CNS /Update Newsletter Feature

Sasser Slows: Blaster Saved the Day?

CNS Document ID: u040607a
Last Updated: 5/27/2004

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

Sasser Slows: Blaster Saved the Day? ...............................................................3
Sasser Slows: Blaster Saved the Day?

The big news in security during the first week of May was the Sasser worm. Sasser is a worm that attempts to exploit the vulnerability described in Microsoft Security Bulletin MS04-011. It spreads by scanning randomly selected IP addresses for vulnerable systems. Unlike most worms, Sasser doesn't require any human intervention-such as opening an e-mail attachment-but scans for vulnerable systems and surreptitiously plants its payload.

Millions of computers around the world were hit. The attacks took their toll in the US and overseas. In the US, Delta Airlines, American Express, Associated Press, two major universities, and a leading hospital were among Sasser's victims. The amount of damage it caused is hard to estimate because it didn't cause any direct damage other than the fact that it made computers crash and stalled networks. The major damage has been in slowed productivity.

Enterprise operations may partially have Blaster to thank for the relative corporate immunity from Sasser. IT security management practices were tightened considerably after the round of Blaster infections. Microsoft has reported fewer than 2 million downloads of its Sasser fix-it tool, where it reported more than 10 million downloads of its Blaster removal tool—a remarkable difference even when taking into account that Sasser only "infects" later versions of the Windows OS.

But while the Sasser problem appears to have slowed down, it has not yet disappeared completely. Five versions of Sasser are known. Police in Berlin have said an 18-year-old German teenager was responsible for all of them in addition to the “Netsky” virus.

The German youth apparently released a new variant of the worm, "Sasser e," shortly before he was arrested last week, investigators said in Berlin. He has now been identified as Sven Jaschan, a technical high school student of Waffensen, Lower Saxony. The teenager was arrested on May 7 after informants seeking a reward tipped off Microsoft. He was released pending charges after questioning May 7 when he admitted to creating Sasser, police said.

UF disconnects users from wireless, walkups, and classrooms if it detects a virus such as Sasser. If you experience problems in these areas, it may be because your computers is infected with Sasser or some other virus worm. For assistance, see http://net-services.ufl.edu/security/public/sasser-alert.shtml or call the UF Computing Help Desk at (352) 392-HELP.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100