Measures infected machine. nowadays, cybercriminals are using

Business, Marketing

MEASURES TO MITIGATE MALWAREBA63273 G3 Information Systems Security BYSWATE TIROMALACHETTYID-548924CAMPBELLSVILLE UNIVERSITY IntroductionNetworks of machines are infected with malicious software are widely treated as a security threat. Measures to mitigate the infected machine are useful but they are inefficient to solve the overall problem. Recent studies have shifted attention to Internet Service Providers (ISPs). Since most of the spam is sent through botnets, the origin of spam messages provides us with a proxy for detecting infected machine. Nowadays, cybercriminals are using malware to target employees in the enterprise instead of consumer desktops.

Some factors like employee mobility and the use of social networks are contributing to the increasing exposure of corporate networks to malware. RSA points out that advanced persistent threats and other types of attacks have the potential to compromise sensitive data and lead to a data breach. The first step to mitigate any malware effects would be to perform malware analysis. Some of the reasons to analyze a malicious program are listed below:· To assess damage from an intrusion.

· To discover indicators of compromise that will reveal other affected machines which have been affected by the same malware.· To identify the vulnerability that allowed the malware to get there in the first place · To identify the intruder that is responsible for installing the malware Static analysis TechniquesStatic analysis is generally safer than dynamic analysis, since the code isn’t running we don’t need to worry about it deleting files, calling home, or stealing data. Generally, the only risk involved in static analysis is the risk of accidentally double-clicking or otherwise accidentally running the malware. Some of the techniques are as below. File Fingerprinting: Compute a cryptographic hash value for each file under investigation. Most widely used and secure hash functions are MD5, SHA1 or SHA256. Virus scanningAnti-virus software's can recognize a well-known malwares and will provide analysis describing it. This analysis may provide only minimal details or it can be through on its capabilities and instructions to remove.

Packer DetectionPackers can be detected using PEiD program. It has definitions for over 600 different packers. We simply open a file with PEiD program to detect packers. PEiD would try to match basic signature of a PE file to known compilers and packers. DisassemblyUse IDA Pro for malware analysis and reverse engineering. A disassembler like IDA Pro and Ollydg debugger can be powerful combination for malware analysis. Dynamic analysis techniquesIn Dynamic analysis, we run the malware in a controlled and logically partitioned host and observe its actions. Process Monitor and Wireshark can be used for monitoring malware interaction with the network and file system.

These tools monitor the entire machine rather than actions of single malware program. It is important that we differentiate normal system background activity and malware activity we are examining. Process Monitor installs device driver to capture kernel activity of the system being monitored. Setting up accurate filters is key in using Processes Monitor effectively.

Use Wireshark for analyzing and filtering network traffic. Mobile Malware: Malicious software that is designed specifically to target a mobile device like a tablet or smart phone in order to damage or disrupt a target device. The objectives of mobile malware can range from spying to key logging, from text messaging to phishing or from unwanted marketing to outright fraud. It can be classified into four types: Spyware and Adware: Spyware secretly gathers confidential information about the mobile users and relaysthis data to the third party. Spyware uses the victim’s mobile connection to relay personal information like contacts, location, message habits, browser history, downloads and user preferences. Trojans and Viruses: Mobile Trojans infect user devices by attaching themselves to seemingly harmlessor legitimate programs installed with the app to carry out malicious actions. Trojans are closely related to mobile viruses.

Phishing Apps: Attackers are now creating mobile phishing apps that look like legitimate services but may steal sensitive information and credentials to perform financial fraud. One such example is a fake security app for Facebook, which claimed to secure user’s Facebook account but in reality stole user’s information for identity theft. Bot Processes: Mobile malware is getting more advanced with programs that work in the foundation on the user devices, disguising themselves and lying in wait for certain behaviors. Hidden processes could run executables by being completely invisible to the user. Symptoms: Signs of malware infection can be like unwanted behaviors and degradation of device performance.

It could also reduce the battery life, processing power and freeze the device entirely. Mobile Malware Detection TechniquesApplication Permission analysis: At the time of installation of the application, Android platform requests the user to grant or deny permissions based on the activities the application can perform. Kirin security service extracts its security configuration and checks them against the security policy rule it has. If an application fails to pass all the security rules, it can either delete the app or alert the user. Cloud-Based Detection: Paranoid Android is a cloud-based malware protection technique that doessecurity analysis and computations on a remote server that hosts multiple replicas ofmobile phones running on emulators. Crowdroid is a lightweight client application that monitors system calls invoked by the mobile application, which then preprocesses the calls, and sends them to the cloud where clustering techniques help the user to determine whether the application is malicious.

Battery Life Monitoring: VirusMeter methodology detects anomalous behavior by abnormal power consumption. The idea is to detect any malicious activity that would consume more battery. VirusMeter monitors the activities in the phone and uses APIs provided by the mobile platform to collect the remaining battery capacity. Protecting against Vulnerabilities: Update your operating system, browsers, and plug-in: Updates to operating systems, browsers, and plug-ins are often released to patch any security vulnerabilities discovered.

To protect against the security flaws we need to make sure the mobile phone software is updated regularly as well.   Enable click-to-play plugins: Click-to-play plugins keep Flash or Java from running unless you specifically tell them to (by clicking on the ad). The bulk of malicious advertising or malicious ads rely on exploiting these plugins and hence we need to enable this feature. Use strong passwords and/or password managers. A strong password is long, is not written down anywhere, is changed often, and isn't tied to personal information and is also not repeated for different logins. Remove software you don't use: Take a look at other legacy apps on your computer like Adobe Reader and if you're not using them, best to remove. Read emails with an eagle eye: Check the sender's address and read the language of the email carefully. Finally, know the typical methods of communication for important organizations.

Cybercriminals also like spoofing banks via SMS/text message or fake bank apps and we can mitigate the risk by reaching out to bank directly. Use firewall, antivirus, anti-malware and anti-exploit technology: The firewall and antivirus programs will detect and block the known viruses. Meanwhile, the anti-malware software can ward off sophisticated attacks from unknown agents, stopping malware infection in real time and shielding vulnerable programs from exploit attack. Log out of websites after you're done: We are always vulnerable if we don't log out, especially while using a public computer or on a public network. It's not enough to just close the browser tab or window since attackers could access login information from session cookies and sign into a site. Conclusion: Security professionals agree on a multi-layer approach, which is using not only multiple layers of security technology but also user awareness that helps us protected from cybercriminals and your own mistakes. In a world where almost everything can be controlled from a Smartphone, it is very essential that an individual’s personal information is not easily compromised. To some extent users can take some simple steps like using security software in conjunction with not clicking on suspicious links or providing personal information on suspicious sites or checking for SSL certificate when entering.

ReferencesZamora, W. (2017). 10 easy ways to prevent malware infection – Malwarebytes Labs. online Malwarebytes Labs. Available at: https://blog.

malwarebytes. com/101/2016/08/10-easy-ways-to-prevent-malware-infection/Rand, D. (2010). The role of internet service providers in botnet mitigation an empirical analysis based on spam data. Retrieved on 23November 2017 from http://ns2.

humantech. dc. hu/~mfelegyhazi/courses/EconSec/readings/08_VanEeten2010roleISP. pdfMalware Threats and Mitigation Strategies . US-CERT , 23November 2017, www.

us-cert. gov/sites/default/files/publications/malware-threats-mitigation. pdf.

Musthaler, L. (2011, March 21). Best practices for stopping malware and other threats. Retrieved November 24, 2017, from https://www.

networkworld. com/article/2201551/smb/best-practices-for-stopping-malware-and-other-threats. html (n. d.).

Retrieved November 24, 2017, from https://msdn. microsoft.

com/en-us/library/cc875818. aspx