OPINION

THE MALWARE BATTLE: REFLECTIONS AND FORECASTS

Jaime Lyndon 'Jamz' A. Yaneza
Trend Micro, Philippines

Another year has come to its end and the malware battle still rages on. It seems to be a never-ending uphill struggle to secure digital information.

By now most enterprises will at least have some form of sentinel guarding their interests, but is it enough? Even as content management solutions that include improved anti-virus, firewall, or other security innovations are developed, the malware landscape continues to evolve. With corporate spending budgets the focus of attention, the question is: how do system administrators forecast their defensive position and provide data to upper management?

Data is usually subjective in terms of the geographic location and period of time over which the information is gathered. Statistical data for a given period will not indicate the development direction that virus writers are taking. Forecasts or predictions should also be based on the outbreaks seen worldwide, along with analysis of the specific details of each outbreak.

Looking at the raw data collected by *Trend Micro* for the busiest months in a three-year period from 2001 to 2003, it can be seen that the number and type of outbreaks observed from 2001 through to 2003 are relatively similar.

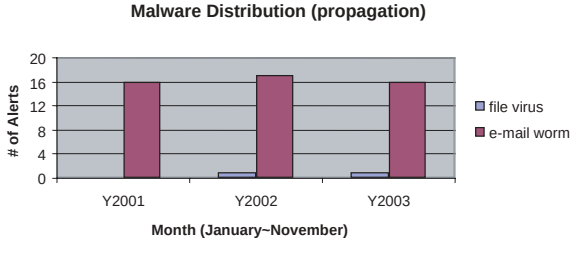

Figure 1. Source: http://wtc.trendmicro.com/wtc/.

Mass-mailing worms are here to stay as the current malware of choice. The standard use of mass-mailing capabilities is the effect of a more inter-connected digital world as well as virus writers having discovered a way to propagate their malicious creations further and faster by wholly depending upon users' bandwidth.

Further scrutiny of the data shows that outbreaks caused by script and macro viruses dropped lower into the charts at the onset of 2002 and had virtually disappeared by 2003. A similar snapshot of data from the *Virus Bulletin* virus prevalence tables over the same time period shows the

percentage of the different basic types of malware in the Wild (ItW).

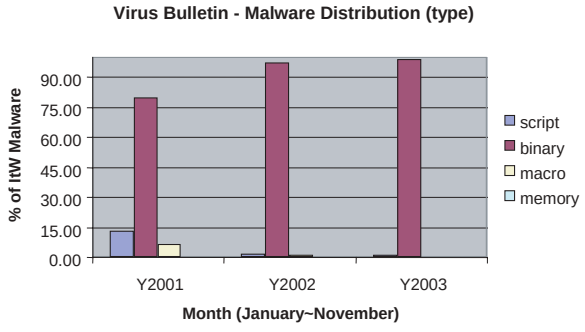

Figure 2. Source: http://www.virusbtn.com/prevalence/.

Observations from *Trend Micro*'s month-to-month comparison of malware-type distribution for the year 2003 show that, on average, scripts, binary executables, and macro viruses account for 16%, 70%, and 14% of malware respectively. It appears that infection growth levels of the basic malware types have stayed more or less the same during 2003. Over approximately the same month-to-month period, the *Virus Bulletin* prevalence data shows a more pronounced differentiation, but more or less matches the rise and fall pattern.

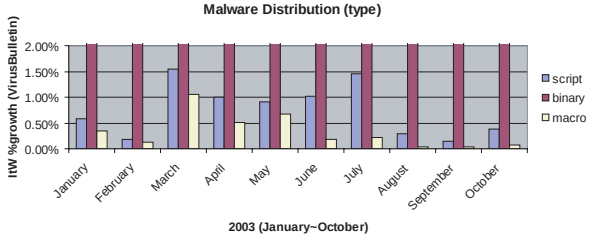

Figure 3. Malware type distribution in 2003.

More information can be gleaned by sifting through the malware types of script, binary, and macro data separately. It is notable that batch file and mIRC script statistics almost match one-for-one owing to malware that attempted to stay resident on the system by cross-dropping its installations. The number and distribution of macro viruses in the Wild reflects approximately the everyday usage of the relevant platforms (see Figure 4).

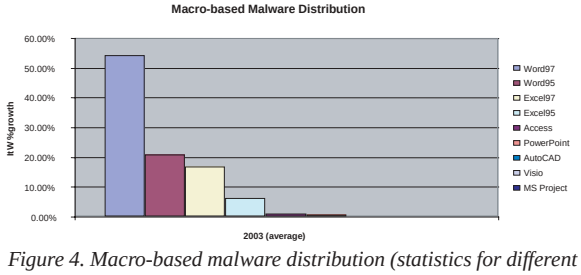

Figure 4. Macro-based malware distribution (statistics for different software versions have been merged, except for MS Word and Excel).

Although only showing up as blips on the radar for now, reports of adware/spyware and Macintosh malware are evident in 2003 (see Figure 5). For those still foolish enough to believe that malware does not exist on *Linux* it is interesting to see the script values added to binary numbers. Trojan-based malware programs that optionally install backdoors are seen in the greatest numbers.

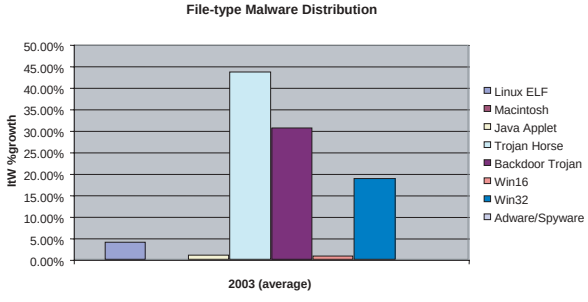

Figure 5. File-type malware distribution.

The use of Internet relay chat (IRC) emerged as a vector of malware distribution in 2002 and a blip or two in the 2003 radar. An interesting individual case we encountered was a large corporate-wide infestation of a backdoor Trojan installation which baffled administrators as it did not have any worming capabilities – only later did they discover that several employees had been connecting to a rogue chat server installation which was accessible externally.

Exploits that abuse system vulnerabilities such as those on *Microsoft Internet Information Service* (IIS) and Apache, proof-of-concept malware on *Microsoft SQL Server*, and various exploits causing auto-execution of email attachments appear to be rising interests as well.

Although the use of mass-mailing features shows a decline due to better attachment filtering practices, it is still the most effective distribution method when coupled with a little social engineering. Mapped and system shared drives are even now becoming a propagation standard – probably

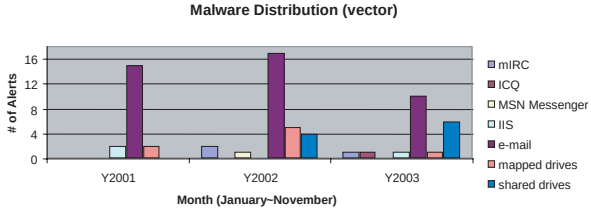

Figure 6. Malware distribution vectors.

due to 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 refer to these types of malware that combine several attack vectors (see Figure 6). When forecasting protection strategies based on the chart above, administrators should be well aware of the unique characteristics that malware programs adapt to ensure their own survival in a penetrated corporate environment.

RECAP

As a summary, our recap of 2003 includes the following observations:

1. Mass-mailing worms are using email with 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, making it harder to analyse a piece of malware.
3. Vulnerabilities and bugs in commonly used software are proving to be the Achilles' heel of protection strategies and as such are becoming favourite tools in hackers' and virus writers' arsenals.
4. There was a noticeable increase in malware employing Denial of Service attacks in 2003, a resurge from 2000.
5. Depending on what elevated user privileges a compromised system provides, backdoors may allow hackers to cause prolonged damage.
6. The use of self-installing malware URLs to pull down updates and components from hacker-compromised Internet locations has proven to be an emerging technique. A simple link combined with ActiveX code can pass through anti-virus and filtering software to be clicked on by the unsuspecting user.
7. Another common characteristic of current malware is the use of self-checks to ensure parasitic presence as well as to disable and unload the running anti-virus, personal firewall, and anti-Trojan monitoring software running in system memory.
8. There is a trend towards packaging malware in archives in order to avoid attachment filtering at the email gateway.
9. Virus writers are now packaging their creations with their own SMTP engines, thus effectively eliminating the dependency on the MAPI used by *Microsoft*'s email solutions.
10. It seems virus writers also learn from their mistakes and are going back to pure virus basics – for example by doing away with destructive payloads.

WHAT'S NEXT?

The bottom line is: what's next? Based on all the facts observed and those presented here, it would be safe to make the following predictions for 2004:

- The use of 'blended threats' to attack networks will remain the present standard.
- Current and future malware will continue to attempt to disable anti-virus, personal firewall, or even anti-Trojan monitoring programs.
- Web-filtering software, or at least Internet surfing policies must be put into effect in corporate environments to prevent inadvertent redirection to malware-related websites.
- Email attachment filtering will continue to provide add-on protection. However, gateway scanning anti-virus software is more efficient at weeding out infected files passing through corporate networks as well as recognizing different types of archive and file format.
- Common public and unmoderated messaging channels such as IRC and P2P will be used increasingly given the increasing need for faster communication as the email glut continues to pound day-to-day operations. Proper port configuration needs to be considered.
- Anti-spam legislation is a hot topic and enterprises should be prepared.
- As enterprises grow the use of centrally managed services becomes more important. Several vendors offer content management solution packages and these may deserve more than a cursory look. Administrators must be careful to note their overall efficiency and ability to provide collaborative data.
- Management tools with the ability to isolate malware-infested segments of a corporate network and the ability to retreat to a safe ground of core functionality will be important capabilities to look for.
- Continuous user education is a must. Corporations will also need to look to provide policy enforcement to ensure secure environments.
- System administrators must be careful in evaluating and considering the general software needs of their corporate network. Criteria should include software whose developers can at least commit to fixes to vulnerabilities on time as well as services that can be delivered reliably and consistently.