

Introduction

During the 2014 Israel–Gaza conflict, dubbed by Israel as “operation protective edge”, a raise in cyber-attacks against Israeli targets was reported. In this report we analyze one case of an operation protective edge themed spear phishing attack. That email contained a malicious excel file, which once opened and its VBA code executed, would infect the victim’s computer.

As for the publication of this report, the file is recognized as malicious by only one antivirus engine.

Based on our analysis, we believe the threat actor behind this malware is a high level professional.

Gholee

Our investigation of the Gholee malware started following a detection of a suspicious file that was sent in an email to an undisclosed recipient. The file name was ‘**Operation Protective Edge.xlsb**’ (MD5: d0c3f4c9896d41a7c42737134ffb4c2e).

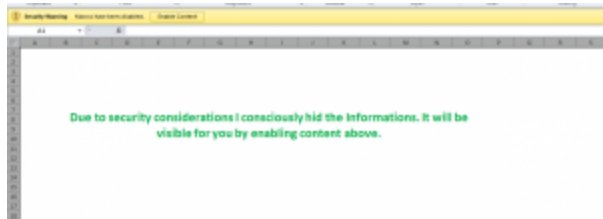
The file was uploaded to Virus Total the first time on 10 August 2014, from Israel. At that time it was not detected as malicious by any of the 52 tested antivirus engines. Nine days later, it was

uploaded again to Virus total, again from Israel. This time it was detected as malicious only by Kaspersky, as Trojan-Dropper.MSExcel.Agent.ce.

Infection

Upon opening the file a message is displayed, saying:

“Due to security considerations I consciously hid the Informations. It will be visible for you by enabling content above.”



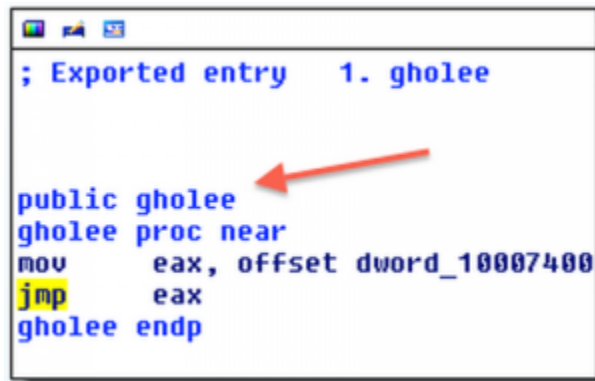
This is a social engineering tactic meant to lure the victim into enabling Macro content. If enabled, the message disappears, and the following information is presented to the victim (it is possible that the unreadable characters in the screenshot below are the result of an encoding error in our lab environment, and that the victim would see different, readable content).

Technical Analysis

Analysis of the Macro code reveals the following structure:

In order to avoid detection by protection measures such as computer antivirus and intrusion detection systems, ASCII

[4]



```
; Exported entry 1. gholee  
  
public gholee  
gholee proc near  
mov     eax, offset dword_10007400  
jmp     eax  
gholee endp
```

[5]

A quick Facebook search for that name and Iran discovered Gholee is a popular Iranian singer:



[6]

Communication

When run, the DLL file is communicating with a Kuwait based IP address: 83.170.33.60, owned by German company iABG Mbh, which provides satellite communication services.

IP Information for 83.170.33.60

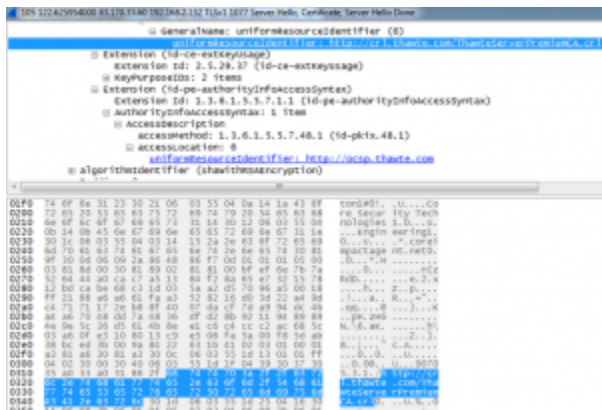
Quick Stats

IP Location	Kuwait (abg Mbh)
ASN	AS29259 DE-IABG-TELEPORT IABG mbh.DE (registered Jul 11, 2003)
Resolve Host	host-03-170-33-60.customer.teleport-iabg.de
Whois Server	whois.ripe.net
IP Address	83.170.33.60

[7]

The malware opens an SSL connection over port 443 using a digital certificate that expired in 2010. The certificate was issued for security company Core Security, the creators of the offensive suite Core Impact, for the address *.coreimpactagent.net.

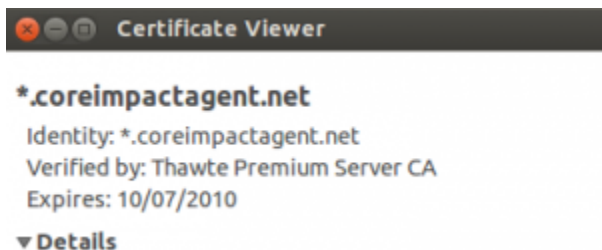
[8]



[9]

It was issued by Thawte certificate authority.

[10]



Subject Name

C (Country): US
ST (State): Massachusetts
L (Locality): Boston
O (Organization): Core Security Technologies
OU (Organizational Unit): Engineering
CN (Common Name): *.coreimpactagent.net

[11]

Certificate Fingerprint MD5: 9C 80 C2 47 40 6D 6C ED FC E0 08 AE
EF D9 98 90

Using a proxy and SSL stripping, the following communication pattern over HTTP can be seen:

GET /index.php?c=Ud7atknq&r=17117d HTTP/1.1

POST /index.php?c=Ud7atknq&r=1710b2 HTTP/1.1

Related incidents

Searching for specific strings from the malicious file, we found another file that we believe is related to this campaign. The file name is “svchost 67.exe” (MD5: 916be1b609ed3dc80e5039a1d8102e82) and it was uploaded to Virus Total[5] on 2 June 2014, more than two months earlier than “Operation Protective Edge.xlsb”. It was uploaded twice from Latvia – potentially to test the malware’s detection rate.

“svchost 67.exe” communicated with 83.170.33.37, which is on the same /26 netblock as the address “Operation Protective Edge.xlsb”

is commutating with.

Detection and prevention

- By using GPO to disable macro code from running, infection by this malware may be avoided. Alternatively, files containing macro code should be blocked at the email gateway or by an anti-spam solution.
- Logs and proxy servers should be checked for communication with the IP addresses with which the malware communicates:

83.170.33.60

83.170.33.37

- If you think you got infected, check in the system root folder for a file called NTUSER.DAT.{ $\$$ GUID}.dll . for example:

NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0b**c}.dll

- The following Yara rule may be used to detect the gholee malware:

```
rule gholee
```

```
meta:
```

```
author = "www.clearskysec.com"
```

```
date = "2014/08"
```

maltype = "Remote Access Trojan"

filetype = "dll"

strings:

\$a = "sandbox_avg10_vc9_SP1_2011"

\$b = "gholee"

condition:

all of them

1. <http://www.clearskysec.com/wp-content/uploads/2014/09/2.png>
2. <http://www.clearskysec.com/wp-content/uploads/2014/09/5.png>
3. <http://www.clearskysec.com/wp-content/uploads/2014/09/5.png>
4. <http://www.clearskysec.com/wp-content/uploads/2014/09/6.png>
5. <http://www.clearskysec.com/wp-content/uploads/2014/09/6.png>
6. <http://www.clearskysec.com/wp-content/uploads/2014/09/1.png>
7. <http://www.clearskysec.com/wp-content/uploads/2014/09/7.png>
8. <http://www.clearskysec.com/wp-content/uploads/2014/09/8.png>
9. <http://www.clearskysec.com/wp-content/uploads/2014/09/8.png>
10. <http://www.clearskysec.com/wp-content/uploads/2014/09/9.png>
11. <http://www.clearskysec.com/wp-content/uploads/2014/09/9.png>