

## **.NET or not, Microsoft Security Vulnerabilities Continue**

**David Mitchell Smith**

Contrary to recent press reports, the "donut" virus is not really a ".NET virus." Nevertheless, it underscores the need for continued vigilance against security vulnerabilities in Microsoft technology.

## NEWS ANALYSIS

---

### Event

Recently, the press has identified the "donut" virus, written by a 19-year old Czech hacker, as the first .NET virus.

### Analysis

This is neither a .NET virus nor a Web services virus but a repackaging of an already known Windows vulnerability. An enterprising hacker augmented a virus native to Windows assembler code with the Microsoft Intermediate Language (MSIL) — the intermediate code used by the .NET Framework. The virus can execute under versions of Windows previous to Windows XP due to backward-compatibility features. On Windows XP, MSIL implementation details correctly prevent execution of this virus.

Neither does the virus propagate through any Web service interface vulnerabilities, nor does the virus constitute a "Web service" itself. The press reporting it as a .NET virus or a Web services virus likely results from the .NET moniker being closely associated with Web services and the general confusion over .NET.

Like Java, the .NET Framework has been engineered to deal with security issues, such as buffer overruns, through its "managed code" concepts, such as type safety enforcement. However, as with all first-generation software and with the continued requirements for backward compatibility, more vulnerabilities associated with .NET will likely come to light. As the term .NET is quite vague, confusion over what constitutes a .NET vulnerability will continue. However, enterprises will not care what piece of software is vulnerable.

The virus has revealed that Microsoft faces continued security problems, even with its nascent .NET technology. Microsoft has made some security progress with managed code under .NET, but, once again, security has proven only as strong as its weakest link.

**Analytical Source:** David Smith, Internet Strategies

### Need to Know: Reference Material and Recommended Reading

- - "Virus and Malicious Code Protection: Comparison Columns" (DPRO-97192) A detailed account of desktop and enterprise-level infrastructure software offering for protection against malicious code and virus infestation. **By Lorraine Reese and Brad Henson**
  - "Microsoft Web Services: A PC-to-Internet Platform Shift (C-14-9007) The case for .Net as an evolution of Microsoft's platform strategy rather than the foundation of the company's Internet strategy. **By David Smith**

(You may need to sign in or be a Gartner client to access all of this content.)

## REGIONAL HEADQUARTERS

---

Corporate Headquarters  
56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

European Headquarters  
Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

Asia/Pacific Headquarters  
Level 7, 40 Miller Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

Latin America Headquarters  
Av. das Nações Unidas 12.551  
9 andar—WTC  
04578-903 São Paulo SP  
BRAZIL  
+55 11 3443 1509