



Media Contacts:

Patricia Koebele

Digital Defense, Inc.

210.582.6128

patricia.koebele@ddifrontline.com

DIGITAL DEFENSE RELEASES VULNERABILITY CHECK FOR ENTERPRISE-WIDE CONFICKER DETECTION ON INFECTED DEVICES

San Antonio, TX – February 17, 2009 – [Digital Defense, Inc.](#) (DDI), a leading provider of information security assessment services and Security Information and Assessment Management (SIAM) solutions, announced they implemented an important consolidated vulnerability check (CVC) within their Frontline Vulnerability Scanner. The new vulnerability check is associated with the Conficker worm and DDI has already made it available to their client base. The importance of this particular CVC is that it does not merely indicate which systems are vulnerable, but it provides the ability to quickly glean which specific hosts the worm has manifested itself on across an entire network, no matter how large or spread out.

“Our Vulnerability Research Team (VRT) quickly recognized that many of the existing detection tools only allowed organizations to check for a Conficker infection one host at a time. Because of our remote scanning ability and Software as a Service (SaaS) approach to fulfillment, DDI’s new consolidated vulnerability check gives our clients the capability to rapidly assess their entire enterprise for Conficker infected hosts,” explained [Gordon MacKay](#), Executive Vice President of Research and Development at Digital Defense. “Due to the gravity of Conficker infections, DDI’s VRT wanted to ensure our clients had the tools necessary to rapidly identify and quarantine infected hosts to limit the overall impact to their corporate networks.”

DDI’s [proprietary assessment engine](#), combined with the Company’s [Frontline™ Vulnerability Lifecycle Management](#) offering, provides enterprise-wide, distributed network scanning capabilities on an on-demand basis. Via the offering, clients can assess any device within their network on an on-demand basis, regardless of its geographic location. Additionally, clients can also avail themselves to the Frontline portal, which DDI architected to best support the needs of each client in terms of scan and penetration test reporting and workflow management. Via additional modules contained within the Frontline portal, clients can also associate business risk with each device, allowing for further optimization of their risk mitigation plans. Simply put, DDI clients subscribing to the Vulnerability Lifecycle Management and [Penetration Test](#) services benefit not only from DDI’s ongoing investment in their SaaS platform and solutions, but the strength and integrity of their [VRT](#) and [Security Operations Teams](#) as well.

About Digital Defense

Digital Defense, Inc. (DDI), an approved scanning vendor by the Payment Card Industry (PCI) Security Standards Council (SSC), delivers a comprehensive portfolio of risk management services including information security programs, regulatory compliance solutions, security testing of IT products and security education offerings. DDI and its Security Operations team uses proprietary Software as a Service (SaaS) technology and industry best practices to deliver a broad array of services to clients, which range from small financial institutions to global Fortune enterprises. Frontline™, DDI's flagship service portal, provides clients with instant access to a SIAM platform that enables independent oversight of their organization's security posture on an autonomous or DDI-managed service basis. For more information about Digital Defense, please visit our web site at www.ddifrontline.com or contact us at 888.273.1412.

Reader Contact Information

Digital Defense, Inc., 9000 Tesoro Drive, Suite 100, San Antonio, Texas, 78217

Phone - 210.822.2645, Fax - 210.822.9216

www.ddifrontline.com

###

Digital Defense and the Shield Logo are Registered Service Marks of Digital Defense, Inc. All other trademarks are the property of their respective owners.