

Catbird Anti-Pharming Suite and Catbird Pharming Shield



Protect your customers' confidential data, and your company's reputation, from pharming attacks.

PHARMING—STEALING YOUR ONLINE INFORMATION AND IDENTITY

Pharming attacks are among the most virulent, and devastating, security breaches a company can suffer. When hackers steal customers' confidential data—or even entire identities—the damage to the company's reputation and revenue can be irreversible.

In a pharming attack, a hacker builds a spoofed home page that looks exactly like the real thing. He then invisibly redirects customers to his fake site, where an unsuspecting user enters ID, password, and other confidential information which the hacker will “pharm” for illegitimate purposes. Eventually the user is automatically switched back to the legitimate site, without any idea his information has been compromised. The hacker can now make charges on a customer's account, or steal their identity.

Pharming is particularly alarming because it usually goes undetected, by both the institution and the end-user, until well after the damage has been done.

PHARMING SHIELD



Catbird's Anti-Pharming Suite can quickly detect a pharming attack so that a remedy can be initiated before any significant harm takes place. Websites protected by Catbird have the option of displaying The Catbird Pharming Shield logo. The Pharming Shield is

a recognized brand synonymous with safe web surfing. Websites protected by Catbird are continuously monitored for pharming attacks, 24x7, 365 days a year. The logo displays the most recent time the page was checked for legitimacy and the results of this check. A clean bill of health is a sign to customers that the website is safe and open for business.

Clicking on the Pharming Shield logo yields more detailed results of Catbird's Pharming protection – in effect a website report card. Easy-to-understand data is displayed including the timing and frequency of Catbird's protective monitoring.

CATBIRD'S ANTI-PHARMING SUITE

The suite consists of three monitors which work together to provide a website with total protection from pharming attacks.

BENEFITS

Maintain customer trust

Catbird's Pharming Shield validates website legitimacy to users

Protect website integrity

Safeguard customers' confidential data, and the company's reputation, against malicious and widespread Pharming attacks.

Protect SSL integrity

Guarantee the integrity of customer's online transactions.

Prevent defacement

Prevent hackers from defacing a website with subtle, dangerous code changes or offensive text and graphics.

Zero-touch install

Catbird's “in the cloud” agents are completely non-invasive with no software to install or integrate within the corporate network.

Immediate notification

Be informed the instant an attack occurs, via automatic monitoring all day, every day, as frequently as every two minutes

Monitor website security from strategic points across the Internet

Catbird's agents are optimally positioned to see your network in the context of the entire Internet.

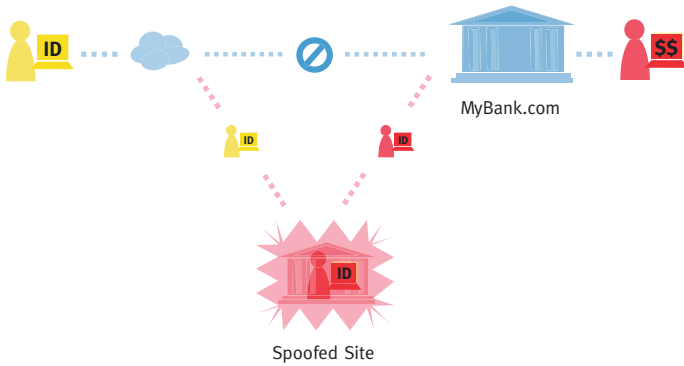
Protect reliably

Catbird's agents are outside of the corporate network and firewall so hackers can't disable or work around them.

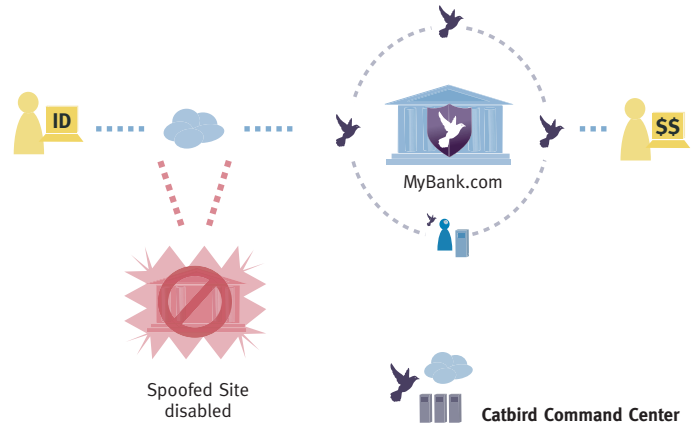
Catbird Anti-Pharming Suite and Catbird Pharming Shield

Pharming Detection Suite

Traffic intended for MyBank.com can be hijacked on the public Internet



- 1 MyBank customer logs on**, but traffic has been pharmed to a “look-alike” or “spoofed” site where customers “give” hijacker account and password. Hackers can go to real bank site, access account, steal money and identity.



- 2 Catbird Pharming Detection Suite** monitors the site and alerts the administrator to pharming attack. Integrity of the site is re-established and MyBank customers connect to the site protected by Catbird's monitoring.

DNS Pharming/Hijacking Monitor

The DNS Pharming/Hijacking Monitor protects a website to ensure its legitimacy. DNS hijackers exploit Internet routing protocol vulnerabilities which are insecure due to lack of two-way authentication. Typically, pharmer will either hack into a DNS server and reroute legitimate URL requests, or poison the BGP routes and exchange an SSL certificate with the customer.

The Catbird Pharming/Hijacking Monitor works by taking a snapshot of all of the company's DNS records. Catbird's extensive network of agents constantly monitor the Internet, comparing these corporate snapshots with current DNS records every two minutes. If they don't match, an alert is sent to appropriate security personnel to resolve the problem immediately.

Secure Certificate Monitor

Catbird's Secure Certificate Monitor is unique in the field. An SSL certificate is a one-of-a-kind fingerprint, meant to validate that a website is what it claims to be and that transactions between the site and its users are secure. By checking the validity of a company's Secure Certificate every two minutes, Catbird's agents work around the clock to ensure routine ecommerce does not fall victim to Internet Pharming.

The Secure Certificate Monitor is ideal at preventing the “man in the middle” attack typical of pharming. In this type of attack, a hacker poisons BGP routes and then exchanges a SSL certificate with the customer, allowing the hacker to

covertly eyeball traffic headed toward the legitimate website. The bad guys now see secure traffic in its unencrypted form, including confidential information such as account numbers and passwords.

To counter this, Catbird uses its swarm of agents around the Internet to follow poisoned BGP paths and detect the accuracy of secure certificates being exchanged with customers. The Secure Certificate Monitor essentially picks up the SSL fingerprint from the target and then continually compares it to results from all over the world. If someone changes the BGP routing to send traffic to the wrong target, remote Catbird agents routed to this malicious destination sound the alarm immediately to inform security personnel.

Defacement Monitor

Catbird's Defacement Monitor proactively identifies unauthorized changes to a corporate website. Such an alteration could be the first indication that a pharming attack is underway. While pharmer often redirect users to lookalike “spoofed” sites, another type of pharming attack makes a subtle change to a legitimate site in order to harvest confidential data or insert malicious code.

Catbird's Defacement Monitor protects a company's website by establishing “baseline content”—approved content for the web site—and comparing it to the live site every 2 minutes, every day. If a mismatch occurs, Catbird's network of agents will immediately detect this and send an alert, so the problem can be addressed before customers are at risk.