SAS® GLOBAL FORUM 2017

April 2 - 5 | Orlando, FL

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

Ryan Paul Lafler, High School Student

Kirk Paul Lafler, Software Intelligence Corporation

USERS PROGRAM

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

Ryan Paul Lafler, High School Student

Kirk Paul Lafler, Software Intelligence Corporation

Go to Dashboard

ePoster Dashboard

Return

Abstract

Introduction

Conclusion

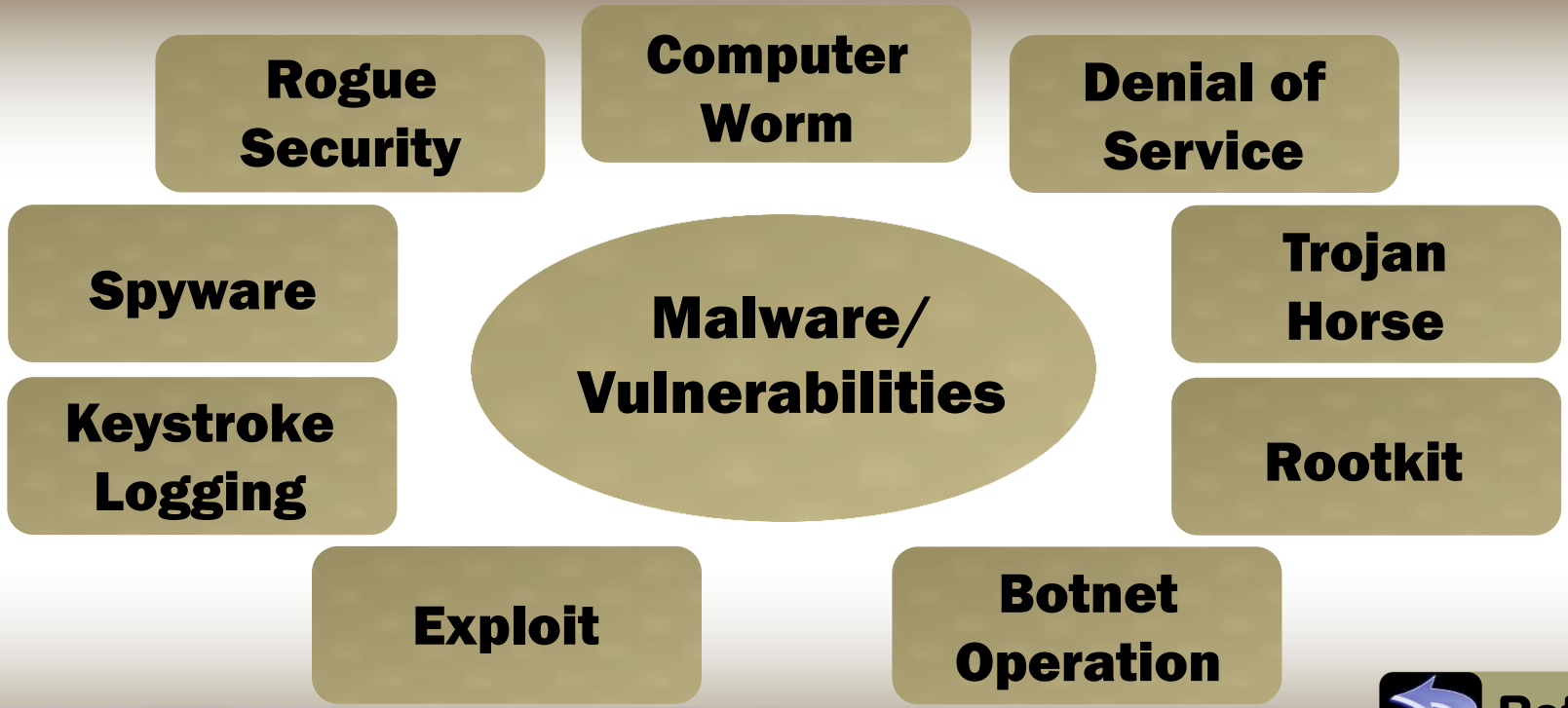
Malware Dashboard

Authors

Recommendations

Return

Malware Dashboard



Return

Return

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.

Return

Return

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. We will illustrate several different types of malware and the most efficient (and price worthy) anti-virus software programs to help support and secure SAS® users everywhere.

Return
Return

What is Malware?

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.

Return

Return

Computer Worm

Characteristics	Self-replicating virus Corrupts, misplaces, and deletes files Difficult for users to detect
Symptoms	Spam emails sent from an unknown sender Programs perform random, uncontrollable tasks
Solutions	Maintain a reliable firewall Do not open spam emails Run anti-malware program

Return

Return

Denial of Service

Characteristics	Network of computers flood a server Server must process overflow of requests Servers crash for short period of time
Symptoms	Internet connectivity to website is slow Website is unavailable Error 404 message (server is down)
Solutions	Ensure extra bandwidth is available Mitigate amount of requests processed by server

Return

Return

Trojan Horse

Characteristics	Backdoor program that gains access into system Allows for malware to enter system undetected
Symptoms	System constantly crashes Files are moved, deleted, or a locked out Pop-up warnings displayed on desktop
Solutions	Do not open spam emails Maintain a stable firewall Run anti-malware software routinely

Return

Return

Rootkit

Characteristics	Backdoor program Embeds in kernel (mainframe) of system Allows for malware to bypass security protocols
Symptoms	Operating system randomly shuts down User loses administrative status over system User is locked out of files/programs
Solutions	Maintain stable firewall Do not download/install suspicious programs

Return

Return

Botnet Operation

Characteristics	Multiple systems linked together over network Infected computers used as “bots” Targets servers/systems through DDoS attacks
Symptoms	System is slow, unresponsive Internet connectivity limited
Solutions	Routinely run anti-malware software Maintain stable firewall Do not download/install suspicious programs

Return

Return

Exploit

Characteristics	A vulnerability/weakness within a system Security weakness targeted by malware Some malware find/establish exploits in system
Symptoms	Software not updated prone to exploits Operating systems not updated prone to exploits
Solutions	Maintain updated operating system Maintain updated cyber-security software Ensure all software is supported

Return

Return

Keystroke Logging

Characteristics	Common feature of spyware Keyboard movements tracked Used to steal passwords and hack accounts
Symptoms	Pop-ups randomly appear on desktop High CPU/RAM usage Suspicious software running in background
Solutions	Routinely run anti-spyware software Maintain strong firewall

Return

Return

Spyware

Return

Characteristics	Malware used to gain/steal information Tracks and monitors system illegally
Symptoms	Web browser settings changed Firewall is disabled
Solutions	Routinely run anti-spyware software Do not download suspicious software Custom install programs instead of default

Return

Rogue Security

Characteristics	Malware designed to look legitimate If installed, creates a backdoor into the system Often disguised as security software to fool user
Symptoms	Software constantly runs in background
Solutions	Do not download/install software from pop-ups Avoid downloading products from ads on web

Return

Return

Recommendations

- ✓ Windows Security Essentials (Windows 7 and earlier);
- ✓ Windows Defender (Windows 8 and later);
- ✓ Malware Bytes;
- ✓ Avast! Internet Security;
- ✓ Adblock Plus;
- ✓ Ghostery;
- ✓ Google Chrome.

Conclusion

Return

This e-poster highlights the different types of computer threats, classification approaches, detection strategies, and removal methods, as well as what malicious software and vulnerabilities are; 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.

Authors

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
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

Return
Return