

The Honorable James L. Robart

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS,

Defendants.

Case No. 2:11-CV-00222-JLR

**MICROSOFT CORPORATION'S
SECOND STATUS REPORT**

In accordance with the Court's directive, issued during the Preliminary Injunction Hearing (Docket No. 47) on April 6, 2011, Microsoft submits the following Status Report regarding its efforts to identify and serve the John Doe Defendants in this action.

Forensic Investigation of Defendants' Hard Drives

Microsoft continues to conduct a forensic investigation of Defendants' hard drives that were seized and imaged pursuant to the Court's March 9th, 2011 Temporary Restraining Order.

Initial forensic analyses have been performed on twenty of Defendants' hard drives. Initial analysis on one of the drives indicated that the system associated with the drive used an email template and the Bing, Viagra, Vicodin, and Valium trademarks. Additional evidence of the system's role in spam-dissemination was also uncovered, including custom written software relating to assembly of spam emails and text files containing thousands of email addresses and

1 username/password combinations; one text file alone contained over 427,000 email addresses.
2 The system was also used to access Russia-based websites, including mail.ru (a web-based email
3 service) and freesoft.ru (a portal for downloading free software).

4 Another of Defendants' drives includes data that indicates that the system associated with
5 the drive was the starting point for cyber-attacks into Russian IP (Internet Protocol) space.

6 The remaining 18 drives all exhibited common characteristics indicating that the systems
7 associated with them were used as TOR¹ nodes to provide anonymized internet access, and were
8 likely used to gain anonymous access to Rustock systems, such as the one described above,
9 which stored email templates, trademarks, and email addresses.

10 The forensic analysis of Defendants' drives also uncovered several email addresses that
11 were likely used in the course of testing of the system and which may be associated with
12 Defendants. Microsoft is investigating these email addresses and is propounding discovery to
13 service providers associated with the email addresses.

14 U.S. Document Subpoenas

15 Pursuant to the Court's April 11, 2011, Order Granting Leave to Conduct Third-Party
16 Discovery (Docket No. 52), Microsoft has served document subpoenas on domain registrars and
17 email providers regarding email addresses used by Defendants to sign up for the command and
18 control servers or otherwise associated with Defendants. Initial responses to this discovery
19 reveal that, to the extent payment was necessary for domain registration or email services,
20 Defendants used stolen credit cards to purchase those services. However, in addition to stolen
21 information there are a handful of further email addresses that have been identified. Microsoft
22 has propounded follow up subpoenas to determine whether further information about Defendants
23 can be identified based on these additional email addresses. Microsoft is awaiting responses to
24 those subpoenas.

25 Additional Investigation

26 Based on its review of documents collected from hosting providers and follow on

27 ¹ TOR (The Onion Router) is a system composed of client software and a network of servers that can hide
28 information about an internet user's location and other identifying characteristics. Additional description may be
found at www.torproject.org.

1 investigation, Microsoft determined that a specific Webmoney² account was used to pay for the
2 command and control servers that were used to host a portion of the Rustock infrastructure.
3 Through counsel in Moscow, Microsoft sent an Advocate Request to Webmoney to discover the
4 identity of the owner of that Webmoney account. Webmoney's records indicate that the owner
5 of the Webmoney account is identified as a Vladimir Alexandrovich Shergin, associated with an
6 address in Khimki, a city near Moscow. Microsoft is continuing its investigation to determine
7 whether the name and contact information are authentic, whether this is a stolen identity and/or
8 whether this person is associated with the events in this action. Similarly, Microsoft is
9 continuing its investigation regarding the nickname "Cosma2k" associated with the individual
10 who signed up for a number of the command and control servers. This nickname has been
11 associated with the several names: Dmitri A. Sergeev, Artem Sergeev, and Sergey
12 Vladimirovich Sergeev. Microsoft is continuing its investigation of these names, to determine
13 whether additional contact information can be identified and to which notice and service can be
14 effected.

15 Service of Process

16 Microsoft has continued service of the complaint and summonses, and all pleadings and
17 orders in this case, by publishing them on a globally accessible website, noticeofpleadings.com,
18 and by sending copies of them to each additional email address that has been identified through
19 the discovery process described above. Since the entry of the preliminary injunction, to date,
20 neither Microsoft nor Microsoft's counsel have received any communication from any Defendant
21 associated with the Rustock botnet.

22 Microsoft is in discussions with newspapers with circulation in Moscow and St. Petersburg
23 regarding placement of legal notices in newspapers in those cities. Microsoft anticipates that such
24 notices will be placed within approximately one week of this status report.

25 ///

26 ///

27 ///

28 ² Webmoney is a global online payment system widely used in Russia.

