Encyclopedia of Multimedia Technology and Networking

Second Edition

Margherita Pagani
Bocconi University, Italy

Volume I
A–Ev

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Director of Editorial Content: Kristin Klinger
Senior Managing Editor: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of multimedia technology and networking / Margherita Pagani, editor. -- 2nd ed.
p. cm.
Includes bibliographical references and index.
Summary: "This publication offers a research compendium of human knowledge related to the emerging multimedia digital metamarket"--Provided by publisher.
ISBN 978-1-60566-014-1 (hardcover) -- ISBN 978-1-60566-015-8 (ebook)
1. Multimedia communications--Encyclopedias. I. Pagani, Margherita, 1971-
TK5105.15.E46 2009
621.38203--dc22
2008030766

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Developments and Defenses of Malicious Code

Xin Luo
University of New Mexico, USA

Merrill Warkentin
Mississippi State University, USA

INTRODUCTION

The continuous evolution of information security threats, coupled with increasing sophistication of malicious codes and the greater flexibility in working practices demanded by organizations and individual users, have imposed further burdens on the development of effective anti-malware defenses. Despite the fact that the IT community is endeavoring to prevent and thwart security threats, the Internet is perceived as the medium that transmits not only legitimate information but also malicious codes. In this cat-and-mouse predicament, it is widely acknowledged that, as new security countermeasures arise, malware authors are always able to learn how to manipulate the loopholes or vulnerabilities of these technologies, and can thereby weaponize new streams of malicious attacks.

From e-mail attachments embedded with Trojan horses to recent advanced malware attacks such as Gozi programs, which compromise and transmit users' highly sensitive information in a clandestine way, malware continues to evolve to be increasingly surreptitious and deadly. This trend of malware development seems foreseeable, yet making it increasingly arduous for organizations and/or individuals to detect and remove malicious codes and to defend against profit-driven perpetrators in the cyber world. This article introduces new malware threats such as ransomware, spyware, and rootkits, discusses the trends of malware development, and provides analysis for malware defenses.

Keywords: Ransomware, Spyware, Anti-Virus, Malware, Malicious Code,

BACKGROUND

Various forms of malware have been a part of the computing environment since before the implementation of the public Internet. However, the Internet's ubiquity has ushered in an explosion in the severity and complexity of various forms of malicious applications delivered via increasingly ingenious methods. The original malware attacks were perpetrated via e-mail attachments, but new vulnerabilities have been identified and exploited by a variety of perpetrators who range from merely curious hackers to sophisticated organized criminals and identify thieves. In an earlier manuscript (Luo & Warkentin, 2005), the authors established the basic taxonomy of malware that included various types of computer viruses (boot sector viruses, macro viruses, etc.), worms, and Trojan horses. Since that time, numerous new forms of malicious code have been found "in the wild."

MALWARE THREAT STATISTICS: A REVISIT

The Web is perceived to be the biggest carrier transmitting threats to security and productivity in organizations, because Web sites can harbor not only undesirable content but also malicious codes. The dilemma for organizations is that the Web is an indispensable strategic tool for all the constituents to collaboratively communicate, though it is also an open route for cybercriminals to seek possible victims. Unlike the past in which most malicious code writers were motivated by curiosity or bragging rights, today's IT world is experiencing the transition from traditional forms of viruses and worms to new and more complicated ones perpetrated by active criminals intent on financial gain. This trend is due to the capitalization of the malware industry where most malicious code writers tend to exploit system vulnerabilities to capture such high profile information as passwords, credentials for banking sites, and other personal information for identify theft and financial

fraud. The trend of virus attacks is that new blended attacks that combine worms, spyware, and rootkits are the major infective force in the cyber world and will likely become more frequent in years ahead. In general, such malware are spreading via increasingly sophisticated methods and are capable of damaging more effectively. Such blended malware's invention is driven by their writers' pursuit for financial fraud.

According to Vass (2007), from a hacker's perspective, the motivation for employing malware attacks has moved from "let me find a vulnerability" to "let me find an application vulnerability and automate it and put it into a bot, load up pages and reinfect the client, which I can then use to populate my bot network." Furthermore, malware writers have paid increased attention to applications and have aimed at the application layer to seek and exploit system vulnerabilities. As such, IT anti-virus teams have encountered extremely difficult predicaments regarding how to proactively prevent the malware disaster and eventually eliminate any malware infection or breach. Table 1 lists the systems and applications most often targeted for attack, and Table 2 entails the top 10 malware attacks by December of 2006.

Computer systems are now less frequently infected via passive-user downloads, because malware is increasingly embedded on Web sites to which users are lured by spammed e-mail invitations. However, e-mail attachments are still a common method of malware distribution as well. E-mail is seen as one of the biggest threats to IT community because it can easily carry malicious codes in its attachment and masquerade the attachment to entice the user's attention. Table 3 shows the top 10 malware hosted on Web sites which can easily disseminate malware infection to unwary cyber visitors, and Table 4 lists top 10 e-mail malware threats in 2007.

In addition, most malware-detection software solely recognizes malware infection by searching for characteristic sequences of byte strings which act as the malware's signature. This out-of-date detection is based on the assumption that these signatures do not change over time. However, malware writers have already

Table 1. Systems and applications targeted (Adapted from Vaas, 2007)

Target: Security Policy and Personnel • Poorly-trained employees vulnerable to phishing scams • Unauthorized devices (USB devices, etc.) • Administrative-level authority for users, who may install unapproved software, and so forth • Employees using unapproved IM and file-sharing at work (tunnel through firewalls and introduce Malware, e.g. Skype)
Target: Network Devices • Common configuration weaknesses • VOIP servers and phones
Target: Operating Systems and Core Applications • Web Browsers (especially Internet Explorer) • DLLs, Windows Libraries • Macro Infections (MS Word and Excel) • Vulnerabilities in MS Outlook and other Office apps • Windows Service Weaknesses • Mac OS X and Leopard OS • Unix Configuration Weaknesses
Target: Cross-Platform Applications • HTML and Java - Web Applications • Microsoft ActiveX controls and Javascript Activity • Database Software • P2P File-sharing Applications (Kazaa, etc.) • Instant Messaging (tunnel through firewall) • Media Players • DNS Servers (URL redirection, etc.) • Backup Software • Servers for directory management • Other enterprise servers

Table 2. Top 10 malware threats by December of 2006 (Adapted from http://www.sophos.com/pressoffice/news/articles/2007/01/toptendec.html)

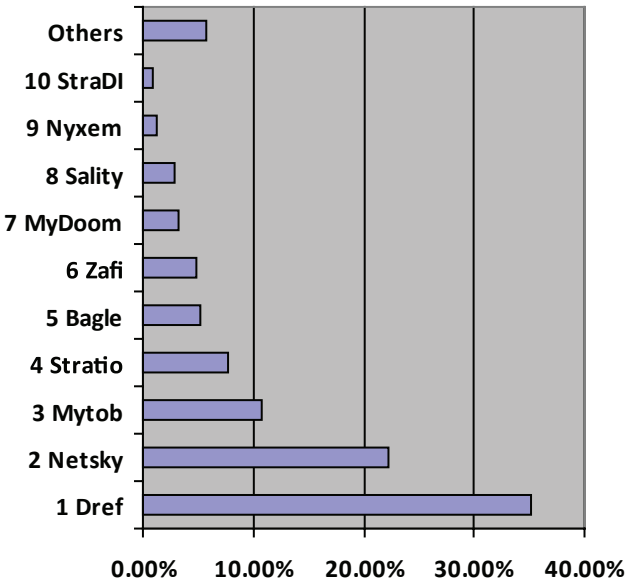
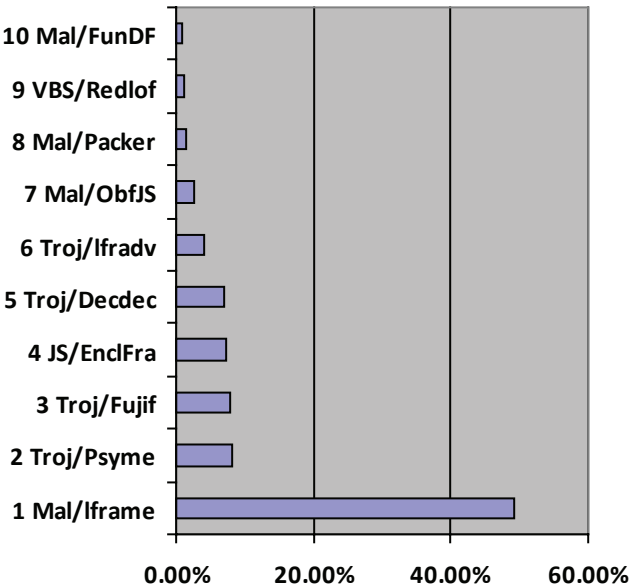
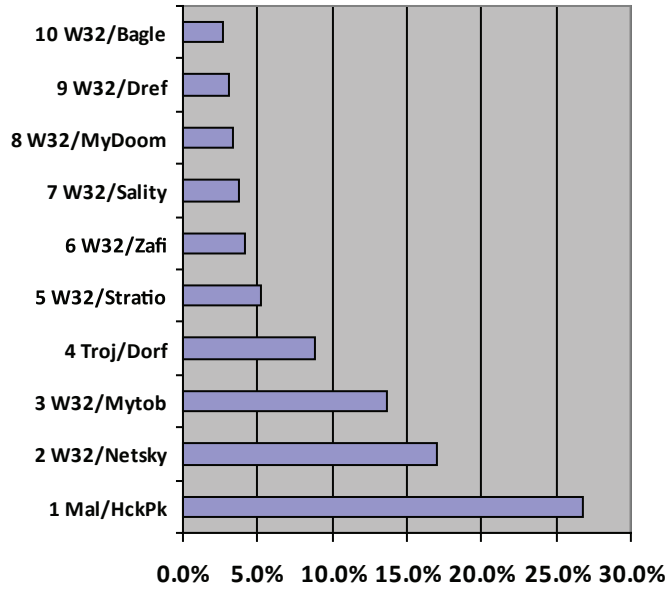


Table 3. Top 10 malware hosted in Web sites in 2007 Adapted from Sophos Security Threat Report, July, 2007, available from Sophos at www.sophos.com (registration required)



adapted to this approach, and thereby have invented polymorphic and metamorphic malware, a self-mutating malicious code that changes itself and, consequently, changes its fingerprint automatically on every execution to avoid detection (Bruschi, Martignoni, & Monga, 2007; Willems, Holz, & Freiling, 2007). This type of advanced code obfuscation has demonstrated efficacy against traditional anti-virus software. Developers of security software suites (anti-virus software, etc.) must adapt to these developments and identify ever-increasingly sophisticated tools for malware detection and removal. In the next section, newer forms of malware are presented and discussed.

Table 4. Top 10 e-mail malware threats in 2007 Adapted from Sophos Security Threat Report, July, 2007, available from Sophos at www.sophos.com (registration required)



EMERGING MALWARE THREATS

New forms of malware are found weekly by the CERT Coordination Center, by security software vendors, and by various other security experts. Vulnerability alerts are frequently published by researchers probing new operating systems and applications in an attempt to get software vendors to "plug the holes" in their code. Certainly, such "white hat hackers" are joined by the criminal and malicious researchers in identifying such vulnerabilities, though the latter group does not publish their findings!

Purveyors of spam have found that networks of "bots," infected PCs organized as a loose network known as "botnets," can be effective tools for distributing their spam e-mails because the anti-spam tools cannot possibly target all the millions of legit users and domains that become the source of such spam attacks. Other botnets have been perpetrated to unleash distributed deliberate denial of service (DDos) attacks against specific targets (such as Microsoft, newspapers, government Web sites, eBay, and Yahoo). Such botware code may do no damage to the infected PC other than usurping bandwidth.

Many other categories of emerging malware can be found, but this article will focus on polymorphic viruses, ransomware, spyware, and rootkits in the following sections.

Ransomware Attacks

Ransomware is defined as a piece of pernicious software that exploits a user's computer vulnerabilities to sneak into the victim's computer and encrypt all files until the victim agrees to pay a ransom to receive these files in their original condition (Luo & Liao, 2007). In a ransomware attack, the perpetrators utilize sophisticated software to enable their extortion scheme. Imposing serious threats to information assets protection, ransomware invariably tries to seize control of the victim's files or computer until the victim agrees to the attacker's demands.

In a typical ransomware attack, the attacker reaches into a compromised computer by seeking the exposed system vulnerabilities. If this system was victimized earlier by a worm or Trojan, the attacker can easily enter the weakly-configured system. He then searches for various types of important files with extension such as txt, doc, rft, ppt, chm, cpp, asm, db, db1, dbx, cgi, dsw, gzip, zip, jpg, key, mdb, pgp, and pdf. Knowing these files are of possible crucial importance to the victims, he then encrypts these files, making them impossible for the victim or owner to access them. Later, the attacker sends the victim a ransom e-mail or pop-up window demanding payment for the encryption key that unlocks the frozen files. These demands usually involve transferring funds to designated online currency

accounts such as eGold or Webmoney or by purchasing a certain amount of pharmaceutical drugs from the attacker's designated online pharmacy stores.

Once the attacker locates these files, there are several processing strategies that he might implement. First, he can compress all the located files into a password-protected zip package, and then he removes the entire group of original files. Secondly, he can individually encrypt each located file, and then remove the original files. For example, if the original file is "FinancialStatement.doc", ransomware will create a file such as "Encrypted_FinancialStatement.doc" in order to label the original file. Thirdly, the attacker might create a hidden folder and move all the located files to this folder, producing a pseudophase to deceive the victim. The third strategy, of course, carries the slightest damage and is comparatively feasible for the victim to retrieve all the "lost" files.

Furthermore, when ransomware attacks successfully take control of an enterprise's data, the attacker encrypts the data using sophisticated algorithms such as up to 660-bit encryption key. The decryption password is only released if a ransom is paid to the attackers. The attacker usually notifies the victim by means of a striking message, which carries specific instructions regarding how the victim can act to retrieve the lost files. A text file or a pop-up window message is generally created in the same folder where files are encrypted. The text file or message box clearly indicates that all the important files are already encrypted, and informs the victim of specific money remittance methods.

Spyware Invasion

Stafford and Urbaczewski (2004) refer to spyware as "a ghost in the machine" due to its surreptitious nature compared to viruses and worms. Warkentin, Luo, and Templeton (2005) further expand the description by arguing that "spyware is a client-side software component that monitors the use of client activity and sends the collected data to a remote machine." The launch of vicious spyware mainly stems from the search for valuable information. As such, spyware is designed and implemented to stealthily collect and transmit information such as keystrokes for usernames and passwords, Web surfing habits, e-mail addresses, and other sensitive information. Much spyware is used to target banner ads to specific user profiles, and is known as "adware." Additionally, spyware is able to trigger system resource misuse and bandwidth waste, thereby posing grave security, confidentiality, and compliance risks.

Spyware can be embedded into the install procedures of file-sharing client software (e.g., Kazaa) or other shareware, it may be attached to e-mails as a Trojan, or it may be installed onto a Web surfer's PC via a process known as "drive-by downloading." Its presence often goes undetected, and it may operate in the background for lengthy periods of time, during which time it can capture valuable information and transmit it back to its perpetrators.

The spyware problem is sizable and growing. Table 5 lists the top 10 spyware threats identified Webroots. Although both home and enterprise computers currently face spyware infections, the scenario is magnified in the latter, owing to the wide scale of computer and network implementation and installation. Despite spyware infiltration in record numbers, the overall negative aftermath of spyware infection for enterprises varies from mild to wild—occasional harassment, productivity loss, resource waste, and threat to business information integrity (Luo, 2006). The human factor is a main consideration when security is at issue in this scenario, because the problem confronting business managers is that most spyware infections stem from unwary or novice employees browsing spyware-affiliated Web pages and downloading free software bundled with spyware programs.

Rootkits Penetration

Defined as a set of software tools or programs that can be used by an intruder after gaining access to a computer system, rootkits are designed to allow an intruder to maintain access to the system without the user's awareness or knowledge (Beegle, 2007). It is created to infiltrate operating systems or databases with the vicious intention to escape detection, resist removal, and perform a specific operation. Often masqueraded within other malware, rootkits can reside in the system for a long period of time without being detected. In addition, sometimes only repartitioning or low-level formatting the hard drive and reinstalling a new operating system can eradicate rootkits. While Ring and Cole (2004) argue that rootkit technology is composed of user level and kernel level, Vass (2007) indicates that the weaponization of two new rootkit technologies, namely virtual rootkits and evil hypervisors, will someday contribute

Table 5. Top 10 spyware threats (Information in this table quoted from Techtarget, 2007)

1. CoolWebSearch (CWS)
CoolWebSearch may hijack any of the following: Web searches, home page, and other Internet Explorer settings. Recent variants of CoolWebSearch install using malicious HTML applications or security flaws, such as exploits in the HTML Help format and Microsoft Java virtual machines.

2. Gator (GAIN)
Gator is an adware program that may display banner advertisements based on user Web surfing habits. Gator is usually bundled with numerous free software programs, including the popular file-sharing program Kazaa.

3. 180search Assistant
180search Assistant is an adware program that delivers targeted pop-up advertisements to a user's computer. Whenever a keyword is entered into a search engine or a targeted Web site is visited, 180search Assistant opens a separate browser window displaying an advertiser's Web page that is related to the keyword or site.

4. ISTbar/AUpdate
ISTbar is a toolbar used for searching pornographic Web sites that, when linked to, may display pornographic pop-ups and hijack user homepages and Internet searches.

5. Transponder (vx2)
Transponder is an IE Browser Helper Object that monitors requested Web pages and data entered into online forms, then delivers targeted advertisements.

6. Internet Optimizer
Internet Optimizer hijacks error pages and redirects them to its own controlling server at http://www.internet-optimizer.com.

7. BlazeFind
BlazeFind may hijack any of the following: Web searches, home page, and other Internet Explorer settings. BlazeFind may redirect Web searches through its own search engine and change default home pages to www.blazefind.com. This hijacker may also change other Internet Explorer settings.

8. Hot as Hell
Hot as Hell is a dialer program which dials toll numbers in order to access paid pornographic Web sites. Hot as Hell may disconnect a user's computer from a local Internet provider and reconnect the user to the Internet using an expensive toll or international phone number. It does not spy on the user, but it may accrue significant long distance phone charges. It may run in the background, hiding its presence.

9. Advanced Keylogger
Advanced Keylogger, a keystroke logger, has the ability to monitor keystrokes and take screen shots.

10. TIBS Dialer
TIBS Dialer is a dialer that may hijack a user's modem and dial toll numbers that access paid, pornographic Web sites.

to the stream of money feeding into the "bot economy." Again, this conversion from initial mischief to criminal profiteering mirrors the psychological evolution of the malicious hackers, who now concentrate on the pursuit of financial fraud. Despite the fact that virtual rootkits and evil hypervisors are only seen in proof-of-concept code to date, these new threats will theoretically allow attackers to stay on a machine undetected for a very long time. Table 6 lists the identified rootkits in just one recent month.

CONCLUSION AND FUTURE TRENDS

The dramatic increase in the level of malware sophistication seen in the last few years portends a challenging period ahead for computer users, IT managers, and anti-malware developers. The "cat-and-mouse" game of malware/anti-malware authors will likely accelerate as malware perpetrators become increasingly motivated by financial successes (identity theft, ransoms, etc.) and as IT managers implement increasingly mature approaches to addressing this powerful threat. Concerns

Table 6. Rootkit attacks in October, 2007 (Note: Each rootkit attacked the Windows Operating System) Adapted from: http://www.antirootkit.com/rootkit-list.htm

Name	Date Discovered
Troj/Inject-BU	22-Oct-2007
W32/Alman-D	21-Oct-2007
Troj/Oscor-L	18-Oct-2007
Troj/RKFaja-Gen	17-Oct-2007
W32/Alvabrig.a!inf	16-Oct-2007
W32/Sdbot-DIE	15-Oct-2007
Troj/MDrop-BPX	15-Oct-2007
Worm_Nuwar.ARC	14-Oct-2007
W32/Zhelatin.KC	12-Oct-2007
Troj/PSW-EI	12-Oct-2007
Troj/NtDwnl-B	09-Oct-2007
Troj/NtDwnl-A	08-Oct-2007
W32/Stucco-B	08-Oct-2007
Troj/DllHid-Gen	05-Oct-2007
Troj/Agent-GDN	03-Oct-2007

about various forms of malware, including identity theft schemes supported by so-called "botnets," have become the leading managerial issue for IT managers in many organizations, as well as home users in the Internet age. This trend is likely to continue as malware developers continue to seek more obscure vulnerabilities in an effort to continue their attacks undetected. The financial gains from such attacks have motivated rings of organized criminals from many nations, and losses have been mounting. Newer operating systems offer the promise of increased safety, but the increased complexity of newer applications and operating systems offer increased opportunities for malware distributors to exploit. This scenario is likely to continue unabated. Only with increased education, awareness, and vigilance will organizations have any hope of fighting the tide of malware attacks. Defenses must be evolutionary and dynamic, and no single solution will be 100% effective. Many organizations are implementing a more centralized approach to security management, which utilizes enterprise perimeter controls, backups, and scanning. This centralized IT security governance structure (Warkentin & Johnston, 2008) is more effective against modern "zero-day" (rapidly spreading) attacks against which individual users cannot adequately defend. But perhaps with increased user awareness and better enterprise-level controls, the balance can shift toward a safer future for the Internet.

REFERENCES

Beegle, L. E. (2007). Rootkits and their effects on information security. *Information Systems Security, 16*.

Bruschi, D., Martignoni, L., & Monga, M. (2007). Code normalization for self-mutating malware. *IEEE Security & Privacy, 5*(2), 46–54.

Luo, X. (2006). A holistic approach for managing spyware. *Information Systems Security, 15*(2), 42-48.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security, 16*(4), 195-202.

Luo, X., & Warkentin, M. (2005). Malware and antivirus procedures. In M. Pagani (Ed.), *Encyclopedia of multimedia technology and networking*. Hershey, PA: Idea Group Publishing.

Ring, S., & Cole, E. (2004). Taking a lesson from stealthy rootkits. *IEEE Computer Society, 2*(4), 38-45.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The ghost in the machine. *Communications of the AIS,* (14), 291-306.

Techtarget (2007, April 2). Top ten spyware threats. *SearchCIO-Midmarket*. Retrieved February 22, 2008, from http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci1075399,00.html

Vaas, L. (2007). Inside the mind of a hacker. *eWeek, 24*(24), 39-46.

Warkentin, M., & Johnston, A. C. (2008). IT governance and organizational development for security management. In D. Straub, S. Goodman, & R. Baskerville (Eds.), *Information security policies and practices*. Armonk, NY: M.E. Sharpe.

Warkentin, M., Luo, X., & Templeton, G. F. (2005). A framework for spyware assessment. *Communications of the ACM, 48*(8).

Willems, C., Holz, T., & Freiling, F. (2007). Toward automated dynamic malware analysis using CWSandbox. *IEEE Security & Privacy, 5*(2), 32-39.

KEY TERMS

Morphing Virus/Polymorphic Virus: These are viruses that are undectable by virus detectors because they change their own code each time they infect a new computer; some change their code every few hours. A polymorphic virus is one that produces varied but operational copies of itself. A simple-minded, scan string-based virus scanner would not be able to reliably identify all variants of this sort of virus. One of the most sophisticated forms of polymorphism used so far is the "Mutation Engine" (MtE) which comes in the form of an object module. With the Mutation Engine, any virus can be made polymorphic by adding certain calls to its assembler source code and linking to the mutation-engine and random-number generator modules. The advent of polymorphic viruses has rendered virus-scanning an ever more difficult and expensive endeavor; adding more and more scan strings to simple scanners will not adequately deal with these viruses.

Ransomware: This is a piece of pernicious software that exploits a user's computer vulnerabilities to sneak into the victim's computer and encrypt all files until the victim agrees to pay a ransom.

Rootkits: This is a set of software tools or programs that can be used by an intruder after gaining access to a computer system. Rootkits are designed to allow an intruder to maintain access to the system without the user's knowledge.

Spyware: This is a client-side software component that monitors the use of client activity and sends the collected data to a remote machine.

Virus Definition File (subscription service): This is a file that provides information to antivirus software to find and repair viruses. The definition files tell the scanner what to look for to spot viruses in infected files. Most scanners use separate files in this manner instead of encoding the virus patterns into the software, to enable easy updating.

Virus Signature: This is a unique string of bits, or the binary pattern, of a virus. The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses. Anti-virus software uses the virus signature to scan for the presence of malicious code.