



▼ **GMO-HS adds Armorize HackAlert™ Malware Detection Service to its Web Hosting Platform**

Santa Clara, US - Apr 22nd, 2009

Armorize Technologies, the Santa Clara based web application security provider, has announced a partnership with leading Japanese web hosting company, GMO HOSTING & SECURITY, INC. of GMO Internet Group.

Leveraging Armorize's position as industry-leader in malware analysis and reengineering, GMO-HS has added security to its web hosting platforms with the Armorize HackAlert™ website malware remote monitoring and alerting service.

Armorize HackAlert™ is a Software-as-a-Service (SaaS) solution that monitors subscriber websites, detecting injected malware and malicious links that target computers browsing the affected web pages. HackAlert™ features customizable alerting and notification options facilitating immediate reaction and remediation.

"In deploying HackAlert™ GMO-HS is demonstrating its commitment to security," said GMO-HS President & CEO Mitsuru Aoyama. "This service will ensure that our clients are equipped with the means to protect their customers, partners and end-users from zero-day exploits and malware."

Web Application Attacks and "Drive-by-Downloads" Target End Users

With increasing frequency, enterprises experience compromise through their websites which are targeted by hackers exploiting vulnerable coding and configuration.

These attacks typically result in the compromised site directing malware at end-user computers, stealing information such as stored files, banking details, account credentials and passwords.

This phenomenon, referred to as "drive-by-downloading", can have a serious impact on compliance efforts and business reputation as well as far-reaching legal implications.

HackAlert™ Hosted Service Detects and Mitigates Web Malware Injection

HackAlert™ is a Software-as-a-Service (SaaS) solution that monitors websites, detecting malware drive-by-downloads and malicious links.

HackAlert™ represents a critical component of the Incident Response process, ensuring that if a website is injected with malicious links or malware targeting end-user PCs, the application administrators can react immediately. Email and Console alerts provide malware details including name, file type and source, as well as the target download destination on computers browsing the site.

With HackAlert™, GMO-HS' clients ensure their website customers, partners and end-users are protected from hackers seeking to steal information stored on their computers.



▼ **GMO-HS adds Armorize HackAlert™ Malware Detection Service to its Web Hosting Platform**

HackAlert™ Boosts Security for GMO-HS Hosting Clients

HackAlert™ provides significant security benefits to GMO-HS' web hosting clients:

Monitoring & Incident Response

- Around-the-clock website monitoring and reporting
- Immediate detection of malware/malicious link injection
- Configurable alerting options (console, Email)
- Extremely low false positives and negatives
- Support for single URL scans and full website crawling
- Protects clients, customers and end user from compromised website

Web Malware Detection

- Behavioral analysis highlights fundamental web application vulnerabilities
- API hooking sandbox traps and passes website malware to Dynamic Malware Analysis engine
- Spyware Behavior Extractor identifies malware name, file type and source as well as download destination on end-user PC
- HTML analysis engine identifies malicious links embedded in the web page
- Scheduled scans provide ongoing analysis, detecting recurring malware injection

Low management overhead

- Hosted service requires no management overhead
- No server software or agent installation required
- Immediate access to updates and upgrades
- Online management console facilitates on-demand or scheduled scans

HackAlert™ Addresses New Hacking Paradigm

"GMO-HS is Japan's leading web hosting provider," said Armorize CEO Wayne Huang. "Their adoption of Armorize HackAlert™ demonstrates their commitment to web application security and, in particular, to addressing the new hacking paradigm where hackers leverage vulnerable websites to attack the computers browsing them."

With HackAlert™, GMO-HS now offers seamless security monitoring for multiple websites from a single Internet-based console. This service places the hosted website under constant vigilance while ensuring administrators and security personnel have the tools to react immediately in the event of a compromise.



▼ **GMO-HS adds Armorize HackAlert™ Malware Detection Service to its Web Hosting Platform**

About GMO Hosting & Security, Inc.

One of Japan's leading hosting providers, GMO HOSTING & SECURITY, INC. (TSE: 3788) has been providing a diverse range of hosting services through the two brands iSLE and RapidSite since it was first established in 1997. While hosting services are the core of GMO-HS' business, the company also provides a range of Internet solution products such as electronic authentication certificates and hosting service OEM to ISPs and web hosting companies. In November 2006 GMO-HS received the ISMS (Information Security Management System) International Standard ISO/IEC27001:2005 and JIS Q 27001:2006 Certification

For more information, visit <http://www.gmo-hs.com/eng>

About GMO Internet Group

GMO Internet Group, headquartered in Japan, is a leading force in the Internet industry offering one of the most comprehensive ranges of Internet services worldwide. The group holds top domestic market share in domain registration, web hosting, and payment processing and provides a host of other Internet services including global online security services, e-commerce solutions, and Internet advertising to both businesses and individuals. At the centre of the group is GMO Internet, Inc., a company listed on the prestigious first section of the Tokyo Stock Exchange (TSE: 9449).

For more information, visit <http://www.gmo-hs.com/eng>

About Armorize Technologies

Armorize Technologies is a software security company focused on web application security

As part of the Armorize Appsec Suite™, the HackAlert™ service integrates with CodeSecure™ Static Source Code Analysis platform and the SmartWAF™ Web Application Firewall (WAF) to provide end-to-end security for web applications.

The Armorize team has deep roots in web application security research and development, winning consecutive awards at the prestigious 2003 and 2004 International World Wide Web Conferences. Subsequent corporate recognition for innovative technology and business practices include winning the Red Herring Asia 100 award and being invited to present at the Dow Jones Venture Wire Technology Showcase 2008.

Headquartered in Santa Clara, CA, with its R&D center in the Nan Kang Software Park in Taipei, Taiwan, Armorize has a global customer base with clients among finance, telecom, government and technology sector leaders.

Contact:

John Linehan
Armorize Technologies Inc.
Phone: +1-408-216-7893 ext.401
Email: pr@armorize.com