

**CATBIRD™ INTRODUCES NEXT WAVE OF HACKER
PROTECTION WITH IMMEDIATE RECOGNITION,
IDENTIFICATION, AND NEUTRALIZATION OF ZERO-DAY
THREATS AS THEY EMERGE**

**Emerging Threat Intelligence™ accurately detects and shields users
from phishing, command and control, “warez,” underground economy
and other ever-mutating sites**

DEERFIELD, IL (August 15, 2006) – Catbird Security™, developer of the most comprehensive hacker protection technology for mid-tier service providers, today announced the latest enhancement to its Catbird Shield™ security system, Emerging Threat Intelligence (ETI).

ETI dynamically protects network users from the constantly mutating world of Internet threats -- including phishing sites, botnet command and control centers, and underground economy dens – with unprecedented reaction time and accuracy.

Emerging Threat Intelligence provides network users with up-to-the-minute protection thanks to its virtually instantaneous ability to detect and prevent access to the transient and insidious parts of the Internet as soon as they emerge. Integrated as a standard component of The Catbird Shield's comprehensive Internal Intrusion Protection Shield™ that already includes rogue-user detection; intelligent internal vulnerability monitoring; credentialed and policy scanning; and email and heartbeat monitoring, ETI is the latest example of Catbird's commitment to regularly introducing new, cutting-edge technologies that keep pace with the evolving security landscape.

The Catbird Shield offers an unmatched breadth of hacker protection on both internal and external networks at an affordable price. It is available through Catbird's network of service providers, bringing best-in-class protection to mid-market end users.

Employing real-time feeds of vetted information regarding new and emerging threats on the Internet, Catbird's Intrusion Prevention System (IPS) with ETI protects a user from being attacked by bad traffic or stumbling into undesirable destinations within unprecedented short times of their first appearance on the Internet.

Until now, state-of-the-art IPS offerings mitigated threats through signature-based or behavioral detection, introducing delays in identifying trouble spots as well as producing high levels of false positives. Catbird's feeds will dynamically change with the landscape of the security scene, providing instant up-to-date information used to make undesirable sites and a user's network inaccessible to each other.

Incorporating feeds of such actionable intelligence about legitimately identified bad sites into Catbird's IPS offers users the benefits of eliminating the false positives and noise that can typically plague standard IPS's. Partners and their customers are able to stay on top of any emerging threat in the Internet security landscape while preventing new strains of malware from infecting the network without the need to retain sophisticated security and forensic personnel.

"This is what the IPS was born to do, but unfortunately specific, unimpeachable data of this scope was never available to populate it," said Edmundo Costa, chief operating officer of Catbird. "Aggregating our real-time intelligence with Catbird's continuous, automated, security-as-a-service architecture takes hacker protection to a new level. No one can take a wrong turn anymore and wind up with a flat tire in the middle of the dark, spooky forest of malware sites."

The dynamic nature of the threat environment means that new vulnerabilities are rapidly exploited by malware and malicious websites. Catbird's ETI maintains an ever-evolving list of up-to-date risky IP addresses and known malicious sites. Specifically, the ETI protects against:

- Distributed Denial of Service (DDoS) and botnet Command and Control Center (C&C) threats

Millions of machines around the world have been infected with viruses and spyware that subjects them to the surreptitious control of other machines. The infected machines function as a virtual network known commonly as "botnets." Botnets actively work to propagate themselves and to attack high-value targets within and outside their location. In many cases,

botnets are used in DDoS attacks. Catbird's IPS with ETI detects any attempt by an infected machine to contact another infected machine or a Command and Control center. Catbird obtains up-to-the-minute listings of these threatening sites, blocks any attempt to access their content, and reports the offending machine.

- Phishing and Malware URLs.

Thousands of web sites on the Internet are fraudulent or malicious. Phishing sites, for example, spoof the look of a legitimate website in order to coax customers into giving confidential information, leading to identity and asset theft. Any attempt to access these sites represents a threat to the user and the spoofed institution. Catbird's IPS with ETI maintains a continuously-updated list of known phishing URLs and blocks attempts by users to reach them.

- Underground Economy - IP addresses with known illegal activity

Thousands of web sites are used to disseminate and traffic in illegal material, such as the trading of credit card numbers or software exploits. Such data is worth millions of dollars on the black market. Catbird's IPS with ETI obtains up-to-the-minute listings of these sites and blocks any attempt to access their content.

- "Warez" - Sites with pirated content

Web sites around the world are known to contain pirated content that violates copyright laws. Warez sites are usually managed by organized groups of thieves, and traffic in everything from movies to software. Catbird's IPS with ETI obtains up-to-the-minute listings of these sites and blocks any attempt to access their content.

- General Emerging Threats

Tracking the ever-mutating types of attacks that creative hackers conjure up is an overwhelming task. The recent Internet Explorer WMF vulnerability and the associated web sites that contained malware WMF files is an example of a fast-moving and wide-ranging assault with serious consequences. Catbird's IPS with ETI is right on the front lines, identifying such new emerging threats, gathering the intelligence regarding who is exploiting the vulnerability, and preventing users from being harmed before they even realize the problem exists.

“We have been using Catbird for years and are impressed with the corporate commitment to staying on top of any new security risk threatening our business,” an enthusiastic Kevin Herrington, Chief Technology Officer of Cumberland Bank noted. “The release of Catbird’s ETI is yet another example of the highly-sophisticated, futuristic protection we’ve come to expect of them. We feel confident that we are shielded against any new type of malware that the hackers might devise.”

“Unless there is a dedicated black-hat security expert on the payroll, actionable intelligence of this nature would never be available to most businesses,” says Tamar Newberger, vice president of marketing at Catbird. “Not only does Catbird aggregate this invaluable data as a no-touch, no-install, no-hassle service, but it does so in conjunction with providers who can then bring enterprise-class levels of security at an affordable price point to their own customer base.”

About Catbird

Catbird Security, a division of Catbird Networks, Inc., is the developer of the most comprehensive and advanced hacker protection technology for mid-tier service providers. Using the completely non-invasive Catbird Shield, service providers are able to easily and immediately build their own branded solutions, offering their end-user customers the benefits of comprehensive and sophisticated hacker protection heretofore out of reach to anyone without large IT security budgets. Hundreds of customers today rely on Catbird to protect their networks from external and internal threats.

For more information, please visit www.catbird.com or contact Tamar Newberger at Catbird Networks at tamar@catbird.com or 212-677-2101.

Catbird, Catbird Security, Catbird Shield, Internal Intrusion Protection Shield and Emerging Threat Intelligence are trademarks of Catbird Networks, Inc.