Statement of Philip Reitinger

Senior Security Strategist, Microsoft Corporation

Testimony before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
U.S. House of Representatives

Hearing on "Worm and Virus Defense: How Can We Protect Our Nation's Computers from These Serious Threats?"

September 10, 2003

Chairman Putnam, Ranking Member Clay, and Members of the Subcommittee: My name is Philip Reitinger, and I am a Senior Security Strategist with Microsoft Corporation, reporting directly to our Chief Security Strategist. Before joining Microsoft, I was a Deputy Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, the Executive Director of the Department of Defense Cyber Crime Center, and the Chair of the G8 Subgroup on High Tech Crime. For some time I have been concerned with criminal threats to people and networks in the United States and around the world, and with the challenges posed in preventing, detecting, deterring, and responding to cyber crime. Accomplishing that mission – and make no mistake about it, it is a mission – requires effective action on many fronts, including improving the security of software, developing and implementing better security policies and practices, strengthening user awareness, understanding more about the threat at a tactical and strategic level, and enhancing law enforcement's capabilities.

Therefore, I want to thank you for the opportunity to appear today to share our recent experiences with the Blaster Worm and to discuss our ongoing initiatives related to software and platform development, patch management, and computer user education that we believe will, over time and in combination with effective law enforcement action, help to reduce the number of successful attacks on computer software.

I would like to begin by providing you with a brief chronology and overview of how we responded to the Blaster Worm that was launched this summer. I will next describe our commitment to Trustworthy Computing, and how it is reflected in our software and our research and development efforts. I then want to discuss the steps under way to streamline our processes for assisting computer users to implement patches to

vulnerabilities that are discovered in software. Finally, I will discuss the importance of an effective law enforcement response in order to deter and investigate cyber crime.

Microsoft's Response to the Blaster Worm

Like many commercial software vendors, we have developed a security response program – Microsoft's is state of the art. I want to use a few moments to describe our Blaster response.

- In the Spring of 2003, a customer reported that an application was not working properly. A review by Microsoft developers revealed a buffer overrun in a core communication protocol in Windows that did not initially appear to be remotely exploitable. The bug was entered into the bug database for repair, and further review indicated that it could be remotely exploitable under certain conditions. Before the repair was made and distributed broadly, an external security researcher reported finding this buffer overrun. The Microsoft Security Response Center (MSRC) investigated this second report and concluded an immediate patch was required.
- Over the next two weeks, the MSRC led an intensive effort to build, test, and release a remedy for the vulnerability. Patches were developed for seven different versions of Windows, some in twenty-five languages. Our teams worked around the clock to ensure that the patches' quality was commensurate with their installation on millions of customers' computers worldwide.

- On July 16, we released the patches and a pair of accompanying security bulletins – one for technical audiences and one for non-technical audiences – that described the vulnerability, the risk it posed to customers' computers, and the steps they should take to protect their systems. We categorized the vulnerability as "critical" – our highest rating. Within the first week of release, well over a million customers either visited the web-hosted bulletins or received them directly via email through our free Security Notification Service.
- Because of the risk the vulnerability posed, we undertook extensive measures to advise enterprise customers of the need to apply the patch immediately. We conducted conference calls with the Information Sharing and Analysis Centers (ISACs) for several industries, collaborated on an advisory issued by the CERT Coordination Center, briefed industry analysts, and through our account teams contacted customers personally and encouraged them to take appropriate steps to secure their software. We followed up this effort by sending a community bulletin to over a million of our Microsoft Certified Professionals and partners. Throughout this process, we worked closely with partners in the intrusion detection and anti-virus communities, including the Virus Information Alliance (VIA).
- We also worked to advise the general public of the situation. In conjunction with the publication of the bulletins, we contacted reporters from major news outlets such as the Associated Press and worked with trade and business reporters from various publications. We sent an alert to every customer who

had contacted our Product Support Services unit for any reason during the previous several months, and we sent another alert to subscribers to our Virus Alert system. Finally, we collaborated with the Department of Homeland Security (DHS) on its July 24 release of an advisory.

- On July 25, an organization called XFOCUS published instructions for exploiting the vulnerability. Recognizing that the release of these instructions raised the risk of attack, we contacted our customers again and undertook a second round of outreach efforts, including collaboration with DHS on an updated DHS advisory, to both technical and non-technical audiences.
- On or before August 11, the Blaster Worm was released. The worm, which used the security vulnerability as the method by which it spread, rapidly infected computers worldwide and disrupted normal operations in many networks. In response, we immediately triggered our emergency response teams – which included Premier Support Services and Microsoft Consulting Services personnel – and mobilized our security teams from across the company.
- Over the next two weeks, thousands of our employees worked around the clock to provide customers with information about the worm (and its subsequently released variants), its effects, and the best ways to protect vulnerable computers and restore infected ones to normal operation. We published and continually updated web pages with information for non-technical audiences, and provided guidance to ISPs and hosting companies about how to protect home user and small business customers. We also

dispatched field engineers to many customer sites to provide hands-on assistance; augmented our Technical Support staff with hundreds of software engineers when customer call volumes exceeded our normal capacity; and developed tools to assist customers in identifying and protecting vulnerable computers. Throughout this period, we worked closely with anti-virus companies to share the latest and most accurate information about Blaster and its variants. In addition, we alerted leading consumer organizations and placed full-page ads in major newspapers to give consumers information about protecting their computers.

- Early in our analysis of the worm's behavior, we determined that infected computers would flood the Windows Update web site with data beginning on August 16, in an apparent effort to disrupt its operation and prevent customers from obtaining security patches. Microsoft developed a solution that provided uninterrupted support for our customers.
- Beginning with the worm's appearance, and continuing even now, Microsoft worked closely with law enforcement authorities' efforts to identify the individuals or organizations who created and released Blaster and its subsequent variants. On August 29, the FBI arrested Jeffrey Lee Parson, whom we understand is alleged to have created and released a Blaster variant. As I will discuss later, effective law enforcement is a critical element in any successful effort to protect people and networks from cyber crime.
- In the wake of Blaster, Microsoft has embarked on a proactive effort to help consumers become better protected in the future. On August 21, we launched

the Protect Your PC campaign, urging that customers take three steps to improve their security: install and/or activate an Internet firewall, stay up to date on security patches, and install an anti-virus solution and keep it up to date. We launched this campaign with a nationwide advertising campaign directing customers to the www.microsoft.com/protect web site, which serves as the focal point for the campaign.

- We also undertook an in-depth review and post-mortem, to understand how the vulnerability occurred and how to reduce the likelihood of similar vulnerabilities occurring in the future. After discovery of the vulnerability, we took steps to improve our tools, and carried out a full scrub of the subsystem that contained the vulnerability. In addition, recognizing that software development is a human process that cannot be made perfect, we also have been taking and are planning to take additional steps to improve our customers' protection against future vulnerabilities. I will discuss some of these steps below.

Microsoft's Commitment to Trustworthy Computing

The efforts I have discussed to respond to the Blaster Worm attacks and the efforts I describe below to achieve further advances in software development practices and in patch management are integral aspects of Trustworthy Computing, which is our top priority and involves every aspect of the company. The focus of Trustworthy Computing is on four core pillars: security, privacy, reliability, and business integrity.

The security pillar is most relevant for today's hearing. Under this pillar, we are working to create software and services for our customers that are Secure by Design,

Secure by Default, and Secure in Deployment, and to communicate openly about security.

- "Secure by Design" means two things: writing more secure code and architecting more secure software and services.

- "Secure by Default" means that computer software is secure out of the box, whether it is in a home environment or an IT department.

- "Secure in Deployment" means making it easier for consumers, commercial and government users, and IT professionals to maintain the security of their systems.

- "Communications" means sharing what we learn both within and outside of Microsoft, providing clear channels for people to talk to us about security issues, and addressing those issues with governments, our industry counterparts, and the public.

The Trustworthy Computing goals are real and specific, and this effort is now ingrained in our culture and is part of the way we value our work.

Although we are working hard, much remains to be done. We accept our responsibility to create ever more secure software. Part of our commitment to Trustworthy Computing is in developing innovative, new technology that will make users less vulnerable to a cyber attack. One key piece of that work is the Next-Generation Secure Computing Base (NGSCB). This is an on-going research and development effort to help to create a safer computing environment for users by giving them access to four

core hardware-based features missing in today's PCs: strong process isolation, sealed storage, a secure path to and from the user, and strong assurances of software identity. These changes, which require new PC hardware and software, can provide greater protection against malicious software attacks.

Our Efforts to Streamline the Patch Process

To be clear, the best way to streamline the patch management process is to create software that is Secure by Design and Secure by Default, thus reducing the number of vulnerabilities in code and reducing the need to patch. That said, there is no such thing as completely secure complex software, regardless of development model or platform. Therefore, when security vulnerabilities are found, the processes to provide customers with the necessary fixes must be easy, fast, and transparent, especially as we move to an environment where an increasingly smaller percentage of computers are managed by IT professionals. We are attacking this issue under the "Secure in Deployment" pillar of the Trustworthy Computing initiative.

The steps we are taking include:

- Improving our testing of patches to ensure patch quality.
- Working to ensure that each patch is uninstallable, so a rollback is possible if deployment raises an unanticipated issue, such as adversely affecting a legacy application. We are reducing the number of installers used in order to simplify the administrator's burden and make patch installation more efficient.
- Ensuring that patches register their presence on the system – and producing improved scanning tools – so a user can quickly determine if his or her machine is patched appropriately.

- Making our security patch releases more predictable. Absent a public exploit, we regularly release patches on Wednesdays, thereby allowing our customers to prepare for them.
- Avoiding reboot of the computer where practicable, as our customers are more likely to apply a patch more quickly, if server availability will not be interrupted.
- Combining patches into service packs to avoid the need for multiple downloads and installations.
- Producing specific technology, such as Software Update Services and Systems Management Server, so enterprises can download patches, test them in their unique environment, and then easily deploy them.
- Including the AutoUpdate feature in recent Microsoft operating systems, which can automatically download updates and then either install them as scheduled or request permission from the user to do so.

In sum, our goal is to make patch application easier, so that every single customer can readily have the appropriate patches installed and their information protected.

The Importance of Effective Law Enforcement

However, as I mentioned above, technical and management solutions cannot prevent every cyber attack. Determined, innovative, sophisticated hackers and cyber criminals will always develop new means to break into systems and otherwise harm the online public, just as criminals in the physical world break into cars, stores, and homes and commit other crimes such as fraud. When criminals steal or attack online, public authorities need to be able to find and punish them. Despite the best and laudable efforts

of the U.S. and international law enforcement communities, and periodic successes, it is still very hard to identify and prosecute hackers, virus writers, and cyber criminals worldwide. As a result there is insufficient deterrent to this criminal activity.

There are specific steps we can and should take.

First, we need increased funding for law enforcement personnel, training, equipment, and capabilities to prevent and investigate cyber crime. Our government's hard-working officials – including those within the Departments of Justice, Homeland Security, and Defense – are often short-staffed, under-funded, under-trained, and lack state-of-the-art technology used by cyber criminals. Increased funding is needed to give the government an edge over those whom they investigate. Additional resources may also help the government coordinate with international, state, and local law enforcement in preventing and investigating cyber crime.

Lacking these additional resources, law enforcement is trapped in a perpetual and accelerating race against hackers and virus writers, as hacker tradecraft and tools are improving faster than are law enforcement's investigative techniques. Investigations are also made considerably more difficult by the increasing scope and diversity of the Internet – the "needle in a haystack" analogy far understates the problem. And the computer forensic challenges facing law enforcement are daunting – the amount of data that is stored electronically is growing exponentially, with law enforcement's technical capability to sort through a mass of electronic data to timely find critical evidence (including clues to the location and identity of an attacker) falling rapidly behind. We must solve these problems while simultaneously ensuring that law enforcement

capabilities and investigations are tailored to intrude on the privacy of law-abiding citizens as little as possible.

Second, because cyber security is inherently an international problem with international solutions, greater cross-jurisdictional cooperation among law enforcement is needed for investigating cyber-attacks. Cyber attackers and criminals easily cross borders, as demonstrated by the many attacks, including recent worms and viruses, which were international in scope. Enhanced law enforcement assistance, collaboration, and information sharing across local, state, and international borders, along with laws in every country criminalizing cyber attacks, are vital for law enforcement to prevent and investigate cyber attacks.

Conclusion

The Blaster Worm and its variants were serious criminal attacks against the owners and users of computer networks. These attacks merited and received equally serious attention from the government and from Microsoft, as well as from our customers and our partners in the computer infrastructure and software industries. In the end, a shared commitment to reducing cyber security risks and a coordinated response to cyber security threats of all kinds — one that is based on dialogue and cooperation between the public and private sectors — offer the greatest hope for promoting security and fostering the growth of a vibrant, trustworthy online economy.

Thank you.