Daily implications of cyber-attacks

Or Katz, 2012-25-01

I don’t know if you had the chance to hear about it but in the last couple of weeks a mini cyber-attack campaign was being held in the Middle East. It all started a couple weeks ago when a hacker (allegedly from the Arabian Peninsula) published several thousand Israeli credit card numbers and email addresses. This was the first round in a potential multi-round skirmish that at its highest peak included Distributed Denial of Service (DDoS) attacks from both parties on both Saudi Arabian and Israeli stock exchange web sites. How did all this transpire? Let’s look at the details and I’ll share how I think it unfolded:

1. Attack method – as far as I understand, the attackers used these attack techniques:

i. SQL injection on each other’s web applications, penetrating into the applications’ databases and stealing sensitive information.

ii. Web Application DDoS attacks, according to information that was published over the media. These attacks involved up to 10,000 different sources (computers that were infected by malware and controlled by attackers).

2. Source of the attack – according to information that was published in the Israeli media, 50% of the sources of the attacks were from Israel.

3. Attack complexity – service of DDoS attacks can be bought for money, and renting an army of infected computers controlled remotely doesn’t require technical skills. SQL injection is a well known vulnerability for more than 10 years and unfortunately it is here to stay. On the web you can find many free tools that can find the vulnerability and create an exploit for it.

What can be learned from it?

While from the common web user’s point of view this seems like a major incident that should be addressed on a nationwide scale (which is probably true), this kind of incident happens all the time on commercial web applications, but in many cases never reaches the news. Protecting your application, allowing confidentiality of customers’ stored data (for example, credit card numbers), supplying 24/7 accessibility to the web application, and maintaining a secure reputation are key objectives for web application administrator.

Here is something to think about: the biggest impact of this affair was on the public's state of mind. It got a lot of the media attention, it raised public awareness regarding the use of credit cards on the web, and started new discussions on threats that we may encounter as a nation in future cyber warfare.

F5 Networks' BIG-IP Application Security Manager supplies the answer for these challenges by allowing the web application administrator to deploy a layer 3 to layer 7 unified security architecture that includes network and application DoS and DDoS protection, while at the same time prevents SQL injection attacks.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com