

BLOG

Gholee – a “protective edge” themed spear phishing campaign

Posted on September 4, 2014 by ClearSky Research Team

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

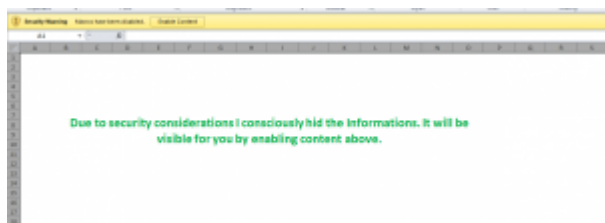
Our investigation of the Gholee malware started following a detection of a suspicious file that was sent in an email to an undisclosed recipient. The file name was '**Operation Protective Edge.xlsb**' (MD5: d0c3f4c9896d41a7c42737134ffb4c2e).

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."



([https://www.clearskysec.com/wp-](https://www.clearskysec.com/wp-content/uploads/2014/09/2.png)

[content/uploads/2014/09/2.png](https://www.clearskysec.com/wp-content/uploads/2014/09/2.png))

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).

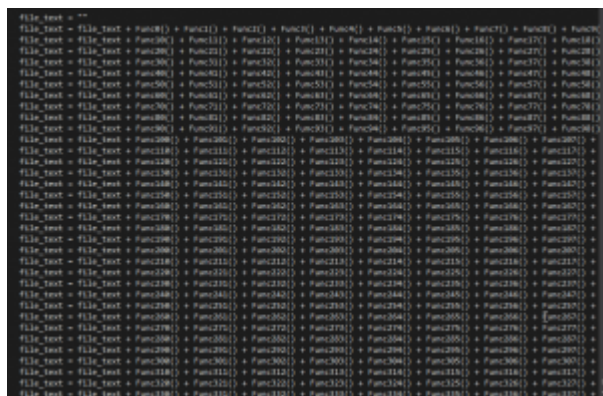
Technical Analysis

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

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



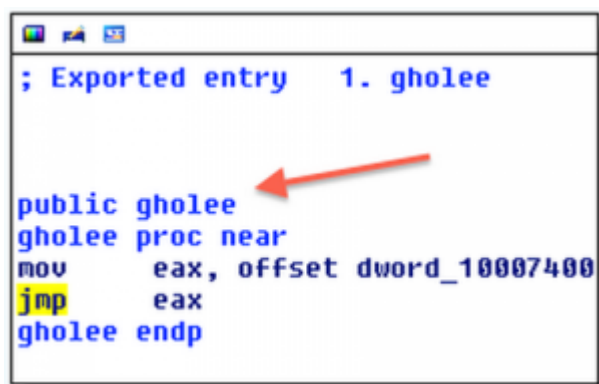
([https://www.clearskysec.com/wp-](https://www.clearskysec.com/wp-content/uploads/2014/09/5.png)

[content/uploads/2014/09/5.png](https://www.clearskysec.com/wp-content/uploads/2014/09/5.png))

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.



([https://www.clearskysec.com/wp-](https://www.clearskysec.com/wp-content/uploads/2014/09/6.png)

[content/uploads/2014/09/6.png](https://www.clearskysec.com/wp-content/uploads/2014/09/6.png))

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



([https://www.clearskysec.com/wp-](https://www.clearskysec.com/wp-content/uploads/2014/09/1.png)

[content/uploads/2014/09/1.png](https://www.clearskysec.com/wp-content/uploads/2014/09/1.png))

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

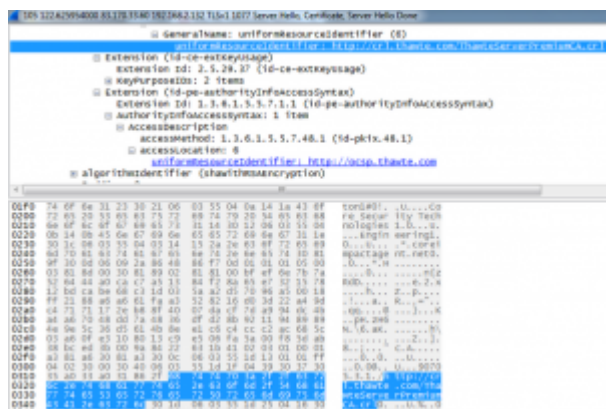
Quick Stats

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

(https://www.clearskysec.com/wp-

content/uploads/2014/09/7.png)

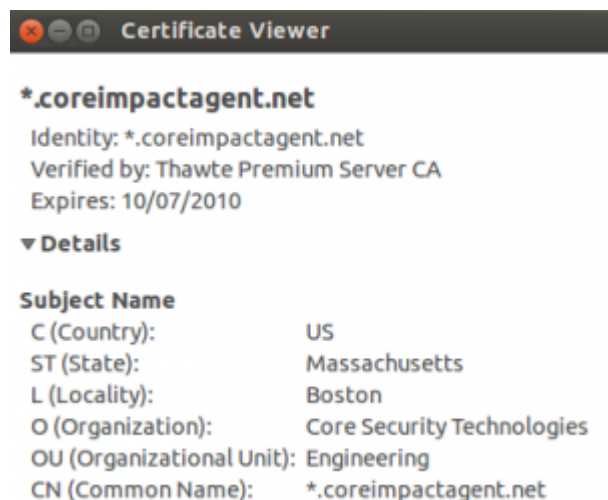
The malware opens an SSL connection over port 443 using a digital certificate that expired in 2010. The certificate was issued for security company Core Security, the creators of the offensive suite Core Impact, for the address *coreimpactagent.net.



(https://www.clearskysec.com/wp-

content/uploads/2014/09/8.png)

It was issued by Thawte certificate authority.



(https://www.clearskysec.com/wp-

content/uploads/2014/09/9.png)

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 communicating 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
}
```

📁 Posted in: Incidents (<https://www.clearskysec.com/category/incidents/>)

🔖 Tagged: featured (<https://www.clearskysec.com/tag/featured/>)

Search



Categories

Campaigns (<https://www.clearskysec.com/category/campaigns/>)

cat2 (<https://www.clearskysec.com/category/cat2/>)

[cyber attack \(https://www.clearskysec.com/category/cyber-attack/\)](https://www.clearskysec.com/category/cyber-attack/)

[Cyber-Crime \(https://www.clearskysec.com/category/cyber-crime/\)](https://www.clearskysec.com/category/cyber-crime/)

[Disinformation \(https://www.clearskysec.com/category/disinformation/\)](https://www.clearskysec.com/category/disinformation/)

[General \(https://www.clearskysec.com/category/general/\)](https://www.clearskysec.com/category/general/)

[Incidents \(https://www.clearskysec.com/category/incidents/\)](https://www.clearskysec.com/category/incidents/)

[Threat actors \(https://www.clearskysec.com/category/threat-actors/\)](https://www.clearskysec.com/category/threat-actors/)

[Uncategorized \(https://www.clearskysec.com/category/uncategorized/\)](https://www.clearskysec.com/category/uncategorized/)

Archive

[April 2020 \(https://www.clearskysec.com/2020/04/\)](https://www.clearskysec.com/2020/04/)

[February 2020 \(https://www.clearskysec.com/2020/02/\)](https://www.clearskysec.com/2020/02/)

[January 2020 \(https://www.clearskysec.com/2020/01/\)](https://www.clearskysec.com/2020/01/)

[October 2019 \(https://www.clearskysec.com/2019/10/\)](https://www.clearskysec.com/2019/10/)

[September 2019 \(https://www.clearskysec.com/2019/09/\)](https://www.clearskysec.com/2019/09/)

[August 2019 \(https://www.clearskysec.com/2019/08/\)](https://www.clearskysec.com/2019/08/)

[July 2019 \(https://www.clearskysec.com/2019/07/\)](https://www.clearskysec.com/2019/07/)

[June 2019 \(https://www.clearskysec.com/2019/06/\)](https://www.clearskysec.com/2019/06/)

[May 2019 \(https://www.clearskysec.com/2019/05/\)](https://www.clearskysec.com/2019/05/)

[April 2019 \(https://www.clearskysec.com/2019/04/\)](https://www.clearskysec.com/2019/04/)

[February 2019 \(https://www.clearskysec.com/2019/02/\)](https://www.clearskysec.com/2019/02/)

[November 2018 \(https://www.clearskysec.com/2018/11/\)](https://www.clearskysec.com/2018/11/)

[July 2018 \(https://www.clearskysec.com/2018/07/\)](https://www.clearskysec.com/2018/07/)

[February 2018 \(https://www.clearskysec.com/2018/02/\)](https://www.clearskysec.com/2018/02/)

January 2018 (<https://www.clearskysec.com/2018/01/>)

December 2017 (<https://www.clearskysec.com/2017/12/>)

November 2017 (<https://www.clearskysec.com/2017/11/>)

October 2017 (<https://www.clearskysec.com/2017/10/>)

August 2017 (<https://www.clearskysec.com/2017/08/>)

July 2017 (<https://www.clearskysec.com/2017/07/>)

May 2017 (<https://www.clearskysec.com/2017/05/>)

April 2017 (<https://www.clearskysec.com/2017/04/>)

March 2017 (<https://www.clearskysec.com/2017/03/>)

January 2017 (<https://www.clearskysec.com/2017/01/>)

November 2016 (<https://www.clearskysec.com/2016/11/>)

October 2016 (<https://www.clearskysec.com/2016/10/>)

June 2016 (<https://www.clearskysec.com/2016/06/>)

January 2016 (<https://www.clearskysec.com/2016/01/>)

November 2015 (<https://www.clearskysec.com/2015/11/>)

September 2015 (<https://www.clearskysec.com/2015/09/>)

June 2015 (<https://www.clearskysec.com/2015/06/>)

May 2015 (<https://www.clearskysec.com/2015/05/>)



September 2014 (<https://www.clearskysec.com/2014/09/>)



 (<https://www.clearskysec.com/feed/>) 

(<https://www.linkedin.com/company/clearsky-cyber-security>) 

(<https://twitter.com/ClearskySec>)

 (<https://www.clearskysec.com/>)  (<https://www.clearskysec.com/>)

Cyber Solutions

Threat Intelligence (<https://www.clearskysec.com/solutions/cyber-defense-intelligence/>)

Cyber strategy (<https://www.clearskysec.com/solutions/cyber-strategy/>)

Cyber architecture (<https://www.clearskysec.com/solutions/cyber-architecture/>)

Pay per report – APT Group research (<https://www.clearskysec.com/solutions/apt-group-in-depth-research/>)

Blockchain Security (<https://www.clearskysec.com/solutions/secure-blockchain/>)

Cyber Tabletop Exercise (<https://www.clearskysec.com/solutions/cyber-tabletop-exercise/>)

Contact us

Head office:

1010 Cambourne Business Park, Cambridge

CB23 6DP UK

Phone: +44 1223 976370

Email: [info \[at\] clearskysec.com](mailto:info@clearskysec.com)

Netherlands branch:

Regus – Diemen

Dalsteindreef 141, 1112 XJ Diemen

Phone: +44 1223 976370

Email: [info \[at\] clearskysec.com](mailto:info@clearskysec.com)

