Operation Electric Powder – Who is targeting Israel Electric Company?

clearskysec.com/iec/

Attackers have been trying to breach IEC (Israel Electric Company) in a year-long campaign.

From April 2016 until at least February 2017, attackers have been spreading malware via fake Facebook profiles and pages, breached websites, self-hosted and cloud based websites. Various artifacts indicate that the main target of this campaign is IEC – Israel Electric Company. These include domains, file names, Java package names, and Facebook activity. We dubbed this campaign "**Operation Electric Powder**".

Israel Electric Company (also known as Israel Electric Corporation) "is the largest supplier of electrical power in Israel. The IEC builds, maintains, and operates power generation stations, sub-stations, as well as transmission and distribution networks. The company is the sole integrated electric utility in the State of Israel. It installed generating capacity represents about 75% of the total electricity production capacity in the country."

It is notable that the operational level and the technological sophistication of the attackers are not high. Also, they are having hard time preparing decoy documents and websites in Hebrew and English. Therefore, in most cases a vigilant target should be able to notice the attack and avoid infection. We do not have indication that the attacks succeeded in infecting IEC related computers or stealing information.

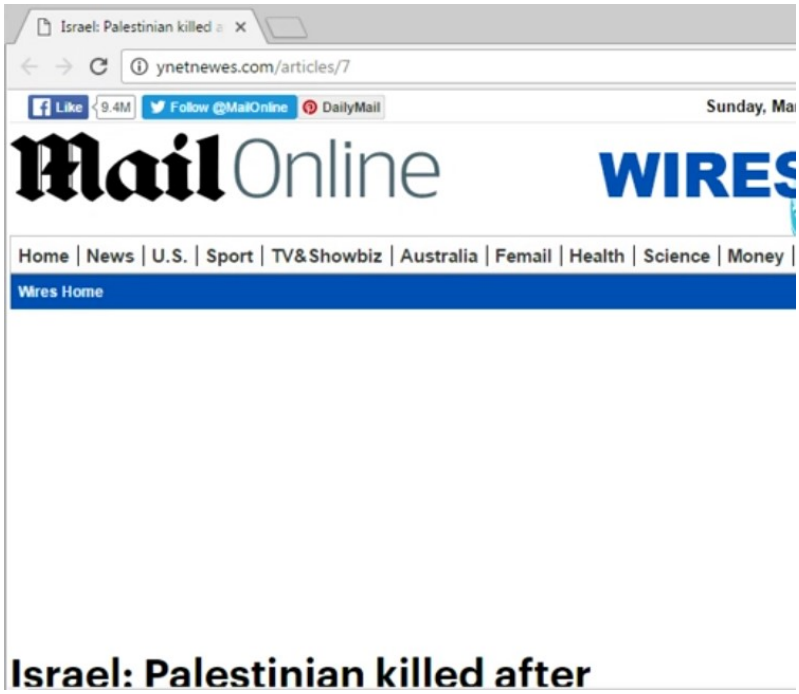
Currently we do not know who is behind Operation Electric Powder or what its objectives are. See further discussion in the Attribution section.

Impersonating Israeli news site

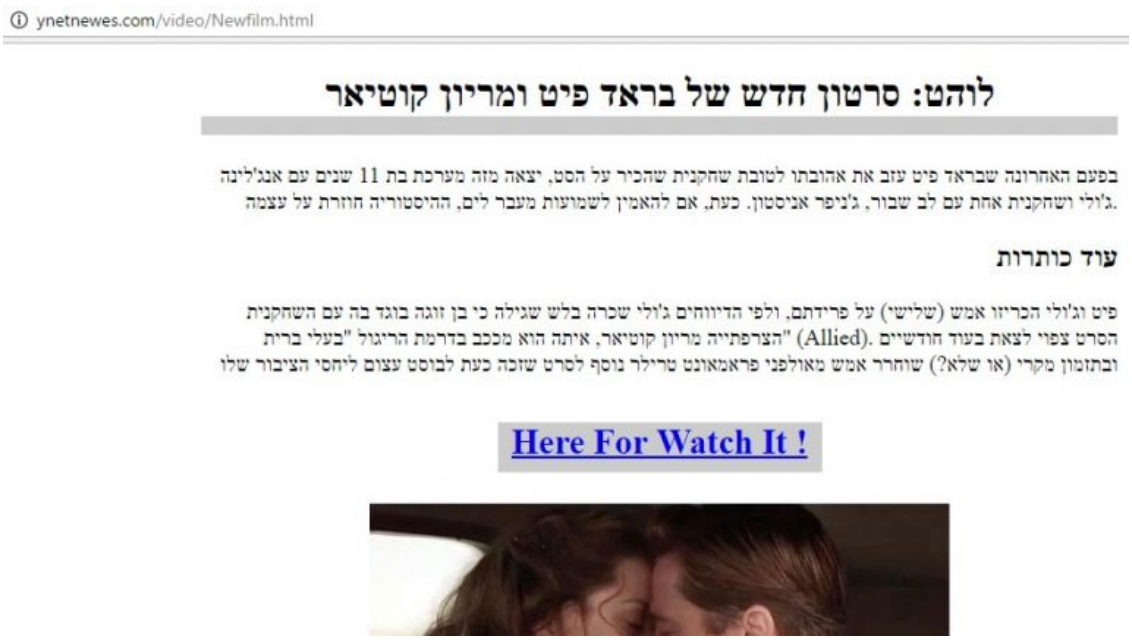
The attackers registered and used in multiple attacks the domain *ynetnew**e**s[.]com* (note the extra e). This domain impersonates ynetnews.com, the English version of ynet.co.il – one of Israel's most popular news sites.

Certain pages within the domain would load the legitimate Ynet website:

Others, which are opened as decoy during malware infection, had copied content from a different news site:



The URL *ynetnewes[.]com/video/Newfilm.html* contained an article about Brad Pitt and Marion Cotillard copied from another site. At the bottom was a link saying “Here For Watch It !”:



The link pointed to goo[.]gl/zxhJxu (Google's URL shortening service). According to the statistics page, it had been created on September 25, 2016 and have been clicked only 11 times. When clicked, it would redirect to *iecr[.]co/info/index_info.php* .

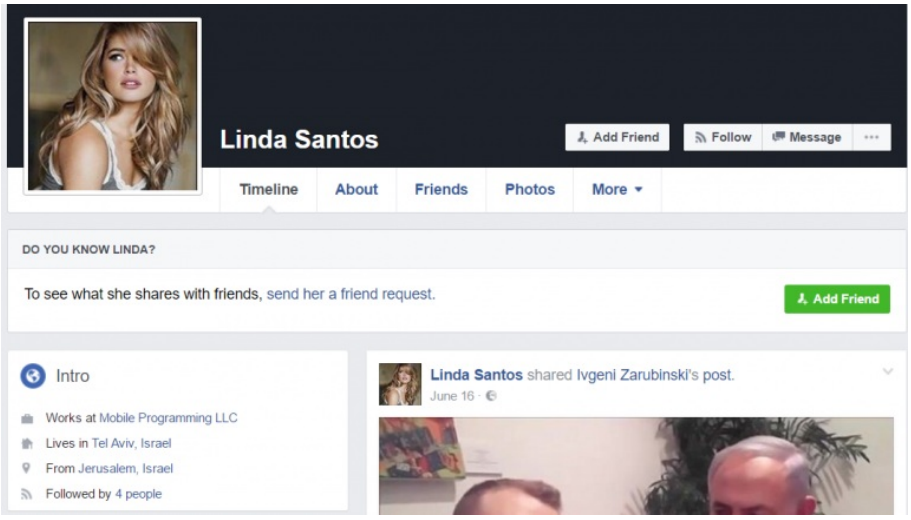
We do not know what was the content in the final URL. We estimate that it served malware. The domain iecr[.]co was used as a command and control server for other malware in this campaign.

Another URL, *http://ynetnewes[.]com/resources/assets/downloads/svchost.exe*

hosted a malware file called program_stream_film_for_watch.exe. (d020b08f5a6aef1f1072133d11f919f8)

Fake Facebook profile – Linda Santos

One of the above mentioned malicious URLs was spread via comments by a fake Facebook profile – Linda Santos (no longer available):



In September 2016, the fake profile commented to posts by Israel Electric Company:

Israel Electric Corporation חברת החשמל לישראל
50 mins ·

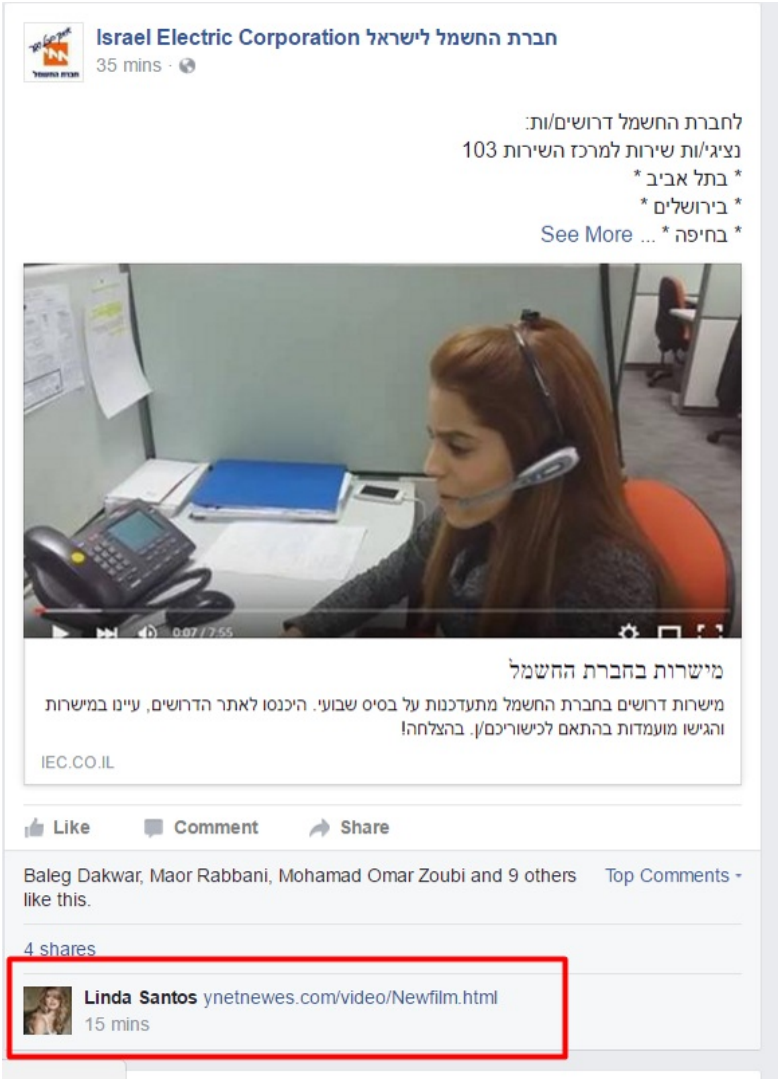
גם באזור טבריה נמשכת ההיערכות לחורף:
כשברקע נוף קסום לכנרת, היום בוצעו עבודות תשתית בקו מתח גבוה בעיר. העבודה בוצעה במתח חי מבלי להפסיק את אספקת החשמל ללקוחות האזור.
את העבודה העבודה בוצעה בשיתוף פעולה בין קבוצות הרשת של מחוז הצפון, השגחת אזור טבריה, מחלקת קשר ואלקטרוניקה צפון ובסיוע של מחלקות התחבורה וציוד מכני נייד (צמ"ן).
Atara Tal Orna Vagman הרצל פרידמן מחזקים את עובדי חברת חשמל שבשטחעיריית טבריה הדף הרשמי Tiberias, Israel

Like Comment

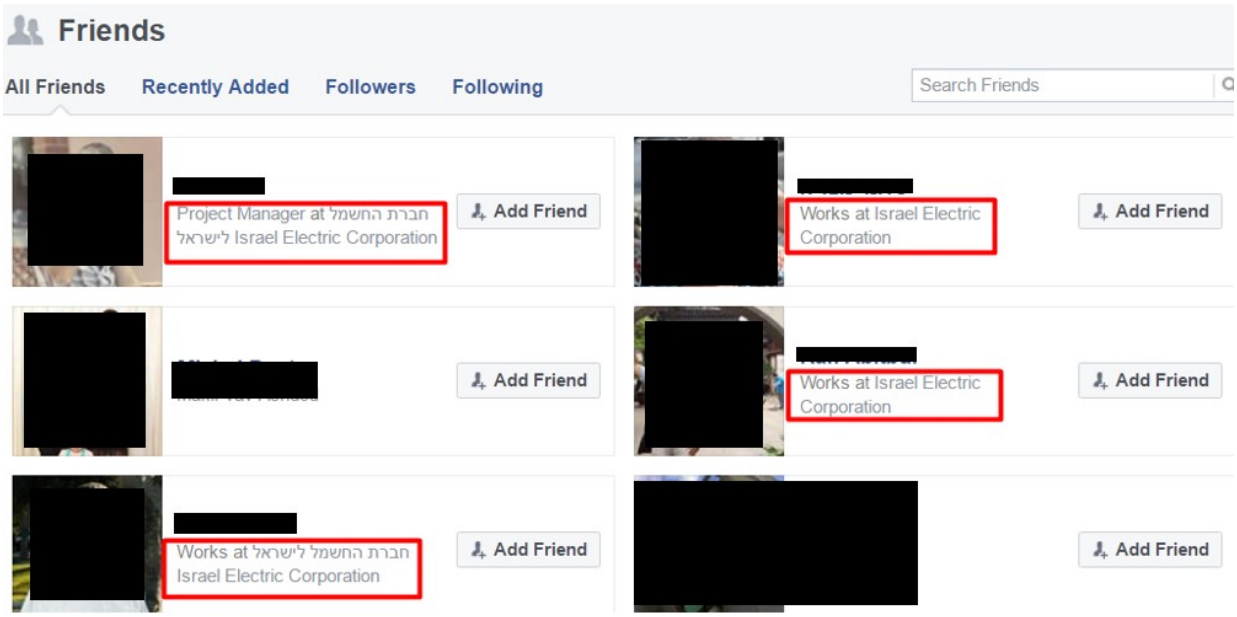
Moti Baikin, Sufyan Adeas, Hosam Gbareen and 11 others like this. Top Comments

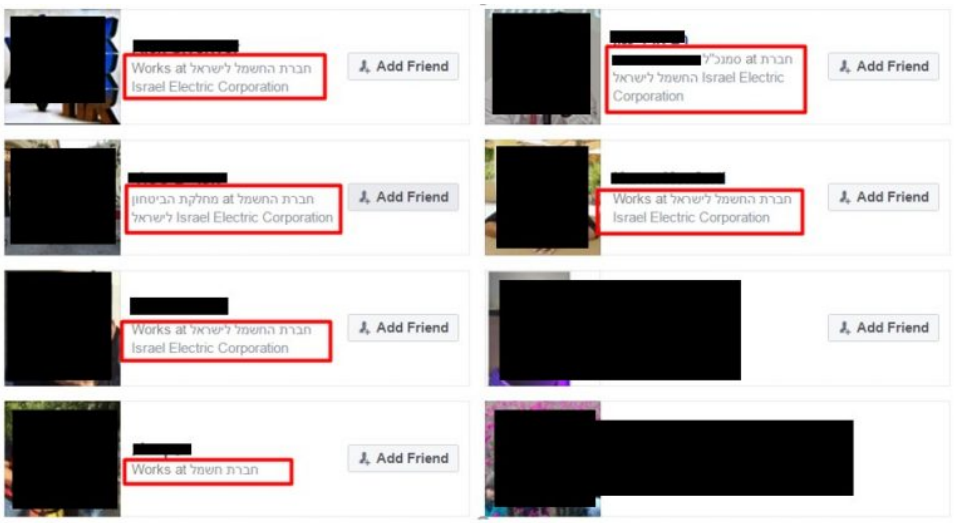
1 share

Linda Santos ynetnewes.com/video/Newfilm.html
16 mins



The profile had dozens of friends, almost all were IEC employees:





The fake profile was following only three pages, one of which was the IEC official page:

Pokemon Go Facebook page

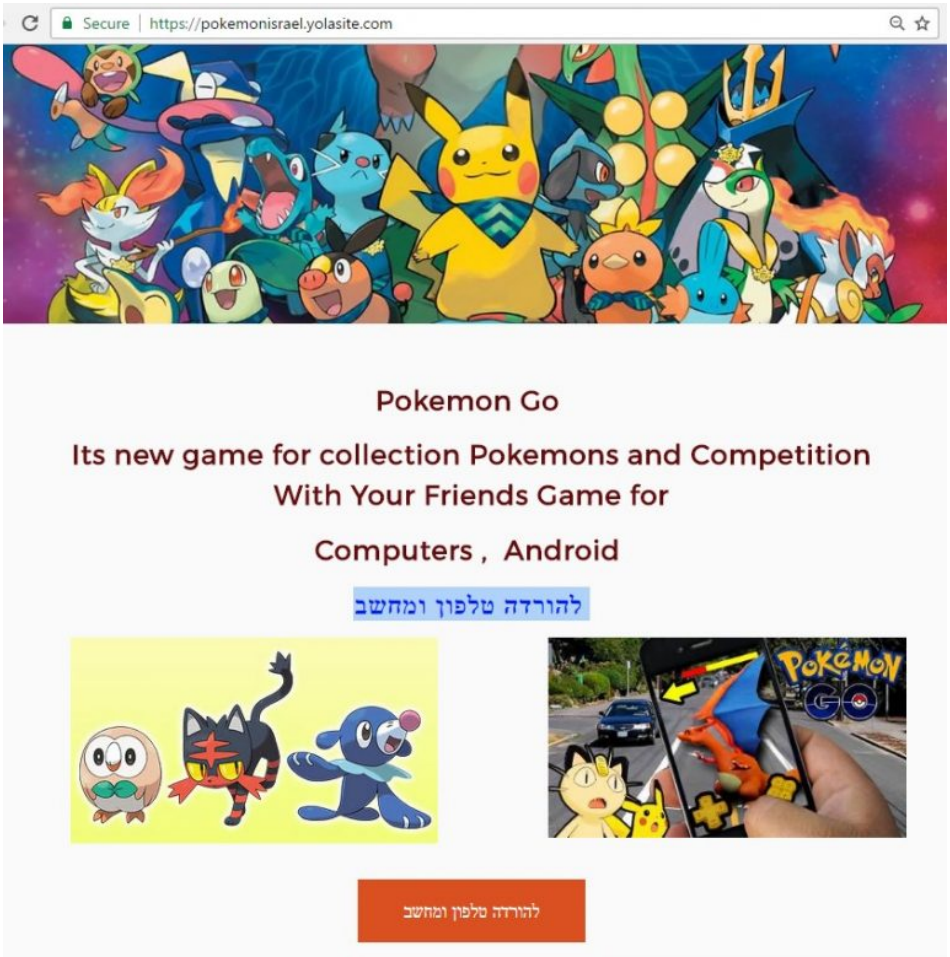
In July 2016, when mobile game “Pokemon Go” was at the peak of its popularity, the attackers created a Facebook page impersonating the official Pokemon Go page:

The page, which is no longer available, had about one hundred followers – most were Arab Israelis and some were Jewish Israelis.

Only one post was published, with text in English and Hebrew. Grammatical mistakes indicate the attackers are not native to both languages:

The post linked to a malicious website hosted in yolasite.com (which is a legitimate website building and hosting platform):

pokemonisrael.yolasite[.]com



The button – "להורדה טלפון ומחשב" (literal translation – "To download phone and computer") linked to a zip file in another website:

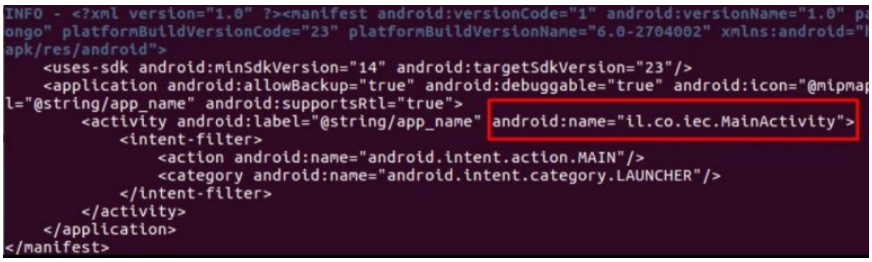
http://iec-co-il[.]com/iec/electricity/Pokemon-PC.zip

Note that the domain being impersonated is that of Israel Electric Company's website (iec.co.il).

Pokemon-PC.zip (40303cd6abe7004659ca3447767e4eb7) contained Pokemon-PC.exe (e45119a72677ed15ee0f04ef936a9803), which at run time drops monitar.exe (d3e0b129bad263e6c0dcb1a9da55978b):

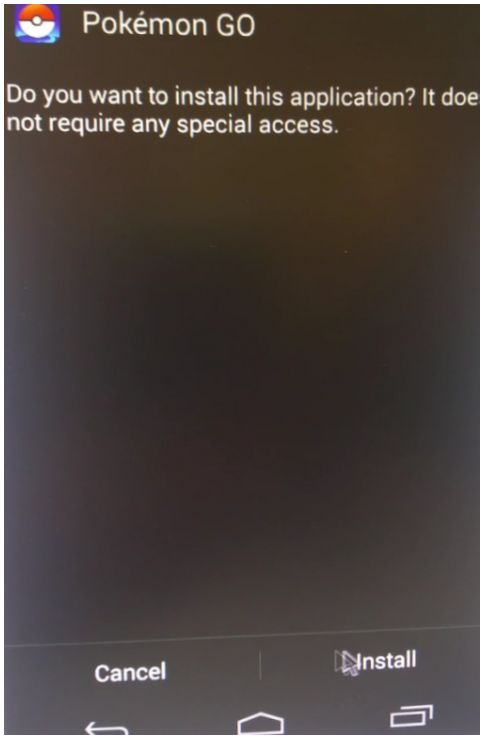
Android phone malware

The attackers also distributed a malicious app for Android devices – pokemon.apk (3137448e0cb7ad83c433a27b6dbfb090). This malware also had characteristics that impersonate IEC, such as the package name:



The application is a dropper that extracts and installs a spyware. The dropper does not ask for any permission during installation:

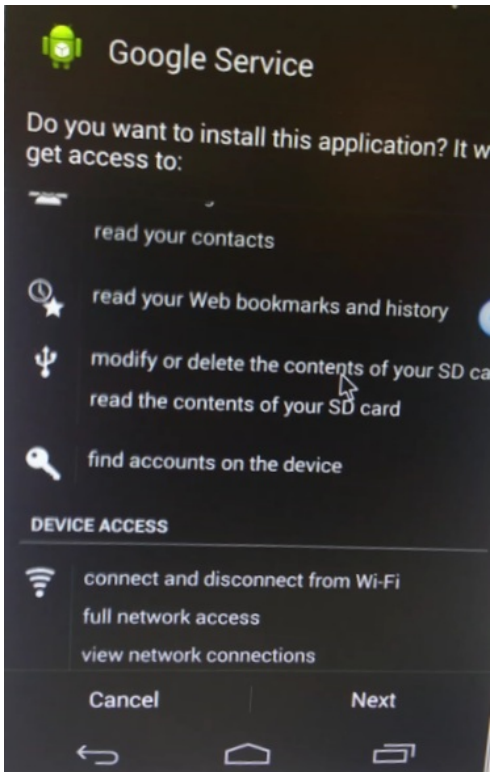
However, when the spyware is installed, it asks for multiple sensitive permissions:

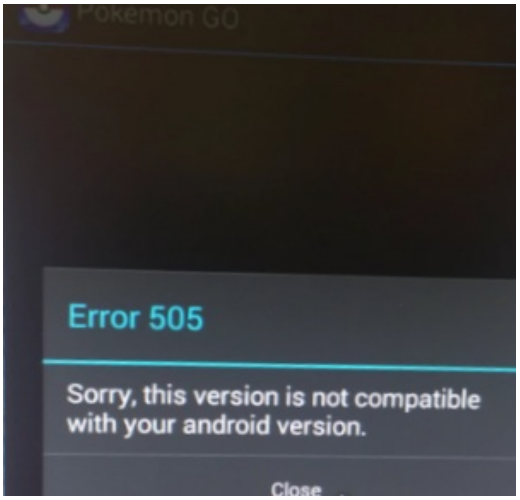


The victim ends up with two applications installed on their device. The Dropper, pretending to be a Pokemon Go app, adds an icon to the phone dashboard. However, it does not have any functionality, and when clicked, this error message is displayed:

Error 505
Sorry, this version is not compatible with your android version.

The dropper does not really check what android version is installed:






```
private void m2d()
{
  try
  {
    AlertDialog.Builder localBuilder = new AlertDialog.Builder(this);
    localBuilder.setTitle("Error 505");
    localBuilder.setMessage("Sorry, this version is not compatible with your android version.");
    localBuilder.setCancelable(false);
    localBuilder.setNegativeButton("Close", new DialogInterface.OnClickListener()
    {
      public void onClick(DialogInterface paramAnonymousDialogInterface, int paramAnonymousInt)
      {
        MainActivity.this.finish();
      }
    });
    localBuilder.show();
```

The message is intended to make the victim believe that the Pokemon game does not work because of compatibility issues.

The victim is likely to uninstall the application at this point. However, because a second application was installed, the phone would stay infected unless it is uninstalled as well.

Websites for Malware distribution

Malware was also hosted in legitimate breached Israeli websites, such as this educational website:

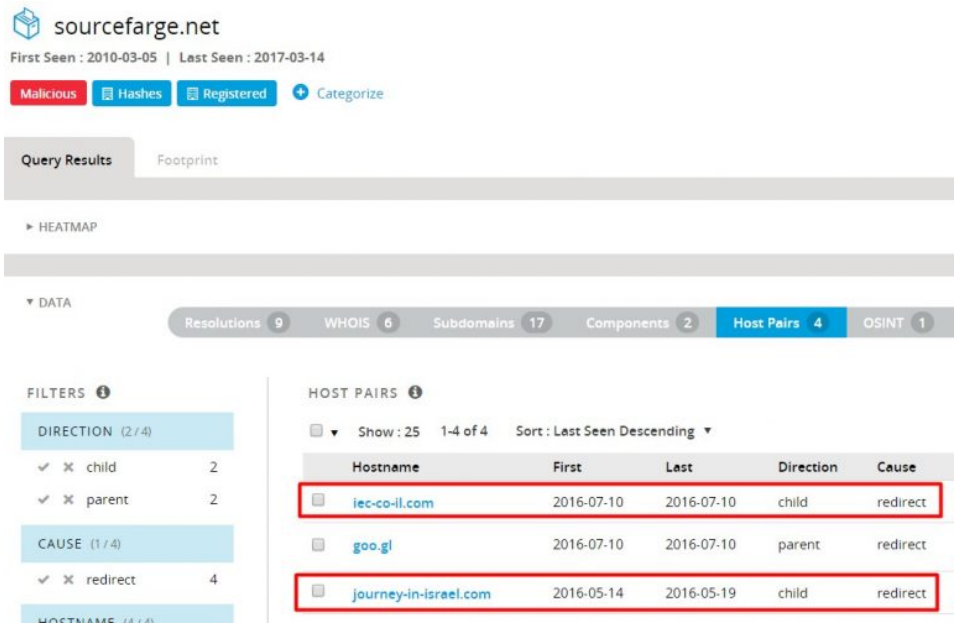
http://www.bagrut3.org[.]il/upload/edu_shlishit/passwordlist.exe (defc340825cf56f18b5ba688e6695e68)

and a small law firm's website:

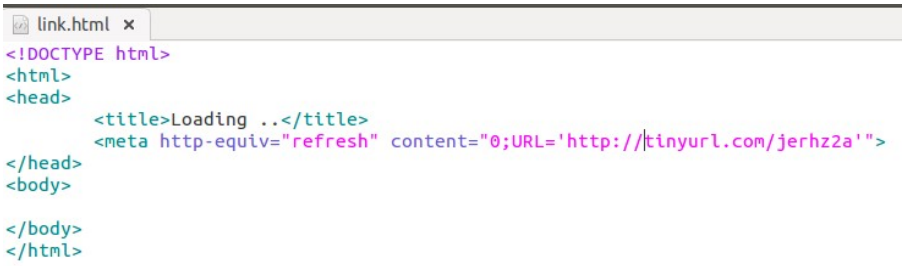
http://sheinin[.]co.il/MyPhoto.zip (650fcd25a917b37485c48616f6e17712)

In journey-in-israel[.]com, the attackers inserted an exploit code for CVE-2014-6332 – a Windows code execution vulnerability. The exploit was copied from an online source, likely from here, as the code included the same comments. The website also hosted this malware: afd5288d9aeb0c3ef7b37becb7ed4d5c.

In other cases, the attackers registered and built malicious websites: users-management[.]com and *sourcef**a**rge[.]net* (similar to legitimate software website sourceforge.net*). The latter was redirecting to journey-in-israel[.]com* and *iec-co-il[.]com* in May and July 2016, according to PassiveTotal:



Sample 24befa319fd96dea587f82eb945f5d2a, potentially only a test file, is a self-extracting archive (SFX) that contains two files: a legitimate Putty installation and *link.html:*

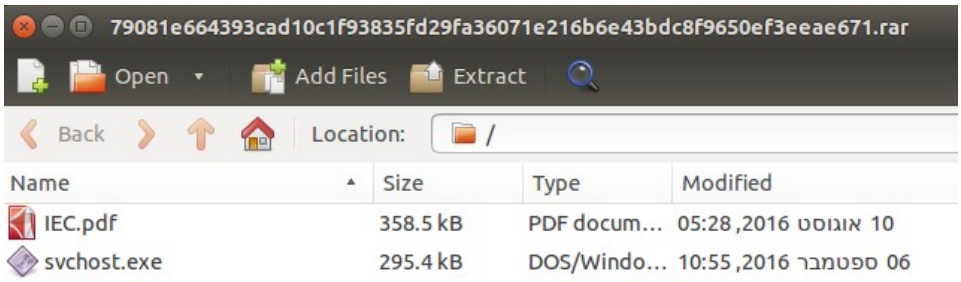


When run, while putty is installed, the html file is opened in a browser and redirects to *http://tinyurl[.]com/jerhz2a* and then to *http://users-management[.]com/info/index_info.php?id=9775*. The last page 302 redirects to the website of an Israeli office supply company Mafil:

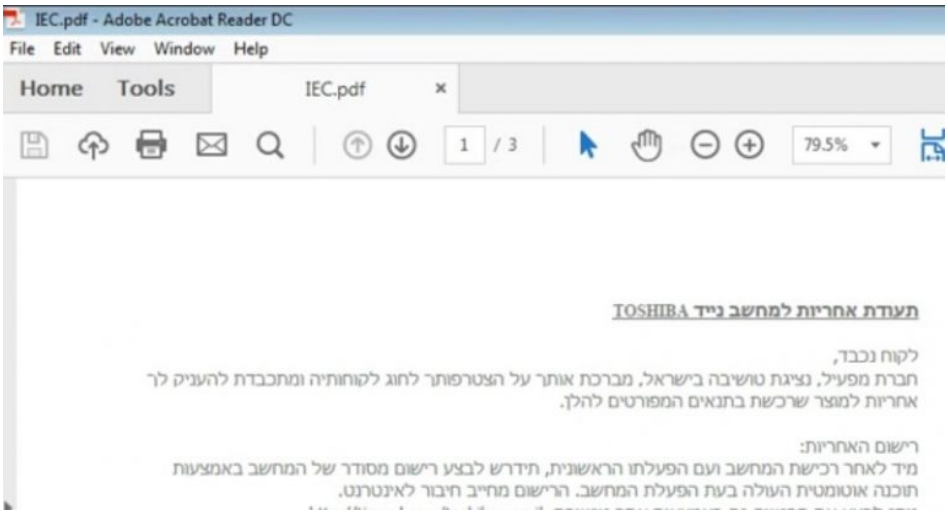
```
GET /info/index_info.php?id=9775 HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/g
application/vnd.ms-excel, application/vnd.ms-powerpoint,
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4
Accept-Encoding: gzip, deflate
Host: users-management.com
Connection: Keep-Alive

HTTP/1.1 302 Moved Temporarily
Date: Thu, 15 Sep 2016 23:02:53 GMT
Server: Apache
X-Powered-By: PHP/5.5.33
Location: http://mafil.co.il/
Content-Length: 0
Keep-Alive: timeout=3, max=120
Connection: Keep-Alive
Content-Type: text/html
```

Sample f6d5b8d58079c5a008f7629bdd77ba7f , also a self-extracting archive, contained a decoy PDF document and a backdoor:



The PDF, named IEC.pdf, is a warranty document taken from Mafil's public website. It is displayed to the victim while the malware (6aeb71d05a2f9b7c52ec06d65d838e82) is infecting its computer:



Windows Malware

The attackers developed three malware types for Windows based computers:

- **Dropper** – self-extracting archives that extract and run the backdoor, sometimes while opening a decoy PDF document or website.
  (For example: 6fa869f17b703a1282b8f386d0d87bd4)
- **Trojan backdoor / downloader –** malware that collects information about the system and can download and execute other files. (909125d1de7ac584c15f81a34262846f)
  Some samples had two hardcoded command and control servers: iecrs[.]co and iecr[.]co (note once again the use of IEC in the domain name).
- **Keylogger / screen grabber** – records keystrokes and takes screenshots. The malware file is compiled Python code. (d3e0b129bad263e6c0dcb1a9da55978b)

An analysis of the malware and other parts of the campaign was published by Mcafee in on November 11, 2016.

The latest known sample in this campaign (7ceac3389a5c97a3008aae9a270c706a) has compilation timestamp of February 12, 2017. It is dropped when "pdf file products israel electric.exe" (c13c566b079258bf0782d9fb64612529) is executed.

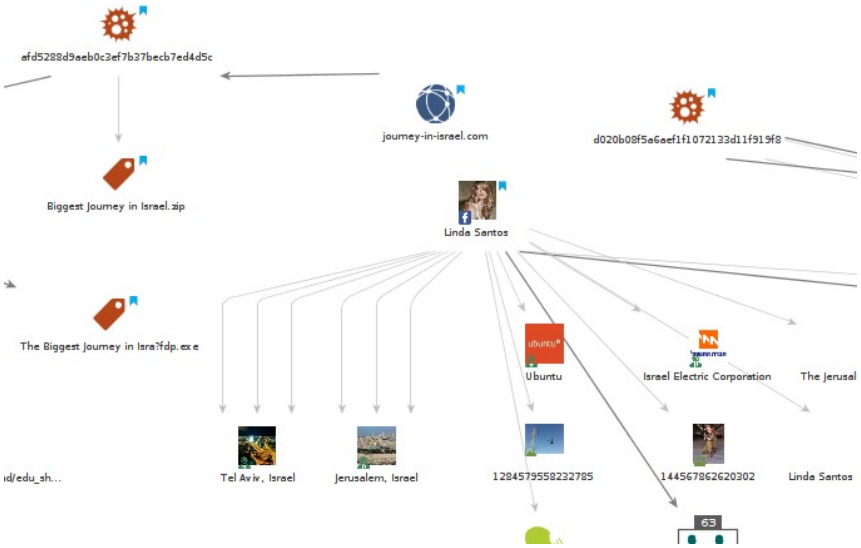
Attribution

In a report that covers other parts of the campaign, Mcafee attribute it to Gaza Cybergang (AKA Gaza Hacker Team AKA Molerats). However, the report does not present strong evidence to support this conclusion.

While initially we thought the same, currently we cannot relate Operation Electric Powder to any known group. Moreover, besides Mohamad potentially being the name of the malware developer (based on PDB string found in multiple
samples: C:\Users**Mohammed.MU**\Desktop\AM\programming\C\tsDownloader\Release\tsDownloader.pdb
), we do not have evidence that the attackers are Arabs.

Indicators of compromise

- Indicators file: Operation-Electric-Powder-indicators.csv (also available on PassiveTotal).
  Notably, all but one of the IP addresses in use by the attackers belong to German IT services provider "Accelerated IT Services GmbH" (AS31400):
  84.200.32.211
  84.200.2.76
  84.200.17.123
  84.200.68.97
  82.211.30.212
  82.211.30.186
  82.211.30.192
- Florian Roth shared a Yara rule to detect the downloader: Operation-Electric-Powder-yara.txt
- The graph below depicts the campaign infrastructure (click the image to see the full graph):



- Live samples can be downloaded from the following link: https://ln.sync[.]com/dl/30e722bf0#f72zgiwk-zxcp3e9t-fa9jyakr-zpbf5hgg (Please email info@clearskysec.com to get the password.)

Acknowledgments

This research was facilitated by PassiveTotal for threat infrastructure analysis, and by MalNet for malware research.