

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

MICROSOFT CORP.,

Plaintiff

v.

JOHN DOES 1-82 CONTROLLING COMPUTER
BOTNETS THEREBY INJURING MICROSOFT
AND ITS CUSTOMERS,

Defendants.

FILED UNDER SEAL

Case No.

**DECLARATION OF ZOE KRUMM IN
SUPPORT OF MICROSOFT'S
APPLICATION FOR AN EMERGENCY
TEMPORARY RESTRAINING ORDER,
SEIZURE ORDER AND ORDER TO SHOW
CAUSE RE PRELIMINARY INJUNCTION**

I, Zoe Krumm, declare as follows:

1. I am a Senior Business Intelligence Manager for the Intellectual Property Crimes Unit, a division of Microsoft's Legal and Corporate Affairs department. I make this declaration in support of Microsoft's Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge, and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein. I have worked for Microsoft since March 4, 2002. My main responsibility is the analysis of piracy related intelligence to identify, understand and respond to piracy vectors impacting sales of genuine Microsoft software. I also provide support for law enforcement proceedings in which Microsoft is a victim. Specifically, I provide analyses of business and financial records of individuals and businesses engaged in the distribution of counterfeit and infringing Microsoft products and in constructing inventory lists of seized

products obtained during search warrants. In these capacities, I have supported more than 20 civil and criminal investigations in the United States. Prior to joining Microsoft, I worked as a Business Analyst on contract to Microsoft; as a Business Manager at The Christensen Firm, LLC; and as a Legal Clerk, Records Division, at Bogle & Gates, PLLC. My degrees include a Master of Business Administration, 2012, Seattle University; Master of Education, 1997, University of Washington; and a Bachelor of Arts, Psychology, 1995, University of Washington.

A. PRODUCT ACTIVATION OVERVIEW

2. Microsoft's product activation technology is intended to enable customers to activate genuine software and receive customer service benefits from Microsoft. Product activation also helps protect Microsoft's intellectual property and reduce piracy. Product activation was implemented broadly on select products in 2001. As described below, in some instances, Microsoft's product activation technology has been attacked by pirates in order to gain unauthorized access to non-genuine software.

3. Software using the product activation technology is shipped with a unique 25-character product key. To install a product successfully, the user enters this product key which triggers the generation of a product ID. The product ID provides product information about each application including the product name, the media (if applicable), the version, the sales channel and the product language.

4. A volume license key (VLK) is a product key issued to a specific Microsoft customer under a specific license agreement and associated to a particular product. VLKs are used when prompted during installation or when a custom image is created.

5. To protect product keys and product IDs, Microsoft uses algorithms developed by Microsoft Research. The algorithms allow each key to have a unique signature.

6. Software pirates attempt to crack Microsoft's product key algorithms to generate counterfeit keys that simulate genuine behavior. In 2002 a "keygen" tool was posted to the Internet that effectively cracked the algorithm for volume license and retail Windows XP product keys. Subsequent versions of keygen tools were also distributed. These tools make it possible to create 25-character product keys which can generate product IDs identical to a genuine key.

A. Authenticity of MXDJT-W3TCG-2KGOH-YPMK3-F6CDG

7. I understand from the Declaration of Vishant Patel that the creator of the botnet known as "Citadel" promotes Citadel in part by selling a Citadel Builder Kit, and that the instructions that come with that Builder Kit provide access to a stolen copy of Window XP and an unauthorized keygen product key, "MXDJT-W3TCG-2KGQH-YPMK3-F6CDG." A true and correct copy of the relevant part of the instructions provided in the Declaration of Vishant Patel is attached hereto as Exhibit 1. This key, MXDJT-W3TCG-2KGQH-YPMK3-F6CDG, is a keygen generated Windows XP Volume license key which has been counterfeited. The key creates the same product ID as the genuine key ending in KPPDG which is assigned to a current Microsoft Volume Licensing customer. Exhibit 2 to this Declaration, which is a true and correct print out of data concerning the keygen key, shows that MXDJT-W3TCG-2KGQH-YPMK3-F6CDG was not generated by Microsoft. Exhibits 3 and 4 to this Declaration, which are true and correct print-outs of data concerning this product key, show that it corresponds to a genuine volume license key, redacted to protect customer confidentiality. The customer is a large financial institution based in the United States. This is shown in Exhibit 5, which is a true and correct print-out of data concerning this product key, redacted to protect customer confidentiality.

B. USE OF MXDJT-W3TCG-2KGQH-YPMK3-F6CDG

8. Microsoft's Windows Genuine Advantage program which is designed to allow customers to verify that their copy of Windows is genuine, shows 2107 devices that have attempted to validate Windows XP enabled by product key MXDJT-W3TCG-2KGQH-YPMK3-F6CDG. Not all Windows XP devices go through the validation process and therefore, behavior attributed to this product key is a sample of the total population. According to this data, 53% of the 2107 devices that attempted to validate using this key were from Russia, 30% from Ukraine and 4% from Belarus. The data shows that 89% of the validations indicate a system configured with Russian language, 5% Ukrainian, and 3% English. This is shown in Exhibit 6, which is true and accurate data concerning the geographic and language distribution of devices that have validated.


9. MXDJT-W3TCG-2KGQH-YPMK3-F6CDG is widely available on the Internet; a search returning over 1700 results; many in Russian language.

10. Microsoft has also received two separate piracy reports from Russian and Ukrainian customers who purchased counterfeit Microsoft software discs with the product ID consisting of 640-4969545-23 which was most likely generated by product key MXDJT-W3TCG-2KGQH-YPMK3-F6CDG.

C. CONCLUSION

11. Product key MXDJT-W3TCG-2KGQH-YPMK3-F6CDG has been distributed in significant volumes throughout the world, especially in Eastern Europe. It has been distributed as a stand-alone component via the Internet and as part of a full packaged counterfeit product sold in retail stores. Microsoft has seen this key used in 35 countries and in 18 languages.

12. All software installations enabled by product key MXDJT-W3TCG-2KGQH-



YPMK3-F6CDG are unauthorized.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 28th day of May, 2013



Zoe Krumm