

# Internet Service Providers: The Little Man's Firewall?

*Johannes Ullrich, Ph.D.*

*SANS Institute, jullrich@sans.org*

*The fast spread of network worms and other malware has forced Internet Service Providers (ISPs) into implementing packet filtering. In some cases, this is the only way to keep the network operating, but it has become common to block certain ports permanently even after the threat diminishes. We argue in favor of limited, long term port blocking. This paper does not intend to present a balanced argument. It intends to provide a starting point for a larger discussion of the issue.*

## **Introduction**

A large percentage of malicious traffic is focused on a small number of vulnerabilities and their associated ports[1]. Blocking some of these ports will isolate infected machines and slow the spread of malicious, autonomous code such as worms. However, the vulnerable services used by these worms do have legitimate uses. If secured properly, they can be used without the risk of infection. In this paper, we focus on ISPs that provide Internet access to consumers. This paper assumes that a consumer is a home user or a small business without dedicated IT staff. This paper does not apply to backbone infrastructure providers or co-location providers.

In part of this paper, we argue for blocking ports commonly used for Microsoft File sharing and related services; specifically, ports 135, 137, 139, and 445. These ports and, in particular, Microsoft File Sharing, draw a lot of attention from malware authors.

## **Arguments**

### **1.Port blocking does not restrict valid applications.**

The ports listed referenced previously (135, 137, 139, and 445) are used by Microsoft File Sharing and various other Microsoft-specific services. However, Microsoft does not recommend use of these services across a public network, and in fact, Microsoft advocates blocking traffic on these ports as a best practice. [2]

### **2.Blocking ports does not prevent innovation.**

A common argument against port blocking is that such a practice, if implemented widely, can reduce innovation. New applications cannot be developed if ports are blocked

---

<sup>1</sup><http://isc.sans.org/top10.html>

<sup>2</sup>[http://www.microsoft.com/serviceproviders/columns/isp\\_security.asp](http://www.microsoft.com/serviceproviders/columns/isp_security.asp)

that could otherwise be used by these applications. However, ports 135, 137, 139, and 445 are already reserved for widely used applications[3]. As a result, new applications should not use these ports even if they are open for use.

### **1.ISPs are not responsible for end user equipment.**

Although ISPs cannot fix bugs or patch customer systems, they are able to limit the impact of unpatched, buggy software. Blocking these ports will do more than protect end user equipment. Exploited machines are frequently used to launch distributed denial of service (DDOS) attacks or to host high traffic “warez” sites[4]. End user systems used for DDOS attacks, as well as “warez” sites create significant traffic. This traffic may be sufficient to overwhelm ISP-owned infrastructure and it will impact other customers of this ISP.

### **3.Exploited machines impact other customers.**

If a customer chooses not to patch a system, and as a result is infected with a worm or hacked, it is up to this customer to clean up. However, other customers may be impacted due to the high use of bandwidth caused by the infected customer[5]. In addition, many recent worms prefer to scan the local network[6]. As a result, customers of ISPs with many infected systems will see more malicious traffic.

### **4.Blocking ports allows ISPs to focus on other problems.**

Port filters are not perfect. In particular, the limited filters discussed here leave plenty of room for other vulnerabilities. However, these ports account for a large percentage of malicious activity. While a simple fix using port filters will not work for some problems, filtering ports 135, 137, 139, and 445 will free resources to deal with the more difficult issues, such as attacks against web servers or mail servers that cannot be blocked by a simple firewall. An example is implementing and monitoring network intrusion detection systems (NIDS). NIDS can be used to identify customers infected with a wide range of malware. ISPs will be able to notify customers identified by the NIDS and assist customers in cleaning up infected systems. This is only possible if the number of infected customers is small. Blocking port 135, 137, 139 and 445 will reduce the number of infected customers and may be sufficient to allow notification of the remaining customers.

---

3<http://www.iana.org/assignments/port-numbers>

4<http://www.honeynet.org/papers/enemy3/>

5<http://www.auscert.org.au/render.html?it=2448&cid=1926>

6<http://isc.sans.org/diary.html?date=2003-08-11>

## **5. Blocking ports is the "seatbelt" of network security.**

Blocked ports should not give end users a false sense of security. Like a seatbelt in a car, blocking ports should not encourage unsafe computing just as a seatbelt should not encourage poor driving; instead, blocking ports should be viewed as a preventative measure. They help prevent damage if something does go wrong. Good security implies "defense in depth." Blocking ports 135, 137, 139 and 445 at the ISP is a sensible additional layer of defense.

## **6. A limited filter is better than no filter.**

Depending on existing infrastructure, the ISP might be limited in the implementation of filters. Frequently, filters can only be applied at given points in the network. However, malicious traffic that can be avoided will reduce the number of infected machines and, as a result, provide an incrementally cleaner network. Improvements in filtering malicious traffic will remove some of the malicious traffic from the network resulting in a cleaner network.

## ***Conclusion***

Filtering port 135, 137, 139, and 445 will reduce malicious traffic. As a result, less customer machines will be compromised. ISPs can provide this added value to their customers and take advantage of the result. The result is evidenced in fewer support calls due to congested connection and fewer complaints about malicious traffic. It is challenging to implement these filters uniformly across ISPs. This paper should provide the necessary arguments to advocate such a change.