The Trend of Malware Today:
Annual Virus Round-up
and 2004 Forecast
TABLE OF CONTENTS

3  Introduction
4  Malware Distribution
7  Summary
8  What's Next

December 2003
Trend Micro, Inc.
As 2003 draws to a close, malware (viruses and other malicious code) continues to pose a challenge for computer users. Whether at the Internet gateway or on home desktops, users need to exercise vigilance to keep their digital information secure as the malware landscape continues to evolve despite content management solutions that include improved antivirus, firewall and other security innovations. By now most enterprises will have some form of protection in place, but is the solution up to the job? How do system administrators decide what solutions to implement? And how do they justify that decision to upper management in the light of current spending budgets? This report from Trend Micro is intended to provide analysis of malware trends, and future predictions, to help answer these questions.

Twelve (12) months ago Trend Micro predicted that mass-mailing worms would be the “next big thing” in malware in 2003. This has proved to be the case and mass-mailing worms are here to stay as the malware of choice, both now and for the foreseeable future.

Looking at the raw data for the busiest months for computer viruses (January to November), in a three-year period from 2001 to 2003 (figure 1), it can be seen that the number of alerts called by Trend Micro is similar for each of the 3 years. We can also see that although the routine blocking of file-types from email attachments works as an initial deterrent, other malware can still penetrate the enterprise.

Historically, malware was spread via floppy-disk drives, virus infected files sent to contacts, stored on shared access points and the like. The virus would infect files one-by-one until it was detected and removed by an updated antivirus product or perhaps brought under suspicion due to a peculiar message or destructive payload.

Today’s use of mass-mailing capabilities is the effect of a more inter-connected digital universe and virus writers discovering new ways to propagate malware further and faster, utilizing the users’ own bandwidth. During the 2001 to 2003 time period 100% of outbreaks had Internet worm-like characteristics.
A further scrutiny of this data shows that outbreaks caused by script and macro viruses have lost their effectiveness, dropping lower in the charts at the onset of 2002 and virtually disappearing by 2003. Figure 2, below, is taken from actual statistics recorded by the Trend Micro World Malware Tracking Center, which is part of TrendLabs, Trend Micro’s global network of research facilities.
A similar snapshot from Virus Bulletin Magazine data matches the percentage growth of the different basic types of malware In-the-Wild (ItW) to the monitored corporate outbreaks experienced in the three-year period. (Figure 3)

Another changing trend is in the use of Internet relay chat (IRC), which re-emerges as a vector of malware distribution in 2002, and remains a potent malware distribution mechanism in 2003. One interesting case involved a large corporate-wide infestation by a well-known backdoor Trojan which at first baffled security administrators as it did not have any worm capabilities; it was subsequently discovered that several employees had been connecting to a rogue chat server via the company network.

Virus writers have demonstrated a growing tendency to exploit system vulnerabilities to propagate their malicious code. These include web publishing services like Microsoft Internet Information Service (IIS) and Apache, dabbling in proof-of-concept malware on Microsoft SQL Server, and, as previously mentioned, various exploits causing auto-execution of email attachments. Although the use of mass-mailing features appears to be on the decline due to better attachment filtering, it is still the most effective distribution method when coupled with a little social engineering. Mapped and system shared drives are now becoming a propagation standard. In the past, this was thought to be an easily solved issue—probably caused by lapses in proper configuration or security with a notable Share Level Password vulnerability affecting Windows 9x-based installations. The term “blended threat” has been
coined to describe these types of malware that combine several distribution methods to attack different areas of the network. (see figure 4 below)

When deciding upon protection strategies based on the chart above, administrators should be aware of the unique characteristics that malware adopts to ensure its survival once it has penetrated a corporate environment.
To summarize, the Trend Micro recap of 2003 includes the following observations:

1. As seen in figure 1, coupled with figure 5, most worms use email and some form of social engineering to entice users to click and execute attachments.
2. Self-compression and encryption, coupled with anti-debugging code is a growing concern as it adds another layer of complexity, thereby affecting the speed with which the behavior of the malware can be analyzed. (See figure 5)
3. Vulnerabilities and bugs in commonly used software are being exploited by virus writers and hackers and are proving to be a weak spot in protection strategies.
4. There was a noticeable increase in malware employing Denial-of-Service attacks this year. These were last seen as a major threat in 2000; the main difference between the two occurrences is a shift from Unix-based malware to implementation on the Windows platform.
5. Depending on what elevated user privileges a compromised system provides, backdoors to the system could allow hackers to return and do more damage. Short of providing links to external solutions or recommending the blocking of specific ports or services, there is little an antivirus or security vendor can do unless software developers release fix patches for the affected software.
6. Using self-installing malware to pull down update components from hacker compromised Internet locations has also become an emerging technique. A simple link, combined with ActiveX code, can pass through antivirus and filtering software only to be clicked on once again by the unsuspecting user.
7. There is an increase in self-checking malware that inserts code into the computer enabling it to recreate itself each time the computer is rebooted. It can also disable and unload antivirus, personal firewall and anti-Trojan horse software running in system memory.
8. There is a trend towards avoiding attachment filtering at the email gateway by packaging malware in archives. It would only need a little crafty social engineering to have users extract the worm and help propagate it.
9. Virus writers are now packaging their creations with their own Simple Mail Transfer Protocol (SMTP) servers, thus effectively eliminating the dependency on the Messaging Application Program Interface (MAPI) used by Microsoft's email solutions.
10. It seems that virus writers, too, learn from their mistakes. As illustrated in figure 5 below, they are going back to pure virus basics by doing away with destructive payloads.
So, the bottom line - what's next? Based on its experience of recent computer virus activity, Trend Micro makes the following predictions and observations regarding 2004:

1. The use of blended threats to attack networks will remain the standard.

2. Current and future malware will continue to attempt to disable antivirus, personal firewall and anti-Trojan horse monitoring programs.

3. Web-filtering software or, at least, Internet surfing policies, must be put into effect in corporate environments to prevent inadvertent redirection to malware related Web sites.

4. Email attachment filtering will continue to provide add-on protection. However, gateway scanning antivirus software is more efficient at weeding out infected files passing through corporate networks as well as recognizing different types of archive and file formats.

5. Common public and un-moderated messaging channels such as IRC and P2P will be used from time to time due to the need for faster communication as the email glut continues to hamper day-to-day operations.

6. Several reports published in 2002 estimated that by 2007 25% of all email content would be some form of commercial spam. However, the reality, as published by Nucleus Research, AmikaNow!, IDC, and the New York Times, shows that as at October 2003, the influx of spam has reached 49%, and is expected to continue growing at about 7% every year.

7. System administrators have to be careful in evaluating and considering the software needs of their corporate networks. They should ensure that the software vendor can commit to timely fixes for vulnerabilities and consistent and reliable delivery of services.

8. As enterprises continue to grow, the use of centrally managed services becomes more important. Several vendors are now offering content management solution packages. However, when evaluating these packages, care should be taken to assess their overall efficiency and ability to provide collaborative data.

9. With network viruses becoming ever more prevalent, administrators will need to look at management tools that will allow them to block off different parts of their networks. For example, downloading outbreak prevention policies to quickly isolate vulnerable or infected areas of networks to prevent further spread of infection until a pattern file is released.
The costs associated with network restoration, post virus outbreak, will continue to be an issue. Companies can limit the time and resources needed to restore their networks using device-specific, attack-specific damage clean-up templates.

For more information please visit: www.trendmicro.com