



Attack Trends

Counterpane Internet Security Inc. monitors more than 450 networks in 35 countries, in every time zone. In 2004 we saw 523 billion network events, and our analysts investigated 648,000 security “tickets.” What follows is an overview of what’s happening on the Internet right now, and what we expect to happen in the coming months.

In 2004, 41 percent of the attacks we saw were unauthorized activity of some kind, 21 percent were scanning, 26 percent were unauthorized access, 9 percent were DoS (denial of service), and 3 percent were misuse of applications.

Over the past few months, the two attack vectors that we saw in volume were against the Windows DCOM (Distributed Component Object Model) interface of the RPC (remote procedure call) service and against the Windows LSASS (Local Security Authority Subsystem Service). These seem to be the current favorites for virus and worm writers, and we expect this trend to continue.

The virus trend doesn’t look good. In the last six months of 2004, we saw a plethora of attacks based on browser vulnerabilities (such as GDI-JPEG image vulnerability and IFRAME) and an increase in sophisticated worm and virus attacks. More than 1,000 new worms and viruses were discovered in the last six months alone.

In 2005, we expect to see ever-more complex worms and viruses in the wild, incorporating complex behavior:

polymorphic worms, metamorphic worms, and worms that make use of entry-point obscurity. For example, SpyBot.KEG is a sophisticated vulnerability assessment worm that reports discovered vulnerabilities back to the author via IRC channels.

We expect to see more blended threats: exploit code that combines malicious code with vulnerabilities in

Hacking has moved from a hobbyist pursuit with a goal of notoriety to a criminal pursuit with a goal of money.

order to launch an attack. We expect Microsoft’s IIS (Internet Information Services) Web server to continue to be an attractive target. As more and more companies migrate to Windows 2003 and IIS 6, however, we expect attacks against IIS to decrease.

We also expect to see peer-to-peer networking as a vector to launch viruses.

Targeted worms are another trend we’re starting to see. Recently there have been worms that use third-party

2004 and 2005

BRUCE SCHNEIER, COUNTERPANE

information-gathering techniques, such as Google, for advanced reconnaissance. This leads to a more intelligent propagation methodology; instead of propagating scattershot, these worms are focusing on specific targets. By identifying targets through third-party information gathering, the worms reduce the noise they would normally make when randomly selecting targets, thus increasing the window of opportunity between release and first detection.

Another 2004 trend that we expect to continue in 2005 is crime. Hacking has moved from a hobbyist pursuit with a goal of notoriety to a criminal pursuit with a goal of money. Hackers can sell unknown vulnerabilities—“zero-day exploits”—on the black market to criminals who use them to break into computers. Hackers with networks of hacked machines can make money by selling them to spammers or phishers. They can use them to attack networks. We have started seeing criminal extortion over the Internet: hackers with networks of hacked machines threatening to launch DoS attacks against companies. Most of these attacks are against fringe industries—online gambling, online computer gaming, online pornography—and against offshore networks. The more these extortions are successful, the more emboldened the criminals will become.

We expect to see more attacks against financial institu-

tions, as criminals look for new ways to commit fraud. We also expect to see more insider attacks with a criminal profit motive. Already most of the targeted attacks—as opposed to attacks of opportunity—originate from inside the attacked organization’s network.

We also expect to see more politically motivated hacking, whether against countries, companies in “political” industries (petrochemicals, pharmaceuticals, etc.), or political organizations. Although we don’t expect to see terrorism occur over the Internet, we do expect to see more nuisance attacks by hackers who have political motivations.

The Internet is still a dangerous place, but we don’t foresee people or companies abandoning it. The economic and social reasons for using the Internet are still far too compelling. ☺

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

BRUCE SCHNEIER is CTO of Counterpane Internet Security. His most recent book is *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer, 2003). He publishes an e-mail newsletter called *Crypto-Gram*, available via subscription at www.schneier.com.

© 2005 ACM 1542-7730/05/0600 \$5.00