Abstract

With the stated goal of “erasing Israel from the internet” in protest against claimed crimes against the Palestinian people, Anonymous will launch its yearly operation against Israel. Named OpIsrael, it is a cyber-attack timed for April 7th by an array of hacktivist groups that join forces with the greater Anonymous collective (see Figure 1). For this year’s attack, hackers have provided tools and technical guidance for the execution of OpIsrael.

Figure 1: OpIsrael Announcement

In past years, Israel has seen moderate attacks launched against its networks and infrastructure. Organizations should take precautions and make sure they are prepared for OpIsrael2016. Since the previous ERT alert outlining OpIsrael, Radware’s Emergency Response Team has identified new hacktivist groups planning to partake in these cyber assaults and new attack vectors/tools that will be used. This alert enhances our initial findings and is updated to provide guidance on how targeted organizations can keep their networks and applications protected from these attacks.

Background

Ideological, political and religious differences are at the core of this operation. Since 2012, Anonymous has launched a yearly campaign in protest against the Israeli governments conduct in the Israeli-Palestinian conflict. Every year, OpIsrael calls for dozens of different hacktivist groups to “hack, deface, hijack, leak databases, admin takeover and DNS terminate” targets associated with Israel. Well known for its advanced technological capabilities, Israel poses a challenge for hackers. Those that attempt and overcome those challenges win prestige and recognition for their expertise inside their communities.

In previous years Israel and Israelis have seen modems hacked, credit card data breached government and personal information posted, Facebook accounts hijacked, websites defaced, emails leaked and a series of network crippling denial of service attacks. In previous weeks, groups like Redcult[i] and AnonGhost have targeted a number of government and corporate sites with denial of service attacks and database leaks (See Figure 2). The time leading up to the official launch in April will show a growing number of operations targeting Israel.

Figure 2: Attacker claims they have stolen personal information

Operational Information

Attackers

- AnonGhost
- RedCult
- Fallaga Team
- Anonymous
- NewWorldHackers
- Laskala Hackers

Video

- https://www.youtube.com/watch?v=fJM8Igf2fjo&feature=youtu.be

Telegram

- Telegram.me/OpIsrael

Hashtags

- #OpIsrael
- #OpIsrael2016
- #OpIsraHell2016
- #FreePalestine

Targets - See Appendix A

Attacks from OpIsrael 2015

In 2015, Israel witnessed a number of different cyber-attack tools and techniques used against its networks and infrastructure. Though the 2015 attacks were modest, hackers were still able to successfully launch several denial-of-service attacks resulting in various database leaks.

Tools & Techniques

DDoS

- **Anonymous External Attack** – generating a UDP Flood with payloads containing multiple zeros against port 80 by default. It can be mitigated by blocking UDP traffic to the targeted port.
- **DoSeR 2.0** - A traffic generator with scanning capabilities using multiple threads and sockets. Its attack vectors include, TCP, UDP, and HTTP floods.
- **LOIC Fallaga** – a unique variation of LOIC UDP/ TCP flood tool created by Fallaga hacker group.
- **Other DDoS tools** – AnonGhostDDoS, Jays Booter, FireFlood, SYN-FLOOD-DoS, njRAT, Turbinas, TorsHammer, THC-SSL, PyLoris

Web Intrusion

- **Dark D0rk3r** - was the most common web intrusion tool (Fuzzing, path traversal and SQLi capabilities). It allows fuzzing, path traversal and SQLi capabilities. http://packetstormsecurity.com/files/117403/Dark-D0rk3r-1.0.html
- Other application vulnerability exploits such as **Brute force, cross site scripting and SQL injections**

```
width="1">
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

Figure 3: Hackers also collected statistics to track successful attacks

Consequences of 2015 Attacks

- 3 hosting servers (hosting several small websites) were hacked
- Data dump of Israeli users' information and credentials – 99% of them are old dumps
- Attackers published credit card details – confirmed as old and inactive
- Government websites confirmed that hackers launched multiple SQL injection attempts against them – all were successfully blocked and failed.
- Israeli home routers hacked - http://pastebin.com/embed_js/84nfwx9U, http://pastebin.com/g8M1GPUJ

2016 Attack Vectors & Tools

Before describing new tools introduced for OpIsrael, the most common threat is a volumetric denial of service attack. Some stresser services today can generate groundbreaking amounts of traffic reaching few hundreds of Gbps.The service hiring price begins at 19.99$ for a 15Gbps attack.

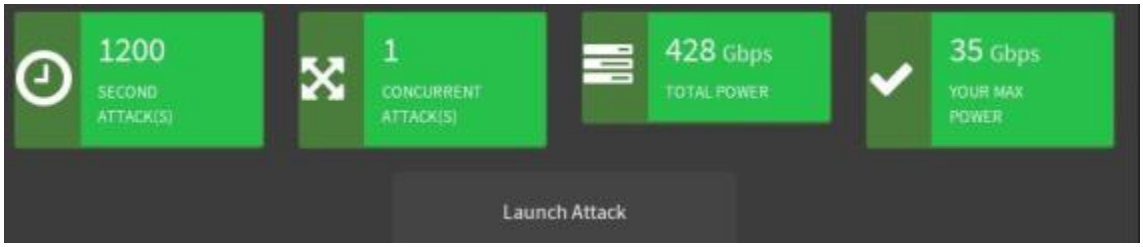

Figure 4: Example to an available stresser service for hire

Specifically, for OpIsrael - Hax Strokes of AnonGhost has also advertised the tool, An0nStr3ss. An0nStr3ss is an executable file that launches a command line based stresser. The An0nStr3ss tool offers seven different attack methods. These attack methods include UDP, RUDY, SSYN, ARME, RDoS, SlowLoris and AR-UDP. This tool is capable of generating a mass amount of traffic and provides the attacker with a number of different methods to choose from.

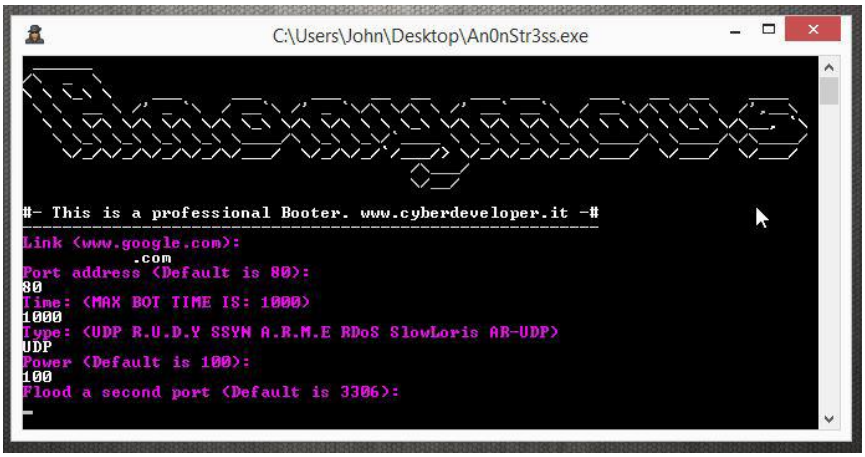

Figure 5: Tool – An0nStr3ss

HaxStroke from AnonGhost recently released a script for OpIsrael2016. SadAttack 2.0 is a python script that is nearly identical to the DoS tool, HTTP Unbearable Load King, also known as HULK. SadAttack 2.0 is a flood tool that is used to generate a mass amount of traffic that will utilize network or application resources, resulting in the degradation or loss of service for users. The attack bypasses caching engines and hits the server resources directly.

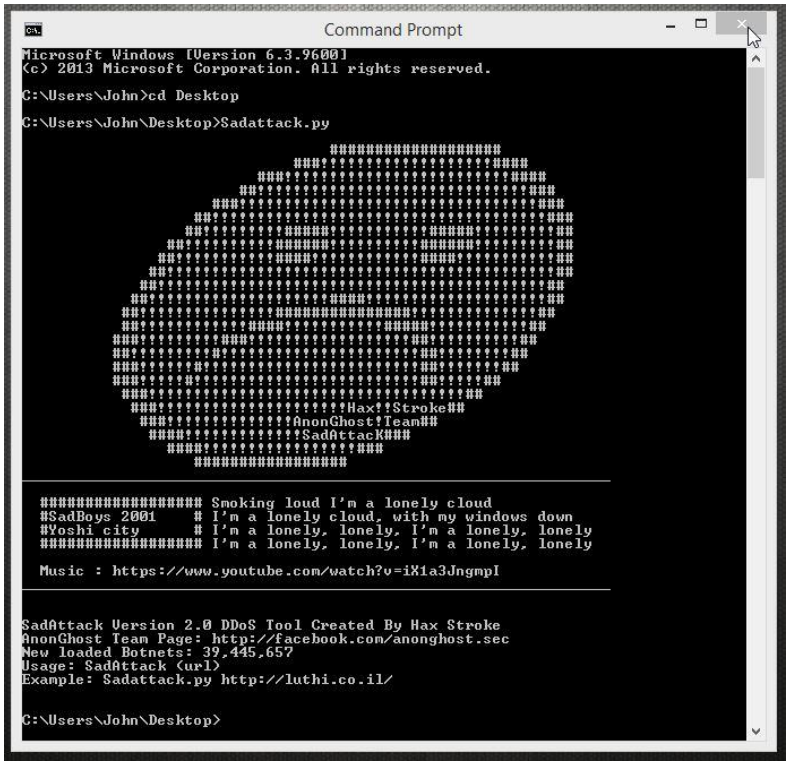

Figure 6: Tool – Sadattack 2.0

Another tool referenced for use in OpIsrael is SwitchBlade v4.0. This is a Layer 7 tool that is capable of producing 3 different attack types. The methods available in for this tool are slow headers, slow POST,

and SSL renegotiation (See Figure 5). You could also expect to see attackers using other tools such as TorsHammer, SlowLoris, PyLoris, Slow HTTP test, Mobile LOIC, and THC-SSL.

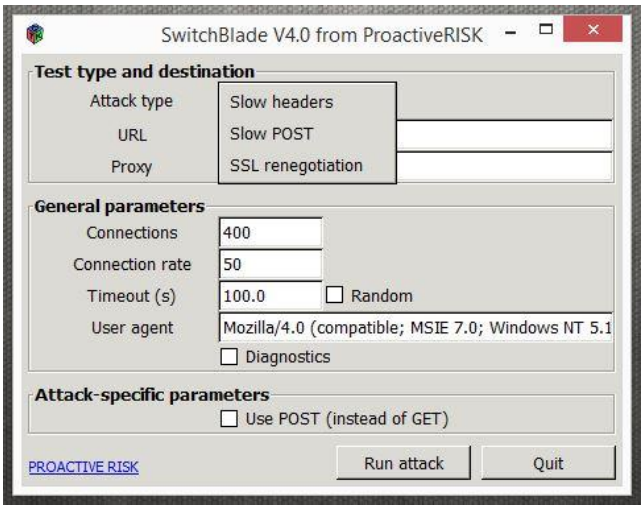

Figure 7: Tool - SwitchBlade

RouterhunterBR 2.0

This tool was designed to compromise home and network routers. It scans the ports (in particular 80 and 443) and identifies open ones in order to exploit the DNSChanger trojan vulnerability.

Figure 8: Tool – RouterhunterBR

Reflective DDoS

Based on the popular hackers 'Parrot' OS, this tool provides amplification capabilities to various attack vectors such as DNS, NTP, SNMP, and SSDP reflective attacks. The attackers send packets to the reflector servers with a source IP address set to their victim's IP therefore indirectly overwhelming the victim with the response packets.

Figure 9: Tool – Reflective DDoS

Current Targets

Attackers are currently organizing and preparing for the official launch of OpIsrael 2016. Radware has begun witnessing various activities from the attackers, including the publication of a number a target lists (see Appendix A).

Reasons for Concern

OpIsrael receives large amounts of attention for several reasons; one of them being the global media coverage surrounding the Israeli-Palestinian conflict. To date, Radware has witnessed several SQL injections, data dumps and service outages in the buildup to the April 7 launch. Currently, OpIsrael is planning on targeting the Israeli Government as well as the telecommunications, education and financial services industry.

How to Prepare

Political and ideological-driven attacks such as these can be difficult to avoid. Government agencies and organizations in Israel should proactively prepare their networks with an attack mitigation solution designed to detect, mitigate, and report today's most advanced threats as well as have an emergency response plan in place.

Organizations Under a Cyber Threat Should Consider

DDoS protection elements:

- A hybrid solution that combines on premise detection and mitigation with cloud-based protection for volumetric attacks. It provides quick detection, immediate mitigation and prevents internet pipe saturation.

- Solution must distinguish between legitimate and malicious traffic, protect the SLA and block the attack.
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.

Web application protection elements (from web intrusions, defacement and data leakage):

- IP-agnostic device fingerprinting – Having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time
- Automatic and real time generation of policies to protect from Zero-day, unknown attacks
- Shortest time from deployment to a full coverage of OWASP Top-10

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

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 DDoS Warriors. 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.

Appendix A: #Anonghost #OpIsrael2016 Target list

Ministries	Education institutes	Financial and Law
• Prime Minister's Office • Agriculture • Communication • Construction and Housing • Environment • Finance • Health • Industry, Trade and Labor • Justice • Social Affairs • Critical National Infrastructure • Tourism • Culture and Sports	http://www.lander.ac.il/ http://www.ariel.ac.il/ http://www.bgu.ac.il/ http://www.clb.ac.il/ http://www.jct.ac.il/ http://www.technion.ac.il/ http://www.telhai.ac.il/ http://www.weizmann.ac.il http://www.sapir.ac.il/ http://www.yvc.ac.il/ http://www.ruppin.ac.il/ http://www.schechter.ac.il/ http://www.mishpat.ac.il/ http://fulbright.org.il/ http://www.science.co.il/ http://mfa.gov.il https://overseas.huji.ac.il/ https://tau.ac.il/ http://www.ono.ac.il/ http://www1.biu.ac.il/ http://www.jamd.ac.il/ http://www.mla.ac.il/ http://www.hadassah.ac.il/ http://www.carmel.ac.il/	• The Custom and VAT Authority • Income Tax Commission • Institute of Certified Public Accountants • Israel Bar Association • Internship and Admissions • Treasury • The National Court • Secretariat • The International Association of Jewish Lawyers • The Pension Fund • The Publishing House • Jerusalem District Committee • Tel Aviv District Committee • Northern District Committee • Southern District Committee • Hadera Extension • Ashdod Extension
Banks	**ISPs**	
http://www.bankisrael.gov.il http://www.bankhapoalim.com/ https://www.discountbank.co.il/ http://www.leumi.co.il/ https://new.fibi-online.co.il https://www.mizrahi-tefahot.co.il	• Bezeq International • Netvision • Smile Communication • Internet Rimon	