

**Join the Dark Side**

Click [here](#) for the DR Weekly Newsletter, and [here](#) to enjoy site member benefits

**WEB SECURITY YOU CAN COUNT ON.**[FREE SECURITY SCAN >](#)

DATE: April 14, 2008

LIVE EVENT: **Ethernet Expo Europe**

LOCATION: The Business Design Centre, Islington, ...

[More Information](#)

# PineApp Rolls Out ZombiCop

## PineApp announces new ZombiCop in fight against increasing threat from Zombies

APRIL 11, 2008 | IRVINE, Calif. -- PineApp, a global leader in securing networks and email systems, has launched its new ZombiCop solution for ISPs to block the growing volumes of spam from zombie computers that is increasingly resilient to existing anti-virus or anti-botnet defences.

Zombie computer networks, comprising desktops or servers that have been attacked and compromised by a Virus or Trojan-horse, account for more than 95% of spam worldwide. They have the ability to break through conventional layers of security around the enterprise and end user to carry out massive distributed denial of service (DDoS) attacks as well as send malware, phishing emails and viruses.

With pressure on ISPs to prevent zombie attacks emerging from their networks, PineApp ZombiCop works by filtering zombie traffic at the perimeter and classifies over 50 million IP addresses, weeding out the majority of malicious attacks. It also uses a combination of advanced methods to detect zombie behaviour patterns and threats, including an IP reputation profile engine that assesses risk and identifies likely sources of zombie emails, while providing a scalable and cost efficient infrastructure for ISPs, saving bandwidth usage and providing business continuity. With ZombiCop, unwanted communication is blocked and ISP mail-server blacklists are significantly lowered.

PineApp ZombiCop can be used as a 'passive inspection sniffer', alerting the ISP once a zombie is detected; or as an 'active policy enforcer', blocking or reducing traffic generated from a detected zombie IP. It can also be used as a 'smart traffic analyser', adding content inspection layers and the ability to detect other protocols, such as P2P and VoIP.

[PineApp Corp.](#)
[DISCUSS](#) [EMAIL](#) [PRINT](#) [LINK/REPRINT](#) [SHARE](#)
**MESSAGE BOARDS**[Discuss this story >](#)

- [DISCUSS](#)
- [EMAIL](#)
- [PRINT](#)
- [LINK/REPRINT](#)
- [SHARE](#)
- [RSS](#)

**RELATED****VIDEO**

**Dan Kaminsky,**  
Director -  
Penetration Testing,  
IOActive  
[PLAY](#) (06:49)  
Flaws: Back to the Future



**Jennifer Granick,**  
Director - Cyberlaw  
Clinic, Stanford Law  
School  
[PLAY](#) (05:33)  
Is That Legal?

**NEWS ANALYSIS**

- [Panel: DLP Outlook Hopeful, But No Silver Bullet](#) 4/11/2008

- [Tech Insight: Virtualization Gets Personal](#) 4/11/2008

**RESEARCH**

- [Identity Management: Telcos vs. Web 2.0 Titans](#)

- [Subscriber Information Management: Who's Doing What](#)

- [Unified Threat Management: The Market Beyond SMBs](#)

- [Mobile Malware: The Enterprise at Risk](#)

**WEBINAR ARCHIVE**

- [From IM to Social Networking: Securing Employee Use of the Web](#) 3/26/2008

- [Security Update: eCards, Email Threats and Compliance](#) 10/24/2007

**COLUMNS**

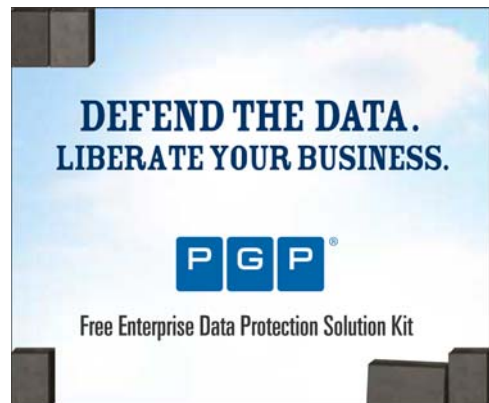
- [Inconvenient Lack of Truth](#) 4/4/2008

- [Hacking WiFi](#) 3/13/2008

**REPORTS**

- [A Peek at Snort 3.0](#) 3/20/2008

- [Ten Myths About Identity Fraud](#) 2/12/2008

[AI Gore Bans Press at RSA](#)[AirPatrol Keeps Tabs on Illicit Mobiles](#)[IBM's 'Phantom' to Study Virtual Security](#)[MORE KEYHOLE](#)**BUGS****ENTERPRISE VULNERABILITIES**

**Vulnerability:** Tumbleweed securetransport\_server\_app  
**Published:** 2008-04-11  
**Severity:** HIGH  
**Description:** stack-based buffer overflow in the iactivextransfer.filetransfer method in the securetransport.filetransferactivex control in cvst\_en.dll 1.0.0.5 in tumbleweed securetransport server before 4.6.1 hotfix 20 allows remote attackers to execute arbitrary code ...

**Vulnerability:** cups CUPS  
**Published:** 2008-04-10  
**Severity:** MEDIUM  
**Description:** multiple integer overflows in (1) filter/image-png.c and (2) filter/image-zoom.c in cups 1.3 allow attackers to cause a denial of service (crash) and trigger memory corruption, as demonstrated via a crafted png image.

**Vulnerability:** Python Software Foundation Python  
**Published:** 2008-04-10  
**Severity:** HIGH  
**Description:** integer signedness error in the zlib extension module in python 2.5.2 and earlier allows remote attackers to execute arbitrary code via a negative signed integer, which triggers insufficient memory allocation and a buffer overflow.

**Vulnerability:** Samba rsync  
**Published:** 2008-04-10  
**Severity:** HIGH  
**Description:** buffer overflow in rsync 2.6.9 to 3.0.1, with extended attribute (xattr) support