radware

RISE OF AUTOMATION
BRINGS BATTLE OF THE BOTS

2015 saw defenses succumb to new threats as the ability to choreograph responses in real-time diminished. **The Global Application and Network Security Report** reveals 2015 attack trends and offers predictions for 2016 as the rise of cyber botted defense approaches.

THE NEED FOR AUTOMATION

Attacks are becoming completely automated and more sophisticated, making it difficult to defend against them manually. New techniques like Burst Attacks and Advanced Persistent Denial of Service (APDoS), demand advanced detection and mitigation.

82% INDICATED MEDIUM TO HIGH DEGREE OF MANUAL TUNING

91% USE MULTIPLE SOLUTIONS

41% HAVE A HYBRID SOLUTION

21% INCREASE FROM LAST YEAR

PROBLEM
MULTI-VENDOR AND MANUAL

Most organizations rely on a collection of solutions that need manual intervention. Ninety-one percent of respondents are using multiple solutions and 82% indicated medium to high degree of manual tuning.

SOLUTION
HYBRID PROTECTION

Multi-vector attacks require a hybrid solution – integrating cloud-based with on-premise protection – to guard both networks and data centers. Forty-one percent of respondents have a hybrid solution, up from 21% in 2014.

Ransom notes used to be made of letters cut out of magazines; now they take a digital format. This year's research underscored a significant growth in ransoms as the primary motivator for cyber-attacks, increasing from 16% in 2014 to 25% in 2015.

CLOUD COMPANIES, BEWARE!
We predict you will experience significant RansomDoS (RDoS) in 2016.

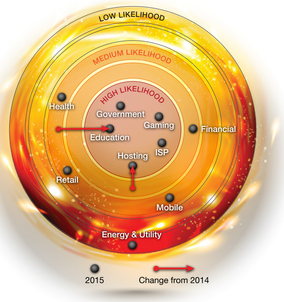
CYBER-ATTACKS
NONE IMMUNE; FEW PREPARED.

There is no safe haven. Ninety percent of respondents experienced attacks and 73% indicated they are only "somewhat effective" at mitigating cyber-attacks.

New risk levels apply to certain industries: both Education and Hosting moved from "Medium" to "High" risk in the Cyber Attack Ring of Fire while ISPs, gaming companies and government remain squarely in hacker's crosshairs.

73% "SOMEWHAT EFFECTIVE" AT MITIGATING CYBER-ATTACKS

90% EXPERIENCED ATTACKS



BATTLE OF THE BOTS

Bot-generated attacks targeting web application infrastructure and associated devices is growing in volume and sophistication. The report highlights key challenges organizations will have to conquer in 2016 to successfully thwart bot-generated attacks:

- Security on IoT devices is abysmal – technical adoption is paramount; security is an afterthought. 2016 will highlight risks to this rich data source – transforming the Internet of Things into an Internet of Zombies.
- One of the most important weapons in the bot battle is IP-agnostic bot detection.
- The ability to differentiate good bots should be a crucial capability of any device fingerprinting solution.

WHAT TO EXPECT

Bet on Bots and Automation.
Fight automated threats with automation technology.

Cover Blind Spots.
Attackers deploy multi-vector attack; if just one goes undetected, the attack is a success.

Plan Mitigation in Lockstep with Risk Level.
Prepare for increased industry risk and be mindful to how hacktivists operate and select targets. Understanding fuels preparation to defend your network.

DOWNLOAD THE FREE REPORT
2015 – 2016 Global Application & Network Security Report

radware ert

About the Emergency Response Team (ERT)

Radware's ERT is a group of dedicated security consultants who are available around the clock. As literal "first responders" to cyber-attacks, Radware's ERT members gained extensive experience by successfully dealing with some of the industry's most notable hacking episodes, providing the knowledge and expertise to mitigate the kind of attack a business's security team may never have handled.

radware
www.radware.com