# Gholee

## A “protective edge” themed spear phishing campaign

29 August 2014

# Introduction

During the 2014 Israel–Gaza conflict, dubbed by Israel as “operation protective edge”, a raise in cyber-attacks against Israeli targets was reported.[1] 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.

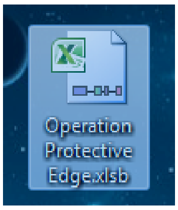
As for the publication of this report, the file is recognized as malicious by only one antivirus engine.

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

[1] http://www.i24news.tv/en/news/israel/diplomacy-defense/38443-140728-cyber-attacks-on-israel-increase-security-services-fight-back

# 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).

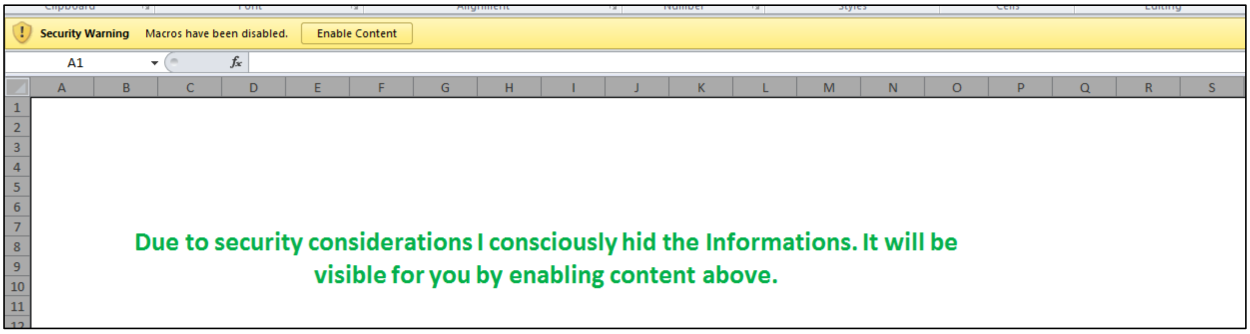


The file was uploaded[2] to Virus Total the first time on 10 August 2014, from Israel. At that time it was not detected as malicious by any of the 52 tested antivirus engines. Nine days later, it was uploaded again to Virus total, again from Israel. This time it was detected as malicious only by Kaspersky, as Trojan-Dropper.MSExcel.Agent.ce.

# Infection

Upon opening the file a message is displayed, saying:

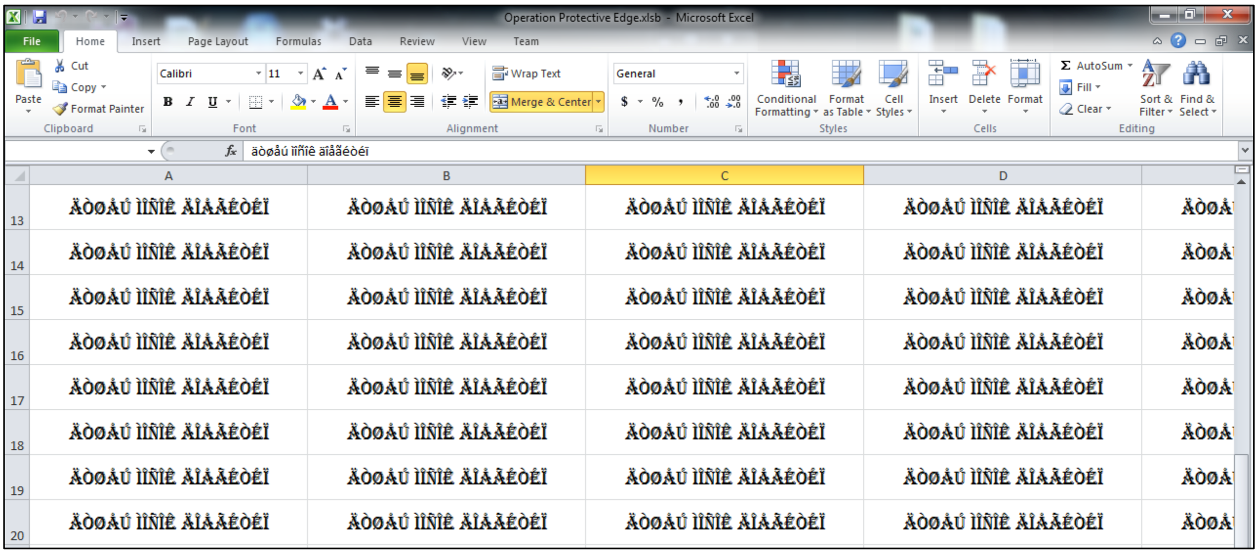
"Due to security considerations I consciously hid the Informations. It will be visible for you by enabling content above."



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).

[2] https://www.virustotal.com/en/file/3f7118a2ff787e61b5d18ba0591a29f90349d8ab93aa7d005cdf833f8c9895b2/analysis/



äòøåú ìîñîê äîåãéòéï

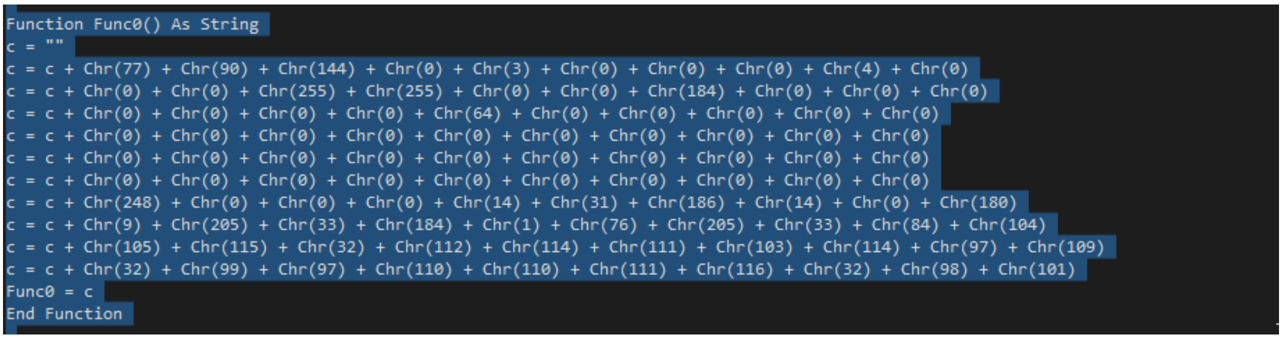
| | A | B | C | D | |
|---|---|---|---|---|---|
| 13 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 14 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 15 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 16 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 17 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 18 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 19 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |
| 20 | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅÚ ÌÎÑÎÊ ÄÎÅÃÉÒÉÏ | ÄÒØÅ |

# Technical Analysis

## Code

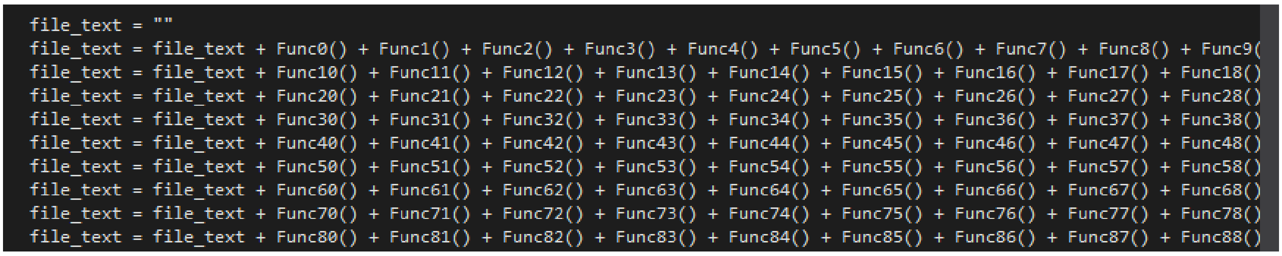
Analysis of the Macro code reveals the following structure:

In order to avoid detection by protection measures such as computer antivirus and intrusion detection systems, ASCII characters codes are used instead of actual characters. The ASCII codes are converted to strings as they are concatenated into a single variable within a function



```
Function Func0() As String
c = ""
c = c + Chr(77) + Chr(90) + Chr(144) + Chr(0) + Chr(3) + Chr(0) + Chr(0) + Chr(0) + Chr(4) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(255) + Chr(255) + Chr(0) + Chr(0) + Chr(184) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(64) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(248) + Chr(0) + Chr(0) + Chr(0) + Chr(14) + Chr(31) + Chr(186) + Chr(14) + Chr(0) + Chr(180)
c = c + Chr(9) + Chr(205) + Chr(33) + Chr(184) + Chr(1) + Chr(76) + Chr(205) + Chr(33) + Chr(84) + Chr(104)
c = c + Chr(105) + Chr(115) + Chr(32) + Chr(112) + Chr(114) + Chr(111) + Chr(103) + Chr(114) + Chr(97) + Chr(109)
c = c + Chr(32) + Chr(99) + Chr(97) + Chr(110) + Chr(110) + Chr(111) + Chr(116) + Chr(32) + Chr(98) + Chr(101)
Func0 = c
End Function
```

Tens of these functions then concatenated, creating a single PE file

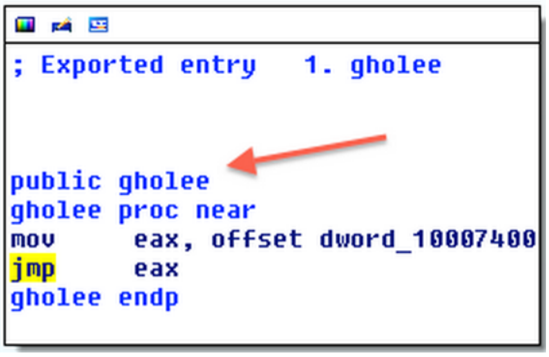


```
  file_text = ""
  file_text = file_text + Func0() + Func1() + Func2() + Func3() + Func4() + Func5() + Func6() + Func7() + Func8() + Func9(
  file_text = file_text + Func10() + Func11() + Func12() + Func13() + Func14() + Func15() + Func16() + Func17() + Func18()
  file_text = file_text + Func20() + Func21() + Func22() + Func23() + Func24() + Func25() + Func26() + Func27() + Func28()
  file_text = file_text + Func30() + Func31() + Func32() + Func33() + Func34() + Func35() + Func36() + Func37() + Func38()
  file_text = file_text + Func40() + Func41() + Func42() + Func43() + Func44() + Func45() + Func46() + Func47() + Func48()
  file_text = file_text + Func50() + Func51() + Func52() + Func53() + Func54() + Func55() + Func56() + Func57() + Func58()
  file_text = file_text + Func60() + Func61() + Func62() + Func63() + Func64() + Func65() + Func66() + Func67() + Func68()
  file_text = file_text + Func70() + Func71() + Func72() + Func73() + Func74() + Func75() + Func76() + Func77() + Func78()
  file_text = file_text + Func80() + Func81() + Func82() + Func83() + Func84() + Func85() + Func86() + Func87() + Func88()
```

Finally, the file is saved to NTUSER.data.{GUIDE}.dll (MD5: 48573a150562c57742230583456b4c02) and the function ShellExecte is used to run it under cmd.exe /C and Rundll32 This is in order to hide the process.

The Dll file is obfuscated and includes various mechanism to hide from Debuggers such as Ollydbg and IDA and from Sandbox software such as Cuckoo and Anubis.

Analyzing the file, we have found an interesting entry point called gholee.

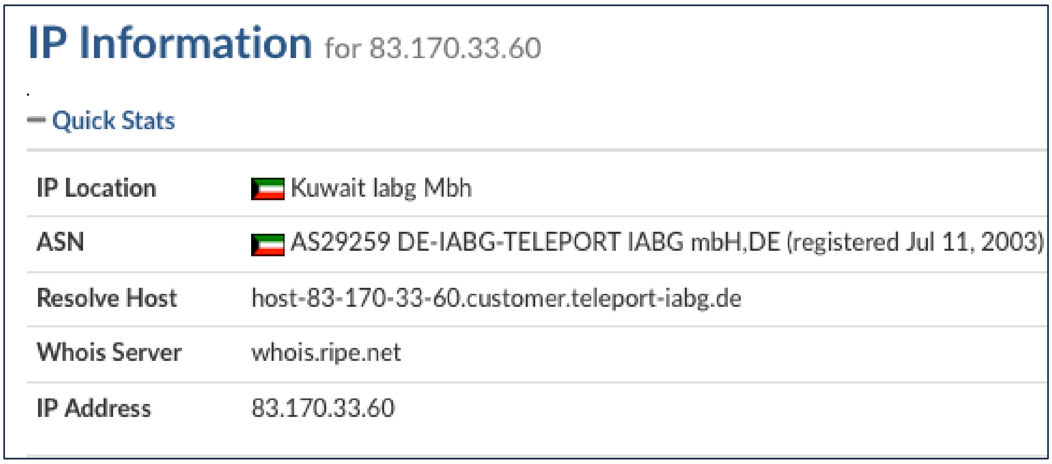


```
; Exported entry   1. gholee


public gholee
gholee proc near
mov     eax, offset dword_10007400
jmp     eax
gholee endp
```

## 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[3].



**IP Information** for 83.170.33.60

− Quick Stats

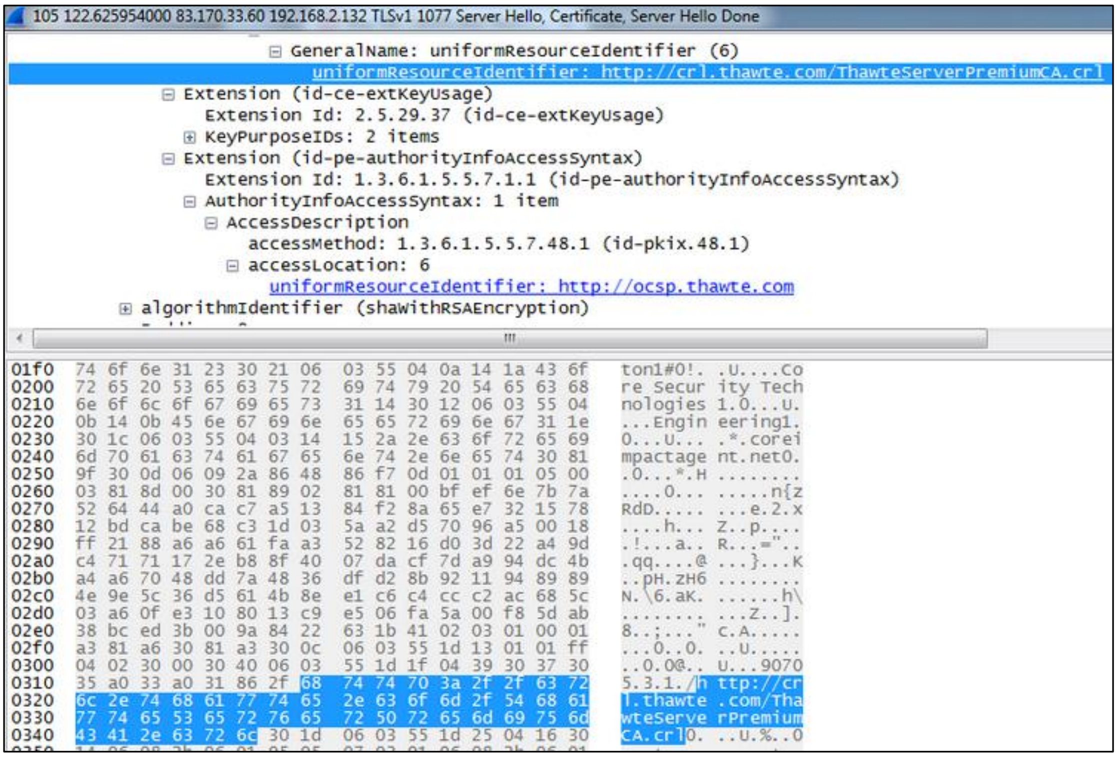
| | |
|---|---|
| IP Location | Kuwait Iabg Mbh |
| ASN | AS29259 DE-IABG-TELEPORT IABG mbH,DE (registered Jul 11, 2003) |
| Resolve Host | host-83-170-33-60.customer.teleport-iabg.de |
| Whois Server | whois.ripe.net |
| IP Address | 83.170.33.60 |

(Source: domaintools.com[4])

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.

[3] http://www.iabg.de/en/business-fields/infocom/teleport-satellitenkommunikation/teleport-operation-and-service.html

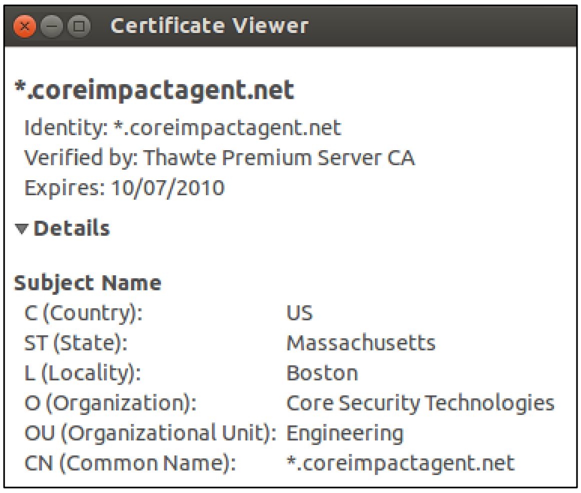
[4] https://whois.domaintools.com/83.170.33.60



```
105 122.625954000 83.170.33.60 192.168.2.132 TLSv1 1077 Server Hello, Certificate, Server Hello Done
                         ⊟ GeneralName: uniformResourceIdentifier (6)
                             uniformResourceIdentifier: http://crl.thawte.com/ThawteServerPremiumCA.crl
              ⊟ Extension (id-ce-extKeyUsage)
                  Extension Id: 2.5.29.37 (id-ce-extKeyUsage)
                ⊞ KeyPurposeIDs: 2 items
              ⊟ Extension (id-pe-authorityInfoAccessSyntax)
                  Extension Id: 1.3.6.1.5.5.7.1.1 (id-pe-authorityInfoAccessSyntax)
                ⊟ AuthorityInfoAccessSyntax: 1 item
                  ⊟ AccessDescription
                      accessMethod: 1.3.6.1.5.5.7.48.1 (id-pkix.48.1)
                    ⊟ accessLocation: 6
                        uniformResourceIdentifier: http://ocsp.thawte.com
          ⊞ algorithmIdentifier (shaWithRSAEncryption)

01f0  74 6f 6e 31 23 30 21 06  03 55 04 0a 14 1a 43 6f   ton1#0!. .U....Co
0200  72 65 20 53 65 63 75 72  69 74 79 20 54 65 63 68   re Secur ity Tech
0210  6e 6f 6c 6f 67 69 65 73  31 14 30 12 06 03 55 04   nologies 1.0...U.
0220  0b 14 0b 45 6e 67 69 6e  65 65 72 69 6e 67 31 1e   ...Engin eering1.
0230  30 1c 06 03 55 04 03 14  15 2a 2e 63 6f 72 65 69   0...U... .*.corei
0240  6d 70 61 63 74 61 67 65  6e 74 2e 6e 65 74 30 81   mpactage nt.net0.
0250  9f 30 0d 06 09 2a 86 48  86 f7 0d 01 01 01 05 00   .0...*.H ........
0260  03 81 8d 00 30 81 89 02  81 81 00 bf ef 6e 7b 7a   ....0... .....n{z
0270  52 64 44 a0 ca c7 a5 13  84 f2 8a 65 e7 32 15 78   RdD..... ...e.2.x
0280  12 bd ca be 68 c3 1d 03  5a a2 d5 70 96 a5 00 18   ....h... Z..p....
0290  ff 21 88 a6 a6 61 fa a3  52 82 16 d0 3d 22 a4 9d   .!...a.. R...="..
02a0  c4 71 71 17 2e b8 8f 40  07 da cf 7d a9 94 dc 4b   .qq....@ ...}...K
02b0  a4 a6 70 48 dd 7a 48 36  df d2 8b 92 11 94 89 89   ..pH.zH6 ........
02c0  4e 9e 5c 36 d5 61 4b 8e  e1 c6 c4 cc c2 ac 68 5c   N.\6.aK. ......h\
02d0  03 a6 0f e3 10 80 13 c9  e5 06 fa 5a 00 f8 5d ab   ........ ...Z..].
02e0  38 bc ed 3b 00 9a 84 22  63 1b 41 02 03 01 00 01   8..;..." c.A.....
02f0  a3 81 a6 30 81 a3 30 0c  06 03 55 1d 13 01 01 ff   ...0..0. ..U.....
0300  04 02 30 00 30 40 06 03  55 1d 1f 04 39 30 37 30   ..0.0@.. U...9070
0310  35 a0 33 a0 31 86 2f 68  74 74 70 3a 2f 2f 63 72   5.3.1./h ttp://cr
0320  6c 2e 74 68 61 77 74 65  2e 63 6f 6d 2f 54 68 61   l.thawte .com/Tha
0330  77 74 65 53 65 72 76 65  72 50 72 65 6d 69 75 6d   wteServe rPremium
0340  43 41 2e 63 72 6c 30 1d  06 03 55 1d 25 04 16 30   CA.crl0. ..U.%..0
```

It was issued by Thawte certificate authority.



**Certificate Viewer**

***.coreimpactagent.net**

Identity: *.coreimpactagent.net
Verified by: Thawte Premium Server CA
Expires: 10/07/2010

▼ **Details**

**Subject Name**

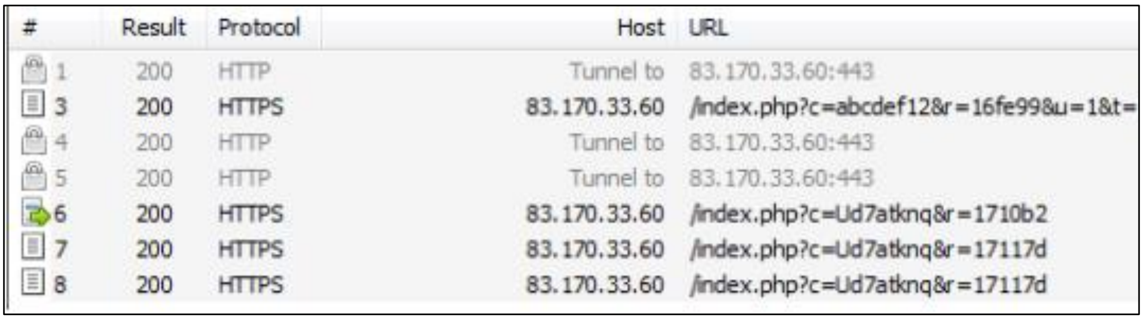
| | |
|---|---|
| C (Country): | US |
| ST (State): | Massachusetts |
| L (Locality): | Boston |
| O (Organization): | Core Security Technologies |
| OU (Organizational Unit): | Engineering |
| CN (Common Name): | *.coreimpactagent.net |

.

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 |



| # | Result | Protocol | Host | URL |
|---|---|---|---|---|
| 1 | 200 | HTTP | Tunnel to | 83.170.33.60:443 |
| 3 | 200 | HTTPS | 83.170.33.60 | /index.php?c=abcdef12&r=16fe99&u=1&t= |
| 4 | 200 | HTTP | Tunnel to | 83.170.33.60:443 |
| 5 | 200 | HTTP | Tunnel to | 83.170.33.60:443 |
| 6 | 200 | HTTPS | 83.170.33.60 | /index.php?c=Ud7atknq&r=1710b2 |
| 7 | 200 | HTTPS | 83.170.33.60 | /index.php?c=Ud7atknq&r=17117d |
| 8 | 200 | HTTPS | 83.170.33.60 | /index.php?c=Ud7atknq&r=17117d |

# 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
}
```

[5] https://www.virustotal.com/en/file/0b75e6364bb63043cf60c8adc98a5749b5167322f8951b128b56768158e3f576/analysis/