

# CYBERSECURITY CYBER-ATTACK SERIES

## MALWARE & RANSOMWARE

Prepared by Keith J. Gomes, J.D., Ph.D.

### What is Malware?

Malware, short for "malicious software," refers to kind of computer program designed to infect a user's computer and inflict harm on the user. Malware today is largely designed by and for professional criminals. The biggest threat to computer users is that sensitive information, such as banking and credit card accounts and passwords, could be stolen.

### Different Types of Malware

Some examples of malware include the following:

1. **Adware:** The most lucrative but also most benign form of malware, adware displays ads on your computer. This might interfere with the user's ability to browse the internet efficiently if the number of pop-up ads becomes intolerable.
2. **Spyware:** Spyware is software that spies on the user, tracking Internet activities in order to send advertising (adware) to the user's computer.
3. **Virus:** A virus is a contagious program or code that attaches itself to another piece of software and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers or by downloading files from disreputable sources. Some viruses have a malicious payload that can cause files, or sometimes, the entire hard drive from a user's computer to be deleted. Viruses known as overwriting viruses write over the original file with their own malicious code rendering the file irrecoverable as a result. "Loveletter" is one of the better known examples of malware that included an overwriting payload.
4. **Worm:** A program that replicates itself and destroys data and files on the computer. Worms attack a computer's operating files and data files until all files are no longer retrievable by the user.
5. **Trojan:** The most dangerous form of malware, Trojans are written with the purpose of discovering the user's financial information. It does this by taking over a computer's system resources. In larger systems, Trojans create denial-of-service attack which aims to make a machine or network resource unavailable to those attempting to access it. Trojans such as CryptoLocker, managed to procure an estimated US\$3 million before it was taken down by authorities, and CryptoWall, was estimated by the US FBI to have accrued over \$18m by June 2015 (Ward 2014; Gallagher 2015). Some examples of Trojans include the following:

- **Ransomware Trojan:** A ransomware trojan attack infects the system, encrypts the files, and then demands payment from its victims. One of the most infamous (discovered in May 2005) is the PGPcoder Trojan. The PGPcoder was originally propagated via malicious websites which exploited the HTML Help Vulnerability (MS04-023) in order to infect susceptible systems with a downloader Trojan. The downloader Trojan installed the PGPcoder Trojan which encoded files on local and mapped drives, then demanded \$200 be paid to obtain a decryption key.
  - **Cryzip Trojan:** The Cryzip Trojan was first discovered in March 2006. Cryzip stores documents found on the infected system in a password-protected zip file and extorts \$300 in ransom money in order to allow those infected to regain access to their files.
  - **Trojans used for DDoS (Distributed Denial of Service) attacks:** The more traditional remote access Trojan has always played a key role in DDoS attacks and many of these DDoS attacks are done for ransom. Victims are generally eCommerce sites that fall into gambling, gaming, or banking/payment categories. After the initial ransom payment, further demands are typically made with amounts increasing dramatically up to tens of thousands of dollars. Many victims are reluctant to risk media exposure and thus this type of crime tends to go largely unreported.
  - **Password Stealers:** Password stealing trojans harvest login credentials for systems, networks, FTP, email, games, as well as banking and ecommerce sites. Many password stealers can be repeatedly custom configured by attackers after they have infected the system.
6. **Rootkit/Bootkit:** This is the hardest of all malware to detect and therefore to remove requiring a complete formatting of the hard drive. Rootkits are designed to permit the other information gathering malware to gather identity information from the user's computer without being detected. Bootkits infect flash BIOS, causing the malware to be loaded even prior to the OS. Combined with rootkit functionality, the hybrid bootkit can be almost impossible for non-experts to detect and remove.
  7. **Backdoors:** Backdoors are similar to Trojans or worms except that they open a "backdoor" onto a computer, providing a network connection for hackers or other malware to enter or for viruses or spam to be sent.
  8. **Keyloggers:** Records everything the user types on their computer or mobile device in order to obtain log-in names, passwords, and other sensitive information, and send it on to the source of the keylogging program. Keyloggers can also be used by corporations to acquire computer usage information. Some keyloggers are sold as commercial software e.g. for a parent to record their children's online activities, or this could also be used by a suspicious spouse to keep tabs on their partner's online activities.

9. **Rogue security software:** This software is designed to deceive or mislead users by appearing to be genuine bona fide software to combat and remove malware, but instead it is the malware. It could disable any real anti-virus software leaving the user's computer completely vulnerable to cyber-attack.
10. **Browser hijacker:** This dangerous malware redirects the user's normal search activity and gives results the developers want you to see. Its intention is to make money off your web surfing allowing the source developers to capture user interests. This is especially dangerous when banking or shopping online. These homepages can look harmless, but in allow other more infectious malware to enter the user's system (Malwaretruth.com; Landesman).

## Symptoms of Malware

Some common symptoms of having malware are the following:

- **Browser crashes & instabilities**
  - Browser closes unexpectedly or stops responding.
  - The home page changes to a different Web site and cannot be reset.
  - New toolbars are added to the browser.
  - Clicking a link does not work or you are redirected to an unrelated Web site.
- **Poor system performance**
  - Internet connection stops unexpectedly.
  - Computer stops responding or takes longer to start.
  - Applications do not open or are blocked from downloading updates (especially security programs).
  - New icons are added to desktop or suspicious programs are installed.
  - Certain system settings or configuration options become unavailable.
- **Advertising**
  - Ads pop up even when the browser is not open.
  - Browser opens automatically to display ads.
  - New pages open in browser to display ads.
  - Search results pages display only ads (UMass Amherst).

## Combatting Malware Infections

These are some steps to take if you think your system is infected with malware:

1. **Back up your personal files:** Hopefully you have already been backing up your files. But you can still copy your personal files elsewhere just to be safe. However, backing up everything on your infected computer could risk saving some infected files.
2. **Disconnect from the Internet:** Disconnecting from the Internet should be one of the first things you do in order to battle any form of malware. Unplug the Ethernet cable, or if on a wireless connection, disabling WiFi on the infected device.



Your Cybersecurity Partner

3. **Boot in safe mode or with a live antivirus rescue disk:** By booting in safe mode, you can prevent any non-core components from running, allowing you to isolate problems easier. If your operating system will not start at all, you can use an antivirus rescue disk. These are available for free from many antivirus companies such as Kaspersky, Avira, AVG, and others.
4. **Get another computer with internet access:** You will more than likely need the aid of another reliable computer connected to the Web in order to resolve your malware problems. This is because you will need to research the problems and symptoms of the specific infection, as well as download various programs to remove the infection. When you download any executable programs on the clean computer, you will also need a way to transport them to the infect computer, such as a flash drive, SD card or portable hard drive.
5. **Identify the malware and search for fixes:** Research the kind of malware with which your computer is infected. There are articles and forums all over the Web that address all kinds of malware infections. Start with a basic search based on the little information you know about the infection. Ideally, you'll find instructions to walk you through the process for ridding your computer of the malware.
6. **Scan with multiple programs until no infections are found:** There are a variety of tools that one can use to remove infections from antivirus software, rootkit removers, anti-adware and anti-spyware to general anti-malware programs. Some well-known tools include the Kaspersky TDSSKiller for removing rootkits, Malwarebytes' Anti-Malware and HitmanPro for removing all kinds of malware, and AdwCleaner for removing adware.
7. **Clean Up temporary files and worthless programs:** Once the infectious files are removed, the remaining files should be cleaned. This can be done using software such as CCleaner, IObit's AdvancedCare, System Ninja, Xleaner or DriveTidy. It would also be a good time to use an app such as GeekUninstaller to remove unneeded or potentially risky software on your computer.

- 8. Remove system restore points:** Although System Restore can be very helpful, system restore points have the potential to contain malware, so it is recommended to delete restore points to ensure that all traces of malware are removed from your computer. If you know for sure when you contracted the malware, you can remove the restore points up to that time. However, to be safe, they should all be deleted.

*According to RedSocks Labs, over 13 million new malicious files were analysed in March 2016 which is a 3 million increase compared to February 2016 (Redsocks Labs 2016).*

- 9. Fix post-malware removal problems:** If there are additional problems that you encounter after you remove the infections from your computer, some options including using software such as Microsoft's Fix It or Re-Enable II (Couch 2013).

## Malware Protection

No protection is absolute but a combination of personal awareness and well-designed protective tools will make your computer as safe as it can be. Take the following steps:

1. Be vigilant: E.g. If you get an email asking you to click on a link or open a file – only do so if you had pre-arranged to receive that type of email. IE password reset request or someone sending you a file you had asked for.
2. Use a robust antivirus software package. This is the primary component of technological defenses that every personal and business computer system should have. This software should do the following:
  - check all newly downloaded programs to ensure that they are malware-free
  - conduct periodic scans of the computer to detect and defeat any malware
  - automatically be updated with the latest virus definitions to recognize the latest threats
  - recognize and warn against malware threats
  - detect and warn against suspicious websites, especially those that may be designed for “phishing” (a technique that tricks users into entering passwords or account numbers)
  - be user friendly (Kaspersky).



Your Cybersecurity Partner

## References

- Couch, Aaron. 2013. "<http://www.makeuseof.com/tag/10-steps-to-take-when-you-discover-malware-on-your-computer/>." *10 Steps To Take When You Discover Malware On Your Computer*. August 27. Accessed July 20, 2016. <http://www.makeuseof.com/tag/10-steps-to-take-when-you-discover-malware-on-your-computer/>.
- Gallagher, Sean. 2015. "FBI says crypto ransomware has raked in >\$18 million for cybercriminals." *Arstechnica*. June 25. Accessed July 20, 2016. <http://arstechnica.com/security/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/>.
- Kaspersky. n.d. "What is Malware and How to Defend Against It?" *Kaspersky*. Accessed July 13, 2016. <http://usa.kaspersky.com/internet-security-center/internet-safety/what-is-malware-and-how-to-protect-against-it#.V4ZQcfrKzc>.
- Landesman, Mary. n.d. "Most Damaging Malware." *About Tech*. Accessed July 20, 2016. <http://antivirus.about.com/od/virusdescriptions/tp/worstvirus.htm>.
- Malwaretruth.com. n.d. "The Truth About Malware." *Malwaretruth.com*. Accessed July 15, 2016. <http://www.malwaretruth.com/the-list-of-malware-types/>.
- Redsocks Labs. 2016. "<http://www.redsocks.nl/blog-2/malware-statistics-march-2016/>." *RedSocks Labs: Malware Statistics March 2016*. April 5. Accessed July 20, 2016. <http://www.redsocks.nl/blog-2/malware-statistics-march-2016/>.
- UMass Amherst. n.d. "Malware: Viruses, Spyware, Adware & Other Malicious Software." *UMass Amherst*. Accessed July 15, 2016. <http://www.umass.edu/it/security/malware-viruses-spyware-adware-other-malicious-software>.
- Ward, Mark. 2014. "Cryptolocker victims to get files back for free." *BBC*. August 6. Accessed July 20, 2016. Cryptolocker victims to get files back for free.