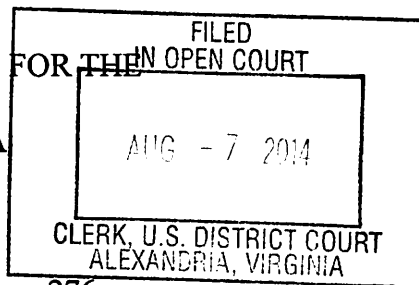


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA



Alexandria Division

UNITED STATES OF AMERICA

) Crim. No. 1:14-cr-276

) Count 1: 18 U.S.C. § 371 – Conspiracy

) Count 2: 18 U.S.C. § 2512(1)(b) – Sale of an
) Interception Device

v.

) Count 3: 18 U.S.C. § 2512(1)(c)(i) –
) Advertisement of a Known Interception
) Device

HAMMAD AKBAR,
Defendant.

) Count 4: 18 U.S.C. § 2512(1)(c)(ii) –
) Advertising a Device as an Interception
) Device

) UNDER SEAL

INDICTMENT

August 2014 Term - at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

1. Defendant HAMMAD AKBAR, and others known and unknown to the Grand Jury, marketed, advertised, and sold a mobile spyware application (“app”) that illegally intercepts wire and electronic communications made using smartphones.

2. Defendant HAMMAD AKBAR is the Chief Executive Officer of InvoCode Pvt Ltd (“InvoCode”), the company that sells the app, which is marketed as “StealthGenie.”

COUNT 1

(18 U.S.C. § 371 - Conspiracy)

THE GRAND JURY CHARGES THAT:

3. Paragraphs 1 and 2 are re-alleged and incorporated as if set forth here in their entirety.

4. From on or about November 5, 2011, to the present, in the Eastern District of Virginia and elsewhere, the defendant,

HAMMAD AKBAR,

did knowingly and intentionally combine, conspire, confederate, and agree, with other persons known and unknown to the Grand Jury, to commit offenses against the United States, namely:

- a. sale of an interception device: that is, to sell a device, knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire and electronic communications, and that such device was transported in interstate commerce and foreign commerce, in violation of Title 18, United States Code, Section 2512(1)(b);
- b. advertisement of a known interception device: that is, to disseminate by electronic means an advertisement of a device, knowing the content of the advertisement and knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire and electronic communications, in violation of Title 18, United States Code, Section 2512(1)(c)(i); and
- c. advertising a device as an interception device: that is, to disseminate by

electronic means an advertisement of a device, where such advertisement promoted the use of such device for the purpose of the surreptitious interception of wire and electronic communications, in violation of Title 18, United States Code, Section 2512(1)(c)(ii).

Ways, Manner, and Means of the Conspiracy

5. It was part of the scheme that:
 - a. Defendant and his co-conspirators created a mobile spyware app named StealthGenie. This app was designed to run on a variety of mobile smartphone platforms, including Google Inc.'s Android platform, Blackberry Limited's Blackberry platform, and Apple Inc.'s iPhone platform.
 - b. Defendant and his co-conspirators provided StealthGenie with numerous functionalities that permitted the app to intercept a variety of both outgoing and incoming wire and electronic transmissions to and from the smartphone on which it was installed. These functionalities included the interception of the following types of wire and electronic communications:
 - i. Call Recording: Records all incoming/outgoing voice calls or those specified by the purchaser of the app (hereinafter "purchaser");
 - ii. Call Interception: Allows the purchaser to intercept calls on the phone to be monitored while they take place, without the knowledge of the monitored smartphone user (hereinafter "user");

- iii. Recorded Surroundings: Allows the purchaser to call the phone and activate it at any time to monitor all surrounding conversations within a fifteen (15)-foot radius without the knowledge of the user;
 - iv. Electronic Mail: Allows the purchaser to monitor the incoming and outgoing e-mail messages of user, read their saved drafts, and view attachments;
 - v. SMS: Allows the purchaser to monitor the user's incoming and outgoing SMS messages;
 - vi. Voicemail: Allows the purchaser to monitor incoming voicemail messages;
 - vii. Contacts: Allows the purchaser to monitor the entries in the user's address book;
 - viii. Photos: Allows the purchaser to monitor the photos on the user's phone;
 - ix. Videos: Allows the purchaser to monitor the videos on the user's phone; and
 - x. Appointments: Allows the purchaser to monitor the user's calendar entries.
- c. Defendant and his co-conspirators created a website to advertise StealthGenie, and hosted this website at a U.S.-based provider, Amazon Web Services, Inc. (hereinafter "AWS"). AWS provides web hosting

services in the United States, including at a data center located in Ashburn, Virginia, which is in the Eastern District of Virginia. Language and testimonials on this website focused significantly on potential purchasers who did not have any ownership interest in the phone to be monitored, including those suspecting a spouse or romantic partner of infidelity.

- d. Defendant and his co-conspirators developed the testimonials for the website advertising StealthGenie, meaning they appear to be fictitious.
- e. Defendant and his co-conspirators sold StealthGenie at this website, to purchasers both inside and outside of the United States.
- f. Defendant and his co-conspirators operated an online portal that allowed purchasers to review the wire and electronic communications intercepted from smartphone users. The intercepted communications, which included volumes of sensitive and personal information, were also stored at AWS.
- g. Defendant and his co-conspirators programmed StealthGenie to permit the app to synchronize the wire and electronic communications intercepted by the app with the server hosting the StealthGenie website in close-to-real time. This allowed users to, at their option, review intercepted communications almost immediately, from any computer with access to the Internet.
- h. Defendant and his co-conspirators programmed StealthGenie to make the app undetectable to average smartphone users, once operational. To install the app, a purchaser needed only to obtain physical control over the phone to be monitored for a few minutes. The purchaser could then review

communications intercepted from the monitored phone without ever again having physical control over the phone.

- i. Defendant and his co-conspirators developed a business plan for the development, sale, and advertisement of StealthGenie. This document explained that “StealthGenie application [once] installed on the phone is 100% undetectable and starts to upload onto the online server instantly.” The document also noted that “[o]nce installed, the [S]tealth[G]enie application is completely undetectable and runs in the background of the mobile phone without disturbing any of the other functions running. . . . User only needs access to the target phone one time. Once installed, everything can be controlled from the online interface.”
- j. Defendant and his co-conspirators’ business plan also stated that the first target population for the marketing of the app was “[s]pousal cheat: Husband/Wife of boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behaviour or if they just want to monitor them.” The document further explained that this “[s]pousal cheat” market would likely constitute sixty-five percent (65%) of total StealthGenie purchasers, and noted, “According to our market research[,] the majority chunk of the sales will come from people suspecting their partners to be cheating on them or just wanting to keep an eye on then [sic].”

Overt Acts

6. It was further part of the conspiracy that the following acts in furtherance of and to effect the objects of the above-described conspiracy were committed in the Eastern District of Virginia and elsewhere:

- a. On or about August 21, 2010, AKBAR sent source code for the StealthGenie app to a co-conspirator.
- b. On or about February 17, 2011, AKBAR and his co-conspirators obtained web hosting services from AWS.
- c. On or about March 1, 2011, AKBAR sent a business plan for the development, sale, and advertisement of StealthGenie to a co-conspirator.
- d. On or about April 4, 2011, AKBAR sent a business plan for the development, sale, and advertisement of StealthGenie to three co-conspirators.
- e. On or about April 9, 2011, AKBAR sent drafted testimonials for the website advertising StealthGenie to a co-conspirator.
- f. On or about November 5, 2011, AKBAR and his co-conspirators disseminated by electronic means an advertisement for StealthGenie from an AWS web server hosted in Ashburn, Virginia by making the StealthGenie website available over the Internet, including in the Eastern District of Virginia and elsewhere.
- g. On or about December 19, 2011, AKBAR and his co-conspirators disseminated by electronic means an advertisement for StealthGenie from an AWS web server hosted in Ashburn, Virginia by making the

StealthGenie website available over the Internet, including in the Eastern District of Virginia and elsewhere.

- h. On or about December 14, 2012, AKBAR and his co-conspirators sold the Android version of StealthGenie to an undercover agent of the Federal Bureau of Investigation in the Eastern District of Virginia.
- i. On or about December 17, 2012, AKBAR and his co-conspirators made available wire and electronic communications intercepted from a smartphone transmitting such communications in the Eastern District of Virginia, to wit, by intercepting wire and communications from an Android smartphone operated by an undercover agent of the Federal Bureau of Investigation and then making such communications available on the StealthGenie website.
- j. On or about February 15, 2013, AKBAR and his co-conspirators disseminated by electronic means an advertisement for StealthGenie from an AWS web server hosted in Ashburn, Virginia by making the StealthGenie website available over the Internet, including in the Eastern District of Virginia and elsewhere.

(All in violation of Title 18, United States Code, Section 371).

COUNT 2

(Sale of an Interception Device – 18 U.S.C. § 2512(1)(b))

THE GRAND JURY FURTHER CHARGES THAT:

7. The factual allegations contained in Paragraphs 1 through 6 are re-alleged and incorporated as if set forth here in their entirety.

8. On December 14, 2012, in the Eastern District of Virginia, the defendant,

HAMMAD AKBAR,

sold a device, knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire and electronic communications, and that such device was transported in interstate commerce and foreign commerce.

(All in violation of Title 18, United States Code, Sections 2512(1)(b) and 2).

COUNT 3

(Advertisement of a Known Interception Device – 18 U.S.C. § 2512(1)(c)(i))

THE GRAND JURY FURTHER CHARGES THAT:

9. The factual allegations contained in Paragraphs 1 through 8 are re-alleged and incorporated as if set forth here in their entirety.

10. On or about November 5, 2011, in the Eastern District of Virginia and elsewhere, the defendant,

HAMMAD AKBAR,

disseminated by electronic means an advertisement of a device, knowing the content of the advertisement and knowing and having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire and electronic communications.

(All in violation of Title 18, United States Code, Sections 2512(1)(c)(i) and 2).

COUNT 4

(Advertising a Device as an Interception Device – 18 U.S.C. § 2512(1)(c)(ii))

THE GRAND JURY FURTHER CHARGES THAT:

11. The factual allegations contained in Paragraphs 1 through 10 are re-alleged and incorporated as if set forth here in their entirety.

12. On or about November 5, 2011, in the Eastern District of Virginia and elsewhere, the defendant,

HAMMAD AKBAR,

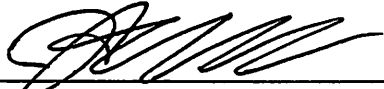
disseminated by electronic means an advertisement of a device, where such advertisement promoted the use of such device for the purpose of the surreptitious interception of wire and electronic communications.

(All in violation of Title 18, United States Code, Sections 2512(1)(c)(ii) and 2).

A TRUE BILL:

~~Pursuant to the E-Government Act,
the original of this page has been filed
electronically in the Clerk's Office.
under seal of the Grand Jury~~

DANA J. BOENTE
UNITED STATES ATTORNEY



Jay V. Prabhu
Chief, Cybercrime Unit
Assistant United States Attorney

LESLIE R. CALDWELL
ASSISTANT ATTORNEY GENERAL

William A. Hall, Jr.
Peter V. Roman
Trial Attorneys
Computer Crime & Intellectual
Property Section
Criminal Division
U.S. Department of Justice