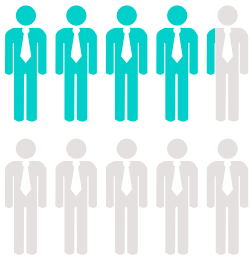
New Business Risks of 'Never Happen to Me'



Forty-two percent of respondents to Arbor Networks' *Worldwide Infrastructure Security Report* saw multi-vector DDoS attacks in the past year. Just as worrisome—the thirty-six percent who did not know.

Source: Arbor Networks' *Worldwide Infrastructure Security Report* 2015

Nowhere are the changes in enterprise cyber-security more under-appreciated than in regards to the risks of Distributed Denial of Service (DDoS) attacks. Hard to believe now, but there used to be a time when the need for firewalls was considered advanced protection. Now, next-generation firewalls with sandboxing, Intrusion Detection/Protection Systems (IDS/IPS), real-time network monitoring solutions—and for some, cloud-based managed security services and Security Incident and Event Management (SIEM) systems—are all considered standard components of a layered cyber-security protection strategy.

While the business implications (read lost revenue, lost customers, mitigation costs and risks to business continuity) of network or application downtime and disruption have dramatically increased, most thinking about DDoS is still simply about capacity consumption. The reality is the newer DDoS attack campaigns are more complicated, and far more common, than you may realize; attack kits and even DDoS services-for-hire can be easily ordered on the web. DDoS campaigns represent a serious threat to virtually any organization with an Internet connection, and protection requires new calculations of risks to the business.

The DDoS Threat Equation: What's Changed?

DDoS attacks have evolved well beyond the Mafiaboy attacks of 2000. Today's DDoS attacks are frequently multi-vector, combining multiple attack techniques concurrently, aimed at the same target, to increase the complexity of mitigation and the attacker's chance of success.

These components include the "traditional" (though much evolved) volumetric attacks. By employing reflection techniques leveraging common transmission control protocols such as DNS, NTP, etc. and the inevitable growth of unsecured servers on the Internet, DDoS campaigns have achieved unprecedented size and speed. The Arbor Networks' *Worldwide Infrastructure Security Report* saw the peak attack this year of 400 Gbps—a 4,900 percent growth over the 10-years of the *Security Report.*

In addition, newer TCP state-exhaustion methods target the connection state tables of the very infrastructure components put in place for protection, like firewalls and load balancers. Over a third of the respondents to the 2015 *Security Report* saw their firewalls or IPS experience a failure that contributed to an outage during a DDoS attack.

And as if that were not enough, DDoS can and has been used in several stages of advanced attack campaigns. During reconnaissance, DDoS is used to assess your general level of security preparedness and help advanced attackers decide whether to target your organization. DDoS is also used as part of delivery and weaponization, when dropping malware, to help avoid detection (think of all those alerts you are trying to prioritize). And finally, DDoS is used to divert attention and cover tracks during data extraction, even after the fact, when it can fill forensic product logs, making the search for planted malware much more challenging.

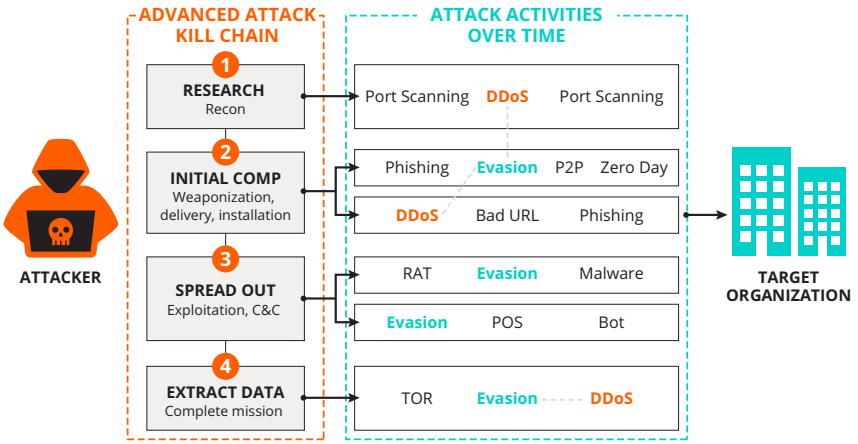
It is an increasingly dangerous assumption to consider DDoS separately from advanced cyber-attacks. Application-layer attacks can be very effective with as few as one attacking machine generating a low rate of traffic. In fact, application-layer DDoS attacks are very much like advanced attacks in that they are targeted, in this case at a specific application or service at Layer 7, and they are stealthy. Arbor Security Engineering and Response Team (ASERT) has determined DDoS botnets are in fact closely related to advanced threat malware, RATs, and other components. But increasing sophistication is only one factor that has changed the business equation of DDoS protection (see image on next page).

ARBOR® NETWORKS

"A common response by many administrators to the challenges of DDoS is the belief that their firewall and IPS infrastructure will protect them from attack. Unfortunately, this is not true. Firewalls and IPS devices, while critical to network protection, are not adequate to protect against complex DDoS attacks."

Richard Martinez, Enterprise Security Analyst with Frost & Sullivan

DDoS Used During Various Stages of Attack Kill Chain



The Cost: You Have More at Stake

The modern enterprise is built upon multiple, more complex web-based services, public-facing or not. The lifeblood of the corporation is on-line business-critical services; direct revenue-generating web-apps are only the tip of the iceberg. Many back end systems may appear like a single interface to the end user but are in fact handling a variety of networked tasks such as Web Services, Database Processing, Authentication, Media Delivery, Communications (Mail, Chat, SMS, etc.) to name a few.

All of these services are driving your business, and represent potential attack surfaces to increasingly sophisticated DDoS campaigns. More attack surfaces, and lower barriers to entry for launching a DDoS attack, have created what the military likes to call a target rich environment. The list of web-based applications where performance and availability impact the business goes on and on.

- Poorly performing or unavailable public-facing helpdesks or self-help sites;
- A down check-in, scheduling and calendaring application for hospitals, airlines, etc.;
- Field resources cannot access customer service history or current account information;
- Job application processes that can't process resumes or alert HR.

Even if you are successful protecting the infrastructure delivering traffic to and from your servers, many attacks targeting the application layer of component services can cripple the larger business-critical applications.

The expanding, target rich environment includes new business services (SDN, VDI, IaaS, SaaS, etc.) rooted in the cloud. While the enterprise is looking to realize cost and productivity benefits perhaps there is a misconception that the scale of cloud-based infrastructure and application paradigms (and service-provider's security) will naturally protect you from the impact of DDoS.

The reality is cloud-based services hosted in public clouds, or even passing through service providers with a range of other customers using such services, only increases your exposure. The proportion of respondents to the 2015 *Security Report* saw attacks targeting cloud-based services grow from 14 percent in 2012, to 19 percent in 2013, to 29 percent last year. Growing reliance on cloud-based business applications challenge traditional security controls based on visibility into and manageability of endpoints, applications and networks. Not only are there more attack surfaces, but they are harder to monitor and build in adequate security and rapid DDoS mitigation.

The proportion of respondents to the 2015 *Security Report* saw attacks targeting cloud-based services grow from 14 percent in 2012, to 19 percent in 2013, to 29 percent last year.

Source: Arbor Networks' *Worldwide Infrastructure Security Report* 2015

The Risk of Old Thinking

Given the evolved threat to your business from DDoS, old ways of thinking about DDoS protection can be dangerous. A 'never happen to me' attitude, or more likely, something like "an attack that big and complicated will never target me" ignores the new reality. Even organizations with substantial resources and the best intentions can get surprised.

Below are three scenarios of how organizations are learning to more fully appreciate the real complexity of defending against today's DDoS, and the significant business risks of failure.

FINANCIAL SERVICES LEARNS FROM A PEER

A major Wall Street financial services organization knew full-well their customer relationships and continued growth depended upon reliable, secure online infrastructure and services. As part of continually upgrading their security posture they were nearing the end of an evaluation of enhanced DDoS solutions. They were in fact about to bring these new defenses in-line when one of their peers suffered a major DDoS attack that actively changed vectors and combined tactics to successfully cripple some of the target organization's customer-facing services. This prompted the security team to take a closer look at what they had running in the lab.

They were evaluating a next generation firewall solution in conjunction with an "upgraded" Intrusion Protection System. What they quickly realized was these solutions were not designed to cope with fast-changing, human-directed DDoS attacks. These devices operated with security configurations that were set and then largely forgotten. But these configuration controls were buried deep in the user interface—in certain cases in a text file. As they had just witnessed with their peer, attackers could leverage many different tactics, perhaps simultaneously, and quickly, in real-time adjust their vectors until they hit upon what worked. Trying to respond quickly, the user struggled with an interface that was not designed for fast, effective response to an urgent security incident.

Also problematic was the poor integration with their existing network monitoring and security analysis solutions. It was difficult to see the bigger picture, such as if the DDoS attack also contained 'low and slow' application layer components (perhaps deliberately concealed by a simultaneous volumetric attack), or if it was part of a stealthy advanced attack. They realized that new business requirements demanded better real-time control and adaptability, such as more easily configuration threat alerts. And they wanted more comprehensive network visibility as embodied in better integration with existing network management systems.

GAMING—CLOUD COVERED

The lifeblood of a growing online gaming company is based on availability, and historically they felt comfortable with cloud-based, out-sourced solutions. They had engaged and felt they were covered with a managed DDoS protection solution, until they started to experience larger, volumetric DDoS attacks deliberately timed to coincide with peak gaming hours. They became frustrated with the speed of mitigation; valuable hours would elapse from the moment an attack began until the service started working again.

One issue was internal; it took too long to recognize an attack. Without better, real-time visibility and a baseline of the usual, expected traffic they were slow to pick up on anomalous performance degradation. Ad hoc processes caused more delay in agreement on traffic re-direct and communicating details to their managed security service provider. Even then it took more time for the provider to effectively mitigate. The result was valuable time lost during peak gaming hours, resulting in tens of thousands in lost revenue and potentially lost customers.

ATLAS®

Arbor's insight can be shared via ATLAS®, a unique collaborative effort with 330+ network operators across the globe sharing 120 Tbps of traffic information that informs numerous business decisions.

Source: Arbor Networks' *Worldwide Infrastructure Security Report* 2015

Online Marketing—Data Center Expansion

A leading online marketing company helps their customers get real results through email newsletters, surveys, web events, Facebook promotions, online listings, and more. The success of their customers depends upon service availability, performance and dependable connections. They were aware of ransomware attacks, but not sure where, how to invest in DDoS protection. Given the size of new volumetric attacks they ruled out building their own infrastructure. At the same time, given the complexity of their traffic, they needed more visibility than just adding cloud bandwidth.

Had they anticipated precisely how DDoS could selectively target and time volumetric attacks, the business equation of lost availability during peak hours—and the challenges of effective hand off to their service provider—they might have invested in an on-premise component to address this "weak-link" of rapid visibility and identification. Another lesson learned was the need for better defined internal communication processes between security or network management teams, and escalation procedures with their service provider.

EDUCATION INSTITUTION—LUCKY TIMING

A large educational institution felt their Internet pipes and firewalls were big enough; in the past they had been able to adjust code to strengthen their firewalls and address DDoS attacks. But there was growing concern about attacks targeting specific users in their community. Time spent beefing up firewalls had become less and less effective against these new DDoS attacks. They realized that the strength of the attack vectors was becoming more than their firewall practice could handle.

With support from the CISO and CIO the network and security teams formed a review committee to investigate solutions. They knew the scale of the problem meant the CISO would have to seek funding once a solution was identified. Their teams worked well together. The security team has a very good understanding of the CPU resources we have available, specifically the connections per second constraints. The teams understood inline versus not inline strategies, for instance, the potential need to look at flow records, or dive deeper into the attack variants.

The team had identified an inline solution capable of handling double their current pipe capacity and connection constraints. The inline solution provided better inspection capabilities of the "low and slow" attacks while still allowing BGP diversion when scale of attacks demanded a cloud-based assist. They were in the midst of a Proof of Concept when a sister institution experienced a DDoS attack that brought their entire network down for an entire weekend. This event brought a sense of urgency to the board, and fast-tracked budget approval. It also made the CIO and review team look like heroes.

Lessons Learned

DDoS attacks are no longer simply about capacity consumption; they are about very real risks to your business. Some best practices have emerged about how to provide a flexible, scalable strategy that can better detect and mitigate DDoS attacks:

- **Look to minimize downtimes** associated with initiation of third party mitigation efforts;
- **Maximize visibility into your traffic**—whether on-premise or coming from the cloud—so as to have a bigger picture of all potential attack components;
- **Implement a clear mitigation process**—a process connecting the on-premise and the cloud visibility, detection, and mitigation services.

Now is the time to re-examine the business equation of protecting your business from DDoS attacks. But this presents some new challenges for security leaders and IT managers. The equation is no longer just about technology, but processes and communication. What might get lost in the day to day of responding to incidents is that this sea-change in the equation of DDoS protection has fundamentally altered the job of security professionals and IT.

The security team now needs to understand—and *communicate better*—the broader business impacts of a DDoS attack. This means far more than "downtime". What happens beyond the dollar cost to mitigate? How will it impact other parts of the organization, business initiatives, customer relationships and productivity? Will the solution set address the changing nature of DDoS and how will it impact our organization?

The challenge for CISO's and their teams is change old ways of thinking. To update the perception among management as to real threats posed by today's DDoS. You need to put the security risks posed by DDoS in terms their colleagues and line of business managers can understand, particularly true when you are planning, prioritizing and pitching to management how you need to invest to best protect your business.

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

SB/NEVERHAPPEN/EN/1015-LETTER