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 DAVID ANSELMI IN SUPPORT OF APPLICATION OF MICROSOFT COPRORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE REGARDING A PRELIMINARY INJUNCTION**

I, David Anselmi, 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 declaration 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 set forth herein.

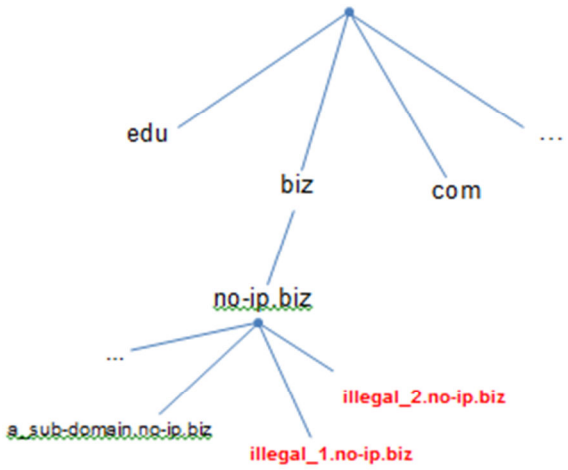
2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 reserve), attaining the rank of Lieutenant Colonel..

3. In this declaration, I will explain the steps needed to block access to Vitalwerks sub-domains being used for illegal purposes, while preserving access to Vitalwerks sub-domains being used for legal purposes, if there are any such sub-domains at Vitalwerks.

4. As explained in the declaration of my colleague, Jason Lyons, the Bladabindi/Jenxcus infected personal computers in the various botnets are programmed to contact one or more domains on the Internet. A domain can be thought of as an address on the Internet. Domains are often associated with websites, but they may just be connection points for computers with no website interfaces. After contacting these domains, the Bladabindi/Jenxcus infected personal computer will download additional malware modules or instructions. The infected personal computer can also upload information, such as stolen financial credentials, to the domain. We have determined that the infected personal computers contact sub-domains of domains owned by Vitalwerks.

A Sub-Domain Is A Sub-Address

5. A sub-domain is essentially a sub-address of another domain. The Internet address system, also referred to as the Domain Name System ("DNS"), is organized in a hierarchy in which top-level nodes branch out into lower-level nodes, and those lower level nodes branch out into still lower levels, and so on. A sub-domain is essentially an address on the Internet that is below a higher-level node in the hierarchy. The following image shows this concept, in which ".biz" is a top-level domain, "no-ip.biz" is a sub-domain of ".biz," and "illegal_1.no-ip.biz" is a sub-domain of no-ip.biz.



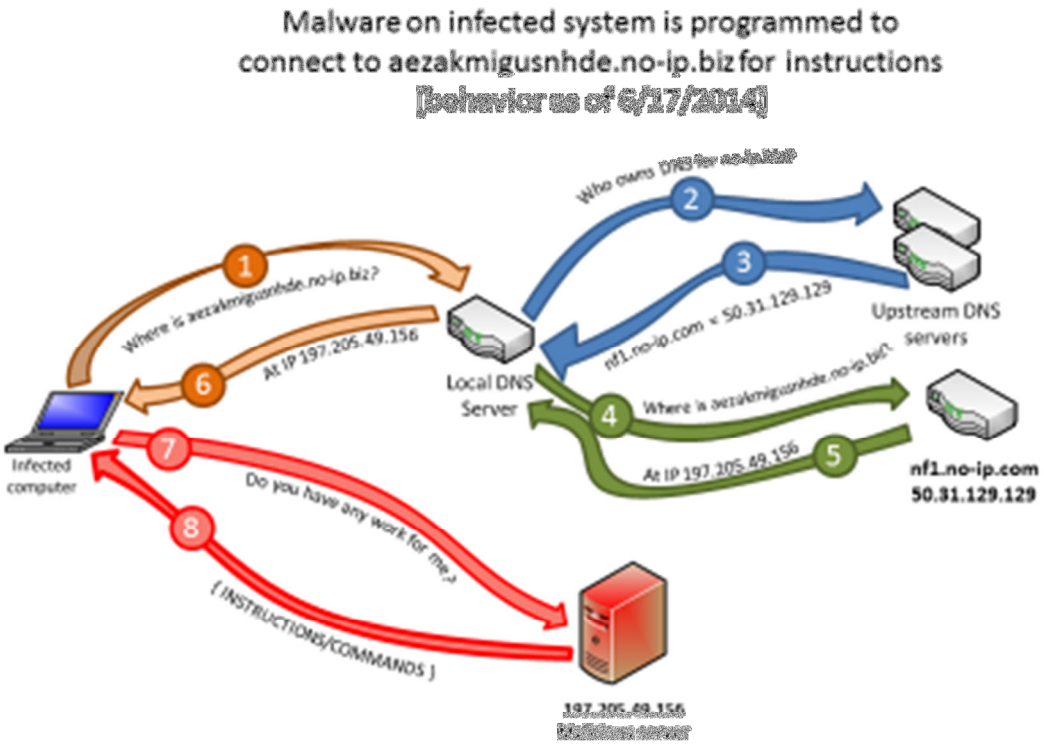
6. A helpful analogy for what a sub-domain is would be a single mailbox in a row of mailboxes in an apartment building lobby. To send a letter to someone in the apartment building, the sender must first identify the state, the city in the state, the street address of the building in the city, and finally, the apartment number of the recipient in the building. In our case, ".biz" is like the city, "no-ip" is like the apartment building, and "illegal_1" and "illegal_2" are like individual mailboxes in the building's lobby.

7. Vitalwerks, the company that runs no-ip.biz, purports to be in the business of renting sub-domains to individuals who want an address on the Internet. Vitalwerks claims to have over 18 million free dynamic DNS customers. At a high-level, Microsoft's goal is to cut-off traffic to "illegal_1.no-ip.biz," while allowing traffic through to any other sub-domains, if there are any such sub-domains at all.

8. To understand how this can be done, the way computers find addresses on the Internet needs to be explained further.

Computers Use The Domain Name Service ("DNS") To Find Other Computers On The Internet

9. When a Bladabindi/Jenxcus infected personal computer seeks to contact its command and control server, it relies on a network of servers that perform the role of keeping track of the IP address associated with every domain name on the Internet. These computers are known as Domain Name Service computers, or "DNS computers." In other words, if a person wants to connect to a website of a certain name, that person's computer needs to request the IP address of that domain from a DNS computer. This process will be explained with reference to the following figure.



10. Assume, for example, that the infected personal computer is programmed to contact "aezakmigusnhde.no-ip.biz," a sub-domain that Bladabindi/Jenxcus-infected personal computers have been seen to contact. In Step 1 of the figure, the infected personal computer contacts a local DNS server, and it asks the local DNS server for the address for aezakmigusnhde.no-ip.biz.

11. In Step 2, the local DNS server contacts an upstream DNS server at a higher level of the DNS hierarchy for that information. At the top of the hierarchy for the ".BIZ" domain, the DNS name-servers are controlled by an entity known as Neustar, Inc. which manages the name-servers.

12. In Step 3, the upstream name-server replies to the local DNS server with the address of the authoritative name server for no-ip.biz, which is, nf1.no-ip.com.

13. In Step 4, the local DNS server then contacts the nf1.no-ip.com DNS server and asks for the address for the sub-domain, aezakmigusnhde.no-ip.biz.

14. In Step 5, the authoritative name server for no-ip.biz replies with the exact address for that sub-domain.

15. In Step 6, the local DNS server sends that information back to the infected personal computer.

16. In Step 7, the Bladabindi/Jenxcus infected personal computer contacts the computer at aezakmigusnhde.no-ip.biz and asks for instructions.

17. Finally, in Step 8, the Bladabindi/Jenxcus command-and-control server replies to the infected personal computer with instructions.

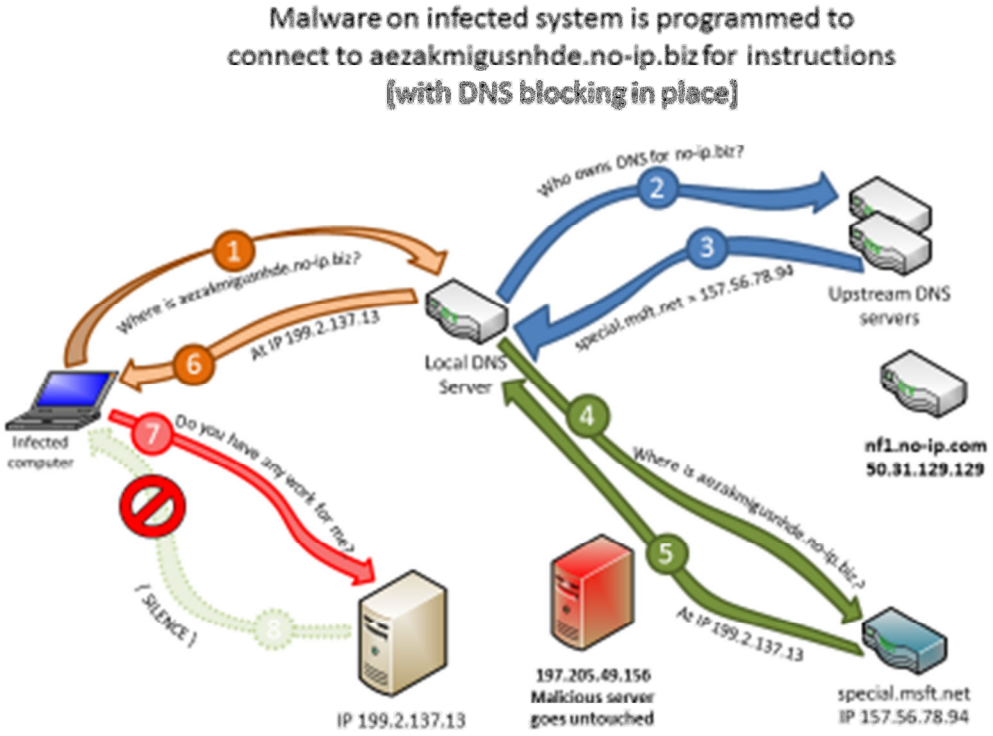
18. As can be seen, Bladabindi/Jenxcus command-and-control could not be accomplished without the use of the authoritative name servers for no-ip.biz. There are five of these, nf1.no-ip.com, nf2.no-ip.com, nf3.no-ip.com, nf4.no-ip.com, and nf5.no-ip.com.

Microsoft Can Be The "Authoritative Name Server" For Vitalwerks domains Pursuant To The Requested TRO And Preliminary Injunction

19. Microsoft's goal is to block traffic to Vitalwerks sub-domains that support malware-infected personal computers, while allowing traffic through to any other Vitalwerks sub-domains, if there are any such sub-domains. By studying thousands of samples of malware, and by watching them to see which domains they attempt to contact on the Internet, Microsoft has been able to identify approximately 18,000 sub-domains of Vitalwerks, spread across 23 domains, that are supporting malware infections. These sub-domains are listed in **Exhibit 1**, attached hereto, and the domains are listed in **Exhibit 2**.

20. In the case of the example sub-domain listed above, under the relief requested in the

TRO and Preliminary Injunction, any request for the address of no-ip.biz domains that goes to the Neustar (BIZ) top-level DNS servers would be routed to a Microsoft computer instead of the normal authoritative name server for no-ip.biz. As described above, what currently happens is that the upstream DNS servers controlled by Neustar direct the local DNS server to the authoritative name servers, ns1.no-ip.com through ns5.no-ip.com. What would happen under the requested TRO and Preliminary Injunction, is that the upstream DNS server controlled by Neustar (BIZ) would instead route the local DNS server to a special Microsoft computer that would take over the role of authoritative name server from ns1.no-ip.com through ns5.no-ip.com. This is shown in the figure below.



21. In this figure, at Step 3, the Neustar (BIZ) controlled upstream DNS server replies to requests for the address for the DNS server for no-ip.biz with the address for "special.msft.net." (Note, "special.msft.net" and "157.56.78.94" are for purposes of illustration only. They are not the actual DNS name or IP address that would be employed for this operation.).

22. In Step 4, the local DNS server requests the address for aezakmigusnhde.no-ip.biz

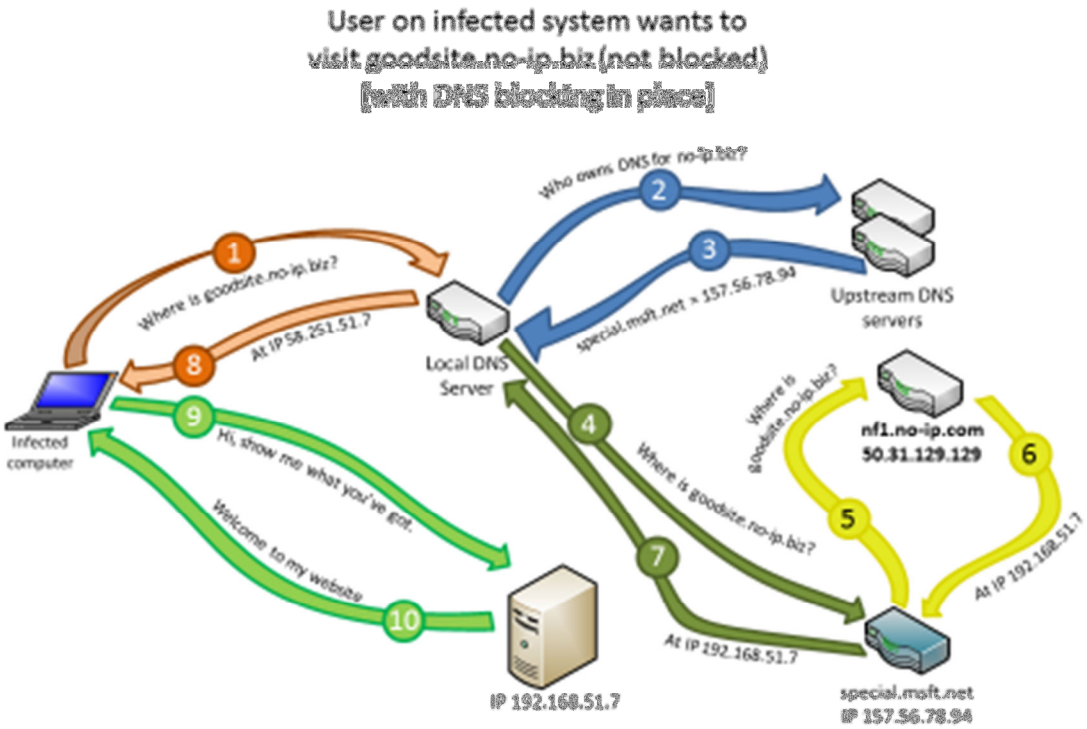
from special.msft.net. This server, managed by Microsoft, would check the requested sub-domain against its list of sub-domains known to be used by malware-infected personal computers.

23. In Step 5, assuming the requested domain is known to be associated with malware, the special.msft.net computer would reply to the local name server with the address of another Microsoft-control computer referred to as a "sinkhole computer."

24. In Step 6, the local name server sends the address of the Microsoft sinkhole computer back to the infected personal computer.

25. In Step 7, the infected personal computer contacts the sinkhole computer, which would log the time of contact and the IP address of the requesting personal computer. But it would not send any information back to the personal computer. In effect, the malware on the end-user's computer would be cut-off from its home-base.

26. If any sub-domains exist that are not on the list of Vitalwerks sub-domains that Microsoft has associated with malware, Microsoft would not interfere with communications between the client and the server. This is explained with reference to the figure below, where the user of a system wants to contact goodsite.no-ip.biz.



27. Here, after the local DNS server contacts the Microsoft-controlled computer, special.msft.net, that computer would check its block list to see if goodsite.no-ip.biz is associated with malware activity. Assuming not, at Step 5, the Microsoft computer would contact the name server for no-ip.biz, get the specific address for goodsite.no-ip.biz (Step 6), and then return the authentic IP address for the sub-domain being requested to the local DNS server (Step 7). The local DNS server would then send that to the personal computer, which would communicate directly with goodsite.no-ip.biz (Steps 7-10, respectively).

28. The relief described above can be implemented by directing third-party Registry Operators (Verisign, Inc., Neustar, Inc., Afilias, Ltd., and Public Interest Registry) to update its top-level DNS servers so that when queried for the authoritative name servers for the Vitalwerks' domains identified in Exhibit 2, they return the address of Microsoft's special name servers. This relief is requested in the proposed TRO and Preliminary Injunction.

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.

David Anselmi