Usage of Windows Event Log Analysis to Improve Cyber Defense

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Geoffrey D. Hicks
Spring, 2020

Technical Project Team Members
Rajiv Sarvepalli
Jake Smith

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Usage of Windows Event Log Analysis to Increase Cyber Defense

Geoff Hicks
University of Virginia
gdh8jh@virginia.edu

Rajiv Sarvepalli
University of Virginia
rs7uxf@virginia.edu

Jake Smith
University of Virginia
jts5np@virginia.edu

Abstract

This research project implements the use of windows event log data analyzation to address the growing threat of phishing attacks against businesses and people alike. By testing different cyber-attacks against vulnerable systems set up within a test server, the existence of event logs that can help in tracking down malicious activity is able to be successfully determined. This is beneficial, as it allows one to trace and stop potential cyber-attacks before they far along enough in their activation process to cause real harm to one's system. This paper presents the process taken for the detection and analyzation of such attacks.

Introduction

Cyber-attacks are a quickly growing threat to both businesses and individuals alike. With the potential to cost companies $200,000 on average (Steinberg, 2019), they are not a security anomaly to take lightly. While there are countermeasures to prevent such vulnerabilities from being taken advantage of, often by the time the attacks are detected and addressed, too much damage to the system will have already occurred. The consequences of letting a cyber-attack affect one's system can be devastating, creating an outcome where the resulting negative impact can be either physical, economic, psychological, reputational, or societal (University of Kent, 2018). This is where the Privacy Enhanced Coordinated Enterprise Representation Learning (P-CORE) project comes in. P-CORE is a government sponsored research project funded by the Defense Advanced Research Projects Agency (DARPA). It is an inter-organizational cooperation and global coordination used to share threat intelligence about attacks after they have occurred ("The fundamental research problem", n.d.). An example of this is when an attack is detected, then Indicators of Compromise (IoC) are disseminated to other organizations so that the latter can add corresponding entries to their firewalls and intrusion detection systems. However, this solution does not leverage global coordination to detect attacks, when in fact, such coordination could make it easier to detect new attack variants and zero-day vulnerabilities. The objective of the project is to create algorithms to detect cyber-attacks as quickly as possible. This is done through global analysis that leverages the power of big data shared across multiple organizations. It is hypothesized that such an inter-organizational globally coordinated effort will expose attacks within a short time frame when the attacks are still largely invisible to any single organization. The fundamental research problem lies in detecting zero-day cyber-attacks from anomalies in network traffic data and host logs. There are two primary constraints that must be taken into consideration: (i) Privacy considerations that prevent a complete sharing of enterprise data with the global-analysis provider, and (ii) Challenges in handling the large volume of data collected by multiple enterprises. In order to circumvent these issues, the P-CORE organization has prepared a few different solutions: (i) Online (stream-mode) machine learning models for early detection of fast attacks; (ii) Generalized deep learning models that can detect new (previously-unseen) attacks when provided a broad set of features; (iii) Application of privacy-preserving federated deep neural network learning methods for global attack detection without requiring enterprises to send their data to the global repository; and (iv) Applications of emerging High-Order Network (HON) representations used in network science to the Cybersecurity domain. P-CORE is the first organization of its kind to propose and attempt to implement such solutions for global attack detection.

Background

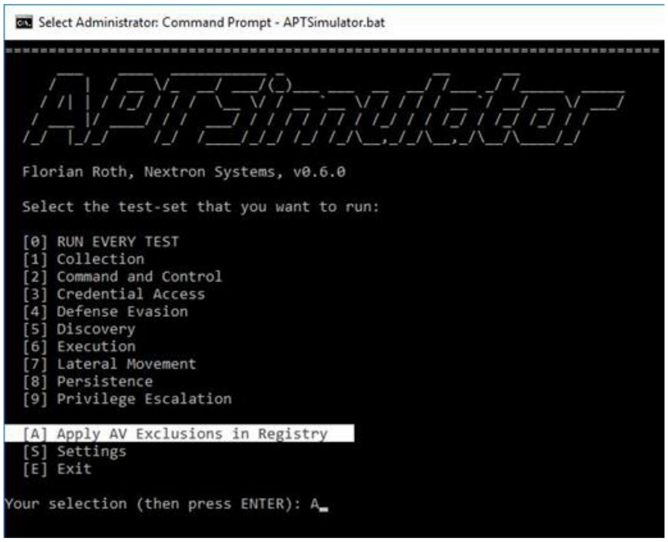
From this project, a subsidiary organization called CHASE (Cyber Hunting at Scale) was created, creating three research tracks to support the goals of P-CORE. The first research track involves developing/running machine-learning algorithms on a network, and hosting data to detect cyber-attacks. The second research track has to do with mapping the landscape of existing malware, reverse engineering their protocols and actions, simulating attacks, capturing packet traffic and host logs of attacks and using that data to build models of malware behavior. The third research track focuses primarily on setting up a Windows domain to understand event logging through the analyzation of windows-based attacks. On December 15th of 2018, I was approached Dr. Yonghwi Kwon of the UVA computer science department to help aide in the work done by the third research track. I accepted, and was assigned to the task of event log analyzation along with fellow colleagues Jake Smith and Rajiv Sarvepalli. The main goal of this task was to set up a few different windows environments within virtual machines installed on a server, and then run various cyber-attacks within the virtual machines. The windows event log information generated by such attacks would be recorded, and then analyzed later in order to identify potentially suspicious activity. This procedure was to be divided into several different steps.

Step 1: Server Preparation

In order to host multiple virtual machines, the use of my laptop would not work. Instead, it was decided that a computer was to be assembled, so it could act as a host to the many virtual machines that were being planned on being created. This computer consisted of an AMD processor, a few terabytes of storage, and 128 gigabytes of RAM. Once the machine was built, it would need to be configured to host the virtual machines properly. To do this, a ESXI (Elastic Sky X Integrated) hypervisor was installed on the machine. A hypervisor is a piece of software that creates and runs virtual machines. The ESXI that was chosen is a type 1 hypervisor, which means that it runs directly on the system hardware without an underlying operating system. ESXI provides a virtualization layer that abstracts the CPU, storage, memory, and networking resources of the physical host into multiple virtual machines. That means that applications running inside virtual machines can access these resources without directly affecting the underlying hardware. ESXI is supported on intel processors and AMD Opteron processors. It includes a 64-bit VMkernel (hypervisor used by ESXI) and hosts with 32-bit-only processors are not supported. However, both 32-bit and 64-bit guest operating systems are supported. Once the ESXI hypervisor was installed, credentials for vCenter Single Sign-On (SSO) was created. This SSO was useful as it allowed one to log into the virtual ESXI hypervisor through a web client, giving the user the ability to remotely access all the features of the server as long as they had internet connection. This is how the ESXI will be accessed in future cases. Then, different virtual machines for the windows environments were installed within the server. Windows 98, Windows 7, Windows 8, and Windows 10 were installed on the machine. In order to ensure proper compatibility for the attacks that were to be performed, it was decided that the Windows 10 machine would be primarily used during testing.

Step 2: Application Configuration

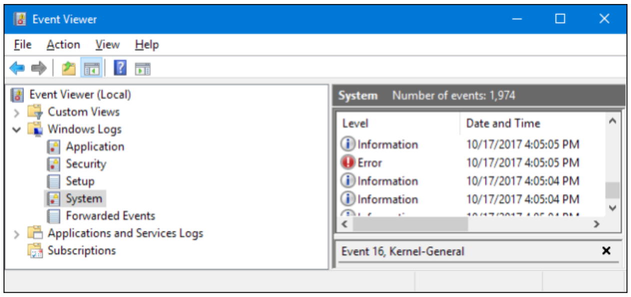
Once the Windows 10 operating system was installed, the necessary software to use for testing needed to be identified as well as configured. As the goal of the assignment was to test various cyber-attacks on a virtual machine, there were two options available: manually write the cyber-attacks through code or download software that have cyber-attacks already pre-installed. The latter option was chosen in order to save time and effort for the project. The software to be used for this was the APT simulator software. The APT simulator is a Windows Batch script that uses a set of tools and output files to make a system think that it was compromised and then makes it act accordingly. In contrast to other adversary simulation tools, APT Simulator is designed to make the process of launching cyber-attacks as simple to use possible. One doesn't need to run a web server, database or any agents on virtual machines in order to get it to work. It only needed to be downloaded, and then ran as an administrator in order to give it the maximum amount of privileges.



```
Florian Roth, Nextron Systems, v0.6.0

Select the test-set that you want to run:

[0] RUN EVERY TEST
[1] Collection
[2] Command and Control
[3] Credential Access
[4] Defense Evasion
[5] Discovery
[6] Execution
[7] Lateral Movement
[8] Persistence
[9] Privilege Escalation

[A] Apply AV Exclusions in Registry
[S] Settings
[E] Exit

Your selection (then press ENTER): A
```

APT Simulator App

The other piece of software used was the windows event viewer that came already pre-installed on every Windows 10 machine. The Windows Event Viewer showed a log of application and system messages, including errors, information messages, and warnings. This was extremely useful as the windows event viewer not only allowed one to view what logs appeared in the system, but also the specific information related to that log. Information such as the log name, the event ID, the user who caused the log to activate, the computer name, and the time the event was logged, are readily available for the user to access.



Level	Date and Time
Information	10/17/2017 4:05:05 PM
Error	10/17/2017 4:05:05 PM
Information	10/17/2017 4:05:04 PM
Information	10/17/2017 4:05:04 PM

Windows Event Viewer App

The event viewer splits the logs into three different categories: Application, Security, and System (“Event logs are local files”, (n.d.). An application log is any event logged by an application. These are determined by the developers while developing the application. For example, an error while starting an application gets recorded in the Application Log. A System Log is any event logged by the Operating System. For example, failure to start a drive during startup is logged under System Logs. A Security Log is any event that matters about the security of the system. For example, valid and invalid Logins, logoffs, and any file deletion etc. are logged under this category.

Step 3: Testing

Before performing testing, the software on the computer needed to be prepped. To start this process, the simulator must first be executed as an administrator. If this is not done, then the framework of the application will not be able to access specific parts of the host computer that it is being run on. Next, the user must confirm that the APT Simulator will attempt to make alterations to the system. Then, the user must give the program permission to make any changes that it must do to the host computer in order to run the various cyber-attacks on the system. With the system and application set up and prepared, the only part left is to run the actual attacks. Before running each attack, the event logs must be cleared within the windows event viewer. The purpose of this is to make sure that there are no foreign activities that the system recorded before the attack was run, as it could alter the results of the output data. Now that the windows event logs are cleared, testing is ready to begin. Within the APT Simulator application, an attack needed to be chosen, activated, then run until finished. The windows event viewer would be opened, and the events consequently caused would be made visible. The recorded logs would be then exported as .evtx files on the host computer, and documented under the specific attack that was run. This helped to categorize the information received so that for every attack, there would be a list of event logs associated with it. Saving the logs as .evtx files was useful in the research process, as those types of files could be opened by the event viewer application and easily display all of the event logs that were saved within the file. After doing this, the event logs that remained in the event viewer were cleared and the next attack was ran, with the same process being repeated until there were no more attacks to test.

Step 4: Classifying Data

Once the event log data was acquired for each attack, they needed to be parsed through and classified to better understand the causation of each log. To do this, a website containing thorough information of event logs called “UltimateITSecurity.com” was referenced, and information regarding each log was collected. The found information was separated into six different categories:

1. Event identification number
2. Description of event log
3. Category of event log
4. Sub-category (if it existed)
5. Example of event log occurring within system
6. Compatible operating system

Then, it was stored within an excel spreadsheet to be referenced later on in the experimentation process. However, a problem that stood out. Just because a specific event occurred under a cyber-attack did not mean it was particularly malicious. It is possible that events found could be only normal windows operating systems processes, occurring in conjunction with the malicious activities in order to support the system itself and not the attack. To separate the neutral logs from the more suspicious ones, the description of the causation of each log was examined. If the log was only caused by a basic function (opening an application, turning on the computer, etc...) then it was put in the “neutral” category. Otherwise, if it performed a more suspicious function like changing privileges or modifying read/write permissions to the disk, then it was put inside the “serious” category.

Results

Looking at the logs in the “serious” category that were found for each attack, many different types of activities were discovered that were shared between the attacks. There were occurrences of read/write permissions being assigned and taken away, changing of firewall permissions, modification of user accounts, removal and addition of user rights, and Kerberos protocol (a computer-network authentication protocol that works on the basis of tickets) access. A common theme between all of these behaviors that quickly stood out was that access to privileges of crucial functions within the windows operating system were always trying to be obtained by the attacking system. As most cyber-attacks need access to permission-protected parts of a system if they ever want to cause any meaningful harm to the user, this is an understandable method of attack. Fortunately, this attempt at undermining a system's defenses are easily recognizable. From this outcome, one can determine that if there are logs on a system that show credentials being accessed without explicit user permission, then that is a red flag than a cyber intruder is trespassing.

Conclusion

The goal of this research was to discover ways of preventing malicious attacks through the event logs that they produced on a windows system. This task was successfully accomplished, and information was gained to aide in solving the problem of early cyber-attack prevention. The information received was deemed valuable enough to be shared with other universities involved with the P-CORE program, so that it can be examined by other researchers to aide in the process of cyber-attack prevention.

References

[1] Event logs are local files. (n.d.). Monitoring Windows Event Logs - A Tutorial. Retrieved May 8, 2020 from https://www.manageengine.com/network-monitoring/Eventlog_Tutorial_Part_I.html

[2] Steinberg, S. (2019, March 9). Cyberattacks now cost companies $200,000 on average, putting many out of business. Retrieved May 8, 2020 from https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.

[3] The fundamental research problem. (n.d.). P-CORE: Privacy Enhanced Coordinated Enterprise Defense via Temporal and Topological Representation Learning. Retrieved May 8, 2020 from https://engineering.virginia.edu/research/multidisciplinary-team-labs-and-groups/p-core

[4] University of Kent. (2018, October 24). At least 57 negative impacts from cyber-attacks. ScienceDaily. Retrieved May 9, 2020 from www.sciencedaily.com/releases/2018/10/181024112203.htm