radware

2017's 5 Most Dangerous DDoS Attacks & Steps to Mitigate Them

Throughout the history of mankind, whether in warfare or crime, the advantage has swung between offense and defense, with new technologies and innovative tactics displacing old doctrines and plans. For example, the defensive advantage of the Greek phalanx was eventually outmaneuvered by the Roman legion. Later, improvements in fortifications and armor led to castles and ironclad knights, until the invention of gunpowder made them obsolete. In the 20th century, fixed fortifications and trenches were rendered outdated by highly mobile armored forces. In all these examples, the common denominator is that one side's tactical advantage spawned new ways of overcoming its opponents, eventually degrading that advantage or reversing it completely.

Enter the digital age, where lines of code and terabytes of information determine who has the tactical advantage. Of late, the pendulum has swung in favor of cyber-attacks. Rate-based technologies, once considered adequate to handle the most advanced distributed denial-of-service (DDoS) threats, have fallen obsolete as tech-savvy adversaries move beyond the static concepts of most conservative corporate budgets and know how to overcome name-brand mitigation technologies. These ultra-adaptive hackers have given rise to the top five nastiest attack techniques in 2017.

ATTACK TYPE 1
Advanced Persistent DoS (APDoS)

Wikipedia defines APDoS as:

> "…a clear and emerging threat needing specialized monitoring and incident response services and the defensive capabilities of specialized DDoS mitigation service providers. This type of attack involves massive network layer DDoS attacks through to focused application layer (HTTP) floods, followed by repeated (at varying intervals) SQLI and XSS attacks."

It is clear that APDoS requires an array of technologies to stop the network floods, HTTP application-level DDoS and encrypted threats. Moreover, Radware is witnessing these attack techniques manifest into SMTP attacks (a relatively new vector) and secure-SMTP such as TLS over SMTP.

APDoS attacks assume many forms, but typically attackers will switch tactically between several targets to create a diversion to fool mitigation tools, all the while eventually concentrating the main thrust of the attack onto a single victim. To successfully mitigate these threats, organizations must understand the threat and make certain it has certain protections in place (e.g. high caliber detection and mitigation). To start, characterize APDoS threats into the following classes:

- “Advanced reconnaissance (pre-attack OSINT and extensive decoyed scanning crafted to evade detection over long periods)
- Tactical execution (attack with a primary and secondary victims but focus is on primary)
- Explicit motivation (a calculated end game/goal target)
- Large computing capacity (access to substantial computer power and network bandwidth resources)
- Simultaneous multi-threaded ISO layer attacks (sophisticated tools operating at layers 3 through 7)
- Persistence over extended periods (utilizing all the above into a concerted, well managed attack across a range of targets)”

The task is daunting and real. As the next generation of DDoS threats emerge, organizations must be diligent and proactive. Companies must rise above the normal corporate culture of security controls and become obsessive about removing risks and compulsive about action.

ATTACK TYPE 2
DNS Water Torture Attack

A DNS NXDOMAIN flood attack, which is also known as a water torture attack, targets an organization's DNS servers. This type of attack involves a flood of maliciously crafted, DNS lookup requests. Intermediate resolvers also experience delays and timeouts while waiting for the end target's authoritative name server to respond to the requests. These requests consume network, bandwidth and storage resources. They can also tie up network connections, causing timeouts.

By understanding the threat, an organization can comprehend two of the largest problems in solving this attack vector:

- **First:** The attacker is coming from a known legitimate source and can’t realistically be blocked while still maintaining healthy DNS resolution operations over the long term
- **Second:** The attacker source is actually also querying legitimate requests at the same time illegitimate requests are being sent.

To counter this resource-draining threat, organizations should monitor their recursive DNS servers, keeping a keen eye for anomalous behavior such as spikes in the number of unique subdomains being queried or spikes in the number of timeouts or delayed responses from a given name server.

Any DNS attack mitigation tool must meet unique challenges. Beyond a limited set of vendors, there is no real automated solution to mitigate this threat, as the tool must contain the following attributes:

- **Mitigation Tools Must Have Deep Knowledge of DNS Traffic Behavior** – The tool must understand DNS traffic and "learn" or establish baseline behaviors continuously to immediately identify abnormal DNS traffic. Moreover, the tool or technique must analyze every field in DNS traffic to identify abnormal packets and to create real time signatures.
- **Mitigating High Rate of DNS Packets** - The tool must be able to challenge large amounts of DNS queries per second and to process up to – often in larger circuits – 10 - 35 million packets per second of attack traffic. The attack traffic does not affect legitimate traffic while under attack.
- **Mitigation Accuracy** – With unique DNS challenges and accurate analyzing of DNS traffic behavior, an organization must be able to accurately distinguish between legitimate DNS traffic and attack-based DNS traffic to minimize false positives. This enables the service provider to continue and serve its legitimate users even under severe attack.
- **Provide Best Quality of Experience Even Under Attack** – Obviously the idea of operating a service is that you must have an architecture that can guarantee minimum latency to all processed traffic, and especially to the legitimate traffic. This guarantees a best quality of experience to legitimate internet users even under attack.

ATTACK TYPE 3
Friend Turned Enemy: SSL-Based Cyber Attacks

There is a new set of challenges facing organizations leveraging encryption technologies. Cyber-attacks, including DDoS attacks and advanced web application attacks, continue to plague businesses as they continuously shift operations online. For both types of assaults, those leveraging encrypted traffic as an attack vector are on the rise, further challenging current security solutions. Most mitigation technologies do not actually inspect SSL traffic, as it requires decrypting/encrypting traffic. Recent surveys show that between 25% - 35% of enterprise communication sent via an LAN and WAN is SSL-encrypted traffic.[1]

SSL-based attacks take many forms, including:

- **Encrypted SYN Floods:** These attacks are similar to standard, non-encrypted SYN flood attacks in that they seek to exhaust the resources in place to complete the SYN-ACK handshake, only they further complicate the challenge by encrypting traffic and forcing resource use of SSL handshake resources.
- **SSL Renegotiation:** These attacks work by initiating a regular SSL handshake and then immediately request the renegotiation of the encryption key. The tool repeats this renegotiation request until all server resources have been exhausted.
- **HTTPS Floods:** These attacks generate floods of encrypted HTTP traffic, often as part of multi-vector attack campaigns. Compounding the impact of "normal" HTTP floods, encrypted HTTP attacks add several other challenges, including the burden of encryption and decryption mechanisms.
- **Encrypted Web Application Attacks:** Multi-vector attack campaigns also increasingly leverage non-DoS, web application logic attacks. By encrypting the traffic masking these advanced attacks, they often pass through both DDoS and web application protections undetected.

1 http://www.networksasia.net/article/3-reasons-ssl-encryption-gives-false-sense-security.1424935771

In the same way SSL and encryption protect the integrity of legitimate communications, they effectively obfuscate many of the attributes used to determine if traffic is malicious or legitimate. Identifying attack traffic within encrypted traffic flows is akin to finding a needle in a haystack . . . in the dark. Most cyber-attack solutions struggle to identify malicious traffic from encrypted traffic sources and isolate that traffic for further analysis (and potential mitigation).

The other major advantage that SSL attacks offer to attackers is the ability to put significant computing stress on network and application infrastructures they target. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic, in many cases beyond the functional performance of devices used for attack mitigation.

Even the most advanced mitigation technologies have gaps in their encryption-based protections. Few of these solutions can be deployed out-of-path, which is a necessity for providing protection while limiting the impact on legitimate users. Many solutions that can do some level of decryption tend to rely on rate-limiting requests, thereby resulting in dropped legitimate traffic. Finally, many solutions require the customer to share actual server certificates, which complicates implementation, certificate management and forces customers to share private keys for protection in the cloud.

Here are 5 tips to protect your organization from encrypted attacks

Stateless Mitigation: As previously mentioned, many security technologies are stateful in nature, meaning they maintain state throughout a session. This requires additional computing resources and poses the risk of filling session tables, at which point the device will fallover. Be sure the technologies you're depending on for encrypted attack protection are stateless in nature to ensure ability to scale to the higher demands of these attacks.

Asymmetric Deployment Options: Most security technologies rely on a symmetric deployment model, meaning they are in the path for both inbound and outbound traffic. This has key benefits for some aspects of security, but in the case of encrypted attack mitigation, adds unnecessary computational strain on the solution. Look for technologies that can support an asymmetric deployment where only ingress encrypted traffic passes through the mitigation engine.

Certificate Management: Some security technologies that claim to cover encrypted attacks do so at the burden of operations teams that manage server certificates. Specifically, these technologies require the sharing of the actual web server certificates, meaning any change to these certificates have to be replicated in the security solution. Look for technologies that can manage the inspection of encrypted traffic through use of certificates legitimately issued to the organization but not tied specifically to the web server.

Ensuring Integrity of the Trust Model: One of the principles behind website authentication through certificates is the confirmation to the end customer that they are engaged in a "private" communication with the intended organization. Some service providers offer SSL capabilities that break this trust model and actually initiate a secure channel between the unknowing end user and themselves. In so doing, they essentially dup the end user into trusting them with the shared information (as well as the service provider's certificate management).

Optimizing Legitimate User Experience: As is so often the case, IT and security professionals are left to strike a balance between having lightweight security and creating such a locked-down user experience as to chase away customers. This balancing act plays out in encrypted attack mitigation as well, where some technologies employ something of an on/off switch for decrypting all encrypted traffic when a potential attack is detected. Look for technologies that can selectively apply challenge-and-response specifically to traffic identified as suspicious, thereby maintaining the user experience for legitimate users sending via encrypted traffic.

The fact that many organizations are seeing an increase in encrypted traffic is, in general, a good thing. It is however, a complicating factor when it comes to encrypted cyber-attacks. The bottom line is that to provide effective protection, solutions need to deliver full attack vector coverage (including SSL), high scalability to meet the growing demands of the consumer, and innovative ways to handle management of encryption technologies (today predominantly SSL/TLS) in a manner that can be operationalized effectively and efficiently.

ATTACK TYPE 4
Fire & Forget: PDoS – Permanent Denial Of Service

A permanent denial-of-service (PDoS) attack is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of the system. It is a contrast to its well-known cousin, the DDoS attack, which overloads systems with requests meant to saturate resources through unintended usage.

One method PDoS accomplishes its damage is via remote or physical administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. In the case of firmware attacks, the attacker may use vulnerabilities to replace a device's basic software with a modified, corrupt, or defective firmware image—a process which when done legitimately, is known as flashing. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced. Other attacks include overloading the battery or power systems.

How to Achieve Permanent Denial-of-Service

Imagine a fast moving bot attack designed not to collect data but rather to completely prevent a victim's technology from functioning. Sounds unlikely, but it's possible. PDoS attacks have been around for a long time; however this type of attack only shows itself to the public periodically.

The most recent example was BrickerBot, which Radware discovered in April, 2017. Over a four-day period, BrickerBot launched thousands of PDoS attempts from various locations leveraging Telnet vulnerabilities to breach a victim's devices.

A recent article published by Help Net Security, detailed how a new USB exploit can be inserted into a computer and render a computer bricked. In fact, according to Help Net, the latest PDoS USB attack "when plugged into a computer … draws power from the device itself. With the help of a voltage converter, the device's capacitors are charged to 220V, and it releases a negative electric surge into the USB port."

Another example, covered in a 2008 article in Dark Reading, highlighted a tool uncovered by HP Labs called PhlashDance. This tool was leveraged to find vulnerabilities in often forgotten firmware and binaries that sit localized on computing devices. The risk lies in the lack of patches and upgrades made to the devices.

This article goes on to say that "remotely abusing firmware update mechanisms with a phlashing attack, for instance, is basically a one-shot attack. Phlashing attacks can achieve the goal of disrupting service without ongoing expense to the attacker; once the firmware has been corrupted, no further action is required for the DoS condition to continue."

Assessing Risks & Taking Action

The following behaviors and trends may increase the risk of a PDoS attack targeting your organization.

- Running a highly virtualized environment that leverages a few hardware devices, but powerfully overloads software functions. One PDoS on the platform can create a disaster recovery situation. This includes Software Defined Networks (SDNs).
- Organizations highly dependent on IoT. “Things” are highly susceptible to PDoS as they are often simple devices with little to no inherent security measures.
- Organizations with centralized security gateways. One powerful PDoS can punch a hole in attack detection and mitigation solutions.
- Organizations that are considered critical infrastructure.

The clear action to take is to conduct an assessment on the type of technology you are running at or below the operating system level. Develop a clear understanding of the different firmware versions, binaries, chip-level software (like ASICs and FPGA) and technology that is in use in your environment. Also consider batteries, power systems and fan system vulnerabilities.

Assessing the likelihood and risk of a PDoS attack can help your organization take the necessary precautions and onboarding controls to protect your most critical assets. Education is an important step in evaluating your risk of PDoS attacks.

ATTACK TYPE 5
IoT Botnets and The Economics of DDoS Protection

In 2016, a long-feared DDoS threat to fruition: cyber-attacks that are launched from multiple connected devices turned into botnets. Botnets are one of the fastest growing and fluid threats facing cyber security experts today and have propelled us into the 1Tbps DDoS era.

First, here is a timeline of the most notable attacks in 2016/17 that propelled botnets into the front pages and onto the desks of C-suite executives.

- **June 28, 2016**: PCWorld reports that “25,000 digital video recorders and CCTV cameras were compromised and used to launch distributed denial-of-service (DDoS) attacks, flooded targets with about 50,000 HTTP requests per second.”[2] Though impressive and startling, this attack was only the beginning.
- **September 20, 2016**: Around 8:00 pm, KrebsOnSecurity.com becomes the target of a record-breaking 620Gbps[3] volumetric DDoS attack from a botnet designed to take the site offline.
- **September 21, 2016**: The same type of botnet is used in a 1Tbps attack targeting the French web host OVH.[4] A few days later, the IoT botnet source code goes public, spawning what would become the “marquee” attack of the year.

2 http://www.pcworld.com/article/3089346/security/thousands-of-hacked-cctv-devices-used-in-ddos-attacks.html

3 https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

4 https://twitter.com/olesovhcom/status/779297257199964160

- **October 21, 2016**: Dyn, a US-based DNS provider that many Fortune 500 companies rely on, is attacked by the same botnet in what is publicly known as a "water torture" attack (see below). The attack renders many services unreachable and causes massive connectivity issues—mostly along the East Coast of the United States.

- **April 5, 2017**: Radware discovers BrickerBot, which over a four-day period, launches thousands of PDoS attempts from various locations around the world. BrickerBot uses Telnet brute force – the same exploit leveraged by Mirai – to breach a victim's devices.

The Appeal of Internet of Things (IoT) Devices

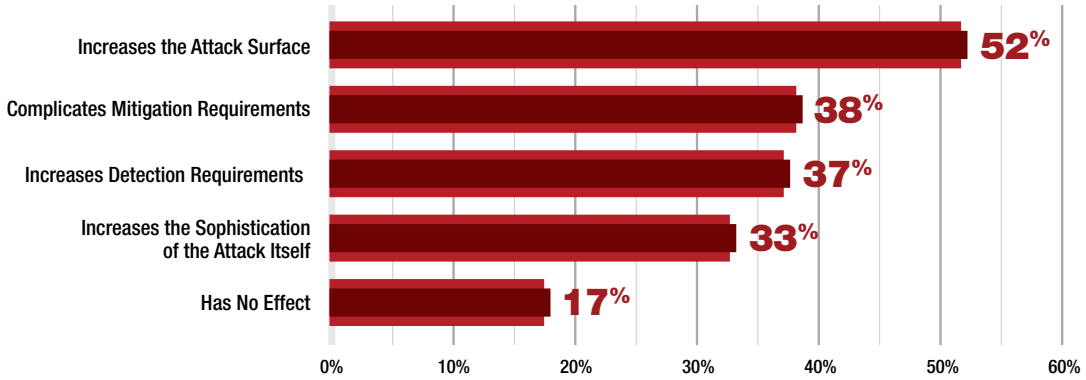
For hackers, IoT devices are attractive targets for several reasons:

- IoT devices usually fall short when it gets to endpoint protection implementation.

- Unlike PCs and servers, there are no regulations or standards for secure use of IoT devices. Such regulations help ensure secured configurations and practices. Among them: changing default passwords and implementing access control restrictions (for example, to disable remote access to administrative ports).

- IoT devices operate 24x7 and can be in use at any moment.

According to Radware's *2016 – 2017 Global Application & Network Security Report*, 52% of security professionals indicated that they believe IoT botnets complicate mitigation or increase detection requirements.



IoT threat impact as perceived by cyber-security professionals. Source: 2016-2017 Global Application & Network Security Report
Source: 2016 - 2017 Global Application & Network Security Report

Botnets: Making Use of Different Attack Vectors

The Mirai botnet provides a perfect example of the various attack vectors one IoT botnet can unleash on its victims. We can all thank a user named "Anna-senpai" for publishing the Mirai source code to a public and easily accessible forum. In short order, the code spread to numerous locations, including several GitHub repositories, where hackers began taking a closer look. Since then, the Mirai botnet has been infecting hundreds of thousands of IoT devices—turning them into a "zombie army" capable of launching powerful volumetric DDoS attacks. Security researchers estimate that there are millions of vulnerable IoT devices actively taking part in these coordinated attacks.

In a surprising departure from previous record-holding amplification attacks, attackers did not use DNS and NTP. Instead, these attacks consisted mainly of TCP-SYN, TCP-ACK and TCP-ACK + PSH along with HTTP and non-amplified UDP floods. In the case of KrebsOnSecurity, the biggest chunk of attack traffic came in the form of GRE, which is highly unusual.[5] In the OVH attack, more than 140,000 unique IPs were reported in what seemed to be a SYN and ACK flood attack followed by short bursts over 100Gbps each over a four-day period.[6]

5 https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
6 https://twitter.com/olesovhcom/status/779297257199964160

The Economics of Botnets

While much has been discussed around Mirai, IoT, “the rise of the machines” and other catchy buzz-phrases, we believe one of the most disruptive changes is the new economics model of IoT botnets.

Not so long ago, hackers were investing a great deal of money, time and effort to scan the Internet for vulnerable servers, build their zombie bots army and then safeguard it against other hackers who might also want to claim ownership of them. All the while, hackers would keep continual watch for new infection targets that could join their zombie army.

Things have changed: There are now millions of vulnerable devices sitting with default credentials. Bot masters—the authors and owners of the botnets—do not even bother to secure their bots after infection. After all, as Mirai demonstrates, it does not even persist infection to disk, so a simple device reboot brings it back to clean and healthy state.

For a bot master, gaining control of powerful servers would cost hundreds of dollars every month. Often he or she would gain illegal access to it and work diligently to hide it from others. Finding these servers was and still is difficult and expensive.

Now with IoT botnets, instead of spending months of effort and hundreds of dollars to control a few powerful servers and several hundred infected PCs, bot masters can take control of millions of IoT devices with near zero cost.

Knowledge is Power

To stay ahead of the threat landscape, knowledge is power. While hackers will continue to evolve these five threats, rest assured, 2018 will bring about a new array of attack vectors that seek to undermine cyber defenses and take advantage of application and network vulnerabilities. Leveraging both the in-house expertise of your organization's cyber security team in addition to the know-how of your DDoS vendor will be key to stay ahead of the threat.

Botnets will remain one of the preeminent threats for years to come. Read ***When the Bots Come Marching In, a Closer Look at Evolving Threats from Botnets, Web Scraping & IoT Zombies*** to understand what made this threat possible, how to protect IoT devices from becoming enslaved, and how to become a ‘botnet killer.’

radware