Syrian Malware, the ever-evolving threat

Kaspersky Lab Global Research and Analysis Team

Version 1.0
August 2014

KASPERSKY lab

1. Executive Summary

The Global Research and Analysis Team (GReAT) at Kaspersky Lab has discovered new malware attacks in Syria, with malicious entities using a plethora of methods from their toolbox to hide and operate malware. In addition to proficient social engineering tricks, victims are often tempted to open and explore malicious files because of the dire need for privacy and security tools in the region. In the hopes of maintaining anonymity and installing the latest "protection", victims fall prey to these malicious creations. A vast majority of the samples obtained were found on activist sites and in social networking forums.

The victims are distributed across different countries:

- Syria
- Lebanon
- Turkey
- Kingdom of Saudi Arabia
- Egypt
- Jordan
- Palestine
- United Arab Emirates
- Israel
- Morocco
- United States

The group members are operating from different locations around the world:

- Syria
- Russian Federation
- Lebanon

The group's attacks are evolving and they are making extensive use of social engineering techniques to trick targeted victims into running their malicious files. Among the principal file extensions observed among the malware samples obtained we can list:

- .exe
- .dll
- .pif
- .scr

The group is relying on RAT (Remote Access Tool) Trojan tools, of which the most common are:

- ShadowTech RAT
- Xtreme RAT
- NjRAT
- Bitcomet RAT
- Dark Comet RAT
- Blackshades RAT

The number of malicious files found is 110, with a big increase seen in recent attacks.

The number of domains linked to the attacks is 20.

The number of IP addresses linked to the attacks is 47.

The samples details and domains lists used by the attackers can be found in the Appendices 1 and 2 in the end of the document.

Protection and resilience against these attacks is ensured through the use of a multi-layered security approach, having up to date security products, and mainly by being sceptical about suspicious files.

Contents

2. Introduction

The geopolitical conflicts in the Middle East have deepened in the last few years; Syria is no exception. The crisis is taking many forms, and the cyberspace conflict is intensifying as sides try to tilt the struggle, by exploiting cyber intelligence and exercising distortion.

In the last few years cyber-attacks in Syria have moved into the front line; many activities in cyberspace have been linked to Syria, especially those conducted by the Syrian Electronic Army and pro-government groups.

The Global Research and Analysis Team (GReAT) at Kaspersky Lab has found new malware attacks in Syria, using new but not advanced techniques to hide and operate malware, in addition to using proficient social engineering tricks to deliver malware by tricking and tempting victims into opening and exploring malicious files. The malware files have been found on hacked activist sites, web pages and in social networking forums.

Cyber Arabs, an Arabic-language digital security project of the IWPR (Institute for War and Peace Reporting), reported four of these samples in March 2014. The same samples were also reported on Syrian Facebook pages (تقنيون لأجل الحرية, Technicians For Freedom): https://www.facebook.com/tech4freedom

Given the complexity of the situation, there are many factors and entities at play in this event, but from the outside these are all largely speculative. Pro-government groups talk about “defense” and opposition activists talk about “offense”. Here, we will only focus on the malware and the facts that have been found during the analysis, presenting only relevant information, in the hope of setting a clear context for this research.

3. Analysis

3.1. Infection Vectors

Malware writers are using multiple techniques to deliver their files and entice the victims to run them, creating an effective infection vector. Mainly depending on social engineering the attackers exploit:

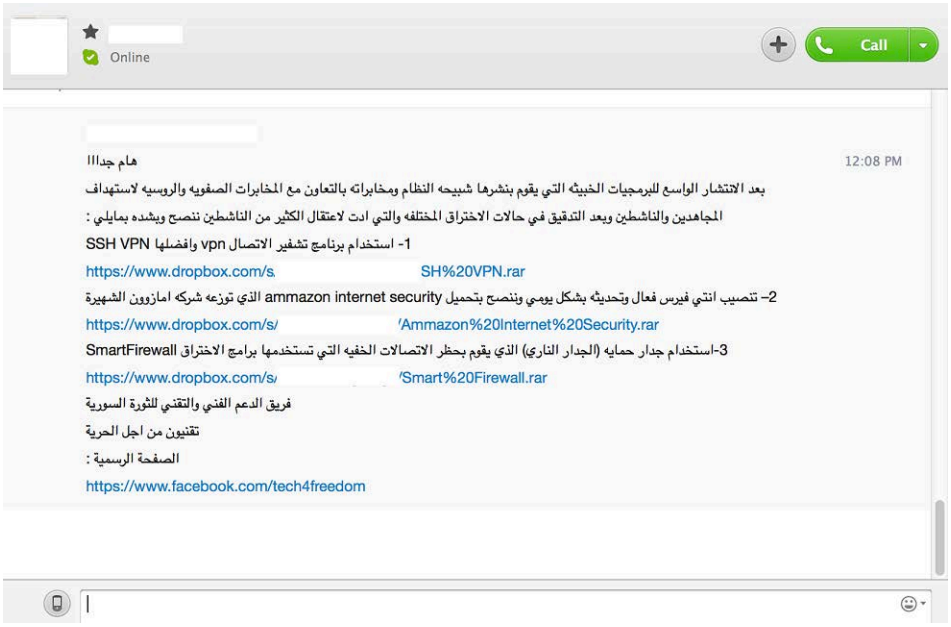
- Victims' trust in social networking forums
- Victims' curiosity in following news related to political conflict in Syria
- Victims' fear of attacks from government
- Victims' lack of technology awareness

Once they have infected the victim's computer, attackers have full access and control over victim's devices. In the following section we show different versions of posts sent via popular file sharing sites or social networking platforms. The sample details and domain lists used by the attackers can be found in the Appendices 1 and 2 in the end of the document.

3.1.1. Skype messages

Messages sent via Skype offer links to download:

1. The "SSH VPN" program to encrypt communication
2. The popular and effective antivirus with daily updates from "Ammazon Internet Security"
3. The "SmartFirewall" to block connections made by malware and bad programs



The messages are usually sent from fake or compromised accounts.

3.1.2. Facebook posts

The same messages sent via Skype are also shared via the Facebook social platform, asking victims to install these “security programs” to protect themselves from malware infections and cyber-attacks, especially government attacks.

3.1.3. YouTube Videos

In the following example, we can see a YouTube video providing links to download fake Whatsapp and Viber applications for PC. By using everyday technologies that are commonly used by a broad audience, attackers increase the effectiveness of their operations and their infection rates.

3.2. Samples and types of files

Analysis has led us to identify the following RAT variants being used in the wild:

- ShadowTech RAT
- Xtreme RAT
- NjRAT
- Bitcomet RAT
- Dark Comet RAT
- BlackShades RAT

The samples collected during our research can be classified as follows.

Old samples

Samples obtained during 2013 are simple RAT executable files, compressed and sent to victims using a wide range of delivery options. Newer samples were typically found to use ".scr" containers in order to hide malicious files and avoid early detection by security solutions.

New samples

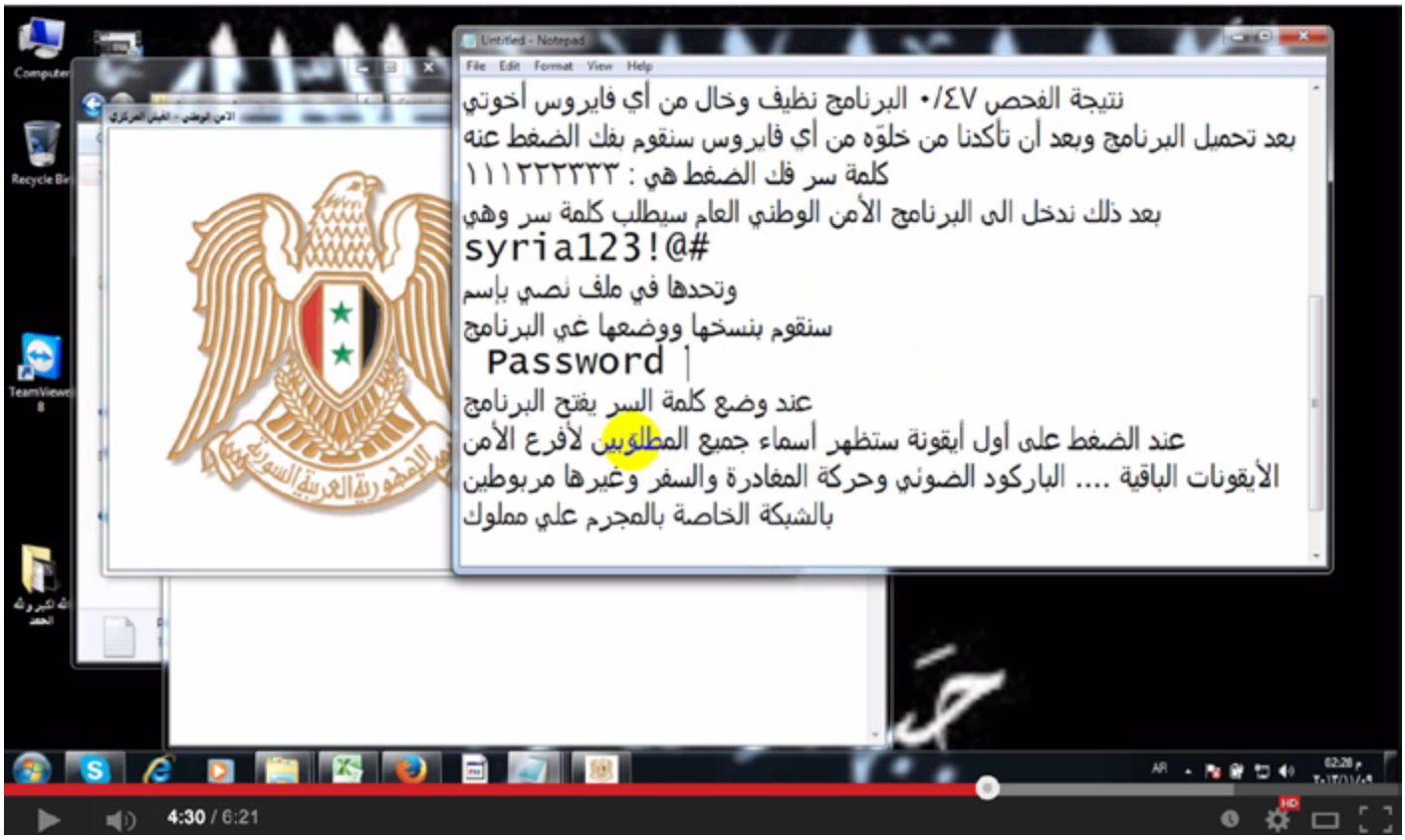
More recent samples, starting from the end of 2013, have shown a more organized development effort, creating highly stealth and graphically-enticing applications.

In this analysis we have seen how Syrian malware has evolved, showing no signs of stopping any time soon. Even though new malicious Syrian samples are appearing each day, the subset presented here will hopefully give the reader an overall view of the techniques and tools that are currently being used to target Syrian citizens.

3.2.1. The National Security Program

Curiosity killed the cat: browsing a previously leaked spreadsheet of wanted activists leads to infection.

We found a set of compressed files on a popular social networking site; when, extracted it showed a database containing a list of activists and wanted individuals in Syria. A video entitled "إختراق أجهزة الكمبيوتر الخاصة بالمجرم علي مملوك وباقي عصابة الاسد" was published on November 9 2013, and the download link for this database application was included in the information section of the video.



The download URL redirected victims to a file-sharing service where the file was being hosted. The compressed RAR file "برنامج الأمن الوطني.rar", with the MD5 signature 0c711bf29815aecc6501671298159a74 and a file-size of 7,921,063 bytes was protected with the password "111222333".

The video requests the victim to scan the password protected ".rar" file using VirusTotal to verify that it is not infected.

After extracting all the files to a temporary folder, we were presented with the application itself and a text file needed to access the "hidden" features of the program.

Barcode.dll	11/9/2013 7:07 AM	Application extension	11 KB
Barcode-driver	11/9/2013 7:05 AM	Windows Installer Package	6 KB
Data-Base	11/9/2013 6:25 AM	Data Base File	7,116 KB
PASSWORD	11/9/2013 9:12 AM	Text Document	1 KB
برنامج الأمن الوطني	11/9/2013 11:53 AM	Application	1,975 KB

The file "PASSWORD.txt file" contained the following text:

syria123!@#

لا تبخلوا علينا بالدعاء قراصنة جبهة النصرة


```
private void txtPass_TextChanged(object sender, EventArgs e)
{
   if (this.txtPass.Text == "syria123!@#")
   {
      MyProject.Forms.frmMain.Show();
      this.Hide();
   }
}
```

Upon closer inspection, the first and last buttons of the application were functional, but the others generated error messages (claiming that some files were missing).

The first button (فيش عام شامل, General Global File) uses “data-base.db.exe” (MD5 8f16efb51fe67961e e31c4f36cbe11db), which was placed into “C:\Users\User\AppData\Roaming“and, when executed, extracts the Excel spreadsheet file “Data-Base.xslx” (MD5 f0a8a1556efbb106b6297700d4cce61b) from the “Data-Base.db” (MD5 95a5c3e91bbb4a3a323433841fbef82a) file in the main folder.

The last button (إنهاء البرنامج) is the exit button.

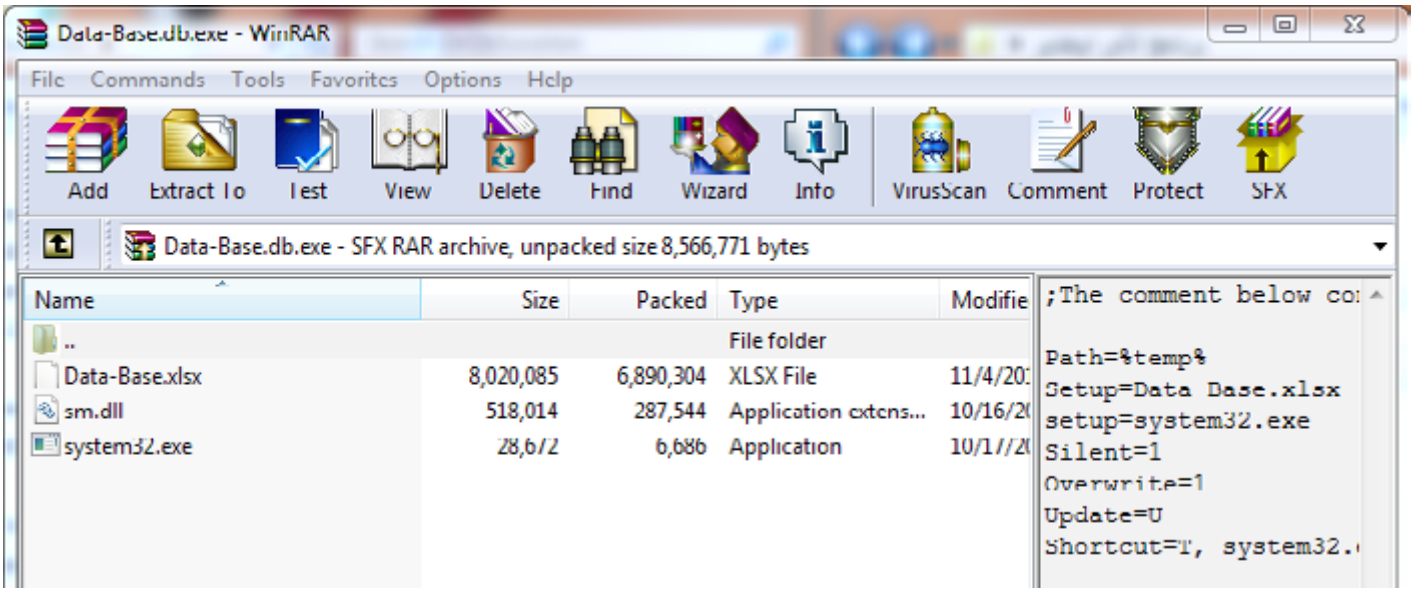
Here is some interesting information worth noting:

- "برنامج الأمن الوطني.exe" is not detected as a malicious file.
- The file "data-Base.db" is detected as a malicious file.

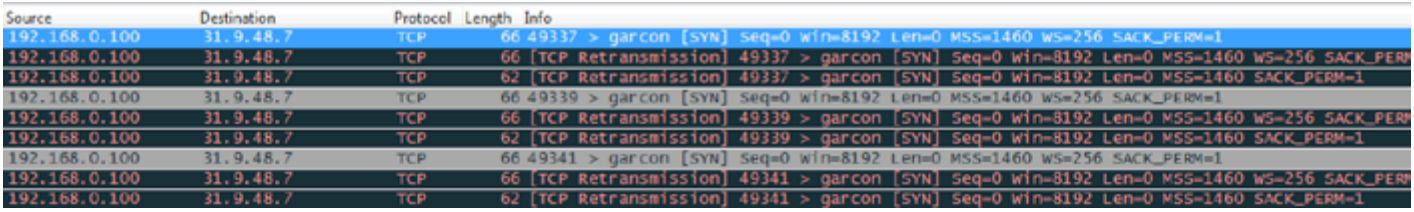
```
[MethodImpl(MethodImplOptions.NoOptimization | MethodImplOptions.NoInlining)]
private void Button1_Click(object sender, EventArgs e)
{
    int num2;
    try
    {
        int num3;
    Label_0000:
        ProjectData.ClearProjectError();
        int num = 1;
    Label_0007:
        num3 = 2;
        if (FileSystem.FileLen(Interaction.Environ("appdata") + @"\Data-Base.db.exe") == 0L)
        {
            goto Label_0041;
        }
    Label_0026:
        num3 = 3;
        FileSystem.Kill(Interaction.Environ("appdata") + @"\Data-Base.db.exe");
    Label_0041:
        ProjectData.ClearProjectError();
        num = 1;
    Label_0048:
        num3 = 6;
        string path = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + @"\Data-Base.db.exe";
    Label_005C:
        num3 = 7;
        if (!File.Exists(path))
        {
            goto Label_0088;
        }
```

The file “data-base.db” is a compressed archive:

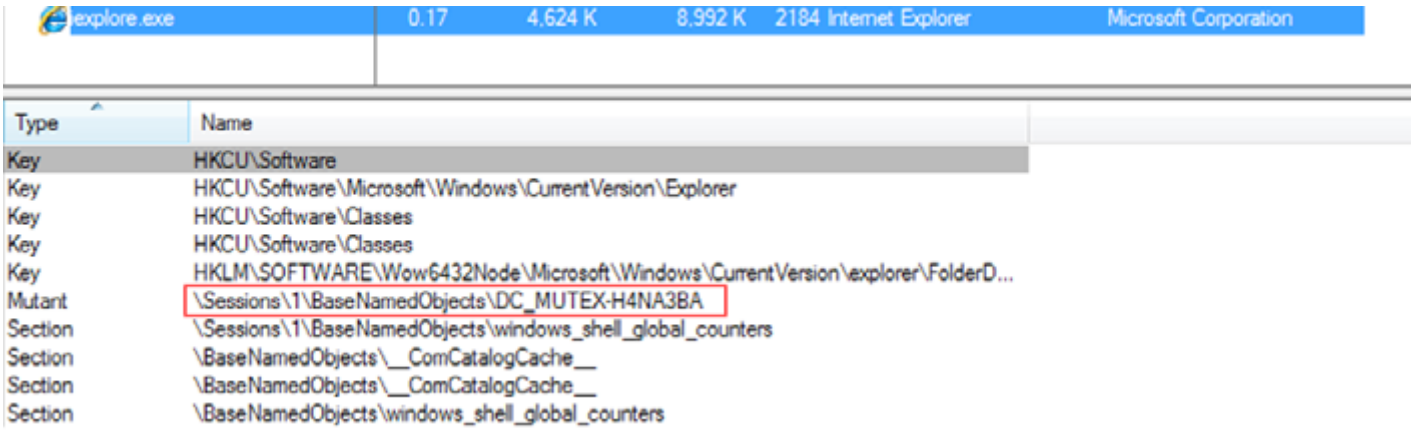
- Product name from the file signature: Project1
- Publisher name from the signature: Syrian malware
- Compilation Timestamp: 2013-11-09 14:47:26



When system32.exe is run, the process “iexplorer.exe” is spawned and is automatically registered for Startup. The file connects to the IP address 31.9.48.7 TCP on port 999. As mentioned in previous reports, the IP address 31.9.48.7 belongs to the Syrian Telecommunications Establishment (STE).



Other temporary files used for the infection were also detected, such as “system32.exe” (MD5: `9424b355a3670fd7749d3d25cbea18cb`) which was copied into the “C:\Users\user\appdata\local\temp\” folder.

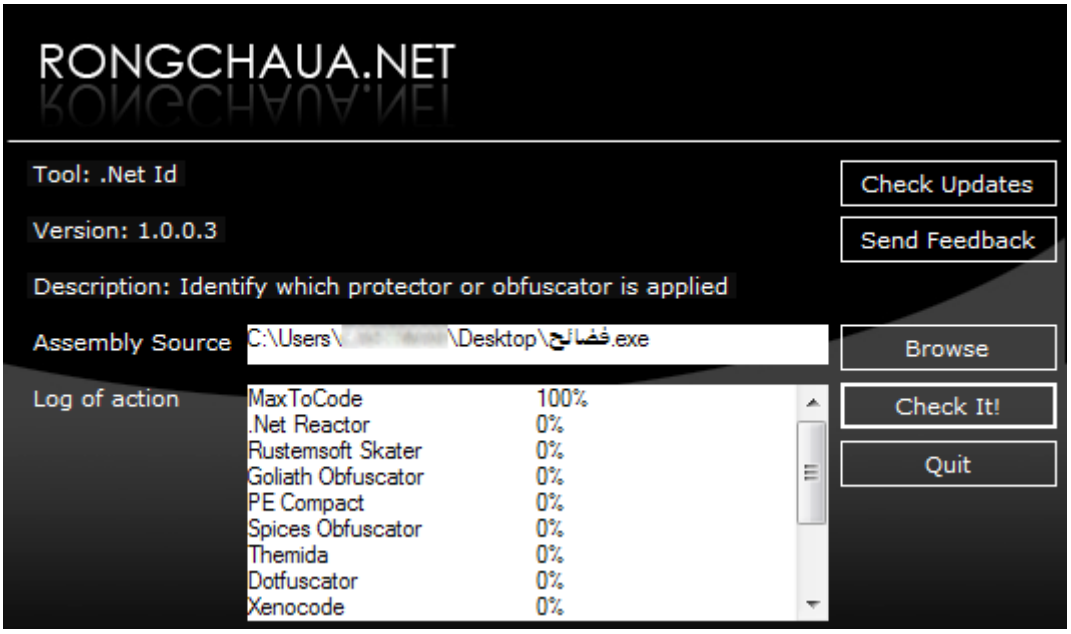


The presence of DarkComet's "DC_MUTEX-*" was a giveaway of the usage of this remote administration tool.

During infection, the Excel spreadsheet is displayed, comprising 96763 rows and 13 columns of activist information. The rows correspond to records of individuals wanted by the government and the columns correspond to information about the individuals. While there is no column description, data in each column reflects the type of data.

3.2.2. Files named "Scandals" are quite attractive
Using shockingly disturbing videos to distribute malware

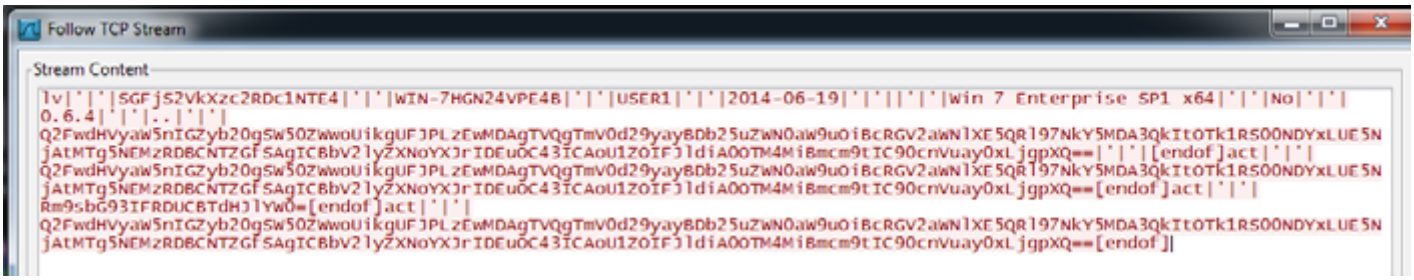
A disturbing video showing injured victims of recent bombings was used to appeal to people's fear and exert them to download a malicious application available in a public file-sharing website. After our initial analysis, the file named "فضائح.exe" proved to be heavily obfuscated with the commercial utility "MaxToCode" for .NET as a means of avoiding early detection by antivirus solutions.



When executed, the original sample created another executable file in the Windows' temporary folder (C:\Users\[USERNAME]\AppData\Local\Temp) named "Trojan.exe", which corresponds to the code of the RAT itself. This is used to save all keystrokes and system activity to another file in the same location, "Trojan.exe.tmp".

```
[DllImport("user32.dll")]
private static extern uint MapVirtualKey(uint uCode, uint uMapType);
[DllImport("user32.dll")]
private static extern int ToUnicodeEx(uint wVirtKey, uint wScanCode, byte[] lpKeyState, [Out, MarshalAs(UnmanagedType.LPWStr)] StringBuilder pwszBuff, int cchBuff, uint wFlags, IntPtr dwhkl);
private static string VKCodeToUnicode(uint VKCode)
{
    try
    {
        StringBuilder pwszBuff = new StringBuilder();
        byte[] lpKeyState = new byte[0xff];
        if (!GetKeyboardState(lpKeyState))
        {
            return "";
        }
        uint wScanCode = MapVirtualKey(VKCode, 0);
        IntPtr foregroundWindow = GetForegroundWindow();
        int lpdwProcessID = 0;
        IntPtr keyboardLayout = (IntPtr) GetKeyboardLayout(GetWindowThreadProcessId(foregroundWindow, ref lpdwProcessID));
        ToUnicodeEx(VKCode, wScanCode, lpKeyState, pwszBuff, 5, 0, keyboardLayout);
        return pwszBuff.ToString();
    }
    catch (Exception exception1)
    {
        ProjectData.SetProjectError(exception1);
        Exception exception = exception1;
        ProjectData.ClearProjectError();
    }
    return ((Keys) ((int) VKCode)).ToString();
}
```

Captured information is sent to a dynamic domain corresponding to the host **"hacars11.no-ip.biz"**, using local port 1177 with no SSL encryption (but base64 encoded), making the analysis of the network traffic a much easier task. During the initial connection to the remote server (after an initial ping to check for internet connectivity), the Trojan will send the machine's name, installed Windows version, logged username, webcam availability and the version of the RAT in use.



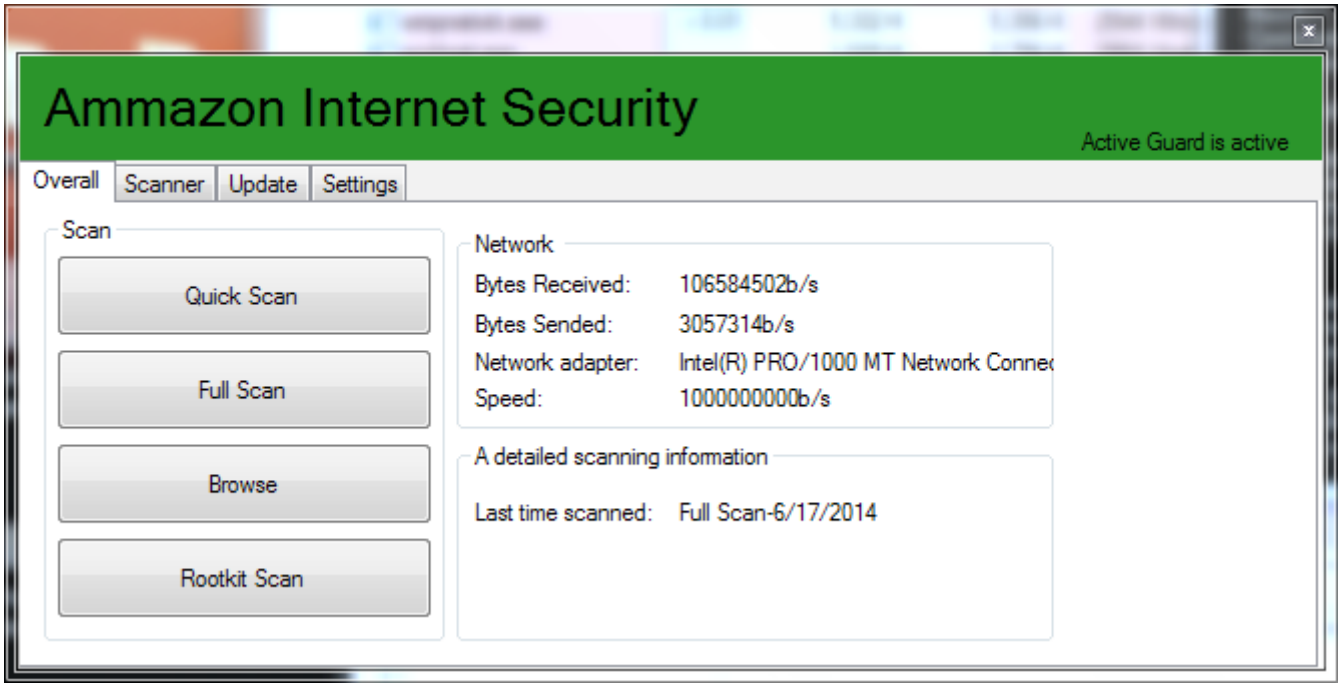
Several embedded command line scripts are in charge of adding the Trojan's executable file to the Windows Firewall allowed list, while at the same time disabling security zone checking in Internet Explorer. System persistence is obtained via a modification in the "Software\Microsoft\Windows\CurrentVersion\Run" registry key and by adding a copy of the malware to the Startup folder.

000000005F49	000000407D49	0	0.6.4
000000005F55	000000407D55	0	Trojan.exe
000000005F75	000000407D75	0	5cd8f17f4086744065eb0992a09e05a2
000000005FF3	000000407DF3	0	False
000000006009	000000407E09	0	[endof]
000000006019	000000407E19	0	Software\Microsoft\Windows\CurrentVersion\Run
000000006077	000000407E77	0	Software\
0000000060A1	000000407EA1	0	Microsoft
0000000060B5	000000407EB5	0	Windows
00000000613D	000000407F3D	0	unknown
00000000614D	000000407F4D	0	abcdefghijklmnopqrstuvwxyz
000000006187	000000407F87	0	SystemDrive
0000000061AF	000000407FAF	0	SEE_MASK_NOZONECHECKS
0000000061DF	000000407FDF	0	netsh firewall add allowedprogram "
00000000622F	00000040802F	0	" ENABLE
000000006287	000000408087	0	windir
000000006295	000000408095	0	\system32\
0000000062C5	0000004080C5	0	Deleted
0000000062DD	0000004080DD	0	Started
0000000062F7	0000004080F7	0	cmd.exe
000000006323	000000408123	0	getvalue
000000006351	000000408151	0	Execute ERROR
000000006375	000000408175	0	Download ERROR
00000000639D	00000040819D	0	Executed As
0000000063D9	0000004081D9	0	start
00000000641B	00000040821B	0	Update ERROR
00000000643B	00000040823B	0	Updating To
000000006475	000000408275	0	length
000000006483	000000408283	0	netsh firewall delete allowedprogram "
0000000064D1	0000004082D1	0	Software
0000000064E3	0000004082E3	0	cmd.exe /c ping 127.0.0.1 & del "
00000000654F	00000040834F	0	yy/MM/dd
000000006561	000000408361	0	??/??/??

Even though different obfuscation techniques are used in the samples we analysed, all of them have underlying dependencies on the .NET framework namespaces, which eventually allows deep source code inspection of the threat.

3.2.3. “Ammazon Internet Security” the “popular Antivirus”

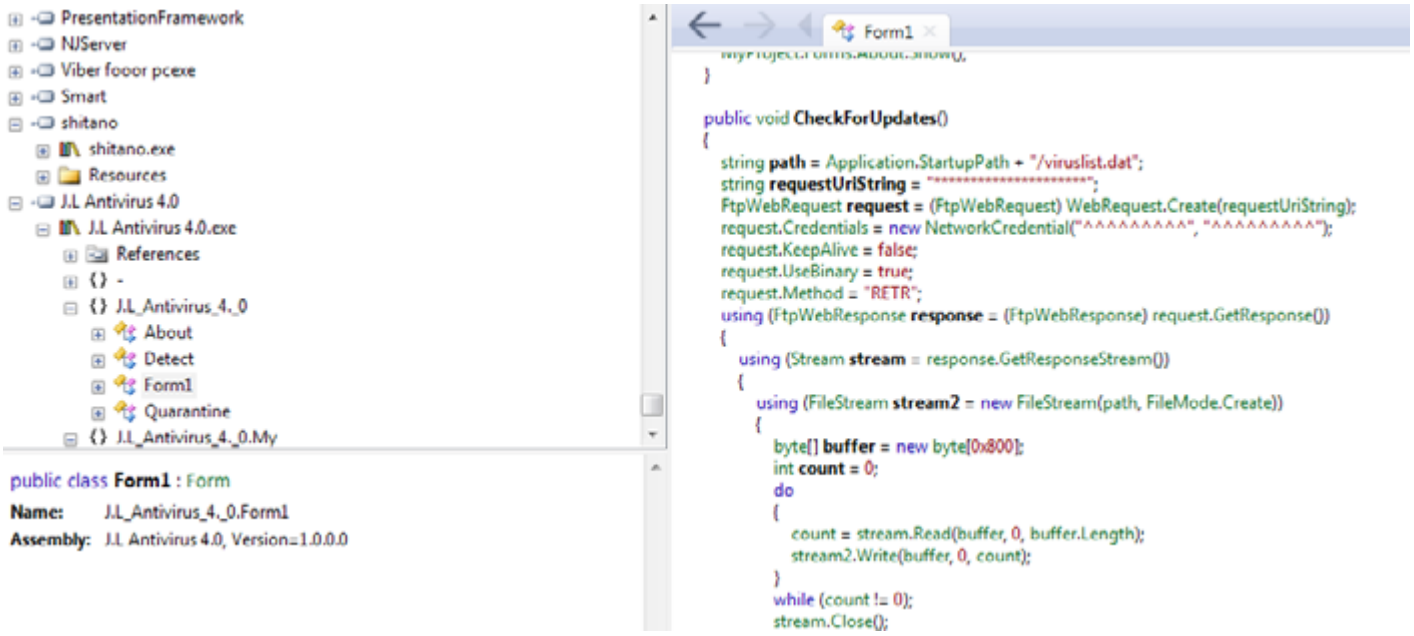
If you thought the era of fake antivirus programs was over, here comes a newly developed sample to challenge your beliefs. With the innocent title of “Ammazon Internet Security”, this malicious application tries to mimic a security scanner, even including a quite thorough graphical user interface and some interactive functionality.



Again, this shows the simplicity of creating a graphical user interface that will trick most of the non-tech-savvy population. Using nothing more than a couple of buttons and a catchy name, Syrian malware groups were hoping that the intended victims would fall for the trap. Analyzing the code interestingly revealed that it has the look--feel of a security application; but, of course, no real security features. While silently executing a remote administration tool when launching this “security suite”, targeted victims were left without their “Ammazon” protection but witha RAT installed.

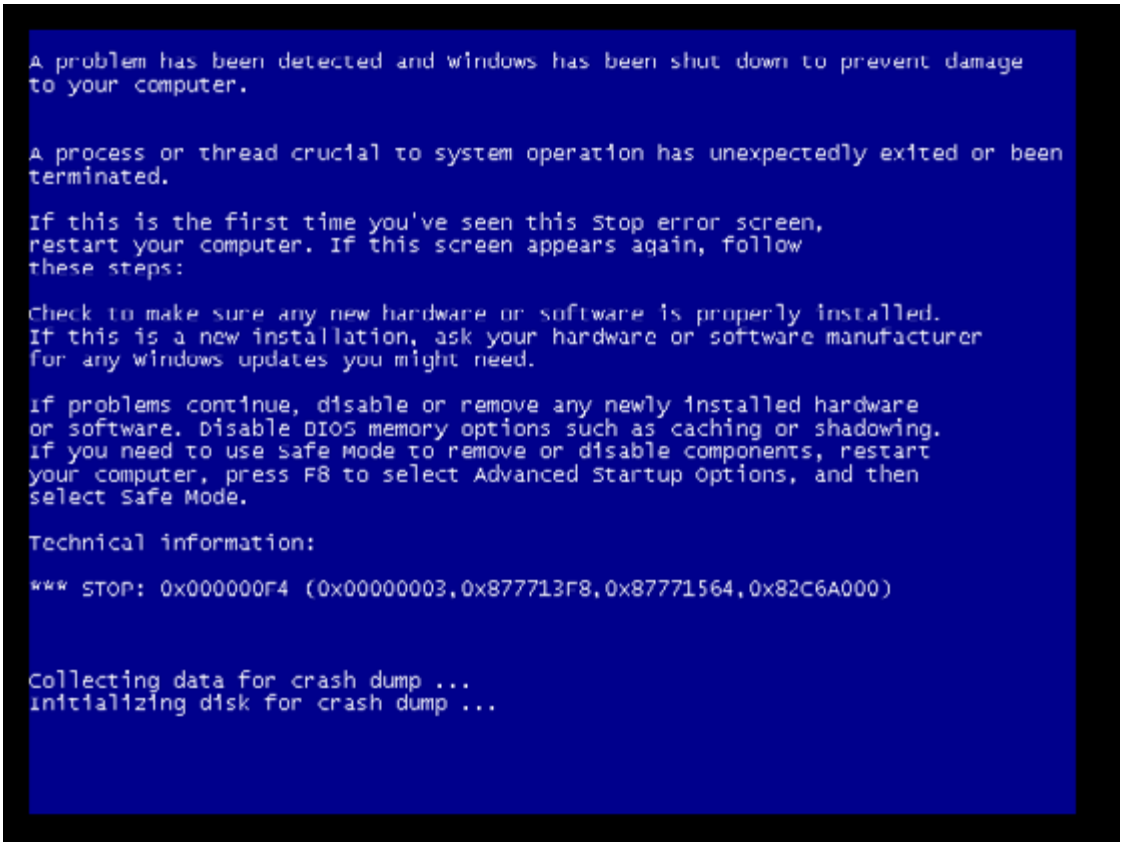
From the Windows process list shown in Process Explorer, we were able to see “J. L Antivirus 4.0” executing in our system, and through Process Monitor we caught the creation of the “analysis” log file for our fake antivirus. Behind the curtains, a connection is made to a remote host, sending real time information on all our activities — the real cost of this free internet security suite!

Among the many programming methods found inside the source code, we were even able to find a “CheckForUpdates” function; and if you look closely enough you can even see “Detection” and “Quarantine” assemblies included in this application. So, not only has a lot of work gone into creating this fake antivirus, the authors also followed good programming practices and implemented modules for each specific (albeit fake) functionality. Maybe at a really quick first sight this could pose as a legitimate tool, but a deeper inspection reveals its true malicious nature.



The real log file was one where all keystrokes were recorded and later sent from the computer via a TCP connection. Even though this type of keylogging functionality is nothing new, when we consider how these malicious applications are being used, and the control they give to the attackers, we can start to measure the importance of reporting these threats and providing protection from them.

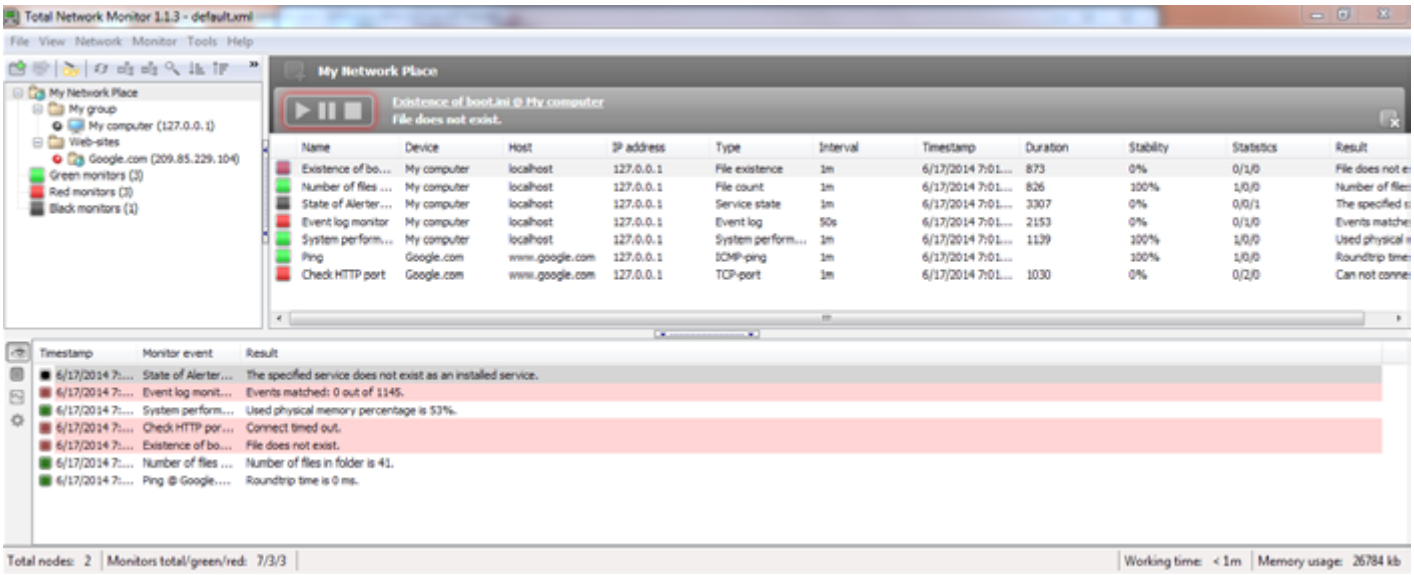
Evidently, the malware authors didn't care much to provide an option to close the "antivirus", and if you were to kill the process you would get a nice 'blue screen of death' and an unexpected system reboot. Surely, the fake application will load again once everything is back up, creating an interesting method for guaranteeing persistence.



3.2.4. You've installed the latest antivirus solution, now let's "protect your network"

Total Network Monitor (which is a legitimate application) was inside another sample we found, used with embedded malware for spying purposes. Offering security applications to protect against surveillance is one of the many techniques used by malware writing groups to get victims who are in desperate need for privacy to execute these dubious programs.

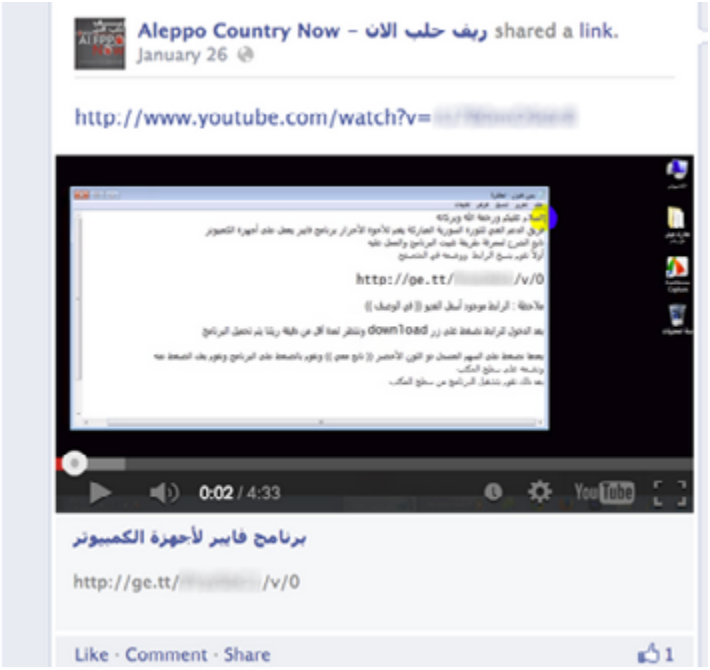
An almost fully functional version of the "Total Network Monitor" utility is included. What this modified version does not show is the remote connection made to a host where f system information is dumped. The actual infection is performed when first clicking on the installer, which uses obfuscation to hide all malicious activity until the "legitimate" tool is completely installed.



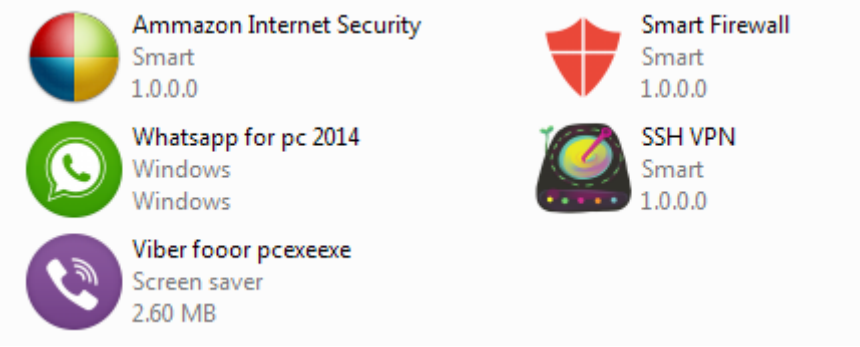
As with other samples reviewed, system persistence is obtained by modifying Windows start-up registry keys. Using names such as "Desktop Manager" increases the likelihood for this threat to go unnoticed. However, the entry name "empty" or "empty.exe" should raise a red flag when auditing these keys.

3.2.5. Whatsapp and Viber for PC: Instant messaging, instant infection

As with other samples, social engineering does all of the heavy work. Instant messaging applications for desktop operating systems have been used in the past to spread malware and it seems that Syrian malware authors have jumped on the bandwagon. In contrast to the "Ammazon Internet Security", these samples don't contain any graphical user interface or even an error message that will tell the victim not to worry about their security. Heading straight for system infection has proven successful for them, and using these popular application names gets the interest of a much larger audience.



The following screenshot shows how the application name, intended functionality and even the icon used, all work in conjunction to create a believable story for the victim. And this is not a comprehensive list, by any means. Framing and social engineering techniques are playing an essential role in all Syrian related malware threats and the trend suggests that the complexity of them will only keep on increasing.



3.2.6. Beware of chemical attacks

Another attack uses social engineering tricks. The sample 38e3bc8776915dbd2e55a4d90f85a872, named “Kimawi.exe” and with JPG icon, is a RAT file bound to the picture “Kimawi.jpg”. This picture is a previously leaked paper supposedly by the regime in Syria warning military units to prepare for chemical attacks from friendly units.

تعميم

إلى كافة قطعات ووحدات الفرقة السابعة /ميكا يطلب إليكم تزويد العناصر المشاركة بمهام أمنية في كل من المناطق التالية : (الكسوة – زاكية – الدرخبية – دروشا – خان الشيح) بمجموعة الوقاية الفردية من الأسلحة الكيميائية لاحتمال استخدام هذه الأسلحة من قبل قوات صديقة .

يأمل قائد الفرقة السابعة /ميكا من جميع القادة وعلى مختلف المستويات إيلاء الاهتمام الخاص والسرية التامة على دقة تنفيذ التدابير الواردة أعلاه بغية تفكيك منظومة الإرهابيين .

اللواء علي حسين العلي
قائد الفرقة السابعة/ميكا

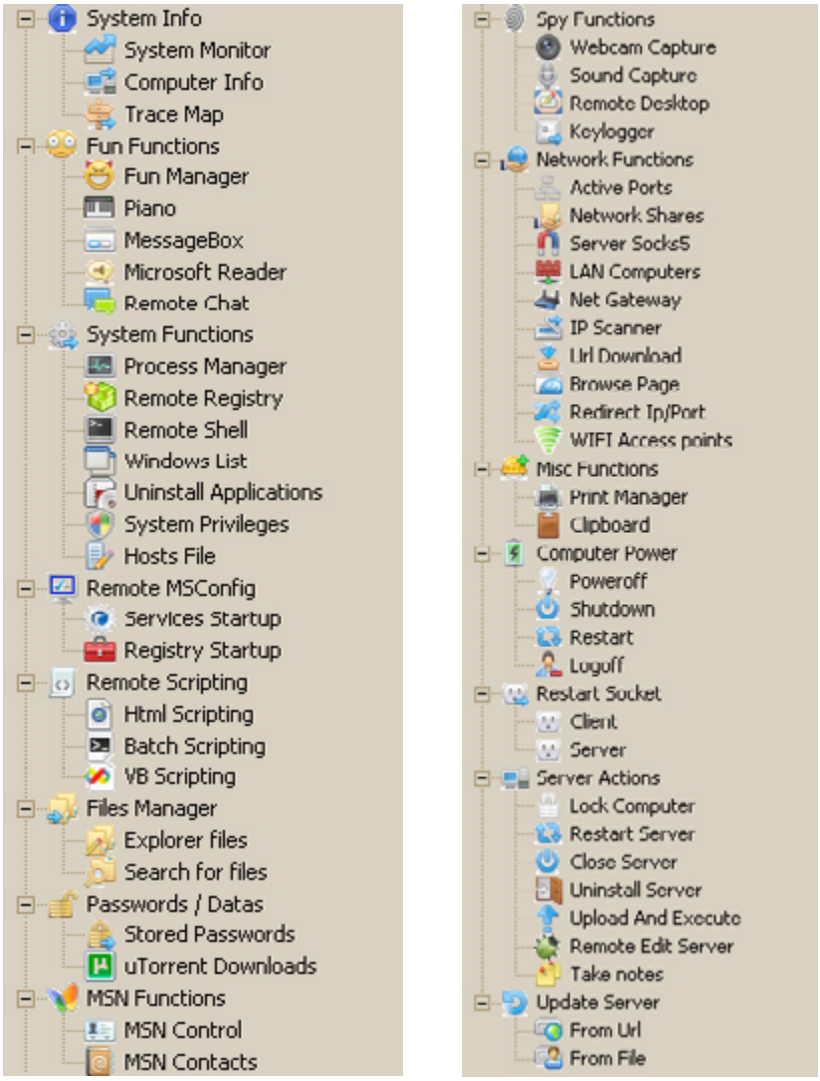
Kimawi.jpg

3.2.7. Commands and functionality

Different remote administration tools have been spotted in the wild; most of them provide an extensive range of functionality to fully control infected systems. These include:

- Keylogging
- Capturing screenshots and webcam control.
- Recording live sound/video.
- Installing programs
- Uploading/downloading files
- File, process and registry key management
- Remote shell
- Executing DDoS attacks

Among the most popular RAT found in the samples subset is Dark Comet, a free remote administration tool that provides a comprehensive command set for the attackers to use in their malicious purposes.



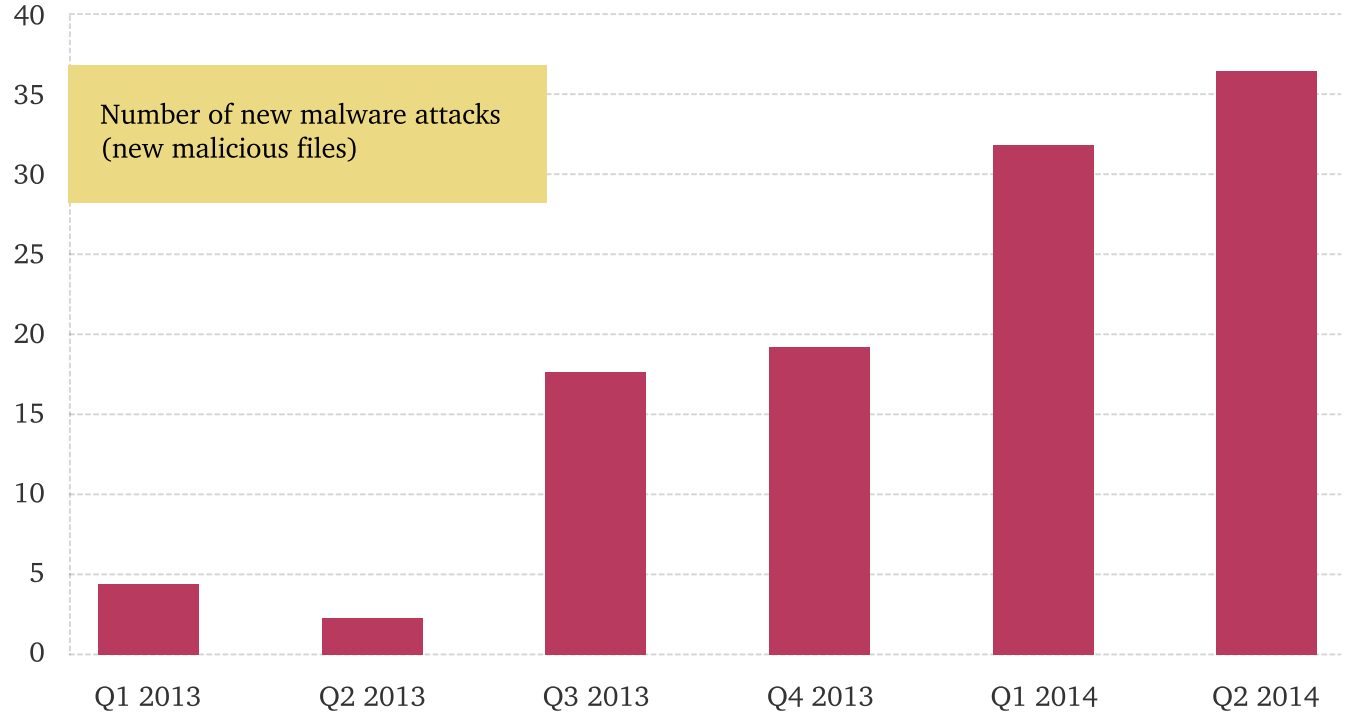
DarkComet Control panel & Functionality

Another RAT widely used in the Arab world is NjRAT, which includes a list of commands (see below) that can be sent from the controller to the infected system.

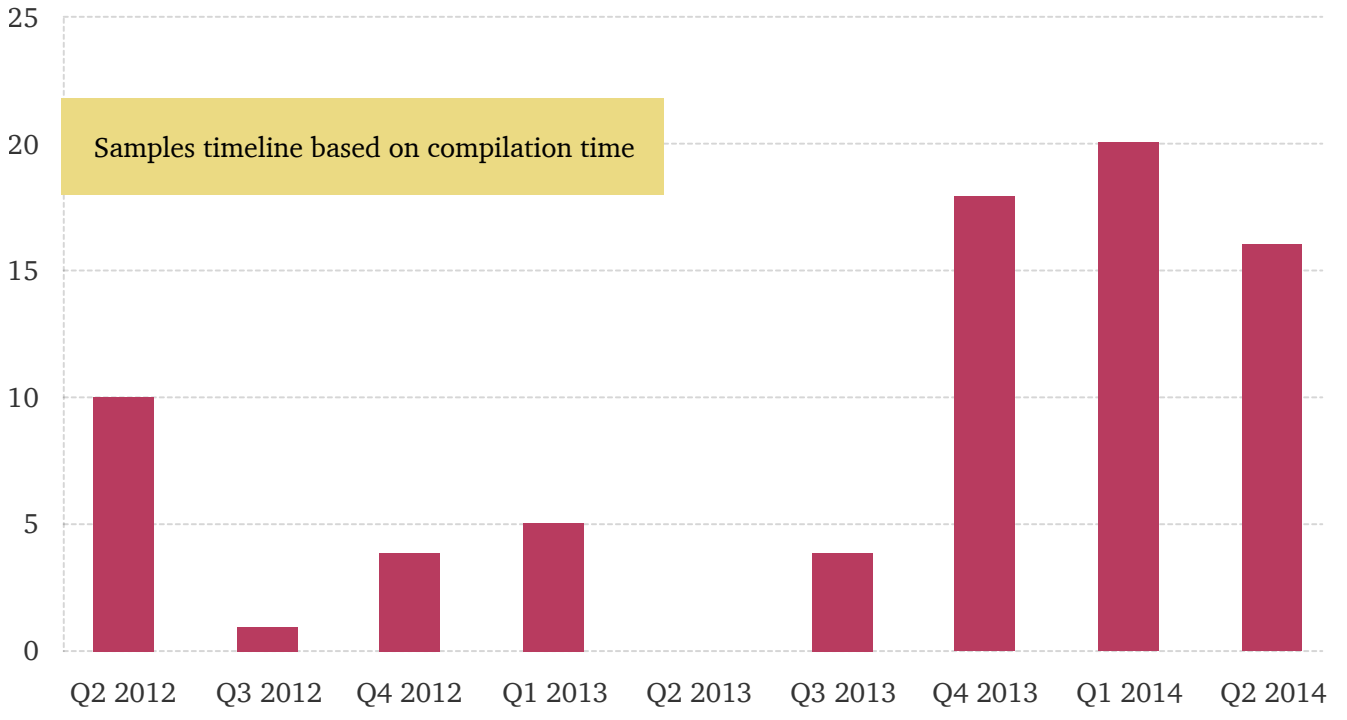
Command	Option	Function
“PROC”	~	Retrieve information about current running process
	K	Kill a process
	KD	Kill list of processes and delete module files
	RE	Restart a running process
“RSS”		Start a CMD and direct STDIN and STDOUT to be controlled by C&C
“RS”		Send command to CMD
“RSC”		Terminate CMD process
“KL”		Retrieves keylogging file
“INF”		Information about system Drive, malware status
“RN”		Download and run a file from a specified URL
“CAP”		Screenshots, desktop monitoring
“P”		Ping
“UN”	~	Completely Uninstall Trojan
	!	Terminate Trojan Process
	@	Restart Trojan
“UP”		Update Trojan
“RG”	~	Enumerate Registry Key
	!	Set Key Value
	@	Delete Registry Key
	#	Create SubKey
	$	Delete SubKey

3.2.8. Evolution of malware attack file numbers

The attackers are working on full power, and the number of attacks and malicious files being distributed is constantly increasing as they become more organized and proficient. Below is the timeline distribution for malicious files distributed during 2013-2014, based on the first time they were distributed or seen in public (Skype, Facebook, file-sharing, email, etc.).



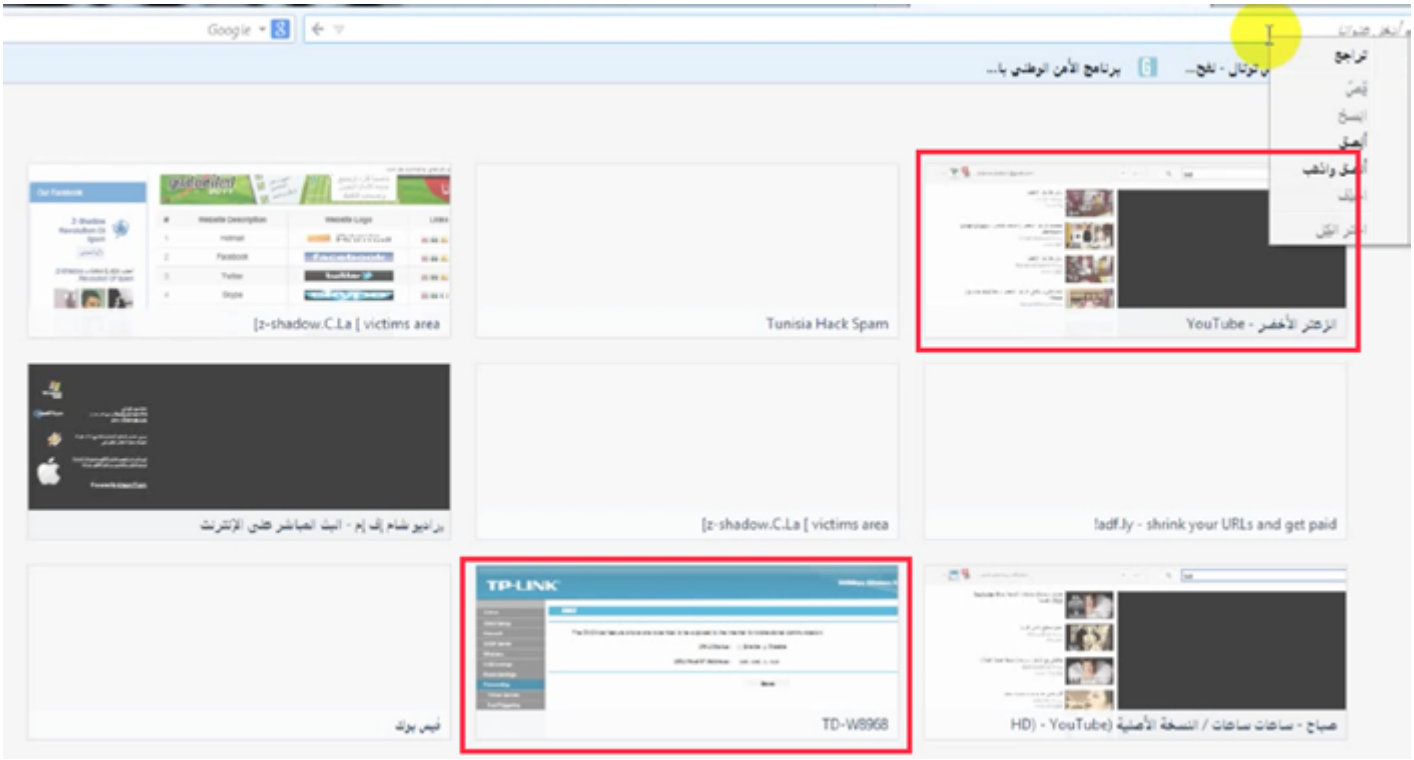
Below is the timeline distribution for the collected samples based on compilation time



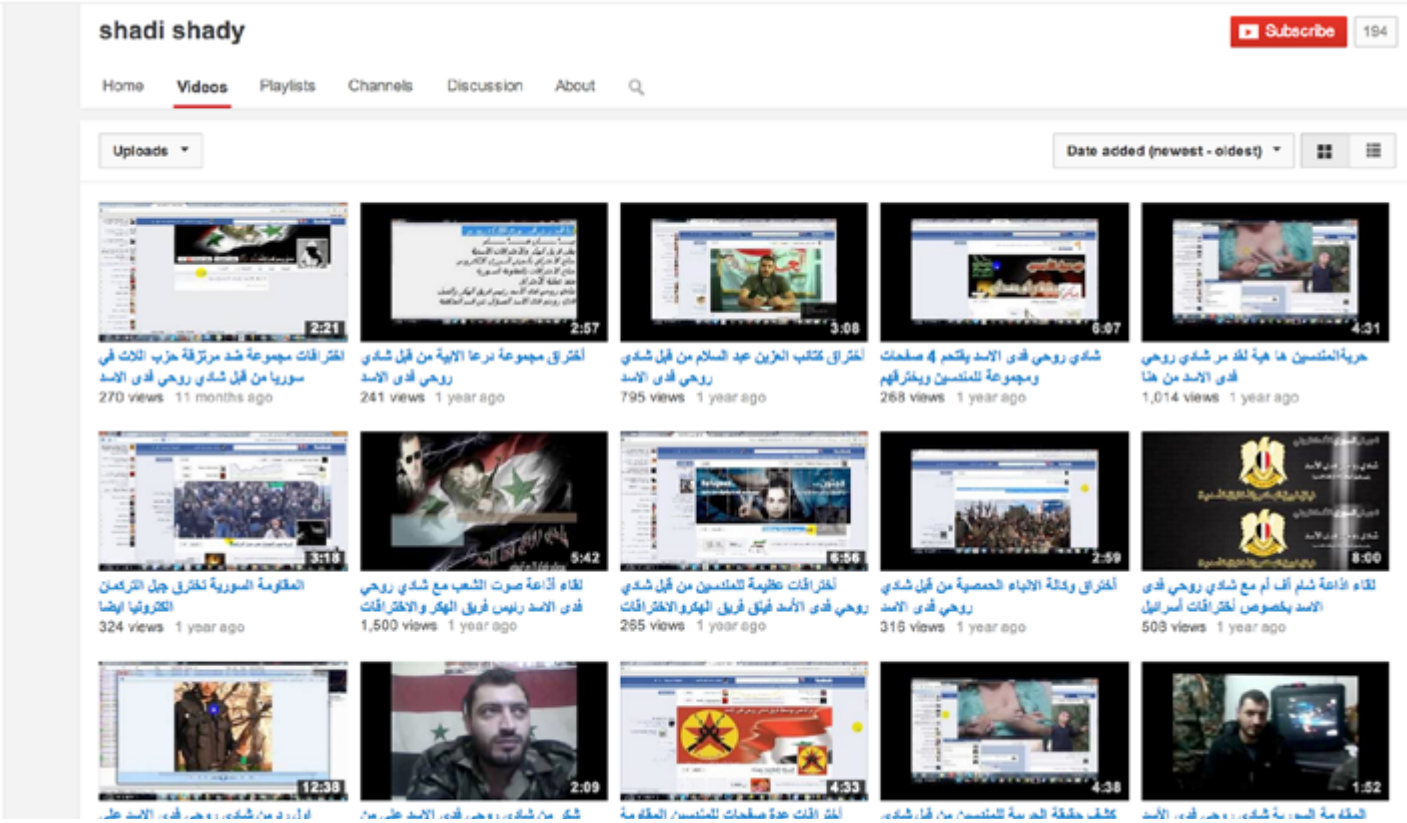
The samples details and domains list used by the attackers can be found in the Appendices 1 and 2 in the end of the document.

3.2.9. Locations, domains and team

The group responsible for the attacks is using common techniques shared by many of the hacking groups around the world. They benefit from dynamic domains that can be linked to their modem devices and configured with forward functionality to a public IP address assigned by the ISP. By restarting their modems they obtain a new address, creating a dynamic infrastructure that can be easily managed. Dynamic Update Clients (DUC) on their computer devices (usually the same as the RAT server) are in charge of having the dynamic domain provider update to the newly assigned address.



One of the videos by one of the attackers has shown one of the group members using a TP-Link modem model TD-W8968, commonly found in SOHO environments.



YouTube page for one of the Attackers Showing videos about their web defacements, cyber-attacks and an interview with radio channel talking about their hacking achievements

Since the end of 2013, the group has extensively relied on a class C IP subnet, 31.9.48.0/24, provided by TARASSUL ISP (Syrian Telecommunications Establishment) for its attacks. We suspect this subnet has been allocated to the group, also an indication that they are now operational from a single location.

In early 2014, the group moved to an IP address in Russia (31.8.47.7), to launch multiple new attacks.

Information on domain "All4Syrian.com"

This domain is registered for the email aloshalaa@gmail.com. It served as a pro-regime website back in 2012 and is being used for the C&C of some of the RAT files.
The domain was registered to okpa1984@gmail.com from 2011 to 2013.
Malware has also been seen connecting to xtr.all4syrian.com and vip.all4syrian.com.

Attackers' geographical distribution

The map below shows the attackers' geograhical distribution based on the geolocation of the IP addresses used by the C&C servers:

3.2.10. Victims

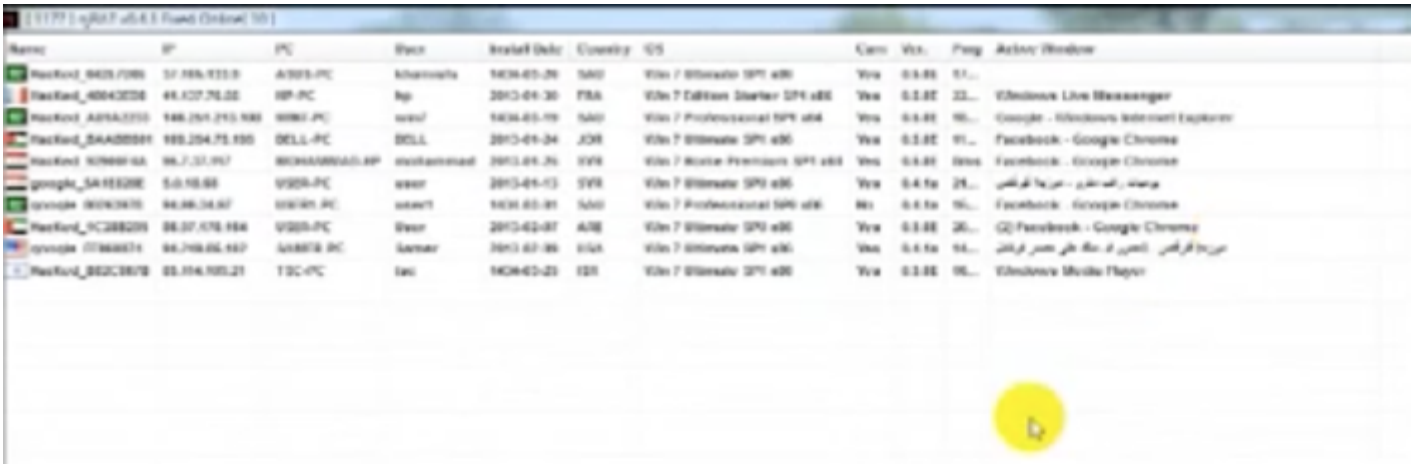
The distribution of victims is confined only to Syria, but also reaches nearby countries. We have observed victims of the Syrian-based malware in:

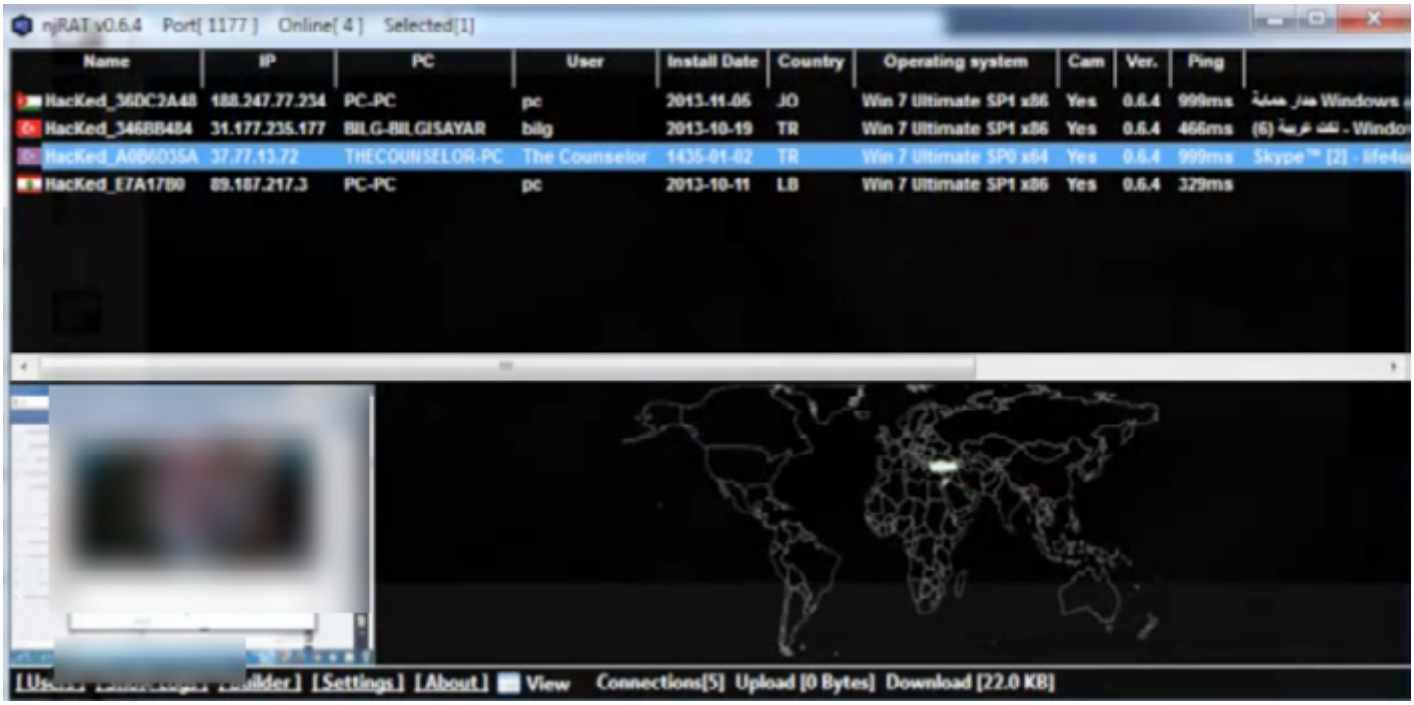
- Syria
- Lebanon
- Turkey
- Kingdom of Saudi Arabia
- Egypt
- Jordan
- Palestine
- United Arab Emirates
- Israel
- Morocco
- United States

Victims geographical distribution map

Map showing geographical distribution of victims with zoom on the most affected areas

Below are snapshots taken from videos published by the attackers, showing their RAT control panel and list of victims. This shows some of the victims located in different countries.





The sample details and domain lists used by the attackers can be found in Appendices 1 and 2 in the end of this document.

3.2.11. Activist Behavior

It is worth noting that we have seen evidence of activists trying to carry out Denial of Service attacks on the RAT domains and servers, in an effort to overwhelm their resources and cause their connections to timeout.

The post below shows a warning from activists about pro-government hacker attacks on Facebook pages, explaining how pro-government groups post links to Trojanized applications in order to infect users The activists announce in the post that they have spotted a C&C domain used by the Trojans and that they are attacking it to remove all hacked victims.

“جاري ضرب الهوست .. لحذف جميع الضحايا الوجودين للهاك أنشالله” translated as “Host Attack in progress .. to remove all hacked victims with help of god”.

3.3. Attribution

Team and positions

From many posts, forums and identification videos, it is clear that the group has an organized structure of teams working together, The names and positions outlined below were collected from posts on infiltrated forums or pages. They are all either nicknames or incomplete names that do not enable full identification of the attackers.

The Resistant Syrian Electronic Army

- Group 1: Team Hacker and Assad Penetrations Unit
- Group 2: Anonymous Syria Al Assad Unit
- Group 3: Management of Electronic Monitoring and Central Tracking Unit

Group1: Team Hacker and Assad Penetrations Unit

Name	Position
Shady	Head of Assad Hacker team
Fadi	Responsible for raids
Sarmad	Responsible for operations in raids unit
Mahmoud	Assistant to the head of management unit
Girl nickname Fidaeya (redemptionist)	Member of support and publishing team
Najma	Member of media and publishing team

Group2: Anonymous Syria Al Assad Unit

Name	Position
Jabbour	Public relations manager
Haydara	Electronic ambushes unit
Alaa Morched	Electronic monitoring unit and follow up
Ahmad	Responsible for team unit
Nariman	Responsible for team unit
Ali	Responsible for team unit
Zina	Responsible for team unit
Derkachli Kordahli	Responsible for destruction of victim accounts
Ahmad and Morad	Engaged in attacks

Group3: Management of Electronic Monitoring and Central Tracking Unit

Name	Position
Kenan	Head of team
Okba	Head of electronic operations
Ahmad	Head of eectronic raids
Ritzel (heart of the lion)	Head of electronic penetration operations

4. Kaspersky Lab MENA RAT Statistics

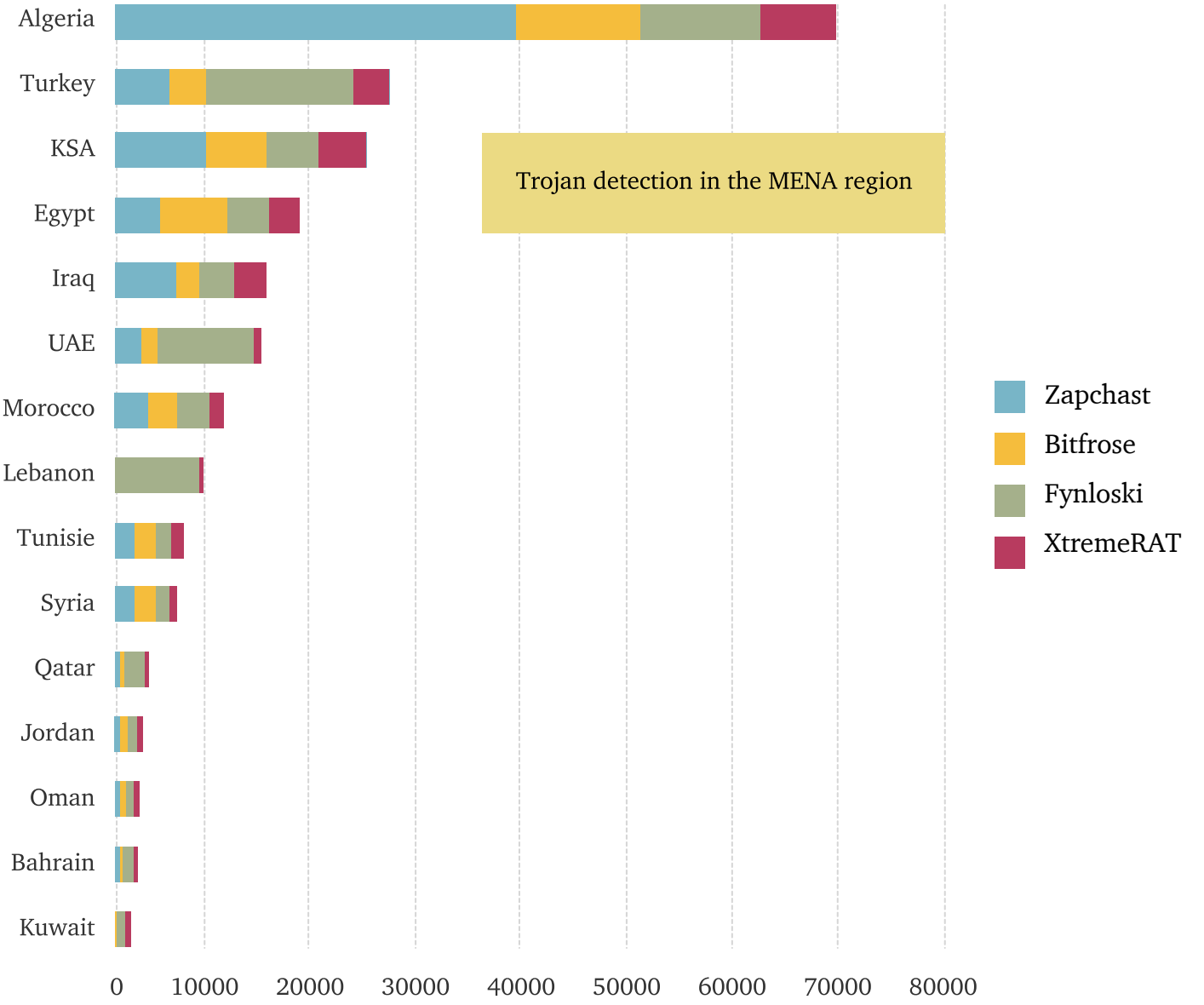
Remote Administration Tool (RAT) Trojans are malicious programs that allow a remote "operator" to control a system as if he has physical access to that system. Malicious RATs are widely used by different types of cybercriminals (hacktivists, script-kiddies, and scammers) and even in some state-sponsored attacks.

Some of the most popular RATs are detected by Kaspersky products as following:

- Trojan.MSIL.Zapchast, also known as Njrat
- Backdoor.Win32.Bifrose, also known as Bitfrose
- Backdoor.Win32.Fynloski, also known as DarkComet
- Backdoor.Win32.Xtreme, also known as Xtremrat

The statistics below, extracted from the Kaspersky Security Network (KSN), show the number of RAT infection attacks blocked by Kaspersky Lab products in the MENA (Middle East North Africa) region in the 2013-2014 period:

Country/Detection	Zapchast	Bitfrose	Fynloski	XtremeRAT	Total
Algeria	39113	12071	11643	7106	69900+
Turkey	6326	3325	14002	3586	27200+
KSA	9616	5555	5336	4516	25000+
Egypt	5567	5883	4325	2634	18400+
Iraq	6756	2280	3235	3055	15300+
UAE	3594	1165	9244	745	14700+
Morocco	4084	2710	3104	1233	11100+
Lebanon	426	297	8073	136	8900+
Tunisia	2844	1888	1495	1004	7200+
Syria	2806	1897	1362	544	6600+
Qatar	1332	327	2177	233	4000+
Jordan	1259	680	1104	414	3400+
Oman	1241	446	915	374	2900+
Bahrain	1218	178	1214	254	2800+
Kuwait	454	407	922	345	2100+


Trojan detection in the MENA region
Algeria
Turkey
KSA
Egypt
Iraq
UAE
Morocco
Lebanon
Tunisie
Syria
Qatar
Jordan
Oman
Bahrain
Kuwait
0
10000
20000
30000
40000
50000
60000
70000
80000
Zapchast
Bitfrose
Fynloski
XtremeRAT

Based on KSN world statistics, the MENA region has one of the highest numbers for RAT attacks, as shown below:

Country	Number of users
Algeria	39113
India	35024
France	10955
Saudi Arabia	9616
Mexico	6862
Iraq	6756
Turkey	6321
Egypt	5567
Russian Federation	5526
Malaysia	5014

NjRAT infection Top 10s

- Algeria has the highest number of users facing NjRat infection for the 2013-2014 period and five countries from MENA are in the NjRat top 10
- Algeria has the highest number of users facing Xtreme RAT infection for the 2013-2014 period and four countries from MENA are in the Xtreme RAT top 10.
- Four countries from MENA are in the Bifrose top 10 infection list.
- Three countries from MENA are in the DarkComent top 10.

5. Conclusion

Syrian malware has a strong reliance on social engineering and the active development of technologically complex malicious variants. Nevertheless, most of them quickly reveal their true nature when inspected carefully; and this is one of the main reasons for urging Syrian users to be extra vigilant about what they download and to implement a layered defense approach.

Antivirus software uses either signature or heuristic-based detection to identify malware. On the one hand, signature detection searches for a unique sequence of bytes that is specific to a piece of malicious code. On the other hand, heuristic detection identifies malware based on program behaviour. In our research we were able to collect more than 100 malware samples used to attack Syrian citizens. Although most of these samples are known, cybercriminals rely on a plethora of obfuscation tools and techniques in order to change the malware structure so as to bypass signature scanning and avoid antivirus detection. This proves how critical heuristic technologies are when it comes to protecting against these types of attack. By being able to identify variants of known malware types or even new malware families, Kaspersky Lab security products detected all the collected samples.

We expect these attacks to continue and evolve both in quality and quantity. We expect the attackers to start using more advanced techniques to distribute their malware, using malicious documents or drive-by download exploits. With enough funding and motivation they might also be able to get access to zero day vulnerabilities, which will make their attacks more effective and allow them to target more sensitive or high profile victims.

Even though the attackers depend mainly on using known RATs, their rapid improvement and application of obfuscation techniques, GUI development for fake applications, and code modification via automated builders, increase the probability that it won't be too long before they start writing their own Trojans to take advantage of customized infection capabilities and implement better security evasion.

Finally, having a comprehensive and up-to-date antivirus and firewall should be the first measure taken by any user that does any type of online activity, especially during these uncertain times when new cyber threats appear almost daily.

Appendix 1: Samples

All samples table

The list of sample files has been collected through the infection vectors detailed above (Skype, Facebook, file-sharing, email, etc.). The samples have been either generated using automated tools (RAT server, obfuscation tools) or developed and bound to RAT files, especially the new samples with graphical content.

File information	First reported	Main file MD5	Special info
• Ammazon Internet Security.rar • Smart Firewall.rar • SSH VPN.rar https://www.dropbox.com/s/f9gpiv2qk4m1r44/Ammazon%20Internet%20Security.rar https://www.dropbox.com/s/65bnrk8x4gt2og8/Smart%20Firewall.rar https://www.dropbox.com/s/c4kwnh6q0r3ymwf/SSH%20VPN.rar https://www.facebook.com/photo.php?fbid=726440034062205&set=a.375478335825045.85979.367002976672581&type=1&theater reported on facebook and https://www.cyber-arabs.com	Mar 18, 2014	23ae669639c1d970aaee6f9f551b82b1 abf93ad254cd01997935863c9e556af8 96ca1d7e45b03f438804d3b46d22df8a 1827acc1cf53e6ac9d9b638fc81f50a1	thejoe.publicvm.com multiple ports: 31.8.48.7
Viber fooor pc%E2%80%AEexe%E2%80%AEexe.rar http://ge.tt/14hNebG1/v/0 http://www.youtube.com/watch?v=rU7B0mO9dr8	Jan 26, 2014	8995ff66bacaf76d1c24660f3092583c	.scr file

File information	First reported	Main file MD5	Special info
Whatsapp for pc 2014.exe http://ar.rghost.net/54001947 other name: NJServer.exe https://www.facebook.com/AlhyytAlshrytLlthwrtFyAlryfAlghrby?sk=timeline&hc_location=timeline&filter=2	April 11, 2014	8995ff66bacaf76d1c24660f3092583c	31.8.48.7, port 1199
فضيحة النظام وداعش.exe, chrome.exe, shitanoxxx.exe, shitano.exe (shitano= the devil) Source from friends at www.cyber-arabs.com	Jan, 2014	10300846f75eb36ad87091ed7f04b5d8	hhhhhkrufnrrrs1982.zapto.org port 1177 Found this resolved back then to 95.212.148.21 from facebook post cached on google
برنامج الأمن الوطني.rar (=national security program) -rar pass: 111222333 -Internal exe pass: syria123!@# http://ge.tt/1v3NB7y/v/0 http://www.youtube.com/watch?v=Cw1vD9DhEc0	Nov 9, 2013	3828971a77d94b6a226064ede528e408 (main executable)	thejoe.publicvm.com extracts with excel sheet with previously leaked details on wanted activists
فضائح.exe (=scandals) http://www.gulfup.com/?X65OmP http://www.youtube.com/watch?v=TBbhUSS-pik	Nov 1, 2013	796cafc1983bc4e8a5d80d390d3cd33a	hacars11.no-ip.biz

File information	First reported	Main file MD5	Special info
Skype.exe Syriatel.exe مضاد فايروس سكايب.zip (anti skype virus) spediti 27 orangealert.zip master.exe PDB Path C:\Users\joe\Desktop\Desktop\Syriatel\Syriatel\obj\Debug\Syriatel.pdb	1 to 5 Jan 2014	ec62a59b10b0e587529d431db18d7b77 ad9a18e1db0b43cb38da786eb3bf7c00 1a6061d02794969ba7d57f808a64c1c2 ac54c78f37eec21d167b1571fc442e84 cddaf92765fd465fcea63a6e4a4e4cbc 037d1cf1f8231f41dd6ae425488445fc 23e936f189611430fffbdd8e1f2a077f bundled with 9424b355a3670fd7749d3d25cbea18cb	N/A
gfbf.exe 202.exe SRGf2.exe VmFP4.exe OYTu4.exe ssss.exe oooo.exe	Jan to Mar 2014	3f86102e70a3d2fc2f94137599e8d9c2 d3f957963f56b8bc5e883984857379d4 4c881505fe577e8d94227bb3e39b9f75 e81bdf099a5e31f955d1d582dabed1d2 ef644d0b444d894d10e7fa8a5072a2e3 05574551467d6730800f7d098b17c98a c46f72cb68b8d729fea8952fc01e1f13	hhhhhkrufnrrrs1982.zapto.org
stub.exe Winrar.exe tr.exe WindowsApplication1.exe	July 2013 to May 2014	409a0b6954d4ff1000a6d7b78cde2b44 0125a39deb6c0fb37853faa9a90162d3 12d63168bac9de71bb9142aa9cf0e533 debb0beac6414b681d050f2fbc2f2719 40527942833ac6ffa25e4f875ab0bd17	thejoe.publicvm.com (31.9.48.146) 64.4.10.33:123
Syria.exe	June 2014	0d4bbd0d646cedea1c3eb5d2079ce804	
server.exe abalse=the devils	April 2014	12cbe97c89634db754bae817e3b177b3	abalse.no-ip.biz (95.212.148.233)
image.scr	June 2014	7ba45daccca21db2e353b9144b29f2e8	31.9.48.164 port 1122
Windows_8_Pro_Build_9300_activation_(KMS).exe	2012 to 2014	f73c643863b20d5843da4636330ff30e	vip.all4syrian.com (31.9.48.11) old but active. data.downloadstarter.net cmp.online-hd.tv (108.161.189.5) alosh66.linkpc.net
Cleaan.exe sent by email	17 June 2014	86e6cc8827bce4837a55ad76133f3125 d96606d128ee726760f84eb8d37918b6 e5c13f46b8fe119f77d0144c78ca9f60 45d4479bdd7d9a3e06e955ad358f1b6a	31.9.48.141 port 5552

File information	First reported	Main file MD5	Special info
chrome.exe	17 June 2014		31.9.48.141 port 5552
فضائح انسحاب الشيعة من سوريا.scr (scandals of Shia retrieval from Syria) asa.exe feras.exe	Nov 2013 to June 2014	e65107c5aeea5c3b3a59d4912905c3def457f4ee2e2532466f180b86fb01c91dc71ccf5b1354d847fd7fae1e5668ea773eb93fd8129aadbcce8d303047a18c9fbc00e320aebb6f780ac4e70a6e183978b5c7a04ae3eed7fd9f076d2a400ba6601a44d73596b0f6755b4ed9651708c9e9b717adfd7a4997ebae49308171d09b1ffa77151f7677e1602338e57c13aeab13b7be9a74048fd64f0562a94e5fa66db2cd92e50ba570b6cc018fbafb6ea7e0ad24db21293792639a3567bf8c1f651885fb2fbca3be381bb1a0b410f66e04f114d2561f4259da6784894ffb1a559c6952	basharalassad1.no-ip.biz (31.9.48.147) port 5552
clean.exe	Oct 2013	dd0965b9bb4d8fa833b59ab41b405c0b	31.9.48.84 port 999 basharalassad1.no-ip.biz
Sent by email, downloads file from gulfup.com file sharing site + connects to the Syrian IP gets 62b1b05cb3c7bb6727541efb79b23442 as Application1.exe from the file sharing site through direct link	9 June 2014	da98248ab1e4a287ac46023eacd08f5b	31.9.48.141 port 5552
image.scr	9 June 2014	7ba45daccca21db2e353b9144b29f2e8	31.9.48.164 port 1122
MSRSAAP.EXE	April and May 2014	ab75661f837537c4efb20ba6e99f23de	tn4.mooo.com (31.9.48.11) port 83
f2.exe MSRSAAP.EXE 1.exe		ebb2acc6e6ff596dea4f034e6e941eeaed9b62e17543b948da81c75ad4db88ad1b1bdfdd0c5218354d7c979afbbf4a760d2f0807233cff088cf69f553553c3bc430c8f11ce5a77e154ebcd0d7eb1501d6ec76cfd10c6ee8e3d8fd81e445abb7b	tn5.linkpc.net (31.9.48.11) resolving in the ed9 sample to 188.139.228.179 (Syria mobile telecom GPRS) and 178.52.194.35 (old IP)

File information	First reported	Main file MD5	Special info
f3.exe f2.exe 1.exe Kimawi.exe	13 May 2014	b4eb0cb0fae200d09e6744f0ede10810 1b1bdfdd0c5218354d7c979afbbf4a76 0d2f0807233cff088cf69f553553c3bc 38e3bc8776915dbd2e55a4d90f85a872	tn5.linkpc.net (31.9.48.11)
yamen.exe	May 2014	288a4ee20880be85af60b1bad4d1d4d7	31.9.48.141 by modifying hosts file, no dns resolution
system32.exe	Oct 2013 to Jan 2014	08947709640922b2d8e3b8d0e5b8e84e 21ec25f685843ec03fdba24837fc61e4	fernando85.no-ip.biz 31.9.48.147
	Oct 2013	a7caf08fba073ac3e92d1faea340cb59	meroassad.no-ip.biz 31.9.48.147
Explorer.exe 13.exe	Mar to Jun 2014	e1f2b15ec9f9a282065c931ec32a44b0	31.9.48.141 port 1960
server.exe	Jan 2014	c85480f1e4731f98e28dc007056615a4	31.9.48.141 port 1990
Sent by email	5 Jan 2014	cd97b9b7494470274e7df66059348d6d 54c178ba89d752be2ae3307fd40db45f 93195146c13ba6fd75b3c0062e3abf05 f387eb11a402c9abb8700604906c00d6 a57f6c06ba7ca5758f1ca48eaa0a9cc5 93195146c13ba6fd75b3c0062e3abf05	31.9.48.141 port 1177
	Dec 2013	b8e7f3b4cbe8e58b0509fc7fde71ddbf	31.9.48.141 port 1920
	Feb 2014	387a285597d3ac51637f6ecc07ba0d5b	ahmdddd.no-ip.biz 31.9.48.141 port 5552
E.exe	Jan 2014	faebf06b7113f47ec2f3089879d765b4	31.9.48.7 port 81
ashdgasd.exe	Jan to Mar 2014	3eeb1677da86e97a12205ff237a3df7d ab5bf9780d365c648fe39e70dc317ca5	31.9.48.7 port 1880
E.exe PDB Path: C:\Users\Syrian Malware\ Desktop\my rat\server\E\obj\ Debug\E.pdb YaAli.exe	Mar 2014	402d806f1b61753bba0ea9bc7a8f76c2	31.9.48.7 port 1520

File information	First reported	Main file MD5	Special info
ممممممممممم.exe doduu.exe rsha.exe juydghj.exe	Jan to Nov 2013	217fe391d46cfd84653e36bc05a32f44 fd42186ffe642d10ea03d5cbec0cb3a0 f8f868b750a24f1a5be6083e80b06f30 ec165a9be618283b6f37646761002f32 ea4542ef5fa6a2682b8c00f97c88ed70 deb4c47abfc873f163693e2cfc9c7800	shadye.zapto.org 178.52.223.166:1177
sent by email freedom.exe fff.exe fun.exe lu04mtrd.exe	Aug 2013 to Jan 2014	a91cf2847fa49fa5422244f85af0d3c5 af77e56fbf9259c5242adb964d0773a5 8918b499ef2015f6988e806da0df8f12 4851de5e6d72f428c4e557b91417c1b4 a91cf2847fa49fa5422244f85af0d3c5 ab3da3252b698b3c7903a824b11418ed	hacker1987.zapto.org 178.52.158.22 port 1177 46.213.188.88 port 1177 94.252.216.187 port 1177 193.227.183.171 port 1604 178.52.158.22 port 1177 178.52.203 port 80
bjwytowe.packed blob	Sept 2013 to May 2014	6c3e84a601b48eefc716936aee7c8374 f9acce2596443c80254a016f426b1c41	shaaa1983.zapto.org 46.53.11.244 port 1177 46.213.210.210 port 1063 to 1077
sexy.pif	Oct 2013	ce47d484447dff1036e2100883320431 52c3674e584ea31aef53b7dc4b2a33c5	beespy.no-ip.org 178.52.0.233 178.52.30.28 port 81 46.57.188.15
Other suspicious files هام-جيش الإسلام.rar (imp the islamic army) الأماكن العسكرية.exe (military locations) خطة دخول دوما من يبرود.exe “syrian rat.exe”	Aug 2013 to Jan 2014	978ad00b35e8ea6f280cd375778884d3 a3493689114f75a61a8102d875001429 946ab0068e5ab64c3c19fb171f55b31a before: 69133513990f6e186cded6745cfade2f after: 846983dc879f12e9dd0500434769856f bb5d66b921a4499c23a339ba2690650f 0e8e1d9bd9d7ae36cda747d6fdd284a3	216.6.0.28 and others
PDB Path: C:\Users\LOVE SYRIA\ Desktop\Syria.pdb	Nov 2013	31aeb34a57ae6b79ffa3d962316f3ec8	

Appendix 2: C&C Domains

The following is a list of domains and corresponding IP addresses used in the attacks.

C&C Domain	C&C IP addresses used	Location Notes
thejoe.publicvm.com	31.9.48.119 31.9.48.146	Syrian Telecommunications Establishment, TARASSUL ISP
thejoe.publicvm.com	31.8.48.7	31.8.48.7 is DSL for OJSC Bashinformsvyaz ISP in Russia, Bashkortostan, Beloretsk
hacker1987.zapto.org	178.52.158.22 46.213.188.88 94.252.216.187 178.52.158.22 178.52.203.80	Syriatel Mobile Telecom Syriatel 3G
hacker1987.zapto.org	193.227.183.171	IP address in Lebanon (IDM Inconet Data Management), indicating the mobility of the group members, not only within Syria, but also to nearby countries
alosh66.linkpc.net	81.9.48.11	Russian Federation VimpelCom PPPOE (Wireless broadband)
abalse.no-ip.biz	95.212.148.233	Syrian Telecommunications Establishment
aliallosh.sytes.net	69.65.5.104 (USA) 65.49.68.142 (USA)	69.65.5.104 65.49.68.142 (proxy IP)
aliallosh.sytes.net	46.57.213.64	Syrian Telecommunications Establishment
vip.all4syrian.com	31.9.48.11	Syrian Telecommunications Establishment
hhhhhkrufnrrrs1982.zapto.org	95.212.148.21 95.212.148.74	Syrian Telecommunications Establishment
basharalassad1.no-ip.biz	31.9.48.147 31.9.48.84	Syrian Telecommunications Establishment
tn4.mooo.com	31.9.48.11	Syrian Telecommunications Establishment
tn5.linkpc.net	31.9.48.11 188.139.228.179 178.52.194.35	Syrian Telecommunications Establishment

C&C Domain	C&C IP addresses used	Location Notes
xtr.all4syrian.com	31.9.48.11 82.137.200.48 from 2012	Syrian Telecommunications Establishment
xtr.all4syrian.com	200.17.216.14	IP is at UFPR Universidade Federal do Paraná, Brazil. Suspected to be SSH VPN
tn1.linkpc.net	**2014:** 178.52.108.207 178.52.166.61 **2013:** 178.52.254.161 31.9.48.11 31.9.48.1 46.213.100.97 46.213.123.97 94.252.217.145 **2012:** 178.52.165.92	Syrian Telecommunications Establishment
tn2.linkpc.net	46.213.235.105	Syriatel Mobile Telecom
fernando85.no-ip.biz	31.9.48.147	Syrian Telecommunications Establishment
meroassad.no-ip.biz	31.9.48.147	Syrian Telecommunications Establishment
shadye.zapto.org	178.52.223.166	Syrian Telecommunications Establishment
ahmdddd.no-ip.biz	31.9.48.141	Syrian Telecommunications Establishment
beespy.no-ip.org	178.52.0.233 178.52.30.28 46.57.188.15	Syrian Telecommunications Establishment
nowarsytia.no-ip.org hacars11.no-ip.biz	N/A	N/A
mail server used to send spam, dictionnary attacks were also launched from this IP	216.6.0.28	216.6.0.28 is AS6453 AS6453 - TATA COMMUNICATIONS (AMERICA) INC,US (registered Apr 18, 1996), Damascus, Syrian Arab Republic, reassigned to STE
Other (No Domain)	31.9.48.141 31.8.48.7 31.9.48.164 31.9.48.84	Syrian Telecommunications Establishment 31.8.48.7 is OJSC Bashinformsvyaz ISP in Russia