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 IV

August 18, 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 related to this report has been based 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"):

Description	Device Make/Model	Acquisition Completed	Acquisition MD5
CyP_168_18 Ex_17_1	TOSHIBA MQ01ABD050	October 8, 2018 16:21:47	91242851f09b747620c63955d5fe7235

Table 1

Arsenal was asked by Mr. Wilson's defense team to identify any references on Mr. Wilson's computer to indicators found in Amnesty International Security Lab's "NSO Group Pegasus Indicator of Compromise" (hereafter, "Pegasus Indicators") GitHub repository at https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso.

Arsenal's findings in this 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. Wilson's computer mentioned above.

II. Executive Summary

Arsenal found Pegasus Indicators on the Windows volume of Mr. Wilson's computer in two iTunes backups from an iPhone 6s, serial C7JQL293GRY9 (hereafter, "Mr. Wilson's iPhone 6s"). Timestamps associated with these indicators span from July 5, 2017 to April 10, 2018. According to the Amnesty International article "Forensic Methodology Report: How to catch NSO Group's

[1] Now known as Consilio

Pegasus”[2], the indicators found by Arsenal reflect not only Pegasus attacks, but successful Pegasus infection of Mr. Wilson’s iPhone 6s. It is important to note that during this entire timespan of Pegasus attacks and infection of Mr. Wilson’s iPhone 6s, the attacker identified in Arsenal Reports I, II, and III was using the NetWire RAT (Remote Access Trojan) on Mr. Wilson’s computer for purposes of both surveillance and incriminating document delivery.

III. Pegasus Indicators

Arsenal found Pegasus indicators on the Windows volume of Mr. Wilson’s computer in the following two iTunes backups from an iPhone 6s, serial: C7JQL293GRY9:

Full Path	Backup Time (UTC)
\Users\Owner\AppData\Roaming\Apple Computer\MobileSync\Backup\5d1781a87538a50ff197c7026174f5de674c6149	04/13/2018 07:45:37
\Users\Owner\AppData\Roaming\Apple Computer\MobileSync\Backup\5d1781a87538a50ff197c7026174f5de674c6149-20170905-111348	09/05/2017 05:17:21

Table 1

The table below provides a de-duplicated summary of the Pegasus Indicators Arsenal found (see Exhibit A for more detail):

Source	Indicator	Timestamp
DataUsage	pcsd	07/05/2017 17:11:35.865
DataUsage	pcsd	07/11/2017 10:12:02.296
sms	Maoists gun down 2 cops in encounter in Rajnandgaon, Chhattisgarh http://bit.ly/2vHMLw2	08/07/2017 13:02:07.000
sms	Gujrat ATS arrests Nagpur activist for 'seditious activities'. http://bit.ly/2wGGc9x	08/09/2017 09:28:00.000
sms	Free Dr Saibaba and Oppose the suppression of Dissent in India. Please sign the petition here clicking http://bit.ly/2vRBs3V	08/10/2017 10:12:22.000
sms	Missing Najeeb, seat cuts to dictate JNUSU elections. Read more at http://bit.ly/2wV87ab	08/31/2017 10:01:45.000
sms	Dear valued customer, UNLOCK exclusive offers designed JUST FOR YOU at : http://bit.ly/2gp2ztM	09/01/2017 12:48:09.000
sms	Justice to Dalit victims of Una-Gujarat. Ban Cow protection groups in India. Express solidarity & sign: http://bit.ly/2gwYwf1	09/04/2017 08:26:56.000
sms	Investigate the Human Rights emergency and attacks on Religious Minorities and Dalits in India.Pls sign http://bit.ly/2wAUb29	09/04/2017 13:06:46.000
sms	Jabong Clearance Sale: Flat 50% off+Extra 25% off on Top Brands. Use Code VISA25 at: http://bit.ly/2vH3gJs	09/05/2017 02:45:36.000
sms	The India Post spreads malicious propaganda of right wingers in Punjab University. Read the article : http://bit.ly/2xO56W9	09/06/2017 10:38:30.000
sms	UNHRC slams India on Rohingya, Gauri Lankesh murder and Cow lynching. Click here for details: http://bit.ly/2wdKJEW	09/15/2017 03:02:34.000

[2] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus

Source	Indicator	Timestamp
sms	Amazon to step-up FMCG discount. Flat 35% to 50%. To avail visit here: http://bit.ly/2winuWf	09/26/2017 11:15:10.000
sms	JNU Chronicles: Real-life tales of love jihad from JNU, the citadel of Indian Marxism. Read details here: http://bit.ly/2BFYvOl	01/31/2018 10:58:20.496
sms	19 Indian Nazi Tweets that will turn you into a hardliner Right Winger right now. Read here: http://bit.ly/2nuLxyN	02/02/2018 08:41:53.329
sms	This controversial website is targeting Radical\u2019 left-wing academics. Read details here: http://bit.ly/2nw1wwi	02/02/2018 12:52:21.704
sms	Padmaavat has Deepika as the hero, Ranveer as the villain, and BJP as the joker. Read full review here: http://bit.ly/2E1Jexw	02/05/2018 13:19:05.714
DataUsage	roleaccountd	02/06/2018 10:07:21.839
DataUsage	stagingd	02/06/2018 10:07:27.256
DataUsage	stagingd	03/11/2018 09:25:50.349
DataUsage	roleaccountd	03/14/2018 12:15:46.654
DataUsage	pcsd	03/14/2018 12:18:02.981
DataUsage	roleaccountd	03/16/2018 03:49:04.194
DataUsage	stagingd	03/16/2018 03:49:11.475
DataUsage	pcsd	03/16/2018 03:55:10.787
DataUsage	pcsd	03/17/2018 03:56:04.206
DataUsage	roleaccountd	03/19/2018 04:27:23.229
DataUsage	stagingd	03/19/2018 04:27:26.123
DataUsage	pcsd	03/19/2018 04:28:08.180
DataUsage	roleaccountd	03/20/2018 05:18:40.527
DataUsage	stagingd	03/20/2018 05:18:44.608
DataUsage	pcsd	03/20/2018 05:28:58.959
DataUsage	roleaccountd	03/22/2018 13:38:21.716
DataUsage	stagingd	03/22/2018 13:38:24.590
DataUsage	pcsd	03/22/2018 13:39:08.203
DataUsage	roleaccountd	03/24/2018 04:33:48.933
DataUsage	stagingd	03/24/2018 04:33:52.653
DataUsage	pcsd	03/24/2018 04:34:30.833
DataUsage	pcsd	03/25/2018 04:34:46.620
DataUsage	pcsd	03/26/2018 04:44:28.720
DataUsage	pcsd	03/27/2018 04:55:04.661
DataUsage	roleaccountd	03/28/2018 04:23:32.986

Source	Indicator	Timestamp
DataUsage	stagingd	03/28/2018 04:23:33.995
DataUsage	roleaccountd	03/29/2018 06:20:23.215
DataUsage	roleaccountd	03/29/2018 06:20:23.226
DataUsage	stagingd	03/29/2018 06:20:31.396
DataUsage	stagingd	03/29/2018 06:21:13.995
DataUsage	pcsd	03/29/2018 06:21:43.773
DataUsage	pcsd	03/29/2018 12:32:57.200
idstatuscache (thumper)	taylorjade0303@gmail.com	04/01/2018 06:26:09.259
idstatuscache (thumper)	lee.85.holland@gmail.com	04/10/2018 05:24:09.849

Table 2

IV. Summary

Arsenal found Pegasus Indicators on the Windows volume of Mr. Wilson's computer in two iTunes backups from an iPhone 6s, serial C7JQL293GRY9 (hereafter, "Mr. Wilson's iPhone 6s"). Timestamps associated with these indicators span from July 5, 2017 to April 10, 2018. According to the Amnesty International article "Forensic Methodology Report: How to catch NSO Group's Pegasus"[3], the indicators found by Arsenal reflect not only Pegasus attacks, but successful Pegasus infection of Mr. Wilson's iPhone 6s. It is important to note that during this entire timespan of Pegasus attacks and infection of Mr. Wilson's iPhone 6s, the attacker identified in Arsenal Reports I, II, and III was using the NetWire RAT (Remote Access Trojan) on Mr. Wilson's computer for purposes of both surveillance and incriminating document delivery.

Mark Spencer

Digitally signed by Mark Spencer
Date: 2021.08.18 12:23:16 -04'00'

[3] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus