The Syrian Malware House of Cards

By GReAT on August 18, 2014. 8:00 am

RESEARCH

CYBER ESPIONAGE CYBER WAR RAT TROJAN SOCIAL ENGINEERING SYRIA

GReAT
Kaspersky Lab's Global Research & Analysis Team
@e_kaspersky/great

Our full Report

Introduction

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

The Global Research & Analysis Team (**GReAT**) at Kaspersky Lab has discovered new malware attacks in Syria, using some techniques to hide and operate malware, in addition to proficient social engineering tricks to deliver malware by tricking and tempting victims to open and launch malicious files. The malware files were found on activist sites and social networking forums, some other files were also reported by local organizations like CyberArabs and Technicians for Freedom.

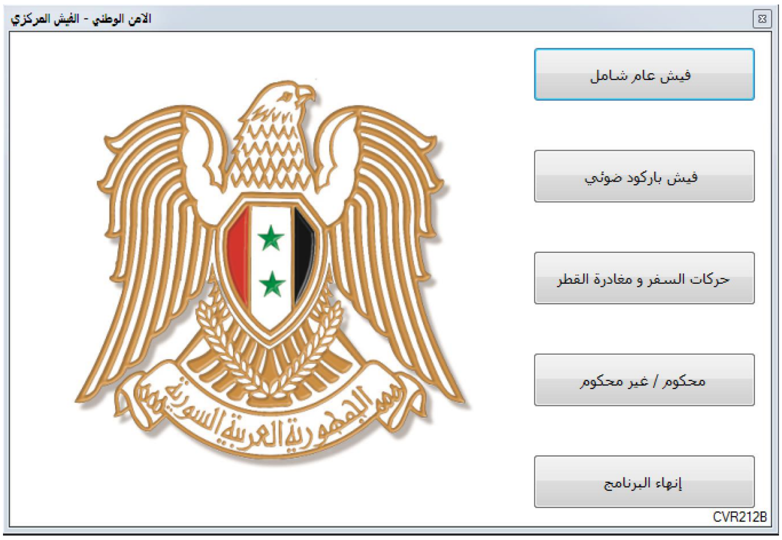
The full report detailing the attacks and related activities can be found here.

A glance at what was discovered

The number of attacks and malicious files being distributed is constantly increasing as the attackers become more organized and proficient. The samples are all based on Remote Administration Trojan Tools (RATs)
The number of malicious files found: 110
The number of domains linked to the attacks: 20
The number of IP addresses linked to the attacks: 47

The National Security Program – what the malware attacks look like

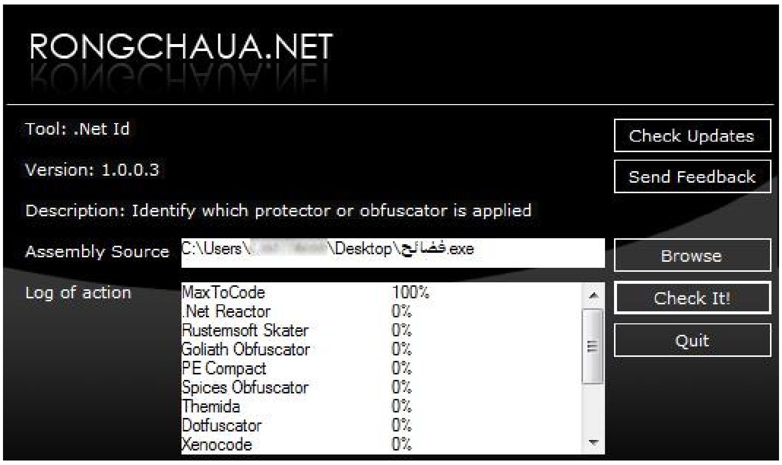
Masquerading as a reportedly “Government leaked program” that has the names of all wanted people in Syria, the National Security Program conceals a full featured RAT client to steal all sorts of information under one of its buttons.


الامن الوطني - الفيش المركزي
فيش عام شامل
فيش باركود ضوئي
حركات السفر و مغادرة القطر
محكوم / غير محكوم
إنهاء البرنامج
CVR212B
الجمهورية العربية السورية

برنامج الأمن الوطني.exe (The national security program)

Using shockingly disturbing videos to distribute malware

A disturbing video showing injured victims of recent bombings was used on YouTube to appeal to people’s fear and prompt them to download a malicious application available on a public file sharing website. After initial analysis, the file named “فضائح.exe” (Scandals.exe) proved to be heavily obfuscated with the commercial utility “MaxToCode” for .NET in order to avoid early detection by antivirus solutions.



Tool: .Net Id

Version: 1.0.0.3

Description: Identify which protector or obfuscator is applied

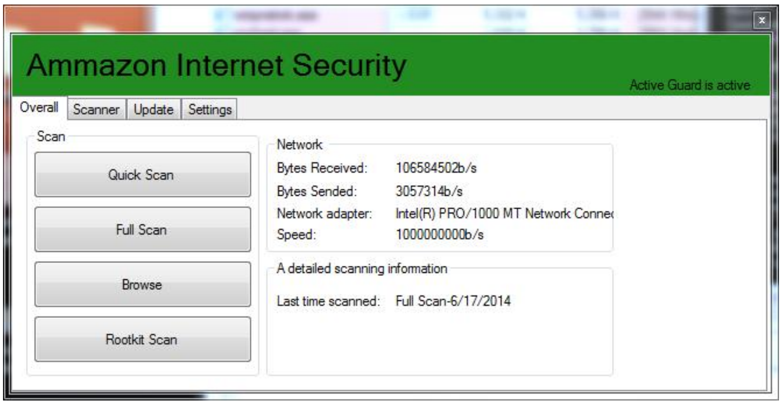
Assembly Source C:\Users\[redacted]\Desktop\فضائح.exe

Log of action

```
MaxToCode            100%
.Net Reactor         0%
Rustemsoft Skater    0%
Goliath Obfuscator   0%
PE Compact           0%
Spices Obfuscator    0%
Themida              0%
Dotfuscator          0%
Xenocode             0%
```

Did you install your “Ammazon” Security Suite?

If you thought the era of fake antiviruses was over, here comes this newly developed Syrian 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.



Network

Bytes Received: 106584502b/s

Bytes Sended: 3057314b/s

Network adapter: Intel(R) PRO/1000 MT Network Connec

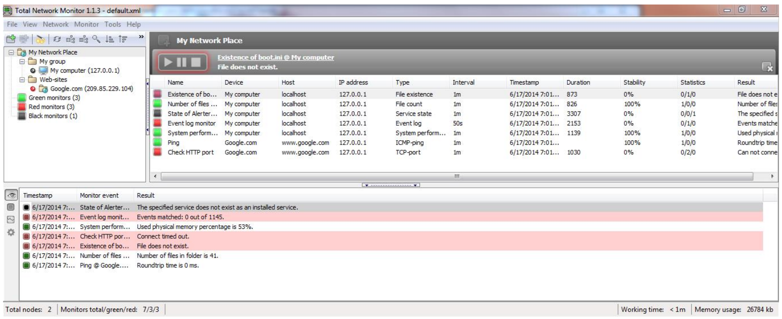
Speed: 1000000000b/s

A detailed scanning information

Last time scanned: Full Scan-6/17/2014

Your “Ammazon” is now secure, what about the rest of your network?

Total Network Monitor (which is a legitimate application) is inside another sample found, being 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 users desperate for privacy to execute these dubious programs.


Total Network Monitor 1.1.3 - default.xml
File View Network Monitor Tools Help
My Network Place

My Network Place
My group
My computer (127.0.0.1)
Web-sites
Google.com (209.85.229.104)
Green monitors (3)
Red monitors (3)
Black monitors (1)

Existence of boot.ini @ My computer
File does not exist.

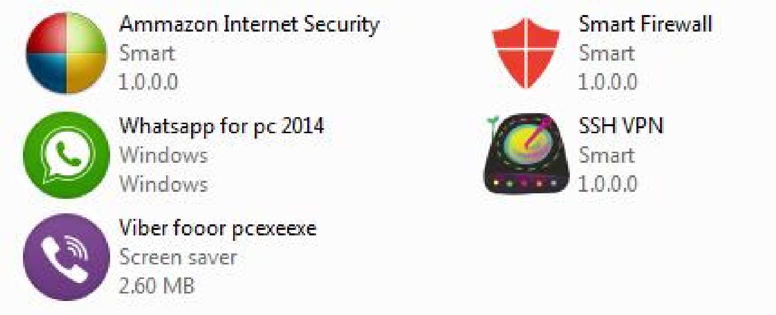
Name	Device	Host	IP address	Type	Interval	Timestamp	Duration	Stability	Statistics	Result
Existence of bo…	My computer	localhost	127.0.0.1	File existence	1m	6/17/2014 7:01…	873	0%	0/1/0	File does not e
Number of files …	My computer	localhost	127.0.0.1	File count	1m	6/17/2014 7:01…	826	100%	1/0/0	Number of file
State of Alerter…	My computer	localhost	127.0.0.1	Service state	1m	6/17/2014 7:01…	3307	0%	0/0/1	The specified s
Event log monitor	My computer	localhost	127.0.0.1	Event log	50s	6/17/2014 7:01…	2153	0%	0/1/0	Events matche
System perform…	My computer	localhost	127.0.0.1	System perform…	1m	6/17/2014 7:01…	1139	100%	1/0/0	Used physical
Ping	Google.com	www.google.com	127.0.0.1	ICMP-ping	1m	6/17/2014 7:01…		100%	1/0/0	Roundtrip time
Check HTTP port	Google.com	www.google.com	127.0.0.1	TCP-port	1m	6/17/2014 7:01…	1030	0%	0/2/0	Can not conne

Timestamp	Monitor event	Result
6/17/2014 7:…	State of Alerter…	The specified service does not exist as an installed service.
6/17/2014 7:…	Event log monit…	Events matched: 0 out of 1145.
6/17/2014 7:…	System perform…	Used physical memory percentage is 53%.
6/17/2014 7:…	Check HTTP por…	Connect timed out.
6/17/2014 7:…	Existence of bo…	File does not exist.
6/17/2014 7:…	Number of files …	Number of files in folder is 41.
6/17/2014 7:…	Ping @ Google.…	Roundtrip time is 0 ms.

Total nodes: 2 | Monitors total/green/red: 7/3/3 | Working time: < 1m | Memory usage: 26784 kb

Instant messaging, instant infection

It's also the case with other samples, where social engineering does all the heavy work. Instant messaging applications for desktop operating systems have been used in the past to spread malware and it seems Syrian malware authors have jumped on the bandwagon.



Ammazon Internet Security
Smart
1.0.0.0

Smart Firewall
Smart
1.0.0.0

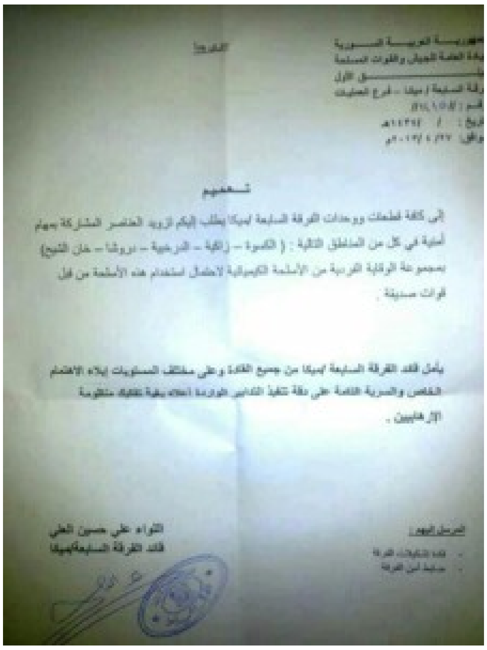
Whatsapp for pc 2014
Windows
Windows

SSH VPN
Smart
1.0.0.0

Viber fooor pcexeexe
Screen saver
2.60 MB

Beware of Chemical Attacks

Another of the attacks using social engineering tricks, the sample named Kimawi.exe (Arabic for Chemicals) with a JPG icon, is a RAT file bound to the image Kimawi.jpg. The picture is a previously leaked paper supposedly from the regime in Syria warning military units to prepare for Chemical Attacks. The file is being sent by email to selected victims.



الفوري

جمهورية العربية السورية
يادة العامة للجيش والقوات المسلحة
ـــــق الأول
رقة السابعة / ميكا – فرع العمليات
قم : ٢/١٠٥/٢١٠
ريخ : / / ١٤٣٤هـ
وافق: ٢٧ / ٤ /٢٠١٣م

تعميم

إلى كافة قطعات ووحدات الفرقة السابعة ميكا يطلب إليكم تزويد العناصر المشاركة بمهام أمنية في كل من المناطق التالية : (الكسوة – زاكية – المرجية – 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 [illegible] الإرهابيين .

اللواء علي حسين العلي
قائد الفرقة السابعة ميكا

المرسل إليهم:
- قائد تشكيلات الفرقة
- شعبة أمن الفرقة

FAQ

What is new?

The threat actors are becoming more organized, the number of attacks is increasing and the samples being used are becoming more sophisticated, while also relying extensively on powerful social engineering tricks that many people fall for.

Where are the victims and the attackers?

The victims infected when accessing the hacked forums and social networking sites tend to be ordinary users or activistshey were, or specific targets if they receive the malware via email, Skype, or messages on social networking sites.

The victims are also located outside Syria. We have seen victims of Syrian-based malware in:

1. Turkey
2. Saudi Arabia
3. Lebanon
4. Palestine
5. United Arab Emirates
6. Israel
7. Morocco

8. France
9. United States

The attackers’ command and control centers were tracked to IP addresses in Syria, Russia, Lebanon, the US and Brazil.

How many have fallen victim?

We believe the number of victims exceeds 10,000, with some of the files being downloaded more than 2000 times.

The attackers’ malware samples and variations have increased dramatically from only a few in Q1 2013 to around 40 in Q2 2014.

What is the impact on victims?

Remote Administration Trojans tools are used to fully compromise the system on victim devices. RATs are capable of stealing user credentials in addition to activating camera and microphone functionalities…

Are users protected?

Kaspersky detects and blocks all the samples that have been found. They are detected as follows:

- Trojan.MSIL.Zapchast
- Backdoor.Win32.Bifrose
- Backdoor.Win32.Fynloski
- Backdoor.Win32.Xtreme

More details and analysis of the attacks and malware samples can be found in the full report here.

Further reading

If you’d like to read more on the subject, CitizenLab and EFF have published several other good analyses of related malware and attacks:

- The Internet is Back in Syria and So is Malware Targeting Syrian Activists
- A Call to Harm: New Malware Attacks Target the Syrian Opposition
- Syrian Activists Targeted with BlackShades Spy Software
- How to Find and Protect Yourself Against the Pro-Syrian-Government Malware on Your Computer
- Fake YouTube Site Targets Syrian Activists With Malware
- Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns

Related Posts

CONTRIBUTING TO THE ANNUAL DBIR

FREEZER PAPER AROUND FREE MEAT

PNG EMBEDDED – MALICIOUS PAYLOAD HIDDEN IN A

THERE IS 1 COMMENT

If you would like to comment on this article you must first login

mohandas mv
Posted on September 29, 2014. 5:24 pm

extreemly thankfull for the informations provided

Reply