# Table of Contents

**Forward: Attack Levels Steady, but Attacker Impact Rises**  
02

## Part One: The Landscape  
04
- Executive Summary
- As Attack Rates Have Grown, so Has Impact
- Regional Combat, Consistent Threats
- Managing the Risk
- When Risk Gets Real
- IoT Paradox: Cyber Target and Business Advantage

## Part Two: Conflict and Consequences  
22
- Detection and Response
- Impact
- Major Industry Fights Against DDoS

## Part Three: Defense Investment Trends  
34
- Investment Trends
- Behind DDoS Defense Investment
- The Rise of WAF

## Summary: Strategic Considerations  
42

## About Neustar  
44
Twice a year, Neustar produces insights into the risks, tempo, and impact of Distributed Denial of Service attacks (DDoS) as organizations continue to conduct more operations and commerce online. A few years ago, much of the business community was still coming to grips learning and understanding how these attacks operated in order to protect their infrastructures. It’s become a much different world since these attacks emerged more formally as threats to the conduct of digital business. Organizations are more aware, security teams are more capable and defenses are more mature in the face of attackers who are craftier and more dangerous. However, there is something much more different now than just a few short years ago – the infrastructure of today’s connected world. The situation has drastically changed from static and stationary infrastructures awaiting an attack to large, multi-dimensional and interconnected enterprises. In many workings of today’s online operations, there are unknown third party dependencies extending from known third party dependencies that many operating organizations may never see, yet nevertheless, incur additional vulnerability.

The emergence of cloud computing and the explosive popularity of Internet of Things devices (IoT) as viable, if not crucial, elements in competing successfully for customers, for revenue and for reputation is unprecedented. This has delivered greater opportunity at a pace only matched by the vulnerabilities by the countless, and some might say inextricable, interdependencies composing the modern enterprise. Combined with the presence of cloud-based applications, a growing and exploitable source for the spread of malware, today’s organizations susceptibility to DDoS attacks is an ever-present threat.

In this latest release of global research we see that the risk and impact from DDoS attacks remains high. In May 2017, organizations around the world reported a fever pitch of harmful and overwhelming DDoS attacks, but they also announced an overwhelming intention to invest in better defenses and get back out in front of trouble. In the following pages, we see an increase in those investments and a return of attack levels similar to Fall 2016. Attack rates remain high, but rather troubling is the increased success attackers have had in breaching organizations while using DDoS as part of the assaults.

Determined DDoS attackers are running into more determined defenders, but unfortunately they are achieving more breach success than a year ago, especially in terms of reported theft. As digital transformation to cloud technologies in the modern enterprise continues to take hold, organizations will need to evolve protection strategies and continue to work to counter ever-evolving DDoS assaults.
In May 2017, the news was dismal as DDoS attacks and their impact had reached a fever pitch. Companies were reeling, attackers were succeeding, and the search for answers to effectively defend against unprecedented DDoS attacks was a struggle for many organizations. While 2017 has been an active year for online attacks, it has not yet seen a significant DDoS event. There has been plenty of industry speculation about the building of hostile attack networks from compromised Internet of Things device (IoT) networks, even the selling of computing power from unsuspecting server farms. Compared to this time in 2016, attack rates have slightly risen and unsolicited, disruptive internet traffic is a reality. The high investment rates in sophisticated DDoS defenses, especially the large jump in Web Application Firewall (WAF) deployments, show that this threat has been institutionalised in the thinking of security professionals.

To provide an accurate and global picture of DDoS’ ramifications in our connected world, Neustar commissioned global, independent research of 1,021 directors, managers, CISOs, CSOs, CTOs, and other c-suite executives to find out how distributed denial of service (DDoS) attacks affect their organizations and what measures are in place to counter these threats. Our current findings show that although attack quantities have slightly decreased, the rate of breach per attack has increased. Attackers are more deliberate, targeting victims with malicious precision. This research represents the second installment of our 2017 bi-annual effort to track and highlight changing trends in the global DDoS threat landscape.

We surveyed participants across six continents and categorized their responses into three distinct regions. The regions include: North America, Europe, and Asia-Pacific (APAC). The respondents span many industries including technology (19%), financial services (15%), retail (12%), healthcare (7%) and energy (4%).

Nearly half (41%) of the organizations reported annual revenues from $500M to $1B per year. On the large enterprise side of the equation, one quarter (24%) of those surveyed claimed $1 billion or more in annual revenue. As for revenue risk amongst these organizations, 49% of the respondents from this cross-section of organizations stated that at least $100,000 per hour is at risk during peak revenue generation periods.

**Increase in breach incidents experienced in concert with DDoS attacks.**

27%
### ROLE

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTO</td>
<td>9%</td>
</tr>
<tr>
<td>CISO/CSO</td>
<td>7%</td>
</tr>
<tr>
<td>CRO</td>
<td>2%</td>
</tr>
<tr>
<td>VP/SVP</td>
<td>7%</td>
</tr>
<tr>
<td>Director</td>
<td>22%</td>
</tr>
<tr>
<td>Manager</td>
<td>44%</td>
</tr>
<tr>
<td>Other</td>
<td>9%</td>
</tr>
</tbody>
</table>

### INDUSTRY

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology (SaaS, IaaS, manufacturers, etc.)</td>
<td>19%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>15%</td>
</tr>
<tr>
<td>Retail</td>
<td>12%</td>
</tr>
<tr>
<td>Healthcare/Pharma</td>
<td>7%</td>
</tr>
<tr>
<td>Government/Public Sector</td>
<td>7%</td>
</tr>
<tr>
<td>Education</td>
<td>5%</td>
</tr>
<tr>
<td>Internet Services (ISP, social networks, etc.)</td>
<td>5%</td>
</tr>
<tr>
<td>Telecommunications or Cable</td>
<td>4%</td>
</tr>
<tr>
<td>Energy/Utility</td>
<td>4%</td>
</tr>
<tr>
<td>Ecommerce/E-tail (100% online sales)</td>
<td>2%</td>
</tr>
<tr>
<td>Media &amp; Advertising (ad agency, media, publisher)</td>
<td>1%</td>
</tr>
<tr>
<td>Video Gaming/Online Gambling</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>18%</td>
</tr>
</tbody>
</table>

### ANNUAL REVENUE

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$50-99M/£30-49M</td>
<td>29%</td>
</tr>
<tr>
<td>$100-499M/£50-299M</td>
<td>30%</td>
</tr>
<tr>
<td>$500-999M/£300-499M</td>
<td>17%</td>
</tr>
<tr>
<td>$1B+/£500M+</td>
<td>24%</td>
</tr>
</tbody>
</table>
The global statistics over the past three years reflect the significant rise and complexity in DDoS activity. The findings reflect a rolling twelve-month window and offer views into what organizations experienced and how they contended with DDoS attacks leading up to the close of these reporting windows.

The investment trend to improve DDoS defenses on the heels of a brutal 2016 was fueled by an overwhelming number of organizations attacked worldwide. Greater threat awareness, high profile outages, and seemingly indefensible assaults all appeared to increase a desire by organizations to detect and respond more quickly. Still, organizations were slower to checking DDoS danger because threats had eclipsed defense strategies and technologies in place or because of a still growing understanding of vulnerability to DDoS. Although, speeds in detection and response have slightly improved in the past seven months these times are slightly higher than they were this time last year. Many organizations attacked had been notified of the attacks from outside parties with nearly half of notifications coming from customers. This does offer some hope that DDoS defense investments are at least starting to arrest attacker momentum – good news for an online community that has been getting the worst of it for the past year.

This is good progress, but despite modest improvement, attackers are having greater impact, especially when it comes to many associated breach activities that are synchronized with DDoS offensives. One third of organizations are being notified of DDoS attacks and/or related impact from their own customers and this is still too high. As well, if attacked, the chances of being attacked again remains highly probable – 76% of those attacked were forced to contend with multiple attacks.

Nine in every ten organizations acknowledged some form of breach or associated activity with DDoS attacks.
Three-year Trends

Summary stats comparing 2015–2017

The following tables show the current state of reported DDoS activity compared to 2015 and 2016. Overall, attack rates and results have decreased modestly from the chaotic pitch of the 2016–2017 straddle. Of the 1,021 organizations reporting, 772 had been attacked with DDoS at least once in the previous 12 months, 588 more than once, and 271 fended off more than 5 attacks each.

Unfortunately, the average rate of breach against organizations attacked with DDoS is up from this time last year. Nine in every ten organizations acknowledged some form of breach or associated activity with DDoS attacks. Given the three year trend, this is not surprising as attackers achieved 1,646 breaches against 772 organizations attacked (2.1 breaches per attacked target) compared to 1,423 breaches against 730 attacked organizations one year ago.

DDoS Attack Rates with Breach Comparison

Global DDoS Attacks & Cyber Security Insights Report
ATTACK EXPERIENCE

- 80% of organizations were attacked.
- 73% of revenue was at risk due to attacks.
- 37% were attacked once.
- 29% were attacked more than once.
- 40% were attacked more than 5 times.

DETECTION AND RESPONSE

- 67% found out about the attack from 3rd-party sources.
- 36% found out from customers.
- 48% required a minimum of 3 hours to detect the attack.
- 45% required a minimum of 3 hours to respond.

ATTACK TRAITS

- 42% of attacks were below 5 Gbps.
- 44% were between 5 Gbps and 50 Gbps.
- 8% were above 100 Gbps.

Global DDoS Attacks & Cyber Security Insights Report
DDoS attacks were well distributed across major industries and organizations of differing annual revenues. Not contained to large enterprises alone, which represented less than a quarter of all of those attacked, the targeting and impact hit growing and mid-sized organizations the hardest – 60% of those attacked reported less than $500M USD in yearly revenue.

**OROrganizations Attacked With DDoS by Annual Revenue Segment**

- **$1B+/£500M+**: 22%
- **$50-99M+/£30-49M**: 28%
- **$500-999M+/£300-499M**: 32%
- **$100-499M+/£50-299M**: 18%
Attack sizes are mixed, with more than half of the average size attacks peaking at less than 10 Gbps. The chance of repetitive attacks against the same targets remains highly probable despite a rise in the number organizations being attacked only once. New tool kits and exploits fueled by an ongoing sharing and selling of attack code means attackers have more than enough means by which to marshal resources. Here’s how average attack sizes compare YoY with the same reporting period in 2016.

Higher breach yield on fewer attacks conducted at a high pace of repetition offers indications that attackers remain cunning, patient, and determined without having made as much noise as in previous months.

Attack sizes have generally risen, but half average less than 10 Gbps which reveals determined targeting.
Regional Combat, Consistent Threats

Compared to one year ago as reported in the fall of 2016, organizations are encountering relentless pressure from attackers. Overall, once attacked, three quarters of those who endure DDoS efforts must contend with repetitive attempts.

**Frequency Organization Experienced a DDoS Attack in Previous 12 Months**

- Once: 24% (2017), 15% (2016)
- 2-5 times: 41% (2017), 40% (2016)
- 6-10 times: 19% (2017), 19% (2016)
- About every month: 11% (2017), 14% (2016)
- About every week: 3% (2017), 7% (2016)
- So frequently, we lost count: 2% (2017), 4% (2016)
Interestingly, of those who reported being attacked only once, the number of those organizations in North America and Europe nearly doubled while respondents in APAC fought at a steady pace. Greeting attackers with stronger defenses may be acting as a deterrent, but the results are mixed showing that breaches are occurring at serious rates regardless of frequency.

As a collective, this group of attacked organizations overwhelmingly was impacted by breaches as these volumes show.
So frequently, we lost count

About every week

About every month

2-5 times

6-10 times

Once

ATTACK FREQUENCY

NORTH AMERICA | EUROPE | ASIA PACIFIC

GLOBAL DDoS ATTACKS & CYBER SECURITY INSIGHTS REPORT
Individually, organizations experienced differing probabilities of specific breaches that accompanied DDoS attacks. For example, organizations that were attacked just once experienced a 35% chance that they saw malware activated.

Cyber attackers using DDoS as a tool to accomplish other goals, such as implanting and activating malware, had success over defenders which shows how much more work needs to be done to frustrate their efforts. For organizations that may not believe themselves vulnerable to DDoS attacks should take note. Yes, persistent repetitive attacks yield the highest results for bad actors, but it only takes once to incur serious damage, some of which is beyond the simple disruption commonly associated with DDoS.
Managing the Risk

Staying online is ever more crucial today. A short time ago, infrastructures were static, stationary beasts that connected to things on the outside to conduct business. In many ways, data center-centric enterprises were stationary targets that were easy to hit and a bit easier to defend. Today, it's different.

The modern enterprise is transforming and involves multiple cloud technologies, and conduct much more business at the application layer of the network stack. Many types of organizations play active roles in multi-infrastructure enterprises comprised of different companies that provide customers – and each other – valuable services. In the age of digital transformation, much more than just revenue is at stake. Still, the basics of being online carries a revenue generation risk, and for those in industries such as retail and financial services, that risk remains large.

Both, collective and by region, here's how hourly revenue risk stacked up in the latest findings as companies examined what was at stake during peak generation periods.

Rather high stakes when nearly half, 49% of 1,021 respondents, estimate have more than $250,000 per hour at risk. Even with some disparity still being revealed between the APAC region and the others, the revenue estimates continue to reflect a equilibrium indicative of a more inter-connected global economy.
When Risk Gets Real

The companies researched in this study faced a lot of risk with many having impacts that disrupted operations. The key element in managing risk is quantifying it and understanding the potential for damages. The 772 organizations attacked collectively experienced a minimum risk of disruption to revenue of ~$1.9 billion dollars during the previous 12 months. This total is approximated by the combined calculations from responses relative to hourly revenue generation, frequency of attack, detection times required, and response timeframes. The estimate does not include extenuating losses from brand damage, customer churn, litigation exposure from stolen data and IP, indemnification applied to incurred losses by customers, nor SLA or compliance remedies.

All told, the risk of serious damages from DDoS attacks can be quite extensive in addition to what can be directly attributed to the duration of events. Based upon respondent data of those that needed at least three hours to detect and another three hours to respond, the individual risks become even more stark.

Based on detection and response to attacks, organizations faced a combined revenue risk disruption of $3.35M USD, or an average of $4.3M each.
<table>
<thead>
<tr>
<th>Country</th>
<th>Industry</th>
<th>Annual Revenue</th>
<th>Hourly Revenue</th>
<th>Attack Frequency</th>
<th>Low Revenue Risk</th>
<th>High Revenue Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Ecommerce</td>
<td>$50-99M/ £30-49M</td>
<td>$25,000-$49,999 USD</td>
<td>Once</td>
<td>$196,000 AUD</td>
<td>$393,000 AUD</td>
</tr>
<tr>
<td>United States</td>
<td>Financial Services</td>
<td>$50-99M/ £30-49M</td>
<td>$100,000-$249,999 USD</td>
<td>2-5 times</td>
<td>$1,200,000 USD</td>
<td>$7,500,000 USD</td>
</tr>
<tr>
<td>China</td>
<td>Energy</td>
<td>$100-499M/ £50-299M</td>
<td>$250,000-$499,999 USD</td>
<td>Once per month</td>
<td>¥122,400,000 CNY</td>
<td>¥244,800,000 CNY</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Healthcare/ Pharma</td>
<td>$100-499M/ £50-299M</td>
<td>&lt;$25,000 USD</td>
<td>2-5 times</td>
<td>€11,000 EUR</td>
<td>€660,000 EUR</td>
</tr>
<tr>
<td>Singapore</td>
<td>Financial Services</td>
<td>$500-999M/ £300-499M</td>
<td>$250,000-$499,999 USD</td>
<td>2-5 times</td>
<td>$4,150,000 SGD</td>
<td>$20,700,000 SGD</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Government/ Public Sector</td>
<td>$500-999M/ £300-499M</td>
<td>$250,000-$499,999 USD</td>
<td>6-10 times</td>
<td>$70,240,000 HKD</td>
<td>$234,000,000 HKD</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Internet Services</td>
<td>$1B+/£500M+</td>
<td>Greater than $1 million</td>
<td>Frequently</td>
<td>£55,660,000 GBP</td>
<td>£111,320,000 GBP</td>
</tr>
<tr>
<td>Germany</td>
<td>Retail</td>
<td>$1B+/£500M+</td>
<td>$100,000-$249,999 USD</td>
<td>2-5 times</td>
<td>€1,100,000 EUR</td>
<td>€6,600,000 EUR</td>
</tr>
</tbody>
</table>

This small sample of excerpts from all of the organizations that were attacked show how much revenue disruption can be at risk when it takes at least six hours to respond to a DDoS attack. All told, in U.S. dollars, this selected group had a low revenue risk of $104M and a top revenue risk of $241M. It should come as no surprise that those who seek to harm companies use DDoS as a weapon. Combined with the additional damages possible, the financial risks faced by this small group alone can exceed far beyond a quarter of a billion dollars and drives home the point that speed in detection and response is an ally to risk mitigation practices.
IoT Paradox: Cyber Target and Business Advantage

The incorporation of Internet of Things (IoT) devices into enterprise operations remains steady with two of every three respondents indicating IoT adoption. As the quest for economic and efficiency benefits are sought by adopters, it’s clear that this comes with a cost in security vulnerability.

<table>
<thead>
<tr>
<th>BEST DESCRIBES CURRENT ADOPTION OF CONNECTED IOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Use</td>
</tr>
<tr>
<td>Actively using connected sensors, actuators, and data to improve process control and provide higher operating efficiency.</td>
</tr>
<tr>
<td>Some devices have been deployed and data being collected and analyzed. Closed vertical solutions in place.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Considered Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluating deployment scenarios and prioritizing likely candidates for trial purposes in the next 6 - 12 months.</td>
</tr>
<tr>
<td>Some consideration and early stage planning, no current deployment timeline but looking to make a decision in the next 12 - 18 months.</td>
</tr>
<tr>
<td>Currently no plans or need for adoption.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Global DDoS Attacks &amp; Cyber Security Insights Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
</tr>
<tr>
<td>8%</td>
</tr>
<tr>
<td>7%</td>
</tr>
</tbody>
</table>
In all, 76% of organizations that suffered at least one DDoS attack report having IoT devices in active operations. Of those adopters, nearly one third (28%) suffered network compromises or physical equipment damage. More problematic is the challenge in keeping these devices safe – 44% of those attacked who use IoT devices report a defense priority of preventing these devices from being compromised.

With so many companies having a discerning eye on blocking device hijack efforts, there is clearly more progress to be made as about half are struggling to fulfill that mission. Until that work can be done, IoT devices remain a tempting target to sabotage or to hijack as a rich source of computing power available for misuse.

The heavy expectation, if not reliance, on third parties to provide security for IoT – one third of all those using or evaluating IoT – reveals a large number of organizations have their hands full attempting to secure the entire enterprise. Comprehensive security aggregates from architecture, methodology, management, and technology and it is clear that the online business community is still working this out while unfortunately suffering attack impacts along the way.
PART TWO: CONFLICT AND CONSEQUENCES

Detection and Response

The times in both detection and responding to DDoS attacks have degraded a bit from this time last year. Overall, 46% of organizations required at least three hours to detect a DDoS attack compared to 39% in late 2016. Though less dramatic, the rise in those who needed another three hours or more to respond once detected increased to 43% from 38%.

Attackers continue to taunt defenses, probe network vulnerabilities, and execute more targeted strikes as seen in the greater breach yield discussed earlier. However, there is some good news. In the Neustar May 2017 report, there was great concern that 40% of those attacked were notified of the attack by their customers, many with IT teams trailing behind in sufficient detection.

The new findings show some improvement as those notified by customers decreased in seven months from 40% to 31%. This may be indicative that perhaps better investments have helped security teams see the attack before customers. Still, having one third of those attacked hearing from customers is far too much as these numbers continue to edge up from 2016.

HOW ORGANIZATIONS LEARNED ABOUT THE DDOS ATTACK

<table>
<thead>
<tr>
<th>Source of Notification</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal security and/or IT team</td>
<td>82%</td>
<td>84%</td>
</tr>
<tr>
<td>Customer (and/or via Customer Service team)</td>
<td>31%</td>
<td>29%</td>
</tr>
<tr>
<td>Partner</td>
<td>20%</td>
<td>18%</td>
</tr>
<tr>
<td>Other Third Party e.g. Social media</td>
<td>5%</td>
<td>4%</td>
</tr>
</tbody>
</table>

*Respondents allowed to select more than one
Within the major regions, the variances and similarities become evident. As attacks have grown in complexity, and often more inconspicuously, there were slips in North American and Europe from those able to detect DDoS attacks in less than one hour. Much of this slip was caught in the 1–2 hour and 3–5 hour timeframes, but in Europe those able to detect attacks in less than 2 hours fell from 63% to 50%. APAC organizations fared less well as rise in detection times put nearly half of those attacked needing 3–12 hours.
Responding to attacks is not getting faster overall, but there are some intriguing contrasts and spotty improvements within the regions. For example, while APAC and North America hold relatively steady in response times, in Europe, times under two hours have noticeably dropped with much of the increase being held within the 3–5 hour range. On average, most organizations report being able to respond within 5 hours, but this latency is still excessive given the velocity of impact possible by today’s attackers.
Impact

It is certainly not news that DDoS attacks are often used as smokescreens to distract and confuse defenses and IT staff. Being in business today means being online and being online means being susceptible to attacks over which there is no control. However, there is a difference between being susceptible and being vulnerable and the research shows that some are doing better than others, but most who are attacked are being hit hard.

Attack accompaniments remain at high rates when a DDoS attack occurs. Unfortunately, the old adage, ‘Half the time, it’s a race against crime’ stands true. There is a slow, but persistent rise in the impact and breach success attackers are enjoying over the pace in 2016.

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

<table>
<thead>
<tr>
<th>Result</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus discovered</td>
<td>49%</td>
<td>46%</td>
</tr>
<tr>
<td>Malware activated</td>
<td>35%</td>
<td>37%</td>
</tr>
<tr>
<td>Network compromise, physical or equipment damage</td>
<td>26%</td>
<td>25%</td>
</tr>
<tr>
<td>Customer data theft</td>
<td>24%</td>
<td>21%</td>
</tr>
<tr>
<td>Ransomware encountered</td>
<td>15%</td>
<td>24%</td>
</tr>
<tr>
<td>Loss of customer trust/damage to brand</td>
<td>21%</td>
<td>23%</td>
</tr>
<tr>
<td>Financial theft</td>
<td>17%</td>
<td>14%</td>
</tr>
<tr>
<td>Loss of intellectual property</td>
<td>17%</td>
<td>15%</td>
</tr>
</tbody>
</table>
Associated attacks and breach activities were felt across revenue segments with no one being spared. The data indicates that companies in the precarious annual revenue band of $100M-$499M/£50-299M encountered the most trouble averaging nearly three breach incidents per organization attacked.
Overall, breach attack activities conducted in concert with DDoS assaults provided high returns to those seeking to harm companies. Beyond simple disruption, the very real danger of breach has grown to be an integral part of DDoS use.

Not surprisingly, detection speeds continue to be a determining factor relative to impact, especially when it comes to theft defined as the loss of customer data, intellectual property, and/or financial resources. The number of theft actions coordinated with DDoS attacks rose to 58% from 49% last year. Worse, 70% of those incidents reported this year took place against organizations that required 3–5 hours to determine that a DDoS attack was underway.

Specific to the relationship of DDoS detection times and associated theft activities, the data shows a strange dichotomy when compared to 2016. Last year, it did not take as long for hackers to steal from targeted organizations. Deeper investments, better awareness, and stronger defenses may explain why a more determined effort has been needed by attackers, but organizations that require at least three hours to detect find a much higher rate of theft. Attackers may be taking longer to affect successful theft, but persistence and patience appear to be paying off for the black hats.
Here is a regional breakdown of how attackers are using DDoS to confuse defenses, distract IT teams, and stymie forensics.

There are few worse things in business than having a security incident turn customers into plaintiffs. With the sharp rise in combined attacks, the risks are even higher today for organizations doing business online. Whether attacked for the first time or hit repeatedly, organizations should be mindful that when DDoS is in play, those behind it have something else on their minds to achieve.
Major Industry Fights Against DDoS

With a nod toward consistency, attackers went after three of the major industries: financial services, retail, and technology, with a determined fervor. However, there are some interesting caveats in this activity. Financial Services and Retail saw an increase in attacks over last year, but a decrease in being attacked more than once. Conversely, companies in the Technology vertical saw a decrease in rate of attacks, but an increase in being attacked more than once.

Unfortunately, those decreases are generally where the good news ends with the exception of slight Retail improvement times in detection and response. All three industries saw sizable activity in malware activation, customer data theft, and ransomware encounters in conjunction with DDoS attacks. Here are some of the primary indicators of how these industries fared in combatting DDoS compared with this same time in 2016.
Experienced ransomware w/DDoS attack

Experienced customer data loss w/DDoS attack

Experienced malware activation w/DDoS attack

Attacked more than once

Learned of attack from Customers

Required minimum 3 hours to DETECT

Required minimum 3 hours to RESPOND

Investing more than previous 12 months

Key insights:

- Rise in attacks, but a decrease in multiple incidents
- One third were notified by customers, attacks are public
- Increase in detection times means more outside notice
- Steady rate of breach activity in concert with attacks
- Investment plans in defenses remains high
Key insights:

- More attacks directed at Retail, but fewer multiple attacks
- Faster detection and response times show some defense improvements
- Faster detection and response possibly means fewer customers noticed
- Malware activation levels are steady and serious
- Good news: Decrease in cases of customer data theft
- Bad news: Rise of malware infections
Key insights:

- Technology companies reported fewer attacks, but a rise in multiples.
- Degradations and interruptions are noticeable to customers.
- Surprisingly, technology companies reporting higher detection times.
- Response times are slower, but not as drastic as detection issues.
- Malware activation up with data theft and ransomware increases.
Investment Trends

The responses in this study continue to affirm that the majority of organizations have institutionalized DDoS as a threat. This is indicated in the consistent rise of planned investments and the combination of those who maintain serious investments to counter what is viewed as a security necessity.

Here we see the increase of protection investments during the past three years. Compared to last year, more than 80% of companies are now investing more in DDoS protection.

The additional indicator is the combined total of those who reported increased investment as well as those who previously invested and rank DDoS threats as a high priority. For the past two years, those taking action to tackle the ever more present threat of denial of service attacks has surpassed the 90% mark.
Compared to this period last year, not only has the number of organizations investing increased, but those who had invested and spurred on to reinvest appears to have risen. This may be indicative of companies seeking to get back in front of modern DDoS tactics as some defenses were eclipsed and overwhelmed in 2016.

It’s not enough to just know what companies are planning to invest, but rather, why they are investing and in what. DDoS is one of the many threats with which security teams must contend and as the response to DDoS has worked its way into security budgets, it is important to understand how those investments are being prioritized and guided.
Behind DDoS Defense Investment

Motivation comes in many forms and from many sources. Neustar asked respondents to rank their top three reasons behind investment levels and intentions compared to actions taken in the previous twelve months. The eleven available options ranged from concerns over major outages to industry compliance and executive mandates. From the more than 1,000 responses emerged an interesting picture of where defense thinking meets budget commitments with the top five motivation factors are ranked in order below.

<table>
<thead>
<tr>
<th>TOP FIVE MOTIVATIONS FOR DDoS DEFENSE INVESTMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preserving customer confidence/brand reputation</td>
</tr>
<tr>
<td>Prevention of associated attacks including ransomware</td>
</tr>
<tr>
<td>Proactively strengthen existing protection</td>
</tr>
<tr>
<td>Concerns over major outages/potential damage</td>
</tr>
<tr>
<td>Risk mitigation accountability</td>
</tr>
</tbody>
</table>

A closer look at the top three motivations reveals how prevalent these concerns are shared amongst the roles and market segments. What the prioritization results show is that IT and security professionals are just as concerned about what happens on the outside as much as what happens on the inside during DDoS attacks. Here’s more detail behind the top three reasons for DDoS investment.
Preserving customer confidence surfaced as the most prevalent motivation behind improving DDoS defenses. Given that only 13% of those that cited this motivation actually reported tangible brand damage as the result of a DDoS attack, it is shows the influence that the epic attacks and outages last year had on security planning. Also of note is how deep the concern for customer confidence reaches through the ranks of IT staffs.

Within individual industries, this chart shows the percentage of all industry respondents that consider preserving customer confidence and protecting brand reputation from impact due to DDoS attacks. Not surprising, half of all retail organizations view this as a key factor in improving DDoS defenses.
One of the most pressing issues in combatting DDoS in the past few years has been the onslaught of additional coordinated activity, particularly with malware activation, data theft, and increasingly, ransomware. As many of these occurrences have risen more than 50% in the past three years, with some rates nearly doubling, security teams are looking beyond simple disruption as a DDoS consequence. For instance, Healthcare/Pharmaceutical organizations have a vested interest in thwarting theft of intellectual property – damages that can range in the countless millions. So far, they are holding the line in keeping focused, just 15% of healthcare organizations in the current findings had IP stolen, yet half of all healthcare industry respondents identify associated attacks as a preeminent concern that is driving denial of service investments.
#3: Proactively Strengthen Existing Protection

As DDoS attacks of unprecedented size ripped through defenses and bowled over organizations of all types last year, security teams took stock of their protective portfolios. Neustar reported global sentiments to correct this balance in May 2017 as the global data concluded that serious investments and concerns were behind the drive to get back ahead of bad actors, to take back the initiative. This is why the investment driver to proactively strengthen and deepen existing defenses shows up in the top three – especially with so many organizations simultaneously managing digital transformation initiatives. Here’s how security professionals around the world see it.

Why organizations are investing is one thing, but what they are investing in provides insight into how much organizations are bringing to the fight. There continues to be a consistent increase in more sophisticated defenses as well as some lesser reliance on ISPs to carry the load.
The Rise of WAF

Layered defenses continue to lead the way as on average, organizations report having at least two separate elements used for DDoS protection. Relative to sophisticated investments involving appliances, third-party services, and hybrid configurations that use a combination of hardware and cloud-based mitigation, those investments are up. Better than 65% of all organizations in this study have at least one of those options in use.

However, what is quite noticeable is the rise Layer 7 protection as the past twelve months have seen a huge spike in the deployment of Web Application Firewalls, or WAF. Organizations that have added WAF to combat DDoS has nearly tripled in the past seven months and more than quadrupled than this time last year. Needing protection in what has rapidly become the most exploited layer in the network stack, especially relative to the vulnerabilities beyond DDoS alone, little wonder why there has been a strong response to offset attacker success.

The search for the right combination of defenses to prevent DDoS impact continues in earnest with security teams leveraging fewer traditional solutions and more transformative services in line with their enterprise evolutions. Getting, if not expecting, DDoS protection from cloud service providers is becoming a standard as nearly half of organizations now incorporate this element in their security portfolios. While digital transformation and the associated operational and security strategies evolve, new demands are driving investment directions to stave off attackers.
Management disciplines and security technologies are just part of what transformative organizations are pursuing in their quest for better security. From a community that had a rough 2016 and has seen some rather difficult episodes this year, especially from ransomware, stems more momentum to share expert perspectives and exchange information.

Within organizations, different roles place different value on working beyond the defenses to best understand how to deal with threats. Security consultants continue to maintain a top spot in helping develop strategies, but there is also marked exchange between peers at different companies.

Work with law enforcement, both in pre- and in post-breach scenarios continues mostly at executive levels. This high level of activity shows the exhaustive efforts being made by security leadership to provide maximum protection and response to security events.

The result is an active security community sharing more ideas and information to get the upper hand on DDoS attackers. This also shows that those who make strategic investments in defenses are thorough in their considerations and decisions to assure stakeholders, partners, and customers of the best protection possible.
Strategic Considerations

The business community continues to invest and improve defenses to offset the sheer power menacing that attackers harnessed in last year. Attack quantities are off the fever pitch reported in the Neustar May 2017 report, but they remain slightly higher than this time last year. The higher yield from the relative same number of attacks demonstrates a stronger set of tools and abilities on behalf of those seeking to cause harm. Combined, this set of circumstances leads to several key considerations that organizations must consider.
1. Security and Digital Transformation Are Linked

As enterprise infrastructures change, traditional defense strategies against denial of service attacks must evolve as well. There are many reputable estimates across the IT industry that roughly three quarters of all organizations online are incorporating public and private cloud elements into their operations. This movement creates opportunity, but it also creates gaps across the security portfolio that hackers look to exploit. Most organizations attacked with DDoS experience some form of associated activity that has unfortunately become a standard practice by bad actors. Traditional DDoS protection approaches will not sufficiently protect enterprises in transition and must be evaluated to protect in both present day and journey states.

2. Attackers like Hitting Soft Targets

With a higher return from attack efforts, speed of detection and move to mitigation is the key ally to frustrating attacker objectives. The research over the past three years concludes that the average organization needs a couple of hours to definitively detect a DDoS attack and those times are getting slower. This translates to greater vulnerability. Mindful that 37% of those who detected attacks in less than one hour still suffered associated theft, those that required 3-5 hours for detection stood little chance to being ahead of theft – which 70% of those companies suffered. Speed is an important consideration that can determine the success or failure of attacker intent.

3. Lessons from Others Can Drive Better Investments

There were notable examples of impact that many organizations wish to avoid and this showed up in the investment motivation responses. Of the top five reasons companies are investing in DDoS, in each category, far fewer organizations had actually experienced those specific problems. Direct exchanges are showing to be more popular in augmenting information gathering and decision-making. Good security comes from solid approaches and there are many lessons to be shared and had to offset the shortage in security talent. For those moving into or through digital transformation processes, hearing and sharing with those a bit more up that road can help neutralize the advantage resting with attackers.
Every day, the world generates roughly 2.5 quadrillion bits of data. Neustar isolates certain elements and analyzes, simplifies and edits them to make precise and valuable decisions that drive results. As one of the few companies capable of knowing with certainty who is on the other end of every interaction, we’re trusted by the world’s great brands to make critical decisions some 20 billion times a day. We help marketers send timely and relevant messages to the right people. Because we can authoritatively tell a client exactly who is calling or connecting with them, we make critical realtime responses possible. And the same comprehensive information that enables our clients to direct and manage orders also stops attackers. We know when someone isn’t who they claim to be, which helps stop fraud and denial of service before they’re a problem. Because we’re also an experienced manager of some of the world’s most complex databases, we help clients control their online identity, registering and protecting their domain name, and routing traffic to the correct network address. By linking the most essential information with the people who depend on it, we provide more than 11,000 clients worldwide with decisions—not just data.

More information is available at

www.home.neustar