Background

With the stated goal of "erasing Israel from the Internet," Anonymous will launch its yearly cyber operation against Israel on April 7, 2017. Named OpIsrael, it is a cyber-attack timed for April 7th and executed by hacktivist groups associated with the greater Anonymous collective. Every year, OpIsrael calls for the hacking, defacement, leaking of databases, hijacking of servers, and launching of DDoS attacks against targets associated with Israel. This year, the perpetrators have begun attempting to hack Israeli websites and steal data, aiming to reach the peak of the attacks and share all the dumps on April 7th. Hacking group RedCult has already begun launching Denial of Service attacks[i] against a number of government organizations ahead of April 7th to drum up attention both for the media and to recruit potential attackers. Radware's Emergency Response Team has analyzed the attack vectors and techniques that will be used for OpIsrael. This alert provides further information about this operation along with information about how to stay protected.

"Greetings world we are AnonGhost! We are always here to punish you, because we are the voice of Palestine and we will not remain silent." -AnonGhost 2017

Figure 1: Quote from AnonGhost hackers pertaining to OpIsrael 2017

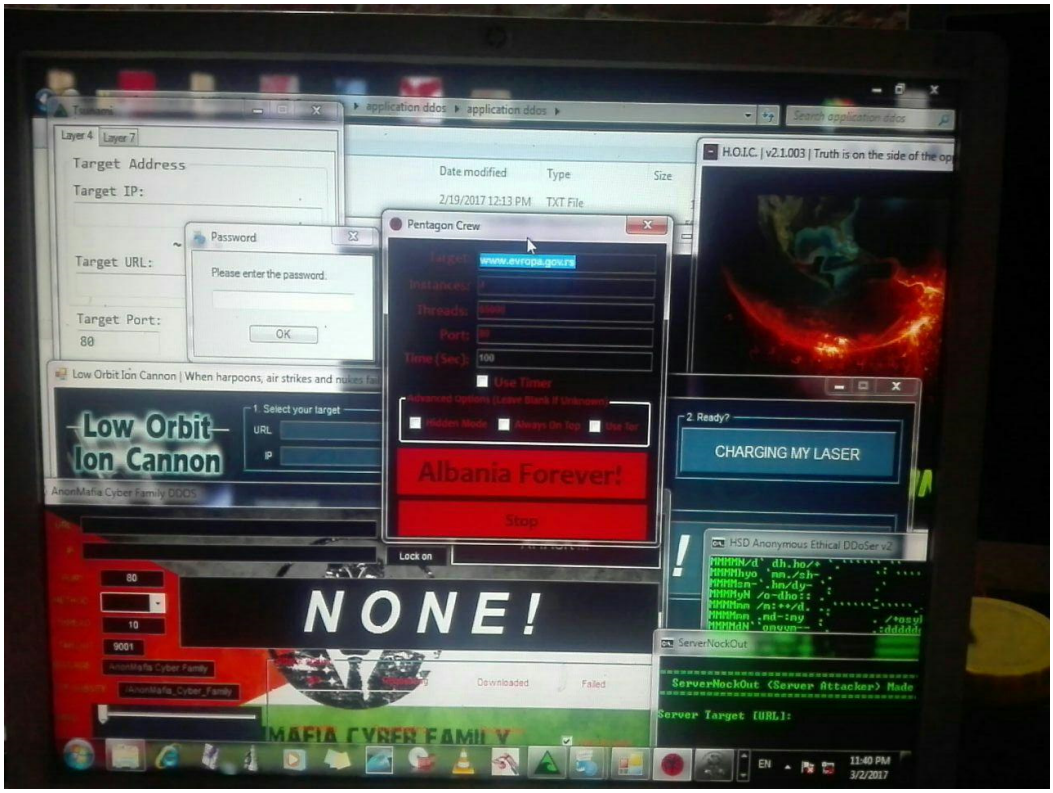

Figure 2: A variety of Denial-of-Service attack tools including LOIC, HOIC and others

Previous Operations:

In previous years, Israel has seen moderate attacks launched against its networks and infrastructure, resulting in defacement of unsecured websites of small businesses. Well known for its advanced technical capabilities, Israel poses a challenge for hackers. Those that attempt and overcome those challenges win prestige and recognition for their expertise inside their communities. Organizations should take precautions and make sure they are prepared for OpIsrael 2017.

In addition to attacks against Israel, skilled Israeli programmers launch counterattacks in in an attempt to expose OpIsrael attackers. Groups like the Israeli Elite Force[ii] have been known to take down opposing servers and leak information on Twitter.

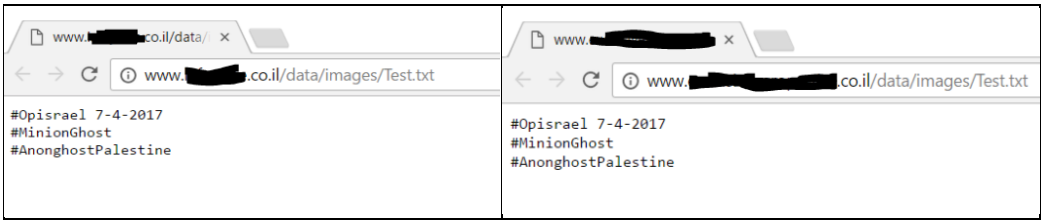

Figure 3: Israeli websites compromised during the reconnaissance phase

Communication Channels:

The majority of the operation's command and control is ran via social networks - Facebook Event pages as well as Twitter and Telegram.

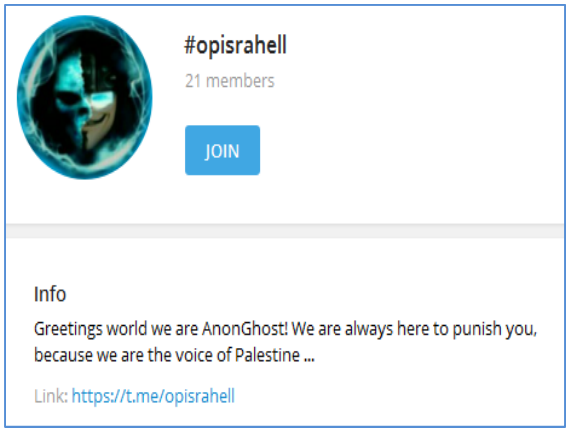

Figure 4: OpIsrahell Telegram chat group

Telegram Channels for AnonGhost

@OpIsrael
@AnonGhostOfficial
@OpIsrahell

Facebook Event Page

https://www.facebook.com/events/177689139398892/ (Minion Ghost)
https://www.facebook.com/events/404912819901140/ (OpIsrael)
https://www.facebook.com/events/1106408086118632/

Videos

- https://youtu.be/6-RVu0bUI9g (RedCult)

Figure 5: YouTube video tutorial

Hashtags

- #OpIsrael
- #OpIsrahell
- #OpIsrael2017

Attackers

- Anonymous
- AnonGhost
- RedCult
- Mauritania Attacker
- @Scode404

Targets

Here is a partial list of Israeli government agencies, top enterprises and premier media outlets[iii] [iv]

- www.mof.gov.il
- www.idf.gov.il
- www.idf.il
- www.isoc.org.il
- www.gov.il
- www.investinisrael.gov.il
- www.mod.gov.il
- www.moag.gov.il
- www.itrade.gov.il
- www.archive.gov.il
- www.mfa.gov.il
- www.embassies.gov.il
- www.asoc.mot.gov.il
- www.iaa.gov.il
- www.police.gov.il
- www.mossad.gov.il
- www.hadshon.edu.gov.il
- www.health.gov.il
- www.ashra.gov.il
- www.boi.org.il
- www.idbny.com
- www.bankofisrael.com
- www.israelbonds.com
- www.israel.deposits.org
- www.discountbank.co.il
- www.fibi.co.il
- www.hanner.co.il
- www.bankaccountsco.com
- www.bdicode.co.il
- www.israeldefense.co.il
- www.justice.gov.il
- www.iibr.gov.il
- www.moia.gov.il
- www.Knesset.gov.il
- www.cert.gov.il
- www.adi.gov.il
- www.moc.gov.il
- www.pmo.gov.il
- www.Google.co.il
- www.Walla.co.il
- www.ynet.co.il
- www.info.org.il
- www.xplace.co.il
- www.jr.co.il
- www.sport5.co.il
- www.bgu.ac.il
- www.mako.co.il
- www.Carlton.co.il
- www.iandm.co.il
- www.hsbc.co.il
- www.idfblog.com
- www.jewishcirtuallibrary.org
- www.breakingisraelnews.com
- www.donate.fidf.org
- www.mahal-idf-volunteers.com
- www.loveisrael.org
- www.globes.co.il
- www.goisrael.com
- www.iris.org
- www.unionbank.co.il

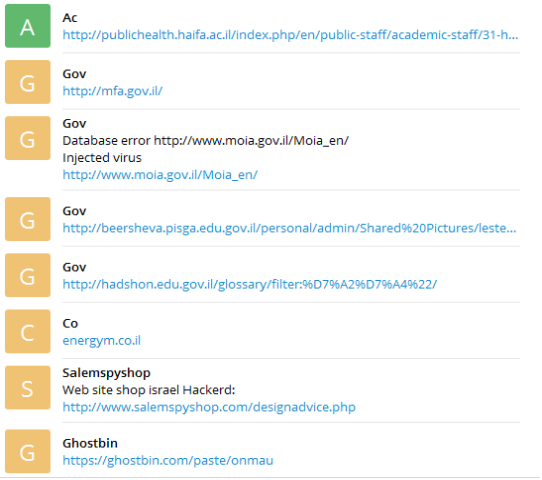

Figure 6: Partial target list that is spread via Telegram chat

#opisrahell
http://pastebin.com/x0pAEvp9

Figure 7: Link to the full target list

Fakes

OpIsrael is also full of opportunists looking to gain fame based on previous hacks or by simply fooling the media. In recent years, Radware has monitored a number of dumps by OpIsrael and has concluded that a majority of the dumps are reposts from earlier operations, while others where simply bogus (for instance – random credit card numbers that do not exist). This year, a hacker named Flyhack has been posting alleged hacks on Pastebin. This hacked information is actually from 2015 and Flyhack reposted it for credit.

- http://pastebin.com/K7HXLNsZ (Flyhack)
- http://pastebin.com/GtfTAEv4 (Old Post)

- http://pastebin.com/4z8M8LJV (Flyhack)
- http://pastebin.com/r43SF9RY (Old Post)

- http://pastebin.com/7wjVazhv (Flyhack)
- http://pastebin.com/Ci7SMUkA (Old Post)

Tools and Techniques

Figure 8: A botnet-based DDoS service

Anonymization

In the Telegram channel, @OpIsrahell a member has posted an .apk file called AnonGhost VPN. Attackers for OpIsrael 2017 will be using a combination of VPNs and Tor to mask their attacks.

Figure 9: AnonOps claim to have 13,000 DNS servers vulnerable for a DDoS attack

Toolkit

Currently, the most common toolkit that has been distributed is from 2012 and lacks the power of the new, recently introduced DDoS tools. Yet, there is no reason to believe this is the only attack vector to be used.

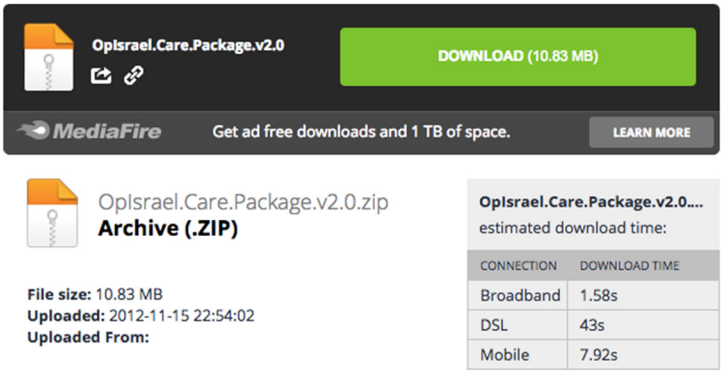

Figure 10: 2012 toolkit

What's Expected Next?

Attackers are currently organizing and preparing for the official launch of OpIsrael 2017. To date, Radware has witnessed several SQL injections, data dumps and service outages in the buildup to the April 7 launch date. Radware is monitoring various activities from the attackers, including the publication of target lists, and will follow the events as they evolve.

Effective DDoS Protection Essentials:

- **Hybrid DDoS Protection** - (on-premise + cloud) – for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan** - that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application 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

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

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.

---

[i] http://pastebin.com/rBiMTwsy
[ii] http://sma-norge.no/wp-content/uploads/pdf/2014/Hackers%20Information%20By%20Buddhax%20@%20iEF.pdf
[iii] Telegram channel @OpIsrahell
[iv] https://pastebin.com/x0pAEvp9