

REN-ISAC Response to Blaster and Welchia/Nachi Threats

August 27, 2003

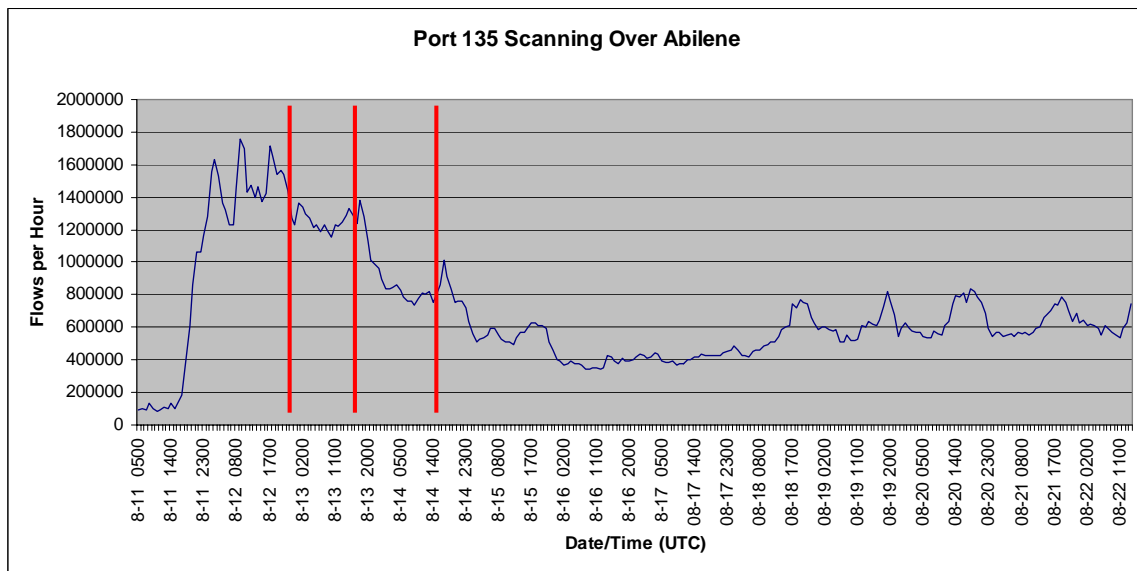
Acting on the W32/Blaster threat advisory released on Monday August 11, the REN-ISAC and Indiana University Advanced Network Management Lab (ANML) began ongoing analysis of aggregate Abilene NetFlow data, to profile overall port 135 scanning activity, and to identify the top network sources of port 135 scans on Abilene.

The next day, a message from REN-ISAC was sent to the EDUCAUSE Security, and Abilene Operators mailing lists, stating that the W32/Blaster threat was active on Abilene, and that signature port 135 scanning was running very high, at seven percent of all network packets. We informed the community that the REN-ISAC would be notifying, via private communication, sites that were sourcing a large amount of worm traffic. Pointers were provided to resources describing mitigation techniques, such as filtering at network borders, for both inbound and outbound traffic.

Tuesday afternoon, private notifications were sent to the managers of the top twelve network sources of port 135 scanning on Abilene. The communication stated that: the institution or network had been identified among the top twenty sources; described REN-ISAC and ANML monitoring; provided pointers to resources describing mitigation techniques; and provided a graph illustrating growth of Blaster activity on Abilene. On Wednesday and Thursday of that week, similar notifications were sent to the then-top sources. In all, forty-four top-twenty notifications were sent.

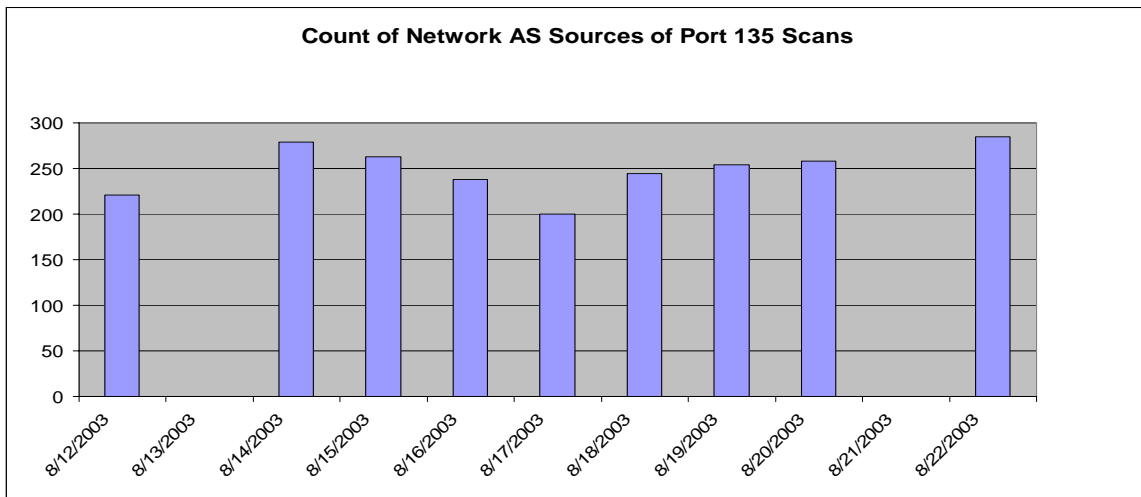
Throughout the week, communications were sent to the EDUCAUSE Security, Abilene Operators, and Internet2 Security Working Group mailing lists, briefing on the status of REN-ISAC activities and providing graphs illustrating the progress of the worm on Abilene. Positive responses to the top-twenty notification letters were received from a half-dozen sites, and favorable overall response from the community was received. No negative responses to the communications were received.

The following graph illustrates port 135 scanning activity on Abilene over the period August 11 0500 UTC to August 22 1100 UTC. The red bars indicate the times at which top-twenty communications were sent.

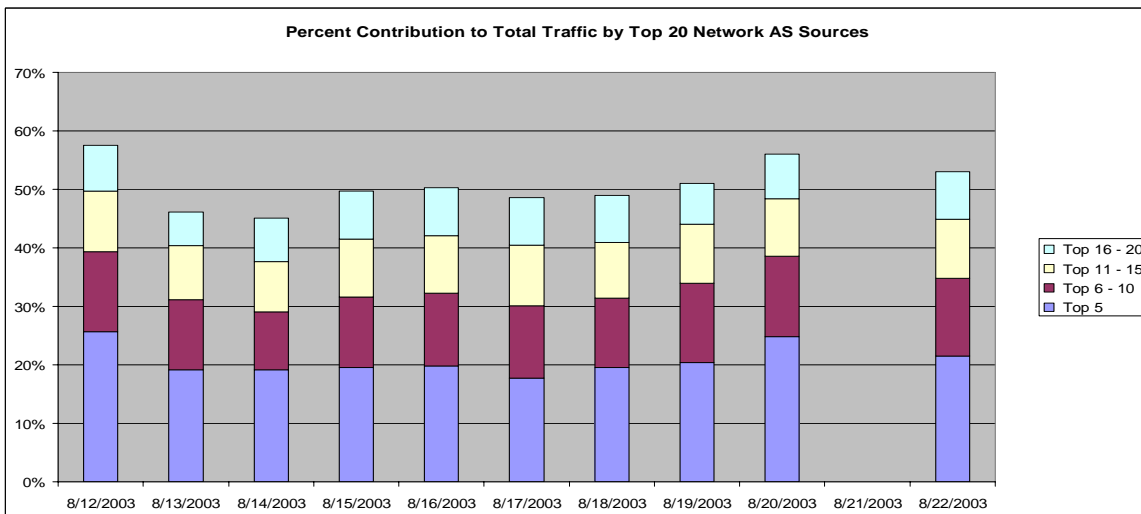


Thursday August 14, acting on revised threat information, that W32/Blaster was programmed to launch a Saturday, August 16 DDoS attack on windowsupdate.com, personnel from the REN-ISAC, the IU ANML and Abilene management conferred with lead technical representatives of Microsoft Corporation regarding the threat and potential ways to reduce the impact on university networks and Microsoft corporate networks. Microsoft had developed a sound and effective approach to mitigate the attack. We determined that no actions would be required on the part of universities. A communication from the REN-ISAC to its constituency was sent, advising that Microsoft had developed sound plans, and that protective actions would not be required.

The following graph represents counts of the number of network sources of port 135 scanning on Abilene over the period August 12-22. Because of limited data, it's difficult to assign a cause to the mid-period dip. A network is counted regardless of the number of sourced scans. Because of that, the dip is not the result of a weekend lull while some desktop computers were turned off. A possible explanation is that network managers began to control Blaster, only to be hit by the more virulent Welchia/Nachi infection starting Monday August 18.

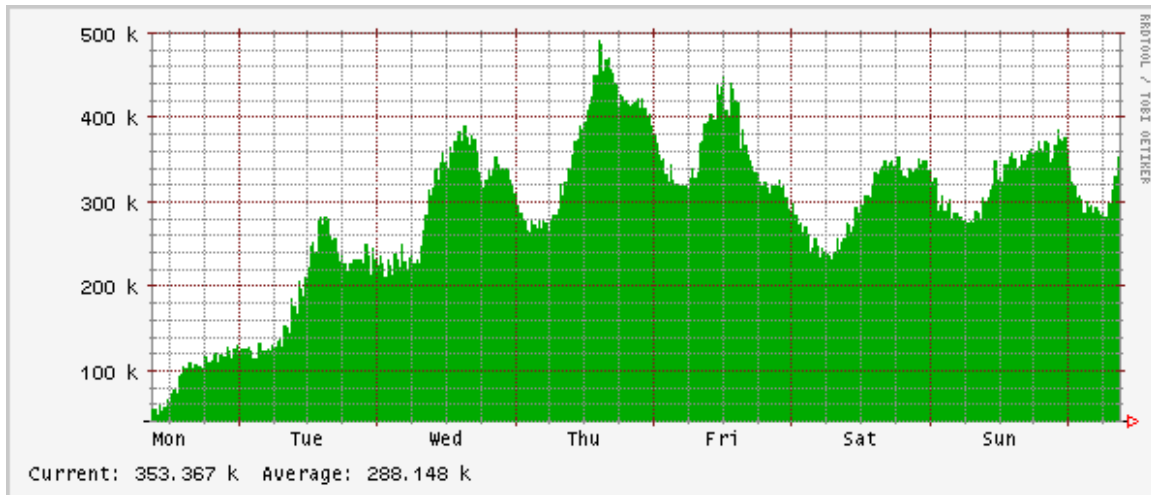


Overall, the network sources of port 135 scans that were among the top tier contributed significantly to the aggregate activity. The following graph presents the percent contribution to total scanning activity, by the top five networks, and by the second through fourth tiers of groups of five.



Acting on the Welchia/Nachi threat, on Tuesday August 19, the REN-ISAC sent an urgent communication to the EDUCAUSE Security, Abilene Operators, and Internet2 Security Working Group mailing lists stating that: Nachi signature ICMP traffic across Abilene was very high; reports of serious campus network degradation due to the Nachi ICMP traffic had been received; and that some universities reported taking temporary measures to block internal, outbound, and inbound ICMP of the signature 92-byte packet size.

Communications sent to the mailing lists throughout the week described the growth of the infections, and pointed to resources for mitigation techniques. The following graph illustrates the dramatic growth of ICMP traffic on Abilene during the course of the growth of Welchia/Nachi.



The REN-ISAC continues to monitor Blaster and Welchia/Nachi activity, report to the R&E community, and notify top sources.