

# COMITÉ DE R&D

---

Gerardo Belmonte Duran

Mario Pineda García

Oswaldo Silva Maldonado

# News

---



F-Secure indica que nunca había registrado tantos virus y programas malignos como durante los primeros 3 meses de 2008. La compañía agrega que si la propagación de códigos malignos continúa al mismo ritmo, para fin de año habrán surgido un millón de nuevos virus.



Intel anuncia el lanzamiento de su sistema IATT, que impedirá el robo de computadoras portátiles.

IATT (Intel Anti Theft Technology o tecnología anti robo de Intel), no es un candado físico o una cadena de acero que impide que el ladrón huya con el PC, sino de un sistema totalmente electrónico, más eficaz que todas las soluciones vistas hasta el momento, indica Intel en un comunicado.

La compañía trabaja en asociación con una serie de fabricantes de PC portátiles con el fin de lanzar el sistema antes de fin de año.

El sistema funciona parcialmente inutilizándolo para cualquier otro usuario que no sea el propietario cuando éste lo abandona. El sistema operativo no puede ser iniciado, todos los datos en el disco duro están cifrados incluyendo la BIOS, que se hace incomprensible para el hardware.

Por lo tanto, para un ladrón será difícil poder usar o vender la computadora robada.

---

# News

---



Internet creció en aproximadamente 33 millones de nombres de dominios en 2007, según el Reporte de la Industria de Nombres de Dominios correspondiente al cuarto trimestre de 2007 publicado por VeriSign. El término del cuarto trimestre muestra una base total de más de 153 millones de nombres de dominios registrados a nivel mundial a través de todos los dominios de primer nivel (TLD, Top Level Domains). Esto representa un aumento del 27% en relación al mismo trimestre del 2006, y un 5% de crecimiento comparado al tercer trimestre del 2007.



Nick White ha renunciado a Microsoft para incorporarse a la compañía de marketing BuzzCorps. Nick White fue el ejecutivo que Microsoft usó para promover Windows Vista entre sus clientes. White era un miembro destacado de The Vista Team, y logró, entre otras cosas, convencer a la gerencia de Microsoft que era conveniente revelar la actualización SP1 para Windows Vista.

La renuncia de White se debería a que, en realidad, no logró hacer su trabajo. Ni White ni el resto de Vista Team lograron crear el entusiasmo que la gerencia de Microsoft esperaba generarían en torno al nuevo sistema operativo.

Ya en octubre de 2007, White declaró "Hemos hecho un mal trabajo"

---



## Ataque de los Clones de IPHONE

HTC's Intuitive (aka Verizon XV6900)

If you think this device from Verizon Wireless looks familiar, that's because it's a HTC-sourced smartphone. The device features Windows Mobile 6 Professional suite, and includes a 2 megapixel camera, microSD slot, 256MB of ROM, 128MB of RAM, Bluetooth, and HTC's TouchFLO interface. Like the others, it's slated for April availability and will run \$349.99 on contract after \$50 rebate

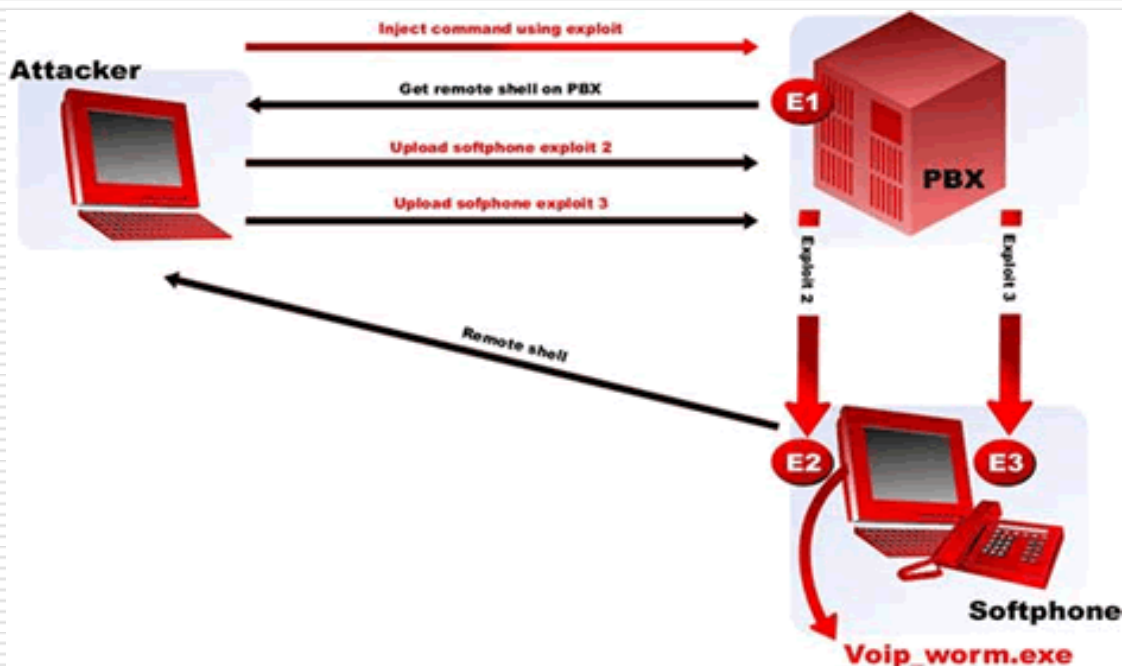
## Outrageously shocking: More than 100 Cisco, Avaya and Nortel VoIP security holes discovered

It is shocking and outrageous that there are more than 100 security holes in VoIP products from Cisco, Avaya and Nortel.

The flaws were discovered by VoIP security solutions vendor VoIPshield, which revealed the vulnerabilities to the public today.

Since VoIPshield Labs is continuously finding new vulnerabilities, they plan on monthly disclosures to VoIP equipment vendors followed by public disclosure.

An interesting example of an identified Cisco VoIP vulnerability revealed today, is shown below:





## **Outrageously shocking: More than 100 Cisco, Avaya and Nortel VoIP security holes discovered**

---

In the above example, a potential attacker exploiting the Cisco Unified Communication Manager (UCM) vulnerability related to its Disaster Recovery Network, could obtain full access to the UCM by getting the remote shell on the attacker's machine.

Subsequently the attacker could either disable UCM completely, download all the information from UCM to the attacker's machine or upload an executable file to the UCM.

Then the attacker could force all the Cisco softphones connected to this UCM to reboot and download that executable file.

It could be a bot, Trojan or worm.

Once the executable is downloaded and executed an attacker is able to have full access to the user's laptop running the softphone.

This scenario could be repeated when, for example, the user of the laptop connects to another UCM.

---

# THE NEW DATA CENTER

STRATEGIES AND TECHNOLOGIES FOR OPTIMIZING IT.

## SECURE THIS!

Virtual stacks open to attack. Hidden XML payloads destined for business partner networks. Mobile applications on unsecured cell phones. How to prepare for the irksome security problems creeping up as virtualization, SOA and mobility technologies meet inside and outside the enterprise



**Four virtualization security companies to watch**  
**These companies aim to keep virtual servers secure by providing access control, patch management and more**

Few reports have surfaced of security breaches in virtual-server environments, but the potential looms large. "Every single platform we have had in IT eventually gets compromised. There is no reason for us to think that the hypervisor is going to be any different," says Pete Lindstrom, a senior analyst with Burton Group. "While hypervisors seem to pose a fairly small attack-surface, as they multiply across a network, so do the attack surfaces. It is a huge unknown."

That's why companies widely adopting virtualization today must have a solid strategy for securing these environments, industry watchers say.

"During the 'Gold Rush' mentality of this server virtualization craze -- the more you deploy, the more you save -- the cost of securing the virtual environment has not been weighed," says Phil Hochmuth, a senior analyst with Yankee Group. "At the same time security has become an afterthought, researchers are publishing rootkits and people are thinking of ways to hack hypervisors -- it has to raise some eyebrows in the security world," he says.



---

Problems include unsecured virtual-machine-to-virtual-machine communications, poor visibility into hosts' server traffic, and virtual-machine configuration and patch management. As concern grows, established security vendors are adding virtualization features to their product road maps and newcomers are delivering purpose-built technology for the virtual realm.

Here are four virtualization-security companies that should be on every network-security manager's radar.

### ALTOR NETWORKS

**Founded:** March 2007

**Headquarters:** Redwood City, Calif.

**Management:** CEO Amir Ben-Efraim, previously head of business development for [Check Point Software](#).

**Funding:** \$1.5 million of Series A funding in spring 2007 from Accel Partners and Foundation Capital.

### BLUE LANE TECHNOLOGIES

**Founded:** February 2003, in stealth mode until November 2005

**Headquarters:** Cupertino, Calif.

**Management:** CEO Jeff Palmer, most recently president of GetThere, an online corporate-travel procurement solution; and Allwyn Sequeira, senior vice president of product operations, previously senior vice president of technology and operations at netVmg, an intelligent route control company acquired by Internap Network Services in 2003.

**Funding:** \$5 million in November 2003 from Matrix Partners and Benchmark Capital; \$13.4 million in September 2005 in Series B funding led by Duff Ackerman & Goodrich and previous investors; \$8.3 million in November 2006 from Presidio STX and previous investors.

**What the company offers:** [VirtualShield software](#)

---



---

## CATBIRD

**Founded:** Established in 2000; shifted focus to virtual network security in July 2007.

**Headquarters:** Scotts Valley, Calif.

**Management:** CEO Ron Lachman, an entrepreneur who served as executive vice president at Interactive Systems and co-founded Praxsys, which he sold to Sun in 1992.

**Funding:** Self-funded.

**How the company got its start:** Launched by Lachman in 2000, its focused on network monitoring. In 2002, the company morphed into a managed security-service provider for the banking industry. In 2005, Catbird transformed its service into physical network-security technology, which eventually matured to include virtual network-security. In July 2007, Catbird introduced V-Agent, a VMware-certified virtual appliance for network security.

**What the company offers:** The V-Agent virtual appliance, which runs as guest software in the VMware hypervisor to monitor and protect virtual machines, and the V-Security software suite. The suite includes HypervisorShield,

## REFLEX SECURITY

**Founded:** 2000; incorporated in June 2003

**Headquarters:** Atlanta

**Management:** Hezi Moore, CTO and founder, is considered a pioneer in network intrusion prevention. Previously, he co-founded and served as president of MicroTech Systems, a firm specializing in network design and configuration point-of-sale systems.

**Funding:** Seed funding in 2000; Series A funding in July 2003; \$12 million in Series B funding led by Spencer Trask Ventures and RFT Investment in September 2006, for a total of \$25 million in funding to date.

**How the company got its start:** Launched by Trellis Network Security in August 2000; in June 2003, Series A investors created Reflex Security, focused on appliance-based gateway security. By early 2007, the company decided to try its hand at addressing security challenges in virtual-server environments. "Visibility is a challenge at the virtual layer, lack of control due to server mobility is an issue, and it is necessary to have a security tool inside the virtual environment," Moore says.

**What the company offers:** Virtual Security Appliance (VSA) software

---