THE Rise OF DrDoS ATTACKS
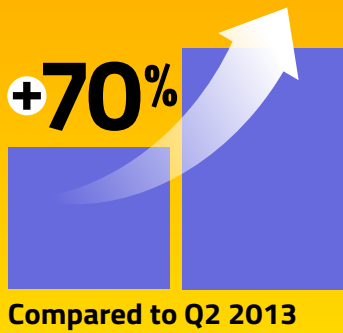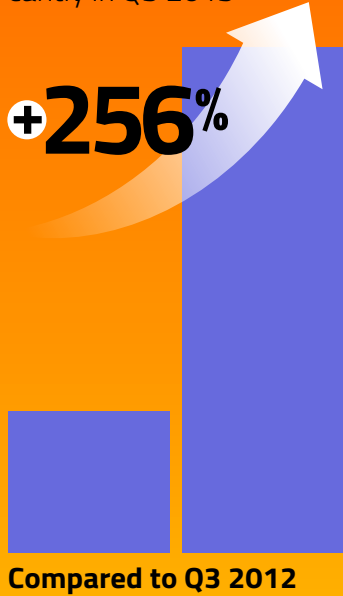
An emerging DDoS threat

Distributed reflection denial of service (DrDoS) attacks increased significantly in Q3 2013

+256%

Compared to Q3 2012

+70%

Compared to Q2 2013

DrDoS attacks explained

MALICIOUS ACTOR

PRIMARY TARGET

ERROR 404 File not found

VICTIM VICTIM VICTIM

PACKET1
Spoofed Source (Target)
Destination (Victim)

PACKET2
Reflected Packet Source (Victim)
Destination (Target)

- Intermediary victim machines unwittingly participate in an attack against the perpetrator's target
- Requests to the intermediary victims are redirected (reflected) from the secondary victims to the primary target

Why DrDoS usage is increasing

- Can obscure attack source (anonymity)
- Can hijack bandwidth of intermediary victims to multiply attack size (amplification)
- Increase in misconfigured servers worldwide
- Easier to obtain lists of misconfigured servers and IP addresses from underground Internet communities

The industries at risk

DrDoS attacks are being seen in most industries:

What you can do

- ✅ Turn off the CHARGEN service to stop this attack method
- ✅ Download the latest updates and patches for your servers
- ✅ Download Prolexic's *Q3 2013 Quarterly Global DDoS Attack Report*

LEARN MORE

To learn more about DrDoS attacks and read a detailed case study of this emerging threat, download a complimentary copy of Prolexic's Q3 2013 Quarterly Global DDoS Attack Report from *www.prolexic.com/attackreports*.

+1 (954) 620 6005
www.prolexic.com

PROLEXIC
DDoS Attacks End Here.