Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

WildFire: Automatically Detect and Prevent Unknown Threats

[1]G. Bala Vasavi Krishna, [2]B. Rajesh
[1](M.Tech) –CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Andhra Pradesh, India
[2]Assistant Professor, Dept of IT, Vasireddy Venkatadri Institute of Technology (VVIT), Andhra Pradesh, India

Abstract: Delay tolerant networks (DTN) utilize the mobility of node and opportunistic contact among nodes for data communication. Due to limitation in resources such as buffer space and contact opportunity, DTNs are vulnerable to malware based attack. So the proposal introduces a novel malware detection technique in DTN is Wildfire it has a unified public/private cloud-based architecture that maximizes the sharing of threat intelligence while minimizing hardware requirements. it simplifies an network response to the most dangerous threats, automatically detecting unknown malware and quickly preventing threats before an activity is determined. Unlike legacy security solutions, Wildfire quickly identifies and stops these advanced attacks without requiring manual human intervention. The service brings advanced threat detection and prevention to every security platform deployed throughout the network Wildfire can also detect unknown malware pervasively throughout the network.

Keyword: Delay-tolerant networking DTN, WildFire

I. INTRODUCTION

Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments or planned networks in space. Recently, the term delay-tolerant networking has gained prevalence in the United States due to support from DARPA, which has funded many DTN projects. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise. Protocols using bundling must leverage application-level preferences for sending bundles across a network. Due to the store and forward nature of delay-tolerant protocols, routing solutions for delay-tolerant networks can benefit from exposure to application-layer information. For example, network scheduling can be influenced if application data must be received in its entirety, quickly, or without variation in packet delay. Bundle protocols collect application data into bundles that can be sent across heterogeneous network configurations with high-level service guarantees. However, when instantaneous end-to-end paths are difficult or impossible to establish, routing protocols must take to a "store and forward" approach, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination[4][5][6]. A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination[7]. This is feasible only on networks with large amounts of local storage and internodes bandwidth relative to the expected traffic. In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities. In others, where available storage and internodes throughput opportunities are more tightly constrained, a more discriminate algorithm is required.

The Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware. The viable communication with mobile consumer electronics equipped with short range communication technologies such as Bluetooth, Wi-Fi Direct is DTN. There exists a general behavior characterization of proximity malware based on Naive Bayesian model, It was identified with two unique challenges for extending Bayesian malware detection to DTNs (Delay Tolerant Networks). So we propose a simple and effective method “look ahead”, to address the challenges with two extensions to look ahead, dogmatic filtering, and adaptive look ahead, they address the challenge of “malicious nodes sharing false evidence.” Real mobile network traces are used to verify the effectiveness Advanced attacks is not point-in-time events. Adversaries deliver attacks persistently, often using non-standard ports, protocols or encryption for subsequent attack stages. Like Palo Alto Networks Next-Generation Firewall, WildFire provides complete visibility into unknown threats within all traffic across thousands of applications, including Web traffic, email protocols (SMTP, IMAP, POP), and FTP, regardless of ports or encryption (SSL).WildFire simplifies an organization’s response to the most dangerous threats, automatically detecting unknown malware and quickly preventing threats before an enterprise is compromised. Unlike legacy security solutions, WildFire quickly identifies and stops these advanced attacks without requiring manual human intervention or costly Incident Response (IR) services after the fact.

II. RELATED WORK

Effective and Efficient Malware Detection at the End Host

Most Internet issues like spam e-mails and denial of service attacks have malware as their underlying cause. That is, computers that are compromised with malware are typically networked along to make botnets, and lots of attacks are

launched victimization these malicious, attacker-controlled networks. With the increasing significance of malware in net attacks, a lot of analysis has focused on developing techniques to gather, study, and mitigate malicious code. Doubtless, it's necessary to gather and study malware found on the net. However, it's even a lot of necessary to develop mitigation and detection techniques supported the insights gained from the analysis work. Current host-based detection approaches (i.e., anti-virus software) suffer from ineffective detection models. These models think about the options of a selected malware instance, and are typically simply evadable by obfuscation or polymorphism. Also, detectors that check for the presence of a sequence of instructions exhibited by a malware instance are typically evadable by system call rearrangement. So as to deal with the shortcomings of ineffective models, many dynamic detection approaches are planned that aim to spot the behavior exhibited by a malware family. Though promising, these approaches are sadly too slow to be used as time period detectors on the top host, and that they typically need cumbersome virtual machine technology. This paper planned a completely unique malware detection approach that's each effective and economical, and thus, are often accustomed replace or complement ancient anti-virus package at the top host.

Our approach 1st analyzes a malware program in a very controlled atmosphere to create a model that characterizes its behavior. Such models describe the knowledge flows between the system calls essential to the malware's mission, and so, can't be simply evaded by straightforward obfuscation or polymorphic techniques. Then, we have a tendency to extract the program slices liable for such info flows. For detection, it dead these slices to match our models against the runtime behavior of associate degree unknown program. This experiment showed that our approach will effectively find running malicious code on associate degree finish user's host with a little overhead. Malicious code, or malware, is one amongst the foremost pressing security issues on the net. Today, several compromised internet sites launch drive-by transfer exploits against vulnerable hosts. As a part of the exploit, the victim machine is often accustomed transfer and executes malware programs. These programs are typically bots that work and switch into a botnet. Botnets are then employed by miscreants to launch denial of service attacks, send spam mails, or host scam pages. The malware threat and its prevalence, it's not shocking that a big quantity of previous analysis has centered on developing techniques together, study and mitigate malicious code. As an example, there are studies that live the scale of botnets, the prevalence of malicious internet sites, and also the infestation of executables with spyware. Also, variety of server-side and client-side honey pots were introduced that permit analysts and researchers to collect malware samples within the wild.

Additionally, there exist tools that may execute unknown samples and monitor their behavior. Some tools give reports that summarize the activities of unknown programs at the extent of Windows API or system calls. Such reports are often evaluated to search out clusters of samples that behave equally or to classify the sort of determined, malicious activity. Different tools incorporate knowledge flow into the analysis, which ends in a very a lot of comprehensive read of a program's activity within the sort of taint graphs. Whereas it's necessary to gather and study malware, this can be solely a way to associate degree finish. In fact, it's crucial the insight obtained through malware analysis is translated into detection and mitigation capabilities that permit one to eliminate malicious code running on infected machines. Hefty effort was dedicated to the extraction of network-based detection models. Such models are typically manually-crafted signatures loaded into intrusion detection systems or larva detectors. Different models are generated mechanically by finding common tokens in network streams made by malware programs (typically, worms). Finally, malware activity is often detected by recognizing abnormal traffic as an example. Many systems attempt to determine bots by probing for similar affiliation patterns. Whereas network-based detectors are helpful in follow, they suffer from variety of limitations. First, a malware program has several choices to render network-based detection terribly troublesome. The rationale is that such detectors cannot observe the activity of a worm directly however have to be compelled to suppose artifacts (the traffic) that this program produces. as an example, coding are often accustomed thwart content-based techniques, and mixing attacks will modification the properties of network traffic to form it seem legitimate. Second, network-based detectors cannot determine malicious code that doesn't send or receive any traffic. Host-based malware detectors have the advantage that they'll observe the whole set of actions that a malware program performs. It's even doable to spot malicious code before it's dead the least bit. despondently, current host-based detection approaches have been main deficiency.

An important downside is that several techniques suppose ineffective models. Ineffective models are models that don't capture intrinsic properties of a worm and its actions however just devour artifacts of a selected malware instance. As a result, they'll be simply evaded. As an example, ancient anti-virus (AV) programs largely suppose file hashes and computer memory unit (or instruction) signatures. Sadly, obfuscation techniques and code polymorphism create it simple to switch these options while not dynamic the particular linguistics (the behavior) of the program. Another example models capture the sequence of system calls that a selected malware program executes. Once these system calls are freelance, it's simple to vary their order or add moot calls, so unsupportive the captured sequence. In an attempt to beat the restrictions of ineffective models, researchers have wanted ways that to capture the malicious activity that's characteristic of a malware program (or a family). On one hand, this has crystal rectifier to detectors that use subtle static analysis to spot code that's semantically appreciate a malware templet. Since these techniques target the particular linguistics of a program, it's not enough for a malware sample to use obfuscation and polymorphic techniques to change its look.

The matter with static techniques is that static binary analysis is troublesome. This issue is more exacerbated by runtime packing and self- modifying code. Moreover, the analysis is dear, and thus, not appropriate for commutation Jewish calendar month scanners that require to quickly scanning giant numbers of files. Dynamic analysis is another approach to model malware behavior. Specially, many systems suppose the trailing of dynamic knowledge flows (tainting) to characterize malicious activity in a very generic fashion. Whereas detection results are promising, these systems incur a

big performance overhead. Also, a special infrastructure (virtual machine with shadow memory) is needed to stay track of the taint info. As a result, static and dynamic analysis approaches are typically used in machine-controlled malware analysis environments (for example, at anti-virus corporations or by security researchers), however they're too inefficient to be deployed as detectors on finish hosts.

III. DTN SECURITY REQUIREMENT

Authentication

As in standard systems, authentication techniques verify the identity of the DTN nodes in communication and distinguish legitimate DTN users from unauthorized users. In DTN,it is essential for each intermediate node to possess the aptitude to verify that the information was extremely sent by a licensed node, at a legitimate rate or category of service that they're granted. Such AN authentication demand may be provided either on a hop-by-hop or end-to-end basis, betting on completely different security style goals. The privacy objective may be achieved exploitation the end-to-end coding, which needs the presence of mutual authentication and key agreement between the supply and also the destination.

Integrity

Integrity demand ought to make sure that the transmitted messages can't be altered throughout the propagation method in the network it does not reveal the user location.

DTN security characteristics

Lack of End-to-end Connectivity

As a significant characteristic of DTNs, lack of end-to-end property not solely brings challenge to routing however conjointly makes the present security solutions that are well studied in standard networks, not applicable in DTNs.

Fragmentation

In DTNs, every network link becomes on the advertise just for a brief amount of your time. Therefore, once a message is massive it may not possible to send the complete message quickly. One potential answer is to separate the message into smaller items and let every become its own bundle, or "fragment bundle", and send some items of an oversized message through the present link and remainder of the message through another link later to form the simplest use of restricted resources.

IV. LITERATURE SURVEY

- Su et al. collected Bluetooth traces and demonstrated that malware could effectively propagate via Bluetooth with simulations.
- Yan et al. developed a Bluetooth malware model. Bose and Shin showed that Bluetooth can enhance malware propagation rate over SMS/MMS.
- Cheng et al. analyzed malware propagation through proximity channels in social networks.
- Aristides et al. quantified the threat of proximity malware in wide-area wireless networks. Li et al. discussed optimal malware signature distribution in heterogeneous, resource-constrained mobile networks.

V. EXISTING SYSTEM

- Previous researches quantify the threat of proximity malware attack associated demonstrate the chance of launching such an attack, that is confirmed by recent reports on hijacking edifice Wi-Fi hotspots for drive-by malware attack.
- With the adoption of latest short-range communication technologies like NFC and Wi-Fi Direct that facilitate spontaneous bulk knowledge transfer between spatially proximate mobile devices, the threat of proximity malware is turning into a lot of realistic and relevant than ever.
- Proximity malware supported the DTN model brings distinctive security challenges that don't seem to be present within the model.

Disadvantages: Central monitoring and resource limits are absent in the DTN model. So it's extremely risk to collecting evidence. And here it filter the false evidence in sequentially and distributed among system.

PROPOSED SYSTEM:

- Behavioral characterization, in terms of System call and program flow, has been antecedently planned as a good various to pattern matching for malware detection.
- In our model, malware-infected nodes' behaviors square measure discovered by others throughout their multiple opportunist encounters: Individual observations is also imperfect, however abnormal behaviors of infected nodes square measure recognizable within the long.
- I determine the challenges for extending Bayesian malware detection to DTNs, and propose
- Complementing conflagration is that the new optical device service, that provides users with the power to quickly investigate extremely targeted and distinctive attacks, discover the context around them, and correlate them with adversaries and campaigns. optical device provides you unjust intelligence and context

- WildFire simplifies associate organization's response to the foremost dangerous threats, mechanically detection unknown malware associated quickly preventing threats before an enterprise is compromised. not like gift security solutions, conflagration quickly identifies and stops these advanced attacks while not requiring manual human intervention or expensive Incident Response (IR) services when the actual fact.

Advantages: The proposed evidence consolidation strategies in minimizing the negative impact of liars on the shared evidence's quality. It is used to identify the abnormal behaviors of infected nodes in the long-run. WildFire simplifies an organization's response to the most dangerous threats, automatically detecting unknown malware and quickly preventing threats before an enterprise is compromised. Unlike legacy security solutions, WildFire quickly identifies and stops these advanced attacks without requiring manual human intervention or costly Incident Response (IR) services after the fact.

VI. WORKING PRINCIPLE OF PROPOSED SYSTEM

AUTOMATED DETECTION AND PREVENTION

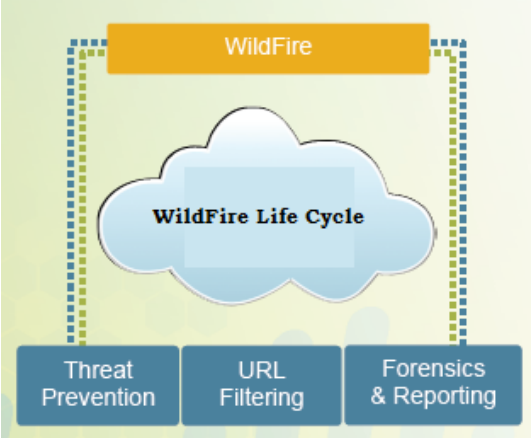

Fig 1. WildFire Life Cycle

The first step is to observe unknown threats, however next you want to mechanically shut the loop to stop them from reaching the network. Once conflagration discovers a brand new threat, the service mechanically generates protections across the attack lifecycle, interference malicious files and command-and-control traffic. Uniquely, these protections square measure content-based, not looking forward to simply modified attributes like hash, computer filename or URL, permitting the service to dam the initial malware and future variants with none extra action or analysis. Conflagration informs the protection of different town Networks security services, interference threats in-line through: conflagration turns unknown threats into best-known, preventable incidents, enabling swift in-line protection and shortening the time between detection and mitigation. Once files square measure confirmed as malicious, protections square measure mechanically created, with complete visibility and management, guaranteeing your organization will observe and forestall attacks conflagration provides the intelligence required to simply investigate suspected infections, like in-depth analysis of all known malware, integration with User-ID™ for fast identification of ill-used users, native visibility into all application traffic via App-ID

VII. CONCLUSION

WildFire simplifies associate organization's response to the foremost dangerous threats, mechanically detection unknown malware associated quickly preventing threats before an enterprise is compromised. not like gift security solutions, conflagration quickly identifies and stops these advanced attacks while not requiring manual human intervention or expensive Incident Response (IR) services when the actual fact. the service brings advanced threat detection and bar to each security platform deployed throughout the network, conflagration provides complete visibility into all traffic — together with advanced threats — across nearly four hundred applications, together with net traffic, email protocols (SMTP, IMAP, POP), and FTP, in spite of ports or coding (SSL).

Obscure malware and apace anticipating dangers before a venture is listed off. Not in the least like gift security arrangements, Fierce blaze apace acknowledges and stops these propelled assaults while not obliging manual human mediation or excessive Episode Reaction (IR) edges when the actual fact. the administration conveys propelled risk discovery and aversion to every security stage sent throughout the system, Out of supervision balefire provides complete deceivability into all movement together with propelled threat crosswise over regarding four hundred applications, together with net activity, email conventions (SMTP, IMAP, POP), and FTP, paying very little mind to ports

REFERENCES

[1] Peng, Wei, et al. "Behavioral Malware Detection in Delay Tolerant Networks."Parallel and Distributed Systems, IEEE Transactions on 25.1 (2014): 53-63.

[2] Govindaraju, Aditya. "Exhaustive statistical analysis for detection of metamorphic malware." (2010).

[3] Tahan, Gil, Lior Rokach, and Yuval Shahar. "Mal-id: Automatic malware detection using common segment analysis and metafeatures." The Journal of Machine Learning Research 13.1 (2012): 949-979.

[4] Kuruva Laxmanna, K.Lakshmi, Dr S.Prem Kumar ," Identifying Malwares By Signature Distribution Algorithm In MANET With Assorted Strategy. "International Journal of Computer Engineering In Research Trends. Volume 2, Issue 9, September 2015, Pp 636-639, Issn (Online): 2349-7084. www.ijcert.org.

[5] http://www.paloaltonetworks.com/products/technologies/wildfire.html

[6] http://www.journalofcomputerscience.com/2013Issue/Jul13/V2No05July13P012.pdf

[7] http://www.academia.edu/11325015/Behavioral_Malware_Detection_in_Delay_Tolerant_Networks

[8] http://en.wikipedia.org/wiki?curid=16623483

