Cybertrust "How the Heck Did This Happen" Presentation
Case A – 1
Full story available at: http://www.sophos.com/pressoffice/news/articles/2006/02/nwhospital.html
February 2006

Man accused of hospital zombie attack that brought down computers

Christopher Maxwell, from Vacaville, California, has been indicted on charges that he launched an attack in January 2005 which struck hard at Northwest Hospital and Medical Center in north Seattle. The attack is said to have shut down computers in the facility's intensive care unit and prevented doctors' pagers from working properly.

When it noticed that 150 of its 1,100 computers were infected, officials at Northwest Hospital contacted the FBI, and put backup measures in place. Nurses are said to have run charts down hallways rather than transferring them electronically.

According to the US Attorney's office in Seattle, 20-year-old Christopher Maxwell first compromised computer networks at California State University, the University of Michigan and the University of California-Los Angeles by exploiting loopholes in their security. Compromised computers were converted into a network of zombie computers (also known as a botnet) which could be remotely controlled for the purposes of planting commission-earning adware.

In total, Maxwell and two un-named youths are said to have created a zombie network of over 13,000 compromised computers. Maxwell is alleged to have fraudulently earned $100,000 from unnamed companies whose adware he installed.

"Although no patients were harmed, any attack against a hospital network is a serious offense," said Graham Cluley, senior technology consultant for Sophos. "All organizations need to put the appropriate resources in place to ensure their computers are not part of a zombie network. Every PC should be properly defended by up-to-date anti-virus software, firewalls, and the latest security patches."

Maxwell has been summoned to appear at the US District Court in Seattle on 23 February. If convicted, the 20-year-old faces up to 10 years in prison and a $250,000 fine. He could also be ordered to pay restitution to Northwest Hospital that estimates its repair bill amounted to $149,000. The two unidentified juvenile co-conspirators are also being prosecuted.

Zombie computers - are your PCs under someone else's control?

Zombie computers can be used by criminal hackers to launch distributed denial-of-service attacks, spread spam messages or to steal confidential information. SophosLabs estimates that more than 60 percent of all spam today originates from zombie computers. In May, the Sober-Q Trojan horse and Sober-N worm worked in tandem to infect and hijack computers around the world, programming them to spew out German nationalistic spam during an election.

As spammers become more aggressive, collaborating with virus writers to create armies of zombie computers, legitimate organizations with hijacked computers are being identified as a source of spam. This not only harms the organization's reputation, but can also cause the company's email to be blocked by others.

Cybertrust "How the Heck Did This Happen" Presentation
Case A – 2
Full story available at:
http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=19301&mode=thread&order=0&thold=0
March 2005

Christopher Maxwell, 20, indicted on computer attack charges

A 20 year-old man was indicted today on charges that he launched an attack that hit tens of thousands of computers. Prosecutors say the attack crippled a Seattle hospital's network, shutting down its intensive care unit and preventing doctors' pagers from working. Christopher Maxwell of Vacaville was ordered to appear in U-S District Court in Seattle later this month, but isn't in custody. Two juvenile co-conspirators are being prosecuted out of state. At least 13,000 computers were infected by attacks Maxwell and his co-conspirators launched beginning around July 2004. Northwest Hospital and Medical Center was attacked in January 2005. Though backup systems prevented patient care from being compromised, prosecutors said lives were endangered and computer repairs cost about $150,000.

Cybertrust "How the Heck Did This Happen" Presentation
Case A – 3
Full story available at: http://www.officer.com/article/article.jsp?id=30453&siteSection=1
March 2005

Safety is another reason courts are getting tough on cybercrime, as we realize how dependent society is on computer networks. On May 4, 20-year-old Christopher Maxwell pleaded guilty in U.S. District Court in Seattle to computer fraud for operating a botnet that disrupted critical care systems used by Seattle's Northwest Hospital in January 2005. Maxwell's crime was particularly odious because the attack disrupted operating room doors, physicians' pagers, and computers in the intensive care unit. He faces up to 10 years in prison and a $250,000 fine.

There's a get-tough response from Congress, too. Last week, six U.S. representatives, including House Judiciary Committee Chairman James Sensenbrenner, R-Wis., proposed the Cyber-Security Enhancement and Consumer Data Protection Act, aimed at updating criminal statutes to keep pace with cybercrooks' methodologies. The bill has three goals,

says Rep. Howard Coble, R-N.C., who chairs the Subcommittee on Crime, Terrorism, and Homeland Security: a stronger deterrent, including heading off the development of new criminal techniques; better protection of personally identifiable data; and adequate resources for the Justice Department and other agencies to investigate and prosecute lawbreakers.

The bill would prohibit the use of botnets-zombie computers that, through use of code sneaked onto them, can be controlled for phishing, spam, and denial-of-service attacks. It would raise the maximum penalty for fraud and other computer crimes from 10 years to 30. It also calls for the Secret Service, Justice Department, and FBI to each get $10 million a year in funding through 2011 to fight computer crimes. And it would require companies, in the case of a major security breach involving data on 10,000 people or more, to notify the Secret Service or FBI within two weeks and give the feds power to decide if notification required under state laws would hurt an investigation.

Cybersecurity laws typically have been created and enforced first at the federal level; state and local police often don't have enough computer forensic resources to investigate cybercrimes, Laura Parsky, the Justice Department's deputy assistant attorney general, told the House subcommittee last week. "Although law enforcement has made inroads into addressing [the cybercrime] problem, it appears to be getting worse," Parsky said.

Last year, 95% of companies experienced more than 10 Web site attacks, involving viruses, unauthorized access, or theft of proprietary information, according to a survey of 700 computer security practitioners by the FBI and the Computer Security Institute. In 2004, just 5% experienced that level of attacks.

Cybertrust "How the Heck Did This Happen" Presentation
Case A – 4
Full story available at: http://seattletimes.nwsource.com/html/localnews/2002798414_botnet11m.html
March 2005

3 accused of inducing ill effects on computers at local hospital

One day last year, things started going haywire at Northwest Hospital and Medical Center. Key cards would no longer open the operating-room doors; computers in the intensive-care unit shut down; doctors' pagers wouldn't work. This might have been just another computer-virus attack, a common and malicious scheme that sometimes is done for little more than bragging rights. But federal officials say it was something far more insidious.

It turns out the Seattle hospital's computers — along with up to 50,000 others across the country — had been turned into an army of robots controlled by 20-year-old Christopher Maxwell of Vacaville, Calif., according to a federal indictment issued Thursday. And

Maxwell, along with two juveniles, earned about $100,000 in the process, court documents state. The trio had created a "botnet," a phenomenon that is on the cutting edge of computer crime, federal officials say.

"Their goal was as old as fraud itself," Assistant U.S. Attorney Kathryn Warma said Friday during a news conference. "To line their own pockets." Maxwell's lawyer declined to comment on the case. Maxwell is not in custody and will make his first appearance in U.S. District Court in Seattle on Feb. 23. The two juveniles, who don't live in Washington, are being charged in other undisclosed jurisdictions. They were not identified.

How the process works

"Botnet" may sound technical, but it describes a process that is relatively simple and is essentially one step beyond a computer virus. A virus exploits software vulnerabilities to infect one computer, which then can transmit the infection to others. To create a botnet, hackers exploit the same sorts of vulnerabilities, then tell the infected computers to wait for further commands — in essence, creating computer sleeper cells. The so-called "bot-herder" commands thousands of these computers at once by taking control of a server, often secretly.

Like other hackers, Maxwell figured out a way to make money out of the deal, court papers state. He entered into affiliate relationships with several mainstream adware companies, which pay a commission each time their adware is installed. Maxwell simply created a program instructing his infected computers, or "bots," to download the adware. The bots then "phoned home" to the adware company, which credits the hacker's account, unaware that he hasn't gotten the computer owner's permission. Since 2004, Maxwell earned more on botnets than he did at his Wal-Mart job, according to court papers.

Difficult to solve

"We're seeing the migration of traditional fraud to the cyber area," said Frank M. Harrill, an FBI expert in computer crime. It's just as difficult to solve. By the time the computer owner figures out what's going on, the bot-herder has covered his tracks. In fact, some companies are reluctant to even report the attack to authorities because it can prove embarrassing to their business, government officials said.

But the Northwest Hospital case played out differently in January 2005. Hospital officials called the FBI immediately, and an agent went to the scene while the attack was in progress. Meanwhile, the hospital used some old-fashioned backup systems. When electronic file transfers didn't work, nurses ran the files up and down hallways. When key cards wouldn't work, they stood guard and inspected ID badges themselves. No patients were harmed, but First Assistant U.S. Attorney Mark Bartlett said this kind of attack could easily endanger lives. In all, about 150 of the hospital's 1,100 computers were infected over the course of three days.

A "twisted and difficult" trail eventually led the FBI to Maxwell, Warma said. Investigators found he had hacked into servers at the University of Michigan, California

State University, Northridge, and the University of California, Los Angeles, to carry out his plan, court papers state. Northwest Hospital was not specifically targeted in the attack, federal officials said. "They're robots; they don't target an individual," Harrill said.

"Blunt-force tool"

Instead, a botnet will repeatedly send out messages looking for computers it can attack. The FBI compared it to yelling out a friend's name in a crowded room — over and over and over again. The more it happens, the more intrusive it is. The repeated messages tie up computer networks and sometimes shut them down, as they did at Northwest Hospital. "It's a blunt-force tool," Harrill explained. Sometimes tying up the network is the sole purpose, as in "denial of service" attacks. Other times, the purpose is extortion. "No longer does someone need to threaten someone physically," Harrill said. "They can threaten to take down their Web site." Maxwell has been charged with one count of conspiracy to intentionally damage a protected computer and with one count of intentional computer damage that interferes with medical treatment. The crimes carry a sentence of up to 10 years in prison, a $250,000 fine and restitution.

Cybertrust "How the Heck Did This Happen" Presentation
Case A – 5
Full story available at: http://www.p2pnet.net/story/7900
March 2005

Hackers' hospital bot army

Some 50,000 hospital computers across the US were turned into a Zombie bot army controlled by 20-year-old California hacker Christopher Maxwell, says a federal indictment. Maxwell, from Vacaville, and two unidentified juveniles, pulled in some $100,000 in the process, court documents state, says the Seattle Times.

Maxwell, who isn't in custody, will make his first appearance in US District Court in Seattle on February 23 while the juveniles are being charged in other undisclosed jurisdictions, says the story. He had affiliate relationships with several mainstream adware companies and then, "simply created a program instructing his infected computers, or 'bots,' to download the adware."

"The bots then 'phoned home' to the adware company, which credits the hacker's account, unaware that he hasn't gotten the computer owner's permission. "Since 2004, Maxwell earned more on botnets than he did at his Wal-Mart job, according to court papers."

He's been charged with one count of conspiracy to intentionally damage a protected computer and with one count of intentional computer damage that interferes with medical treatment, says the story, adding: "The crimes carry a sentence of up to 10 years in prison, a $250,000 fine and restitution."