



# Incurable Viruses: How Real Is the Threat?

By Pam Baker  
TechNewsWorld  
08/23/07 4:00 AM PT

The only type of virus that is truly incurable is a physically destructive virus. If the virus is a Trojan, worm or other file infecter, it can be cleaned up. An incurable virus would be one that alters or damages the system in some way. The question is: If there is no damage to the hardware and you can reload the OS, is the virus truly incurable?

Pimpily faced pranksters and lone profiteers who poison computer systems have been replaced by organized criminals of a different breed.

"These guys are professional organizations. They are fully funded and they're writing specifically for profit," David Frazer, director of technology services at [F-Secure](#), told TechNewsWorld. "Notoriety virus writers are all but gone now."

This new wave of organized crime is churning out professional-grade, so-called "incurable viruses" that are leaving hundreds of thousands of victims in their wake.

## Mouse Chases Cat

Malware writers are cunning, determined and largely undeterred by the security programs currently in play. Indeed, they find such programs helpful to their cause. "Malware writers have an advantage in creating viruses to get on the system without detection in that the virus writers use anti-virus products to test if their new virus is detected," Javier Santoyo, senior manager of development at [Symantec](#) (Nasdaq: SYMC), told TechNewsWorld.

"The virus writers use packers to compress and obfuscate their threats until they find a combination anti-virus vendors don't support," he added. "This is a continuous cat-and-mouse chase between security vendors and malware writers."

The types of organizations behind threats today are highly organized.

"These organizations employ people who perform a typical 9-to-5 job. They have full quality assurance and testing before they try to infect," Frazer said. "Typically, they are targeting specific organizations or companies, and the infection is usually followed with a ransom demand."

"In the consumer segments they are using users' PCs as botnets in proliferating spam out to the Internet or using loggers to steal passwords, credit card and bank details from unprotected online banking and credit-card users," Frazer detailed.

## **The Incurable Lie**

Malware writers do share one trait with their pimpled predecessors: arrogance.

"One interesting case was the Bagle / Netsky viruses. Each was authored by a separate virus writer, and they launched an ongoing war against each other in which they sought to remove the other's worms," confides Frazer. "In one day, F-Secure sent out 14 signature updates to keep up."

The viruses malware writers produce are far from the iron-clad monsters the creators purport them to be.

"Right now, there's no such thing as an incurable virus," said Frazer.

The only type of virus that is truly incurable is a physically destructive virus. If the virus is a Trojan, worm or other file infecter, it can be cleaned up. An incurable virus would be one that alters or damages the system in some way. The question is: If there is no damage to the hardware and you can reload the OS, is the virus truly incurable?

"A truly incurable virus would have to cause hardware damage," says Santoyo. "Very few viruses have existed that caused hardware damage with no chance of remediation."

However, that is not to say that the damage is not real or tangible.

"Ultimately, any malicious program can be wiped by re-imaging the hard drive; however, re-imaging may result in data loss unless you regularly back up data," Peter Firstbrook, research director at [Gartner](#) (NYSE: IT), told TechNewsWorld.

There is also the problem of invisibility that allows malware to strike repeatedly without notice.

"Malware may be very well hidden so that users don't realize they have a virus," added Firstbrook.

## **Morph Morbidity**

Viruses share a common mode of attack, according to Santoyo. First, if they can penetrate a system without being detected, they try to disable any security software from updating. This is one way that a virus can remain persistent on a system; the other is to use a watchdog process to re-launch or re-create themselves if they get deleted for any reason. Lastly, viruses also embed themselves in the operating system to be launched after a reboot.

Viruses that stop there are more easily caught and sterilized by anti-virus software. It is the more sophisticated and insidious generation that creates the most havoc.

"In general, metamorphic and polymorphic viruses are the most difficult to deal with," confided Santoyo. Both types, as their names suggest, change, mutate and move in order to avoid detection.

Zmist is a recent example of the serious threat posed by this class of viruses. Zmist replicated itself differently each time it infected a new computer. Zmist -- a.k.a. Zombie.mistfall -- is termed a metamorphic virus, one that recreates itself every time it is detected. Unless you have the exact signature, they're more difficult to detect.

"Zombie.mistfall was significant because it introduced code integration, a new vector of infection," explains Frazer. "This is where a virus would insert itself into a file and actually move code in a program out of the way and rebuild the executable that made it difficult to find within that file."

## **Tough to Track**

Polymorphic malware has been around for awhile, but it is becoming more common.

"Packers and encryption software are useful for changing the characteristics of the malware each time it is distributed to avoid signature based detection mechanisms," said Firstbrook.

The latest round of metamorphic and polymorphic viruses includes Code Red, SASSER, NIMDA, the Melissa virus, and MS Blaster. "These were very destructive and propagated very quickly," says Frazer.

Rootkits can hide malicious programs from antivirus software so that they are difficult to detect.

"Some malicious programs have multiple components that have a heartbeat message every few seconds so that if one component is deleted in an attempt to remove the malware, the remaining component will create a new version of the deleted file, making it difficult to remove unless you delete both files simultaneously," says Firstbrook.

Then there is the garden variety of stealth viruses with a hefty new dose of aggressiveness finely aimed at specific victims.

"Targeted malware (vs. mass propagation) is also difficult to detect because it takes a while for the malware sample to get to the antivirus vendors for analysis and signatures," explained Firstbrook.

## **Horrors on the Horizon**

As if viruses that jump to a different sector on a disk or move to another part of memory that has already been scanned are not difficult enough to deal with, there are other malware tricks breaching the horizon.

"In the spam community, the big trend has been sending malware in the forms of .pdf," says Frazer. "It's an accepted and universal standard and as such isn't filtered by most anti-spam software programs."

Mobile technology is also opening the door to new virus frights. Bluetooth enables mobile worms to spread by virtue of mere proximity, like an influenza virus. A Bluetooth-equipped phone can identify and exchange files with other Bluetooth devices from a distance of 10 meters or more.

As victims travel, their phones can leave a trail of infected bystanders in their wake -- although with current viruses, the recipients have to actively acknowledge the virus transmission before they can get infected.

That may soon change, however.

"Any event that gathers a large crowd presents a perfect breeding ground for Bluetooth viruses," warned Frazer.

With the advent of the iPhone, which delivers the Internet in its original glory, and the phones that will inevitably follow suit, malware writers will find new ways to exploit Bluetooth spreadability with their newly fortified arsenal of standard Internet deliverability.

It's enough to give security vendors more than just a few sleepless nights.

"The challenge is to stay ahead," said Santoyo. "Understanding the threat landscape is very important."

Researchers are busting it to bust the bad guys, however. So hope, too, is on the horizon.

Host-based intrusion prevention techniques are increasingly used in antivirus programs to detect new threats, Firstbrook said.

Some successful HIPS techniques include:

- Memory access protection (buffer overflow), since 60 percent of malicious code depends on memory manipulation techniques to inject its payload;
- Vulnerability shielding is a HIPS capability that protects known vulnerabilities from attack, regardless of the form the particular attack takes;
- Genetic heuristics -- broad signatures of exploit families designed to detect variants by using higher-level characteristics of a malicious code rather than more-detailed signatures;
- Application whitelisting/ blacklisting and "standard user" reduced privileges limit all new applications;
- Sandboxing and virtualization techniques to run the unknown "gray" code in a restricted environment show promise, but Firstbrook says they are rare in current HIPS solutions.


However, the problem of stopping these crooks in their tracks is not solely of the technical realm.

"As far as regionally, we're seeing a lot of spamming, ID theft and even targeted attacks coming out of Asia, Russia and South America. The laws and challenges in working with different governmental bodies contribute to this," said Frazer. "By no means are these the only regions, but socioeconomic and legal challenges play a role here."

Indeed, the horizon shows the potential for a true "cyber-war."

## User Armor

The best cure remains the same despite the many virus mutations: prevention. Firstbrook says there are seven steps to thwarting viruses before they can strike:

1. Use up-to-date antivirus and personal firewalls (not the Windows Personal Firewall),
2. Maintain all software (use auto update in windows) to current versions,
3. Do not use shareware or advertising  sponsored software unless it comes from a very reputable source,
4. Do not add software to view Web content of questionable sources,
5. Do not use P2P networks,
6. Do not open e-mail or attachments from people you don't know (even from people you know but were not expecting),
7. Periodically scan your PC with an online scanner (i.e. not your incumbent AV vendor.)

He suggests using one of the following:

- [Webroot](#)
- [Trend Micro](#)
- [Symantec](#)
- [McAfee](#)

ECT

[Print Version](#) [E-Mail Article](#) [Digg It](#) [Reprints](#) [More by Pam Baker](#) [Talkback](#) [XML](#) “

Copyright © 1998-2008 ECT News Network, Inc. All Rights Reserved.

