FILED
LODGED
ENTERED
RECEIVED

MAR 17 2014

CLERK U.S. DISTRICT COURT
AT SEATTLE
WESTERN DISTRICT OF WASHINGTON
BY   DEPUTY

Magistrate Judge Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. ALEX A. KIBKALO Defendant.	CASE NO. MJ 14-114 COMPLAINT for VIOLATION Title 18, U.S.C. Section 1832

BEFORE, Mary Alice Theiler, United States Magistrate Judge, U. S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE

Theft of Trade Secrets

On or about August 18, 2012, within the Western District of Washington and elsewhere, ALEX A. KIBKALO with intent to convert trade secrets belonging to Microsoft, specifically Microsoft's Activation Server Software Development Kit, to the economic benefit of someone other than Microsoft, which trade secrets were related to and included in products that were produced for and placed in interstate and foreign commerce, did knowingly and without authorization download, upload, transmit, deliver,

COMPLAINT/Kibkalo- 1
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 send, communicate, and convey such information from Microsoft's computer system, and

2 did attempt to do so, intending and knowing that such acts would injure Microsoft.

3   All in violation of Title 18, United States Code, Section 1832(a)(2), (a)(4), and 2.

4   And the complainant states that this Complaint is based on the following

5 information:

6   I, Armando Ramirez III, being first duly sworn on oath, depose and say:

7 **INTRODUCTION AND AGENT EXPERIENCE**

8   1.   I am a Special Agent of the Federal Bureau of Investigation (FBI) currently

9 assigned to the Seattle Field Division. I have been employed as a Special Agent of the

10 FBI since May of 2006. I have received basic federal law enforcement training,

11 including the training at the FBI Academy, as well as other specialized federal law

12 enforcement training. I have participated in the investigation of numerous white collar

13 offenses, including health care fraud, financial institution fraud, copyright infringement,

14 theft of trade secrets and counterfeit goods. I have used many investigative techniques.

15 For example, I have interviewed and operated informants, conducted numerous searches,

16 interviews, and physical and electronic surveillance.

17   2.   The facts set forth in the Affidavit are based on my own personal

18 knowledge, knowledge obtained from other individuals during my participation in this

19 investigation, including review of documents and records related to this investigation,

20 communications with others who have personal knowledge of the events and

21 circumstances described herein, and information gained through my training and

22 experience.

23   3.   The information set forth below does not detail each and every fact and

24 circumstance of the investigation or all of the information known to the investigative

25 participants. Rather, this Affidavit serves solely to establish that there is probable cause

26 to believe that Alex A. Kibkalo committed the crime of Theft of Trade Secrets, in

27 violation of Title 18, United States Code, Section 1832.

28

COMPLAINT/Kibkalo- 2
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF INVESTIGATION

4.   In July 2013, Microsoft Corporation provided me the results of an internal investigation they had conducted related to the theft of Microsoft trade secrets. According to Microsoft, their investigation revealed unauthorized transmissions of proprietary and confidential Microsoft trade secrets from ALEX A. KIBKALO, a Russian national and former Microsoft employee in Lebanon, to a technology blogger in France (hereafter "the blogger"). Microsoft's investigation revealed that in July and August 2012, KIBKALO had uploaded proprietary software including pre-release software updates for Windows 8 RT and ARM devices, as well as the Microsoft Activation Server Software Development Kit (SDK) to a computer in Redmond, Washington and subsequently to his personal Windows Live SkyDrive account.

5.   According to Microsoft, the SDK is an internal product development kit that was not generally known to or readily ascertainable through proper means by the public. The SDK is used for product key validation and was distributed for internal Microsoft use only. Microsoft product teams use the SDK in customizing their product code to ensure proper validation in the product key activation process. Proper validation of product keys is part of Microsoft's efforts to protect against copyright infringement of its products.

6.   After uploading the SDK to his SkyDrive account on August 18, 2012, KIBKALO provided the blogger with links to the file on his SkyDrive account and encouraged the blogger to share the SDK with others who might be able to reverse engineer the software and write "fake activation server" code.

7.   At the conclusion of Microsoft's internal investigation, Microsoft investigators interviewed KIBKALO on September 24, 2012. KIBKALO admitted he had provided confidential Microsoft products and information to the blogger and confirmed that he did so via his SkyDrive account and the computer in Redmond, Washington. Among the products KIBKALO admitted to stealing, he listed a large number of internal unreleased "hotfixes" for Windows 8, "code for the PID generator" (a

COMPLAINT/Kibkalo- 3
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 technical description of the SDK), unreleased versions of Windows Live messenger, and

2 documents and presentations about products.

3   8.   As a result, I believe there is probable cause to find that violations of Title

4 18, United States Code, Section 1832, Theft of Trade Secrets, have been committed by

5 ALEX A. KIBKALO.

6   **RELEVANT STATUTE**

7   9.   Title 18, United States Code, Section 1832 provides that:

8   **(a)**   Whoever, with intent to convert a trade secret, that is related to a product or

9 service used in or intended for use in interstate or foreign commerce, to the economic

10 benefit of anyone other than the owner thereof, and intending or knowing that the offense

11 will, injure any owner of that trade secret, knowingly—

12   **(1)** steals, or without authorization appropriates, takes, carries away, or

13 conceals, or by fraud, artifice, or deception obtains such information;

14   **(2)** without authorization copies, duplicates, sketches, draws, photographs,

15 downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends,

16 mails, communicates, or conveys such information;

17   **(3)** receives, buys, or possesses such information, knowing the same to

18 have been stolen or appropriated, obtained, or converted without authorization;

19   **(4)** attempts to commit any offense described in paragraphs (1) through (3);

20 or,

21   **(5)** conspires with one or more other persons to commit any offense

22 described in paragraphs (1) through (3), and one or more of such persons do any act to

23 effect the object of the conspiracy,

24 shall, except as provided in subsection (b), be fined under this title or imprisoned not

25 more than 10 years, or both.

26   **THE INVESTIGATION**

27 **I.   BACKGROUND ON THE BLOGGER**

28

COMPLAINT/Kibkalo- 4
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1   10.   The blogger was known to those in the Microsoft blogging community for

2 posting screenshots of pre-release versions of the Windows Operating System. The

3 blogger began his online persona by posting Windows-related comments on forums

4 related to Microsoft products. The blogger later started posting Microsoft news and

5 information to his own websites. The blogger used his Twitter account to post comments

6 about internal Microsoft build specifications for unreleased software and news relating to

7 his latest postings. The blogger deliberately hid his identity, stating falsely that he was

8 from Quebec, and ensured that key identifying information was not posted.

9   11.   Trustworthy Computing Investigations (TWCI), a Microsoft department

10 responsible for protecting the company from external threats such as hackers, and internal

11 threats such as information leaks, had been tracking the blogger's postings and had

12 attempted to ascertain his identity prior to Kibkalo's leak. At the time, TWCI could not

13 determine if the blogger was an external party obtaining information from a contact

14 within Microsoft, or whether the blogger was a Microsoft employee.

15 II.   MICROSOFT'S INVESTIGATION

16   12.   On September 3, 2012, an outside source who requested that Microsoft not

17 reveal the source's identity, contacted Steven Sinofsky, the former President of the

18 Windows Division of Microsoft, and indicated that the source had been contacted by the

19 blogger who sent the source proprietary Microsoft code. The blogger asked the source to

20 examine the contents of the code to help the blogger better understand its contents. A

21 subsequent interview of the source by TWCI and an examination of the code determined

22 that the code transmitted to the source by the blogger was the Microsoft Server SDK

23 sample code.

24   13.   The source indicated that the blogger contacted the source using a

25 Microsoft Hotmail e-mail address that TWCI had previously connected to the blogger.

26 After confirmation that the data was Microsoft's proprietary trade secret, on September 7,

27 2012 Microsoft's Office of Legal Compliance (OLC) approved content pulls of the

28 blogger's Hotmail account.

COMPLAINT/Kibkalo- 5
USAO#2014R00100

14.   An e-mail from Microsoft employee ALEX KIBKALO was found within the blogger's Hotmail account which established that KIBKALO shared confidential Microsoft information and data with the blogger through KIBKALO's Windows Live Messenger account, akibkalo@mail.ru. Specifically, on or around July 31, 2012, KIBKALO used his akibkalo@mail.ru e-mail account to send the blogger an e-mail with the subject line of "Alex A. has shared a folder with you." That e-mail contained six zip files of pre-release "hot fixes" for Windows 8 RT for ARM devices, which KIBKALO made accessible through his SkyDrive account. The fixes were not publicly available, as Microsoft had not yet released Windows 8.

15.   The Microsoft investigation further revealed that because KIBKALO was located in Lebanon and his Microsoft corporate network connection was slow and unreliable, he elicited the assistance of an acquaintance in Washington State to set up a virtual machine on a computer server at Microsoft in Redmond, Washington. KIBKALO used the virtual machine to upload the data and products he stole from Microsoft to his SkyDrive account and then subsequently transmitted links to the materials he uploaded, to the blogger. Microsoft investigators conducted a forensic examination of the virtual machine as part of their investigation. Digital trace evidence was found on the virtual machine which contained the same files that were shared from KIBKALO's SkyDrive account to the blogger. This trace evidence included log files demonstrating KIBKALO had uploaded the Activation Server SDK to his SkyDrive account on August 18, 2012, and shared the file with the blogger.

16.   The SDK files uploaded by KIBKALO were contained in a file with the name "PIDGENXSDK RAR" which was an archive file similar to a .zip file. Microsoft's investigation showed that on August 1, 2012, KIBKALO requested access to Microsoft's Out of Band (OOB) server, which was granted on August 2, 2012. Data traces to the OOB server showed that KIBKALO accessed it on August 18, 2012, and that he subsequently placed one RAR file on his personal Windows Live SkyDrive account. Microsoft Network (MSN) chat logs later recovered from the blogger revealed

COMPLAINT/Kibkalo- 6
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1   KIBKALO notified the blogger via MSN messenger that the file was available on his

2   SkyDrive account.

3   17.   While reviewing the blogger's e-mail account, Microsoft also located

4   Instant Message (IM) communications between the blogger and KIBKALO on or around

5   September 09, 2012, in which they discussed the logistics of exchanging data amongst

6   themselves. A subsequent review of KIBKALO's accounts found references to the

7   Activation Server SDK sample code in the unallocated clusters of the virtual machine

8   used by KIBKALO, as well as in the log file for KIBKALO's SkyDrive account. The

9   sample code in KIBKALO's accounts was the same sample code that the Microsoft

10   source received from the blogger, prompting Microsoft's investigation.

11   **III.   THE STOLEN DATA**

12   **A.   Windows 8 RT Software Updates**

13   18.   According to Microsoft, the software updates that KIBKALO uploaded to

14   his SkyDrive account on or about July 31, 2012, and provided to the blogger, were pre-

15   release Windows 8 "hot fixes," which updated and corrected operating system critical

16   flaws prior to the operating system's release. These fixes are not sold separately and are

17   only distributed through Original Equipment Manufacturing (OEM) partners as preloaded

18   software or through updates to end-users. Microsoft reported that the files were not

19   published at the time KIBKALO took them, as Microsoft had not yet released Windows

20   8.

21   **B.   Activation Server SDK**

22   19.   According to Microsoft, the Activation Server Software Development Kit

23   that KIBKALO uploaded to his SkyDrive account on or about August 18, 2012, and

24   provided to the blogger, was used for product key validation and was distributed for

25   internal Microsoft use only. Its purpose was for Microsoft product teams to use in

26   customizing their product code to ensure proper validation in the product key activation

27   process. The SDK included sample code and test keys to enable product developers to

28   configure products to communicate properly with the activation servers and correctly

COMPLAINT/Kibkalo- 7
USAO#2014R00100

1   validate and activate. Therefore, the SDK was related to products that Microsoft placed

2   in interstate or foreign commerce and had independent economic value because it was

3   part of Microsoft's system of protecting its copyrights.

4   20.   Microsoft further reported, however, that the sample keys in the SDK

5   would not enable product activation or allow product key generation on their own

6   because the SDK contained obfuscated binaries and did not include the security

7   algorithm. Nonetheless, Microsoft explained that the technology within the SDK could

8   allow someone external to understand better the overall Microsoft product key validation

9   scheme. Ultimately, while the potential for harm from misuse of the SDK is generally

10 considered low, Microsoft Windows Principal Development Manager stated that the

11 samples in the SDK "could help a hacker trying to reverse engineer the code." Based on

12 Microsoft's review of KIBKALO's communications with the blogger, KIBKALO was

13 aware of this and intended to attempt to reverse engineer the SDK. For example, when

14 KIBKALO first discussed the idea of transmitting the SDK to the blogger on or around

15 August 18, 2012, KIBKALO asked if the Blogger knew any hackers who would like to

16 participate in writing fake activation server codes. KIBKALO later added that he wanted

17 a developer to "play" with the SDK to "check what is inside."

18   21.   While information regarding product activation servers is available through

19 online sites (such as http://forums.mydigitallife.info/threads/38289-Windows-8-KMS-

20 Activation and http://technet.microsoft.com/en-us/library/jj612867.aspx), information as

21 to the product key validation is not posted or distributed externally and the SDK itself is

22 not available to the public. Microsoft also takes numerous measures to protect the

23 confidentiality of the SDK including electronic access controls that monitor the use of its

24 corporate network, and physical controls including security guards, key card controlled

25 access to their buildings, and video surveillance. Employees are also advised that they

26 may not disclose Microsoft proprietary information outside of Microsoft and employees

27 are required to sign a confidentiality agreement at the beginning of their employment.

28

COMPLAINT/Kibkalo- 8
USAO#2014R00100

C.   Measures Taken by Microsoft to Protect Proprietary Information

22.   The software at issue was custom developed code designed for internal Microsoft use in producing Windows operating system products. The code was protected by copyright and kept confidential as a proprietary trade secret of Microsoft. Access and use of the software was controlled under the Windows Intellectual Property (WIP) security program.

23.   All WIP assets (Windows program builds, development tools, Software Development Kits, Windows Driver Kits, etc.) are stored on a series of file servers located in specially secured rooms on Microsoft premises. These rooms are secured and access is controlled via special card-key access rights limited to a defined set of employees. The rooms are monitored at all times by camera and alarm by Microsoft's Corporate Security team.

24.   Electronic access to WIP stored on these servers is by default restricted to those employees who are actively engaged in Windows projects and who are authenticated users on the corporate network. There is a single access control tool that is used to provision access for employees. This tool checks to ensure that an employee is assigned to a Windows project before it grants the employee access to any WIP. If an employee who is not working on a Windows project wishes access to the Windows IP they must provide a detailed justification, obtain their manager's approval, and then the approval of a sponsor within the Windows organization. If the justification is sufficient and all approvals are met then access can be granted at the discretion of the WIP security program management. Electronic files downloaded from WIP may be signed by a unique identifier to facilitate tracking back to the person who downloaded files.

25.   Electronic access to WIP is granted subject to the employee agreeing to the WIP Terms of Service (TOS). This is in addition to any Microsoft Non-Disclosure Agreement signed at the start of employment. Microsoft's TOS, signed by KIBKALO, states in part:

"By acquiring access: You agree to the following statement.

COMPLAINT/Kibkalo- 9
USAO#2014R00100

The resources (i.e. builds, source code, bug information, schedules, etc.) you are about to access constitute highly sensitive confidential and proprietary information of Microsoft Corporation. Under the terms of your employment agreement, NDA, and/or license agreement with Microsoft you are required to protect these materials. If you fail to do so, you could face civil and/or criminal liability.

These resources are provided only to you with no provision for redistribution. You may not share or attempt to share any of this information, repost this data on another server, or take any other action to distribute or disseminate these builds without express prior approval from the Windows IP Security team (WIPS).

The builds that you will be granted access to via this website are Microsoft confidential. When you download or install the build it will be signed with a unique identifier that is associated with your user credentials. By downloading these builds you are agreeing to this practice."

26. A request by KIBKALO to Microsoft for permission to distribute or disseminate the builds was neither made nor granted.

IV.   INTERVIEWS

A.   Alex Kibkalo Interview

27. KIBKALO was a seven-year employee at Microsoft who was working as a software architect in Lebanon at the time of Microsoft's investigation. He had previously worked at a location in his native Russia and had requested a transfer to Lebanon. Microsoft OLC learned shortly before the interview that KIBKALO had indicated he was leaving Microsoft. In 2012, KIBKALO received a poor performance review and threatened to resign if the review was not amended. KIBKALO was advised that the review would not be changed and that he needed to provide a formal resignation letter.

28.   KIBKALO was interviewed by Microsoft TWCI over the course of two days. He acknowledged leaking confidential and proprietary Microsoft information, products and product-related information to the blogger. KIBKALO said he met the blogger in an online forum and communicated with him three to four times a week for several months. KIBKALO acknowledged that he leaked the information via his SkyDrive account which had been uploaded to a virtual machine that was physically located in Redmond, Washington, on a Microsoft corporate machine made available to him by a friend.

B.   The Blogger Interview

29.   During his interview, the blogger admitted to posting information on Twitter and his websites, knowingly obtaining confidential and proprietary Microsoft IP from Kibkalo, and selling Windows Server activation keys on eBay.

30.   Among the items found in the blogger's home were files from his computer containing his Microsoft Network (MSN) chat history, which included chats between his account and KIBKALO's akibkalo@mail.ru account between August 2, 2012 and September 21, 2012. Within these chats were examples of the blogger trying to get KIBKALO to find pre-release software, the blogger attempting to use KIBKALO's corporate network access to access Microsoft servers, discussions about transferring data between themselves, direct discussions of KIBKALO leaking data, as well as discussions about how they might get caught. Some examples of the chats are as follows:

08/02/2012:

KIBKALO:	I would leak enterprise today probably
BLOGGER:	Hmm
	are you sure you want to do that? lol
KIBKALO:	why not?
BLOGGER:	1st time I speak with a "real" leaker since Zuko era
KIBKALO:	Mm
	To be honest, in nwin7_rtm and win7_sp1 I leaked 250GB :)

COMPLAINT/Kibkalo- 11
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1	BLOGGER:	when do you plan to leak it over the internet?
2	KIBKALO:	when would download and upload
3		I am on slow internet
4	BLOGGER:	you done this from lebanon?
5	KIBKALO:	Yes
6	BLOGGER:	wow you're crazy
7		
8	**08/03/2012:**	
9	KIBKALO:	I gonna leak server 2012
10		That is it
11	BLOGGER:	enterprise vl was leaked last night
12		
13	**08/18/2012:**	
14	KIBKALO:	Your hacker friend is in MSFT or out?
15	BLOGGER:	Out
16	KIBKALO:	Would he like to participate in writing fake activation server
17	BLOGGER:	but...his GF is now msft employee, she start in December
18	KIBKALO:	If I have sources of the real one
19	BLOGGER:	I can ask now
20	KIBKALO:	Sure
21		I have SDK, tokens, binaries, website, etc
22		need some developer to play with it, I am not
23		no commitments of course, but I won't share
24		that just for collection, - if we do that, let's
25		someone try to check what is inside
26	BLOGGER:	Asked
27		reply:
28		"that's crossing a line you know pretty illegal

COMPLAINT/Kibkalo- 12
USAO#2014R00100

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1		lol"
2	KIBKALO:	I know
3		:)
4		
5	**09/18/2012:**	
6	KIBKALO:	when i stayed at Hyatt in Bellevue, I got ISOs
7		from winbuilds like I was sitting in Building 9
8	BLOGGER:	nice!
9		you didn't keeped a VM into the building? :)
10	KIBKALO:	Lol
11		I may tell you, that in feb 2011 I sneaked to
12		building 9 at night and plugged laptop to cable
13		network instead of one servers' tried to got
14		pre build over PXE but failed, as they
15		controlled MACs
16		
17	**09/21/2012:**	
18	BLOGGER:	Lca
19		Grr
20		they scaring me
21		they have my name about leaks i think
22	KIBKALO:	Guess they can't prove it
23		otherwise we won't be speaking
24		and if they can't prove – don't care
25	BLOGGER:	Lol
26		why you think we wont speaking?
27		cuz i will be in jail?
28	KIBKALO:	:)

1 Based on my experience with Microsoft, I believe "Lca" may be a reference to

2 Microsoft's Office of Legal and Corporate Affairs.

3   **CONCLUSION**

4   31.   After the termination of KIBKALO's employment with Microsoft, he

5 relocated to Russia. Based on open source searches on the Internet, I located a LinkedIn

6 account for Alex Kibkalo that indicates he is currently working for another U.S. based

7 technology company with offices in Moscow and St. Petersburg, Russia.

8   32.   The above facts are true and correct to the best of my knowledge and belief.

9 Based on the foregoing information provided by Microsoft, to include details of the

10 company's internal investigation of Kibkalo, I submit that probable cause exists to

11 believe that Alex A. Kibkalo engaged in violations of Title 18, United States Code,

12 Section 1832, Theft of Trade Secrets.

13

14   _____

15   ARMANDO RAMIREZ III,
                                           Complainant
16   Special Agent, Federal Bureau of
                                           Investigation
17

18

19
    Based on the Complaint and Affidavit sworn to before me, and subscribed in my
20
   presence, the Court hereby finds that there is probable cause to believe the Defendant
21
   committed the offense set forth in the Complaint.
22
       Dated this _____ day of March, 2014.
23

24

25   _____

26   MARY ALICE THEILER
                                           United States Magistrate Judge
27

28

COMPLAINT/Kibkalo- 14   UNITED STATES ATTORNEY
USAO#2014R00100   700 STEWART STREET, SUITE 5220
                                                        SEATTLE, WASHINGTON 98101
                                                        (206) 553-7970