APRIL 2016 NEUSTAR DDOS ATTACKS & PROTECTION REPORT

THE THREATSCAPE WIDENS: DDOS AGGRESSION AND THE EVOLUTION OF IOT RISKS

neustar®

CONTENTS:

INTRODUCTION

IN THIS REPORT:

THE GLOBAL RESPONSE TO PERSISTENT DDOS THREATS

In the winter of 2015, Neustar surveyed 1,005 directors, managers, CISOs, CSOs, CTOs and other c-suite executives to learn their levels of alarm, preparation and interaction with distributed denial of service (DDoS) attacks. Specific industries sampled include technology (18% of respondents), financial services (16%), retail (12%), and government (8%).

Globally, 79% of these organizations report yearly revenues of more than $100 million, with $1 billion or more in annual revenue.

Until now, Neustar has divided its findings into two separate versions: North America, and the EMEA (Europe, the Middle East, and Africa) regions. This report, which includes North America, Europe and Asia-Pacific, signifies a global view of the DDoS outlook, with insights and data from 6 continents and more than one thousand executives.

The findings are clear: DDoS attacks continue to pose a legitimate threat as a dangerous weapon used to create chaos and hold organizations hostage.

As we examine the trends of 2015, this report also looks at what the future portends for companies that have already invested in the Internet of Things (IoT), and demonstrates why security needs to be a central tenant for devices in the future.

73% OF GLOBAL BRANDS AND ORGANIZATIONS WERE ATTACKED

Slightly more than seven out of ten organizations reported a DDoS attack in 2015.

82% OF ATTACKED CORPORATIONS SUFFERED REPEATED ASSAULTS

More than 8 in 10 organizations were hit by multiple DDoS attacks. 45% were struck 6+ times.

56% OF THOSE BREACHED LEARNED OF THE ATTACK BY A THIRD PARTY

Evolved attacks continue to go unnoticed until it's too late.

MORE THAN HALF OF ATTACKED RESPONDENTS REPORTED THEFT

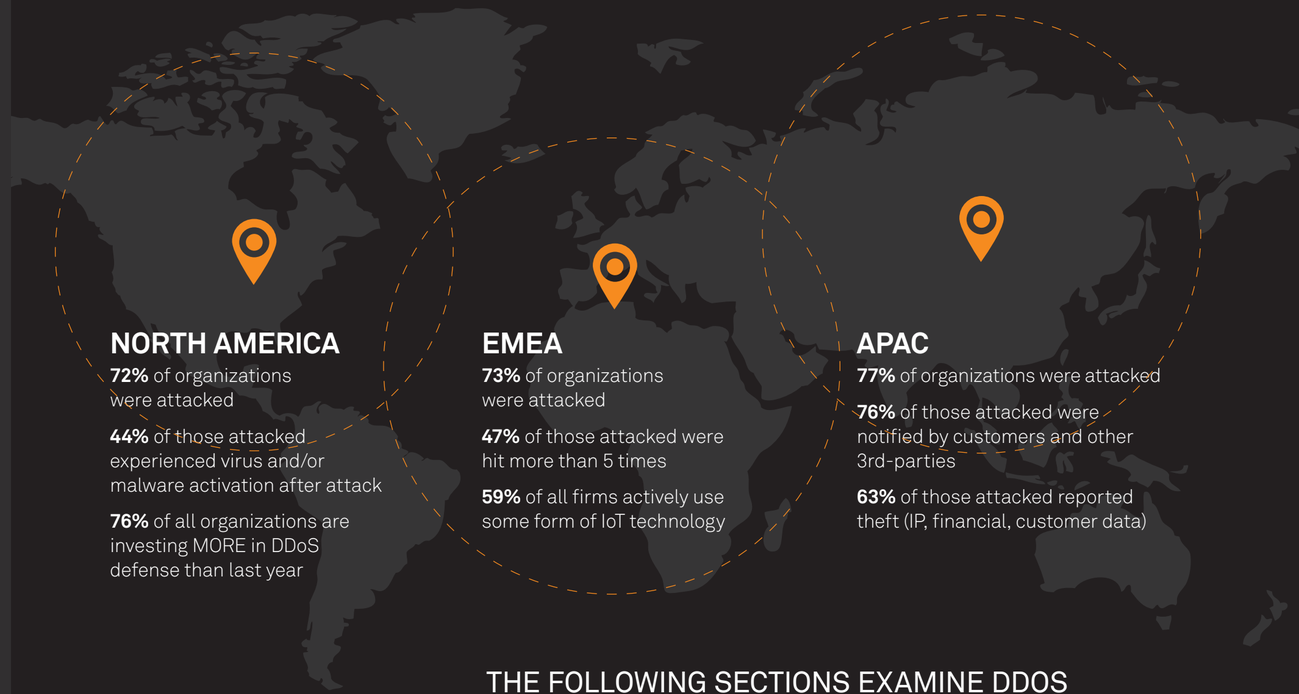
57% of attacked companies reported loss of customer data, finances or intellectual property.

EIGHT OUT OF TEN COMPANIES THAT HAVE IOT DEVICES WERE ATTACKED

43% of companies that use or deploy IoT devices have experienced some form of theft as the result of a breach.

76% ARE INVESTING MORE THAN LAST YEAR IN RESPONSE TO DDOS THREATS

DDoS is institutionalized, as both a weapon and necessity to defend.



NORTH AMERICA

72% of organizations were attacked

44% of those attacked experienced virus and/or malware activation after attack

76% of all organizations are investing MORE in DDoS defense than last year

EMEA

73% of organizations were attacked

47% of those attacked were hit more than 5 times

59% of all firms actively use some form of IoT technology

APAC

77% of organizations were attacked

76% of those attacked were notified by customers and other 3rd-parties

63% of those attacked reported theft (IP, financial, customer data)

THE FOLLOWING SECTIONS EXAMINE DDOS TRENDS IN 2015, AND DISCUSS WHAT THEY COULD MEAN FOR THE FUTURE.

THE RISK WORSENS

Attackers were unrelenting

DDoS attacks weren't a matter of if – or when – but how often.

Few organizations were spared

82% OF ATTACKED COMPANIES SUFFERED MORE THAN ONE STRIKE

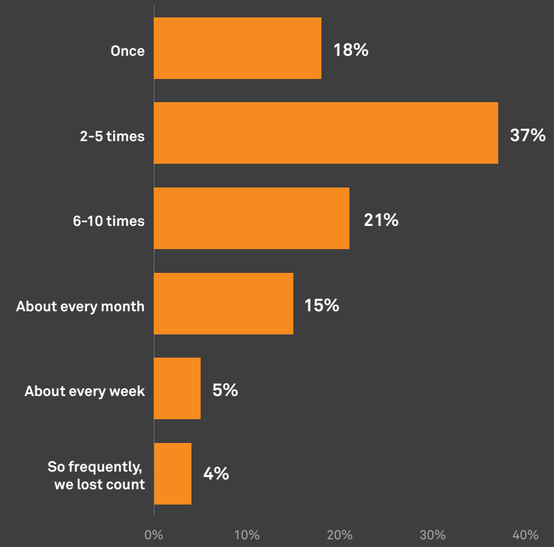
45% OF ATTACKED COMPANIES WERE HIT SIX OR MORE TIMES

The DDoS bombardment was constant and felt by nearly all. Every organization with a digital presence was put on notice: **YOU COULD BE NEXT.**

47%

47% of attacked EMEA companies were assaulted **6 or more times last year.**

2015 DDOS ATTACK FREQUENCY

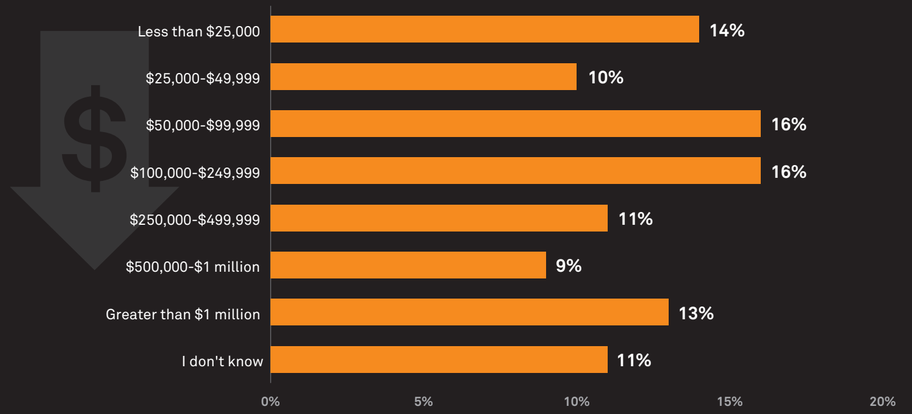


Globally, 81% of companies that adopted IoT were attacked.

More Money, More Problems

Worldwide, there's a global recognition of DDoS' destruction. With so much on the line – especially during peak periods – there's good cause for concern.

AVERAGE PEAK HOURLY REVENUE LOSS

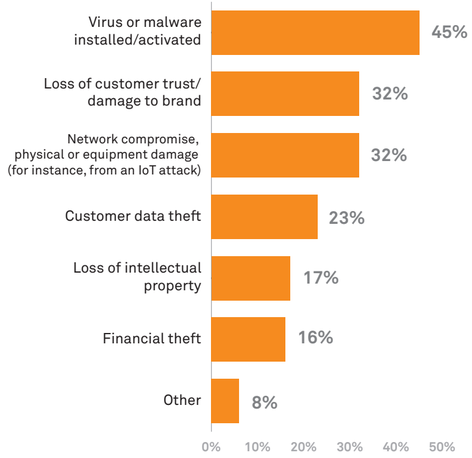


Globally, 50% of organizations would lose $100K or more per hour in a peak-time DDoS related outage. 33% would lose more than $250K or more.

Attacking with Purpose

Hackers left a wake of destruction in their paths, touching all parts of the enterprise and exposing valuable secrets.

RESULT OF DATA BREACH OR THEFT SUFFERED AS A RESULT OF DDOS ATTACK



*Multiple responses allowed.

57%
of all breaches involved some sort of theft – financial, intellectual or customer data.

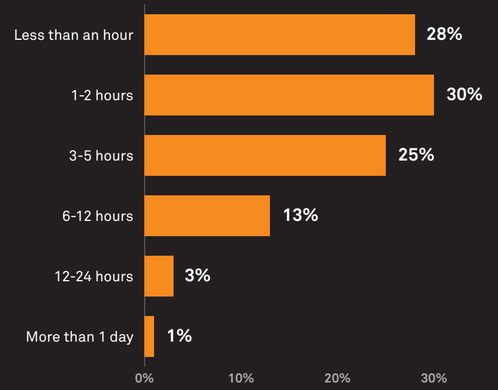
48%
of companies already invested in IoT reported virus or malware installation/activation.

More bad news for breached companies engaged in IoT: **73% reported loss of customer trust/damage to the brand as a result of an attack.**

You Can't Stop What You Can't See

42% OF COMPANIES TOOK 3 OR MORE HOURS TO DETECT A DDOS ATTACK ON THEIR INFRASTRUCTURE

LENGTH OF TIME TO DETECT A DDOS ATTACK



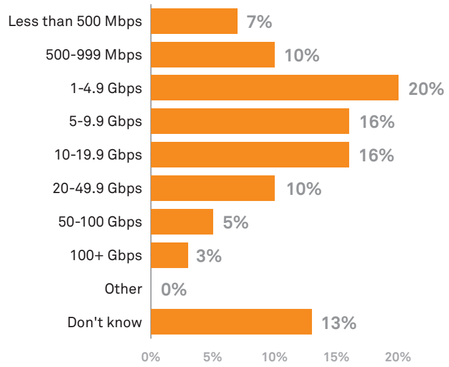
Almost half (46%) of EMEA companies took 3 or more hours to detect the attack.

As The Attacks Increase, So Does The Intensity

ATTACK SIZES WERE UP ACROSS THE BOARD, WITH NORTH AMERICA GETTING HIT ESPECIALLY HARD

53% of attacks in North America were 5Gbps or higher, big enough to cause a serious outage or service disruption.

BANDWIDTH OF TYPICAL DDOS ATTACK



38% of the organizations that adopted IoT were hit with DDoS attacks greater than 10Gbps.

DNSSEC
THE UNINTENDED CONSEQUENCE

Distributed denial of service attacks aimed at the domain name system (DNS) are nothing new. As an important, yet overlooked element of the Internet, DNS is responsible for connecting users to websites or devices. But since it's usually left unprotected, DNS is often a favorite reflective tool used to bombard targets. In other words, DNS needs protection; enter the domain name system security extension, or DNSSEC.

In addition to creating a layer of security around DNS, DNSSEC was also meant to stop cache poisoning – the ability of a hacker to hijack and redirect users to a nefarious website. But the sheer volume of encryption used to make DNSSEC secure can also be hacked and repurposed as an amplifying factor – turning a potential strength into a sizable weakness.

In fact, attacks that use DNSSEC as an amplifier can reach up to 100Gbps, more than enough to easily overwhelm standard DDoS mitigation defenses.

MULTI-VECTOR ATTACKS
PERSISTENCE PAYS OFF

In the early days of DDoS attacks, the goal was simple: launch a big enough attack to take the website offline. But as companies caught on and increased their defenses, hackers diversified their tactics, and are now using multi-vector attacks as a means to infiltrate.

Multi-vector attacks signal a troubling and persistent trend. Ranging in size and strike area, these attacks play out as a form of real-time interactive combat. If the initial assault is thwarted, attackers usually follow up with a series of coordinated strikes to keep the IT department guessing where and when the next attack will take place.

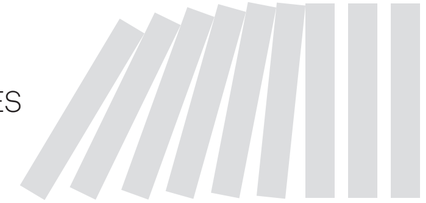
With three or four attacks taking place at the same time, the hacker knows it's tough for security to identify and mitigate all of the attacks. This assault on multiple fronts affords the opportunity to plant malware or viruses that often go undetected until it's too late. Attackers are persistent; they know it just takes one successful attempt.

MEASURING BUSINESS IMPACT

DDoS attacks are no longer "just an IT problem." From security to marketing, no department within an organization is immune from the effects of a DDoS attack. And when the attacks are successful, they indiscriminately affect the bottom line.

DDoS Domino Effect

WHEN AN ATTACK HITS, IT REVERBERATES THROUGHOUT THE ENTERPRISE



AREAS AFFECTED FROM A DDOS ATTACK

1. **Security**
2. **IT Group**
3. **Risk Management**

BUT THE IMPACT DOESN'T JUST STOP THERE.

In the Asia Pacific region, 1 out of 3 organizations said their BIGGEST cost increase came in customer-facing functions (Call Center, Customer Service and Marketing).

Every department within the organization drains additional resources in the wake of an attack.

Well, this is embarrassing…

One third of enterprises learned of an attack on their infrastructure from their customers.

IN THE ASIA-PACIFIC REGION, A THIRD PARTY ALERTED ORGANIZATIONS OF AN ATTACK **76%** OF THE TIME

How companies learned of the DDoS attack

Internal security and/or IT team	**79%**
Customer (and/or via Customer Service team)	**29%**
Partner	**22%**
Other Third Party	**6%**

*Multiple responses allowed.

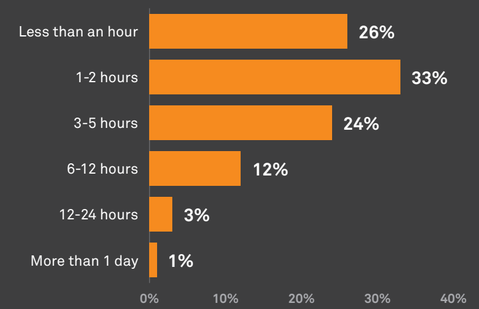
Among companies that are either using or have deployed IoT devices, **42% found out their infrastructure was under a DDoS attack by a third party,** putting their proprietary and customer personal information at a great risk.

Tick, Tock, Tick, Tock

Learning of the threat is great, but quickly responding to the threat is better – but not happening.

41% OF COMPANIES TOOK **3 OR MORE HOURS** TO RESPOND TO THE DDOS ATTACK

LENGTH OF TIME TO RESPOND TO DDOS ATTACK FOLLOWING DETECTION



In EMEA, 23% of companies that suffered an attack took 6 or more hours to respond. For the average company, that's more than half a million dollars a day lost during peak time periods.

See Something, Say Something

Information sharing is the latest trend, and for good reason.

47% OF PREVIOUSLY ATTACKED ORGANIZATIONS ARE PARTICIPATING IN SECURITY CONSORTIUMS

What extent is your IT team sharing threat info. and/or adopting new technology

Engagement with security consultants	**55%**
Participating in security consortiums to share threat information	**47%**
Proactively working with law enforcement to learn more about threat information	**41%**
Directly exchanging insights with other companies	**38%**
Working with law enforcement as a result of a previous breach	**35%**
Other	**3%**
None of the above	**3%**

*Multiple responses allowed.

Roughly 40% of the victimized companies are joining forces to share best practices and educate themselves on evolving DDoS threats.

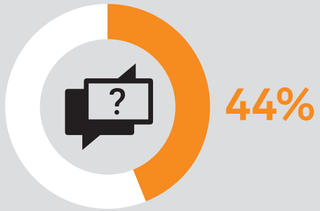
Financial Services:
AN EXPENSIVE BATTLEGROUND

Financial services institutions had their hands full fending off DDoS attacks in 2015. With big money, customer trust and regulatory implications on the line, 79% of financial services organizations surveyed are investing more this year than last.

As it turns out, the investments proved to be prudent:

43% put their hourly revenue loss risk at **more than $250,000**

62% of all financial organizations were attacked **more than once, 32%** were attacked **more than 5 times**



44% were informed of the attack **by their CUSTOMERS and other 3rd parties**

2 HOURS

THERE ARE MORE THAN 8,700 HOURS IN A YEAR. **DDOS ATTACKS CAN WREAK HAVOC IN JUST 2.**

63% of those attacked took **more than one hour** to detect

64% of those attacked then needed **at least one hour** before responding

As it turns out, six out of ten attacked organizations would lose at least $500,000 in revenues before putting the DDoS attacks down - but the losses didn't stop there. Costs spread across the organizations as 21% of those attacked stated that customer-facing operations (customer service, marketing, and call centers) experienced the largest cost increases. And yet, the bad news continued – 71% reported a form of theft (customer data, financial assets, intellectual property) compared to the overall rate of 57% for all industries.

Since attackers know where the prized targets are, they launch methodical strikes that combine complexity and aggression to fulfill their intentions. As attack activity continues to ramp up, financial services firms will need to be even more vigilant against direct DDoS assaults and smokescreen attacks that shield other sinister actions.

EXAMINING PROTECTION TRENDS

Investments rise to meet the looming threats.

The Arms Race is On

The tangible response to an imminent danger

76% OF COMPANIES ARE INVESTING MORE IN DDOS PROTECTION

80% OF ORGANIZATIONS IN THE ASIA-PACIFIC REGION ARE INVESTING MORE THIS YEAR THAN LAST YEAR

WHETHER INVESTING MORE OF ANNUAL BUDGET

YES

Yes, investing more than a year ago, but should invest even greater	**39%**
Yes, investing more than a year ago, in proportion to the threat of DDoS attacks	**37%**

NO

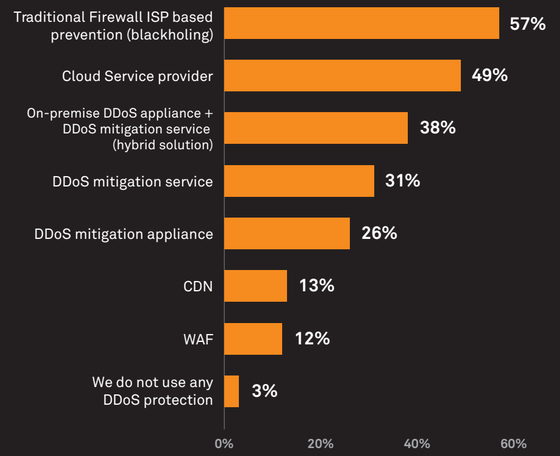
No, not investing more than a year ago, although DDoS threats considered high priority	**16%**
No, not investing more than a year ago, and DDoS threats not considered high priority at this time	**5%**
No, currently no budget specifically for DDoS defense	**3%**

84% of organizations that adopted IoT are investing more in DDoS defenses than they did last year. One reason why – 47% were attacked more than 5 times in the last 12 months.

The Cloud's Silver Lining

ALMOST HALF (49%) OF RESPONDENTS ARE TURNING TO THE CLOUD TO PROTECT THEIR INVESTMENTS AND INFRASTRUCTURE

TYPES OF DDOS PROTECTION USED



*Multiple responses allowed.

IOT – INVESTING IN A SECURE FUTURE

The Internet of Things is here. But how secure is it?

IoT right N-O-W

63% OF COMPANIES ARE ALREADY USING IOT DEVICES

Best describes current adoption of connected IoT

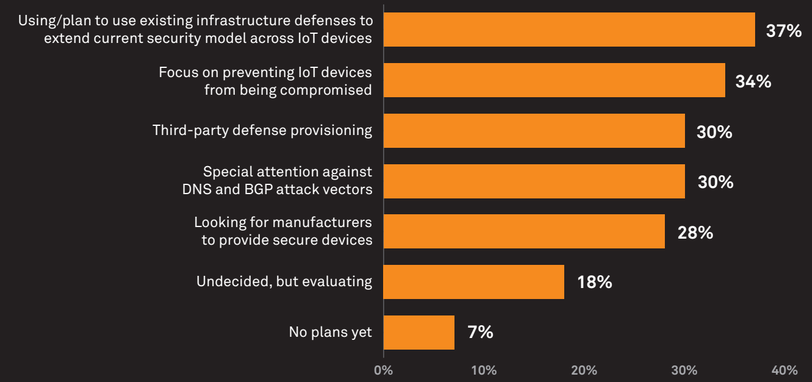
Some devices have been deployed and data being collected and analyzed. Closed vertical solutions in place	**32%**
Actively using connected sensors and actuators to improve process control, provide higher operating efficiency	**31%**
Evaluating deployment scenarios and prioritizing likely candidates for trial purposes in the next 6 - 12 months	**18%**
Some consideration and early stage planning, no current timeline, decision in the next 12 - 18 months	**11%**
Currently no plans or need for adoption	**8%**

By 2017, 81% will either use or deploy an IoT device.

IoT Already Vulnerable

SOME SCARY NEWS: JUST 34% ARE FOCUSED ON PREVENTING IOT DEVICES FROM BEING COMPROMISED

PREVENTION OF IOT DEVICES FROM BEING USED TO CREATE OR BECOME THE TARGETS OF DDOS ATTACKS



*Multiple responses allowed.

Almost one-third of companies are outsourcing the security of their IoT devices.

WHY IOT GIVES US A SECOND CHANCE TO IMPROVE SECURITY

AN INSIDER'S THOUGHTS

Hank Skorny, Senior Vice President, IoT, weighs in on security and IoT

IoT is not a distant concept. It's in the lights that know our preferences the second we enter a room, it's in the engine sensor that provides us with unprecedented reliability and efficiency while we drive to see our loved ones, it's in the chip that accurately measures our vitals when we're pushing ourselves at the gym, and it's the AEDs (automatic defibrillators) that save lives. The fact is, IoT is already here; but unfortunately its security is too often lagging behind.

The Internet was never built with security in mind; ease of use and convenience were paramount. This came at the cost of security, a fact we're reminded of far too often. Today, we have the opportunity to learn from our mistakes and make security a cornerstone of every IoT device moving forward. From design conception to product sunsetting, every IoT device, sensor, and software system needs a multi-tiered security driven approach, including timely patches and updates. Just as important, or perhaps more so, is for security to be an intrinsic part of every network. Network based security is essential in a world where there are a massive number of devices connected with little ability to monitor the state of every one or in some cases even access the device embedded in a remote area.

Every IT professional knows it can take just one successful hack on an IoT device to access and compromise an entire network. As we continue to ingrain IoT devices into our electrical grid, hospitals, assembly lines and other essential areas of life, the stakes are too high to leave security to chance. Let's get this right the first time.

SUMMARY

5 KEY TAKEAWAYS FROM THIS REPORT

1. **Attacks Aplenty.** Worldwide, 73% of companies suffered a DDoS attack, with almost half (45%) struck six or more times. In EMEA, 47% of organizations were assaulted 6 or more times.

2. **Leaving a Lethal Legacy.** After the breach, 45% of attacked organizations reported the installation of a virus or malware - a troubling sign of the attacker's intent to cause harm beyond the initial intrusion.

3. **The Response is Real.** Overall, 76% of respondents are investing more in DDoS defense. In the Asia-Pacific and EMEA regions, those numbers are 80% and 77% respectively. DDoS' lethality is a certified threat.

4. **It Takes a Village.** Around the world, companies are motivated to share threat intelligence. 47% of the previously attacked companies are actively participating in security consortiums to learn what works in the evolving threat against DDoS attacks.

5. **Prepare for IoT NOW.** 81% of companies that adopted IoT were attacked in 2015, with 43% reporting theft of finances, customer data and/or intellectual property. Now is the time to build the devices around security, rather than the other way around.

We present this data as a means to inform the public of the dangers associated with DDoS attacks, and start a conversation about the importance of cybersecurity. As we prepare to further integrate IoT into our daily routines, it remains to be seen how IoT – and its security – will affect our lives. Will more attacks be thwarted as a result of better defenses? What will be the next big attack vectors? We look forward to continuing the conversation with you in subsequent reports and via our Twitter handle, @NeustarCTO.

TO LEARN MORE ABOUT DDOS PROTECTION, VISIT Neustar.biz/services/ddos-protection

Neustar defends organizations from DDoS attacks by utilizing top-notch technologies, expertise and personnel. Neustar SiteProtect, our DDoS mitigation service, provides features capable of scaling to meet your level or risk, budget and technical environment. Whether it's cloud-based, on-promise, always on, or a hybrid, Neustar's protections are customizable to meet client demands. SiteProtect is backed by the Neustar Security Operations Center, whose experts bring years of knowledge to blocking attacks and safeguarding enterprises.

ABOUT NEUSTAR

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz**.

neustar®

www.neustar.biz

RPRT-DDOS-XXXXX 04252016