

'North Korean' Attacks Show Lack of Basic Internet Protections

John Pescatore

A highly publicized series of "cyberattacks" really just represents business as usual on the Internet. Businesses and government agencies that depend of the Internet should already have protections against such attacks.

NEWS ANALYSIS

Event

On 8 July 2009, media outlets worldwide reported that a series of distributed denial-of-service (DDoS) attacks had been launched against information systems and networks in the United States and South Korea beginning 4 July. The attacks, which unnamed government and intelligence sources in South Korea blame on the North Korean government, reportedly used malicious code to disable the public Web sites of a number of government agencies in the U.S. (including the Secret Service, Treasury Department and Federal Trade Commission) and South Korea (including the Defense Ministry). Further reports on 9 July indicated that attacks against South Korean targets were still continuing.

Analysis

The targets of these attacks, and the differences in their ability to protect themselves, are actually much more interesting than the attacks themselves. The malicious code used appears not to be very sophisticated, and the scope of the attack — with approximately 50,000 PCs apparently compromised — is not very large, compared with many other DDoS attacks in recent years. The media's attention has been captured by the high visibility of the targets and the claims of association with North Korea at a time when relations with that country are even more tense than usual.

Attacks of this type are essentially the Internet equivalent of bad weather: unpleasant but predictable, and not difficult to prepare for and protect against. At the height of the dot-com era, in 2000, similar types of DDoS attacks struck and impacted Yahoo and other high-visibility sites. Those sites quickly learned to protect themselves, but DDoS attacks have continued to hit many businesses during the past five years, partly because they have failed to recognize that preventing impact is simply part of the cost of doing business on the Internet.

Businesses and government agencies that have deployed due-diligence levels of protection should have routinely detected these latest attacks and quickly mitigated their impact. DDoS protection is widely available in the form of service offerings from telecommunications carriers and service providers and — less effectively — customer premises equipment that can be owned and operated locally. But any business or government agency that depends on its Internet presence and is operating without DDoS protection is placing its operations at unacceptable risk.

RECOMMENDATIONS

Business and government agencies should require DDoS protection for all Internet connections that require any level of reliable connectivity. Enterprises that believe they are unlikely to be targets of DDoS attacks should consider "on demand" DDoS protection offerings or have workaround plans for alternative connectivity in place to deal with inevitable DDoS attacks on their unprotected systems.

RECOMMENDED READING

- "Toward a National Cybersecurity Strategy" — The U.S. government should focus on developing a national cybersecurity strategy that addresses the real issues with a chief information security office. **By John Pescatore**

- "Obama Helicopter Plans Traced to Iran Highlight P2P Risks" — The reported transfer of information about the U.S. president's helicopter to a node in Iran clearly shows the security risks of peer-to-peer file sharing. **By Avivah Litan and Peter Firstbrook**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509