

Microsoft Corporation
Law and Corporate Affairs
1401 Eye Street NW, Suite 500
Washington, DC 20005

Tel. 202-263-5900
Fax 202-263-5901 or 5902
<http://www.microsoft.com/>



November 2, 2009

Ex Parte

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: GN Docket Nos. 09-47, 09-51, and 09-137

Dear Ms. Dortch:

On November 1, 2009, Mr. Scott Charney of Microsoft provided Mr. Shomik Dutta and Mr. Carlos Kirjner of the FCC's Broadband Team with a description of a "World Health Organization" model for network security. A copy of that description is attached hereto.

Pursuant to the Commission's rules, a copy of this letter is being filed electronically in the above-referenced dockets. Please let me know if you have any questions.

Sincerely,

/s/ Paula Boyd

Paula Boyd
Regulatory Counsel for Microsoft Corp.

Attachment

From: Scott Charney
Sent: Sunday, November 01, 2009 8:11 PM
To: Shomik Dutta; Carlos Kirjner
Cc: David Pritchard; Craig Mundie; Anoop Gupta (TECHSTRAT&POLICY); Paula Boyd (LCA)
Subject: WHO Model for Network Security

Shomik, Carlos –

Shomik -- Nice to “meet” you via mail; I am sorry our schedules did not allow us to meet in person while I was in D.C. last week.

Carlos – Craig Mundie indicated you had an interest in knowing more about our WHO-related ideas and asked me to include you on this mail.

The purpose of this mail is to explain the World Health Organization (WHO) model for network security. Admittedly this mail is not as comprehensive or polished as I would like, but I understand that you need this information quickly.

The basic concept is that, not unlike the way we address human illnesses, the IT profession can engage in a more methodical examination, prevention, quarantine, and treatment of computers that may be infected with malware. This holistic approach is particularly important because of the myriad of threats faced by computer users, threats that have changed significantly over time. As I am not sure how well you are versed on the threat model, I will provide a little background here.

Over the past twenty years, threats to computer systems have changed dramatically. While early threats to computer systems involved mostly individuals exploring networks, the current threat model includes criminals (including organized crime groups) and nation states. These newer attackers are persistent, well-funded, and more technically adept. Additionally, in the early years, most attackers focused on finding vulnerabilities in products or misconfigurations in deployed systems, but as products have become more secure and tools have reduced errors in configuration management, attackers have focused increasingly on a technique that is widely successful in the consumer space: social engineering. In a social engineering attack, the attacker convinces someone to visit a compromised site (e.g., a website taken over by an attacker) or click on an attachment and thereby install malware. That malware may be a program which is designed to call back to the attacker and seek instructions. The attacker may be able to direct hundreds or even thousands of compromised machines and can direct these “botnets” to spew out spam or launch denial of service attacks against specific targets.

Faced with these threats, the IT industry has engaged in many activities designed to help mitigate risks in both the enterprise and consumer space. In the consumer space in particular, the IT industry, along with governments and consumer groups, have worked to educate users about common threats and how to mitigate them. Microsoft has also built tools to ensure that automatic installation of the latest patches and provides the Malicious Software Removal Tool (MSRT), a tool which removes known malware from consumer machines during the automatic update process. As helpful as education and these tools are, they have proven to be inadequate to the task of preventing botnets for a host of reasons. So long as some people

choose not to run automatic updates (from Microsoft or other vendors), fail to install anti-virus software, and engage in other unsafe actions such as downloading executables from unknown sources, some large number of machines will remain infected. Thus, we have recognized that we need a better process ensuring the health of the ecosystem, a process which examines machines and then treats them as necessary to ensure network health. Indeed, at least one access provider is now attempting this approach, at least in a limited fashion. See <http://www.pcmag.com/article2/0,2817,2354001,00.asp> (noting that Comcast began testing a service that alerts its broadband subscribers with pop-ups if their computers appear to be infected with malware). It is our view that this approach needs to be broadened significantly, even globally.

That said, there are practical implementation issues with any such an approach and I thought it might be wise to raise five of them here: (1) cost, (2) social acceptance, (3) technical maturity, (4) convergence, and (5) issues related to broader situational awareness. I will discuss each in turn.

The first issue is how the costs of such a program should be funded. If Comcast is successful with its service (either because reducing malware drives down network costs or because consumers are willing to pay for the service), it may be true that “market forces” are enough to drive enforcement of this model and cost becomes a non-issue. But if market forces prove insufficient and the government does not wish to create an unfunded mandate, then a different funding model must be identified. Possible solutions include a usage fee (similar to the way travelers pay a security tax on an airline ticket or phone users paid a universal access fee to ensure widespread availability of phone services) or to fund this from general tax funds (an approach that may well be appropriate if this is truly a national security and public safety issue; the Communications Assistance for Law Enforcement Act was funded in such a way).

The second issue is social acceptance; that is, whether users will find access provider scanning, quarantine and treatment acceptable. We believe that the way society addressed smoking may be illustrative. We allowed individuals to smoke – notwithstanding the health risks to smokers and the indirect costs on society (e.g., insurance costs, health care costs) – on the theory that individuals have a right to engage in certain self-destructive activities. When the EPA came out with reports on second hand smoke, however, smoking was banned in a wide range of public places. The argument was that an individual might have the right to risk their own health but they did not have the right to injure others. One could argue that computer security is not much different. Consumers have been told for years to update their systems, run anti-virus programs, and backup their data. Like smokers, they were told that the failure to follow the advice given would put them at risk. With botnets, however, one is not simply risking one’s own computer; one is putting others at risk too. Notwithstanding the parallel, we recognize that smoking has been regulated in public places and computers may sit in the most private of places (the home). That said, Internet connected users are using a shared resource that needs to be protected for the good of others.

The third issue, which is related to consumer acceptance, relates to convergence. As devices converge, denying a user access to the Internet, even for a short period, could well have damaging consequences. For example, an individual might be using their Internet device to contact emergency services and, if emergency services were made unavailable, social acceptance for examination and quarantine might wane. But there are technical solutions for

this; for example, a cell phone may require a password but still allow emergency calls to be made without logging on. In the computer context, similar accommodations could be made; the point is that these issues need to be considered. Related, it should be considered whether access providers should be granted safe harbor for engaging in protective activities that may occasionally lead to an unfortunate result.

The fourth issue relates to technical maturity. To the extent inspection leads to quarantine and treatment, the risk of false positives may raise legitimate concerns. One can reduce the risk of false positives, in part, by scanning only for those things with very well defined signatures, but that may reduce the effectiveness of the scanning activity. These trade-offs will have to be considered carefully.

Finally, there is the issue of situational awareness and how access providers and others (e.g., the government, technology vendors, and backbone providers) should share and disseminate “health” information learned through the examination process. Since malware spreads far faster than humans can react, the ability to have health information and signatures shared rapidly takes on increased importance, as does the ability to automate the detection, quarantine and treatment process itself. Today, such information is not shared for a host of reasons that has been well-documented by assorted commissions and advisory committees. These issues are, if slowly and imperfectly, being addressed. But the FCC should appreciate that the ability to rapidly share threat information and signatures will be critical to increasing the effectiveness of this model.

Anyway, those are our initial thoughts and I hope they are helpful. Please let me know if you have any questions.

Scott Charney
Corporate Vice President
Trustworthy Computing
Microsoft Corporation