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

National Investigating Agency

VS

Sudhir Pralhad Dhawale & others

Report II

March 27, 2021

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 produced a report ("Report I") in this case on February 8, 2021 and was then asked by Mr. Wilson's defense team to produce a report regarding 24 additional files ("additional files of interest"[2]) found on Mr. Wilson's computer.

Arsenal's findings in this follow-up report can be replicated by competent digital forensics practitioners (having the necessary expertise in digital forensics, reverse engineering, etc.) with access to the forensic images obtained from Mr. Wilson's computer and the SanDisk Cruzer Blade thumb drive mentioned above.

Please note:

• It is important to understand the findings in Report I before reading this report

---

[1] Now known as Consilio

[2] Brief summaries of the additional files of interest can be found in Appendix A

- 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

II.   Executive Summary

Arsenal has determined that there is no evidence of legitimate interaction with the additional files of interest on Mr. Wilson's computer, and that 22 of the 24 of the files are directly connected to the attacker identified in Report I. Arsenal has also provided a "process tree" with this report which effectively caught the attacker red handed, by revealing both how NetWire and a temporarily deployed UnRAR (from WinRAR v4.20) were used to deliver an additional file of interest to a hidden folder on Mr. Wilson's computer, and capturing a command-line syntax mistake (and quick correction) made by the attacker. Details regarding how Mr. Wilson's computer was initially compromised, and the attacker's malware infrastructure, can be found in Report I.

III.   Additional Files of Interest

Arsenal has used many methods to identify both the source and any subsequent interaction with important files on Mr. Wilson's computer. Details on some of these methods[3] can be found in Report I. Arsenal has found no evidence which would suggest that any of the additional files of interest were ever interacted with in any legitimate way on Mr. Wilson's computer, and can confirm that 22 of the 24 files were delivered to a hidden folder on Mr. Wilson's computer by NetWire and not by other means.

The table below provides a brief summary of the additional files of interest, put in context with attacker sessions based on NTFS file system transaction information. See Exhibit A for more detail related to the table below.

Full Path on Secondary Volume	Created Time (IST)	Source	Attacker Session (IST)
\Rbackup\docs.rar	12/25/2017 22:28:49	NetWire/Direct	12/25/2017 22:28:48 - 12/25/2017 22:32:31
\Rbackup\Letter.pdf	12/25/2017 22:29:50	NetWire/RAR	12/25/2017 22:28:48 - 12/25/2017 22:32:31
\Rbackup\Final_Dispatch.rar	12/27/2017 21:23:45	NetWire/Direct	12/27/2017 21:23:45 - 12/27/2017 21:31:43
\Rbackup\Final_Dispatch.pgp	12/27/2017 21:30:55	NetWire/RAR	12/27/2017 21:23:45 - 12/27/2017 21:31:43
\Rbackup\CC5_Res\mohila meeting jan.rar	01/11/2018 11:39:40	NetWire/Direct	01/11/2018 11:39:15 - 01/11/2018 11:42:20
\Rbackup\CC5_Res\mohila meeting jan.pdf	01/11/2018 11:42:02	NetWire/RAR	01/11/2018 11:39:15 - 01/11/2018 11:42:20
\Rbackup\Accounts2k17.rar	02/01/2018 22:47:19	NetWire/Direct	02/01/2018 22:47:19 - 02/01/2018 22:49:11
\Rbackup\Accounts2k17.txt	02/01/2018 22:48:48	NetWire/Direct	02/01/2018 22:47:19 - 02/01/2018 22:49:11
\Rbackup\IMPCorres.rar	02/11/2018 15:41:17	NetWire/Direct	02/11/2018 15:41:17 - 02/11/2018 15:41:48
\Rbackup\NXPICS.rar*1	02/24/2018 02:13:23	NetWire/Direct	02/24/2018 02:04:22 - 02/24/2018 02:14:03
\Rbackup\DKComrades.rar*1	02/24/2018 02:13:23	NetWire/Direct	02/24/2018 02:04:22 - 02/24/2018 02:14:03
\Rbackup\ltr_from_Prakash.rar	03/02/2018 01:31:00	NetWire/Direct	03/02/2018 01:31:00 - 03/02/2018 01:31:04

---

[3] For example, analysis of NTFS file system metadata (such as object identifiers) and multiple types of transaction modeling

Full Path on Windows Volume	Created Time (IST)	Source	Attacker Session (IST)
\Users\Owner\AVCHDCoder\Saved files\picsdk.rar	01/22/2018 20:09:40	Suspicious*2	N/A
\Users\Owner\AVCHDCoder\Saved files\mobile.rar	02/01/2018 19:30:45	Suspicious*2	N/A

Full Path within IMPCorres.rar	Created Time (IST)	Source	Attacker Session (IST)
for your drafts.txt	N/A	NetWire/Direct*3	See IMPCorres.rar
Letter_to_GN_30July.pdf	N/A	NetWire/Direct*3	See IMPCorres.rar
ltr_CC_2_P.pdf	N/A	NetWire/Direct*3	See IMPCorres.rar
Received Naveen.doc	N/A	NetWire/Direct*3	See IMPCorres.rar
special.doc	N/A	NetWire/Direct*3	See IMPCorres.rar
\one\JP resolution.doc	N/A	NetWire/Direct*3	See IMPCorres.rar
\one\Letter to G.doc	N/A	NetWire/Direct*3	See IMPCorres.rar
\one\Loans to be cleared and future programmes.xls	N/A	NetWire/Direct*3	See IMPCorres.rar
\one\Note.doc	N/A	NetWire/Direct*3	See IMPCorres.rar
Report on Gautam Navlakha.doc	N/A	NetWire/Direct*3	See IMPCorres.rar

Table 2

*1: "NXPICS.rar" was renamed to "DKComrades.rar" on February 24, 2018 at 4:01 PM.

*2: As with the rest of the additional files of interest, Arsenal has found no evidence of legitimate interaction with "picsdk.rar" and "mobile.rar" on Mr. Wilson's computer. In addition, the location of these two files within the AVCHDCoder folder is suspicious due to them having no connection to AVCHDCoder usage.

*3: "IMPCorres.rar" was never unpacked on Mr. Wilson's computer, so these documents only exist on Mr. Wilson's computer within "IMPCorres.rar" - which the attacker delivered directly using NetWire.

One of the thumb drives seized from Mr. Wilson by the Pune police (a SanDisk Cruzer Blade, otherwise known as evidence number CyP_168_18 Ex_26), contained 7 of the 24 additional files of interest. Please see Report I (and its Exhibit E) for more information regarding attacker activities on the thumb drive. The table below contains a summary of activity involving the 7 aforementioned files on the thumb drive:

Full Path on Thumb Drive	Created (IST)	Deleted?
\System Volume Information\Accounts2k17.txt	03/14/18 16:10:18	Yes
\System Volume Information\DKComrades.rar	03/14/18 16:10:27	Yes
\System Volume Information\Final_Dispatch.pgp	03/14/18 16:10:30	Yes
\System Volume Information\IMPCorres.rar	03/14/18 16:10:51	Yes
\System Volume Information\Letter.pdf	03/14/18 16:10:53	Yes
\System Volume Information\Ltr_from_Prakash.rar	03/14/18 16:10:58	Yes

Full Path on Thumb Drive	Created (IST)	Deleted?
\System Volume Information\da-DK\mohila meeting jan.pdf	03/14/18 16:11:27	Yes
\System Volume Information\1041\Accounts2k17.txt	03/14/18 22:15:55	No
\System Volume Information\1041\DKComrades.rar	03/14/18 22:16:02	No
\System Volume Information\1041\Final_Dispatch.pgp	03/14/18 22:16:04	No
\System Volume Information\1041\IMPCorres.rar	03/14/18 22:16:24	No
\System Volume Information\1041\Letter.pdf	03/14/18 22:16:25	No
\System Volume Information\1041\Ltr_from_Prakash.rar	03/14/18 22:16:30	No
\System Volume Information\1041\CC5_Res\mohila meeting jan.pdf	03/14/18 22:16:55	No

Table 3

IV. Application Execution Analysis

Quick Heal antivirus (and other Quick Heal tools) were in use on Mr. Wilson's computer. Quick Heal's Behavior Detection System (BDS) normally stores application execution data for approximately one week, but Arsenal has recovered this application execution data from a variety of locations on Mr. Wilson's computer (in addition to intact Quick Heal databases on the active file system and backed-up within Volume Shadow Copies) which include active memory within Windows hibernation, Windows hibernation slack, file slack, and unallocated space. Arsenal has created "process trees" from this vast volume of recovered application execution data. Each process tree contains events (application executions and sometimes file creations) which rely on each other (as can be seen from process and parent process IDs, and even more uniquely from process descriptors) and flow in an orderly fashion from the first to the last. These process trees provide unique and very granular insight into particular events that have occurred on Mr. Wilson's computer over time.

One process tree which contains events from January 11, 2018, between 11:34 AM and 11:42 AM, is particularly important in regard to the additional files of interest (see Exhibit B for more details including timestamps and process descriptors):

Description	PID	PPID	File Path	Command Line
Core NetWire Process Tree	3220	0	C:\CORELDRAW\HPFFRONT.EXE	
Command Prompt Launch	4872	3220	C:\Windows\system32\cmd.exe	
Attempt to Unpack CC_5th_Res_2017_for SC-SAC-SZCs.rar	4372	4872	D:\Rbackup\CC5_Res\Adobe.exe	X CC_5TH_RES_2017_FOR SC-SAC-SZCS.RAR
Unpack CC_5th_Res_2017_for SC-SAC-SZCs.rar	7192	4872	D:\Rbackup\CC5_Res\Adobe.exe	X "CC_5TH_RES_2017_FOR SC-SAC-SZCS.RAR"
Unpack CC_Circular-1-3-2017_T,E,H_Corrected.rar	6872	4872	D:\Rbackup\CC5_Res\Adobe.exe	X "CC_CIRCULAR-1-3-2017_T
File Delivery	6872	N/A	d:\rbackup\cc5_res\cc circular-1-3-2017_eng.pdf	
File Delivery	6872	N/A	d:\rbackup\cc5_res\cc circular-1-3-2017_eng_book.pdf	
File Delivery	6872	N/A	d:\rbackup\cc5_res\cc circular-1-3-2017_eng_view.pdf	
Unpack mohila meeting jan.rar	2328	4872	D:\Rbackup\CC5_Res\Adobe.exe	X "MOHILA MEETING JAN.RAR"
File Delivery	2328	N/A	d:\rbackup\cc5_res\mohila meeting jan.pdf	

Table 4 (Note: PID = Process ID, PPID = Parent Process ID)

This process tree first reflects NetWire[4] being launched automatically on January 11, 2018 at 11:34 AM after Windows has started (more specifically, during an initial login), as BDS reports PPID 0 for processes which are launched in this manner. Arsenal recovered a script named "MTSMBlaze_v2.1.vbs" that was placed in Mr. Wilson's startup folder to ensure this particular NetWire would effectively maintain its persistence across Windows shut downs and restarts:

```
set wshell = WScript.CreateObject("WScript.Shell")



wShell.Run "cmd /c C:\CORELDRAW\hpffront.exe", 0
```

Image 1

This process tree then reflects the attacker, connected to Mr. Wilson's computer via NetWire, opening a command prompt and unpacking three files between 11:40 and 11:42 AM - one of which contains "mohila meeting jan.pdf", a document among the additional files of interest. These files are unpacked into the hidden Rbackup[5] folder using a temporarily deployed UnRAR (from WinRAR v4.20) renamed to "Adobe.exe". Please note PIDs 4372 and 7192, which are consistent with an attacker making a mistake (by omitting quotation marks when a filename contains whitespace) and then correcting that mistake.

Additional confirmation regarding the sequence of events in the process tree above can be found in Exhibit C, which contains two types of file system transactions related to this session of attacker activity. Also, the document "mohila meeting jan.pdf" has been converted to PNG image format and its two pages are being included with this report as Exhibits D1 and D2.

V. <u>Summary</u>

Arsenal has determined that there is no evidence of legitimate interaction with the additional files of interest on Mr. Wilson's computer, and that 22 of the 24 of the files are directly connected to the attacker identified in Report I. Arsenal has also provided a "process tree" with this report which effectively caught the attacker red handed, by revealing both how NetWire and a temporarily deployed UnRAR (from WinRAR v4.20) were used to deliver an additional file of interest to a hidden folder on Mr. Wilson's computer, and capturing a command-line syntax mistake (and quick correction) made by the attacker. Details regarding how Mr. Wilson's computer was initially compromised, and the attacker's malware infrastructure, can be found in Report I.

---

[4] Arsenal recovered "hpffront.exe" from active memory within Mr. Wilson's Windows hibernation and confirmed it is NetWire v1.6a Final R4

[5] More specifically, the "CC5_Res" folder within the Rbackup folder. See Report I for more detail on the Rbackup folder.

Appendix A - Brief Additional Files of Interest Summaries

docs.rar: RAR archive which contained "Letter.pdf" and was deleted after unpacking was complete.

Letter.pdf: Alleged letter from "Ki" to "A" on October 17, 2017. Includes congratulations on Maoist party's 13th anniversary and directs "A" to have a "picnic" regarding the work of Anti-Fascist Front. This document is in Hindi.

Final_Dispatch.rar: RAR archive which contained "Final_Dispatch.pgp" and was deleted after unpacking was complete.

Final_Dispatch.pgp: PGP-encrypted file.

mohila meeting jan.rar: RAR archive which contained "mohila meeting jan.pdf" and was deleted after unpacking was complete.

mohila meeting jan.pdf: Alleged "mohila" (women in Hindi/Bengali) meeting minutes from January 2, 2018. Contains a list of Maoist party members, names of some Jawaharlal Nehru University ex-student leaders, and names of organizations like "JAC", "JAGLAG", "IAPL", "CPDR", and "DSU". Mentions "Intensify tactical training for women PLGA members including booby traps/directional mines" and contains suggestions from "SG" regarding various matters. This document is in English.

Accounts2k17.rar: RAR archive delivered alongside "Accounts2k17.txt" and then deleted.

Accounts2k17.txt: Alleged details of funds transferred amongst Maoist party members. Contains details of transfers involving "Milind", "Surendra", "Shoma", "Sudhir", "Anand", "Rona", "Arun", "VV", and others. This text file is in English.

IMPCorres.rar: RAR archive containing "for your drafts.txt", "Letter_to_GN_30July.pdf", "ltr_CC_2_P.pdf", "Received Naveen.doc", "special.doc", "JP resolution.doc", "Letter to G.doc", "Loans to be cleared and future programmes.xls", "Note.doc", and "Report on Gautam Navlakha.doc".

NXPICS.rar: RAR archive renamed to DKComrades.rar.

DKComrades.rar: RAR archive which appears to contain photographs of Maoist party PLGA guerrillas.

Ltr_from_Prakash.rar: RAR archive containing "Ltr_from_Prakash.pdf" which is an alleged letter from "Prakash" to "Rona". Gives approval of a program on "Naveen Babu" at JNU. Refers to "Surendra", "Sudha", "Gadchiroli", "Mahesh Raut", and "Sudhir". Mentions that the Bhima Koregaon movement is getting weaker and discusses party initiatives to strengthen it in BJP-ruled states, in order to hit the BJP in 2019 elections. Also mentions using PGP to exchange messages and destroying the letter immediately so that the enemy does not get ahold of it. This document is in Hindi.

picsdk.rar: RAR archive which appears to contain photographs of Maoist party PLGA guerrillas.

mobile.rar: RAR archive which appears to contain a photograph of Milind Teltumbde.

for your drafts.txt: A text file that mentions "For your drafts use only" along with an email account username and password. This text file is in English.

Letter_to_GN_30July.pdf: Alleged letter from "Sudarshan" on July 30, 2017 to "Gautam Ji". Mentions state repression and says "The CC is well aware of the ground realities and difficulties faced by our comrades and party activists from CLC, PUDR, CDRO and other civil rights organizations while they are on FF missions in Bastar." Also mentions contacting Comrade Surendra and defeating "fascist forces both politically and otherwise". This document is in English.

ltr_CC_2_P.pdf: Alleged letter from "dada" (brother in Hindi/Bengali) to "Prashant" on February 10, 2017 on Maoist party Central Committee letter head. Mentions state repression and problems in communicating. Requests that legal work be sped up for particular jailed activists. Shares concerns about "Sai" and the present situation of "CRPP" in Delhi. Also requests that "SG" call on the "safe number" on particular days and times before the "final hearing". This document is in English.

Received Naveen.doc: Alleged letter from "Anand" on May 7, 2015 as a reply to a letter from "Naveen". Mentions problems coordinating with "legal mass" organizations in urban areas and updates on various military matters. Concludes with "Please destroy immediately after reading". This document is in English.

special.doc: Alleged letter from "Mahesh" to "Comrade General Secretary" of the Maoist party. The letter writer complains about his expulsion from the party while jailed, and mentions that while he broke under torture, he "guarded the major secrets". This document is in English.

JP resolution.doc: Document containing possibly obfuscated text as well as four sets of contact information.

Letter to G.doc: Alleged letter to "Comrade" that mentions coordination of international Maoist movements. Contains details about meetings held in 2010 (Greece), 2011 (Germany) and 2012 (Greece). Includes suggestions provided at the last meeting. This document is in English.

Loans to be cleared and future programmes.xls: Spreadsheet that lists "Programmes" ("All India Cordination against Military Deployment", "Maoism Seminar", etc.) and expenses, as well as loans which need to be paid back urgently. This spreadsheet is in English.

Note.doc: Document which contains what appears to be a preliminary secret encoding of cities, date/times, individuals names (including "VV" and "Anand Teltumbde"), organization names, and passwords. This document is in English.

Report on Gautam Navlakha.doc: Document which contains "A report on Gautam Navlakha (GN)". This document includes a history of various interactions with "GN". Mentions "VV" multiple times - for example: "He again walked out after his attempts to convince VV and others failed." This document is in English.