DOWNLOAD PDF MOBILE MALWARE MITIGATION MEASURES.

Chapter 1 : Recon GPUs for Mobile Malware, Mitigation and More

The chapter provides a model by which one can evaluate the risk of the mobile device and identify which defensive measures are the most appropriate. The risk model was based primarily on the nature of use of the device, the use model, and the type of information and access stored on it.

A mobile malicious software mitigation component is provided that obtains an internet protocol address that is exhibiting malicious software behavior, a profile of the malicious software behavior, and a time of the malicious software behavior. The malicious software mitigation component can determine an identity of a mobile device that was assigned the internet protocol address during the time it was exhibiting malicious software behavior, and transmit the profile to the mobile device. In addition, the malicious software mitigation component determine if the duration of the assignment of the internet protocol address to the mobile device is sufficient for positive identification. Technological advances have provided significant increases in the computing power and networking capabilities of mobile devices. For instance, a number of smart phones and personal digital assistants PDA currently run full-fledged operating systems, employ powerful processors, and have broadband connectivity to the internet that rivals desktop computers and laptops. The technical capabilities of these devices have made them appealing to professionals, students, and casuals users alike. This broad appeal has resulted in a large user base that is non-technical in nature, and has little understanding of digital security threats, which makes the ever more powerful mobile devices an attractive target for cyber criminals. In particular, malicious software infecting mobile devices is a growing concern for mobile device users and wireless network administrators. Since these devices are ubiquitous and are expected to outnumber personal computers in the near future, they are high-value targets for cyber criminals intending to control, own and rent them for cyber criminal activities. A compromised mobile device can cause serious issues for both the user and the associated communication infrastructure. Accordingly, it would be desirable to implement techniques for effectively mitigating malicious software malware in mobile devices and wireless communication systems. The above-described deficiencies of wireless systems with respect to malware are merely intended to provide an overview of some of the problems of conventional systems and techniques, and are not intended to be exhaustive. Other problems with conventional systems and techniques, and corresponding benefits of the various non-limiting embodiments described herein may become further apparent upon review of the following description. SUMMARY The following presents a simplified summary of the disclosure in order to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is intended to neither identify key or critical elements of the invention nor delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented later. Systems and methods are provided for the mitigation of mobile malicious software malware. A malware detection engine can analyze data traffic and data flows on a network, and employ a plurality of techniques to identify internet protocol IP addresses that are suspected of engaging in malware behavior. The malware detection engine can generate traffic profiles of the suspected malware behavior, and forward the IP addresses and traffic profiles to a malware mitigation component. The malware mitigation component can leverage logging mechanisms available to core mobility network elements to identify devices associated with the IP addresses, and forward the traffic profiles to the identified devices. Upon receipt of the traffic profile, individual devices can correlate data traffic on the devices to the traffic profiles in order to identify one or more applications on the devices responsible for the suspected malware behavior. The devices can remove the applications, or take other mitigating actions, such as selectively dropping data packets generated by the applications. In accordance with one aspect, a method is provided for malicious software mitigation in a wireless network that includes the steps of receiving an internet protocol address that is exhibiting malicious software behavior, and a profile of the malicious software behavior being exhibited, comparing the internet protocol address to a set of mobility logs maintaining information about activities of a set of devices associated with the wireless network, and determining an identity of a device associated with the internet protocol address based on the comparing. In accordance with another aspect, a system is provided that includes an alert acquisition component configured to receive an internet protocol address that is engaging in malicious software behavior, a profile of the malicious software behavior, and a time frame when the internet protocol address was engaging in the malicious software behavior, a correlation component configured to analyze a set of logs that maintain records regarding activities of a set of devices associated with the wireless network, and configured to determine an identifying characteristic of a mobile device that was assigned the internet protocol address during the time frame the internet protocol address was engaging in the malicious software behavior, and a communication component configured to send the profile to the mobile device. In accordance with yet another aspect, a method is provided for botnet mitigation in a wireless network that includes the steps of obtaining, from a core network, an internet protocol address that is exhibiting bot behavior, a profile of the bot behavior, and a time when the internet protocol address was exhibiting the bot behavior, analyzing a set of mobility logs maintaining internet protocol address assignments by a mobility network and determining that at least one device in a set of devices associated with the wireless network was assigned the internet protocol address at the time the internet protocol address was exhibiting the bot behavior, determining an identity of the at least one device based on the analyzing, and communicating the profile to the at least one device. To the accomplishment of the foregoing and related ends, the invention, then, comprises the features hereinafter fully described. The following description and the annexed drawings set forth in detail certain illustrative aspects of the invention. However, these aspects are indicative of but a few of the various ways in which the principles of the invention may be employed. Other aspects, advantages and novel features of the invention will become apparent from the following detailed description of the invention when considered in conjunction with the drawings. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It may be evident, however, that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate describing the present invention. The entities disclosed herein can be either hardware, a combination of hardware and software, software, or software in execution. By way of illustration, both an application running on a server and the server can be a component. Also, these components can execute from various computer readable media having various data structures stored thereon. The foregoing terms are utilized interchangeably in the subject specification and related drawings. It should be appreciated that such terms can refer to human entities or automated components supported through artificial intelligence e. The network includes a core network , a mobility network , and a plurality of mobile devices The core network can have a plurality functions including, but not limited to, session management, and transport for data packets in the network The core network is also referred to as the backbone network, in part, because it connects the mobility network to the Internet. For example, the core network can be comprised of a wired internet protocol IP network where both wired traffic and wireless or mobility traffic traversing the internet flows. Virtually all data transacted on the mobility network e. The mobility network can have a plurality of functions including, but not limited to, enabling access to the network by the mobile devices , allocating network resources e. Mobility management can include, but is not limited to, tracking the location of the mobile devices , and enabling: The mobility network can include a plurality of base stations or access points not shown that enable the mobile devices to communicate with a plurality of devices on the Internet, wherein the traffic is carried by the core network The mobile devices can include, but are not limited to, tablet computers, smart phones, mobile phones, netbooks, portable music players, personal digital assistants PDAs , laptops, electronic book devices, global positioning systems GPS , and so forth. The enhanced connectivity and technical capabilities of mobile devices can leave them vulnerable to malicious software malware , including malicious bots controlled by cyber criminals. The malware can attack various functionality or memory sectors of the mobile devices , or can integrate compromised mobile devices into a botnet, wherein the malware interacts with other compromised devices to form a small network, so that they can attack targets cooperatively discussed below. Malware can include but is not limited to computer viruses, worms, Trojan horses, spyware, adware, scareware, crimeware, rootkits, key loggers, and botnets. Turning now to FIG. The botnet includes a plurality of compromised mobile devices

When the mobile devices are compromised, the malware can integrate the compromised mobile devices into the botnet Each of the compromised mobile devices can be controlled by a set of command and control servers It is to be appreciated that the set of command and control servers can be comprised of a single command and control server. Typically, the set of command and control servers are operated by a user acting as a bot master. For example, the bot master can issue commands to the compromised mobile devices , via the set of command and control servers , to generate spam messages directed toward a set of remote targets It can be desirable for a bot master to generate spam using a large number of compromised mobile devices , as opposed to a single source, in order to escape detection. As an additional example, the bot master can issue commands to the compromised mobile devices , via the set of command and control servers , to execute a denial of service DoS attack against the set of remote targets During a DoS attack, essentially, the bot master will use the compromised mobile devices to saturate the set of remote targets e. Additionally or alternatively, the compromised mobile devices can be arranged in a peer-to-peer bot network P2P botnet. In the P2P botnet, there is not a command and control server ; rather, each compromised mobile device is both a server and a client. The bot master can inject commands at any point in the P2P botnet, and the commands are disseminated among the compromised mobile devices using a peer-to-peer P2P communication protocol. The malicious software malware mitigation system includes a malware detection component , a malware mitigation component , and a malware defense component The malware detection component operates, functions, or otherwise executes in the core network The term core network as used herein can refer to the core network , or an edge of the network , where the core network connects to the mobility network The malware detection component can identify, recognize, or otherwise detect a set of IP addresses behaving in a manner consistent with a malware infection e. If the bot is an internet relay chat IRC bot, then the traffic profile of the bot can include sending traffic on a specific IRC port. Additionally or alternatively, the malware detection component can detect data flows from a bot on a compromised mobile device to a known command and control server See FIG. Additionally or alternatively, the malware detection component can detect peer-to-peer botnets in the mobility network The malware detection component can provide information relating to detected malware, including IP addresses, and traffic profiles, to the malware mitigation component The malware mitigation component operates, functions, or otherwise executes in the mobility network As discussed supra, the functionality of the mobility network can include, but is not limited to, allocating network resources e. The mobility network can include a mobility component that tracks mobility information, such as an assigned IP address, physical location, and so forth of the mobile device The responsibilities of the SGSN can include, but are not limited to, delivery of data packets to and from mobile devices within its geographical service area, packet routing and transfer, and authentication and charging functions. The GGSN can be responsible for maintaining current location information for the mobile device , and maintaining routing data necessary to tunnel data to the SGSN that services the particular mobile device It is to be appreciated, that the aspects described herein are not limited to 2G or 3G networks, but can also be employed on various other communications networks, including, but not limited to, fourth generation 4G wireless communication networks, such as those complying with the long term evolution LTE standards. In a wireless network the mobile device can be assigned a virtually unique IP address for different communication sessions. For example, the mobility component can assign the mobile device a disparate IP address for each data request from the mobile device The IP address may be selective assigned from a set of available IP addresses at the time of assignment. Typically, an individual mobile device will have a unique IMEI associated only with that mobile device In addition, a mobile subscriber, typically, will have a unique IMSI that is associated only with the individual mobile subscriber and provisioned on a mobile device, for example, via a SIM card. The malware mitigation component can correlate the suspect IP addresses with the mobility logs maintained by the General Packet Radio Service Support Nodes e. The malware mitigation component can transmit, send, or otherwise communicate a warning message to the malware defense component on the suspect mobile device The malware mitigation component can determine a physical location of the mobile device , and communicate with the mobile device via the mobility component The malware defense component operates, functions, or otherwise executes in kernel space of the mobile device The malware defense component can correlate the flow of data in the kernel space of the mobile device to the traffic profile included in the warning message in order to indentify, locate, or otherwise determine an application or binary that is generating the information contained in the traffic profile. When the malware defense component has identified the application or binary related to the traffic profile the malware defense component can remove, delete, or otherwise erase the application or binary from the device. Additionally or alternatively, the malware defense component can prompt a user to inform them that the binary or application is behaving as malware, and allow the user to determine to remove, delete, or otherwise the erase the application or binary from the device. If the user determines not to remove the binary or application behaving as malware, the malware defense component can perform additional mitigating actions including, but not limited to, selectively dropping packets originating from the binary or application behaving as a malware. For instance, a user may have downloaded a plurality of games from the same publisher, wherein each game is infected with the same bot. It is to be appreciated that the malware defense component can additionally or alternatively operate on a wired device not shown , wherein the malware defense component operable on a wired device can obtain the warning message from the malware detection component or the malware mitigation component The malware detection component includes an analysis component , a profile generation component , and an alert component The analysis component analyzes data in the core network or at the edge of the network where the core network connects to the mobility network see FIG. In addition, the analysis component can determine if the suspect IP addresses are part of or associated with the mobility network See FIG. The analysis component can detect the existence of malware in the network via a plurality of techniques. For instance, the analysis component can start with information related to one or more pieces of malware previously known to be residing in the network , and can identify data traffic and data flows that are similar to the data traffic and data flows generated by the known malware. In addition, where the malware includes a botnet or similar software, the analysis component can follow data traffic to a known command and control server See FIG. Additionally, the analysis component can employ cluster analysis and single out groups of IP addresses that behave in a similar manner that might be indicative of malware, such as scanning the network , sending spam messages, etc.

Chapter 2 : Mobile Malware Attacks and Defense - Ken Dunham - Google Books

Mobile malware consistently increasing To nearly no one's surprise, the recent McAfee Labs Threat Report found that mobile malware is on the rise. According to Forbes, this is the fifth quarter in a row where these findings have been confirmed, illustrating an overall pattern in the industry.

Hereby issued to you, please realistically and effectively implement and carry out. The Ministry of Industry and Information Technology MIIT shall be responsible for organizing and developing national public internet cybersecurity threat monitoring and mitigation work. Communications authorities of provinces, autonomous regions, municipalities shall be responsible for organizing and developing public internet cybersecurity threat monitoring and mitigation work in their respective administrative areas. Ministry of Industry and Information Technology and provincial, autonomous region, and municipal Communications Authority are hereafter collectively referred to as principal telecommunication departments. Cybersecurity threat monitoring and mitigation work shall adhere to the principle of timely, discovery, scientific identification, and effective mitigation. Relevant professional organizations, basic telecommunication companies, cybersecurity companies, Internet companies, domain name registration management and service organs shall strengthen the monitoring and disposal of cybersecurity threats, specify responsible departments, responsible persons and contact persons, strengthen the establishment of relevant technical measures, and constantly improve the timeliness, accuracy, and effectiveness of cybersecurity threats to monitoring and mitigation. Article 6 After cybersecurity threats are discovered by relevant professional organizations, basic telecommunication enterprises, cybersecurity enterprises, Internet companies, domain name registration management and service organs, etc. The Ministry of Industry and Information Technology will establish cybersecurity threat information sharing platform, unified collection, storage, analysis, notification, release network security threat information; formulate relevant interface specifications, and develop interoperability with related cybersecurity monitoring platforms. The principal telecommunication departments shall entrust CNCERT, China Information Communications Research Institute, and other specialized organs to identify threat information submitted by relevant units and issue mitigation recommendations. Identification work shall be carried out under the principles of scientific rigor, just, fair, timely, and effective. Principal telecommunication departments shall strengthen the management and training of professional organs and personnel involved in identification work. After the identification and mitigation recommendation has been approved by principal telecommunication organs, they may take the following mitigation measures for network security threats: Mitigation notices from principle telecommunications departments must be sent to relevant units in written or verifiable electronic sources. In emergency circumstances, it is permissible to first make a telephone notice, then later supplement with a written notice. Basic telecommunication companies, internet companies, domain name registration management and service organs, etc, shall provide technical support and assistance for principal telecommunication organs inquiries into IP address attribution, domain name registration, and other information, and in accordance with notices from principal telecommunications departments and time limitations adopt mitigation measures and provide feedback on mitigation results. Specialized organization responsible for identifying cybersecurity threats shall be responsible for conducting verification of relevant mitigation situations. Where a relevant organization or individual is dissatisfied with the mitigation measures taken in accordance with Article 8 1 of the present Measures, it shall have the right to appeal within 10 working days to the principal telecommunication departments that issued the mitigation decision. Relevant telecommunications departments shall promptly organize and investigation after receiving the complaint and reply within ten working days. Relevant units shall be encouraged to carry out cybersecurity threat monitoring and mitigation work in the form of industry self-discipline, technical cooperation, or technical services, and shall be responsible for handling mitigation, monitoring and mitigation results shall be reported to principal telecommunications organs in a timely manner. Where a basic telecommunications companies, internet companies, domain name registration management and service organ, etc. Monitoring and mitigation work of public internet cybersecurity emergencies that cause or may cause serious social harm or influence shall be carried out in accordance with relevant emergency plans of the State and principal telecommunications departments. Communications authorities of provinces, autonomous regions, municipalities may, in accordance with these Measures, formulate detailed rules for implementation of cybersecurity threat monitoring and disposal within their respective administrative regions. These Measures shall come into force on January 1,

Chapter 3 : Public Internet Cybersecurity Threat Monitoring and Mitigation Measures Â« China Copyright a

Stay ahead with the world's most comprehensive technology and business learning platform. With Safari, you learn the way you learn best. Get unlimited access to videos, live online training, learning paths, books, tutorials, and more.

Chapter 4 : Buy Mobile Malware Attacks and Defense - Microsoft Store

** Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. * Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks * Analyze Mobile Device/Platform Vulnerabilities and Exploits * Mitigate Current and Future Mobile Malware Threats.*

Chapter 5 : Mobile Malware Attacks and Defense - O'Reilly Media

Share Mitigating Malware in a Modern, Mobile World on Twitter Share Mitigating Malware in a Modern, Mobile World on Facebook Share Mitigating Malware in a Modern, Mobile World on LinkedIn.

Chapter 6 : Memeo :: Top BYOD security risks and mitigation strategies: Mobile malware, missing devices

Malware has gone mobile, and the security landscape is changing quickly with emerging attacks on cell phones, PDAs, and other mobile devices. This first book on the growing threat covers a wide range of malware targeting operating systems like Symbian and new devices like the iPhone.

Chapter 7 : How to mitigate 85% of threats with only four strategies | Securelist

** Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. Key Features Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks.*

Chapter 8 : USA1 - Mobile malicious software mitigation - Google Patents

Mobile malware poses a major threat to enterprises, their customers and employees, and each of us as individuals â€” but there are ways to fight back.