Paper 187-2017

Guidelines for Protecting Your Computer, Network and Data from Malware Threats

Ryan Paul Lafler, High School Student, Spring Valley, California
Kirk Paul Lafler, Software Intelligence Corporation, Spring Valley, California

Abstract

Since many SAS® Users either work for or own companies that house big data, the threat that malicious software poses becomes even more extreme. Malicious software, often abbreviated as "malware", includes many different classifications, ways of infection, and methods of attack. This e-Poster highlights the types of malware, detection strategies, removal methods, and provides guidelines to secure essential assets and prevent future malware breaches.

Introduction

Hackers, phishers, and crackers manipulate and engineer code, scripts, active content and other software to compromise, destroy, disrupt or steal confidential information from computer systems, networks and databases and other data sources/ repositories. Their main goal is to compromise and disrupt hardware, software, firewalls, data, information, servers, standalone computers, server-based computers and mainframe computers. However, anti-malware software developers 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.

What is Malware (or Malicious Software)?

Malicious software, or malware, is software that is designed to disrupt, compromise and function in some undesirable way for purposes of impacting a computer's operation, access and collect information, or gain access to a computer system with hostile or sinister intent in-mind.

Safety Essentials 101

Personal computer users, internet users, organizations small and large, and data centers have a huge burden in front of them – remain vigilant and do everything possible to safeguard computer systems, firewalls, networks, data centers, databases and data sources from being compromised from malicious software. But how is that done? We've identified a few things everyone should consider when surfing the web, downloading Internet content, accessing emails and their attachments, clicking misleading links and accessing infected external devices:

- ✓ Always protect your core data, databases and data sources;
- ✓ Maintain an up-to-date, safe and effective malware software on your computer;
- ✓ Firewall is enabled;
- ✓ Only download updates and files from websites 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 such as, Google Chrome or Mozilla Firefox;
- ✓ Do online banking on HTTPS web addresses only;
- ✓ Back up all files and documents;
- ✓ Identify and classify sensitive information;
- ✓ Review, understand and grant rational access rights to databases, data, files, etc.;
- ✓ Routinely use analytics to sift through large volumes of data activity.

Types of Malicious Software (Malware) Security Threats

Malicious Software (malware) does everything in its power to damage, disable, take control, alter, steal, change or compromise confidential, sensitive and other types of 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.

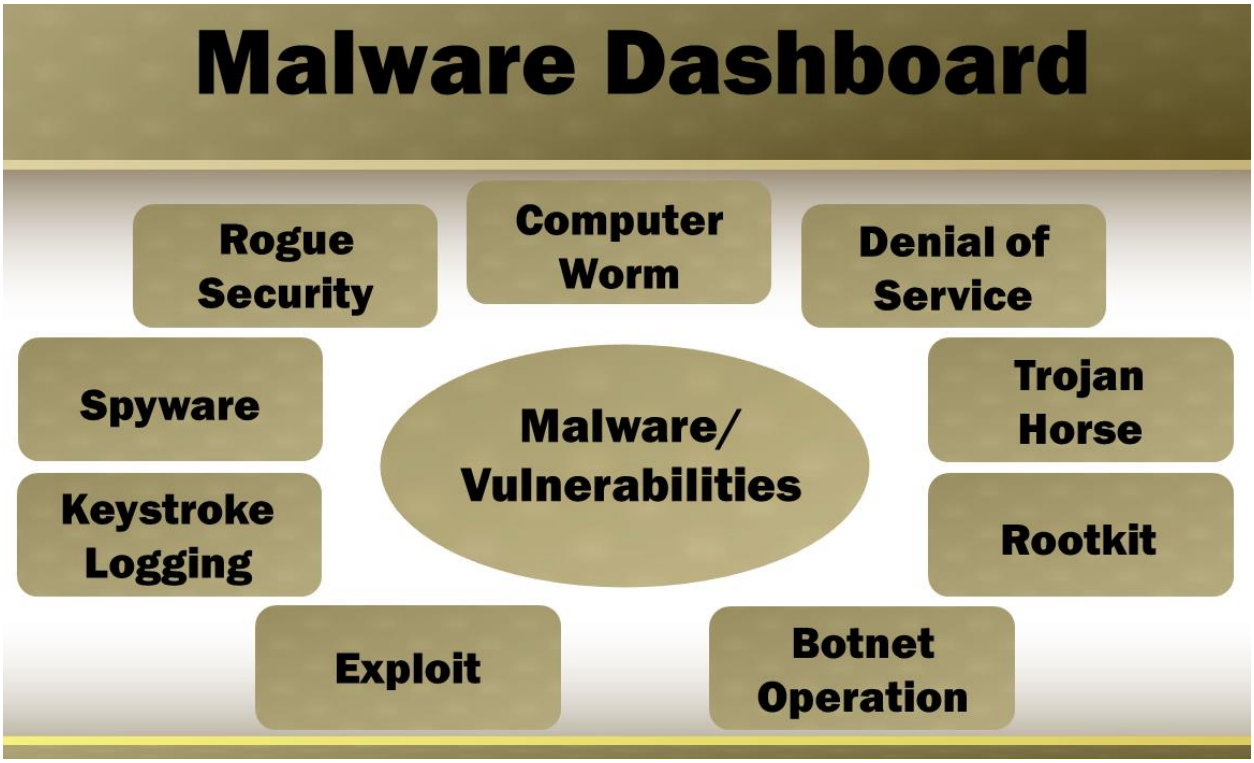

Figure 1. Malware Classification

With the number of malware threats compromising computer systems on the rise, it becomes more important than ever to be able to recognize key characteristics such as malware's ability to mutate to avoid detection by antivirus software. Key characteristics for each malware category are listed 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

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 types, the following descriptions illustrate the symptoms associated with 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

Malware Threats of 2015 and 2016

Symantec®, *Trend Micro*® and *Kaspersky Labs*® released data and statistics regarding Malicious Software Threats in 2015 ranging from DDOS Attacks, Backdoor Program Implementation, Virus Executables (.exe) and Visual Basics (.VBE). Various reports also include software/security vulnerabilities exploited by worms.

- ***Symantec*®: http://www.symantec.com/security_response/**
- ***Kaspersky Labs*®: https://securelist.com/**
- ***Trend Micro*®: http://www.trendmicro.com/us/security-intelligence/current-threat-activity/**

According to Malwarebytes, Ransomware dominated the malware threat landscape in 2016. In January 2017, Forbes contributor, Kevin Murnane, wrote about the 2016 malware threat landscape.

- ***The Malwarebytes Report: The 2016 Malware Threat Landscape: https://www.forbes.com/sites/kevinmurnane/2017/01/31/the-malwarebytes-report-the-2016-malware-threat-landscape/#247479a821ee***

New and Emerging Malware Threats

- "**Man-in-the-Cloud-Attacks**": This attack targets the **cloud**, the virtual space containing files stored on the internet outside of your own computer's physical hard drive, during *file synchronization*

  - ✓ People using **Google Drive, Dropbox, OneDrive** and any other Cloud Service are at risk, particularly when not using file encryption
  - ✓ **Link to Article**: http://www.darkreading.com/cloud/man-in-the-cloud-owns-your-dropbox-google-drive----sans-malware-/d/d-id/1321501

- **Crypto-Ransomware**: This specific piece of Malware can be downloaded from the internet (a.k.a. "the Wild") in the form of a ZIP File that when unzipped, contains a Visual Basic Program that runs the Malicious Software Code. Once successfully run, files, data, pictures, and the entire computer is encrypted and can only be decrypted by paying a "fine" in the Bitcoin® Currency to the attacking group.

  - ✓ **Link to Article:** http://www.symantec.com/connect/blogs/breaking-bad-themed-los-pollos-hermanos-crypto-ransomware-found-wild

- **GHOST Vulnerability:** As of March 31st, 2015, SAS is aware of the vulnerability found in the SAS University Edition and has issued a patch to correct the vulnerability. Simply update SAS University Edition and the vulnerability will be fixed.

  - ✓ **Link to Article:** http://support.sas.com/security/Ghost.html

- **OpenSSL Vulnerabilities:** As of March 4th, 2015, vulnerabilities were found within SAS's Secure Socket's Layer- a protocol between the server and web browser communicating to each other for information exchange. The FREAK and SKIP-TLS OpenSSL were affected and SAS is currently "taking steps to ensure our servers are protected from attacks."

  - ✓ **Link to Article:** https://support.sas.com/security/freak-OpenSSL.html

Recent Malicious Software Threats

Every year, the statistics show that malicious software threats and attacks have dramatically increased as technology continues to evolve. A study done by CNN in April of 2015 detailed that over "one million new malware threats are released everyday". With numbers like this, it becomes all too important that users who deal with both small and big data are well-protected and secured. The developers at SAS Institute are taking steps to address vulnerabilities that have been recently exploited (as of 2015) within their software.

In Alison DeNisco's article from Kaspersky Labs (February 28, 2017), "Mobile malware attacks increased more than three times between 2015 and 2016." She also indicated that, "Geographically speaking, the nations with the highest number of attacks were Bangladesh, Iran, Nepal, China and Indonesia."

In 2015, two major vulnerabilities arose concerning the OpenSSL of SAS's main product and the Linux glibc (GNU C Library) in the SAS University Edition. It is important to keep in mind that vulnerabilities are not malicious software programs or viruses, but rather a door that is no longer secured by a lock, thus leaving it susceptible to viruses and backdoor programs. OpenSSL stands for Open (open-source) Secure Sockets Layer, which serves as a communication line for the main server and the web browser. Within the SAS University Edition, the GHOST vulnerability was found within the programming library of SAS University, and as of March 31st, 2015, SAS released the following statement: "A patch is now available for SAS University Edition…the vulnerability is minimal".

Link to CNN Article: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

Article Name: "Nearly 1 million new malware threats released every day!".

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

The Criteria Used to Determine the Best Malware Protection Software

Now that you've learned about the threats that malware presents to your computer, firewall, network, databases, data, and personal information, you may be wondering what the best, if any, malware protection software is available. The authors have tested many leading free and fee-based malware protection software, referred to as antimalware, using a consistent set of criteria in deriving their final recommendations. The set of criteria include:

- ✓ Ease of use
- ✓ Effectiveness in protecting and safeguarding systems
- ✓ Comprehensiveness
- ✓ Support for Windows 8, Windows 7, Windows 2000, Windows Vista and Windows XP

- ✓ Cost-effectiveness
- ✓ Ability to apply automatic updates
- ✓ Background operation support
- ✓ Ability to detect malware
- ✓ Ability to remove (or eradicate) malware
- ✓ Access to technical help and support

The Best Malware Protection Software

Now that you've learned about the threats that malware presents to your computer, firewall, network, databases, data, and personal information, you may be wondering what the best, if any, malware protection software is available. The authors have tested many leading free and fee-based malware protection software, referred to as antimalware, using a consistent set of criteria in deriving their final recommendations. The set of criteria include:

- ✓ Ease of use
- ✓ Effectiveness in protecting and safeguarding systems
- ✓ Comprehensiveness
- ✓ Support for Windows 8, Windows 7, Windows 2000, Windows Vista and Windows XP
- ✓ Cost-effectiveness
- ✓ Ability to apply automatic updates
- ✓ Background operation support
- ✓ Ability to detect malware
- ✓ Ability to remove (or eradicate) malware
- ✓ Access to technical help and support

Microsoft Security Essentials

Free Download from Microsoft 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. A "free" download of the software can be accessed 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. The Best Malware Protection Software

Conclusion

This paper and e-poster presented the different types of computer threats, 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, and free, malware software.

References

DeNisco, Alison (2017), *"Report: 2016 Saw 8.5 Million Mobile Malware Attacks, Ransomware and IoT on the Rise,"* Kaspersky Labs. http://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/.

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,"* "Best" Contributed Paper at the 2013 Western Users of SAS Software (WUSS) 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.

Murnane, Kevin (2017), *"The Malwarebytes Report: 2016 Malware Threat Landscape,"* Forbes. https://www.forbes.com/sites/kevinmurnane/2017/01/31/the-malwarebytes-report-the-2016-malware-threat-landscape/#247479a821ee.

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

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 the e-Posters Section Chair for accepting our abstract and paper; the SAS Global Forum (SGF) 2017 Conference Chair; SAS Institute Inc.; and the SGF Executive Committee for organizing a great conference!

Trademark Citations

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, software tool design and development, and the application of security strategies and techniques. Ryan works with proprietary and open-source operating systems; 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 an entrepreneur, consultant and founder of Software Intelligence Corporation, and has been using SAS since 1979. Kirk is a SAS Certified Professional, provider of IT consulting services, advisor and professor at UC San Diego Extension and educator to SAS users around the world, mentor, and emeritus sasCommunity.org Advisory Board member. As the author of six books including Google® Search Complete (Odyssey Press. 2014) and PROC SQL: Beyond the Basics Using SAS, Second Edition (SAS Press. 2013); Kirk has written hundreds of papers and articles; been an Invited speaker and educator at hundreds of SAS International, regional, special-interest, local, and in-house user group conferences and meetings; and is the recipient of 25 "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

~ ~ ~ ~ ~

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