Abstract

OpIsrael is a yearly campaign created by Anonymous in 2012 with the stated goal of “erasing Israel from the internet” in protest against the Israeli government’s conduct in the Israeli-Palestinian conflict. Ideology, politics and religious differences are at the core of this operation. Every year the operation begins on April 7th (typically concluding April 14th) and sees participants from Anonymous and a number of other low-level hacktivist groups. Heading into the operation, Radware’s Emergency Response Team has observed hacktivists organizing groups on social media, forums and Internet Relay Chat (IRC) leading up to the operation.

Figure 1: *This is a message to the foolish Zionist entities. We are coming back to punish you again, for your crimes in the Palestinian territories. All we see is continuous aggression, bombing, killing and kidnapping of the Palestinian people. We refuse to stand by idly. Our response to these heinous crimes against humanity will be on the 7 of April 2018. As we did many times, we will take down your servers, government websites, Israeli military websites, your banks and your public institutions. We’ll erase you from cyber space as we do every year. We will continue to electronically attack you until the people of Palestine are free.*

***Source**: https://www.cyberguerrilla.org/blog/anonymous-opisrael2018-7-april/*

Background

In the past years, Israel has seen moderate attacks launched against networks and infrastructure. The most common tactics are website defacements and denial-of-service (DoS) attacks but have also included application attacks and data dumps.

Each year, hackers organize in public channels like IRC, Twitter and Facebook to discuss operational details in the open. Attackers provide others with tools and technical guidance leading up to the operation’s launch date. They post links to videos, attack tools and recommend VPN’s along with target lists and content for social media posts.

Several tools that are shared leading up to the operation are outdated and easy to mitigate due to exising signatures. Typical tools shared are GUI-based tools like Windows DoS, LOIC, HOIC, Tsunami, An0nStr3ss as well as basic script tools like Torshammer and other HULK varients. TorsHammer, a slow-rate HTTP POST (Layer7) DoS tool that can be carried out through the Tor network, has been a recommended tool since 2012.

OpIsrael receives a large amount of attention for several reasons, one of them being the global media coverage surrounding the Israeli-Palestinian conflict. The other is due to past operational successes by Anonymous, but in recent years this has been slowly fading. OpIsrael is losing its reputation as a successful operation overall. In recent years, pro-Israeli hackers have launched counter attacks against the operation. These attack are often more successful and gain more attention than the operation itself.

The main activity for the operation occurs leading up to April 7th via limited attacks for the rest of the campaign. Defacements are normally the most common attacks seen during the operation and normaly plague unprotected

small businesses as the hackers normal can not launch successful attacks against secured targets. DDoS attacks are normally limited and infact just standard DoS attacks since the hacktivist are unable to create botnets of their own for distributed attacks. Successful attacks only last for a few moments as most attackers do not have enough power to keep a website offline.

Web Application Attacks

Cross-Site Scripting - In this attack, malicious scripts are injected into websites through a web application flaw where there is no validation of user input used by the application. The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine or spoof content to fool the user.

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.

Remote File Inclusion (RFI) - This is a type of vulnerability most often found on PHP running websites. It allows an attacker to include a remotely hosted file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, can lead to arbitrary code execution.

Local File Inclusion (LFI) – This is very much like RFI; the only difference is that in LFI the attacker has to upload the malicious script to the target server to be executed locally.

Figure 2: Deface by Giant's PS and Electronic Thunderblot

Denial-of-Service

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.

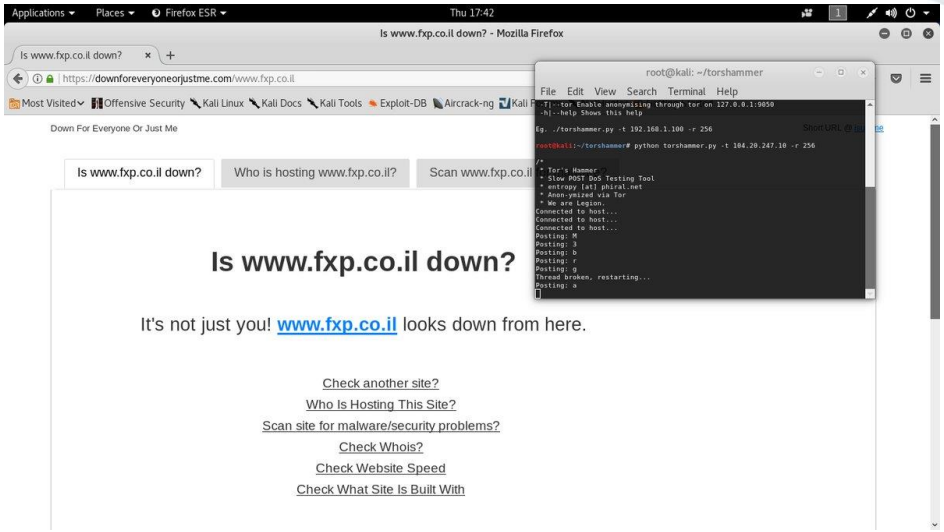

Figure 3: TorsHammer – Slow POST HTTP

Amplification Attack: Amplification attack is a sophisticated denial-of-service attack that takes advantage of legitimate third-party components to enlarge an attack. To launch an amplification attack, the attacker sends packets to a reflector (DNS, NTP, Memcache) with the source address replaced with the victims IP address. This will cause the servers to respond, sending large replies to the spoofed IP, the victim, thus flooding the victim. This attack generates a great deal of traffic and can easily cause a denial-of-service.

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

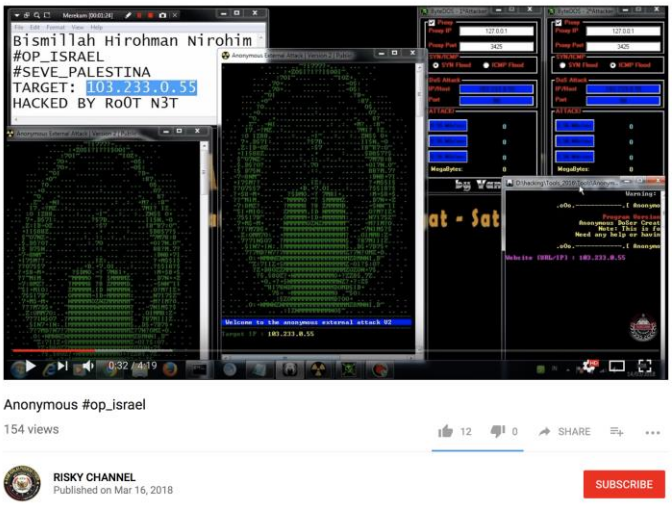

Figure 4: OpIsrael Attack Video

Other Attacks

Phishing - A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim to these the hacker will then have the sensitive information required to gain access to certain systems.

Social Engineering - A process of psychological manipulation, more commonly known as human hacking. The goal is to have the targeted victim divulge confidential information or give you unauthorized access because you have played off their natural human emotion of wanting to help or provide them with something. Most of the time the attacker's motives are to either gather information for future cyber-attacks, to commit fraud or to gain system access for malicious activity.

Google Dorking – Dorking is a term that referes to the practice of applying Google advanced search techniques by using specialized serach engine parameters to discover vulnerabilities or information that was not intended to be discovers. For example, OpIsrael hacktivist could use the dork "co.il admin login.php." This search will return login pages for Israeli based websites.

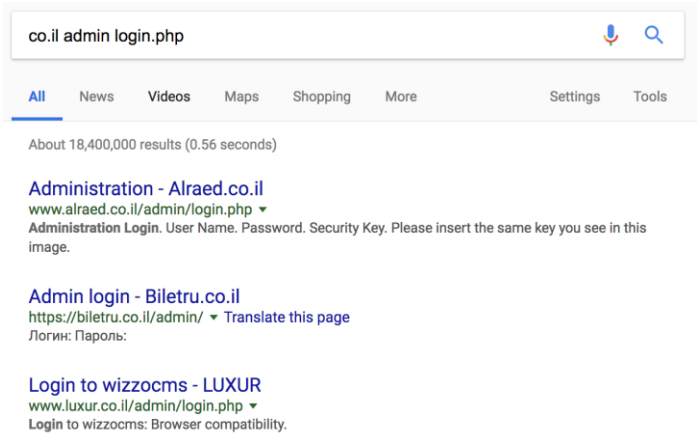

Figure 5: Google Dork

Shodan – Hackers often abuse legitimate services for illegitimate purposes. Shodan is a search engine for Internet of Things (IoT) where you can find anything from webcams and refrigerators to power plants and other Internet connected devices. By using different keywords and search parameters users are able to find and located specific connected devices. For example, "content/smarthome.php," returns over 140 login panels for an Internet connected devices

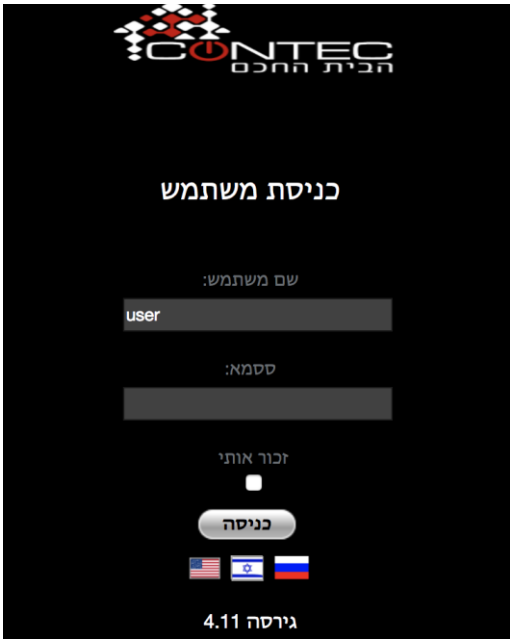

Figure 6 & 7: Example of Shodan search for Israeli smart homes

Operational Information

Video:

- https://youtu.be/5xfnc0Fekms

Paste Sites:

- Pastebin.com
- Ghostbin.com
- Zerobin.net
- Zerobinqmqd236y.onion

Attacking Groups

- Anonymous
- Giant's PS
- Electronic Thunderbolt Team
- MCA DDOS Team
- Red Cult
- DarkCoder/Th3Falcon

Facebook Pages

- https://www.facebook.com/events/1909439512701420/
- https://www.facebook.com/events/135611853669135/

Hashtags

- #OpIsrael
- #OpIsrael2018
- #FreeGaza
- #FreePalestine

Targets

- pmo.gov.il/Pages/default.aspx
- mossad.gov.il
- gov.il
- knesset.gov.il
- jerusalem.muni.il
- haifa.muni.il
- idf.il
- yadvashem.org
- israelpost.co.il
- israelinarabic.com
- makan.org.il
- al-masdar.net
- terrorism-info.org.il
- altawasul.com
- antiquities.org.il
- mevaker.gov.il
- tavisrael.co.il
- jewishagency.org
- birthrightisrael.com
- police.gov.il
- education.gov.il
- danhotels.com
- israelbar.org
- egged.co.il
- next.co.il

Recon Tools Used by Anonymous

SQLmap - Automatic SQL injection and database takeover tool
Recon-ng - A full-featured Web Reconnaissance framework written in Python
SET - The Social-Engineer Toolkit (SET) repository from TrustedSec
theHarvester - E-mails, subdomains and names Harvester - OSINT
OWASP ZAP - An open-source web application security scanner
Metagoofil - Metadata harvester
Sublist3r - Fast subdomains enumeration tool for penetration testers
XST - A small python script to check for Cross-Site Tracing
WAFW00F - A tools that allows one to identify and fingerprint Web Application Firewall (WAF) products protecting a website.
webvulnscan - automated web application vulnerability scanner
sn1per - Automated Pentest Recon Scanner
SCANNER-INURLBR - Advanced search in search engines, enables analysis provided to exploit GET / POST capturing emails & urls, with an internal custom validation junction for each target / url found.
CloudFail - Utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network
TestSSL - Testing TLS/SSL encryption anywhere on any port
F5 BIGIP Decoder - Detecting and decoding BIGIP cookies in bash
WAscan – Wascan is a Web Application Scanner that scans pages extracting links and forms, sending payloads and using attack scripts to look for error messages.
Skipfish – Prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probe

Advertised Attack Tools

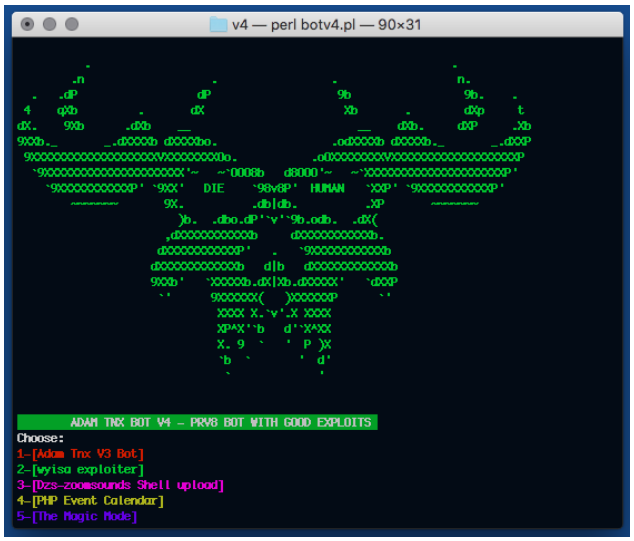

Figure 8: Adam Tnx Bot V4

Adam Tnx Bot v4 is a tool released on Github that Radware's ERT has observed OpIsrael hacktivist sharing on social platforms. This is a tool designed to abuse several content management systesms (CMS) including WordPress, Joomla, Drupal and Prestashop. This tools has the ability to check, dork, brute force and exploit targeted websites in mass. Adam Tnx Bot also has the ablitity to upload defacements to Zone H, an archive of defaced websites.

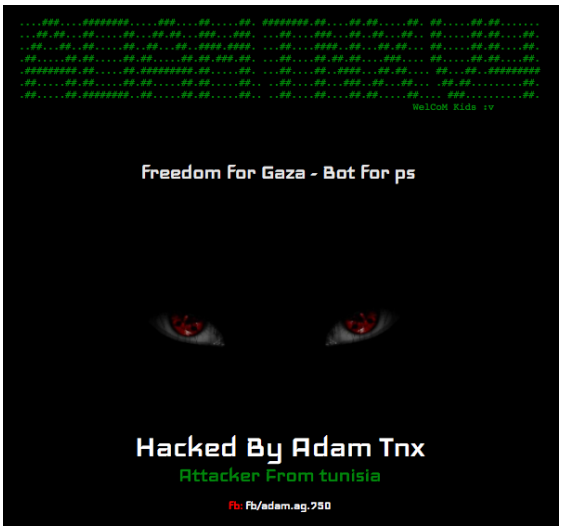

Figure 9: Deface HTML template in Adam Tnx Bot v4

Reasons for Concern

Radware's Emergency Response Team over the last several days has witnessed several SQL injections, data dumps and service outages. Criminal hackers have already begun listing private information about Israelis and attacking targeted websites. One of the main concerns around 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, including innocent citizens. Israelis can expect online harassment via SMS bombing or doxing. In past operations, hackers have changed the SSID of Israeli routers to display offensive content and spammed Israeli Facebook users.

Currently, OpIsrael is planning on targeting Israeli servers, including government and military as well as telecommunications, education, hospitals, financial services and home connections. It's expected that those that support Israel directly and indirectly could be targeted by SQL injections, cross-site scripting (XSS), data dumps and service outages caused by DoS attacks. It is expected that these attacks will continue through the rest of the operation, ending on April 14th.

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
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application 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** 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 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.