Sponsored by:

Author:
Megha Kumar
May 2017

Understanding the DDoS Landscape in the GCC

Evolving IT Ecosystems Create New Opportunities and Challenges

The IT ecosystems within Gulf Cooperation Council (GCC) countries — particularly those in the UAE and Qatar — are rapidly evolving as organizations increasingly adopt technologies such as cloud, enterprise mobility, social business, big data analytics, and the Internet of things (IoT) to sustain a competitive edge, modernize business processes, and meet the growing demands of customers and citizens alike.

Investments in Internet and mobile connectivity have enabled an increasingly mobile workforce to be provided with eservices, mobile applications, and "anytime, anywhere" access to corporate systems. According to the World Economic Forum, mobile phone penetration in the UAE and Qatar stood at 178% and 148%, respectively, in 2016 (World Economic Forum's *Global Information Technology Report, 2016*). With mobile devices increasingly becoming the computing tools of choice, organizations have had to invest heavily in ensuring they are able to provide their customers (i.e., consumers and businesses) with the right level of experience and superior quality of service.

This need for agile and responsive service delivery is heightened by the deployment of IoT technologies. Indeed, the increased use of IoT to optimize business processes and service delivery requires improved connectivity, as well as the deployment of sensors and applications to ingest data and produce the right level of response. IoT is creating new use cases across industries; according to IDC's *Worldwide Semiannual Internet of Things Spending Guide, May 2016* the IoT market in the Middle East is expected to reach $6.03 billion in 2020. Investments in 3rd Platform technologies and rapidly changing ecosystems make it imperative for IT to move from being a business enabler to actually being the business.

This shift will become more of a reality as organizations in the UAE and Qatar engage in digital transformation (DX). DX goes beyond the deployment of technologies; it encompasses innovation with new business models, the creation of new customer experiences, and engagement in strategic decision making, all underpinned by enabling operational efficiencies, improved performance, and — more importantly — relevance to the customer through agility and responsiveness. This last aspect requires IT to become a major part of the business itself rather than just remaining in a support role.

According to IDC's *Middle East CIO Summit Survey, 2016*, nearly 92% of organizations are either engaging in or planning to undertake DX. Ultimately, DX creates higher levels of interaction and engagement with organizations across various networks and leads to far more open and dynamic ecosystems, the majority of which may fall outside the control of any single organization or entity.

However, the achievement of these outcomes may be halted if IT is unable to deliver the required service level, user experience, or performance. In the above-referenced survey, CIOs in the Middle East, including those in UAE and Qatar, identified maintaining security (59%), ensuring performance (52%), and ensuring the availability of systems and services (47%) as their top three technology-related challenges. Clearly, downtime can have severe implications for an organization from financial, legal, and branding perspectives.

Maintaining a secure environment is a major challenge for organizations, particularly since the adoption of new technologies and devices creates many new endpoints, all of which need to be secured. In an integrated and open ecosystem, security is a challenge because organizations become part of a far more expansive and connected network. With IoT and connected smart devices, organizations and consumers are vulnerable to security incidents, which can be triggered by anything from a standard virus infection to hackers taking control of connected home appliances. Security will thus play a critical role in ensuring success for any organization as it enters the digital era.

An Increasingly Challenging Security Landscape in the UAE and Qatar

Organizations in the UAE and Qatar are increasingly susceptible to cybercrime as a result of more extensive connectivity, the adoption of new technologies, and the deployment of online and mobile services — as reflected in increases in security incidents in many sectors over the past few years. The majority of these incidents are financially motivated, although hacktivist attacks are also common, particularly on government entities.

Insider threats and a shortage of IT security skills add to this complexity. Insider threats remain a major cause for concern, particularly as employees often fail to adhere to security policies. Indeed, insider threats were identified in the abovementioned survey as the second biggest challenge to maintaining security (after limited budgets). Insider threats, whether based on unintentional or malicious actions, can leave organizations vulnerable to serious breaches. Alongside optimizing budgets, organizations face a major challenge in finding the right level of IT security skills to manage their environments — a situation that is driving demand in the region for security services and solutions that enable security automation.

Rise in Distributed-Denial-of-Service Attacks

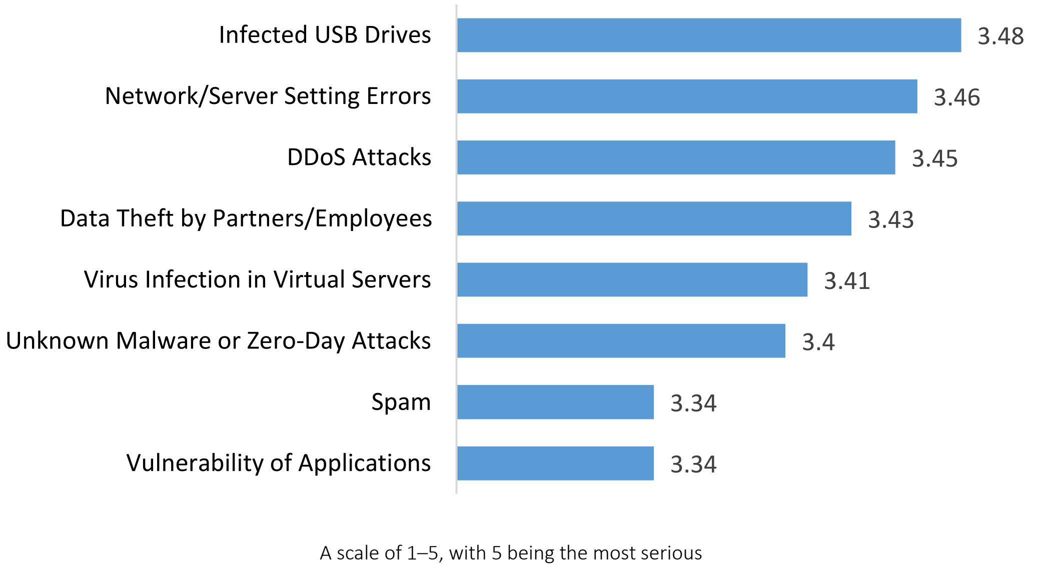
Among the largest distributed-denial-of-service (DDoS) incidents on record occurred in late 2016. Many websites experienced downtime or became slow due to an attack on Internet company DYN, impacting users across numerous countries. Hackers were suspected of using millions of malware-infected devices connected to the Internet to create the "botnet" needed to execute the attack, which, in turn, brought to light the vulnerabilities of the "world of things."

DDoS incidents are increasingly common and rising in complexity in the UAE and Qatar. DDoS incidents have impacted the websites and service levels of government, telecommunications, media, and finance organizations in these countries. DDoS attacks are increasingly being used as a method of extortion or as smoke screens for data theft. In 2016, the computer emergency response team of the UAE's Telecommunications Regulatory Authority revealed that hackers were using the threat of DDoS attacks to extort payments from banks.

In a recent survey conducted by IDC in the UAE and Qatar (see Figure 1), organizations were asked to rank the threats they consider to be the most serious to their ecosystems. DDoS attacks were referenced as a major threat. In Qatar, DDoS attacks ranked the highest, while infected USB drives were viewed as a more serious threat in the UAE — results that directly reflect incidents in these two countries over the months prior to the survey. The results also suggest that the integrity of network traffic is a major concern in Qatar, while insider risk is the biggest threat in the UAE. Regardless of their rankings, however, infected USBs, network/server setting errors, and vulnerabilities in applications can all be exploited to execute DDoS attacks.

FIGURE 1

Most Serious Threats to the IT Ecosystem in the UAE and Qatar, 2016

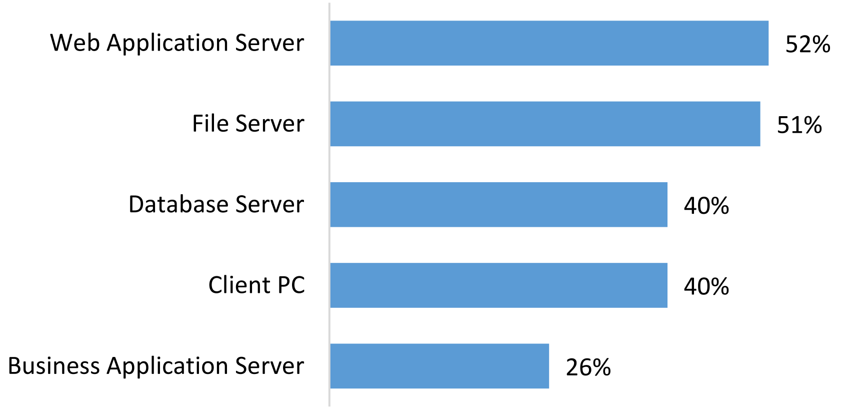


Source: IDC, 2016 N = 82

Many web application servers and file servers in both countries have been impacted by security incidents over the past 12 months (see Figure 2). Attackers are increasingly targeting web applications as a way of gaining access to corporate networks and user information. Hackers can utilize vulnerabilities in web applications to undertake DDoS attacks and essentially bring down services. The same applies to file servers: Weaknesses in a file server can be utilized to introduce malware and execute denial-of-service attacks.

FIGURE 2

Top 5 IT Assets Affected During Security Incidents in the UAE and Qatar, 2016

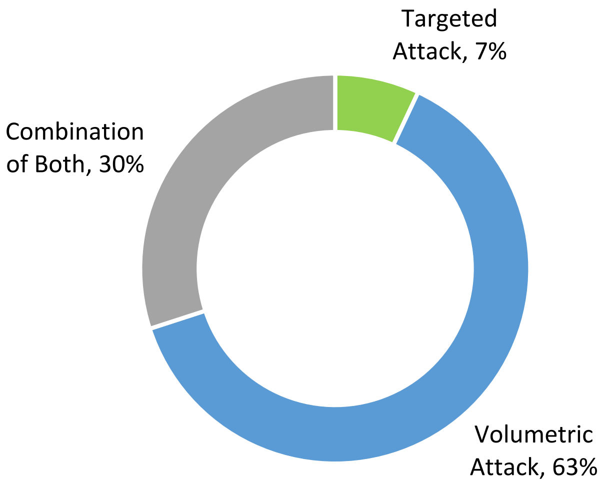


Source: IDC, 2016 N=82

Many of the surveyed organizations in the UAE and Qatar (see Figure 3) had experienced DDoS attacks over the past 12 months. Nearly 63% of those attacks were volumetric attacks; 7% were targeted attacks; and the remaining 30% were a combination of both. Volumetric attacks are the most common DDoS attacks, with multiple infected systems used to flood a network and impact its services. Such attacks are harder to combat, since several systems are used in their execution.

FIGURE 3

Types of DDoS Attack Experienced by Organizations in the UAE and Qatar, 2016

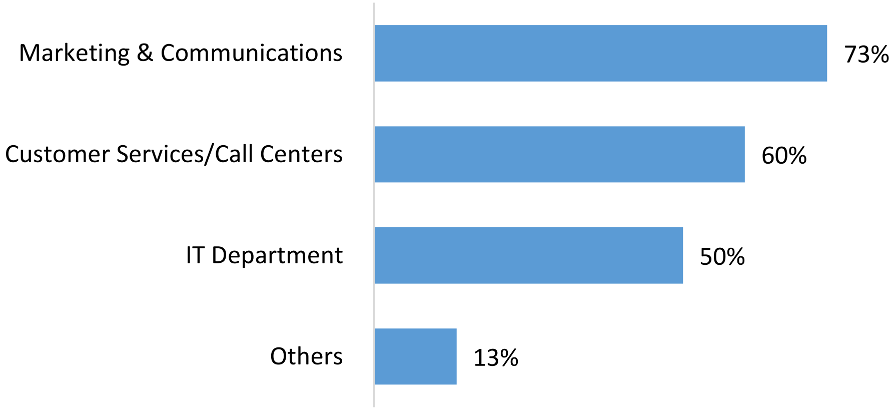


Source: IDC, 2016, N=30- Organization experienced DDoS Attacks

DDoS attacks lead to service disruptions and downtime, with nearly 50% of the organizations surveyed indicating that they were offline for 6–8 hours as a result of such attacks. These attacks restrict access to services for customers, prevent employees from accessing internal systems, and have severe financial implications. In 2016, marketing and communications departments were impacted the most by DDoS incidents, followed by customer services and call centers (see Figure 4). As a result of such attacks, the brand reputation of the organization suffers and the customer's ability to interact with personnel is curtailed. Service downtime essentially frustrates customers, negatively impacting customer loyalty and lowering brand/service expectations. It also impacts employee productivity, not least due to the service backlog it creates. The downtime of the IT department can bring all operations to a standstill and essentially disable the business.

FIGURE 4

Departments Impacted by the DDoS Attacks



Source: IDC, 2016, N=30- Organization experienced DDoS Attacks

Most organizations discovered attack incidents through security systems (77%), system and performance anomalies (50%), and reports from employees (30%) — a situation that reflects such organizations already have solutions in place, but without proper mitigation strategies. Most of the organizations surveyed (72%) indicated that they have deployed on-premises solutions to address DDoS threats. Such solutions are far more effective at dealing with targeted attacks than with volumetric attacks.

Organizations in the region need to become increasingly proactive when it comes to mitigating DDoS threats. DDoS attacks are increasing in sophistication and becoming more pervasive and persistent than ever before. This makes it absolutely critical for IT and security teams in the region to plan and deploy solutions that facilitate effective detection and mitigation.

Strategies for Effective DDoS Mitigation

This section aims to provide guidance on the security aspects that IT decision makers should consider addressing as their organizations evolve.

- **Leverage Intelligence:** An effective DDoS mitigation strategy requires organizations to understand their network traffic and detect anomalies and malicious behavior. Organizations should leverage their knowledge of the entire network, such as the reputation of the DNS, domain names, and registration details. This would enable IT to preempt concerns about traffic flow. In addition, organizations in an open ecosystem need to be more aware of the threat landscape, both regionally and internationally, so they can better evaluate the potential impacts on their networks.
- **Seek Security Services:** Organizations can leverage the services of ISPs, or even security services providers, to help them remain up to date in terms of the latest threat intelligence. Many ISPs and security services providers also provide DDoS mitigation services. In addition, organizations could consider DDoS mitigation as a service, as it may take away the pressure of having to manage the solution internally. Such services enable network monitoring and protection of corporate networks, as well as effective detection and mitigation.
- **Adopt a Hybrid Strategy:** The majority of organizations IDC surveyed have deployed on-premises solutions for DDoS mitigation. However, on-premises solutions are not effective in defending organizations against high-volume attacks. A much better strategy for organizations would be to embrace a hybrid approach — one that combines on-premises and cloud-based solutions. A cloud-based solution will provide corporate networks with comprehensive security, covering different types of attack and DNS-based data exfiltration. In addition, cloud-based solutions enhance protection by being closer to the source of the attack and provide a strong abstraction layer for corporate enterprise resources.
- **Understand that DDoS Is More than Denial of Service:** Many DDoS attacks are used as smoke screens for other critical security breaches. Following the occurrence of a DDoS attack, organizations must immediately evaluate whether any data breaches have occurred or whether any other security incidents have taken place or are still in progress. Swift detection and mitigation are critical, meaning organizations should aim for a high degree of automation.