A Clear & Emerging Cyber-Security Threat: APDoS

The advanced persistent denial-of-service (APDoS) attack represents the very best of the worst. It is a clear and emerging cyber security threat that takes the finest that cyber assailants have developed in recent years and combines it into a multi-vector attack campaign that targets all layers of the IT infrastructure: network, server, and application.

Specifically, APDoS attacks involve massive network-layer DDoS attacks and focused application layer (HTTP) floods, followed by repeated SQLI and XSS attacks occurring at varying intervals. Typically, perpetrators simultaneously use five to eight attacks vectors involving up to tens of millions of requests per second, often accompanied by large SYN floods.

APDoS Attributes

At its core, APDoS assaults are a plethora of attack vectors combined into a single campaign, and thus representative of a number of cyber security trends and attributes being seen in the marketplace today. APDoS attacks target an organization's "blind spot" by increasing the number of attack vectors launched in parallel targeting different layers of the network and data center. This can include not just the target organization, but also service providers that provide Internet and cloud computing services and/or managed DDoS mitigation capabilities to the target organization as well. If only one vector goes undetected, the attack is successful and the results can be highly destructive.

Research underscores the increasing frequency of simultaneous, multi-vector attacks that combine network and application assaults. In its *2015 – 2016 Global Application & Network Security Report*, Radware explores attack frequency – the frequency of attacks for top network and application vectors. While there is some variation in the different types of attacks, overall, there is a similar spread of frequency between network and application attacks (see Figures 1 & 2). This is yet another indication that today's attack campaigns, specifically APDoS, involve multiple vectors from both the network and application layers and organizations must be able to protect themselves from both categories.

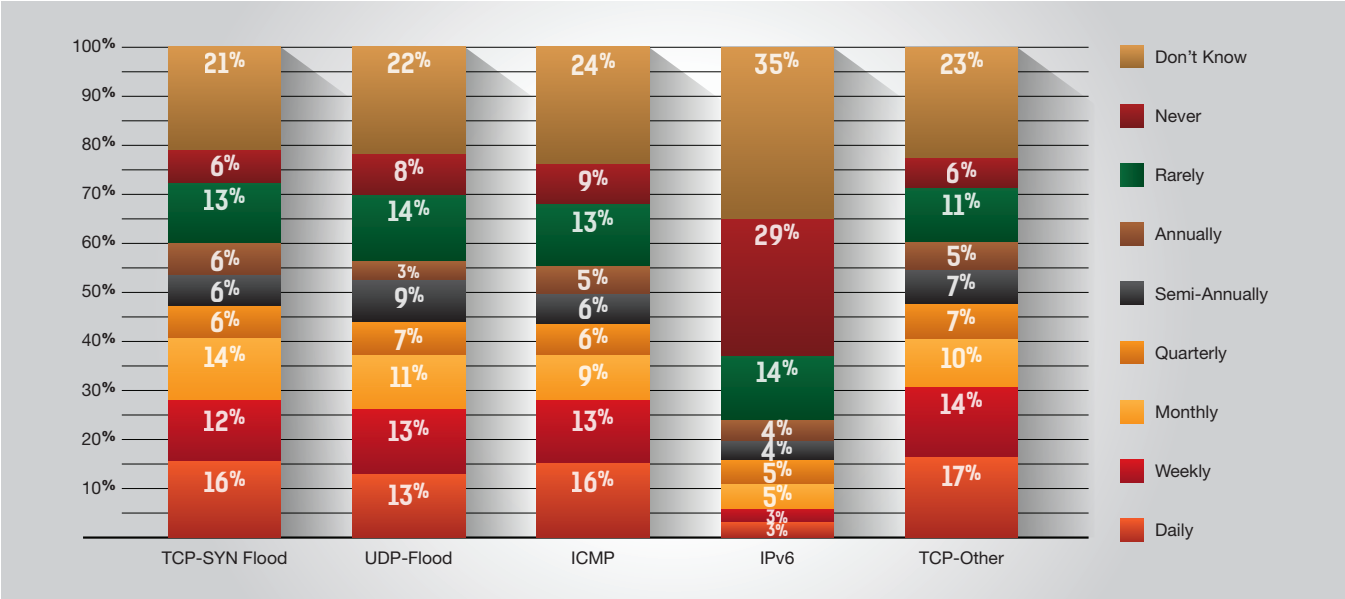

Figure 1: Frequency of Network Attacks in 2015

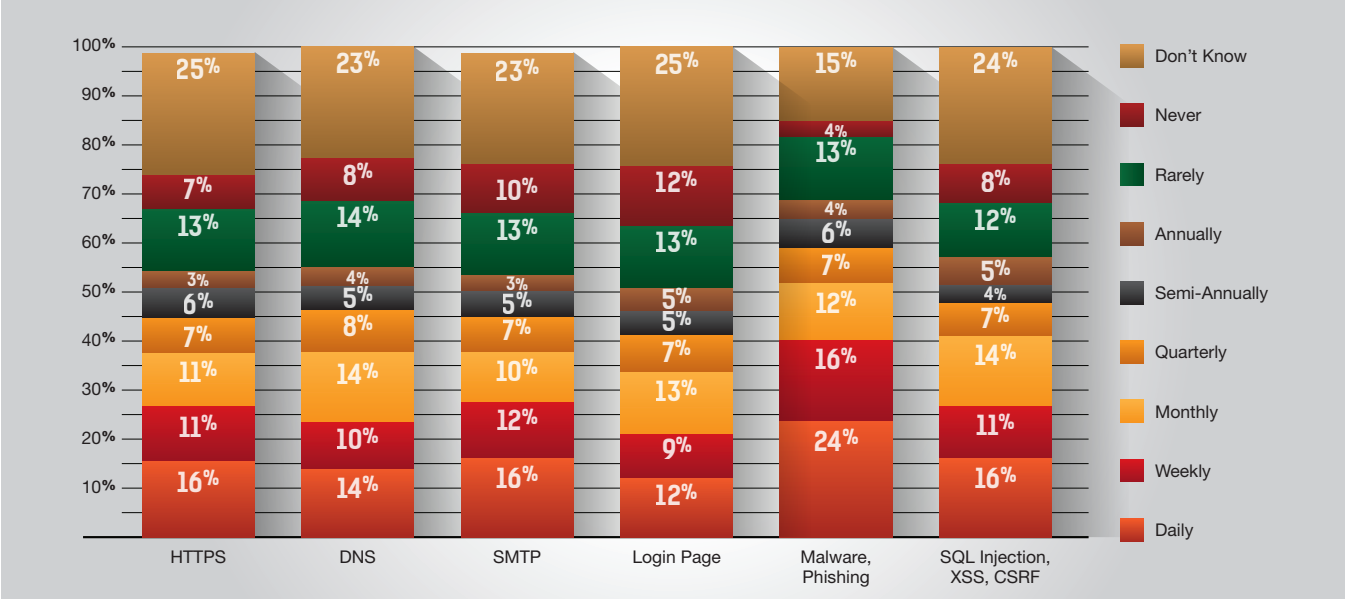

Figure 2: Frequency of Application Attacks in 2015

Automation is the name of the game for APDoS attacks. Cyber defenses continue to succumb to new, more sophisticated and automated attack techniques. In particular, the use of bot-generated attacks within APDoS campaigns is increasing as it offers a quick and efficient way for hackers to amplify the volume and scope of an APDoS assault.

These "bad bots" are used to support sinister objectives. This can include web attacks such as SQL injections and Cross-Site Request Forgery, web scraping, and web application DDoS. In addition, they present a stealthy challenge by dramatically complicating the detection process via a multitude of tricks and technologies, including:

- **Mimicking user behavior**: Using a browser-based plugin, several tools are able to mimic user behavior. Techniques include running JavaScript, downloading images and other referenced content.
- **Serving dynamic IP addresses**: Changing the source IP address enables tools to maintain a low-rate of activity per IP – thus evading IP-based detection systems.
- **Passing Challenges**: Some services are relaying CAPTCHA challenges to low-cost human "solvers."

Finally, APDoS is quickly becoming the preferred technique of hacktivists groups, and thus, the cause of a significant portion of business outages. Hackers in this scenario often switch tactically between several DDoS countermeasures while eventually directing the main thrust of the attack on a single victim. When hacktivists have continuous access to several, powerful network resources, they are capable of sustaining a prolonged campaign generating enormous levels of unamplified DDoS traffic.

Conclusion

It's not all doom and gloom. While the rise of APDoS is having far reaching impacts on cyber security, countermeasures – both new cyber security solutions and best practices – are being developed to effectively mitigate these assaults.

First and foremost, as defenses continue to succumb to the endless flood of more automated attack types, the idea that humans will have the ability to effectively deploy detection and mitigation technologies and choreograph responses in real time will disappear. These new attack modalities (APDoS, Burst Attacks, volumetric pipe attacks) will make it increasingly difficult to defend against using manual mitigation solutions.

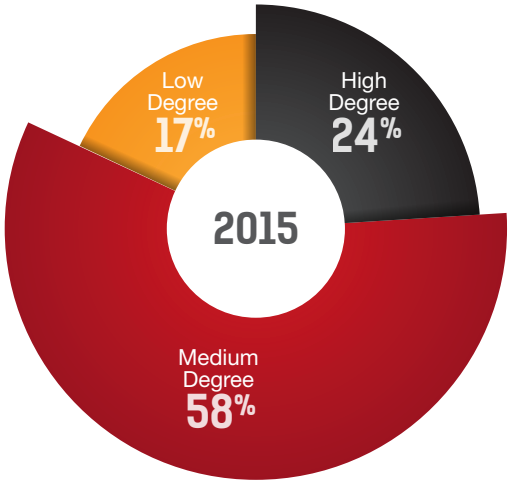

Figure 3: Degree of Manual Tuning or Configuration Required

Leveraging a heterogeneous collection of solutions requires a heavy degree of manual intervention to properly configure and protect an organization. According to the *2015 – 2016 Global Application & Network Security Report*, 91% of organizations are using multiple solutions, with just 6% relying on one solution against cyber-attacks. Almost three-fifths of survey respondents indicated a medium degree of tuning required by its current solution, pointing to a big vulnerability given the increase in fully automated cyber-attacks.

To combat APDoS, organizations will require a single vendor, hybrid cyber security solution that protects networks and applications from a wide range of attacks. Ideally, such a solution includes all the different technologies needed for effective detection and mitigation, including DoS/DDoS protection, behavioral analysis, IPS, encrypted attack protection and web application firewall (WAF). Additionally, organizations will also require new levels of partnership with their DDoS mitigation service provider and any ISP that provides managed DDoS services to coordinate for the effective detection and mitigation of a multi-vector assault.

Lastly, the rise of APDoS and volumetric pipe attacks, the use of detection-evading techniques such as user behavior and dynamic IP addresses, and across-the-board assaults that target all layers of a victim's IT infrastructure simultaneously will result in the rise of cyber botted-defense. In the quest to provide superior attack mitigation and protection, bots will take over a wide array of functions—including network and application security, compliance, cyber-attack mitigation, incident response, disaster recovery, and identity and access management.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.