Understanding and Detecting Malware Threats Based on File Sizes

Fortinet Global Threat Research Team

White Paper

High Performance Multi-Threat Security Solutions

Introduction

Nearly 25-years after the first computer virus—the Elk Cloner virus—appeared, malware continues to evolve and pose significant risks to organizations today. Before the Internet, malware was typically transmitted by floppy disks, limiting a malware threat's propagation rate. In 2006 and the foreseeable future, every networked computer with an email client, web browser or any other portal to the Internet is a prime target, allowing malware threats to spread more rapidly than ever before.

While many people use the term virus and malware interchangeably, there is an important difference. Malware is a broader term that includes viruses, but also includes any type of threat that is file-based in nature. Newer threat types such as: spyware, adware, Trojan horses and worms all fall under the category of malware.

Malware is typically found within files that are less than one megabyte (MB) in size. According to Fortinet research, 97% of malware discovered since the beginning of 2006 is below one MB in size. The small size of the malware file allows malicious content to be downloaded and executed quickly, creating an unnoticeable infection.

File Sizes and Malware Detection by Fortinet Products

File sizes being transferred on the network are directly related to observed network performance when Fortinet products are in place. In order to prevent malware code from being passed into the secured area of the network, a file must be cached by the Fortinet product then scanned in its entirety to ensure that the complete file is not infected with malware using polymorphic techniques to avoid detection. In this scenario, users typically notice that the file arrives very quickly at the destination after an observed delay. As the file size grows, the delay caused by the caching operation can be interpreted as performance degradation.

Fortinet products contain a *maximum file size scanned* parameter, which allows the administrator to customize how large files are processed. The 10 MB default value has been determined to offer the best possible balance between protection and network performance. Organizations prioritizing network performance over protection can reduce the *maximum file size scanned* parameter to decrease latency caused by file caching. If the default parameter value is lowered, however, there is an increased risk of malware passing through the Fortinet product undetected.

Malware Types, Sizes and Associated Risk Level

Several types of malware have evolved since the age of floppy disks' boot and file-infector virus types. Macro viruses became commonplace after the release of WM/Concept.A, which was the first concept macro virus malware type. The new varieties and rate of infection from macro viruses quickly subsided after the enhancement of security features within the applications the viruses were targeted (i.e. MS-Word, MS-Excel, etc.). As antivirus technology improved over time, Trojans, spyware and worm malware types all became popular following the validation that they could circumvent the protection technology available at the time.

Of all malware types, mass-mailer types generally have the highest propagation rates in the wild. This type of malware spreads by sending hundreds of emails from each infected computer. Once an infected email is opened, it harvests email addresses stored on the newly infected host in order to propagate. The amount of traffic generated on a network by mass-mailer malware types can be exponential.

> Example: Over a 10 month period ending October 2006, only 3.3% of newly discovered malware samples were identified as mass-mailers (Figure 1). Yet, mass-mailers represent the highest percentage of activity detected during the same period.

The Phishing threat type is one of the newer threat types. Phishing combines an email message and web sites to deceive unsuspecting users. First, emails are spammed out with the intention of enticing the recipients to click a link in the email that leads back to a website that appears to be a legitimate business. Then the web site gathers personal information from the unsuspecting user, more often than not bank account information. Phishing threats always first manifest themselves within a small email message due to the shear volume of messages generated by the spam generator.

Trojans and spyware are purpose-built malicious applications that steal information from a host or allow the attacker to gain control of a host. These two malware types comprise more than 69.3% of the observed 2006 malware activity. Spyware, in particular a subtype called Adware, sends user information back to an ad server for delivery of targeted advertisements. The file sizes for spyware payloads also remain small, with 95% of spyware installers totaling less than one MB in size.

Worm malware types are categorized on how they propagate through the Internet or network. The most common worm subtype is the email-worm, which is also known as mass-mailers. The next are Instant Messaging (IM), Peer-to-Peer (P2P) and Network/Shared Folders worms. IM Worms send instant messages containing a malware payload to the compromised users' contact list. When an unsuspecting user downloads and executes the file either directly or from a web site link, the worm penetrates the user's local machine and repeats the cycle over and over again.

P2P and Network File Share Worms are almost identical. The only difference between the two malware subtypes is in their method of replication. P2P Worms copy themselves to the shareable download folder of P2P programs. Network File Share Worms copy themselves to a shared network folder. Some types of Network File Share Worms scan the local network for a fully writable shared network folder. Both of these worm subtypes are now uncommon, comprising less than 1% of activity during the month of October 2006.

Standard viruses generally infect normal files by attaching or inserting part of their malicious code into a benign file. The detection of virus activity has dropped considerably in 2006 compared to the year 2000 and before. During the month of October 2006, Fortinet attributes virus activity to 1.72% of all detected malware activity.

The table below shows the percentage of detected malware activity by type for the past 10 months, ending Oct 2006. In addition, detection rate statistics are cross-referenced with Oct 2006 alone to illustrate trends in the activity level of each malware type.

Malware Type	2006's Distribution of Malware (by Type)	October 2006's Detection Rate
Exploits	1.5 %	7.36 %
Instant Messaging Worm	0.2 %	0.01 %
Macro Virus	0.3 %	0.02 %
Mass-Mailer	3.3 %	40.33 %
Mobile Virus	0.1%	0.19 %
Phishing Emails	0.2 %	16.37 %
Scripts	1.0 %	2.25 %
Spyware	19.9 %	11.65 %
Trojan	49.4 %	19.50 %
Virus	19.7 %	1.72 %
Worm	4.5 %	0.61 %

Table 1: Malware Distribution and Detection Rates

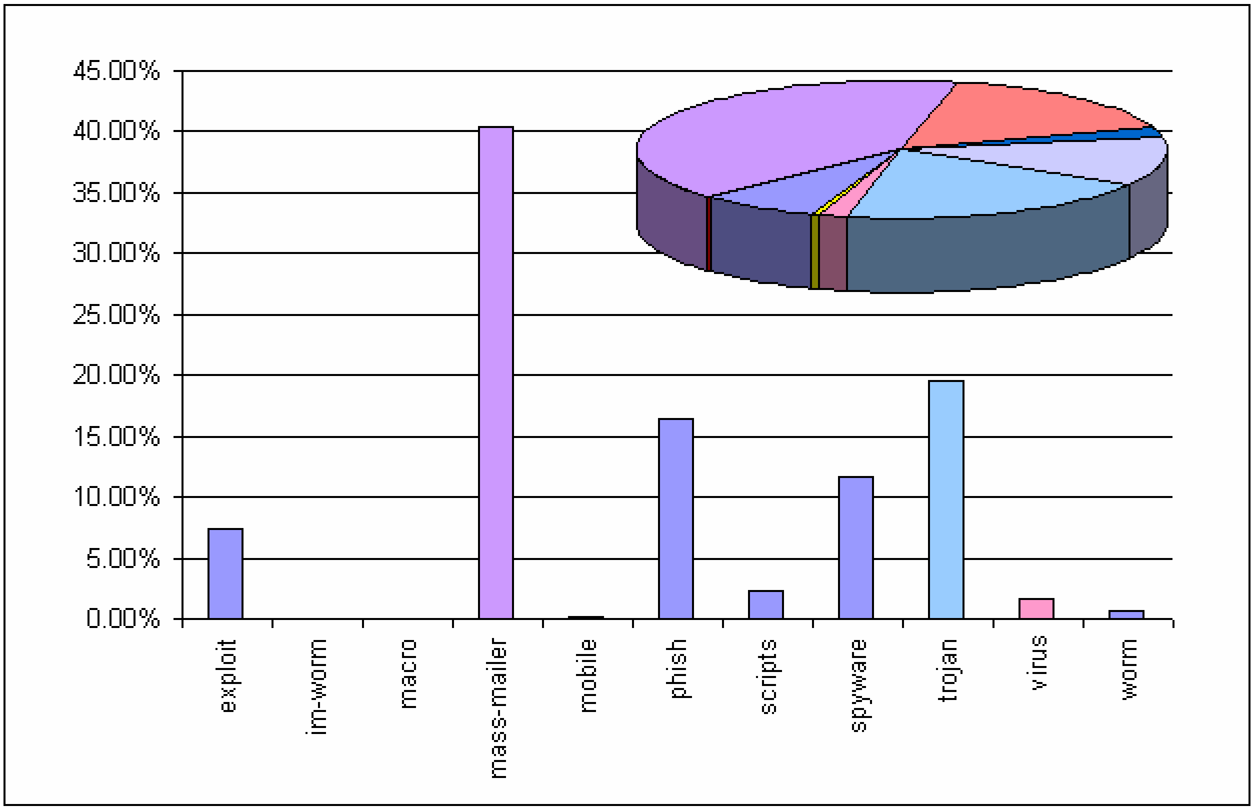


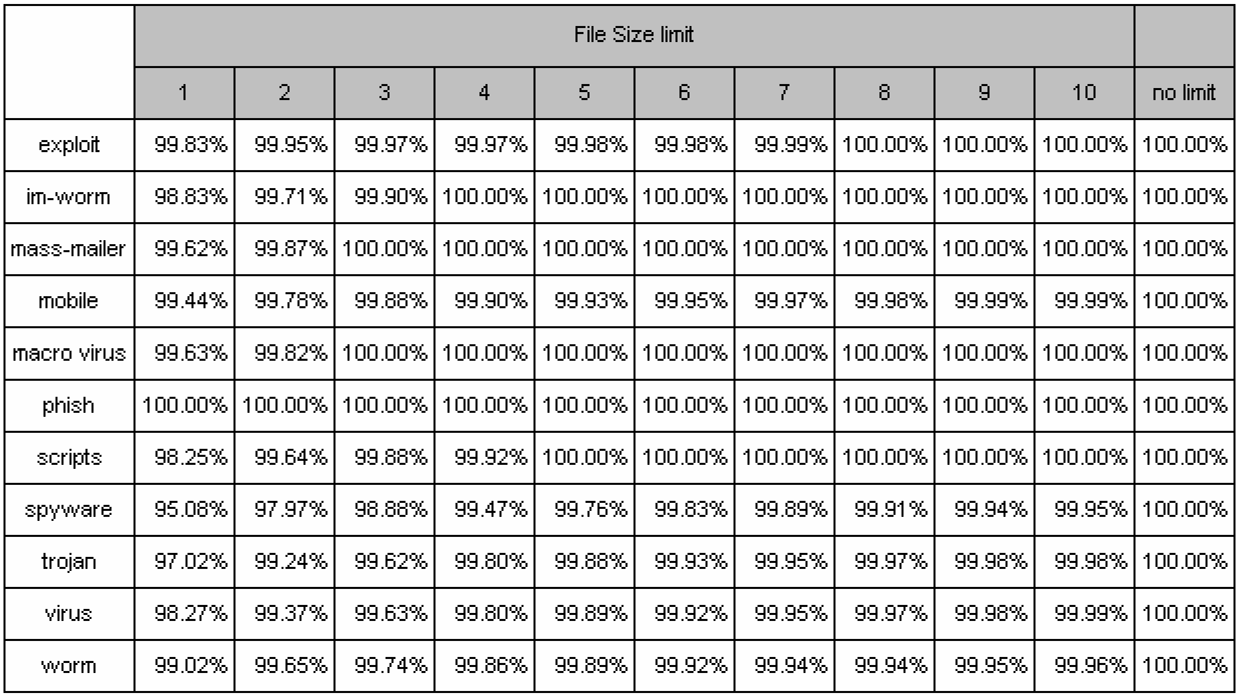
Figure 1: October 2006’s Detection Rate

Mitigating Risks from Malware

To achieve 100% detection of known malware, a broad range of file sizes should be scanned. Ideally, all files should be checked before they reach their destination. Detected malware files are stripped off or blocked, preventing collateral damage that could occur if the malware were delivered to the target system. In modern business networks, organizations commonly use applications with proprietary file formats that transfer large amounts of data between client and server. It is also common practice to store large documents on network file shares for common access. Scanning large files of this type repeatedly insures that malware replication does not occur, but can also cause noticeable delays for users who perform this type of repeated operation.

Adjusting the *max file size* parameter in Fortinet products can decrease the delay caused by caching. Increased risk of a malware infection, however, is involved in lowering the default value. Once a malware infection occurs on a network, a network-wide outbreak may occur depending on the malware type, setting off significant network issues and causing financial loss.

The table below shows the percentage of the effectiveness of detection by file size limit scanned for each malware type for the last 10 months.



	File Size limit										
	1	2	3	4	5	6	7	8	9	10	no limit
exploit	99.83%	99.95%	99.97%	99.97%	99.98%	99.98%	99.99%	100.00%	100.00%	100.00%	100.00%
im-worm	98.83%	99.71%	99.90%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
mass-mailer	99.62%	99.87%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
mobile	99.44%	99.78%	99.88%	99.90%	99.93%	99.95%	99.97%	99.98%	99.99%	99.99%	100.00%
macro virus	99.63%	99.82%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
phish	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
scripts	98.25%	99.64%	99.88%	99.92%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
spyware	95.08%	97.97%	98.88%	99.47%	99.76%	99.83%	99.89%	99.91%	99.94%	99.95%	100.00%
trojan	97.02%	99.24%	99.62%	99.80%	99.88%	99.93%	99.95%	99.97%	99.98%	99.98%	100.00%
virus	98.27%	99.37%	99.63%	99.80%	99.89%	99.92%	99.95%	99.97%	99.98%	99.99%	100.00%
worm	99.02%	99.65%	99.74%	99.86%	99.89%	99.92%	99.94%	99.94%	99.95%	99.96%	100.00%

Table 2: Percentage of detection per Malware Type
Note: Malware rated on the above table are only the discovered and known ones.

As the file size limit is reduced, the rate of detection decreases too. Mass-mailers are best detected for all sizes. Phishing attempts, exploits, mobile viruses, macro viruses and instant messaging worms are detected with excellent accuracy with anything greater than a 2 MB max file size to scan limit. Spyware and Trojans have excellent detection rates anywhere higher than a 1 MB max files size to scan setting.

To determine whether to modify the default max file size limit where files should pass uninspected, two factors should be considered:

1. The risk involved for the type of malware threat that may go undetected as a result of the change
2. The average file size transferred and transfer rate during normal network operation

Setting a lower than default value for the maximum file size to scan will result in higher-risk of infection and may not be acceptable for certain types of organizations. In some organizations with multiple layers of network protection or end-point security in place, setting a lower *max file size to scan* value may be advisable to increase the network throughput.

There are additional tweaks that may enhance the protection from malware while not altering the *max file size to scan* parameter. Using file extension blocking on executable files (.exe, .com, .dll, .scr & .pif) generally eliminates most types of malware threats.

Summary

Malware continues to evolve, but is still typically observed in files less than one MB in size. By adjusting the *max file size to scan* limit and enabling file extension blocking, improved network performance can be achieved with minimal additional risk. In an ideal scenario, all files passing through the network should be scanned to attain the best possible protection. Users of Fortinet antivirus products are advised to carefully weigh the benefits and risks of modifying default settings before making changes to their configuration

About the Authors

Bryan Lu is a technical account manager for Fortinet's Antivirus Premier Service and an antivirus researcher for the Fortinet Threat Research Team. In these roles, Bryan assures customers a three-hour response time for Antivirus Premier Support, analyzes malware trends, and provides reports to WildList.org and VB100. He has been instrumental in the creation and management of Fortinet's World Virus Map, a live representation of current threats around the world, and the FortiGuard Center, which contains up-to-the-minute information on the latest threats and updates. Prior to Fortinet, Bryan spent six years at Trend Micro, Inc. He is a Microsoft Certified Database Administrator and Sun Certified Java Programmer. He received his computer science degree from De La Salle University in Manila, Philippines.

Steve Fossen is a senior manager for the Fortinet Global Threat Research Team, responsible for the antivirus and intrusion prevention (IPS) research and development teams. Drawing on his experience as a malware and vulnerability researcher and analyst for both antivirus and IPS, he has designed and developed scanning modules, as well as sophisticated automation tools and a highly optimized pre-processor. Fortinet has applied for patents on advanced detection techniques of which Steve is a co-inventor.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam—providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPSec, SSL, IDS, client antivirus detection, cleaning and antispyware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com