



Secure Wireless Management

PRESS RELEASE

Contact:

Drew Tick
Code Red Systems
Tel: +972-2-642-3401, ext. 100
Cell: +972-54-453-3798
Fax: +972-2-678-3403
Email: drew.tick@code-red.biz

FOR IMMEDIATE RELEASE

February 14, 2007

PHILIPS SELECTS AIRSTOP® TO PREVENT WIRELESS BRIDGING ATTACKS

Israeli Office Deploys AirStop Endpoint Security Software to Thwart Wireless Attacks via Mobile Computers

Yakum, Israel (February 14th, 2007) – Royal Philips Electronics is a leading global company with 125,500 employees worldwide. Philips Israel, located in the high tech industrial park in Yakum, is responsible for the company's Israeli commercial activities.

System administrator Alex Zeifman, noticed that neighboring companies in the EuroPark high tech office complex had implemented wireless networks and even the coffee shop had a WiFi Hot Spot.

Since all the company laptops had an enabled wireless connection, Zeifman became concerned about potential security threats. He then observed that users logged-in to the wired corporate network were simultaneously connected to neighboring wireless networks. It seems that the user-friendliness of Microsoft Windows' Wireless Zero Configuration coupled with the intelligence of Intel's Centrino chipset resulted in automatic connection to any wireless connection in range – without asking permission, or notifying the user that a wireless connection was being made.

While authorized users innocently connected to the wired network using a standard Ethernet port, they were not even aware that their internal wireless card was connected to someone else's wireless network. In data security jargon, simultaneous connection to two networks is a serious breach also known as a "wireless bridging attack".

System administrator Zeifman immediately recognized the severity of the threat and set out looking for a solution.

Code Red Systems
21 HaVaad HaLeumi
POB 16120, Jerusalem, Israel
T +972-2-642-3401, F +972-2-678-3403

Email: info@code-red.biz; Web: <http://www.code-red.biz>



Secure Wireless Management

“We looked at profiling solutions.” said Zeifman, “but realized that these could easily be circumvented accidentally or intentionally, which is not consistent with the strict enforcement of our data security policy.”

Recalling an earlier meeting with Code Red Systems, Zeifman requested an evaluation copy of the company’s AirStop Endpoint Security Software. After extensive testing the product was approved and successfully implemented.

AirStop enforces security policy by preventing simultaneous connection to more than one network. For example, if a machine is connected using a wired Ethernet connection, AirStop automatically disables all other network connections including WiFi, 3G/Cellular, Bluetooth and others. There is nothing the user can do to enable these communications adapters once they have been disabled. In terms of storage devices, they can be disabled when connected to the network or require an embedded code to enable the device.

“AirStop is exactly what corporate IT is looking for.”, said Drew Tick the CEO of Code Red Systems, “It enforces security policy, is simple to implement, and can be easily distributed and tracked across the enterprise.”

The AirStop software is currently available on a 30-day trial basis from most major software download sites.

About Code Red Systems:

Code Red is a software developer specializing in management and security solutions for wireless networks. The company is headquartered in Jerusalem, Israel, and has a staff of software engineers with hands-on military and civilian data management and security experience. For more information please visit the company web site at: <http://www.code-red.biz>