

What are "blended threats"?

by Gregg Zepp

The online glossary from Symantec ¹ defines blended threats as follows:

Blended threats combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, **blended threats** can rapidly spread and cause widespread damage. Characteristics of **blended threats** include:

- *Causes harm: Launches a Denial of Service (DoS) attack at a target IP address, defaces Web servers, or plants Trojan Horse programs for later execution.*
- *Propagates by multiple methods: Scans for vulnerabilities to compromise a system, such as embedding code in HTML files on a server, infecting visitors to a compromised Web site, or sending unauthorized email from compromised servers with a worm attachment.*
- *Attacks from multiple points: Injects malicious code into the .exe files on a system, raises the privilege level of the guest account, creates world read and writeable network shares, makes numerous registry changes, and adds script code into HTML files.*
- *Spreads without human intervention: Continuously scans the Internet for vulnerable servers to attack.*
- *Exploits vulnerabilities: Takes advantage of known vulnerabilities, such as buffer overflows, HTTP input validation vulnerabilities, and known default passwords to gain unauthorized administrative access.*

Effective protection from **blended threats** requires a comprehensive security solution that contains multiple layers of defense and response mechanisms.

Trendmicro's older definition ² breaks the conceptual notion of blended threats into two scenarios:

*A **blended threat** can describe one of two different scenarios. In the first, a blended threat refers to a multi-threat, or a combination of threat technologies into a single vector (e.g., a [Trojan](#) exhibits [worm](#) -like capabilities). In the second, a blended threat refers to a single threat that attacks via multiple vectors (e.g., a worm gains entry via email and then leverages back-door vulnerabilities for further infection and destruction). **Blended threats** are inherently malicious and spread rapidly.*

More recently, their definition ³ for blended threat has been shortened to:

... bundles of malicious programs that combine the functionality of different types of malware, including Trojans, worms and backdoors. A blended threat often involves an infection chain whereby a visitor to a website is first diverted to a malicious URL, then compelled via social engineering to download a malicious file which then continues to download additional

malicious files. By using multiple methods and techniques cybercriminals are able to quickly and surreptitiously spread threats.

In Chapter 1 of our Principles of Computer Security texts, it discusses select security incidents from the past. Of those mentioned, several could be considered "blended threats." For example, the Morris Worm of 1988. This worm exploited security several vulnerabilities in unix-based systems. Morris propagated by exploiting vulns in unix's sendmail, fingerd, and rsh components. It used buffer overflow and other techniques to exploit these vulns. Another is discussed is the Code Red Worm of 2001. First, Code Red would check the host's system clock. If the date was between the 1st and 19th of the month, it attacked exploiting a buffer overflow vuln in IIS server and spread itself via a random list of IP addresses it generated. If the date was between the 20th and 28th of the month, instead, the worm stopped infecting other systems and used currently infected machines to launch a DoS attack against WhiteHouse.gov. If it was after the 28th, the worm did nothing.

Blended threats attack using multiple techniques. Defending against such threats means the same, using multiple techniques. Practicing "defense in depth" through hardening network devices, customized set of firewall rules for your enclave, NIDS, HIPS, and A/V, along with other monitoring devices and software, such as rogue system detection applications, and even decoys, such as honeypots can help protect your organizations systems from attacks that use multiple attack vectors.

-
1. Symantec: http://www.symantec.com/business/security_response/glossary.jsp
 2. TrendMicro: (available as cached page only):
[http://webcache.googleusercontent.com/search?q=cache:8hiccQ83VIJ:us.trendmicro.com/us/threats/enterprise/threats-summary/blended-threats/+"blended+threats"&cd=6&hl=en&ct=clnk&gl=us](http://webcache.googleusercontent.com/search?q=cache:8hiccQ83VIJ:us.trendmicro.com/us/threats/enterprise/threats-summary/blended-threats/+)
 3. TrendMicro: (once at this site, click on the "B" tab): <http://us.trendmicro.com/us/trendwatch/awareness-and-prevention/threat-glossary/index.html>