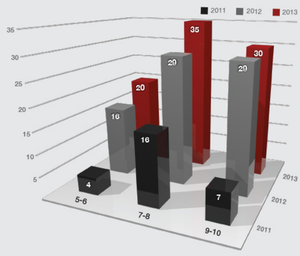
Attackers Up the Ante

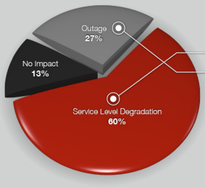
Change is headed your way whether you're prepared or not. As DoS/DDoS attacks continue to rise, concerns among organizations continue to grow. The 2013 Global Application & Network Security Report provides insight to help organizations better detect, mitigate and win the extended and persistent DoS/DDoS battle.

DoS/DDoS Attacks Leave Path of Destruction

DoS/DDoS attacks have increasingly become the weapon of choice for cyber-hactivist groups - like Anonymous and Cyber Fighters of Izz Ad-Din Al-Qassam. To quantify the severity of attacks, Radware uses a DoS/DDoS Risk Score that ranks DoS/DDoS attacks methodically by severity and assigns each attack a score between 1 and 10 (10 being the powerful). **2013 showed a 28% increase in DoS/DDoS attack scores of 8 and above, as compared to 8% in 2012.** And so the path of destruction begins.



Don't Be Fooled – Service Degradation is Enough to Interrupt Business



87% of respondents to Radware's Security Industry and Security Executive Surveys stated that they are likely to experience service level issues – **60% encounter service degradation and 27% experience outage.** While this may appear to be good news, targets of service degradation can experience negative financial impact, harmful effects on customer satisfaction, and brand equity. Not problems any organization wants to have.

The Industry Hit List Expands

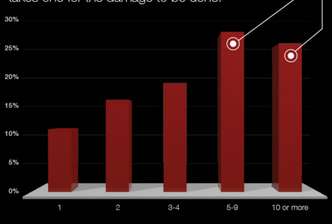
So who's up next? As the frequency and intensity of attacks increased, financial services felt the heat and joined government agencies in the DoS/DDoS Ring of Fire. 2013 hit both financial and government verticals hard, reinforcing the correlation between geo-political events and DoS/DDoS attacks. While these two remain a top target for DDoS attacks, cyber hactivists didn't stop. Hosting companies, ISPs and energy and utility companies changed position, and not for the better.

New Attack Vectors, One Dangerous Commonality

Several attack vectors emerged in 2013 causing significant issues for organizations. **50% of all Web attacks were encrypted application based attacks. 15% of organizations reported attacks targeting Web application log in pages on a daily basis. And DNS based volumetric floods increased from 10% to 21% in 2013,** becoming the second most common attack vector. But what makes them so dangerous? They're difficult to detect, require very few resources and can easily maintain anonymity. ***Need a better reason to improve network security?***

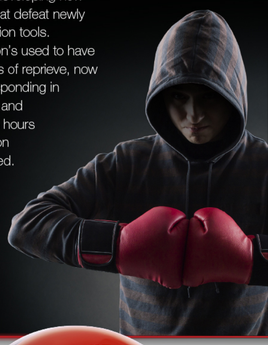
Not Just a Party of One Anymore – Multi-Vector Attacks Take Aim

More than 50% of attack campaigns deployed five or more attack vectors in 2013. Why? Attackers would rather keep the target busy by releasing one at a time, than launch the entire arsenal all at once. You may be successful at blocking four or five attack vectors, but it only takes one for the damage to be done.



And the Hits Just Keep on Comin' – Attackers (Quickly) Strike Back

Attackers drastically shortened the response time, developing new attack vectors that defeat newly deployed mitigation tools. While organization's used to have weeks or months of reprieve, now attackers are responding in a matter of days and sometimes even hours after the mitigation tools are deployed.



Prompt. **Protect.** **Prepare.**

Don't press the panic button just yet. You can keep your organization safe with a few simple steps.

Start now.

- **Timing is Everything** *Organizations need to look at time-to-mitigate as a key success factor, and ensure that thy solution they deploy provides the shortest time-to-mitigate.*
- **Fill in the Holes** *DDoS mitigation solutions need to offer a wide attack coverage that can detect from not just one attack vector, but also a multi-vector attack that hits different layers of the infrastructure.*
- **Single Point of Contact** *In the event of an attack, it's crucial to have a single point of contact that can be called to help divert Internet traffic and deploy mitigation solutions.*
- **Multi-Layer Approach** *Resolve the issues of single-point solutions with a cloud – based protection that blocks volumetric attacks and an on-premise solution that blocks all other, non-volumetric attacks.*
- **SSL Mitigation** *2014 is upon us and SSL attacks appear to be a major threat moving forward. Look for SSL based DoS/DDoS mitigation solutions with a deployment that doesn't affect the legit traffic performance.*

About Radware's ERT

The Emergency Response Team (ERT) has extensive experience handling attacks 'in the wild' as they occur. The findings in this report are a compilation of their front-line insights and formal surveys of worldwide security professionals on the state of cyber security.

radware
www.radware.com