Strategies and Techniques for Getting the Most Out of Your Antivirus Software for SAS® Users

Ryan Paul Lafler, High School Student, Operating System and Software Enthusiast, Spring Valley, California
Kirk Paul Lafler, Software Intelligence Corporation, Spring Valley, California

Abstract

Malware, sometimes referred to as malicious software, represent software threats engineered to damage computer systems without the knowledge of the owner using the system. SAS® users are increasingly becoming more prone to malware attacks and need to have strategies and a set of guidelines to help them get the most out of their antivirus software. This presentation highlights the many different types of computer threats, classification approaches, detection strategies, and removal methods. Attendees learn what malware is; the types of malware including viruses, Trojans, rootkits, zombies, worms, spyware, adware, scareware, spam email, and denial of service (DOS) attacks; password protection and management strategies; software to detect and protect computer systems; techniques for the removal of malicious software; and strategies and techniques for protecting your computer and data assets.

Introduction

Each day, hackers, phishers, and crackers manipulate and engineer codes to compromise and internally destroy or disrupt computer systems. Their main goal is to compromise or disrupt hardware, software, data and information on standalone, server-based and mainframe computers. However, anti-virus software makers also update and engineer their software and programs to deter and provide cyber security to many computer systems across the globe. In this paper, we will illustrate several different types of malicious software (malware) and the most efficient (and price worthy) anti-virus software programs to help support and secure SAS® Users everywhere.

Computer Safety Essentials 101

Here are a few simple things to keep in mind when it comes to computer safety:

- ✓ Always keep a safe and effective Antivirus software on your computer
- ✓ Firewall is enabled
- ✓ Only download updates and files from web sites that have scanned them with trusted Antivirus Software
- ✓ Never open any Email or attachment link you are unsure of
- ✓ Use a safe and trusted Web Browser (see Authors Picks)
- ✓ Do online banking on HTTPS web addresses only
- ✓ Back up all files and documents

Types of Malicious Software (Malware) Security Threats

Malicious Software (malware) does everything in its power to damage, disable, take control, alter, change or compromise information from a computer system. Figure 1 shows nine of the most common malware threats including Denial of Service, Trojan Horse, Rootkit, Botnet Operation, Exploit, Keystroke Logging, Spyware, Rogue Security, and self-replicating viruses such as the Computer Worm.

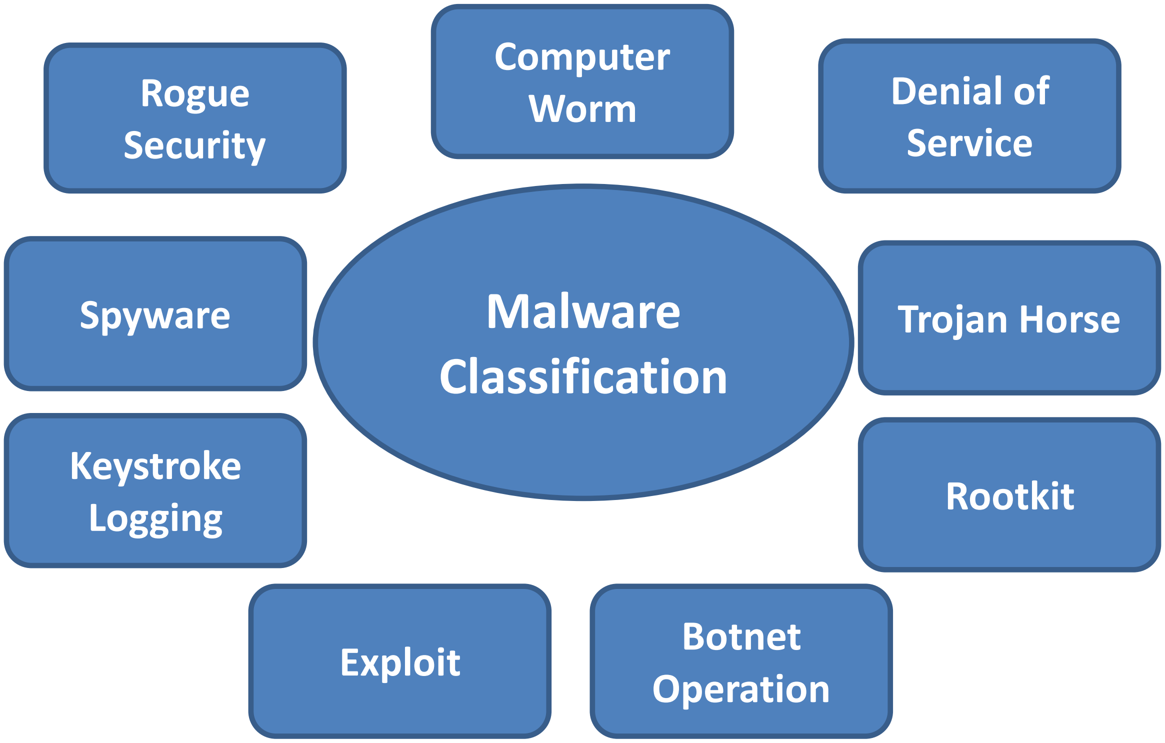

Figure 1. Malware Classification

With the number of security threats on the rise, it is imperative to be able to identify characteristics associated with malicious software, including its ability to avoid antivirus detection through mutation. Recent news accounts have cited a new and more malicious software, called the ***Heartbleed bug*** (April 2014), operating under the radar to compromise the communications between computers and network servers. This bug penetrated the vulnerabilities in the OpenSSL, or Secure Sockets Layer, allowing hackers access to passwords, classified documents and confidential information on many websites and private accounts. Going unnoticed for as long as two years, impact has been felt by as much as 75% of ecommerce websites, firewalls and beyond.

As the world of technology forges ahead, malicious software can rear its ugly side at any time. Consequently, we must remain vigilant and recognize any, and all, characteristics that malware exhibits. To assist in this vigilance, key characteristics within each malware category are presented below.

Computer Worm

- ✓ Self-replicating virus
- ✓ Corrupts, misplaces and deletes files
- ✓ Difficult for users to detect

Denial of Service (DoS) Attack

- ✓ Utilizes a Zombie Computer Army
- ✓ Floods a network/website with access requests
- ✓ Crashes the network/website for a short time

Trojan Horse

- ✓ Disguised as a legitimate download/program
- ✓ Used as a backdoor program
- ✓ Works stealthily without the user's knowledge

Rootkit

- ✓ Used as a backdoor to gain access to a system
- ✓ Illegally acquires Administrator status
- ✓ Implants itself within kernel of the computer

Botnet Operation

- ✓ Creates a "Zombie Computer Army"
- ✓ Spammer sends viruses to computers over network
- ✓ Functions stealthily

Exploit ("Exploits" and attacks security vulnerabilities)

- ✓ Targets a glitch or bug in a computer system
- ✓ Commands Trojan horses, Rootkits, DoS Attacks
- ✓ Open-source OpenSSL Cryptography Library Security bug – Heartbleed bug

Keylogger (Tracks all keystrokes made on computer)

- ✓ Form of Malicious Hardware/Software
- ✓ Tracks the victim's keyboard strokes
- ✓ Used to crack security passwords

Spyware

- ✓ Collects information on the user illegally
- ✓ Places tracking cookies on a user
- ✓ Sells personal information to Third Parties

Rogue Security Software

- ✓ Appears in the form of a Pop-Up
- ✓ Scares user into thinking computer is infected
- ✓ Results in additional problems to computer system
- ✓ Comes bundled with Trojan, keylogging software

The Symptoms of a Malicious Software Infection

After researching the most common types of malicious software forms, we present information about the symptoms of a system infection. The various symptoms include your computer not shutting down properly; to deleted, misplaced, or altered files and documents; and other symptoms.

Self-Replicating Viruses

- ✓ Files are misplaced or deleted
- ✓ Decrease in Internet browsing speed
- ✓ Frequent computer lock ups
- ✓ Frequent Advertisements (pop-ups)
- ✓ New icons created on home page
- ✓ Firewall Disabled
- ✓ Applications unable to start
- ✓ Blue screen of death (BSOD)
- ✓ Computer can't power on
- ✓ Updates aren't installed successfully

Trojan Horse

- ✓ CPU/RAM Usage greatly increases
- ✓ Background programs running without consent of owner
- ✓ Blue Screen of Death
- ✓ Constant annoying Pop-Ups
- ✓ Slow, unusable internet connection
- ✓ Account passwords altered
- ✓ Mouse and key commands changed

Rootkit

- ✓ Major CPU/RAM Usage
- ✓ Antivirus software disabled
- ✓ Extensive web browser tabs open
- ✓ Blue Screen of Death
- ✓ Slow computer performance
- ✓ Altered keys, time, and commands

Denial of Service (DoS) Attack on a Web Page

- ✓ Web page unable to open
- ✓ Slow connection to web page
- ✓ Your computer slows to a halt after visiting an attacked webpage

Botnet Operation

- ✓ CPU Fans goes into overdrive when computer is not undertaking an action
- ✓ Emails sent with your name on them that you did not send
- ✓ Programs open and shut down unexpectedly
- ✓ Cannot download antivirus software/updates
- ✓ Pop-Up windows appear frequently

Spyware

- ✓ Pop-Up Advertisements
- ✓ Browsing cookies enabled without owner's consent
- ✓ Web browser includes many toolbars
- ✓ Unfamiliar home page
- ✓ Default search engine changed
- ✓ New web bookmarks
- ✓ New and/or altered "Favorites"

Rogue Security Software

- ✓ Unexpected ads popping up on web browser
- ✓ Ads saying that your computer is infected with a virus
- ✓ Ads placing infected websites at the top of Google searches (SEO)
- ✓ Spam emails which include links for:
  - – Special deals
  - – Free trial offers

Removing Malicious Software Threats

Once a malware threat has been identified, you will want to follow these instructions to remove it:

- ✓ Disconnect your computer from the internet or any network (will help to prevent the spread of a self replicating virus)
- ✓ Run a FULL Antivirus scan on your computer
- ✓ Remove quarantined items
- ✓ While your computer is compromised DO NOT back it up

Authors Picks – Antivirus Software

The authors have tested many leading free and fee-based antivirus software using a consistent set of criteria in coming to their final recommendations. The following criteria were used to derive their final recommendations:

- ✓ Ease of use
- ✓ Effectiveness in protecting and safeguarding operating systems and browsers
- ✓ Comprehensiveness
- ✓ Support for Windows Vista, Windows XP (Note: Microsoft stopped supporting XP in 2014), Windows 7 and Windows 8
- ✓ Cost-effectiveness
- ✓ Ability to apply automatic and timely updates and patches
- ✓ Background operation support

Microsoft Security Essentials

Free Download from Microsoft website at http://windows.microsoft.com/en-us/windows/security-essentials-download
Microsoft Security Essentials boasts the following features:

- ✓ Protects users from backdoor programs, computer viruses, worms, spyware, and Trojan horses
- ✓ Self-updating software
- ✓ Solid record of fixing issues
- ✓ Available for Windows XP, Vista, 2000, and 7 operating systems

Microsoft Anti-spyware

- ✓ Protects users from backdoor programs, computer viruses, worms, Trojan horses and Spyware
- ✓ Self-updating software
- ✓ Solid record of fixing issues
- ✓ Integrated into Windows Vista and Windows 7; However it can also be downloaded from Microsoft.com/downloads for Windows XP and Windows 2000 operating systems

Windows Defender (Formerly known as Microsoft Anti-spyware)

- ✓ Protects users from backdoor programs, computer viruses, worms, Trojan horses and supports enhanced Spyware features
- ✓ Self-updating software
- ✓ Solid record of fixing issues
- ✓ Integrated into Windows 8, 8.1 operating systems and Runtime versions

Avast! Internet Security

Avast! Internet Security for Web Browsers running under Windows and Mac Operating Systems
Free Download from the Avast website at http://www.avast.com/en-us/index
Avast! Internet Security supports the following features:

- ✓ Uses familiar color-coded icons, (green, yellow and red), to indicate website safety
- ✓ Self-updating software
- ✓ Verifies the certificates of the website

Adblock Plus

AdBlock for Web Browsers running under Windows

Free Download from the AdBlock website at https://adblockplus.org/en/chrome
Adblock Plus supports the following features:

- ✓ Protects users from keyloggers
- ✓ Blocks any “annoying ads” from the user
- ✓ Disables Pop-Ups and tracking
- ✓ Compatible with Google Chrome and Firefox

Ghostery

Ghostery for Web Browsers running under Windows

Free Download from the Ghostery website at https://www.ghostery.com/en/
Ghostery supports the following features:

- ✓ Protects users privacy
- ✓ Shows who’s tracking your web browsing experience
- ✓ Self-updating software

Google Chrome – Recommended Web Browser

- ✓ Advanced privacy settings
- ✓ Add on security protection extensions
- ✓ Self-updating web browser
- ✓ Good record of fixing any issues
- ✓ Shows user memory usage of each tab

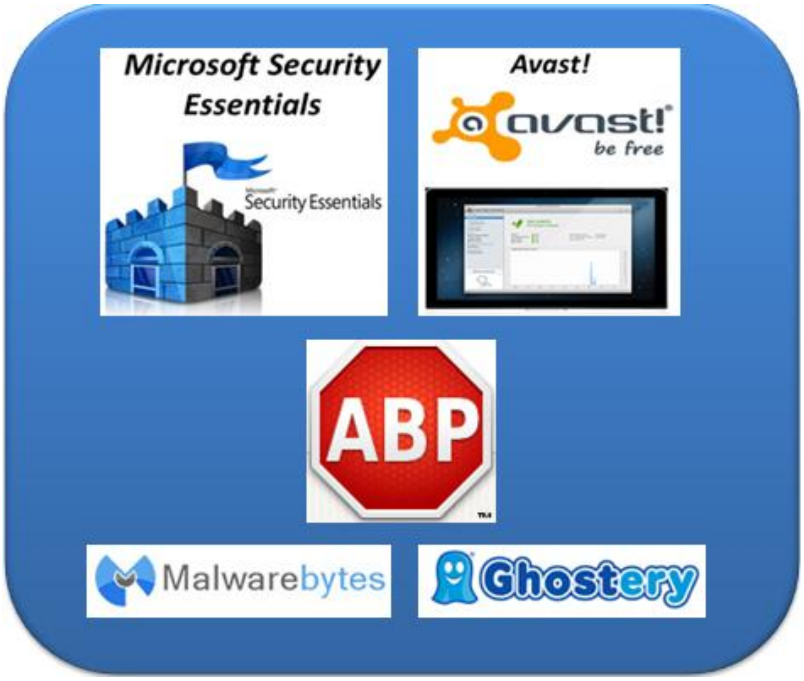

Figure 2. Authors Picks – Antivirus Software

Conclusion

This paper presented the different types of computer threats including the Heartbleed bug, classification approaches, detection strategies, and removal methods, as well as what malicious software (malware) is; the types of malware including viruses, Trojans, rootkits, zombies, worms, spyware, adware, scareware, spam email, and denial of service (DOS) attacks. Various strategies and techniques on password protection and management; software to detect and protect computer systems; techniques for the removal of malicious software; and the methods for protecting your computer and data assets were presented. Finally, we recommended our choice for the best, free, anti-virus software for SAS users.

References

Emigh, Aaron (2006), *"The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond,"* A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council, the Anti-Phishing Working Group, and IronKey, Inc.

Evans, Alan; Kendall Martin and Mary Anne Poatsy (2013), *"Technology in Action – Securing Your System: Protecting Your Digital Data and Devices,"* Copyright © 2013 by Pearson Education, Inc., Publishing as Prentice Hall.

Lafler, Ryan Paul and Kirk Paul Lafler (November 2013), *"Strategies and Techniques for Getting the Most Out of Your Antivirus Software for SAS® Users,"* Western Users of SAS Software (WUSS) 2013 Conference, Copyright © 2013 by Ryan Paul Lafler and Kirk Paul Lafler, Spring Valley, California, USA.

Lafler, Ryan Paul and Kirk Paul Lafler (August 2013), *"Strategies and Techniques for Getting the Most Out of Your Antivirus Software for SAS® Users,"* San Diego SAS Users Group (SANDS) 2013 Meeting, Copyright © 2013 by Ryan Paul Lafler and Kirk Paul Lafler, Spring Valley, California, USA.

Miller, Lawrence C. (2012), *Modern Malware for Dummies®,* John Wiley & Sons, Inc., Hoboken, New Jersey, USA.

Nahrstedt, Klara (Spring 2013), *"CS 423 – Operating System Design, Lecture 38: Security Threats,"* Department of Computer Science; University of Illinois, Urbana, Illinois, USA.

Nieva, Richard (2014), *"How To Protect Yourself From the Heartbleed Bug,"* Copyright © 2014 by Richard Nieva.

Russell, Kyle (2014), *"Here's How To Protect Yourself From The Massive Security Flaw That's Taken Over The Internet,"* Copyright © 2014 by Kyle Russell.

Stefani, Evanthia and Eudoxia Sianou (2012), *"How to from Malware Attacks, Antivirus Techniques,"* Department of Informatics and Computer Technology; Technology Educational Institution (TEI) of Western Macedonia, Greece.

Singh, Sudhakar; P.K. Khare and Prashant Mor, "*Malware Detection and Removal Techniques*," International Journal of Electronics and Computer Science Engineering (pps. 273-280); ISSN- 2277-1956.

The Threat of Evasive Malware (2013), Lastline Labs, Copyright © 2009-2013 Lastline, Inc., Goleta, California, USA.

Acknowledgments

The authors thank Lizette Alonzo and Lisa Mendez, SCSUG 2016 Conference Co-Chairs; the South Central SAS Users Group (SCSUG) Executive Board; and SAS Institute for organizing and supporting a great conference!

Trademark Citations

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Security Essentials and Windows Defender are the registered trademarks of Microsoft Corporation, Redmond, Washington, USA. Google and Google Chrome are the registered trademarks of Google Inc., Mountain View, California, USA. Other brand and product names are trademarks of their respective companies.

About the Authors

Ryan Paul Lafler is a senior at Valhalla High School in El Cajon, California with interests in the implementation and use of operating systems, statistics and SAS University Edition software, and the application of security strategies and techniques. Ryan works with proprietary and open-source operating systems including SAS University Edition software; uses malware and antivirus tools and software to identify and remove malicious software (malware) issues and threats; and is the recipient of a "Best" contributed paper at the 2013 Western Users of SAS Software (WUSS) Conference.

Kirk Paul Lafler is consultant and founder of Software Intelligence Corporation and has been using SAS since 1979. He is a SAS Certified Professional, provider of IT consulting services, trainer to SAS users around the world, and sasCommunity.org emeritus Advisory Board member. As the author of five books including PROC SQL: Beyond the Basics Using SAS, Second Edition (SAS Press 2013); PROC SQL: Beyond the Basics Using SAS (2004), Kirk has written more than five hundred papers and articles, been an Invited speaker and trainer at four hundred-plus SAS International, regional, special-interest, local, and in-house user group conferences and meetings, and is the recipient of 23 "Best" contributed paper, hands-on workshop (HOW), and poster awards.

Comments and suggestions can be sent to:

Ryan Paul Lafler
High School Student, Operating System and Software Enthusiast
E-mail: RPALafler@aol.com
LinkedIn: http://www.linkedin.com/in/RyanPaulLafler

~~~
~~~

Kirk Paul Lafler
Senior Consultant, Application Developer, Data Analyst, Trainer and Author
Software Intelligence Corporation
E-mail: KirkLafler@cs.com
LinkedIn: http://www.linkedin.com/in/KirkPaulLafler
Twitter: @sasNerd