Randall D. Haimovici (*Pro Hac Vice Pending*)
rhaimovici@shb.com
Rachael M. Smith (*Pro Hac Vice Pending*)
rxsmith@shb.com
SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
San Francisco, California 94104-4505
Telephone: 415.544.1900
Facsimile: 415.391.0281

Tony M. Diab (Nevada State Bar No. 12954)
tdiab@shb.com
SHOOK, HARDY & BACON L.L.P.
5 Park Plaza, Suite 1600
Irvine, California 92614-2546
Telephone: 949.475.1500
Facsimile: 949.475.0016

Robert J.B. Flummerfelt (Nevada State Bar No. 11122)
rflummerfelt@hotmail.com
Rami Hernandez (Nevada State Bar No. 13146)
rhernandeznsj@hotmail.com
CANON LAW SERVICES, LLC
7251 W. Lake Mead Blvd., Suite 300
Las Vegas, Nevada 89128
Telephone: 702.562.4144
Facsimile: 702.866.9868

Attorneys for Plaintiff
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

MICROSOFT CORPORATION, Plaintiff, vs. NASER AL MUTAIRI, an individual; MOHAMED BENABDELLAH, an individual; VITALWERKS INTERNET SOLUTIONS, LLC, d/b/a NO-IP.com; and DOES 1-500, Defendants.	Case No. 14-cv-0987 **FILED UNDER SEAL** **DECLARATION OF JASON LYONS IN SUPPORT OF APPLICATION OF MICROSOFT COPRORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE REGARDING A PRELIMINARY INJUNCTION**

I, Jason Lyons, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs group. I make this decoration in support of Microsoft's Application for an Emergency Temporary Restraining Order and Order to Show Cause Regarding 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 discussed in this declaration.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact on such threats on Microsoft's business. As part of my day to day activity I work directly with other Microsoft subject matter experts to identify, investigate and possibly neutralize threats to Microsoft.

3. I have Bachelor of Science in Liberal Arts from Excelsior College. While enlisted in the United States Army, I led investigations on security threats to government computers. After leaving the Army I worked for Xerox on its Cyber Intelligence Response Team. On that team, I investigated threats to company computers and how to mitigate those threats. Attached as **Exhibit 1** is a correct copy of my resume.

4. Microsoft is the provider of the Windows operating system and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows marks.

5. Defendant Vitalwerks provides a free Dynamic Domain Name System ("Dynamic DNS") service free to the public. DNS is the system by which computers connected to the Internet locate and communicate with other computers. A domain is simply a network location. Although domains are often associated with websites, they can also be connection points for computers with

no website interface. When a computer user types an Internet address into his web browser such as www.microsoft.com, the user's computer must resolve the domain name (microsoft.com) into an IP address (12.10.38.33). Once the IP address is known, the computer will be able to connect to the computer or server that hosts the microsoft.com website.

6. A computer will not have IP addresses for every computer on the Internet stored in its memory. Instead, this information is stored on many DNS or name servers. Collectively, these servers constitute an IP address database that serves as an address book for the Internet. If a person wants to connect to a particular domain, that person's computer will need to request the IP address from the DNS server, which will ultimately submit the request to the name server for that domain.

7. When a user enters www.microsoft.com into a web browser, his computer will reach out to a local DNS server requesting the site's IP address. The local DNS server will forward this request to an upstream DNS server, and it will reply to the local DNS server with the IP address of the authoritative name server for microsoft.com. The local DNS server will then contact the authoritative name server and request the IP address for microsoft.com, and the authoritative name server will respond with 12.10.38.33. The user's computer can then connect with the computer that hosts the microsoft.com website.

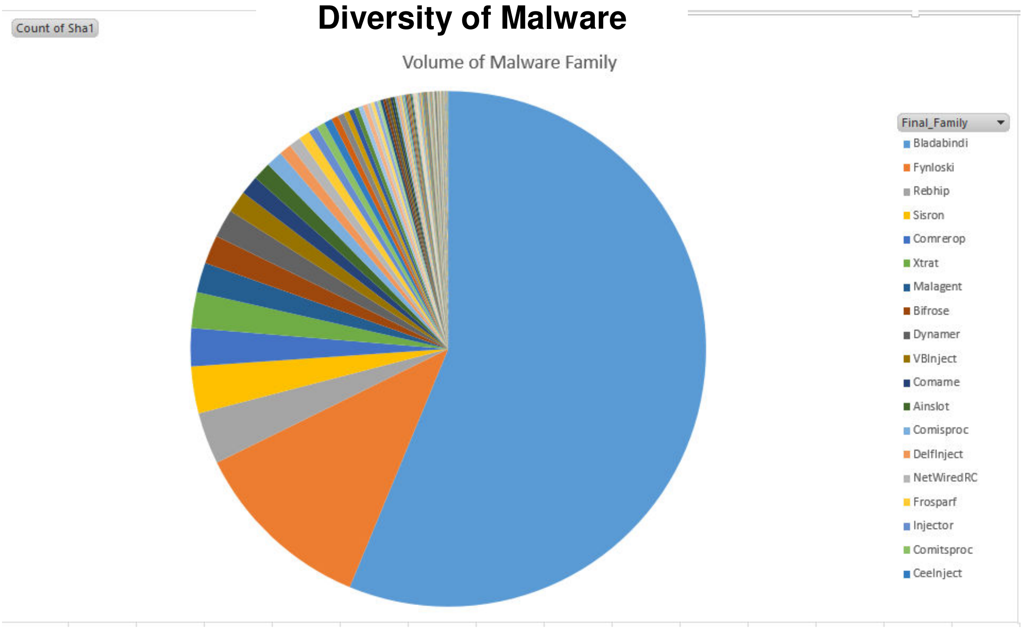
8. Computers can have either static or dynamic IP addresses. When a computer has a static or permanent IP address assigned to it, that address will be stored in the DNS database. When a request is made for the IP address for that computer's domain, the requesting computer will be directed to the authoritative name server that will have the correct IP address. However, not all computers have static IP addresses. Internet Service Providers typically provide their customers with dynamic, or changing, IP addresses because this is a more cost-effective way to do business and there is a finite number of IP addresses available. Instead of having an IP address for every customer subscribing to its Internet service, the ISP will have a smaller number of IP addresses, and it will lease an IP address to its customers' computers for a defined period of time. When the lease is up, the computer is assigned a different IP address.

9. Vitalwerks offers a free service that will constantly update IP address changes with DNS servers so that a computer user with a dynamic IP address can have a domain name that will

always point back to his computer. If a user would like to subscribe to Vitalwerks' free Dynamic DNS service, he can do so through the company's website. After creating a user name and password and giving an e-mail address, the subscriber will receive up to three domain names, which will expire in 30 days unless the subscriber renews his free service. The subscriber installs Vitalwerks' Dynamic Update Client ("DUC") to his computer, and this program will update the computer's changing IP address to Vitalwerks' name servers so that the subscriber's domain name will always point to the current IP address.

10. This case began as an investigation into the top malware threats impacting its customers. Malware is malicious software that infects computers typically without the user's knowledge or consent. To begin its investigation, Microsoft started to monitor data it was receiving from anti-malware utilities running on its consumers' computers. When malware is detected, it sends data back to Microsoft, and from this data, Microsoft can identify the type of malware, whether it can be safely removed, and whether the malware is hard coded to communicate with other computers. Microsoft detected that a significant number of cases involved malware programmed, or hard coded, to communicate with domains that we traced back to belonging to Defendant Vitalwerks operating as No-IP.

11. Although Dynamic DNS is an important service for many Internet users, it can be exploited by computer hackers and cybercriminals. As our investigation showed, Vitalwerks is functioning as a major hub for 245 varieties of malware circulating on the Internet. The figure below shows the diversity of malware that Vitalwerks supports, each a threat to Microsoft and its consumers.

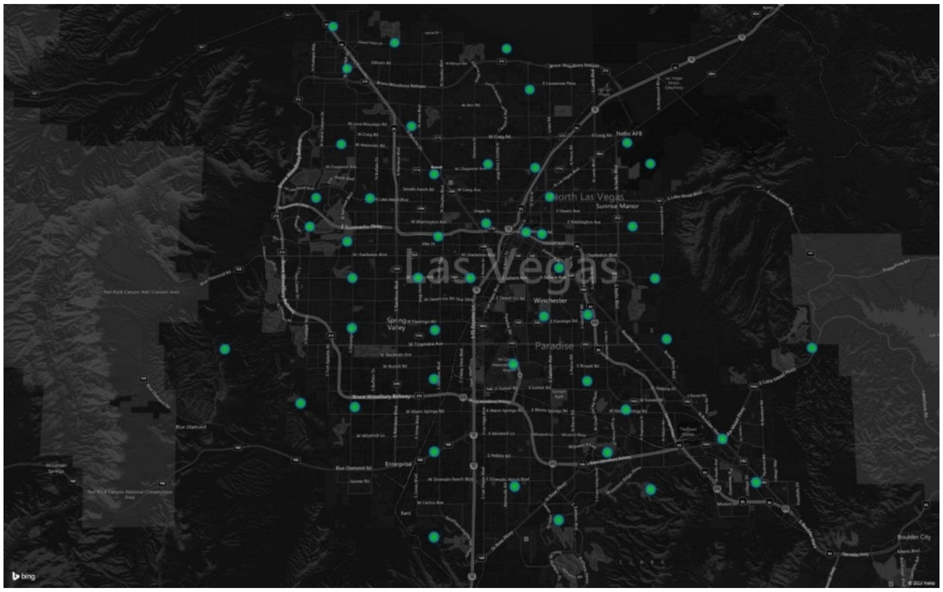


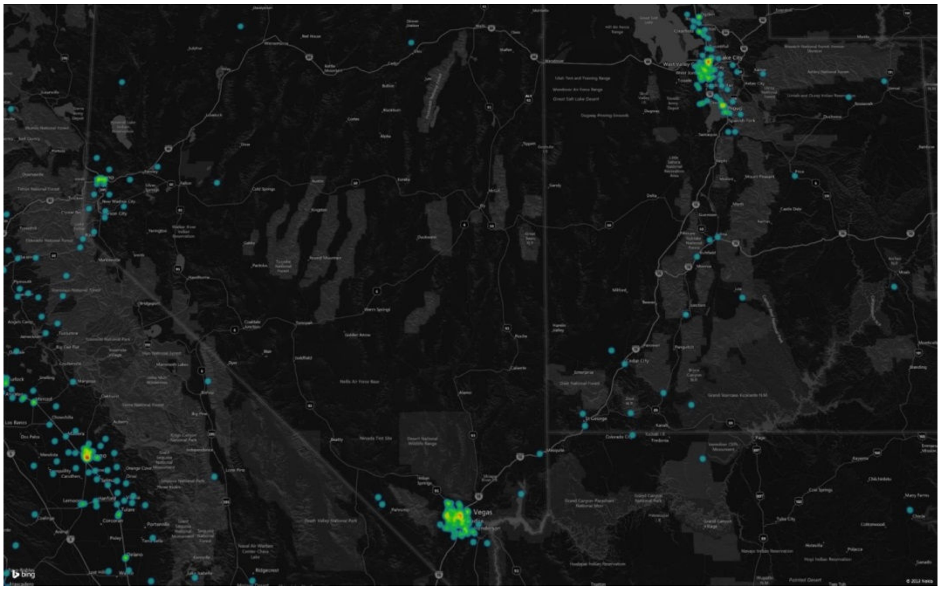
12. Through Vitalwerks sub-domains, a very large number of small, transient websites are provided a continuous Internet presence. For example, malware on a person's infected computer might be programmed to contact "hacker-0005.no-ip.biz." The person's computer would first contact no-ip.biz to get the address of the virus sub-domain, which has a dynamic IP address and is frequently changing. No-ip.biz, however, would have the current IP address due to the DUC constantly updating Vitalwerks' servers, and no-ip.biz would be able to direct the person's computer onward. Thus, the Dynamic DNS system provides computers that move from IP address to IP address a stable domain name for malware infected computers to contact. As long as that computer updates no-ip.biz as to its current IP address, malware infected machines attempting to reach it will always be able to do so.

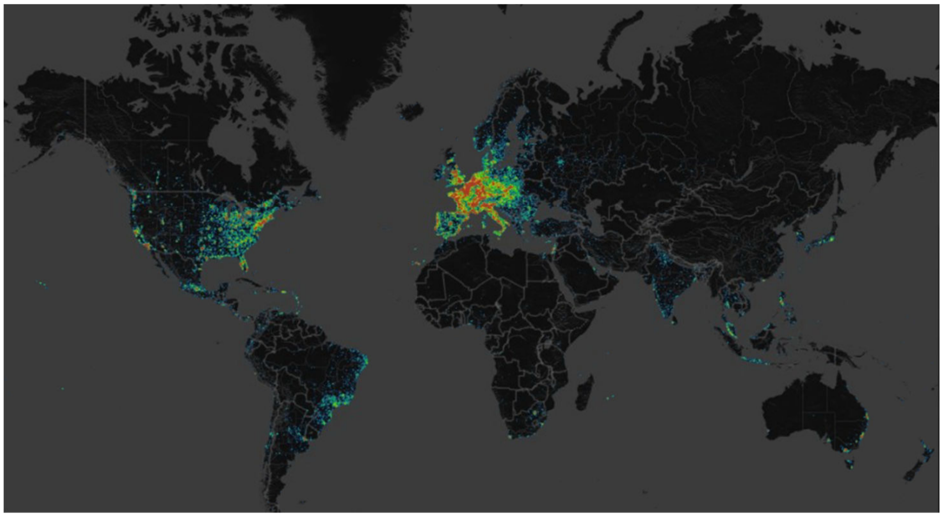
13. By studying millions of samples of malware, Microsoft has been able to identify approximately 18,472 sub-domains of Vitalwerks that are used by malware distributors, and there are likely many more. Other Internet security researchers have observed the same. The following security firms have published reports noting the abuse of Vitalwerks' Dynamic DNS service: Cisco (February, 11, 2014), Symantec (March 31, 2014), FireEye (August, 30 2013 and September 24, 2013), General Dynamics (June 28, 2013), and Open DNS Security Labs (April 2013). After the February

2014 Cisco report was published, Microsoft continues to see 2,000-3,000 new unique malware samples per month that are supported by Vitalwerks.

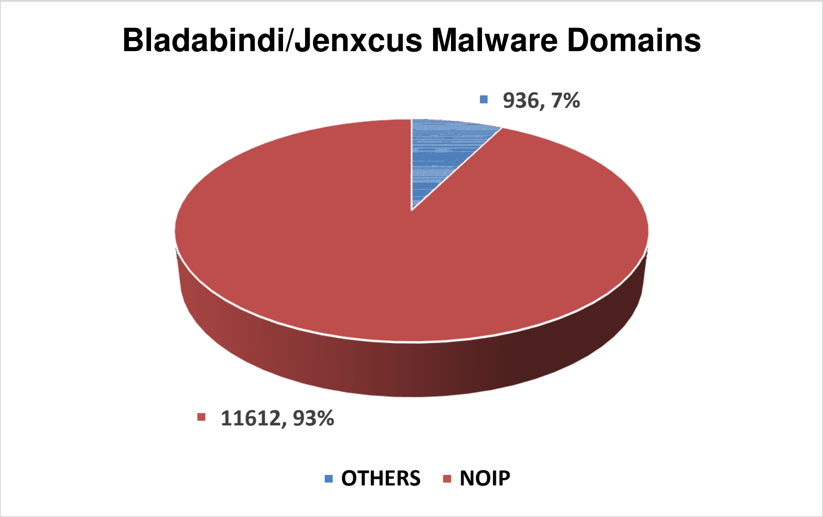
14. Based on data from Microsoft's Malware Protection Center, the spread of Bladabindi/Jenxcus has been prolific. When Microsoft started monitoring this family of malware in May 2013, there were only 51,000 detections worldwide. A "detection" is defined as either a computer was infected and has been cleaned, or there was an attempted infection that was blocked. Currently, there are approximately two million detections worldwide. Bladabindi/Jenxcus has one of the highest detection rate of any other malware that Microsoft monitors. The following is map showing the detections in Las Vegas, Nevada, and worldwide.







15. By far, the majority of malware using Vitalwerks' domains is from the Bladabindi/Jenxcus family of malware. Furthermore, as shown in the figure below, 93% of domains supporting Bladabindi/Jenxcus are Vitalwerks domains.



16. When a computer is infected with Bladabindi /Jenxcus, it becomes part of a "botnet." A botnet is a collection of individual computers, each running malware that allows communications between the infected computers to one or more other computers controlled by the distributor of the malware, typically referred to as the "command and control." Through the command-and-control computer or computers, cybercriminals are able to control the infected computer, steal information from the infected computer, and provide instructions or additional malware modules to the infected

personal computers and upload data from them. Cybercriminals often use botnets because of their ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them.

17. A Bladabindi/Jenxcus botnet consists of two tiers: the infection tier and the command-and-control tier. The infection tier is comprised of infected personal computers owned by innocent and unsuspecting people. These might be office or home desktop computers, laptop computers, computers in public libraries, and so forth.

18. Once a computer is infected with the malware and the malware has been activated, the malware will instruct the computer to contact the botnet controller's command-and-control computer. The command-and-control is the second tier of the botnet. Typically, botnets have many command-and-control computers in this tier, which are in turn controlled by a bot herder. In contrast, a Bladabindi/Jenxcus botnet consists of one command-and-control computer through which a single hacker (a Malware Defendant) communicates and controls the infected computers through the malware's dashboard. However, there can be many Bladabindi/Jenxcus botnets at any given time, each one controlled by a different Malware Defendant, creating a syndicate of botnets.

19. When a Malware Defendant creates his version of Bladabindi/Jenxcus, he programs the malware to let the infected computer know to reach out to a specific domain, which will resolve to the IP address for Malware Defendant's command-and-control computer.

20. Once the infected computer is directed to the command and control, the Malware Defendant can then directly communicate with the infected computer. Vitalwerks' domains are a significant part of the botnet infrastructure. Without Vitalwerks domains, the infected computers would not be able to locate the Malware Defendants' command-and-control computers, which have dynamic IP addresses. Through Vitalwerks' Dynamic DNS service, an infected computer is able to locate the command-and-control through the Vitalwerks sub-domain. Vitalwerks domains are the necessary means by which the first point of contact occurs between the infection tier and the command-and-control tier.

21. Defendant Vitalwerks' service is susceptible to abuse because the company does not collect or make available identifying information about its sub-domain subscribers, and failing to

keep its subscribers' user names and passwords safe, making it easy for bad actors to hack legitimate subscribers' accounts. Defendant could engage in any one of the following best practices that based on my experience, would help curtail the abuse:

- Require free Dynamic DNS subscribers to provide a name, address, telephone number, and IP address to register for a free sub-domain;
- Make the subscribers' information including sub-domain names publicly available in a searchable database;
- Use of a web reputation service that would identify bad sub-domain activity; and
- Encrypting user names and passwords and storing them someone other than the subscriber's registry.

22. In my experience, malware infections tarnish Microsoft and its products' reputation because consumers often incorrectly attribute the source of their problems to Microsoft.

23. Microsoft has devoted a significant amount of time to investigating Bladabindi/Jenxcus malware infections and helping customers determine whether or not their computers are infected, and if so, cleaning them.

24. Microsoft has observed and is aware of situations in the past in which even a hint of action against the infrastructure of cybercriminals resulted in them changing or moving their operations to avoid detection which prevented mitigation of the harm caused to the public and resulted in the destruction of evidence important to proving a claim.

I declare under the 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 on 19th day of June, 2014.

Jason Lyons