ZLAB

Malware Analysis Report

Chinese APT 27’s long-term espionage campaign in Syria is still ongoing

23/07/2018

CSE CyberSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Table of Contents

CSE CyberSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

The Open Repository and the Fake Promotional Site

A few days ago, the security researcher Lukas Stefanko from Eset discovered an open repository containing some Android applications.

Figure 1 - Lukas Stefanko's Twitter about the open repository.

The folder was found on a compromised website at the following URL:

hxxp://chatsecurelite.uk[.]to.

This website is written in Arabic language and translating its content it seems to offer a secure messaging app. The homepage shows how the application works and includes some slides about it.

Figure 2 - Screens of the fake security website

The content on the website says that most common messaging applications are vulnerable and attackers can compromise them to spy on the users. The author claims to have developed an app called “ChatSecure” to mitigate security vulnerabilities that have been reported in popular messaging apps, including WhatsApp and Telegram.

ChatSecure is the name of a legitimate free and open source iOS messaging app that features OMEMO encryption and OTR encryption over XMPP.

The content of the bogus website explains that also Office applications are vulnerable to cyber attacks and offers patches to address the vulnerabilities exploited by the hackers.

Figure 3 - ChatSecure legitimate iOS app.

Threat actors exploited the interest in the ChatSecure, currently available only for Apple iOS device, to trick Android users into believe that the Android version of the app is not available.

Index of /wp-content/uploads/2018/android/apks/store

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[ ]	تحديث أوفي..>	2018-04-13 17:15	1.5M	
[ ]	AndroidOfficeUpdate2..>	2018-04-13 17:15	1.5M	
[ ]	OfficeUpdate.apk	2018-04-13 17:15	1.5M	
[ ]	chatsecure2018.apk	2018-04-13 17:15	1.5M	
[ ]	telegram2018.apk	2018-04-13 17:05	1.6M	
[ ]	whatsapp2018.apk	2018-04-13 17:21	1.6M	

Apache/2.4.17 (Win32) PHP/5.6.15 Server at chatsecurelite.uk.to Port 80

The Android app poses itself as fake update for the legit app.

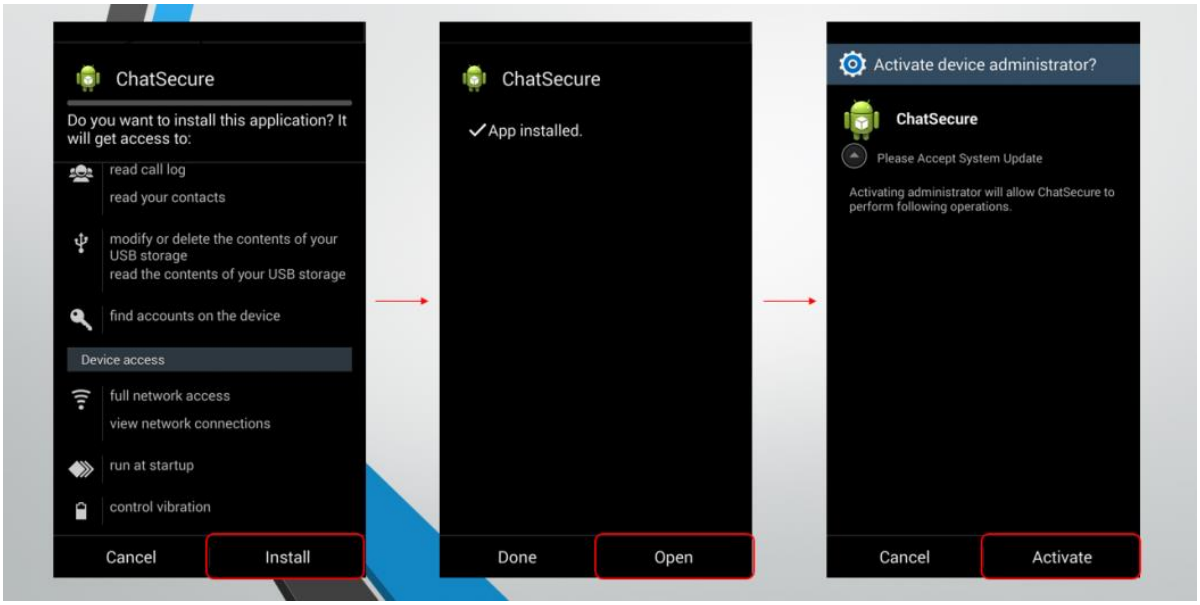


Figure 4 - Example of installation

The malicious apk files

In this paragraph, we'll report the gathered samples that were stored in the open repository.

"AndroidOfficeUpdate2018.apk"
"تحديث أوفيس للجوال.apk" ("UpdateOfficeforMobile.apk")
"chatsecure2018.apk"
"OfficeUpdate.apk"

MD5	6296586cf9a59b25d1b8ab3eeb0c2a33
SHA-1	5d9c175d8b84c03c7e656e5b29a7b9ab69e5a17b
SHA-256	54d6dc8300fad699c3fdfaa6614250f1151208dc6c5a4ede6097470e4af7817b
File Size	1517 KB
Icon	--

"telegram2018.apk"

MD5	c741c654198a900653163ca7e9c5158c
SHA-1	0c5611b383537faa715c31fa182cff92b73c97db
SHA-256	db70c8d699a3173028e768914b297a4c0c3a96c457845b38dfac535bc1b48eb3
File Size	1613 KB
Icon	

"whatsapp2018.apk"

MD5	cf5e62ebbf4be2417b9d3849c3c3f9c9
SHA-1	fcc38a0acdfcde59bf1bc4b4227feb47b5f71ad4
SHA-256	041b9066f42b78c5f2c9ff25a3bba3155a21c21fa0ee55aea510f456b3bc1847
File Size	1675 KB
Icon	

"chatsecure2018.apk"

MD5	f59cfb0b972fdf65baad7c37681d49ef
SHA-1	eace586f5b1a4eae6d1e0503e079753e0ac88176
SHA-256	caf0f58ebe2fa540942edac641d34bbc8983ee924fd6a60f42642574bbcd3987
File Size	1518 KB
Icon	--

"telegram2018.apk"

MD5	5de80e4b174f17776b07193a2280b252
SHA-1	6867eff4edc425606ac746e87a9df1b7424a1e49
SHA-256	2d0a56a347779ffdc3250deadda50008d6fae9b080c20892714348f8a44fca4b
File Size	1613 KB
Icon	

"whatsapp2018.apk"

MD5	f0d240bac174e38c831afdd80e50a992
SHA-1	f4cc667a05fb478b126207848a8da340327d3329
SHA-256	b15b5a1a120302f32c40c7c7532581ee932859fdfb5f1b3018de679646b8c972
File Size	1675 KB
Icon	

Actually, the above apk files contain the same malicious code, they differ the used icons of the application and the variable package name in which is written the code.

The malware shows a classical RAT behavior, it includes a series of hard-coded commands that the C2 can send to the bot. The list of accepted commands, with the relative opcodes is the following:

```
public static final short Command_Camera_Snap = 36;
public static final short Command_Change_CC = 39;
public static final short Command_Connect = 17;
public static final short Command_Copy_File = 22;
public static final short Command_Delete_File = 21;
public static final short Command_Download_File = 19;
public static final short Command_GPS_End = 38;
public static final short Command_GPS_Start = 37;
public static final short Command_Get_Apps = 41;
public static final short Command_Get_CC = 40;
public static final short Command_Get_CallLog = 33;
public static final short Command_Get_Contacts = 31;
public static final short Command_Get_Files = 18;
public static final short Command_Get_Messages = 32;
public static final short Command_Make_Dir = 28;
public static final short Command_Move_File = 23;
public static final short Command_Rename_File = 24;
public static final short Command_Run_File = 25;
public static final short Command_Shell = 29;
public static final short Command_Start_Audio = 34;
public static final short Command_Stop_Audio = 35;
public static final short Command_Uplaod_File = 20;
public static final String Delimiter = "</HAMZA_DELIMITER_STOP>";
public static final short Error_Camera = 102;
public static final short Error_FileManager = 101;
public static final short Error_Main = 100;
public static final short HeartBeat = 16;
public static final int Max_Packet_Size = 4096;
public static final short PING = 30;
```

Figure 5 - Command list

After installation and according to the list of commands, the first opcode captured during the analysis is “Connect to Server”, associated with the 17 opcode, in order to register the new bot on the Command and Control (Figure 6). As we can see in the Figure, the new bot sends to the Command and Control other information about the compromised device, such as:

- Which apk starts the infection
- Android version of the device
- Wifi or mobile internet network
- Installation of the bot date
- Device Name
- IMEI
- Mobile operator
- Root permissions enabled check

```
 4 0.438504789   10.0.2.15          82.137.255.56      TCP      801 42266 → 1740 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=747
 5 0.438719804   82.137.255.56      10.0.2.15          TCP       60 1740 → 42266 [ACK] Seq=1 Ack=748 Win=65535 Len=0
 6 0.478458824   10.0.2.15          82.137.255.56      TCP      209 42266 → 1740 [PSH, ACK] Seq=748 Ack=1 Win=29200 Len=155
me 4: 801 bytes on wire (6408 bits), 801 bytes captured (6408 bits) on interface 0
ernet II, Src: PcsCompu_43:da:5d (08:00:27:43:da:5d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
ernet Protocol Version 4, Src: 10.0.2.15, Dst: 82.137.255.56
nsmission Control Protocol, Src Port: 42266, Dst Port: 1740, Seq: 1, Ack: 1, Len: 747
a (747 bytes)

52 54 00 12 35 02 08 00  27 43 da 5d 08 00 45 00   RT..5... 'C.]..E.
03 13 03 ce 40 00 40 06  d6 46 0a 00 02 0f 52 89   ....@.@. .F....R.
ff 38 a5 1a 06 cc 62 5e  ce 7e 0a 01 86 02 50 18   .8....b^ .~....P.
72 10 60 d6 00 00 3c 48  6d 7a 61 50 61 63 6b 65   r.`...<H mzaPacke
74 3e 0a 20 20 3c 58 4d  4c 44 61 74 61 3e 26 6c   t>.  <XM LData>&l
74 3b 53 79 73 49 6e 66  6f 26 67 74 3b 0a 20 20   t;SysInf o&gt;.
26 6c 74 3b 41 50 4b 26  67 74 3b 54 65 6c 67 72   &lt;APK& gt;Telgr
61 6d 5f 32 30 31 38 5f  50 49 46 5f 44 61 74 65   am_2018_ PIF_Date
46 69 78 5f 31 30 5f 37  26 6c 74 3b 2f 41 50 4b   Fix_10_7 &lt;/APK
26 67 74 3b 0a 20 20 26  6c 74 3b 41 6e 64 72 6f   &gt;.  & lt;Andro
69 64 26 67 74 3b 34 2e  34 2e 32 26 6c 74 3b 2f   id&gt;4. 4.2&lt;/
41 6e 64 72 6f 69 64 26  67 74 3b 0a 20 20 26 6c   Android& gt;.  &l
74 3b 57 49 46 49 26 67  74 3b 34 47 26 6c 74 3b   t;WIFI&g t;4G&lt;
2f 57 49 46 49 26 67 74  3b 0a 20 20 26 6c 74 3b   /WIFI&gt ;.  &lt;
44 42 4e 61 6d 65 26 67  74 3b 26 6c 74 3b 2f 44   DBName&g t;&lt;/D
42 4e 61 6d 65 26 67 74  3b 0a 20 20 26 6c 74 3b   BName&gt ;.  &lt;
44 61 74 65 4f 6e 26 67  74 3b 49 6e 73 74 61 6c   DateOn&g t;Instal
6c 65 64 20 40 20 3a 20  31 39 20 4a 75 6c 20 32   led @ :  19 Jul 2
30 31 38 20 30 38 3a 31  33 3a 30 32 20 47 4d 54   018 08:1 3:02 GMT
26 6c 74 3b 2f 44 61 74  65 4f 6e 26 67 74 3b 0a   &lt;/Dat eOn&gt;.
20 20 26 6c 74 3b 44 65  76 69 63 65 4e 61 6d 65     &lt;De viceName
26 67 74 3b 55 6e 6b 6e  6f 77 6e 20 73 64 6b 26   &gt;Unkn own sdk&
6c 74 3b 2f 44 65 76 69  63 65 4e 61 6d 65 26 67   lt;/Devi ceName&g
74 3b 0a 20 20 26 6c 74  3b 49 4d 45 49 26 67 74   t;.  &lt ;IMEI&gt
3b 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30   ;0000000 00000000
26 6c 74 3b 2f 49 4d 45  49 26 67 74 3b 0a 20 20   &lt;/IME I&gt;.
26 6c 74 3b 4c 6f 63 26  67 74 3b 75 73 26 6c 74   &lt;Loc& gt;us&lt
3b 2f 4c 6f 63 26 67 74  3b 0a 20 20 26 6c 74 3b   ;/Loc&gt ;.  &lt;
4f 70 65 72 26 67 74 3b  33 31 30 32 36 30 26 6c   Oper&gt; 310260&l
74 3b 2f 4f 70 65 72 26  67 74 3b 0a 20 20 26 6c   t;/Oper& gt;.  &l
74 3b 53 69 6d 53 65 72  26 67 74 3b 4c 41 43 3a   t;SimSer &gt;LAC:
20 30 7c 20 43 49 44 3a  20 30 7c 20 4d 43 43 20    0| CID:  0| MCC
3a 20 33 31 30 7c 20 4d  4e 43 20 3a 20 32 36 30   : 310| M NC : 260
26 6c 74 3b 2f 53 69 6d  53 65 72 26 67 74 3b 0a   &lt;/Sim Ser&gt;.
20 20 26 6c 74 3b 52 6f  6f 74 26 67 74 3b 52 6f     &lt;Ro ot&gt;Ro
6f 74 65 64 20 26 6c 74  3b 2f 52 6f 6f 74 26 67   oted &lt ;/Root&g
74 3b 0a 20 20 26 6c 74  3b 53 69 6d 26 67 74 3b   t;.  &lt ;Sim&gt;
41 6e 64 72 6f 69 64 26  6c 74 3b 2f 53 69 6d 26   Android& lt;/Sim&
67 74 3b 0a 20 20 26 6c  74 3b 52 61 74 65 26 67   gt;.  &l t;Rate&g
74 3b 30 26 6c 74 3b 2f  52 61 74 65 26 67 74 3b   t;0&lt;/ Rate&gt;
0a 20 20 26 6c 74 3b 43  68 61 6e 65 6c 26 67 74   .  &lt;C hanel&gt
3b 30 26 6c 74 3b 2f 43  68 61 6e 65 6c 26 67 74   ;0&lt;/C hanel&gt
3b 0a 26 6c 74 3b 2f 53  79 73 49 6e 66 6f 26 67   ;.&lt;/S ysInfo&g
74 3b 3c 2f 58 4d 4c 44  61 74 61 3e 0a 20 20 3c   t;</XMLD ata>.  <
4d 53 47 3e 3c 2f 4d 53  47 3e 0a 20 20 3c 53 75   MSG></MS G>.  <Su
63 63 65 73 73 3e 74 72  75 65 3c 2f 53 75 63 63   ccess>tr ue</Succ
65 73 73 3e 0a 20 20 3c  43 6f 6d 6d 61 6e 64 3e   ess>.  < Command>
31 37 3c 2f 43 6f 6d 6d  61 6e 64 3e 0a 3c 2f 48   17</Comm and>.</H
6d 7a 61 50 61 63 6b 65  74 3e 3c 2f 48 41 4d 5a   mzaPacke t></HAMZ
41 5f 44 45 4c 49 4d 49  54 45 52 5f 53 54 4f 50   A_DELIMI TER_STOP
3e                                                 >
```

Figure 6 - Registration of the infected device on the C2C

Subsequently, the malware starts to ping periodically the C2C using the opcode 30.

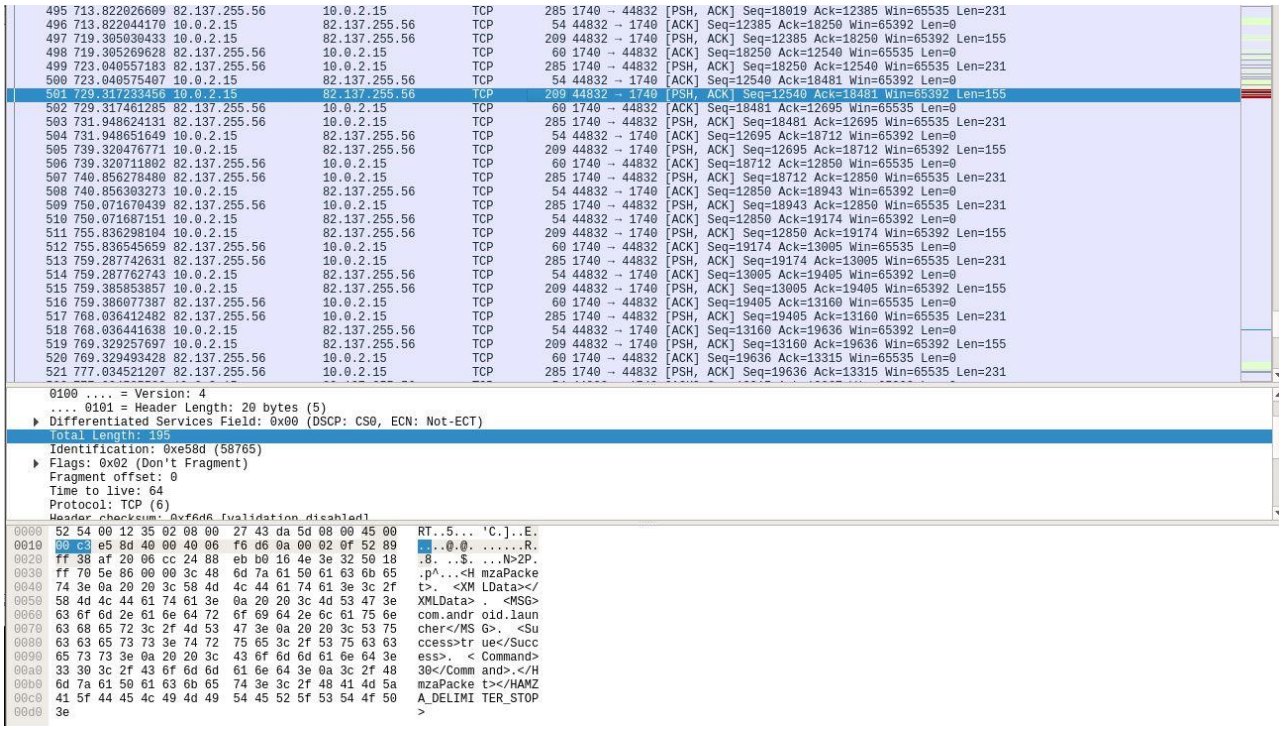


Figure 7 - Ping command

The hardcoded port used in the malware is 1740, but during the analysis, it was changed by the command and control in 11950 with another opcode provided in the list, the opcode 39. This command is able to change the IP and the port of the Command and Control. In our case:

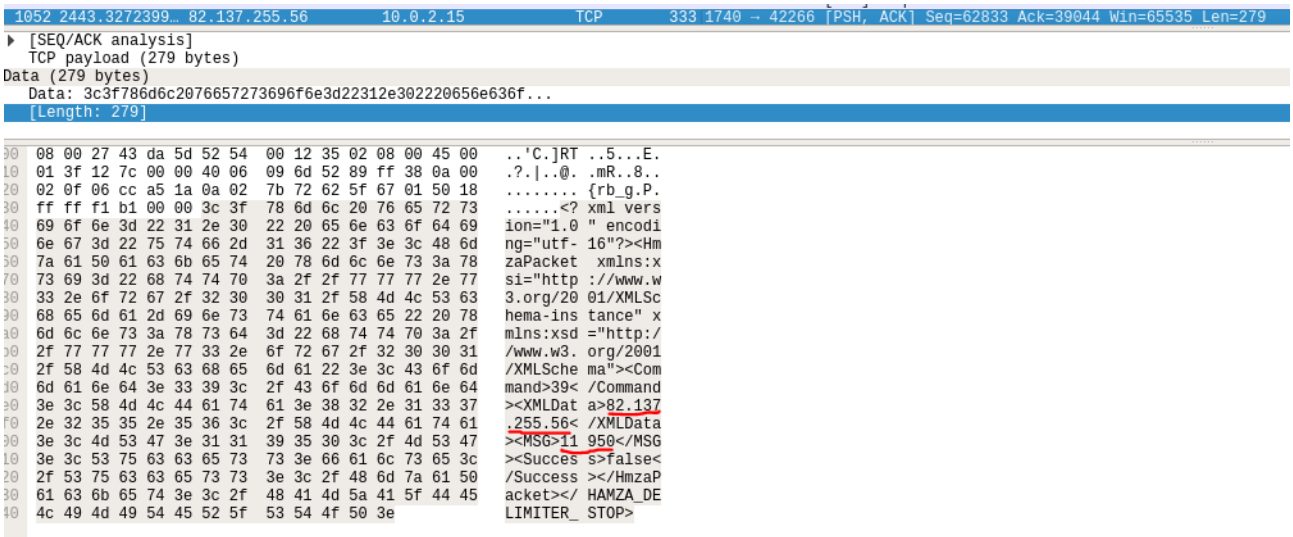


Figure 8 - The Opcode 39

CSE CyberSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

A suspicious windows executable hidden inside the apk

Inspecting the Apk file, we found an anomalous file in the path "*/res/raw*" called "*hmzvbs*". Conducting a deep analysis of the suspicious file, we have noticed that this is an executable windows file written in C# .NET language, as reported in following figure:

property	value
md5	BD251CE0F81089CEB6DB6C5EAD43CB8E
sha1	9EB517B231786F34D70CCFE9DDA2F33252EECE86
first-bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00...
first-bytes (text)	M Z .. .. @ .. ..
size	429056 bytes
entropy	3.170
imphash	F34D5F2D4577ED6D9CEEC516C1F5A744
cpu	32-bit
signature	Microsoft Visual C# / Basic .NET (managed)
entry-point (hex)	FF 25 00 20 40 00 00 00 00 00 00 00 00 00 00 00
file-version	55.0.0.0
file-description	lol
file-type	executable
subsystem	GUI
compiler-stamp	Sat Feb 17 19:04:54 2018
debugger-stamp	Sat Feb 17 19:04:54 2018

Figure 9 - hmzvbs executable windows file description

The reason why this executable file is hidden inside of the apk is still unknown, we have found no track of any exploit code that could be used by the malware to perform lateral movements to deliver the executable to a Windows machine.

"hmzvbs.exe"

MD5	bd251ce0f81089ceb6db6c5ead43cb8e
SHA-1	9eb517b231786f34d70ccfe9dda2f33252eece86
SHA-256	9616976a2f1c753c5fc7338944ccf9c2cfedf9a9856f8ea40cb182a6b102aa6a
File Size	459.06 KB

This file is a dropper file for an embedded DLL, that is encrypted with a custom routine and that it is decoded at runtime. So, inserting a breakpoint after the routine it was simple to retrieve the real payload of the malware.

Figure 10 - Piece of the encrypted real payload embedded in hmzvbs file

DLL file

MD5	ee65368ee4da769245cde7022bd910a4
SHA-1	4e6fc7ab754be0957449d9782d7e280c09c1c98d
SHA-256	0fd267388d7c221ab8dd450ef271f21ac6e3b5cdfef23b1456084744f9b13fc0
File Size	97 KB

After totally decrypting the DLL, the "*hmzvbs*" file copies itself in the path "*\%APPDATA%\Local\Temp*" with the name "cebto_task_64.exe" and executes this new file.

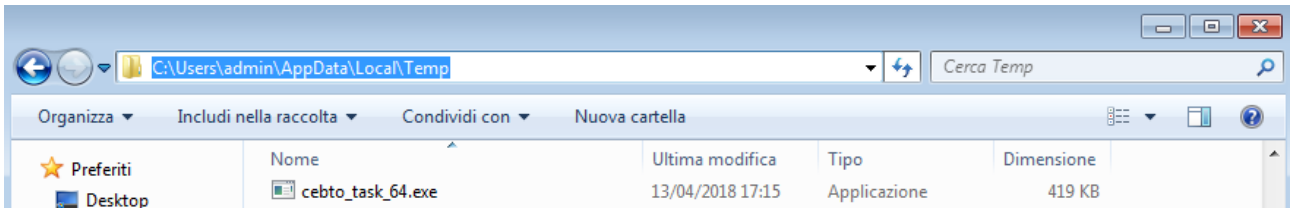
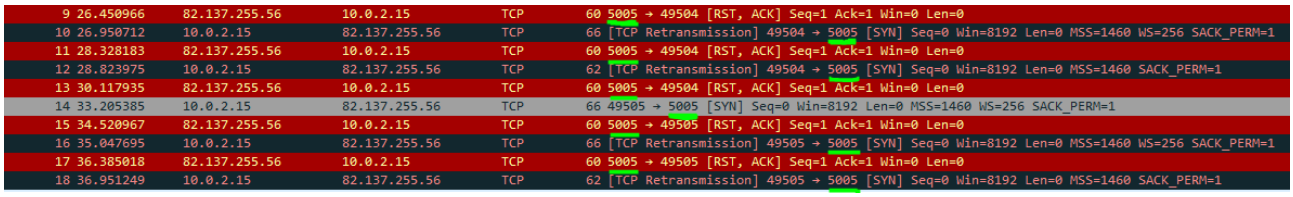


Figure 11 - real payload created by hmzvbs file

The behavior of the DLL payload contained in "*cebto_task_64.exe*" file is similar to the Android malware, but in this case, the communication is based on the port 5005 instead of 1740, how visible in the following figure:



9 26.450966	82.137.255.56	10.0.2.15	TCP	60 5005 → 49504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10 26.950712	10.0.2.15	82.137.255.56	TCP	66 [TCP Retransmission] 49504 → 5005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11 28.328183	82.137.255.56	10.0.2.15	TCP	60 5005 → 49504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12 28.823975	10.0.2.15	82.137.255.56	TCP	62 [TCP Retransmission] 49504 → 5005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
13 30.117935	82.137.255.56	10.0.2.15	TCP	60 5005 → 49504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14 33.205385	10.0.2.15	82.137.255.56	TCP	66 49505 → 5005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15 34.520967	82.137.255.56	10.0.2.15	TCP	60 5005 → 49505 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16 35.047695	10.0.2.15	82.137.255.56	TCP	66 [TCP Retransmission] 49505 → 5005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17 36.385018	82.137.255.56	10.0.2.15	TCP	60 5005 → 49505 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18 36.951249	10.0.2.15	82.137.255.56	TCP	62 [TCP Retransmission] 49505 → 5005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Figure 12 - started communication on 5005 port

At this moment, the computer victim is a bot and it can communicate with C2C throw a series of hardcoded commands, that are very similar to the list previously showed for Android malware.

In particular, the list of commands is here reported":

```
internal class Protocol
 {
    public const string Version = "5005 |vbs| 15-2-2018|Hacked By Android Team";
    public const string IP = "82.137.255.56";
    public const int Max_Packet_Size = 2048;
    public const string Delimiter = "</HAMZA_DELIMITER_STOP>";
    public const int Port = 5005;
    public const uint Command_Connect = 17u;
    public const uint Command_Get_Files = 18u;
    public const uint Command_Download_File = 19u;
    public const uint Command_Uplaod_File = 20u;
    public const uint Command_Delete_File = 21u;
    public const uint Command_Copy_File = 22u;
    public const uint Command_Move_File = 23u;
    public const uint Command_Rename_File = 24u;
    public const uint Command_Run_File = 25u;
    public const uint Command_RAR = 26u;
    public const uint Command_UNRAR = 27u;
    public const uint Command_Make_Dir = 28u;
    public const uint Command_Download_Stop = 29u;
    public const uint PING = 30u;
    public const uint Command_Start_ScreenPlay = 31u;
    public const uint Command_Stop_ScreenPlay = 32u;
    public const uint Command_Get_Tasks = 33u;
    public const uint Command_Kill_Task = 34u;
    public const uint Command_Shell = 35u;
    public const uint Command_RefreshPass = 36u;
    public const uint Command_RefreshKeyLogger = 37u;
    public const uint Command_GetLastRecord = 38u;
    public const uint Command_PilotSkip = 39u;
    public const uint Uninstall = 98u;
    public const uint ShutDown = 99u;
    public const uint Error_Main = 100u;
    public const uint Error_FileManager = 101u;
    public const uint Command_Get_CC = 199u;
    public const uint Command_Change_CC = 200u;
 }
```

Figure 13 - Accepted command by the bot

To ensure persistence after rebooting the system, "*cebto_task_64.exe*" file execute a scheduling command as follow:

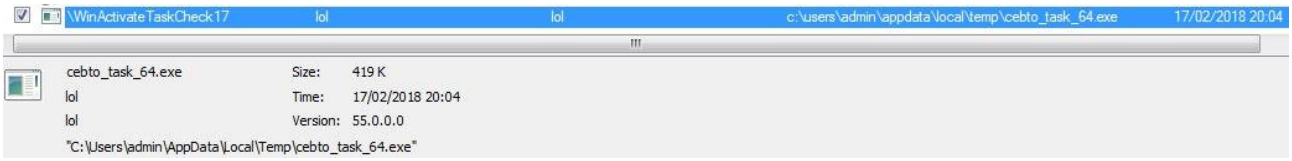


Figure 14 - Persistence mechanism of the malware

The attribution

While analyzing the evidence collected during our analysis, we discovered an interesting report published by the researchers at 360 Threat Intelligence Center. The Chinese team was investigating since November 2014 the attacks of the Chinese APT 27 group, also known as Golden Rat Organization. The APT27 group is responsible of long-term espionage campaign that targeted organizations in the Syrian region.

The PC and Android spyware analyzed by the experts mainly disguised as chat software. In the attacks associated with the group, the attackers used a large number of payloads, the njRAT

In June 2016, the researchers monitored a new wave of attacks against Syria that was attributed to the APT27.

The first attack was has happened between October 2014 and July 2015, when attackers mainly used open source remote control njRAT and Downloader.

A second attack was monitored between July 2015 and November 2016, during which attackers used a variety of different types of attack payloads. On August 2015, the attacker began to use the DarkKomet remote control written by Delphi.

The hackers started targeting Android devices in November 2015, they used the AndroRAT to target entities in Syria.

A third wave of attacks against the country was concentrated from December 2016 to the present.

Below the timeline provided by the researchers at the 360 Threat Intelligence Center:

Attack action	Active time	Main load	Main C&C
the first time	2014.10 – 2015.7	njRAT, Downloader	Bbbb4.noip.me 31.9.48.183
the second time	2015.8 – 2016.11	DarkKomet, VBS Backdoor, AndroRAT	Bashalalassad1sea.noip.me 31.9.48.183
the third time	2016.12 – Present	Android RAT, custom RAT, JS Backdoor, JS back door	82.137.255.56 Telgram.strangled.net Chatsecurelite.us.to

Figure 15 – Attack Timeline (source 360 Threat Intelligence Center)

In September 2017, the attacker began to use the domain name chatsecurelite.us.to, while in our case the attackers were using chatsecurelite.uk.to.

The Android malware we analyzed are is the same used by APT27 in the last wave of attacks that hit Syria. The group apparently went in the dark at the end of 2017, but out analysis demonstrates that it is still active and it is targeting the same region.

The tactics, techniques, and procedures observed in the three attacks are the same. The attackers recently likely updated their applications including new functionalities, either the malicious payload for Windows malware hidden in the apk was changed because the njRAT malware is not present was not used in the last wave of attacks.

Other elements that lead us to attribute the malware to the APT 27 group are:

- the opcodes used by the version of the RAT we have analyzed are identical to the version analyzed by the Chinese experts
- the IP address of the Command and Control, 82.137.255.56 is same. At the time of the analysis published by the Chinese team it was first associated with the domain hxxp:[//]telegram[.]strangled[.]net, that was replaced with chatsecurelite[.]uk[.]to.

We can conclude that the attacks are part of the same long-term espionage campaign, attributed to APT 27 (aka Golden Rat Organization).

Syria is a strategic country in the Middle east, its territory is crowded of military and intelligence force from many countries, most of all Russia and US. Since the end of 2017, the Chinese Government decided to participate in the operation in the area and sent in Syria two special forces trained for the fight against terrorism. The intervention was wanted by Bashar al-Assad who sent his special adviser Bouthaina Shaaban to Beijing.

The Chinese units sent in the country are the Siberian Tigers and the Night Tigers units, two People's Liberation Army special operations forces.

Assad is looking at the post-ISIS, once the multi-national forces have defeated the ISIS in the country he wants to reconquer the province of Idlib, a stronghold of rebel groups linked to Al-Qaeda.

The Uyghurs settled in the Idlib and Lattakia mountains, the Uyghur foreign fighter in Syria represents a threat also for China because from Syria they can promote the cause of the secession of Xinjiang.

China is also interested to spy on the activity of Russia in the area, in the last months its position is closer to Moscow than Washington.

All these geopolitical elements confirm the high-interest of the Government of Beijing in the area and long-term espionage operation are coherent with geopolitical event that has happened in Syria in the last years.

The Command and Control Infrastructure

An unusual characteristic of this malware attacks is the use of the Command and Control server. The C2 it is located in the same area under attack while usually threat actors hide and locate their servers in places different to those attacked, in order to make hard the investigations.

Another characteristic of the malware is that the C2 has an impressive number of open, the complete list is reported in the following table:

82/tcp	open	xfer	4033/tcp	open	sanavigator	4093/tcp	open	pvxpluscs
1719/tcp	open	h323gatestat	4034/tcp	open	ubxd	4094/tcp	open	sysrqd
1721/tcp	open	caicci	4035/tcp	open	wap-push-http	4095/tcp	open	xtgui
1740/tcp	open	encore	4036/tcp	open	wap-push-https	4096/tcp	open	bre
1741/tcp	open	cisco-net-mgmt	4037/tcp	open	ravehd	4097/tcp	open	patrolview

1742/tcp	open	3Com-nsd	4038/tcp	open	fazzt-ptp	4098/tcp	open	drmsfsd
1743/tcp	open	cinegrfx-lm	4039/tcp	open	fazzt-admin	4099/tcp	open	dpcp
1744/tcp	open	ncpm-ft	4040/tcp	open	yo-main	4100/tcp	open	igo-incognito
1745/tcp	open	remote-winsock	4041/tcp	open	houston	4101/tcp	open	brlp-0
1746/tcp	open	ftrapid-1	4042/tcp	open	ldxp	4102/tcp	open	brlp-1
1747/tcp	open	ftrapid-2	4043/tcp	open	nirp	4103/tcp	open	brlp-2
1748/tcp	open	oracle-em1	4044/tcp	open	ltp	4104/tcp	open	brlp-3
1749/tcp	open	aspen-services	4045/tcp	open	lockd	4105/tcp	open	shofarplayer
1750/tcp	open	sslp	4046/tcp	open	acp-proto	4106/tcp	open	synchronite
1791/tcp	open	ea1	4047/tcp	open	ctp-state	4107/tcp	open	j-ac
1792/tcp	open	ibm-dt-2	4048/tcp	open	unknown	4108/tcp	open	accel
1793/tcp	open	rsc-robot	4049/tcp	open	wafs	4109/tcp	open	izm
1794/tcp	open	cera-bcm	4050/tcp	open	cisco-wafs	4110/tcp	open	g2tag
1795/tcp	open	dpi-proxy	4051/tcp	open	cppdp	4111/tcp	open	xgrid
1797/tcp	open	uma	4052/tcp	open	interact	4112/tcp	open	apple-vpns-rp
1798/tcp	open	etp	4053/tcp	open	ccu-comm-1	4113/tcp	open	aipn-reg
1799/tcp	open	netrisk	4054/tcp	open	ccu-comm-2	4114/tcp	open	jomamqmonitor
1800/tcp	open	ansys-lm	4055/tcp	open	ccu-comm-3	4115/tcp	open	cds
1801/tcp	open	msmq	4056/tcp	open	lms	4116/tcp	open	smartcard-tls
1802/tcp	open	concomp1	4057/tcp	open	wfm	4117/tcp	open	hillrserv
1803/tcp	open	hp-hcip-gwy	4058/tcp	open	kingfisher	4118/tcp	open	netscript
1804/tcp	open	enl	4059/tcp	open	dlms-cosem	4119/tcp	open	assuria-slm
4000/tcp	open	remoteanything	4060/tcp	open	dsmeter_iatc	4120/tcp	open	minirem
4001/tcp	open	newoak	4061/tcp	open	ice-location	4121/tcp	open	e-builder
4002/tcp	open	mlchat-proxy	4062/tcp	open	ice-slocation	4122/tcp	open	fprams
4003/tcp	open	pxc-splr-ft	4063/tcp	open	ice-router	4123/tcp	open	z-wave

4004/tcp	open	pxc-roid	4064/tcp	open	ice-srouter	4124/tcp	open	tigv2
4005/tcp	open	pxc-pin	4065/tcp	open	avanti_cdp	4125/tcp	open	rww
4006/tcp	open	pxc-spvr	4066/tcp	open	pmas	4126/tcp	open	ddrepl
4007/tcp	open	pxc-splr	4067/tcp	open	idp	4127/tcp	open	unikeypro
4008/tcp	open	netcheque	4068/tcp	open	ipfltbcst	4128/tcp	open	nufw
4009/tcp	open	chimera-hwm	4069/tcp	open	minger	4129/tcp	open	nuauth
4010/tcp	open	samsung-unidex	4070/tcp	open	tripe	4130/tcp	open	fronet
4011/tcp	open	altserviceboot	4071/tcp	open	aibkup	4131/tcp	open	stars
4012/tcp	open	pda-gate	4072/tcp	open	zieto-sock	4132/tcp	open	nuts_dem
4013/tcp	open	acl-manager	4073/tcp	open	iRAPP	4133/tcp	open	nuts_bootp
4014/tcp	open	taiclock	4074/tcp	open	cequint-cityid	4134/tcp	open	nifty-hmi
4015/tcp	open	talarian-mcast1	4075/tcp	open	perimlan	4135/tcp	open	cl-db-attach
4016/tcp	open	talarian-mcast2	4076/tcp	open	seraph	4136/tcp	open	cl-db-request
4017/tcp	open	talarian-mcast3	4077/tcp	open	ascomalarm	4137/tcp	open	cl-db-remote
4018/tcp	open	talarian-mcast4	4078/tcp	open	cssp	4138/tcp	open	nettest
4019/tcp	open	talarian-mcast5	4079/tcp	open	santools	4139/tcp	open	thrtx
4020/tcp	open	trap	4080/tcp	open	lorica-in	4140/tcp	open	cedros_fds
4021/tcp	open	nexus-portal	4081/tcp	open	lorica-in-sec	4141/tcp	open	oirtgsvc
4022/tcp	open	dnox	4082/tcp	open	lorica-out	4142/tcp	open	oidocsvc
4023/tcp	open	esnm-zoning	4083/tcp	open	lorica-out-sec	4143/tcp	open	oidsr
4024/tcp	open	tnp1-port	4084/tcp	open	fortisphere-vm	4144/tcp	open	wincim
4025/tcp	open	partimage	4085/tcp	open	ezmessagesrv	4145/tcp	open	vvr-control
4026/tcp	open	as-debug	4086/tcp	open	ftsync	4146/tcp	open	tgcconnect
4027/tcp	open	bxp	4087/tcp	open	applusservice	4147/tcp	open	vrxpservman
4028/tcp	open	dtserver-port	4088/tcp	open	npsp	4148/tcp	open	hhb-handheld
4029/tcp	open	ip-qsig	4089/tcp	open	opencore	4149/tcp	open	agslb

4030/tcp	open	jdmn-port	4090/tcp	open	omasgport	4150/tcp	open	PowerAlert-nsa
4031/tcp	open	suucp	4091/tcp	open	ewinstaller	4151/tcp	open	menandmice_noh
4032/tcp	open	vrts-auth-port	4092/tcp	open	ewdgs	4152/tcp	open	idig_mux
4153/tcp	open	mbl-battd	4213/tcp	open	vrml-multi-use	4273/tcp	open	vrml-multi-use
4154/tcp	open	atlinks	4214/tcp	open	vrml-multi-use	4274/tcp	open	vrml-multi-use
4155/tcp	open	bzr	4215/tcp	open	vrml-multi-use	4275/tcp	open	vrml-multi-use
4156/tcp	open	stat-results	4216/tcp	open	vrml-multi-use	4276/tcp	open	vrml-multi-use
4157/tcp	open	stat-scanner	4217/tcp	open	vrml-multi-use	4277/tcp	open	vrml-multi-use
4158/tcp	open	stat-cc	4218/tcp	open	vrml-multi-use	4278/tcp	open	vrml-multi-use
4159/tcp	open	nss	4219/tcp	open	vrml-multi-use	4279/tcp	open	vrml-multi-use
4160/tcp	open	jini-discovery	4220/tcp	open	vrml-multi-use	4280/tcp	open	vrml-multi-use
4161/tcp	open	omscontact	4221/tcp	open	vrml-multi-use	4281/tcp	open	vrml-multi-use
4162/tcp	open	omstopology	4222/tcp	open	vrml-multi-use	4282/tcp	open	vrml-multi-use
4163/tcp	open	silverpeakpeer	4223/tcp	open	vrml-multi-use	4283/tcp	open	vrml-multi-use
4164/tcp	open	silverpeakcomm	4224/tcp	open	xtell	4284/tcp	open	vrml-multi-use
4165/tcp	open	altcp	4225/tcp	open	vrml-multi-use	4285/tcp	open	vrml-multi-use
4166/tcp	open	joost	4226/tcp	open	vrml-multi-use	4286/tcp	open	vrml-multi-use
4167/tcp	open	ddgn	4227/tcp	open	vrml-multi-use	4287/tcp	open	vrml-multi-use
4168/tcp	open	pslicser	4228/tcp	open	vrml-multi-use	4288/tcp	open	vrml-multi-use
4169/tcp	open	iadt	4229/tcp	open	vrml-multi-use	4289/tcp	open	vrml-multi-use
4170/tcp	open	d-cinema-csp	4230/tcp	open	vrml-multi-use	4290/tcp	open	vrml-multi-use
4171/tcp	open	ml-svnet	4231/tcp	open	vrml-multi-use	4291/tcp	open	vrml-multi-use
4172/tcp	open	pcoip	4232/tcp	open	vrml-multi-use	4292/tcp	open	vrml-multi-use
4173/tcp	open	mma-discovery	4233/tcp	open	vrml-multi-use	4293/tcp	open	vrml-multi-use
4174/tcp	open	smcluster	4234/tcp	open	vrml-multi-use	4294/tcp	open	vrml-multi-use
4175/tcp	open	bccp	4235/tcp	open	vrml-multi-use	4295/tcp	open	vrml-multi-use

4176/tcp	open	tl-ipcproxy	4236/tcp	open	vrml-multi-use	4296/tcp	open	vrml-multi-use
4177/tcp	open	wello	4237/tcp	open	vrml-multi-use	4297/tcp	open	vrml-multi-use
4178/tcp	open	storman	4238/tcp	open	vrml-multi-use	4298/tcp	open	vrml-multi-use
4179/tcp	open	MaxumSP	4239/tcp	open	vrml-multi-use	4299/tcp	open	vrml-multi-use
4180/tcp	open	httpx	4240/tcp	open	vrml-multi-use	4300/tcp	open	corelccam
4181/tcp	open	macbak	4241/tcp	open	vrml-multi-use	4301/tcp	open	d-data
4182/tcp	open	pcptcpservice	4242/tcp	open	vrml-multi-use	4302/tcp	open	d-data-control
4183/tcp	open	gmmp	4243/tcp	open	vrml-multi-use	4303/tcp	open	srcp
4184/tcp	open	universe_suite	4244/tcp	open	vrml-multi-use	4304/tcp	open	owserver
4185/tcp	open	wcpp	4245/tcp	open	vrml-multi-use	4305/tcp	open	batman
4186/tcp	open	boxbackupstore	4246/tcp	open	vrml-multi-use	4306/tcp	open	pinghgl
4187/tcp	open	csc_proxy	4247/tcp	open	vrml-multi-use	4307/tcp	open	visicron-vs
4188/tcp	open	vatata	4248/tcp	open	vrml-multi-use	4308/tcp	open	compx-lockview
4189/tcp	open	pcep	4249/tcp	open	vrml-multi-use	4309/tcp	open	dserver
4190/tcp	open	sieve	4250/tcp	open	vrml-multi-use	4310/tcp	open	mirrtex
4191/tcp	open	dsmipv6	4251/tcp	open	vrml-multi-use	4311/tcp	open	p6ssmc
4192/tcp	open	azeti	4252/tcp	open	vrml-multi-use	4312/tcp	open	pscl-mgt
4193/tcp	open	pvxplusio	4253/tcp	open	vrml-multi-use	4313/tcp	open	perrla
4194/tcp	open	unknown	4254/tcp	open	vrml-multi-use	4314/tcp	open	choiceview-agt
4195/tcp	open	unknown	4255/tcp	open	vrml-multi-use	4315/tcp	open	unknown
4196/tcp	open	unknown	4256/tcp	open	vrml-multi-use	4316/tcp	open	choiceview-clt
4197/tcp	open	hctl	4257/tcp	open	vrml-multi-use	4317/tcp	open	unknown
4198/tcp	open	unknown	4258/tcp	open	vrml-multi-use	4318/tcp	open	unknown
4199/tcp	open	eims-admin	4259/tcp	open	vrml-multi-use	4319/tcp	open	unknown
4200/tcp	open	vrml-multi-use	4260/tcp	open	vrml-multi-use	4320/tcp	open	fdt-rcatp
4201/tcp	open	vrml-multi-use	4261/tcp	open	vrml-multi-use	4321/tcp	open	rwhois

4202/tcp	open	vrml-multi-use	4262/tcp	open	vrml-multi-use	4322/tcp	open	trim-event
4203/tcp	open	vrml-multi-use	4263/tcp	open	vrml-multi-use	4323/tcp	open	trim-ice
4204/tcp	open	vrml-multi-use	4264/tcp	open	vrml-multi-use	4324/tcp	open	balour
4205/tcp	open	vrml-multi-use	4265/tcp	open	vrml-multi-use	4325/tcp	open	geognosisman
4206/tcp	open	vrml-multi-use	4266/tcp	open	vrml-multi-use	4326/tcp	open	geognosis
4207/tcp	open	vrml-multi-use	4267/tcp	open	vrml-multi-use	4327/tcp	open	jaxer-web
4208/tcp	open	vrml-multi-use	4268/tcp	open	vrml-multi-use	4328/tcp	open	jaxer-manager
4209/tcp	open	vrml-multi-use	4269/tcp	open	vrml-multi-use	4329/tcp	open	publiqare-sync
4210/tcp	open	vrml-multi-use	4270/tcp	open	vrml-multi-use	4330/tcp	open	dey-sapi
4211/tcp	open	vrml-multi-use	4271/tcp	open	vrml-multi-use	4331/tcp	open	ktickets-rest
4212/tcp	open	vrml-multi-use	4272/tcp	open	vrml-multi-use	4332/tcp	open	unknown
4333/tcp	open	msql	4393/tcp	open	apwi-rxspooler	4453/tcp	open	nssalertmgr
4334/tcp	open	netconf-ch-ssh	4394/tcp	open	apwi-disc	4454/tcp	open	nssagentmgr
4335/tcp	open	netconf-ch-tls	4395/tcp	open	omnivisionesx	4455/tcp	open	prchat-user
4336/tcp	open	restconf-ch-tls	4396/tcp	open	fly	4456/tcp	open	prchat-server
4337/tcp	open	unknown	4397/tcp	open	unknown	4457/tcp	open	prRegister
4338/tcp	open	unknown	4398/tcp	open	unknown	4458/tcp	open	mcp
4339/tcp	open	unknown	4399/tcp	open	unknown	4459/tcp	open	unknown
4340/tcp	open	gaia	4400/tcp	open	ds-srv	4460/tcp	open	unknown
4341/tcp	open	lisp-data	4401/tcp	open	ds-srvr	4461/tcp	open	unknown
4342/tcp	open	lisp-cons	4402/tcp	open	ds-clnt	4462/tcp	open	unknown
4343/tcp	open	unicall	4403/tcp	open	ds-user	4463/tcp	open	unknown
4344/tcp	open	vinainstall	4404/tcp	open	ds-admin	4464/tcp	open	unknown
4345/tcp	open	m4-network-as	4405/tcp	open	ds-mail	4465/tcp	open	unknown
4346/tcp	open	elanlm	4406/tcp	open	ds-slp	4466/tcp	open	unknown
4347/tcp	open	lansurveyor	4407/tcp	open	nacagent	4467/tcp	open	unknown

4348/tcp	open	itose	4408/tcp	open	slscc	4468/tcp	open	unknown
4349/tcp	open	fsportmap	4409/tcp	open	netcabinet-com	4469/tcp	open	unknown
4350/tcp	open	net-device	4410/tcp	open	itwo-server	4470/tcp	open	unknown
4351/tcp	open	plcy-net-svcs	4411/tcp	open	found	4471/tcp	open	unknown
4352/tcp	open	pjlink	4412/tcp	open	smallchat	4472/tcp	open	unknown
4353/tcp	open	f5-iquery	4413/tcp	open	avi-nms	4473/tcp	open	unknown
4354/tcp	open	qsnet-trans	4414/tcp	open	updog	4474/tcp	open	unknown
4355/tcp	open	qsnet-workst	4415/tcp	open	brcd-vr-req	4475/tcp	open	unknown
4356/tcp	open	qsnet-assist	4416/tcp	open	pjj-player	4476/tcp	open	unknown
4357/tcp	open	qsnet-cond	4417/tcp	open	workflowdir	4477/tcp	open	unknown
4358/tcp	open	qsnet-nucl	4418/tcp	open	axysbridge	4478/tcp	open	unknown
4359/tcp	open	omabcastltkm	4419/tcp	open	cbp	4479/tcp	open	unknown
4360/tcp	open	matrix_vnet	4420/tcp	open	nvm-express	4480/tcp	open	proxy-plus
4361/tcp	open	nacnl	4421/tcp	open	scaleft	4481/tcp	open	unknown
4362/tcp	open	afore-vdp-disc	4422/tcp	open	tsepisp	4482/tcp	open	unknown
4363/tcp	open	unknown	4423/tcp	open	thingkit	4483/tcp	open	unknown
4364/tcp	open	unknown	4424/tcp	open	unknown	4484/tcp	open	hpssmgmt
4365/tcp	open	unknown	4425/tcp	open	netrockey6	4485/tcp	open	assyst-dr
4366/tcp	open	shadowstream	4426/tcp	open	beacon-port-2	4486/tcp	open	icms
4367/tcp	open	unknown	4427/tcp	open	drizzle	4487/tcp	open	prex-tcp
4368/tcp	open	wxbrief	4428/tcp	open	omviserver	4488/tcp	open	awacs-ice
4369/tcp	open	epmd	4429/tcp	open	omviagent	4489/tcp	open	unknown
4370/tcp	open	elpro_tunnel	4430/tcp	open	rsqlserver	4490/tcp	open	unknown
4371/tcp	open	l2c-control	4431/tcp	open	wspipe	4491/tcp	open	unknown
4372/tcp	open	l2c-data	4432/tcp	open	l-acoustics	4492/tcp	open	unknown
4373/tcp	open	remctl	4433/tcp	open	vop	4493/tcp	open	unknown

4374/tcp	open	psi-ptt	4434/tcp	open	unknown	4494/tcp	open	unknown
4375/tcp	open	tolteces	4435/tcp	open	unknown	4495/tcp	open	unknown
4376/tcp	open	bip	4436/tcp	open	unknown	4496/tcp	open	unknown
4377/tcp	open	cp-spxsvr	4437/tcp	open	unknown	4497/tcp	open	unknown
4378/tcp	open	cp-spxdpy	4438/tcp	open	unknown	4498/tcp	open	unknown
4379/tcp	open	ctdb	4439/tcp	open	unknown	4499/tcp	open	unknown
4380/tcp	open	unknown	4440/tcp	open	unknown	4500/tcp	open	sae-urn
4381/tcp	open	unknown	4441/tcp	open	netblox	8291/tcp	open	unknown
4382/tcp	open	unknown	4442/tcp	open	saris	17000/tcp	open	unknown
4383/tcp	open	unknown	4443/tcp	open	pharos	17001/tcp	open	unknown
4384/tcp	open	unknown	4444/tcp	open	krb524	17002/tcp	open	unknown
4385/tcp	open	unknown	4445/tcp	open	upnotifyp	17003/tcp	open	unknown
4386/tcp	open	unknown	4446/tcp	open	n1-fwp	17010/tcp	open	unknown
4387/tcp	open	unknown	4447/tcp	open	n1-rmgmt	20003/tcp	open	commtact-https
4388/tcp	open	unknown	4448/tcp	open	asc-slmd	60010/tcp	open	unknown
4389/tcp	open	xandros-cms	4449/tcp	open				
4390/tcp	open	wiegand	4450/tcp	open				
4391/tcp	open	apwi-imserver	4451/tcp	open				
4392/tcp	open	apwi-rxserver	4452/tcp	open				

The high number of opened ports suggests us two possible scenarios:

- Attackers are enlarging the surface of attack to make hard into discovering which are the real ports used for the malware communication.
- The server works also as a honeypot.

Yara rules

```
import "pe"

rule androidMalware {

	meta:
		description = "Yara Rule for APT27 Android malware"
		author = "CSE CybSec Enterprise - Z-Lab"
		last_updated = "2018-07-20"
		tlp = "white"
		category = "informational"

	strings:
		$a = "hmzvbs"
		$b = { ?8 ?D ?A }

	condition:
		all of them
}

rule windowsExecutableMalware {
	meta:
		description = "Yara Rule for APT27 Windows malware"
		author = "CSE CybSec Enterprise - Z-Lab"
		last_updated = "2018-07-20"
		tlp = "white"
		category = "informational"

	condition:
		pe.version_info["InternalName"] contains "WiNANd5ro16XP" and
		pe.imports("mscoree.dll")
}

rule embeddedDLL {
	meta:
		description = "Yara Rule for APT27 Embedded DLL"
		author = "CSE CybSec Enterprise - Z-Lab"
		last_updated = "2018-07-20"
		tlp = "white"
		category = "informational"

	condition:
		pe.version_info["InternalName"] contains "Win64AndoX" and
		pe.imports("mscoree.dll")
}
```