radware

# In the Crosshairs: Six Cyber Security Threats Gunning for Your Online Business

In today's hyper-connected world, nearly all businesses, regardless of size or industry, have some element of their operations based online. From the largest online retailers and financial service companies to gaming and social media brands, organizations are transforming how they conduct business and have become increasingly dependent on network-based services. Even the smallest service-oriented organizations rely on the Internet for ecommerce or as a platform to deliver services to employees and partners.

These pros also come with some cons. Online businesses have become juicy targets for cyber assailants. Certain industries face a heightened level of threat due to the unique level of business operations and revenue generated online. The threat landscape targeting these organizations is growing in virulence, driven by hackers seeking to take advantage of the knowledge that these businesses cannot afford downtime or loss of customer trust.

Because of this, security teams from online businesses have always been among the leaders in exploring and adopting security capabilities that protect online revenue generation, service delivery platforms and sensitive customer data. However, the threat landscape continues to adapt to new protections, forcing a continuous effort to stay innovative and ahead of the latest cyber assault trends, tactics and tools. To help online businesses reduce the risk of downtime, lost revenue and resulting customer churn, here are six of the most common cyber security threats targeting online businesses.

## Availability Attacks (including distributed denial of service)

For decades, information security has focused on the 'security triad' of confidentiality, integrity and availability. In many cases, investments in information security have focused much more on the first two of these principles much more than the third. However, as more critical aspects of business operations shift towards online models, availability becomes an equal tenant to the others. Attackers have become adept at exploiting remaining deficiencies however, largely through distributed denial-of-service (DDoS) attacks. DDoS attacks are consistently among the most frequently experienced attacks.

## $ Ransom Attacks

There has been an increase in ransom as a motivation for cyber-attacks, increasing from 16% in 2014 to 25% in 2015, according to Radware's *2015 – 2016 Global Application & Network Security Report*. These ransom attacks are on the rise for a number of reasons. First, the ease of access and relative low cost of launching disruptive attacks makes the motive of immediate financial gain attractive. So too does the increased ease of masking the source of attacks through spoofing IPs or accessing targets via a CDN or global NAT that will obfuscate the exact attacking resources as part of a broader network.

## Advanced Bot Attacks

Bot-generated attacks targeting web application infrastructure are increasing in both volume and scope, with the list of attack vectors—and associated risk profiles—growing. Among the most common: web attacks, such as SQL injections and Cross-Site Request Forgery (CSRF), web scraping, web application DDoS, brute-force attacks on login pages for password cracking, comment spammers, clickjacking and fraud. Some bot-generated attacks are static; others are dynamic over time. Simple, script-based bots are not much of a challenge to detect and block. The same cannot be said of more advanced bots. Those based on headless browser technology, such as PhantomJS, dramatically complicate the detection process by mimicking user behavior, passing challenges (e.g. CAPTCHA), or by serving up dynamic IP addresses.

## Transaction Fraud

Online transaction fraud costs an estimated $3.5 billion annually[1]. Much of this activity is attributed to the theft of consumer credit card information breached by application attacks that exploit online business applications. The impacts of transaction fraud also extend beyond the immediate transactions. Consumers consistently say that if their sensitive data is breached, they will likely no longer conduct business with that merchant. A common set of attack references with regard to transaction fraud are those tracked by the Open Web Application Security Project as part of their OWASP Top 10 list. Among those, SQL Injection consistently ranks as a top threat targeting illegitimate access to applications and backend databases.

## Encrypted Attacks

In the same way, SSL and encryption protect the integrity of legitimate communications, they equally obfuscate many attributes of traffic used to determine if it malicious versus legitimate. Identifying attack traffic within encrypted traffic flows is akin to finding a needle in a haystack...in the dark. Most cyber security solutions struggle to identify potentially malicious traffic from encrypted traffic sources and isolate that traffic for further analysis (and potential mitigation).

The other major advantage that SSL attacks offer to attackers is the ability to put significant computing stress on network and application infrastructures they target. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic, in many cases beyond the functional performance of devices used for attack mitigation.

---

1 http://www.pymnts.com/news/2015/2014-fraud-spike-cost-u-s-retailers-32-billion/

## Dynamic Content and CDN-based Attacks

As online businesses mature and build global web properties, they often turn to Content Delivery Network (CDN) providers to support site performance. CDNs provide a particularly insidious cover for bad actors as they cannot be blocked by origin servers as accepting transactions and requests from their IPs is the basis for use of their content distribution capabilities. Malicious actors have made an art form out of spoofing IP addresses to not only obfuscate their identity but also to possibly masquerade as seemingly legitimate users based on geolocation or positive reputational information about IP addresses they are able to compromise. Dynamic content attacks further exploit CDN-based protection by overloading origin servers with requests for non-cached content that the CDN nodes simply pass along.

## Ensure the Availability of Your Online Business

- Reduce the risk of lost revenue, customer churn, and employee productivity by learning about Radware's Online Business Protection Solution.
- Download the eBook *Opportunities, Threats and Security Strategies for Online Business* to learn more about the most common types of attack targeting online businesses