

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

FILED

2010 FEB 22 A 9:03

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS

Defendants.

Civil Action No:

1:10CV156
(LMB/UFA)

FILED UNDER SEAL

**DECLARATION OF ANDRÉ M. DIMINO IN SUPPORT OF APPLICATION OF
MICROSOFT CORPORATION FOR AN EMERGENCY TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, André M. DiMino, declare as follows:

1. I am President and Director with The Shadowserver Foundation. I make this declaration in support of the Application of Microsoft Corporation 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.

2. The Shadowserver Foundation is a watchdog group of security professionals that gather, track, and report on malware, botnet activity, and electronic fraud. Our relevant activities

include:

- Capturing and receiving malicious software, or information related to compromised devices
- Disassembling, sandboxing, and analyzing viruses and trojans
- Monitoring and reporting on malicious attackers
- Tracking and reporting on botnet activities
- Disseminating cyber threat information
- Coordinating incident response

3. My background and experience includes malware and network traffic analysis, botnet research, intrusion detection, secure network design, penetration testing, detection and defense strategies, and network security monitoring. My Certifications and Affiliations include CISSP - GCIH - GSEC - GREM - CFCE - ISSA - HTCIA - FBI Infragard - IACIS - SANS GIAC Advisory Board - NY/NJ ECTF. My *curriculum vitae* is attached as Exhibit A to this declaration.

Overview Of Botnets

4. A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task. Although such a collection of computers can be used for useful and constructive applications, the term botnet typically refers to such a system designed and used for illegal purposes. Such systems are composed of compromised machines, often called "drones," that are assimilated without their owner's knowledge.

5. For a botnet to form and grow, it must accumulate drones, and each drone must be individually exploited, infected, and assimilated into the botnet. The more drones a botnet owner (herder) has at their disposal, the more impact the botnet may potentially have. Therefore, scanning and recruiting new drones to the botnet is a key task for the bot herder.

6. For this reason, most bot software contains spreaders that automate the task of scanning IP addresses for vulnerabilities. Once found, these vulnerable machines are attacked and infected with the bot software, and the pattern continues. With each newly compromised drone, the botnet gains more power to infect more. The only difference between a bot and a conventional worm is the existence of a unifying control system.

7. The Command and Control, or C&C, constitutes the control interface between the botnet and the herder. One common and popular control topology is Internet Relay Chat (IRC). This framework has been favored for its simplicity, flexibility, and ease of administration. Bot software is designed to connect the infected host to an IRC server and accept commands from a control channel. Although herders do not directly communicate with the bots, they must communicate with the C&C server to issue commands. Another very popular botnet communications protocol is HTTP. In this case, the attacker instructs the drone to “check in” to the HTTP C&C periodically to receive new instructions. The advantage of HTTP to the attacker is that it is usually not blocked on firewalls and the drone connection traffic may not appear anomalous to typical network IDS systems.

8. The very nature of botnets gives the bot herder a great deal of power to engage in many sophisticated criminal activities. Some of the typical activities carried out by botnets include:

- Spam
- Malware Distribution
- Click Fraud
- Distributed Denial of Service Attacks (DdoS)
- Keylogging and Identity Theft

The Waledac Botnet

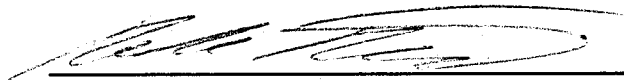
9. The complete architecture of the Waledac botnet is unknown. The botnet consists of thousands of compromised Microsoft Windows machines that are globally distributed. The botnet may be a successor of the Storm Worm botnet. Waledac appears to use a blended capability of HTTP and P2P that we call HTTP2p. When a system is infected, the malware is seeded with a list of Waledac server IP addresses that it will communicate with on TCP port 80 by passing encoded data via HTTP POST requests. Based on information we have from third-parties with insight into Waledac web server nodes, we believe they take inbound requests and then forward them to other Waledac nodes. It is unclear where these requests terminate or how the botnet master sends and receives data to the botnet. The botnet frequently sends updates and other instructions back through these web server nodes to the infected client nodes. The malware

also generally has an embedded domain name that it uses as a fall back in the event that it is not able to communicate with any of the seeded IP addresses. This domain is often used to download a new version of the malware which will have an updated list of IP addresses. Waledac domains utilize Fastflux techniques and frequently return different IP addresses of infected Waledac nodes that act as web servers.

10. Client systems are usually sent Spam E-mail templates that include e-mail addresses, subjects, bodies, and other information and are then instructed to send Spam e-mails based on those templates. Waledac has been observed to send Spam related to many different products as well as e-mail "lures" designed to further infect additional clients. Waledac tends to infect systems via e-mail Spam lures that are topical. The Spam e-mail sent to users contains links that attempt to cause users to visit those domains or IP addresses controlled by the Waledac botnet. If a user visits the link, they will find that the website attempts to get them to install executable code. This executable code is the Waledac malware. In multiple cases the websites have also delivered exploits that would install the malware without user interaction.

11. Waledac domain names generally serve two purposes. 1) They act as a distribution point for the Waledac malware and other related files that they host. Links to these domains are often sent out in the Spam e-mails in which they utilize social engineering tactics to trick people into visiting their URLs from the e-mails. These domains have TTL ("time to live") values of 0 and frequently rotate IP addresses. Various parties have extracted several thousand IP addresses of web server nodes by constantly resolving the domains. 2) The domains also serve as a fall back mechanism for the Waledac malware should it not be able to contact any of the seeded IP addresses. Some domains have also been observed simply acting as the name servers for the Fastflux botnet. In reality Waledac is a double flux botnet as the name server IPs also periodically change.

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.

A handwritten signature in black ink, appearing to be "John Doe", written over a horizontal line.

André M. DiMino

Executed this 18 day of February, 2010.

Curriculum Vitae
Andre' M. DiMino
12 Kent Rd. - Hillsdale, NJ 07642
201-497-5189
adimino77@gmail.com

Education:

Bachelor of Science, Electrical Engineering, Fairleigh Dickinson University, 1983.
Computer and Systems Emphasis.

Certifications:

- Global Information Assurance Security Essentials Certification (GSEC)- November, 2003
- Certified Information Systems Security Professional (CISSP) - March, 2006
- Global Information Assurance Certified Incident Handler (GCIH) - January, 2007
- Global Information Assurance Reverse Engineering Malware (GREM) - June, 2007
- Certified Computer Forensic Examiner (CFCE) – June, 2009

Professional Experience:

Forensic Analyst - Bergen County Prosecutor's Office December 2007 – Present

- Computer Forensic Examiner
 - Conduct forensic examinations on data extracted from seized evidence.
 - Conduct on-site “live” and “dead” forensic examinations and system analysis.
 - Proficient in EnCase and FTK, as well as open source forensic tools.
- Network and Intrusions Forensic Examiner
 - Gather and analyze network based evidence of e-fraud, “hacking” and intrusion related activity, including wireless.
- Investigations - Computer Crimes
- Assist in the execution of search warrants and evidence seizure.
- Experienced in the writing of subpoenas and probable cause statements relating to digital data preservation and acquisition.
- Declared as an Expert Witness in Digital Computer Forensics - 2008

Co-Founder & Director – The Shadowserver Foundation April 2005 – Present

- Lead all divisions in the various phases of the group's process and operation. This includes honeypot design and deployment, malware analysis, tracking and analysis of botnet and other malicious activity, network flow and traffic analysis, disseminating cyber threat information, and coordinating incident response.
- Perform detailed studies of malware infection, botnet analysis, and network traffic analysis. Develop and implement various detection and defense systems. Utilize various network security monitoring techniques including full content, session, alert, and statistical analysis to analyze botnet and malware behavior.
- Perform static and behavioral reverse engineering of malware specimens. Analyze various Web and network based attacks and correlate to detected botnet activity.
- Develop strategic alliances with outside groups and organizations to better coordinate data exchange, incident observation and research, detection and defense strategies, and process and system integration.
- Conduct training and workshops for various groups and organizations, including Federal Law Enforcement.

Independent Computer and Systems Consultant

April 2005 – December 2007

- Design and implement secure network architectures. Design and deploy intrusion detection systems. Perform vulnerability assessments and penetration testing. Design and deploy methods of mitigation and risk reduction.
- Conduct incident handling and response to security incidents including containment and recovery.

Vice President – Chief Information Officer – Skyline Displays

June 1999 - April 2005

- Chartered to build an information security organization with overall responsibility for technology risk management, information protection, and security assurance of corporate operations. Responsible for all aspects of information security, physical security, and business continuity planning.

Senior Consultant - Apostle Computer Systems

June 1994 – June 1999

- Designed enterprise network and security solutions for a variety of corporate, educational, and public-sector clients. Acted as the project manager for the life-cycle of each project.
- Advised and supported various clients in the administration and maintenance of their network infrastructure. Performed information security and vulnerability assessments. Proposed methods of mitigation and risk reduction.

IT Mgr. & Trading Strategist - GPR, Inc. - Rafferty Assoc.

June 1993 - June 1994

- Utilized the derivatives and options markets to design, develop, and implement various risk management techniques for commercial and institutional client base. Wrote a weekly market commentary for a national magazine. Provided regular market comments and observations to various financial wire services.
- Responsible for the administration and operation of the firm's network and information systems infrastructure.

June 1990 - June 1993: IT Mgr. & Technical Analyst - The Sinclair Group - R.F. Lafferty

Oct. 1988 - June 1990: Senior Sales Engineer - Telerate Systems

May 1987 - Oct. 1988: Technical Support Manager - Kentek Information Systems

May 1986 - May 1987: Business Development Mgr. - Global Teleservices

June 1982 - May 1986: Application Engineer & Technical Support Mgr - HHB Systems Inc.

Lectures and Presentations

- Information Systems Security Association - **Botnets, Detection and Defense** - January, 2007
- United States Secret Service Electronic Crimes Task Force - **Botnets and Internet Threats** - April, 2007
- Telestrategies ISS World - Invited Faculty Lecture - **Botnet Analysis** - May, 2007
- Telestrategies ISS World - Invited Faculty Lecture - **Malware Analysis** - May, 2007

- MS-ISAC - State Agency CSO Briefing - **Current Information Security Threat Landscape** - May, 2007
- University of Albany - Invited Lecture - **Server and Client Side Security Trends, Detection and Defense** - June, 2007
- Internet Security Operations and Intelligence Workshop - Washington DC - "**Correlative Analysis of Data sets for Botnet and Malicious Software Investigation**" - August, 2007
- AntiPhishing Workgroup - Pittsburgh PA - "**The Black Art of Mapping Criminal Actors to Correlative eCrime Events**" - October, 2007
- Information Systems Security Association - **Keynote Address** - November, 2007
- MS-ISAC - Webcast - **Current Trends in Internet Threats, Botnets and Malicious Software** - December, 2007
- Bergen County Municipal Police Dept. Lecture Series - **Network Security - Detection and Defense** - June 2008
- International Botnet Task Force – **Current Threat Landscape, Distributed Denial of Service Attacks** – October, 2008
- Internet2 – Collaborative Data-Driven Security for High Performance Networks – **Data Correlation and Operational Process for Internet Criminal Investigations** - May, 2009

Training and Education

- SANS Institute - "**Security Essentials**" - November 2003
- SANS Institute - "**Hacker Techniques, Exploit and Incident Handling**" - Sept. 2006
- Intelligence Support Systems for Lawful Interception, **Cybercrime Investigations** - May, 2007
- SANS Institute - "**Reverse Engineering Malware**" - June 2007
- Bergen County Law & Public Safety Inst - "**Strategies for the Recorded Interview**" - April 2008
- High Technology Crime Investigation Association - "**Next Evolution in Digital Forensics**" - April 2008
- Bergen County Law & Public Safety Inst. - "**Undercover Online Investigations**" - May, 2008
- Guidance Software - **Encase Computer Forensic Techniques** - June 2008
- National White Collar Crime Center- "**Basic Data and Recovery Analysis**" - June, 2008
- Peer-to-Peer Undercover Investigations – NJ ICAC (Internet Crimes Against Children)

Professional Associations

- Information Systems Security Association (ISSA)
- High Technology Crime Investigation Association (HTCIA)
- Institute of Electrical and Electronics Engineers (IEEE)
- SANS Global Information Assurance Advisory Board
- Federal Bureau of Investigation Infragard
- International Association of Computer Investigative Specialists (IACIS)
- International Information Systems Security Consortium
- Microsoft Botnet Task Force

Press Interviews

- Washington Post - March, 2006
- SC Magazine - June, 2006
- Washington Post - July 2006
- BBC News - October, 2006
- Dark Reading - January, 2007
- NY Times - January, 2007
- IEEE Computer Society - April, 2007
- BBC News - July, 2007
- San Francisco Chronicle - July, 2007
- SC Magazine - September, 2007
- Processor Magazine - October, 2007
- SC Magazine - November 2007
- Dark Reading - November, 2007
- Casino City Times - February, 2008
- U.S. News and World Report - August, 2008
- Agence France-Presse - August, 2008
- Corus Radio Network - Canada - August, 2008
- Christian Science Monitor - August, 2008
- SC Magazine – August, 2008
- Popular Science Magazine – September, 2008
- Dark Reading – October, 2008
- IT Conversations – November, 2008
- PaulDotCom Security Weekly – December, 2008
- SecurityFocus – June, 2009
- Financial Times – August, 2009

Software and System Proficiencies

- Network Forensic Tools
 - Wireshark, ChaosReader, Argus, Snort IDS, etc.
- Host Forensic Tools
 - EnCase, FTK, ProDiscover, SleuthKit, etc.
- Malware Analysis Tools
 - IDA-Pro, OllyDbg, LordPE, Volatility, Memoryze
- Various Penetration Testing Tools
 - Metasploit, fuzzing, nmap, BurpSuite, Paros, Nessus, Nikto, etc.
- Microsoft Operating Systems
- Linux
- Macintosh (OS-X)
- Server System Services & Applications
 - ie. DNS, SSH, Email, HTTP, Security Hardening, etc.
- Forensic and Security aspects of Internet Applications
 - Email, Peer-to-Peer, IRC, IM, etc.