

# Attacks against Israeli & Palestinian interests - Cyber security updates

[pwc.blogs.com](http://pwc.blogs.com) Updated Apr 27th, 2015

## Attacks against Israeli & Palestinian interests

27 April 2015

By Tom Lancaster

[Follow @tlansec](#)

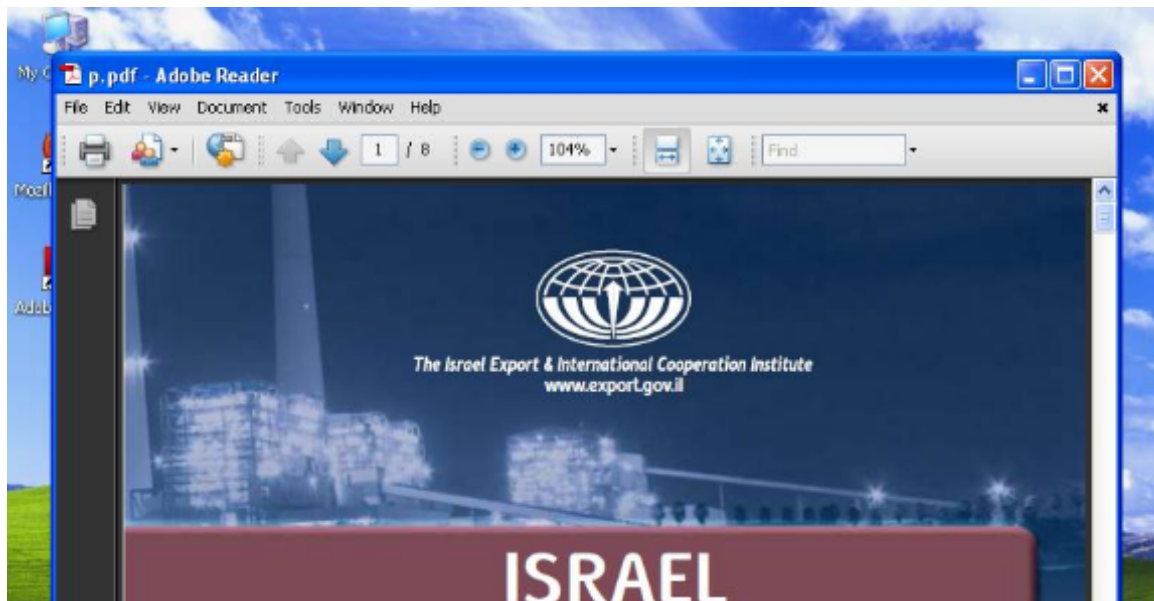
### Executive Summary

This short report details the techniques being used in a series of attacks mostly against Israel-based organisations. The decoy documents and filenames used in the attacks suggest the intended targets include organisations with political interests or influence in Israel and Palestine. Although we are unable to link this campaign to any already documented in open source, it bears similarities to some described by others previously<sup>[1],[2]</sup>.

The earliest samples in the campaign we have identified date back to the summer of 2014. The number of samples discovered and relatively small scale of infrastructure suggest the attackers have limited resources with which to conduct attacks.

### Introduction

Our investigation begins by taking a look at the following file:  
ecc240f1983007177bc5bbebca50eea27b80fd3d14fd261bef6cda10b8ffe1e9. According to the analysis published on malwr.com<sup>[3]</sup>, this file was originally named 'Israel Homeland Defense Directory 2015 \_Secured\_.exe' and, once executed, the following decoy document was presented:





The initial file in this case is a self-extracting RAR file that contains three components, including a decoy document (in this case, the PDF shown above) and the malware.

Further inspection of the malware extracted showed it wasn't a family our analysts recognised. This, coupled with the nature of the decoy document used, led us to take a more in depth look at the malware, and associated infrastructure.

*We'd like to give special thanks to Eyal Sela of ClearSky Security for his collaborative efforts in this research.*

## Delivery

The most common way this malware packaged is via a self-extracting RAR file; however the attackers also appear to have used a number of other solutions to drop their malware, including a Visual Basic based wrapper and an Auto-IT based wrapper.

In terms of how the malware is delivered, it's most likely that it's done via spearphishing. For example, there are also several occasions where the VirusTotal 'ITW' tab suggests that the original dropper was available to download on a 3<sup>rd</sup> party website. In the case of the sample discussed in the introduction we can see:

**File information**

Identification Content Analyses Submissions **ITW** Additional Comments

**Prevalence metrics**

First seen ITW	2015-04-15 09:31:26
First submission	2015-04-15 09:31:48
Last submission	2015-04-16 16:46:17
Number of submissions	5
Distinct source submissions	2

**Propagation, dissemination and distribution strategies**

This file has been spotted in-the-wild at certain URLs that are later detailed, it may be part of some drive-by download strategy or simply legitimately hosted goodware.

**Download URLs**

This file has been spotted as the response content of the following URLs.

<http://a.pomf.se/xlvunq.rar>

Download file Re-scan file Close

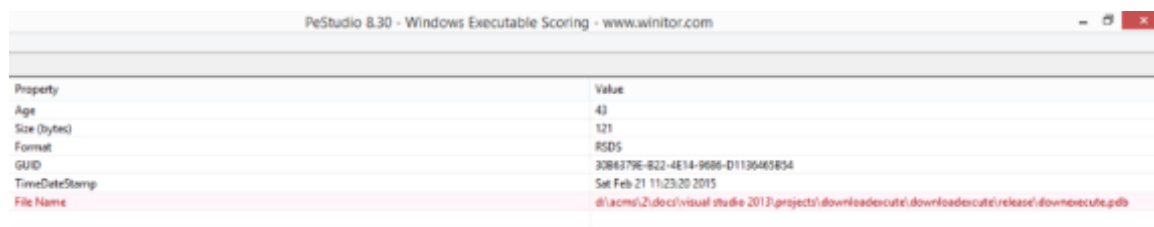
Pomf.se is a relatively low-profile file sharing/hosting website currently based in Sweden. The use of low-key file-sharing sites appears to be a feature of the campaign as far as we can tell, with a few other similar sites being used in the same way.

This, in conjunction with the nature of the related files we have discovered (all of them are directly executable files) means it is likely that the malware is primarily delivered via spear phishing attempts, rather than any other method.

## DownExecute – Brief Analysis

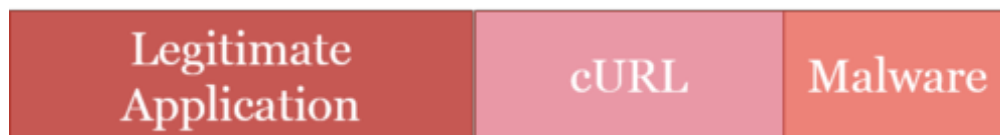
In this analysis, we'll go over the file with a SHA256 hash of ecc240f1983007177bc5bbebca50eea27b80fd3d14fd261bef6cda10b8ffe1e9.

We've chosen to refer to the malware as 'DownExecute' due to the .pdb string left in the malware (leaving debug paths in malware seems to be very fashionable at the moment...):



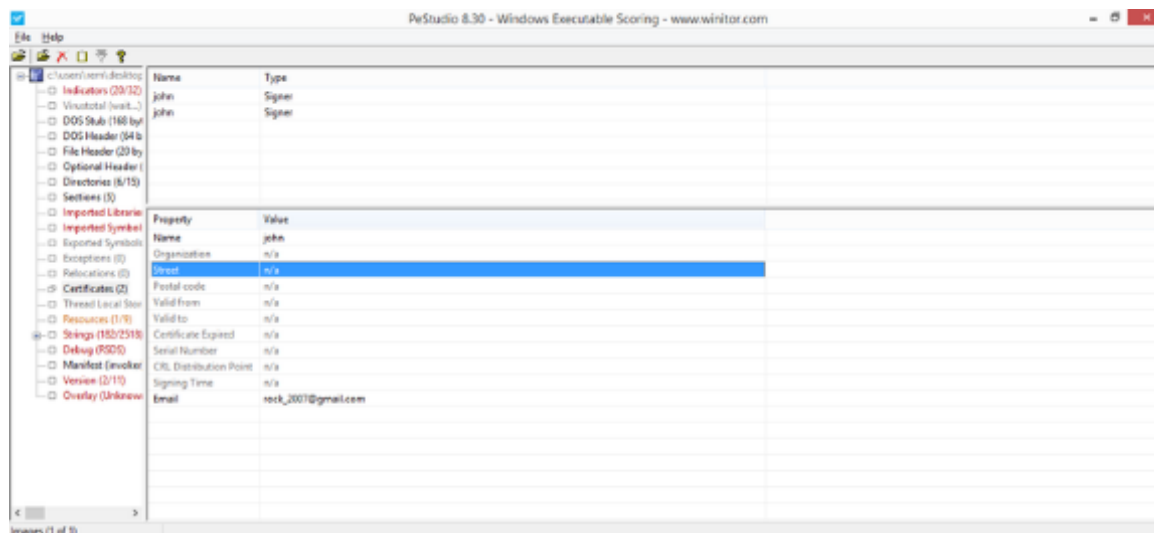
Property	Value
Age	43
Size (bytes)	121
Format	RSOS
GUID	3086379E-822-4E14-9886-D1136403B34
TimeStamp	Sat Feb 21 11:23:20 2015
File Name	d:\acmi\2\docs\visual_studio_2013\projects\downloader\downloader\release\downexecute.pdb

All variants of the DownExecute' malware we've identified come packaged in the following fashion:



From the samples we have analysed so far, the decoy application included is never used by the binary, and is presumably included so that anyone taking a cursory look at the file will conclude it is in fact the real deal. Whilst the cURL<sup>[4]</sup> binary included is used for internet connectivity but it's currently unclear why the attackers chose to use this method of adding connectivity to their file.

Some of the binaries are also self-signed:



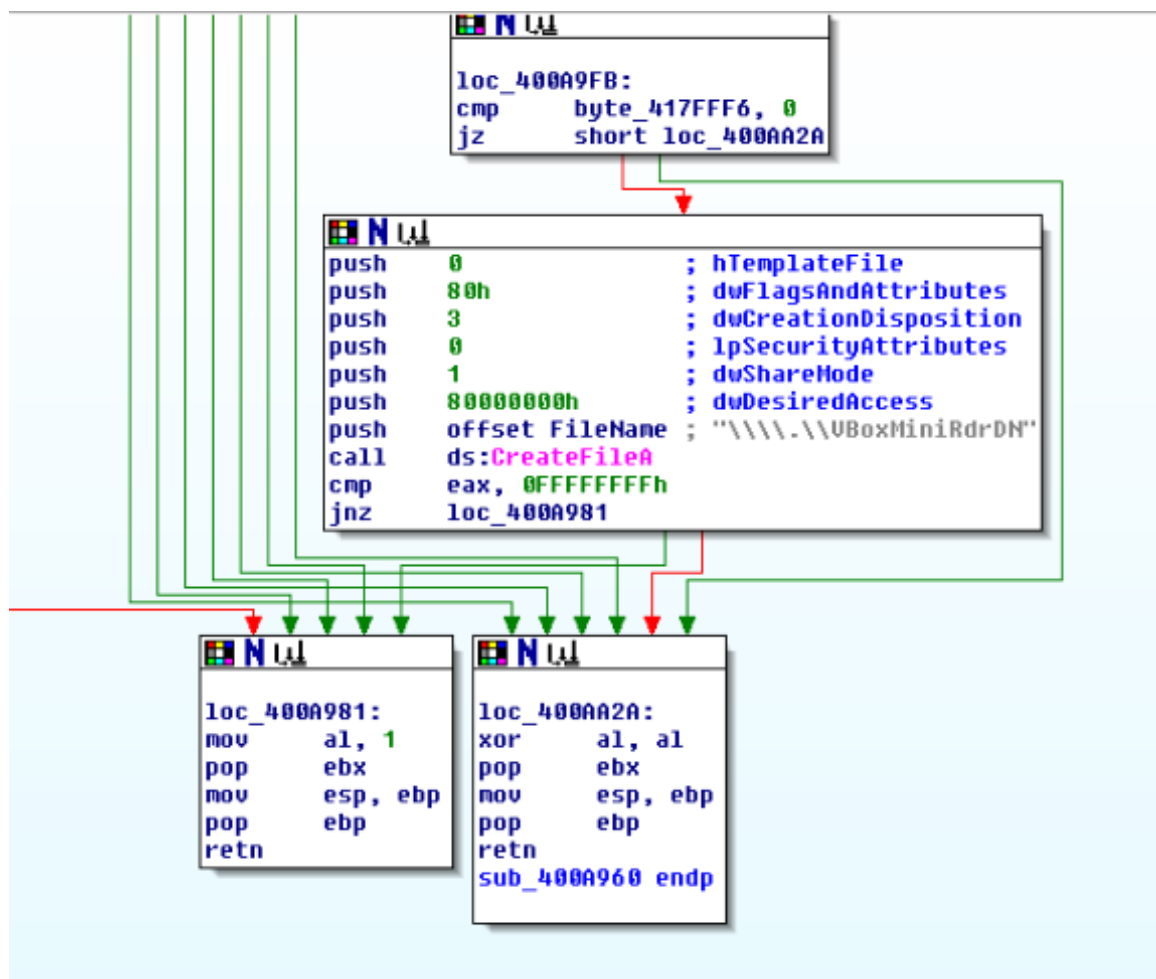
Name	Type
john	Signer
john	Signer

Property	Value
Name	john
Organization	n/a
Issued	n/a
Valid to	n/a
Valid from	n/a
Valid to	n/a
Certificate Expiry	n/a
Serial Number	n/a
CRL Distribution Point	n/a
Signing Time	n/a
Email	reck_2007@gmail.com

So what can this malware do? Not all that much – it's just a downloader.

Before execution, the malware makes a couple of checks to avoid analysis, including checking for the presence of a debugger using IsDebuggerPresent as well as checking for the presence of VirtualBox by looking for the device name \\.\VBoxMiniRdrDN:



The malware also checks for the presence of several anti-virus solutions, as well for any processes including the word 'security':

```
; Attributes: bp-based frame
```

```
sub_4018C30 proc near
```

```
var_34= dword ptr -34h
var_30= dword ptr -30h
var_2C= dword ptr -2Ch
var_28= dword ptr -28h
var_24= dword ptr -24h
var_20= dword ptr -20h
var_1C= dword ptr -1Ch
var_18= dword ptr -18h
var_14= dword ptr -14h
var_10= dword ptr -10h
var_C=  dword ptr -0Ch
```

```

var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 38h
lea    eax, [ebp+var_34]
push    eax
mov     [ebp+var_34], offset aAvira ; "avira"
mov     [ebp+var_30], offset aAvast ; "avast"
mov     [ebp+var_2C], offset aAvg ; "avg"
mov     [ebp+var_28], offset aEset ; "eset"
mov     [ebp+var_24], offset aKaspersky ; "kaspersky"
mov     [ebp+var_20], offset aAlwil ; "alwil"
mov     [ebp+var_1C], offset aOnecare ; "onecare"
mov     [ebp+var_18], offset aSecurity ; "security"
mov     [ebp+var_14], offset aMcafee ; "mcafee"
mov     [ebp+var_10], offset aSymantec ; "symantec"
mov     [ebp+var_C], offset aNorton ; "norton"
mov     [ebp+var_8], offset aDefender ; "defender"
mov     [ebp+var_4], offset aBitdefender ; "bitdefender"
call   sub_4018990 ; checkProcesses
add     esp, 4
mov     esp, ebp
pop     ebp
retn
sub_4018C30 endp

```

The malware then proceeds to decrypt some basic configuration data, including the command & control domain, and information about the origin of the infection, tracked via ID:

The screenshot shows the OllyDbg interface with the assembly window on the left and the hex dump window on the right. The assembly window displays instructions for the function `pssecurity.KERNEL32.CreateMutex`. The hex dump window shows the following data:

```

Arg1 = 0a
ASCII "hostname:"
Arg1 = 0a
ASCII "http://fastbingcom.sytes.net/dw/setup"
Arg1 = 0a
ASCII "mckname:"

```

Meanwhile, the malware begins calling home, whilst also keeping a log of its actions in a plaintext file that is created in the same folder as where the binary was executed from.

```
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
log.txt
1 -----<<<2015-4-20
2 >>>-----
3 starting
4 -----<<<====>>>-----<<<2015-4-20
5 >>>-----
6 config
7 HostName: http://fastbingcom.avtes.net/dw/setup
8 nickName:
9 Gid:1
10 -----<<<====>>>-----<<<2015-4-20
11 >>>-----
12 GET Token at host http://fastbingcom.avtes.net/dw/gtk
13 is
14 -----<<<====>>>-----<<<2015-4-20
15 >>>-----
16 GET Token at host http://fastbingcom.avtes.net/dw/gtk
17 is
18 -----<<<====>>>-----
```

### After successful compromise...

It appears as though the clue for the main functionality of this malware is in its name (it downloads, and then executes) files, as it offers little else for the attacker. The DownExecute malware is used as a way for the attackers to gain an initial foothold on the victim machine. The basic information reported back by the malware would also certainly allow the attacker a way to triage infections to ensure they had reached their intended victim rather than a researcher.

We don't have great visibility into post-compromise activity at this stage; however there are a number of other malware samples which communicate with the same infrastructure as the DownExecute samples. It's not unreasonable to infer that if these are more fully featured backdoors, that they are likely the 2<sup>nd</sup> stage malware families used in conjunction with DownExecute. Specifically, we've observed the well-documented Xtreme RAT and Poison Ivy malware families in use with the same domain names as DownExecute. The Poison Ivy passwords observed for the group were 'admin2014' and 'admin!@#\$%'.

### Command & Control Infrastructure





the other actors we see from the region.

## Inferred Targeting

As we have mentioned in a number of our other reports[5], attackers often use C&C domains which contain phrases relevant to their targets so as to make them appear legitimate. With this in mind we performed some simple analysis on the domain names used in this campaign to identify legitimate organisations being impersonated. For a full list of C&Cs used, please see Appendix B.

Domain name	Legitimate Entity	Description
Rotter2.sytes.net	rotter.net	Israeli news outlet
haartezenglish.strangled.net	haaretz.co.il	Israeli news outlet
wallanews.sytes.net	walla.co.il	Israeli news outlet
ynet.sytes.net	ynet.co.il	Israeli news outlet
safar.selfip.com	Safar	Islamic 2 <sup>nd</sup> month
depka.sytes.net	debka.com	Israeli news outlet

As shown, there appears to be a theme here, with a number of Israeli news organisations being used as C&C themes and hence probably being targeted. So do we believe this campaign is focused only at Israeli companies? Perhaps not entirely.

## Targeting

Whilst there are a number of documents clearly aimed at Israeli nationals , using political and military themes, one of the lures[6] included an Arabic language decoy document pictured below:

### عباس لـماجد فرج: جهاز المخابرات مخترق

قال مصدر أمني مطلع لنا من داخل جهاز المخابرات العامة - التابع لسلطة رام الله - أن رئيس السلطة محمود عباس وبخ مدير الجهاز - اللواء ماجد فرج بلغة عنيفة، على خلفية الفضائح المتتالية للوثائق المسربة من داخل جهاز المخابرات.

وأفاد المصدر ذاته، بأن التوبيخ جاء على خلفية التسريبات الإعلامية الأخيرة والفضائح المنشورة فيما يخص أداء المخابرات و " كولساتها " الداخلية ، حيث قال عباس لفرج : " جهازك مخترق تماما ، نصفه لمحمد دحلان والنصف الآخر للطيراوي ، ووثائقك في الشارع وفي متناول العامة " وذلك حسبما أفادت المصدر.

The document in question discusses an alleged leak of information relating to Abbas, leader of the Palestine Liberation Organization. Whilst this is a subject which is clearly of key interest to all parties in the region, the fact the attackers sent an Arabic language version of the story may indicate that the recipient was expected to be fluent in Arabic, and possibly therefore less likely to be Israeli, but rather



someone from another adjacent region.

## Conclusion

Whilst, in this case, we're unable to attribute this set of activity to a specific group or entity in the Middle East, it does bear a significant resemblance to many attacks seen from the Middle East that have been previously documented. Specifically, the following aspects of this campaign remind us of existing write-ups on Middle Eastern campaigns:

- **Consistent use of the dynamic DNS provider no-ip.com and associated domains:** it's unclear why there is a preference for this, however in several 'how-to' videos on Arabic language underground forums the video creators recommend using no-ip.com as opposed to other dynamic DNS providers;
- **Use of publically available malware:** many groups operating in the Middle East use malware families (such as Poison Ivy/Xtreme RAT) which are publically available rather than developing their own binaries;
- **Variety of targeting:** the targeting seems entirely restricted to Middle Eastern issues and, whilst there appears to be a heavy focus on Israel in the decoy documents we've observed, there is the possibility that Palestinians have been targeted as well. This is consistent with the complex relationships between the different nations and political groups in the region;
- **Password schema:** In their August 2013 blog<sup>[7]</sup>, FireEye noted that a group they refer to as MoleRats used Poison Ivy and Xtreme RAT, in conjunction with a password of "!@#GooD#@!" The keyboard walk used for the symbols "!@#" across the top of a keyboard is similar to the password observed in some of our Poison Ivy samples.

The fact that the attackers chose to develop their own dropper may be indicative that their biggest problem when conducting network intrusions is getting their foot in the door – particularly as it seems as though they still prefer the more fully featured Poison Ivy and Xtreme RAT backdoors as 2<sup>nd</sup> stage malware families.

When we pivoted and looked for the earliest examples of the DownExecute malware, the first samples we could find were compiled in June 2014. We have no reason to believe in this case that the threat actor has tampered with the compile time on any samples, as all other samples discovered were identified shortly after they were compiled. As such we believe the campaign using this downloader malware has been on-going for approximately 12 months.

## Appendix A – Samples

### SHA256

8993a516404c0dd62692f3ce5055d4ddee7e29ad4bb6aa29f67114eeeeae26b9

bfe727f2f238f11eb989e5b76efd24ad2b41df3cf7dabf7077dfaace834e7f03

dad34d2cb2aa9662d4a4148481ae018f5816498f30cc7aee4919e0e9fe6b9e08

2cb9df0d52d09c98f0a97ce71eb8805f224945cadab7d615ef0257b7b09c80d3

f53fd5389b09c6ad289736720e72392dd5f30a1f7822dbc8c7c2e2b655b4dad9

1d533ddaefc7859a3f6c6751114e895b7aa5935eb0ed68b01ec61aa8560ae3d9

95b2f926ae173ab45d6dac4039f0b91eb24699e6d11b621bbcebd860752e5d5e

da63f6392ce6af83f6d944fa1bd3f28082345fec928647ee7ef9939fac7b2e6c

a7aeead233fcdf1c7475db982497a82d8ae745ec1c58bd87215e8869c3f9e4  
2eb7aa306551d693691d14558c5dc4f6d80ef8f69cf466149fba23953c08f7f  
e945b055fb4057a396506c74f73b873694125e6178a40d10cabf24b2d89d598f  
c9e084eb1ce1066ee063f860c13a8f7d2ead97495036855fc956dacc9a24ea68  
047e8d542e2fcd0f4dd45e2b19848771d01abc90d161d05242b79c52cdd248d  
25e6bf67410dff95c527c19dcff5223dbc3bf4c987650e45fba1267072e8ff  
b0edbd0f44df72e0fad3fb73948444a4df5143ed954c9116eb1a7b606841f187  
da63f6392ce6af83f6d944fa1bd3f28082345fec928647ee7ef9939fac7b2e6c  
de3e25a69ba43b9f236e544ece7f2da82a4fab4489ad2e263754d9b9d88bc5c  
ecc240f1983007177bc5bbebca50eea27b80fd3d14fd261bef6cda10b8ffe1e9  
f969bf3b7a9821b3b2d5de889b5af7af25972b25ba59e4e9439f87fe90f1c404  
14be3a9a2a4261cb365915e720486a0632dbebb06fe68fb669ae67aa9b18507b  
488ba22d6cb8c9b0310c58fa4c4739692cdf45676c3164b357314322542f9dff  
b3a47e0bc0af49b46bc0c1158089bf200856ff462a5334df2b5c11e69c8b1ada  
324ce011b913feec4adb916f32c743a243f07dccb51b49c0122c4fa4a8e2bde  
d6df5943169b48ac58fc28bb665fe8800c265b65fff8a2217b70703a4d3a7277  
88e7a7e815565b92af81761ae7b9153b7507677df3d3b77e8ce68787ad1826d4  
f51d4155534e10c09b531acc41458e8ff3b7879f4ee7d3ee99f16180c4caf0ee  
b3a47e0bc0af49b46bc0c1158089bf200856ff462a5334df2b5c11e69c8b1ada  
bc846caa05939b085837057bc4b9303357602ece83dc1380191bddd1402d4a2b

## Appendix B – C&C Infrastructure

Value	Value Type
cbbnews.tk	Domain
haartezenhish.redirectme.net	Domain
wallanews.sytes.net	Domain
kaliob.selfip.org	Domain
deapka.sytes.net	Domain
download.likescandy.com	Domain

orango.redirectme.net	Domain
ynet.sytes.net	Domain
kaswer12.strangled.net	Domain
nazer.zapto.org	Domain
rotter2.sytes.net	Domain
kaswer13.zapto.org	Domain
tango.zapto.org	Domain
kolabdown.sytes.net	Domain
rotter2.publicvm.com	Domain
safar.selfip.com	Domain
bandao.publicvm.com	Domain
safari.linkpc.net	Domain
thenewupdate.chickenkiller.com	Domain
backjadwer.bounceme.net	Domain
ajaxo.zapto.org	Domain
downloadskype.cf	Domain
redirectlnk.redirectme.net	Domain
thenewupdatee.redirectme.net	Domain
chromeupdt.tk	Domain
duntat.zapto.org	Domain
ynet.ignorelist.com	Domain
haartezenenglish.strangled.net	Domain
gaonsmom.redirectme.net	Domain
store-legal.biz	Domain
fastbingcom.sytes.net	Domain
downloadlog.linkpc.net	Domain
downloadmyhost.zapto.org	Domain
depka.sytes.net	Domain

wallanews.publicvm.com	Domain
noredirecto.redirectme.net	Domain
safara.sytes.net	Domain
help2014.linkpc.net	Domain
totoman.no-ip.biz	Domain
lilian.redirectme.net	Domain
webfile.myq-see.com	Domain
185.33.168.150	IPv4 Address
185.45.193.4	IPv4 Address
167.114.62.213	IPv4 Address
131.72.136.11	IPv4 Address
131.72.136.171	IPv4 Address
192.253.246.169	IPv4 Address
198.105.122.96	IPv4 Address
131.72.136.124	IPv4 Address
107.168.129.29	IPv4 Address
198.105.122.9	IPv4 Address

### **Appendix C – Signatures**

rule DownExecute\_A

meta:

author = "PwC Cyber Threat Operations :: @tlansec"

date = "2015-04"

reference = "[http://pwc.blogs.com/cyber\\_security\\_updates/2015/04/attacks-against-israeli-palestina-n-interests.html](http://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestina-n-interests.html)"

description = "Malware is often wrapped/protected, best to run on memory"

strings:

\$winver1 = "win 8.1"

\$winver2 = "win Server 2012 R2"

\$winver3 = "win Srv 2012"

\$winver4 = "win srv 2008 R2"

\$winver5 = "win srv 2008"

\$winver6 = "win vsta"

\$winver7 = "win srv 2003 R2"

\$winver8 = "win hm srv"

\$winver9 = "win Strg srv 2003"

\$winver10 = "win srv 2003"

\$winver11 = "win XP prof x64 edt"

\$winver12 = "win XP"

\$winver13 = "win 2000"

\$pdb1 = "D:\\Acms\\2\\docs\\Visual Studio  
2013\\Projects\\DownloadExcute\\DownloadExcute\\Release\\DownExecute.pdb"

\$pdb2 = "d:\\acms\\2\\docs\\visual studio  
2013\\projects\\downloadexcute\\downloadexcute\\downexecute\\json\\rapidjson\\writer.h"

\$pdb3 = ":\acms\\2\\docs\\visual studio  
2013\\projects\\downloadexcute\\downloadexcute\\downexecute\\json\\rapidjson\\internal\\stack.h"

\$pdb4 = "\\downloadexcute\\downexecute\\"

\$magic1 = "<Win Get Version Info Name Error"

\$magic2 = "P@\$sw0rd\$nd"

\$magic3 = "\$t@k0v2rF10w"

\$magic4 = "|\*|123xXx(Mutex)xXx321|\*|6-21-2014-03:06PM" wide

\$str1 = "Download Excute" ascii wide fullword

\$str2 = "EncryptorFunctionPointer %d"

\$str3 = "%s\\%s.lnk"

\$str4 = "Mac:%s-Cpu:%s-HD:%s"

\$str5 = "feed back responce of host"

\$str6 = "GET Token at host"

\$str7 = "dwn md5 err"

condition:

all of (\$winver\*) or

any of (\$pdb\*) or

any of (\$magic\*) or

2 of (\$str\*)

Network IDS

alert http any any -> any any (msg:"--[PwC CTD] -- Unclassified Middle Eastern Actor - DownExecute  
URI (/dw/gtk)"; flow:established,to\_server; urilen:7; content:"/dw/gtk"; http\_uri; depth:7; content:"GET" ;  
http\_method:content:"" http\_header:content:"" http\_header:

http\_method; content: User-Agent: ; http\_header; content: Referer: ; http\_header;  
reference:md5,4dd319a230ee3a0735a656231b4c9063; classtype:trojan-activity; metadata:tlp  
WHITE,author @ipsosCustodes; sid:99999901; rev:2015200401;)

alert http any any -> any any (msg:"--[PwC CTD] -- Unclassified Middle Eastern Actor - DownExecute  
URI (/dw/setup)"; flow:established,to\_server; urilen:>8; content:"/dw/setup"; http\_uri; depth:9;  
content:"POST" ; http\_method; reference:md5,4dd319a230ee3a0735a656231b4c9063;  
classtype:trojan-activity; metadata:tlp WHITE,author @ipsosCustodes; sid:99999902; rev:2015200401;)

alert http any any -> any any (msg:"--[PwC CTD] -- Unclassified Middle Eastern Actor - DownExecute  
Headers"; flow:established,to\_server; urilen:>7; content:"Accept \*/\*"; http\_client\_body;  
content:"Content-Type: multipart/form-data; boundary=-----"; http\_header; content:  
"ci\_session="; http\_cookie; depth:11; content: "POST"; http\_method; content:!"Referer:"; http\_header;  
content:!"User-Agent:"; http\_header; reference:md5,4dd319a230ee3a0735a656231b4c9063;  
classtype:trojan-activity; metadata:tlp WHITE,author @ipsosCustodes; sid:99999903; rev:2015200401;)

---

[1]

[https://github.com/kbandla/APTnotes/blob/master/2012/Cyberattack\\_against\\_Israeli\\_and\\_Palestinian\\_targets.pdf](https://github.com/kbandla/APTnotes/blob/master/2012/Cyberattack_against_Israeli_and_Palestinian_targets.pdf)

[2] <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html>

[3] <https://malwr.com/analysis/N2I1YmExMjNkMmM3NGQwMThINjg5YmI4OGY3Mjc3Zml>

[4] <http://curl.haxx.se>

[6] [ca78b173218ad8be863c7e00fec61f2f](https://ca78b173218ad8be863c7e00fec61f2f)

[7] <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html>

*Evernote makes it easy to remember things big and small from your everyday life using your computer, tablet, phone and the web.*