radware

SEE THROUGH THE DDoS SMOKESCREEN TO PROTECT SENSITIVE DATA

by Paul Mazzucco, Chief Security Officer, TierPoint

DDoS attacks can be costly and risky. TierPoint is witnessing a growing trend of using such attacks as the means to another, potentially more devastating, end: stealing sensitive data. Call this new breed of attack the “DDDoS”—deceptive distributed denial-of-service. For two recent examples, look to attacks on Carphone and Linode. By bombarding Carphone Warehouse with online traffic, hackers were able to steal the personal and banking details of 2.4 million people. Similarly, cloud provider Linode suffered more than 30 DDoS attacks which appeared to be a ruse to divert attention away from a breach of user accounts.

With these “DDDoS” attacks, cybercriminals distract business and IT resources to pursue larger objectives. The most recent Radware security industry survey shows that a growing number of security leaders are aware of escalating threats.

These are true concerns. DDoS as a smokescreen isn't new. Yet, as with so many cyber security trends, its rise can be traced to financial motives. The value of stolen data in the dark market intrigues potential cyber-delinquents to find ways to get access to it. The darknet offers a marketplace for capturing that value. Consider the following based on research by McAfee:

- Average estimated price for stolen credit and debit cards: $5 to $30 in the United States, $20 to $35 in the United Kingdom, $20 to $40 in Canada, $21 to $40 in Australia and $25 to $45 in the European Union

- Bank login credentials for a bank account with a $2,200 balance: $190

- Patient Health Information (PHI): $500 to $1,800 depending on patient age and insurance coverage

- Login credentials for online payment services, such as PayPal: $20 to $50 for account balances from $400 to $1,000; $200 to $300 for balances from $5,000 to $8,000[1]

Why Attacks Succeed

Lack of preparedness for DDoS detection and mitigation is a boon to cybercriminals. Indeed, about two-thirds of businesses are still mitigating attacks with tools not designed for DDoS. Web application firewalls switches, routers and traditional firewall ISP-based protection are unlikely to save a business from a DDoS attack. In fact, firewalls often create bottlenecks and accelerate outages. Unfortunately, due to inappropriate DDoS mitigations in place, organizations expose themselves not only to DDoS but also to other data-theft oriented attacks that arrive in conjunction with the DDoS attack. The unintended consequence? Companies not only suffer data leakage & reputation loss, their human and technological resources of rectifying the situation is at least doubled.

TierPoint observations and experience point to these as the most common vectors for DDoS smokescreen attacks:

- **Encrypted/non-volumetric attacks.** This includes protocol attacks, such as SYN floods, fragmented packet attacks and Pings of Death. These types of attacks consume actual server and/or firewall resources. Such resource starvation attacks use service calls to the IP stack, such as TCP-SYN requests and calls to the underlying authentication or operating system, to tie up and eventually overwhelm system memory and computing processes.

- **Application-layer attacks.** These include Slowloris and zero-day DDoS attacks, as well as DDoS attacks targeting Apache, Windows or openBSD vulnerabilities. Built around seemingly legitimate and innocuous requests, these attacks aim to crash the web server. Their magnitude is measured in requests per second.

- **Volumetric attacks.** These include User Datagram Protocols (UDP) floods, ICMP flood and other spoofed-packet floods. The goal: to saturate the bandwidth of the attacked site. Magnitude is measured in bits per second.

Mounting a Defense

Given their reach and impact, DDoS attacks are no longer an issue for just the security team or IT department. Such attacks—particularly when used as a smokescreen for more nefarious tactics—are now an executive and board-level concern:

TierPoint is witnessing a growing percentage of organizations turning to hybrid IT solutions to address security risks and concerns. This approach incorporates a mix of cloud and managed security services with products and services employed at a business' own data center.

An example is an organization combining a mitigation appliance and a mitigation service. While the appliance blocks attacks at the application layer, a cloud-based service scrubs higher volumes of malicious traffic. In the financial service industry, 45% of institutions have already adopted this approach.

As the stakes get higher—and the “smoke” grows thicker—TierPoint advises organizations to solidify a strategic DDoS detection and mitigation plan before an attack takes place. This includes understanding your risk profile and tolerance as well as determining the right balance of managed security services and security solutions administered internally.

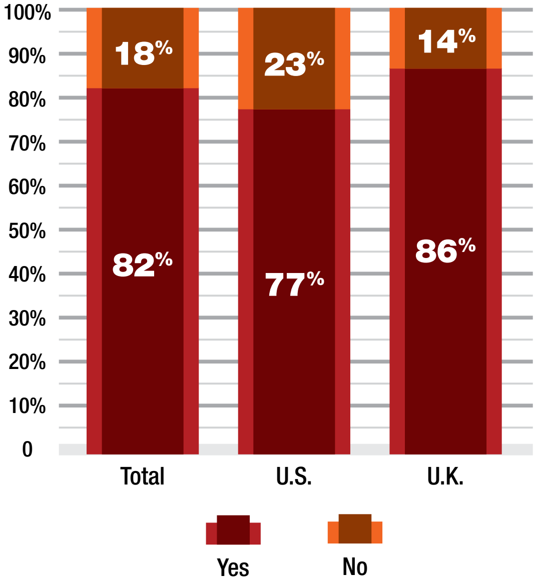

Figure 1: Radware 2016 Security and the C-Suite: Threats and Opportunities, Radware, 2016

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.