Sep 23, 2021

RE: COMMONWEALTH OF PENNSYLVANIA v. Weiwu Zhao, Docket No: CP-48-CR-665-2016

To Whom It May Concern:

I, Fan Jiao, am a Silicon Valley veteran computing scientist with 32 years working experience in computer networking software design and implementation. Formerly I was a Senior Engineer Manager of Cisco Systems, and a Distinguished Engineer for Verizon. See my resume attached.

I, Xiaoyi Liu, am an IT professional in California, who has 21 years of software development in IP Security. See my resume attached.

I, Shawn Xiaochuan Wang, an IT professional at Minneapolis, Minnesota, has 26 years of software development experience across different industry domains. See my resume attached.

We believe Mr. Weiwu Zhao is a victim of illegal government hacking & planting violence, based on the facts as following:

1)All the documents that the police officers used to accuse Zhao, especially the "Police Criminal Complaint" (Complaint/Incident Number: X43-0050966, See Exhibit A), including the AFFIDAVIT of PROBABLE CAUSE authored by Trooper James Ford that, on Jan 5, 2015, Corporal Gerhard Goodyear utilized "undercover" software for remote access search on Zhao's internet-connected computer. At this point, without either search warrant or Zhao's consent, the police officers illegally and remotely intruded Zhao's computer, moreover,

2)The police officers' own computer logs (See Exhibit B) provided by themselves show that: at least during 10 days, from December 23, 2014 to January 7, 2015, without either search warrant or Zhao's consent, the police officers illegally controlled RCN(See Note 1), Zhao's ISP, to lock Zhao's home network IP address to the only one static IP address of 65.78.83.141 (See Note 2), utilizing their own multiple computers with the "undercover" software (actually the illegal hacking software), illegally, secretly, repeatedly and remotely attacked and intruded Zhao's internet-connected computers for 209 times, and remotely planted the child porn files on Zhao's hacked computer (See Exhibit C).

The logs above show that the police officers falsely testified that "but our software, again, doesn't search for specific users" (See Exhibit D, page 99).

Note 1:
"RCN" refers to "RCN Corporation", "RCN Telecom Services, Inc.", "RCN Telecom Services, LLC." (See Exhibit E). Their addresses are reportedly in Princeton, New Jersey.

Note 2:
For subscriber's IP address, RCN regulates that "By default, RCN's Internet service comes with one dynamic IP address" (See Exhibit F). Exhibit B and Exhibit G show that, the police officers illegally controlled RCN, Zhao's ISP, to lock Zhao's home network IP address to the only one static IP address of 65.78.83.141 at least until October 25, 2017, three years after the alleged "incident", making all of Zhao' computers related with this IP address as an easier hacking target at any time for themselves.

3)The police officers also remotely deleted all the child porn files (See Exhibit D, Page 97, lines 22 to 24, "there were 14 files total and were recovered from his computer"), which they remotely planted

on Zhao's computer, making impossible for the victimized Zhao to be aware that the child porn files were ever remotely planted on his computer.

4)The police officers intentionally did not search Zhao's home until nearly four months after the alleged "incident" reported by themselves, so that at that time Zhao's ISP RCN's Internet access activity logs, the key evidence for remotely planting on Zhao's computer disappear already, and it's impossible for Zhao and his lawyer to obtain it.

5)After the police officers unlawfully seized Zhao's computer, they continued to plant the child porn on Zhao's computer: without any lawful evidence, Investigating Officer Brian Mengel alleged that he "discovered file names consistent with child pornography (e.g. PTHC, 13 yo)" (See Exhibit I, page 2), the professional terms of child porn which is even unknown to majority of native English speaker, to accuse Zhao, who does not speak English as proven by themselves (See Exhibit J, page 10, lines 11 to 12).

6)Trooper James Ford admitted his capability of remotely planting child porn: "As a result of my training and experience, I am familiar with the use of computers in the collection of child pornography, the use of computers in the sexual exploitation of children and the tools and materials utilized by individuals carrying out their attacks against computer systems or by way of a computer system." (See Exhibit H, page 5).

7)Corporal Gerhard Goodyear testified: "the software that we use for -- to conduct these investigations was developed by the University of Massachusetts in conjunction with law enforcement members" (See Exhibit D, page 82)

8)Please refer to the scientific forensic report titled "Why Mr. Zhao didn't do it?" (See Exhibit C) by Mr. Bin Xie, CISSP, CISA, a senior computer network security expert witness in Texas. Based on the contents in the police officers' own computer logs (See Exhibit B), Encase Examiner Report (See Exhibit K), search warrant for Zhao's home (See Exhibit H), etc., this expert report proves that:

Firstly, in the Complaint, Trooper James Ford falsified the AFFIDAVIT of PROBABLE CAUSE about "finding a needle in a haystack" (See Exhibit C, page 1-2): when Corporate Gerhard Goodyear allegedly and remotely searched for child porn files among massive amounts of internet-connected computers [by extracting "random" sampling with the 32-digits SHA1 hash values of 4.5 million child porn files, See Exhibit I, page 84], on Jan. 5, 2015 he remotely "found" a child porn file named "苏联惹小女孩（3分钟） (1)大乳 奶 精品 收藏 无码 穴 女 少妇 强奸 另类 后门 暴 迷药.avi" (hereinafter "File A") on Mr. Zhao's computer.

Before the police officers conducted their many remote access search targeting Zhao's computers, they actually already had known before hand, based on the 32-digits SHA1 hash values of these specific child porn files, which they accused Zhao later (See Exhibit C, pages 4-7). Especially, the page 5 through page 6 of this expert report shows, on Jan 5, 2015 Corporal Gerhard Goodyear only spent 2 seconds (See Note 3), which was enormous times faster than human beings, in remotely "finding" the File A on Zhao's computer among massive amounts of internet-connected computers by extracting "random" sampling with the 32-digits SHA1 hash values of 4.5 million child porn files.

Note 3:
In sharp contrast with 2 seconds, for the police officers' physical access search on one computer, they admitted "This sorting process can take weeks or months". (See Exhibit H, page 9)

Secondly, the creation time of the File A is the SAME as the last accessed time - meaning File A was never opened on Zhao's computer. Therefore, only the police officers, who had known File A existing on Zhao's computer, were the creator who remotely planted it (See Exhibit C, pages 8-10).

The child porn file named "处女 破处 强奸 血腥.mpeg" is the same too.

Therefore, this expert report scientifically concludes that "With all the information above, that makes the police prime suspect!", which we agree.

Sincerely,


| | | |
|---|---|---|
| Fan Jiao<br>Email:<br>jiaofang gmail.com | Xiaoyi Liu<br>Email:<br>xliu92@yahoo.com | Shawn Xiaochuan Wang<br>Email:<br>shawn_xc_wang@yahoo.com |


The Exhibits:
https://drive.google.com/drive/folders/1SckV-Nmu5Q7cMHTwdcKWaXF0jGf6ZWdW?usp=sharing