**How DDoS Attacks Cripple Your Business**

**What is a DDoS attack?**
It's a malicious attempt by cybercriminals to prevent your legitimate visitors and customers from reaching your server.

**The DDoS Attack Disrupt & Halt Your Business Operations**

Legitimate traffic begins the connection process to the server. A DDoS attack floods the network with massive amounts of illegitimate traffic. Routers analyze traffic and attempt to connect users with server resources. Network and server resources become saturated and performance drops. User experience is significantly degraded or the website goes offline completely.

**Negative Consequences of DDoS Attacks**

- **Revenue Loss from Disruption & Outages**
- **Legal Ramifications**
  - Companies can face suspension and penalties for compliance violations.
  - Industries are starting to step up with DDoS guidelines on compliance, such as the Financial Institutions Examination Council (FFIEC).
- **Reputation Crisis**
  - 78% of security professionals said loss of customer trust was the #1 consequence of DDoS attacks.
  - Customer trust decreases
  - Lowered customer confidence
  - Potential to lose customers
  - Intellectual property loss
  - Brand damage
  - Lost prospect opportunities

A 2017 global survey showed that 849 companies averaged a revenue loss of $2.5 million.

**Revenue loss risk during DDoS Attacks:**
- 63% of companies risk losing $100,000 per hour
- 43% of companies risk losing $250,000 per hour

Average revenue lost $2,500,000 per month.

**Enterprise DDoS Attacks in the News**
- Github Knocked offline. DDoS attack peaked at 1.3 Tbs.
- 70% of Enterprises are victimized by 50 DDoS attack attempts per month.
- Average businesses are victimized by 8 DDoS attack attempts per day.
- Kaspersky Labs DDoS attack lasted 297 hours.
- Yahoo and Amazon faced $1.2 billion in damages to recover from DDoS attacks.
- Sony spent $170 million to recover from a DDoS attack.

**Where does DDoS Data come from?**

- **Botnets**
  - Compromised devices are grouped together to simultaneously flood a network with traffic.
- **Reflection**
  - Sending a large number of requests to devices and spoofing the reply IP to flood an IP with responses.
- **Amplification**
  - Publicly accessible DNS servers congest the network with response traffic.

**The highest global DDoS attack distribution % in Q1 2018 went to:**
- South Korea 10%
- China 48%
- U.S.A. 24%

**Top Four Benefits of DDoS Protection**
- No lost revenue due to service outages.
- Ensure maximum performance of your servers and websites.
- No bandwidth overage charges due to unwanted traffic from attacks.
- Protect brand reputation and customer confidence.

**How do you protect your website from a DDoS attack?**
Ensure your hosting provider includes these features in their DDoS Protection:
- **Instant Filtering**
  - DDoS attacks are detected and mitigated within 0 to 90 seconds.
- **Guaranteed Protection**
  - Protection against all known DDoS attacks.
- **Downtime Denied**
  - Legitimate traffic remains unaffected during attacks.

**Don't become a victim of a DDoS attack**
Visit [www.servermania.com](http://www.servermania.com) or contact sales@servermania.com today for a free DDoS assessment or to learn more about ServerMania.

**© 2018 ServerMania Inc., ® All Rights Reserved.**

[facebook.com/servermaniainc/](http://facebook.com/servermaniainc/)
[twitter.com/servermaniainc](http://twitter.com/servermaniainc)
[youtube.com/user/servermaniainc](http://youtube.com/user/servermaniainc)