



WatchGuard Announces Leading Threats to Voice over IP

April 15, 2009 – WatchGuard Technologies

Highlights / News Facts:

- **Strong Growth of VoIP Makes it a Target** – Recently published reports predict that nearly 75 percent of corporate phone lines will be using Voice over IP (VoIP) in the next two years; expectations are that half of small-to-medium sized businesses and two-thirds of all enterprise organisations will be using VoIP. By this year's end, the global total number of VoIP subscribers (residential and commercial) is expected to reach nearly 100 million users. Because of the ubiquity of VoIP, it is quickly emerging as a new and substantive threat to businesses worldwide. The following are the leading threats to business networks that use VoIP:
- **Denial of Service (DoS)** – Similar to DoS attacks on data networks, VoIP DoS attacks leverage the same tactic of running multiple packet streams, such as call requests and registrations, to the point where VoIP services fail. These types of attack often target SIP (Session Initiation Protocol) extensions that ultimately exhaust VoIP server resources, which cause busy signals or disconnects.
- **Spam over Internet Telephony (SPIT)** – Much like the majority of e-mail spam, SPIT can be generated in a similar way with botnets that target millions of VoIP users from compromised systems. Like junk mail, SPIT messages can slow system performance, clog voicemail boxes and inhibit user productivity.
- **Voice Service Theft** – VoIP service theft can happen when an unauthorized user gains access to a VoIP network, usually by way of a valid user name and password, or gains physical access to a VoIP device and initiates outbound calls. Often, these are international phone calls to take advantage of VoIP's toll by-pass capabilities.
- **Registration Hijacking** – A SIP registration hijack works by a hacker disabling a valid user's SIP registration and replacing it with the hacker's IP address instead. This allows the hacker to then intercept incoming calls and reroute, replay or terminate calls as they wish.

- **Eavesdropping** – Like data packets, voice packets are subject to man-in-the-middle attacks where a hacker spoofs the MAC address of two parties and forces VoIP packets to flow through the hacker’s system. By doing so, the hacker can then reassemble voice packets and literally listen in to real-time conversations. From this type of attack, hackers can also gain access to all sorts of sensitive data and information, such as user names, passwords, and VoIP system information.
- **Directory Harvesting** – VoIP directory harvesting attacks occur when attackers attempt to find valid VoIP addresses by conducting “brute force” attacks on a network. When a hacker sends thousands of VoIP addresses to a particular VoIP domain, most of the VoIP addresses will bounce back as invalid, but from those that are not returned, the hacker can identify valid VoIP addresses. By harvesting the VoIP user directory, the hacker now gains a new list of VoIP subscribers that can be new targets to other VoIP threats, such as SPIT or vishing attacks.
- **Vishing (Voice Phishing)** – Vishing mimics traditional forms of phishing – attempts to get users to divulge personal and sensitive information, such as user names, account numbers and passwords. The trick works by spamming or “spitting” users and luring them to call their bank or service provider to verify account information. Once valid user information is given, criminals are free to sell this data to others, or in many cases, directly siphon funds from credit cards or bank accounts.
- Because of these quickly emerging threats, WatchGuard recommends that businesses using VoIP systems review their perimeter and VoIP security to ensure they have the most proficient security solutions in place.

Keywords:

Voice over IP, VoIP Security Risks, VoIP Denial of Service (DoS), SPIT, Voice Service Theft, SIP Registration Hijacking, Eavesdropping, Directory Harvesting, Vishing

Quotes:

- “Just as data networks have succumbed to pernicious threats, voice over IP systems face a parallel path,” said Eric Aarrestad, Vice President at WatchGuard Technologies. “As organisations continue to converge networks and adopt VoIP, businesses both large and small will have to evolve their security architecture to ensure that their customers, users and data are safe from VoIP threats.”

About WatchGuard Technologies, Inc.

Since 1996, WatchGuard® Technologies, Inc. has been the advanced technology leader of network security solutions, providing mission-critical security to hundreds of thousands of businesses worldwide.

The WatchGuard family of wired and wireless unified threat management appliances and WatchGuard SSL VPN remote access solutions provide extensible network security, unparalleled network visibility, management and control. WatchGuard products are backed by WatchGuard LiveSecurity® Service, an innovative support, maintenance, and education program. WatchGuard is headquartered in Seattle and has offices serving North America, Europe, Asia Pacific, and Latin America. To learn more, visit <http://www.watchguard.com/>.

Contacts:

Natasja de Groot
WatchGuard Technologies Inc
+ 31- 70 711 2085
natasja.degroot@watchguard.com

Allie Andrews
PRPR
+ 44 (0)1442 245030
allie@prpr.co.uk