplification, attackers exploit UDP-based protocols

**WHERE DO ATTACKS ORIGINATE?**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**TD&Ps and COUNTRIES OF ORIGIN**
- Over 800,000 DDoS weapons in Q4 2019.
- With reflected amplification, attackers exploit UDP-based protocols

**TOP TRACKED DDOS WEAPONS**
- Top malware drone source
  - Claro S.A.
- Top ports scanned for fresh TCP and UDP services to exploit.

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**TOP REFLECTED AMPLIFICATION**
- Top reflected amplifier source
  - Guangdong Mobile Communication Co. Ltd.
- Top malware drone source
  - Claro S.A.

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**WHERE DO BOTNETS LIVE?**
- 1. Brazil 9%
- 2. China 24%
- 3. Iran 6%
- 4. Taiwan 4%
- 5. Thailand 4%

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**ATTACKERS' FAVORITE PORTS**
- Malware family leads the pack so far.
- Launch amplified reflection DDoS attacks.
- Top protocols and countries of origin

**ATTACKS: TARGETS OF choice**
- Brand of choice for weaponized WS-Discovery
- Attackers are flocking to internet-exposed IoT devices

**ATTACKERS' FAVORITE PORTS**
- Top reflected amplification
- Top ASNs
- Worms and botnets thrive on

**DISARMING DDOS**
- Sophisticated DDoS threat intelligence, real-time threat detection,
- and automated signature extraction can help protect your
- organization against even the largest DDoS attacks.

**TRENDS**
- Top ports scanned for fresh TCP and UDP services to exploit.
- Over 800,000 DDoS weapons in Q4 2019.
- With reflected amplification, attackers exploit UDP-based protocols

**WHERE DO BOTNETS LIVE?**
- 1. Brazil 9%
- 2. China 24%
- 3. Iran 6%
- 4. Taiwan 4%
- 5. Thailand 4%

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**TOP REFLECTED AMPLIFICATION**
- Top reflected amplifier source
  - Guangdong Mobile Communication Co. Ltd.
- Top malware drone source
  - Claro S.A.

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**WHERE DO BOTNETS LIVE?**
- 1. Brazil 9%
- 2. China 24%
- 3. Iran 6%
- 4. Taiwan 4%
- 5. Thailand 4%

**MALWARE LOVES IT AND CAN’T WAIT FOR 5G**
- MIRAI LOVES IOT AND CAN’T WAIT FOR 5G
- Secure your devices
- By understanding the threats

**ATTACKERS' FAVORITE PORTS**
- Malware family leads the pack so far.
- Launch amplified reflection DDoS attacks.
- Top protocols and countries of origin

**ATTACKS: TARGETS OF choice**
- Brand of choice for weaponized WS-Discovery
- Attackers are flocking to internet-exposed IoT devices

**DISARMING DDOS**
- Sophisticated DDoS threat intelligence, real-time threat detection,
- and automated signature extraction can help protect your
- organization against even the largest DDoS attacks.

**TRENDS**
- Top ports scanned for fresh TCP and UDP services to exploit.
- Over 800,000 DDoS weapons in Q4 2019.
- With reflected amplification, attackers exploit UDP-based protocols

**WHERE DO BOTNETS LIVE?**
- 1. Brazil 9%
- 2. China 24%
- 3. Iran 6%
- 4. Taiwan 4%
- 5. Thailand 4%