Report finds online attacks shift toward profit

August 2 2005

IBM reported that virus-laden emails and criminal driven security attacks increased by 50 percent in the first half of 2005 - underscored by a significant rise in 'customized' attacks on the government, financial services, manufacturing and healthcare industries.

This substantial increase, along with a decrease in less profitable threats, such as spam and simple computer viruses, indicates a growth in targeted attacks against specific organizations and industries -- apparently created with the purpose of stealing critical data, identities or extorting money.

The Global Business Security Index, a worldwide barometer of security trends collected and analyzed by IBM's Global Security Intelligence team and its partners, indicates that such customized, 'for profit' attacks have been predominantly directed at government agencies, financial services companies, healthcare organizations and large multinational corporations, particularly within the aerospace, petroleum, and manufacturing industries.

According to the report, there were more than 237 million overall security attacks in the first half of the year. The government was the most targeted industry, with more than 54 million attacks, while manufacturing ranked second with 36 million attacks, financial services was third with approximately 34 million, and healthcare was hit with more than 17 million attacks - accounting for more than 137 million of all attacks this year.

IBM has seen a resurgence of targeted phishing attacks for money laundering and identity fraud purposes, believed to be largely driven by criminal gangs that have become more astute in the creation and delivery of such attacks. According to its latest Global Business Security Index, in the first half of the year, there were more than 35 million phishing attacks launched to steal critical data and personal information for financial gains.

Spawns of phishing threats such as 'spear phishing' - highly targeted and coordinated attacks at a specific organization or individual designed to extract critical data - increased more than ten-fold since January of this year alone. Unlike in previous years, when viruses were mainly created and launched to slow down and cripple IT systems, these types of 'customized' attacks have shown their potential to defraud businesses, steal identities and intellectual property and extort money, while damaging the brand and eroding customer trust.

The ratio of spam to legitimate email continuously decreased over the course of the last six months, from 83 percent in January to 67 percent in June 2005, while virus-laden email increased fifty percent over the same period. At first glance what appears to be good news - the leveling off of massive outbreaks that cripple IT environments on a regional or global basis in the past six months - seemingly indicates that hijacking computers to send spam is no longer the network disruption of choice.

Hackers have turned toward more criminal and lucrative areas of directing attacks to specific individuals or organizations, often financially, competitively, politically or socially motivated. IBM's Global Business Security Index shows that in December of 2004, one in every 52 emails was infected by some sort of malicious security threat; by January it was one in every 35 emails, and by June, that ratio increased to one in every 28 emails - signifying a fifty percent increase from last year - a disturbing trend for businesses and consumers alike.

"IBM advises its clients to rapidly adopt a holistic, enterprise-wide approach to security and risk management," said John Lutz, general manager, Financial Services Sector, IBM. "To protect their critical data, infrastructure, brands, and money, IBM advises businesses to rethink how they protect their operations, business processes and governance structures. Companies can employ the latest protective technology, while ensuring that their own customers get highest level of protection available."

Additional key findings from IBM's First Half 2005 Global Business Security Index:

Virus-laden emails increase: In January of 2004, 1 in every 129 emails was virus laden; by December 2004, it increased to one in every 51 emails. In January of 2005, the number was one in every 35; by June, the number had grown to one in every 28 emails

- Phishing gains: 35.7 million emails contained some form of phishing attack; spear phishing directed attacks rose from one of every 56 emails in January, to more than 600,000 in June
- Spam levels off: Spam consistently decreased from 83 percent of all emails in January to 67 percent of all emails in June 2005
- Attacks by industry: the government was the most targeted industry with more than 54 million targeted attacks, manufacturing ranked second with almost 36 million attacks recorded, and financial services was third with a little over 34 million**
- Attacks by location: Over the past six months, the United States was the source of the most attacks with 12 million, followed by

New Zealand with 1.2 million, and China with approximately one million; Ireland was last with more than 30,000 attacks

- Attacks by day: Increased critical security events are seen on Fridays and Sundays

- Attacks by category: Reconnaissance attacks - probes to discover what devices, software, or vulnerabilities may exist - totaled more than 108 million, followed by service attacks of more than 61 million, web attacks with 29 million, denial of service attacks with 26 million; security administration was last with more than 230,000 attacks
  Top 10 malware (malicious software) detected, by family, included: W32.Mytob; W32.Agobot; W32.Opaserv; W32.Sober; Ranky and Sdbot Dropper; W32.Backdoor; W32.Ranky; W32.Mydoom; W32.Sdbot and W32.Maslan

  New threats emerged:
  In March 2005, the emergence of a potential new threat affecting the Internet - pervasive Domain Name Service (DNS) cache poisoning was discovered. DNS cache poisoning is the act of corrupting a DNS server's ability to map machine host names to its proper IP address and would hijack visitors to an advertisement or inappropriate web site instead. While these types of threats have been seen for a few years, the new version uses two new technologies and any DNS server that is not configured properly may be susceptible to this type of attack
  In May 2005, a malware business was uncovered operating from iframeDOLLARS.biz. This Web site attempted to recruit partner Web sites to host a variety of malicious code to exploit Internet Explorer browsers, which paved the way for numerous trojans, backdoors and spyware installed on a computer .

The IBM Global Business Security Index Report is a monthly report that assesses, measures and analyzes potential network security threats based on the data and information collected by IBM's 3,000 worldwide information security professionals and thousands of monitored devices.

For more information, please visit: www-1.ibm.com/services/us/inde … fering/bcrs/a1008776 .