Data Centers in the Crosshairs: Today's Most Dangerous Security Threats

Table of Contents

Introduction

Every day, attackers conspire to take down applications and steal data, leaving your data center infrastructure in the crosshairs. Storing the most valuable and most visible assets in your organization – your web, DNS, database, and email servers – data centers have become the number one target of cyber criminals, hacktivists and state-sponsored attackers.

This paper analyzes the top five most dangerous threats to your data center, namely:

1. DDoS Attacks
2. Web Application Attacks
3. DNS Infrastructure: Attack Target and Collateral Damage
4. SSL-Induced Security Blind Spots
5. Brute Force and Weak Authentication

This paper describes the impact of these threats and it reveals the latest methods, tools and techniques used by attackers to exploit data center resources. Then it lays out a framework to mitigate these threats leveraging technologies that are already present in most data centers today.

1) DDoS Attacks

Servers are a prime target for Distributed Denial of Service (DDoS) attacks and, increasingly, they are an attack weapon in the escalating war to disrupt and disable essential Internet services. While web servers have been at the receiving end of DDoS attacks for years, attackers are now exploiting web application vulnerabilities to turn web servers into "bots." Once attackers have drafted unwitting web servers into their virtual army, they use these servers to attack other websites.

By leveraging web, DNS and NTP servers, attackers can amplify the size and the strength of DDoS attacks. While servers will never replace traditional PC-based botnets, their greater compute capacity and bandwidth enable them to carry out destructive attacks, where one server could equal the attack power of hundreds of PCs.

With more and more DDoS attacks launched from servers, it's not surprising that the size of DDoS attacks have grown sharply in the past few years. In fact, between 2011 and 2013, DDoS attacks have surged in average size from 4.7 to 10 Gbps[1]. But the real story has been the staggering increase in the average packets per second in typical DDoS attacks; in fact, DDoS attack rates have skyrocketed 1,850% percent to 7.8 Mpps between 2011 and 2013. At the current trajectory, DDoS attacks could reach 37 Mpps in 2014 and 175 Mpps in 2015. Even if packet rates do not rise as sharply, DDoS attacks will be powerful enough to incapacitate most standard networking equipment.

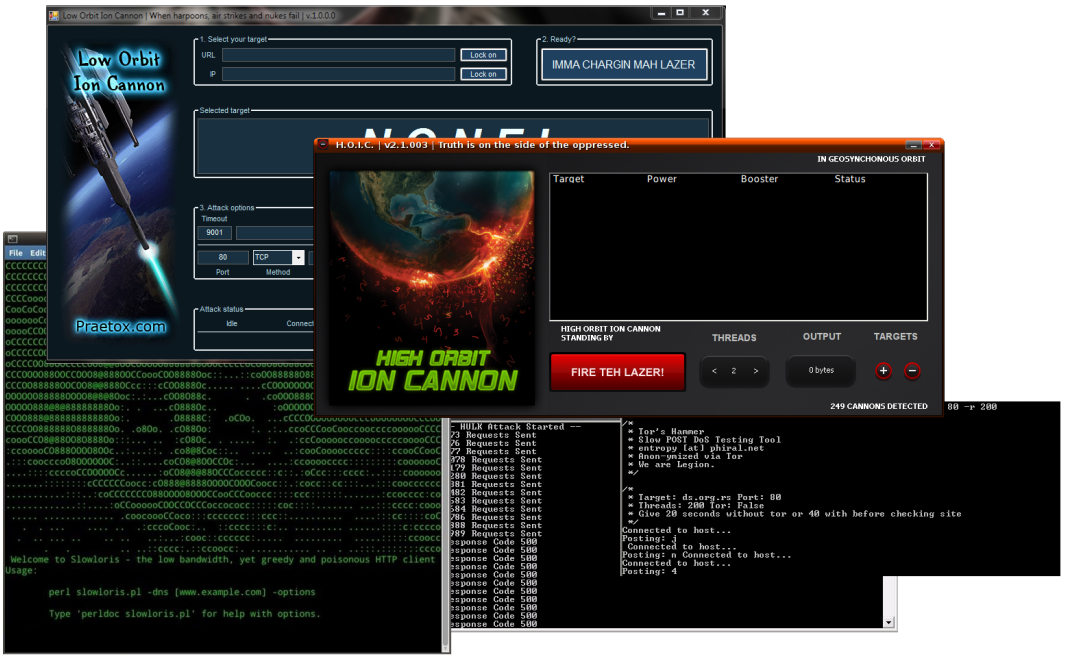

Figure 1. A variety of off-the shelf attack toolkits allow attackers to launch multi-vector attacks.

[1] Verizon 2014 Data Breach Investigation Report

DDoS for hire services, often called "booters," have mushroomed in the past few years. Many advertise their capabilities in slick (or in some cases not-so-slick) YouTube videos and forum posts. While some masquerade as "stress testing" services, many boldly claim to "take enemies offline" and "eliminate competitors." Offering DDoS attacks for as little as $5 an hour, these services enable virtually any individual or organization to execute a DDoS attack.

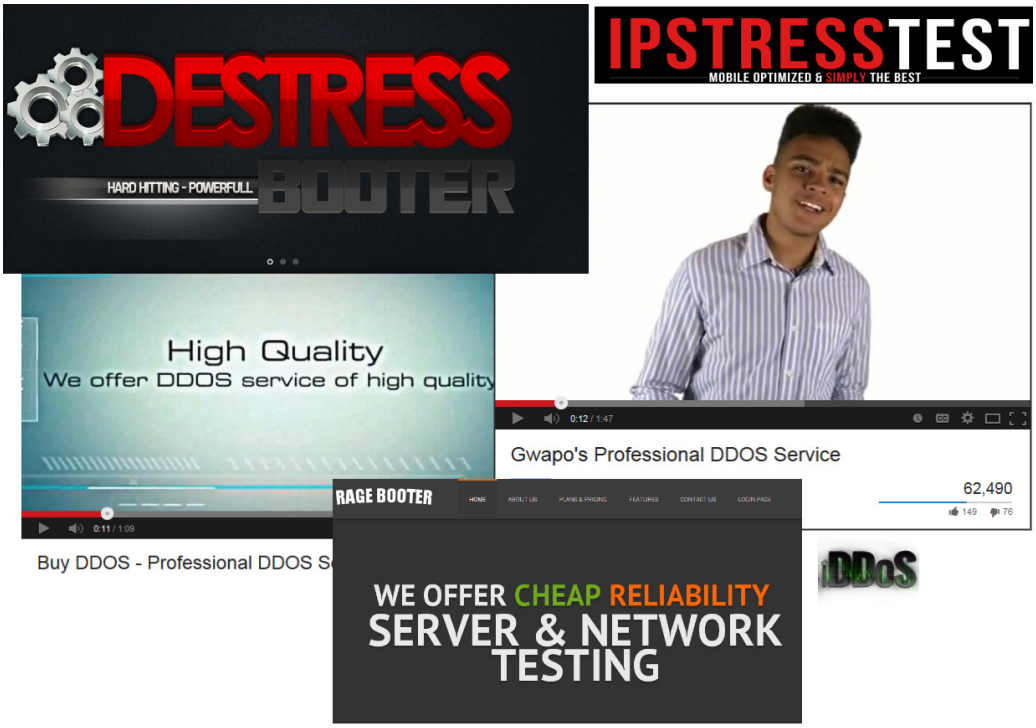

Figure 2: Examples of publicly available booters and DDoS attack services

FFIEC and MAS Guidelines for DDoS Protection

DDoS threats are growing and regulators have taken note. For example, the Federal Financial Institutions Examination Council (FFIEC), the Monetary Authority of Singapore (MAS) and the National Credit Union Administration (NCUA) have issued guidelines or risk alerts for DDoS mitigation. MAS specifically instructs financial institutions to "install and configure adequate devices…[to] divert and/or filter network traffic in real time once an attack is suspected or confirmed." [2]

While FFIEC, MAS, and NCUA guidelines only impact financial institutions, attackers are less discriminating, launching DDoS assaults against all types of organizations. Therefore, every organization should build up defenses to fend off the next DDoS attack.

2) Web Application Attacks

When cyber criminals and hacktivists aren't busy taking down websites with DDoS attacks, they are launching web attacks like SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF). They strive to break into applications and steal data for profit. And increasingly, attackers target vulnerable web servers and install malicious code in order to transform them into DDoS attack sources.

In 2013, hacktivists took aim at Content Management Systems (CMS) like WordPress, Joomla and Drupal as well as third-party CMS plugins. Once hacktivists uncovered a CMS vulnerability, they were able to quickly uncover and exploit countless CMS sites, before organizations could patch their vulnerable CMS applications.

[2] MAS Technology Risk Management Guidelines section D.2.2

Motives for Web Application Attacks

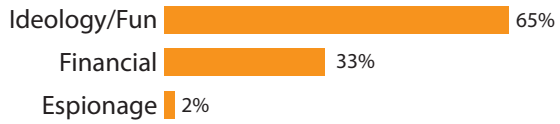

Figure 3. Hacktivism accounted for almost two-thirds of web attacks in 2013, according to the Verizon 2014 DBIR.

CMS applications aren't the only applications at risk. In fact, 96% of all applications currently have or have had vulnerabilities, and the median number of vulnerabilities per application was 14 in 2013.[3] Today's most dangerous application threats, like SQL injection and cross-site scripting, aren't new but they are still easy to perform and they are lethally effective. Attack tools like the Havij SQL injection tool enable hackers to automate their attack processes and quickly exploit vulnerabilities.

The recent wave of web attacks on CMS applications has also revealed a gaping hole in the age-old strategy to lock down applications by writing secure code. Because CMS applications are usually developed by third parties and not internally, organizations can't rely on secure coding processes to protect these applications. With 35% of all breaches caused by web attacks in 2013,[4] organizations, now more than ever, need a proactive defense to block web attacks and "virtually patch" vulnerabilities.

3) DNS Infrastructure: Attack Target and Collateral Damage

DNS servers have gained the dubious distinction of becoming a top attack target for two reasons. First, taking DNS servers offline is an easy way for attackers to keep thousands or millions of Internet subscribers from accessing the Internet. If attackers incapacitate an ISP's DNS servers, they can prevent the ISP's subscribers from resolving domain names, visiting websites, sending email and using other vital Internet services. DNS attacks have brought down service providers' DNS services for hours, even days, and in extreme cases have led to class-action lawsuits by subscribers.

Second, attackers can exploit DNS servers to amplify DDoS attacks. In the case of DNS reflection attacks, attackers spoof, or impersonate, the IP address of their real attack target. They send queries that instruct the DNS server to recursively query many DNS servers or to send large responses to the victim. As a result, powerful DNS servers drown the victim's network with DNS traffic.

Even when DNS servers are not the ultimate target of the attack, they can still suffer downtime and outages as the result of a DNS reflection attack. With DNS accounting for 8.95% of all DDoS attacks,[8] organizations that host DNS servers must protect their DNS infrastructure.

4) SSL-Induced Security Blind Spots

To prevent the continuous stream of malware and intrusions in their networks, enterprises need to inspect incoming and outgoing traffic for threats. Unfortunately, attackers are increasingly turning to encryption to evade detection. With more and more applications supporting SSL – in fact, over 40% of applications can use SSL or change ports[9] – SSL encryption represents not just a chink in enterprises' proverbial armor, but an enormous crater that malicious actors can exploit.

While SSL usage has been steadily climbing for years, the Edward Snowden revelations in June 2013 spurred on even greater adoption. After NSA whistleblower Snowden revealed that the NSA was snooping on citizens, privacy concerns soared. As a result, countless websites, from search engines to social media and file sharing to blogging sites, now offer SSL-enabled versions of their websites, and some websites such as Google only support SSL. Not reserved just for credit card transactions, SSL has become ubiquitous.

Data Center Security Risks

50% increase in number of DDoS attacks from 2012 to 2013[5]

1,850% increase in average DDoS packets per second from 2011 to 2013[6]

35% of data breaches caused by web app attacks[7]

80% of web-based breaches, for retailers, due to SQL injection

65% of web attacks launched by hacktivists in 2013

[3] Trustwave 2014 Global Security Report
[4] Verizon 2014 Data Breach Investigation Report
[5] Akamai's State of the Internet Report Q4 2013
[6] Verizon 2014 Data Breach Investigation Report
[7] Verizon 2014 Data Breach Investigation Report
[8] Prolexic Quarterly Global DDoS Attack Report Q1 2014
[9] Palo Alto Networks' Application Usage and Risk Report

While many firewalls, intrusion prevention and threat prevention products can decrypt SSL traffic, they can't keep pace with growing SSL encryption demands. The transition from 1024- to 2048-bit SSL keys, spurred on by NIST Special Publication 800-131A, has burdened security devices because 2048-bit certificates require approximately 6.3 times more processing power to decrypt.[10] With SSL certificate key lengths continuing to increase – and 4096-bit key lengths accounting for 20% of all certificates for one certificate authority[11] – many security devices are collapsing under these increased decryption demands.

For end-to-end security, organizations need to inspect outbound SSL traffic originating from internal users, and inbound SSL traffic originating from external users to corporate-owned application servers to eliminate the blind spot in corporate defenses. In its report, *SSL Performance Problems*, NSS Labs found that eight leading next-generation firewall vendors experienced significant performance degradation when decrypting 2048-bit encrypted traffic. This led NSS Labs to assert it had "concerns for the viability of SSL inspection in enterprise networks without the use of dedicated SSL decryption devices."[12] If the gamut of security devices can't keep up with growing SSL encryption demands, then organizations need a high-powered solution to intercept and decrypt SSL traffic, offloading intensive SSL processing from security devices and servers.

5) Brute Force and Weak Authentication

Applications often use authentication to verify the identity of users. With authentication, application owners can restrict access to authorized users and they can customize content based on user identity. Unfortunately, many application owners only enforce single-factor, password-based authentication. With weak single-factor authentication, application owners are exposed to a host of threats, from simple password guessing and stolen credentials to highly automated brute force attacks from password cracking tools.

Analysis from large-scale breaches of passwords, like the 38 million passwords exposed in the Adobe hack, reveal the limitations of simple, single-factor authentication. Researchers have discovered that many users select the same, common passwords, like "123456" and "password." In fact, 50% of password records in the RockYou breach included names, dictionary words, or trivial passwords based on adjacent keyboard keys,[13] and the 100 most common passwords account for 40% of all passwords chosen by users.[14]

Besides the risk of simple passwords, many users select the same password for multiple accounts. Unfortunately, when one of these accounts is compromised as part of a data breach, all other accounts sharing the same password are at risk. Within hours of a breach, hackers will crack stolen password lists – even password hashes – and use them to break into other online accounts.

Two-factor authentication can drastically reduce the risk of password cracking. Combining passwords with out-of-band authentication such as SMS messages to mobile devices or with hardware tokens or software tokens greatly decreases the risk of brute force or password cracking. In addition, user context, such as a user's browser and operating system or a user's geographic location, can help identify fraudulent activity. Application owners can build advanced rules to identify high-risk users or password cracking tools to safeguard user accounts.

For many organizations, simply rolling out and managing authentication across many different web applications can be daunting. Setting up client authentication schemes for dozens of applications entails costly and time-consuming development work. As a result, organizations need an integrated solution that can centrally manage authentication services and can block users with repeated failed login attempts.

Protecting Your Servers and Applications from the Top Five Data Center Threats

To shield data center infrastructure from attack, organizations need a solution that can mitigate a multitude of threat vectors and still deliver unmatched performance. Application Delivery Controllers (ADCs) can help organizations safeguard their data center infrastructure. Deployed in the heart of the data center, ADCs can block attacks, intercept and inspect encrypted traffic and prevent unauthorized access to applications.

[10] On commodity hardware, 2048-bit RSA certificates require 6.3x and 3.4x more computational effort, respectively than 1024-bit RSA certificates per a StackExchange analysis.
[11] NetCraft SSL Survey, May 2013, http://www.netcraft.com/internet-data-mining/ssl-survey/
[12] NSS Labs, "SSL Performance Problems"
[13] Imperva, "Consumer Password Worst Practices"
[14] Xato, "10,000 Top Passwords"

With malicious users increasingly setting their sights on data center servers, ADCs can provide best-of-breed protection against data center security threats. Next-generation ADCs offer the following defenses to shield data center infrastructure from emerging threats:

- DDoS Protection
- Web Application Firewall (WAF)
- DNS Application Firewall (DAF)
- SSL Insight™ (SI)
- SSL Offload
- Application Access Management for Authentication

Organizations should carefully evaluate the security features of ADCs to make sure they effectively mitigate data center risks. The A10 Thunder™ ADC product line helps organizations protect servers and applications from data center risks while still providing unmatched application performance. All A10 Thunder ADC appliances include a comprehensive set of security features at no additional cost. This is just one of the benefits of A10's all-inclusive licensing.

Conclusion

Attackers have set their sights on data centers. Whether seeking financial gain, competitive intelligence, notoriety or "the lulz," they have centered their focus on data center servers and applications. To carry out their assaults, attackers:

- Leverage off-the-shelf toolkits, automation techniques and armies of bots to launch devastating DDoS attacks
- Target web and DNS servers, not only to steal and manipulate data, but also to transform these servers into weapons to unleash powerful DDoS attacks
- Conceal their exploits from security devices using SSL encryption, exposing blind spots in corporate defenses
- Exploit weak authentication controls to compromise user accounts

Organizations need a solution that can lock down their data centers against these threats. If they ignore them, they incur the risk of a high-profile data breach, downtime and even brand damage. Because data centers host critical applications and data, organizations must safeguard these assets against attack and abuse.

About A10 Thunder ADC

A10 Thunder ADC helps thousands of organizations defend against the most dangerous data center threats. Thunder ADC prevents DDoS attacks, web application attacks, and DNS exploits. It streamlines and consolidates authentication, and it can decrypt encrypted traffic for inspection by third-party devices. With its integral role protecting applications and users, Thunder ADC has become a central security platform of the data center, ensuring that applications are highly available, accelerated and secure. To learn more about Thunder ADC's security capabilities, please visit www.a10networks.com.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-WP-21111-EN-02
Sept 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.