Abstract

In 1995, the United States Congress passed the Jerusalem Embassy Act, which was created for the purposes of initiating and funding the relocation of the Embassy of the United States in Israel from Tel Aviv to Jerusalem.

The law has remain unimplemented by U.S. Presidents Clinton, Bush and Obama, who viewed it as a Congressional infringement on the executive branch's constitutional authority over foreign policy. President Donald Trump signed the waiver in June 2017 before announcing the recognition of Jerusalem as Israel's capital on December 6, 2017 and beginning the relocation process.

Following this announcement anti-American and anti-Israeli groups under the Anonymous collective umbrella declared that they would be launching attacks against any and all websites deemed to be Israeli and in addition to the United States government. These Anonymous groups are calling for hacktivists around the world to join forces and urges participants to hack, deface, dox, hijack, leak and DDoS any target in Israel and websites associated with the US government. In previous years, Israel has seen moderate attacks launched against its networks and infrastructure, resulting in defacements of unsecured websites of small- and medium-sized businesses.

Figure 1: Hacktivist - GatorLeague

Reasons for Concern

Research by Radware's Emergency Response Team has witnessed several SQL injections, data dumps and service outages because of this current operation. Anonymous has also posted lists of names, emails and passwords of Israeli public employees from various websites. One of the main concerns with this operation is Anonymous's targeting. Since large government agencies are typically well protected, the group is focusing attacks on small- and medium-size businesses that are indirectly involved.

Updates for this operation can be found at: https://www.cyberguerrilla.org/blog/

Operation Video

Figure 2: https://youtu.be/AHEC6eWsikY

Attack Vectors

Web Application Exploits

- **SQL Injection** - This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database and more.
- **Defacement** – Attacker changes the visual appearance of the website by breaking into a web server and replacing the current website with one of their own. This attack is most commonly associated with SQL.
- **Injection** - This form of an attack allows administrative access and usually involves obtaining user credentials first. It allows hackers to make changes to a website.
- **Data Theft** – compromising sensitive data while data at rest or in transit, via stealing encryption keys, hashed passwords, clear text data off the server, and even from a user's browser.

Denial-of-Service Attack Vectors

- **TCP flood** - One of the oldest, yet still very popular denial-of-service attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be, it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application-level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.
- **UDP Flood** – In a UDP flood, the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC (source) IP.
- **HTTP/S Flood** - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests

sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

```
intext:"error in your SQL syntax" +site:gov.il
intext:"mysql_num_rows()" +site:gov.il
intext:"mysql_fetch_array()" +site:gov.il
intext:"Error Occurred While Processing Request" +site:gov.il
intext:"Server Error in '/' Application" +site:gov.il
intext:"Microsoft OLE DB Provider for ODBC Drivers error" +site:gov.il
intext:"Invalid Querystring" +site:gov.il
intext:"OLE DB Provider for ODBC" +site:gov.il
intext:"VBScript Runtime" +site:gov.il
intext:"ADODB.Field" +site:gov.il
intext:"BOF or EOF"+site:gov.il
intext:"ADODB.Command" +site:gov.il
intext:"JET Database" +site:gov.il
intext:"mysql_fetch_row()" +site:gov.il
intext:"Syntax error" +site:my intext:"include()" +site:gov.il
intext:"mysql_fetch_assoc()" +site:gov.il
intext:"mysql_fetch_object()" +site:gov.il
intext:"mysql_numrows()" +site:gov.il
intext:"GetArray()" +site:my intext:"FetchRow()" +site:gov.il
intext:"Input string was not in a correct format" +site:gov.il
```

Figure 3: List of suggested SQL dorks

Hashtags

- #OpUSA
- #OpIsrael
- #FreedomInWorld

Original Targets

Israel

https://www.gov.il/
http://www.president.gov.il/
http://itrade.gov.il/
http://www.investinisrael.gov.il/
http://www.antitrust.gov.il/
http://www.boi.org.il/en/
http://www.space.gov.il/
https://www.shabak.gov.il/

USA

https://www.usa.gov/
https://www.state.gov/
https://www.whitehouse.gov/
https://www.ssa.gov/
https://www.data.gov/
https://www.irs.gov/
https://www.federalreserve.gov/

How to Prepare

It's expected that those involved directly and indirectly could be targeted by SQL injections, cross-site scripting (XSS), data dumps and service outages caused by denial-of-service attacks. It is expected that these attacks will continue through the rest of December as the United States begins to move their embassy to Jerusalem and officially recognize it as the capital of Israel.

Radware offers a full range of solutions to help your network properly mitigate attacks. Radware's DefensePro provides network protection with real-time, behavioral-based attack mitigation while its Attack Mitigation Service can also aid in detection and mitigation with cloud-based volumetric attack scrubbing.

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further DDoS protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10 vulnerabilities coverage**– against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto-policy generation capabilities** for the widest coverage with the lowest operational effort
- **Bot protection** and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

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.