BIZCOMMUNITY

Visibility: your top defence against rising cyber attacks

By Martin Walshaw

7 Jul 2016

Anonymous Africa's recent Distributed Denial of Service (DDoS) attacks on the SABC and Oakbay Investments aimed to flood the websites of both companies with tons of information, eventually rendering the sites virtually unusable. These incidents demonstrate the alarming rate at which local organisations are falling victim to cyberattacks. They also show the extent to which companies are unprepared to protect themselves.

©Dmitriy Shironosov via 123RF

The attacks on the SABC and Oakbay were meant to just cause inconvenience, but these types of attacks can be far more damaging and, not to mention, financially draining. Although it may be tempting to say that companies must work harder to not make themselves obvious targets, this is not always feasible or even in a company's direct control. And this approach doesn't account for intentional internal leaks, orchestrated by disgruntled or unethical employees.

Organisations are facing a growing number of cyber security attack vectors. We've seen a dramatic rise in the number of exploits that seek to overwhelm servers with requests, and those that use encryption to target networks and applications in ways that leave traditional security methods struggling to detect and defend as required. Although these two types of threats diverge in their methods, their unifying factor is how targeted they have become.

Not only that, but as security professionals, we can't fall into the trap of romanticising the motives of 'hacktivists' – no matter where our political or social sympathies lie. Instead, the cyber security industry needs to evolve to be able to best counter the new trends in this sphere.

Denial of service attacks

A DDoS attack is one of the more popular methods employed recently. These attacks typically attempt to overwhelm a network or website to make it unavailable to users. Naturally, this is a big reputational and operational risk for businesses. DDoS is not a new method of attack, but certainly one that is enjoying prominence again. In the case of the SABC, Anonymous Africa executed a reflection attack that makes it appear as if the traffic is internal. Hybrid DDoS defenders offer a solution to these kinds of attacks, facilitating offsite cloud scrubbing to remove illegitimate requests.

According to Akami's State of the Internet Security Report Q1 2016, there was a 125% increase in DDoS attacks compared to the previous year. The research also revealed that the largest DDoS attack during the quarter measured 289

Gbps. As security practitioners, we've also seen a lot more attention given to this method in the last six to eight months, and recently encountered – and defended against – an attack of 448 Gbps.

Visibility in the face of rising encryption

Another trend in targeted attacks is the exploitation of increased encryption. Since the now-infamous Edward Snowden data leak in 2013, there has been a paradigm shift in encryption, especially across enterprise networks and applications.

There is more and more encryption happening on the internet today. Consumers and users are generating encrypted traffic both into and out of enterprise networks. Yes, encryption offers a degree of security, but for the cybersecurity industry, SSL may also create loopholes or gaps in the visibility of traditional security tools, and could actually negate some of the security measures that companies currently have in place.

This is especially pertinent for data leaks, such as outgoing information that is deliberately or accidentally shared from within the organisation. People may use encryption to try hide their sharing of sensitive information. An intrusion prevention device is able to inspect the packet that is coming in and out of the network, and flag potential issues, but if all of the traffic is encrypted, this device is rendered ineffective.

What is needed is something that can fit seamlessly into the flow, while decrypting, inspecting and re-encrypting, before sending on, or stopping the leak in its tracks. There are recently launched products that are able to do this, and pass the necessary information out to other security applications (service chaining), as well as traffic steering and load distribution.

New solutions like these will give businesses visibility into the areas of the network that are otherwise rendered inaccessible to their current security measures, and help them manage DDoS-type attacks. Integrated into existing security, these types of solutions offer simple remediation and eliminate blind spots. It is another indication of the sophistication security practitioners are having to adopt as the threats we face evolve at an ever-increasing pace, and becoming increasingly targeted.

ABOUT MARTIN WALSHAW

Martin Walshaw is a senior engineer at F5 Networks and has multiple accreditation from being a CCIE to being a CISSP to being an F5 Certified Professional. His background is in security, but he has also has skills in multiple different areas including unified communications, application acceleration and optimisation.

- Visibility: your top defence against rising cyber attacks - 7 Jul 2016
- How context can provide application-centric security - 30 May 2016
- The challenges and benefits of hybrid cloud migration - 12 May 2016
- What does SSDC mean for your business? - 28 Apr 2016
- Check your blindspot on the information superhighway - 13 Apr 2016

View my profile and articles...

For more, visit: https://www.bizcommunity.com