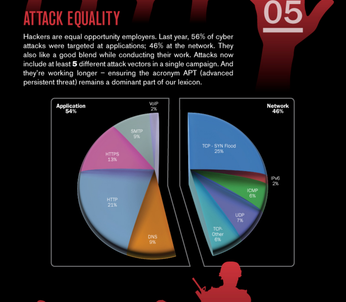
FALSE SENSE OF SECURITY

No Nostradamus, end-of-the-world, scare-mongering predictions here. We're tired of all the hype too. The "2011 Global Application and Network Security Report" analyzes the state of cyber security, exposing some important fallacies about DoS/DDoS attacks.

THE TIMES THEY ARE A-CHANGIN'

The motivation behind cyber attacks has changed dramatically over the years. In the beginning, it was youth in revolt with simple acts of vandalism and underground hackers seeking notoriety. Today's hackers have grown up and gone to work. Now it's all about getting rich, taking out the competition or the fight against injustice. **22%** of attacks are now forms of 'hactivism'. Almost makes you nostalgic for a simple Blaster worm.

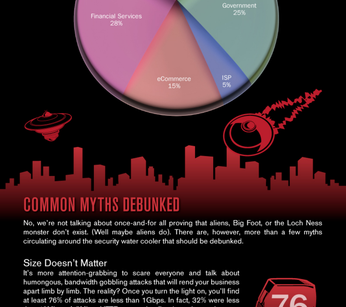
22



ATTACK EQUALITY

Hackers are equal opportunity employers. Last year, 56% of cyber attacks were targeted at applications, 46% at the network. They also like a good blend while conducting their work. Attacks now include at least **5** different attack vectors in a single campaign. And they're working longer – ensuring the acronym APT (advanced persistent threat) remains a dominant part of our lexicon.

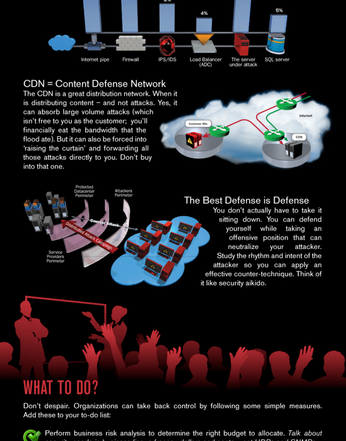
05



THE FRONT LINE IS EVERYWHERE

In times past, if you weren't on a specific hit list – then you gladly found yourself outside the 'ring of fire'. But groups like Anonymous and LulzSec have changed the playing field. New victims large and small, across sectors including e-gaming, e-commerce, energy, financial services, ISPs, wireless (even drug cartels!) now wake up daily to find themselves on the front lines. The top 3? Financial (28%), government (25%), and gaming (25%).

28



COMMON MYTHS DEBUNKED

No, we're not talking about once-and-for all proving that aliens, Big Foot, or the Loch Ness monster don't exist. (Well maybe aliens do). There are, however, more than a few myths circulating around the security water cooler that should be debunked.

Size Doesn't Matter

It's more attention-grabbing to scare everyone and talk about humongous, bandwidth-gobbling attacks that will rend your business apart limb by limb. The reality? Once you turn the light on, you'll find at least 76% of attacks are less than 1Gbps. In fact, 32% were less than 10Mbps. A 5Mbps HTTP connection flood attack can also stop you dead in your tracks. Don't fall prey to the hype.

76

Firewall and Fall Asleep

We're sorry firewall, but you are...the weakest link. Hackers love the firewall because it's so easy to overwhelm. **24%** of the time it's going to let you down as it fails first. So don't plug it in expecting to snuggle in all warm and secure for the night.

24

CDN = Content Defense Network

The CDN is a great distribution network. When it is distributing content – and not attacks. Yes, it can absorb large volume attacks (which isn't free to you as the customer, you'll financially eat the bandwidth that the flood ate). But it can also be forced into 'raising the curtain' and forwarding all those attacks directly to you. Don't buy into that one.

The Best Defense is Defense

You don't actually have to take it sitting down. You can defend yourself while taking an offensive position that can neutralize your attacker. Study the rhythm and intent of the attacker so you can apply an effective counter-technique. Think of it like security aikido.

WHAT TO DO?

Don't despair. Organizations can take back control by following some simple measures. Add these to your to-do list:

- Perform business risk analysis to determine the right budget to allocate. *Talk about security needs in business lingua franca - dollars and cents – not UDPs and SNMPs.*
- Make sure you're honest about the state of your security readiness. Identify potential security holes, have the right tools and people in place, and be wary of 'free' or 'bolt-on' tools. *Be a boy scout – be prepared.*
- Collect information about attacks such as type, size and frequency. *Use the correct measures per attack type.*
- Induct everyone in the security team. Responsibility for security is no longer the sole province of the security group. *It takes a village.*

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 survey of worldwide security professionals on the state of cyber security.

Download the "2011 Global Application & Network Security Report" at: http://www.radware.com/2011globalsecurityreport

radware ert

radware

www.radware.com