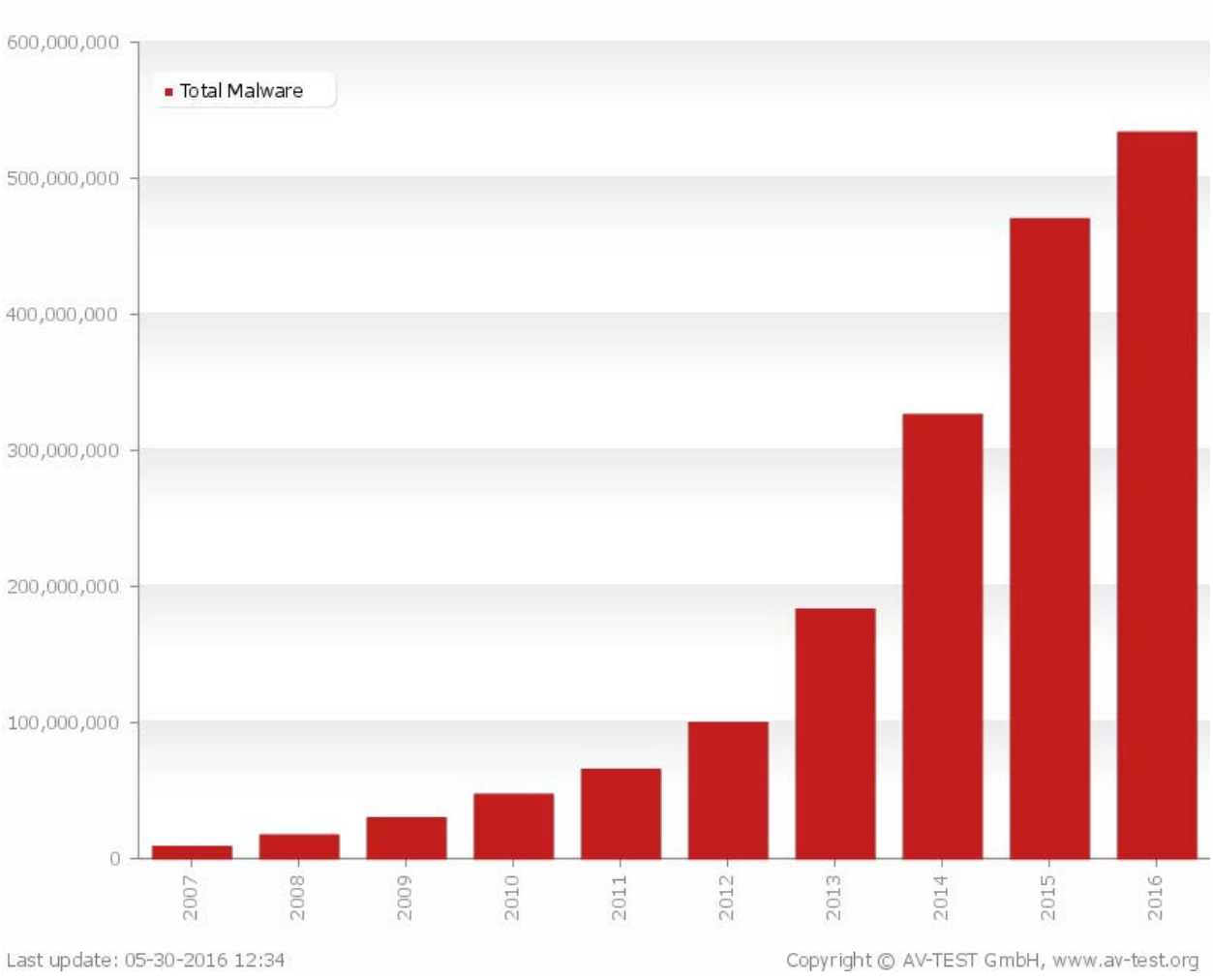
An Evidence-Based Malware Report Using the Captured Malware Data At ODU And NC A&T

General Introduction

Malicious software, or malware, is used by cybercriminals, hacktivists and nation states to disrupt computer operations, steal personal or professional data, bypass access controls and otherwise cause harm to the host system. Appearing in the form of executable code, scripts, active content or other software variants, there are many different classes of malware which possess varying means of infecting machines and propagating themselves. The malware threat landscape is getting worse and many organizations continue to suffer security breaches as a result.



Popular malware that are attacking our campuses:

Our anti-malware software captured a variety of malware that are attacking our campuses in the past year. Below is a list of the popular malware:

[1] Backdoor.APT.DarkComet
[2] Data.Encoding.xor
[3] Eicar-Test-Signature
[4] Exploit.Generic
[5] Exploit.Java
[6] FE_CVE_2013_2460_Malware_Jar_2
[7] FE_Data_Obfuscation
[8] FE_Evasion_VMDetect
[9] FE_Generic_TaskSchedular
[10] FE_Heuristic_Malware_Reflection_Jar
[11] FE_Java_Security_Suspicious
[12] FE_PUP_Softpulse
[13] Infostealer.Banker.Zbot
[14] Local.Infection
[15] Malicious.URL
[16] Malware Name
[17] Malware.archive
[18] Malware.Binary
[19] Malware.Binary.Dll
[20] Malware.Binary.Jar
[21] Malware.ZerodayCallback
[22] Trojan.Adaebook
[23] Trojan.Asprox
[24] Trojan.Downloader
[25] Trojan.Downware
[26] Trojan.Gen
[27] Trojan.Generic
[28] Trojan.GenericKD
[29] Trojan.Java
[30] Trojan.Medfos
[31] Trojan.Packed.28257
[32] Trojan.PWS.Banker
[33] Trojan.Rerdom.A
[34] Trojan.Spy.Zbot.qrkh
[35] Trojan.Spy.Zbot.sima
[36] Trojan.VOPackage
[37] Trojan.Zbot
[38] Trojan.Zeprox
[39] Win.Adware.Adgazelle
[40] Win.Adware.Agent
[41] Win.Adware.Domaiq
[42] Win.Adware.Downloadadmin
[43] Win.Adware.Installcore

[44] Win.Adware.Linkular
[45] Win.Adware.PCFixSpeed
[46] Win.Adware.Toggle
[47] Win.Trojan.Agent

Malware examples

- Trojan.Zbot, also called Zeus, is a Trojan horse that attempts to steal confidential information from the compromised computer. The Trojan.Zbot files using a toolkit in marketplaces for online criminals allows an attacker a high degree of control over the functionality of the final executable that is distributed to targeted computers. The user may receive an email message purporting to be from organizations such as the FDIC, IRS, MySpace, Facebook, or Microsoft. The message body warns the user of a problem with their financial information, online account, or software and suggests they visit a link provided in the email. The computer will be compromised if the user visits the link, if it is not protected.
- Malicious URL is a URL created with malicious purposes, among them, to download any type of malware to the affected computer, which can be contained in spam or phishing messages. Phishing involves sending emails that appear to come from reliable sources (such as banks) and that try to get users to reveal confidential banking information. One of the most widely used tactics is to include a link in the message which, when clicked on, takes users to spoofed web pages. In this way, users, thinking that they are in a trusted site, enter the requested information which is really falling into the hands of the fraudster.
- SQL programming language is used when a website needs to retrieve a piece of information from its database, either to process it or to present to a user. In SQL injection (SQLi) attack, hackers typically enter malicious commands into forms on a website to make it reveal juicy bits of data. It was used in biggest data breaches such as Wall street journal hack, hacking into federal agency databases, personal details of World Health Organization employees, etc. SQLi is an easy way to hack and relatively easy to defend against. As a result, SQLi is repeatedly placed at the top of vulnerabilities in the Open Web Application Security Project (OWASP) reports.

How to tell if your computer is showing symptoms of Malware

- **IF you start noticing pop-up advertisements all the time, this could be due to malware**
- **My settings have changed.** Some unwanted software can change your home page or search page settings. Even if you adjust these settings, you might find that they revert back every time you restart your computer.
- **My web browser contains additional components that I don't remember downloading.**

- **My computer seems to slow down.** Malware and other unwanted software are known to track your activities and deliver advertisements and can slow down your computer. In some case they may crash your system, If you notice a sudden increase in the number of times a certain program crashes, or if your computer is slower than normal at performing routine tasks, you may have malware, spyware and unwanted software.

How to prevent and remove malware

- By installing effective anti-malware software, you can defend your devices – including PCs, laptops, Macs, tablets and smartphones – against Trojans.
- Input sanitization, penetration testing, web application firewall are some popular means to address the SQLi attack.
- Keeping the operating system and browser software up to date

Additional Resources

1. What is a Trojan Virus? More information can be found at

http://www.kaspersky.com/internet-security-center/threats/trojans

2. SQL injection attack. More information can be found at
http://blog.checkpoint.com/2015/05/07/latest-sql-injection-trends/

http://motherboard.vice.com/read/the-history-of-sql-injection-the-hack-that-will-never-go-away

3. Free Online Tools for Looking up Potentially Malicious Websites

https://zeltser.com/lookup-malicious-websites/