BTECH 451 – MID YEAR REPORT

THREAT DETECTION AND BEHAVIOUR PROFILING

MUHAMMED RAAFEY KHAN

Department of Computer Science

University of Auckland

Auckland, New Zealand

Email: mkha411@aucklanduni.ac.nz | raafey.khan@asb.co.nz

ABSTRACT

This report outlines the progress of a Bachelors of Technology (Honours) final year project being conducted at the University of Auckland. My project is to evolve, grow and mature the security practices currently being implemented at ASB Bank. In this report I have outlined the company and the goals of the project. I then go onto several case studies related to security breaches and have conducted an in depth technical case study of Carbanak. I have then conducted analysis of the current system in place at ASB Bank, and followed through with my implementation of new systems that will enhance the security intelligence that is currently being gathered. The follow up to this report will contain a full description of my work with final research into behaviour profiling and my implementation.

KEY WORDS

Information security, threat detection, security information and event management, SIEM, data analysis

TABLE OF CONTENTS

1 ACKNOWLEDGEMENTS

I would like to thank the following people for their help and support throughout the first phase of this project:

DR ANIKET MAHANTI

Academic Supervisor

Senior Lecturer – University of Auckland

a.mahanti@auckland.ac.nz

DR SATHIAMOORTHY MANOHARAN

B.Tech Co-ordinator

Senior Lecturer – University of Auckland

s.manoharan@auckland.ac.nz

RYAN COTTERELL

Industry Supervisor

Head of Information Security – ASB Bank

Ryan.cotterell@asb.co.nz

MALCOLM ALLEN

Industry Supervisor

Information Security Analyst – ASB Bank

Malcolm.allen@asb.co.nz

2 PROJECT INTRODUCTION

2.1 THE COMPANY

ASB Bank was first established in 1847, known at the time as Auckland Savings Bank and is now owned by Commonwealth Bank of Australia. ASB provides a range of financial services such as retail, rural and business banking, as well insurance services through its subsidiary Sovereign and investment and securities services through ASB Securities. ASB employs over 5,000 people across New Zealand and is considered a leader in technology innovation (ASB Bank Limited, 2015). The bank has had success by being the first to introduce innovative services and features to the people of New Zealand, including:

- 1997 - Internet banking
- 1998 - Open branches seven days a week
- 1999 - Online share trading on both New Zealand and Australian markets
- 1999 - Mobile banking via ASB Mobile
- 2003 – Ability for customers to opt-out of paper statements
- 2003 – Introduce 2-factor authentication for Internet Banking (NetCode)
- 2006 – PDA and browser based banking
- 2012 – ASB payments via Facebook (iOS, Android and Windows phone)
- 2012 – Dedicated retail App

ASB also employs a full-time information security team as well as a full time operational security team. In my time at ASB thus far, I have had the opportunity to work with and learn from members of these teams in order to achieve the objectives of this project.

2.2 PROJECT BRIEF

The overall goal of this project is to evolve, mature and grow the security practices currently being implemented at ASB Bank. ASB is continually looking to mature and raise the level of efficiency and effectiveness of its Security Information and Event Management (SIEM) implementation and associated practices. This project is being used as an opportunity to evolve and mature existing practices regarding threat profiling and detection and the use of behavioral profiling to improve on the detection.

The project is broken into two phases:

1. THREAT PROFILING AND DETECTION

- Establish a customized system that provides a single view of potential threats

- The single view presented is to be based on defined pattern rules
- The defined pattern rules are to be established through research and analysis
- All aspects of the dashboard are to be automated, scalable and changeable

2. BEHAVIOURAL PROFILING AND BASE LINING

- Devise an easily adoptable and scalable behavioral profiling and base lining threat detection scheme
- Deliver a working prototype of the above-mentioned system
- As part of the recommendation include a working implementation of this methodology
- The working implementation will be based around the system administrator user community

I will consider multiple aspects when designing the system including resource and process requirements, platform limitations, and complementary practices.

2.3 PROJECT STATUS

Due to the nature of this project and the given milestones, the majority of this mid-semester report will be focused on achieving the first milestone related to threat detection and profiling. Based on the research conducted in the first half, the second milestone may be modified to fit the needs of ASB and this project. The end goal is to evolve, grow and mature the security practices currently being utilized at ASB. This can be achieved through multiple ways, which may require altering the project deliverables as the project progresses.

3 PROJECT MOTIVATIONS

The cybercrime landscape is quickly changing and evolving. It is important for organizations, especially financial institutions to evolve and counter this threat. McAfee (2014) estimates that the cost of cybercrime to the global economy could be as high $575 billion per year. This takes into account both the gains to criminal organizations and the costs to companies for recovery and defense.

Ponemon Institute (2014) conducted a worldwide survey of 257 companies across seven countries to assess the state of cybercrime in the world. Some of the results they were able to gather from this survey were:

- Cybercrime continues to be on the rise for organization, there was a 10% increase in the annualized cost from 2013-2014

- The cost to cybercrime varies depending on organization size. There is a positive relation between organization size and annualized cost

- There is a positive relationship between the time to contain an attack and the cost to an organization. If attacks are not resolved quickly, it can get very costly for a company. The average time to contain a cybercrime was 31 days, with an average cost of approximately US$640,000, representing a 23% rise from the year 2013 to 2014.

The way in which cyber criminals are attacking targets has now changed; they are no longer rogue hackers, but organized groups. Because of this, it is important to detect a threat early. Through this project I aim to improve upon the security practices at ASB, with the objective to empower enable security professionals to detect and assess potential threats in their early stages. An improved and streamlined threat detection scheme would reduce false alarms and enable the security team to focus on real threats, thus saving time and money.

The first phase of the project deals with creating an automated threat visualization system that provides a broad overview of the security concerns in a given timeframe. This will allow the user to spend more time looking at potentially suspicious activity and make better decisions related to management of time and resources.

4 CASE STUDIES

To fully understand the ramifications of targeted attacks on systems, it is important to look at particular instances where enterprise systems have been compromised. For this report I will be looking into seven such occasions that has had a major impact on society.

From these seven I will choose one such case which I believe are the most relevant and will be analysing why the compromise occurred, what the attacker hoped to gain and most importantly provide ways in which the victim could protect themselves. In order to evaluate these complicated attacks, I will be using the cyber kill chain model as presented by from Lockheed Martin (Hutchins, Cloppert, & Amin). The definitions for these kill chain phases are as follows:

Reconnaissance – Research and identification of targets. Often done by the means of social networks, social engineering or browsing the web for conference information etc.

Weaponization – Using a control action Trojan in combination with a deliverable payload. Usually done by the means of an automated tool known as a weaponizer.

Delivery – Transmitting the weapon into the target system. Generally done by the means of mail attachments, websites and USB removable media.

Exploitation – After the weapon is delivered to the host, exploitation code is triggered. This code may look to take advantage of system software or the OS itself.

Installation – Installing a remote access Trojan inside the compromised system, allowing the attacker to stay persistent.

Command and Control (C&C) – A compromised host must “beacon” to an internet controller server to establish a channel. Once this is complete the attacker may have “hands on the keyboard access”.

Action on Objectives – The attacker may now take actions to achieve their objective. This in most cases is data exfiltration. It is also possible that the attacker only wanted to gain access to the fist compromised machine so they may move laterally though the system and compromise other machines.

In this section I will provide a brief overview of several cyber-attacks before picking the most relevant cyber-attack to this project to conduct an in-depth technical case study on.

TJ Max and Marshalls (TJX) Breach - 2007

TJX was the victim of the largest (by number of cards) cyber-attack in history when announced in 2007. It is estimated that 45.6 million credit card numbers were stolen in an attack that lasted over one and a half years. The attack on the American retail giant was initially launched from a store in Miami, Florida by exploiting a WiFi vulnerability.

Carbanak 2012 - Present

Carbanak is the name given to a series of attacks on financial institutes around the world. The factor which sets Carbanak apart from other such attacks is that the attackers did not see data, but money as their primary target. The attackers were able to extract between 2.5 – 10 million US Dollars each from financial institutes and the total approximate loss is measured to be at around 500 million – 1 billion US Dollars based on different reports. (Kaspersky Lab HQ, February, 2015)

Shell Shock (Bashdoor) - 2014

Shell Shock is a group of security vulnerabilities in the Unix Bash Shell, which was first disclosed in September 2014. Bash is widely used in the Internet facing machines to process certain requests. This allowed an attacker to target a vulnerable version of bash to execute arbitrary code and take control of the infected machine. Several attacks targeting this vulnerability have come to surface with one of the most notable being the scanning of the United States Department of Defence. (Cyren, October 2014)

Heartbleed - 2014

Heartbleed is a security bug in the OpenSSL cryptography library and is classified as a buffer over-read. In simple terms it allows more data to be read than should be allowed. At the time of disclosure approximately 17% of the Internet's secure Web servers were said to be vulnerable to the attack, allowing theft of private keys, session cookies and user passcodes. The vulnerability was found in a number of well-known sites such as, Yahoo, Imgur, Stack Overflow and DuckDuckGo. (Zakir Durumeric)

Sony Pictures Entertainment Breach - 2014

The hacking of Sony Pictures' systems occurred in November 2014 and resulted in confidential data about employees, executive salaries and copies of unreleased movies being released. The attackers held data for ransom and demanded the unreleased movie "The Interview" be scrapped. US

Intelligence believed the hack was sponsored by North Korea, however those charges were denied by the North Korean authorities. Many security experts doubted the involvement of North Korea and believe that ex-Sony employees were likely the ones to blame. (The Associated Press, 2015)

JP Morgan and Chase Breach - 2014

The 2014 cyber-attack on American bank JPMorgan Chase is believed to have compromised approximately 83 million accounts. It is considered to be one of the largest data breaches in history. The attack was detected by the banks security staff in July 2014 but was not halted until mid-August. The bank has claimed that no login information was compromised however data such as name, email addresses and postal addresses were stolen.

Apple iCloud Breach - 2014

In early September of 2014 a large number of personal photos belonging to Hollywood celebrities were leaked onto the internet through the forum "4chan". Initially it was believed that hackers had exploited a number of vulnerabilities in the "Find my IPhone" application but these rumours were denied by Apple. It is believed the attackers were able to gather information on celebrities though online research and correctly guess the answers to security questions in order to get access to the data from the online storage platform iCloud, which can be accessed via a web browser. (Cyren, October 2014)

4.1 Technical Case Study: Carbanak

From late 2013 onwards, banks and financial institutes across the world have been attacked by a group of unknown cyber criminals. These attacks continue to this day with the attackers not having been identified.

Carbanak is the name given to a group of malware that is designed for espionage, data exfiltration and access to infected machines. It is now also the name given to the group of cyber criminals that have used the back-door malware to attack financial institutions. This case study will be a technical analysis of these attacks using the cyber kill chain model. Kaspersky Lab HQ (2015) has released an extensive report into the proceedings and all the information in this section is taken from said report.

Reconnaissance

The reconnaissance phase for the Carbanak attacks was particularly complex and at times lasted for months before the attack actually occurred. It has been discovered that video recordings of bank employees, particularly system administrators were taken and sent back to the C2 server, meaning the reconnaissance phase continued on through the entire cyber kill chain process.

Once access is achieved to the infected system, attackers perform manual reconnaissance of the victim's network to find vulnerabilities that may be exploited. Based on the results of this reconnaissance, more machines are compromised to find the correct system or user that will be used to conduct the attack. Sort of like target identification

WEAPONIZATION, DELIVERY AND EXPLOITATION

All of the cases observed so far have used spear phishing emails with vulnerable versions of Microsoft Word 1997 - 2003 attachments. The attachments exploit both Microsoft Office and Microsoft Word. The exact CVE (what is CVE?) numbers are as follows:

- Microsoft Office – CVE-2012-0158, CVSS Score: 9.3
- Microsoft Office – CVE-2013-3906, CVSS Score 9.3
- Microsoft Word – CVE-2014-1761, CVSS Score 9.3

The recipients of these phishing emails were all employees of the target institution. The emails appeared legitimate and were at times sent from a co-worker's compromised account, using compromised systems as a transmission vector.

The victim institutions were mostly Russian; therefore the names of the infected attachments found have been mostly in Russian. Examples of names include *Соотвветсмвие Ф3-115* which roughly translates to "Accordance with Federal Law", this is in most cases enough to induce an employee to click on and open the attachment.

The following is a translated version of a Carbanak phishing email:

Good Day!

I send you our contact details

The amount of deposit 32 million rubles and 00 kopnecks, for a perios of 366 days, % year---end contribution term

Sincerely, Sergey Kuznetsov;

+ 7 (953) 3413178

f205f@mail.ru

FIGURE 1: TRANSLATED CARBANAK SPEAR PHISHING EMAIL EXAMPLE

In the case of this spear phishing email, the attachment was a compressed Roshal Archive (.rar) file.

In addition to spear phishing it is also possible that exploit kits were used in conjunction to perform drive-by-download attacks, a malware delivery technique where data is downloaded by the target machine by simply visiting a website. Traces of the Null and RedKit exploit kits have been found on compromised systems

Once the user has clicked and/or opened the attached file, the remote execution vulnerability is exploited. This installs Carbanak onto the victim system.

INSTALLATION

Once the exploit in the phishing email or exploit kit is able to execute its payload, Carbanak is installed onto the victim's system. Carbanak will initially copy itself into "%system32%\com" with the filename of "svchost.exe". It also has the file attributes of hidden and read-only. At this point the original file which is created by the exploit payload is permanently deleted.

Carbanak will in the next phase ensure that it has auto run privileges by creating a new service. A naming convention is in place to ensure that the given name does not appear suspicious to the average user. Before creating this service, however a number of tasks are performed in order to bypass Internet security and anti-virus detection, this is different for every organization attacked and comes from the reconnaissance phase of the attack.

Carbanak then creates a file with a randomly generated name and a .bin extension in %COMMON_APPDATA%\Mozilla where commands are stored that are executed later on in the process.

The next step in the process is to get the proxy configuration from the registry entry:

[HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

And the Mozilla Firefox configurations file in:

%AppData%\Mozilla\Firefox\<ProfileName>\prefs.js

Carbanak injects its code into svchost.exe and is now able to communicate with the C2 servers

COMMAND AND CONTROL (C&C)

At this stage, the system is infected with the Carbanak malware, which is able to communicate back to its C2 server. Carbanak now logs keystrokes and takes screenshots on a regular basis, typically 20 seconds.

To communicate with the C2 server, Carbanak will use the HTTP protocol with RC2 +Base64 encryption. It will also insert strings with extensions such as .gif, .pdf etc. at random locations in the HTTP request.

Carbanak will send the collected data to the C2 server and also receive commands. The incoming commands are compared with a hash table. If a match occurs, the associated action is performed. Examples of the commands include:

HASH	COMMAND TYPE	DESCRIPTION
7CFABF	Video	Sends captured screen video to C2
6533C4	Download	Download and run .exe file from C2 server. This file is stored in %TEMP% with a random name

ACTION ON OBJECTIVES

After fully surveying the victim organization for a prolonged period of time, the attackers were able to use intelligence gained from video and other monitoring techniques to create a profile of the typical user. This allowed the attackers to personalize each attack to the target organization. Examples of malicious operations conducted include:

- Creation of fake transactions in internal databases after the verification process, therefore avoiding discovery of fraudulent activity.

- Use of internal command utilities to insert fraudulent operations into the transaction queue

- Control over the internal ATM Network, If the bank had enabled remote access to ATMSs, the criminals used standard utilities used to control and test ATM's to dispense cash at their will

- Retrieve sensitive bank documents such as emails, manuals, passwords and crypto keys. A particular example of this being a document found on a Carbanak C2 server outlining ATM keys used to verify the integrity of ATM pins being entered.

5 THE PLATFORM

In this section of the report, I will be outlining the platform I will be using as well as some of the key security mechanisms that have been put in place by ASB in regards to the SIEM platform.

5.1 SIEM

SIEM is seen as the integration of two key technologies, Security Information Management (SIM) and Security Event Management (SEM). SEM deals with real time monitoring of data, event correlation, notifications and console view, whilst SIM deals with the long term storage, analysis and reporting. For this project, I will be mainly working with the McAfee SIEM platform that is currently being implemented by ASB Bank. At ASB the current SIEM implementation was first introduced in 2014, taking over from its predecessor Nitro. SIEM is used to gather, correlate and report on data within the ASB enterprise.

The key features we see in most SIEM/Log Management solutions of SIEM systems include:

- **Log Aggregation:** Collection and aggregation of log records from the network, security, servers, databases, identity systems, and applications.

- **Correlation:** Attack identification by analyzing multiple data sets from multiple devices to identify patterns not obvious when looking at only one data source.

- **Alerting:** Defining rules and thresholds to display console alerts based on customer-defined prioritization of risk and/or asset value.

- **Dashboards:** Presentation of key security indicators within an interface to identify problem areas and facilitate investigation.

- **Forensics:** Providing the ability to investigate incidents by indexing and searching relevant events.

- **Reporting:** Documentation of control sets and other relevant security operations or compliance activities.

ASB's SIEM implementation takes in data from a variety of sources, it can essentially be thought of as a large data warehouse. The problem with any large quantities of data becomes effectively using the data to create intelligence. The data sources currently feeding into SIEM include:

- **Security Infrastructure** – Intrusion detection/prevention systems, firewalls, proxies
- **Network Infrastructure** – network devices (e.g. Routers and Switches), network services (e.g. DNS, DHCP)
- **Platforms** – Operating systems (e.g. UNIX, Windows), DBMS (Database Management Systems)
- **Applications** – Over 400 internal applications feed directly into the SIEM environment

Given the sophistication of today's attacks, having all security related data in a centralized location helps the security team identify events of concern faster, analyse the information and incorporate data from different sources more easily and effectively.

5.1.1 SIEM ARCHITECTURE

ASB's current SIEM architecture is relatively mature, in terms of set-up and redundancy. In Figure 2 the primary location, whilst the right hand side is the secondary location.

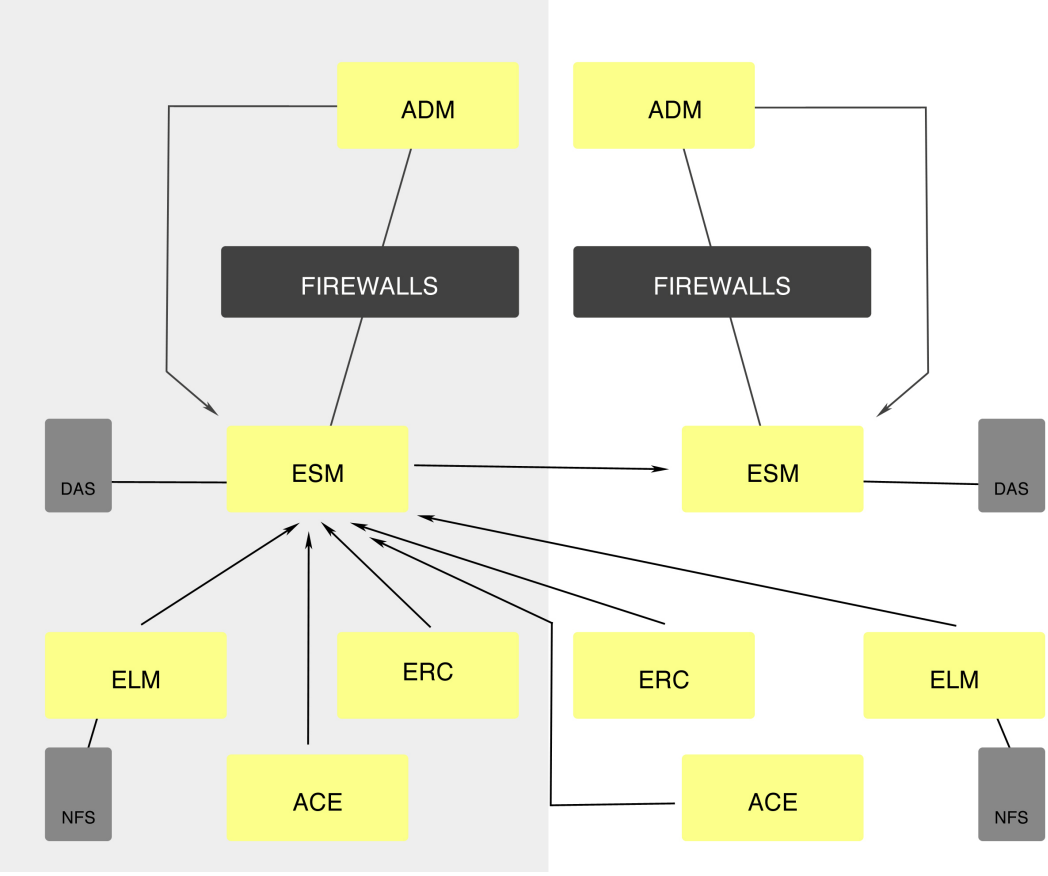

FIGURE 2: ASB SIEM ARCITECTURE

ESM – Enterprise Security Manager

The ESM is the main component of the SIEM architecture; it is the physical interface that is used to display information and where customized sub-systems can be built in order to perform specific tasks. The physical display is broken down into three distinct portions as seen in Figure 2. The left-hand side encompasses the different incoming data sources. In the centre, is where SIEM's event analysis is displayed, this area is easily customizable in order to fit the needs of the specific task. On the right hand side of the interface, the user can select from a number of filters in order to look for and select distinct types of data. The filters are extensive, with options available to filter on protocols, traffic and many other characteristics.

The ESM also has a DAS (directly attached storage) attached to it, allowing it to store more records.

ADM – Application Data Monitor

The ADM primarily provides NetFlow data to the ESM. NetFlow allows us to collect IP Network traffic as it enters or exits the interface. By analysing this type of data in the ESM, we are able to determine the source/destination of the traffic.

The ADM is also able to look into the application data and detect sensitive information that is being transmitted inside email attachments, file transfers, HTTP posts etc. You are able to pick up sensitive data types, log them and inform the appropriate parties.

One of the key issues related to the SIEM architecture, is the location of the ADM. As seen in Figure 2 the ADM is placed above all firewalls, this means that all incoming traffic is logged and sent to the ESM, thus creating an enormous amount of data. There are both advantages and disadvantages to this, as this method of collection can give a good indication as to what is going on in the enterprise as a whole but also creates un-needed data.

ERC – Event Receiver

The Event Receiver is responsible for collection of events and flow information, from data sources such as those listed in the previous section, including firewalls, applications and work stations. The ERC is able to collect tens of thousands of events per second and store them.

The ERC feeds raw log files directly into the ELM at a set interval. The ESM also retrieves data directly from the ERC at a set interval.

ELM – Enterprise Log Manager

The ELM receives the non-indexed and non-aggregated data directly from the ERC. The data here is parsed into a standardized format in order to standardize the data from the various sources it is retrieved from. It also stores the original record so that the activity cannot be repudiated. This enables easy access for compliance monitoring and forensic investigation. Since the original files are not altered, the ELM is able to support chain-of-custody efforts.

The ELM also has a NFS (network file share) attached to it for additional storage needs.

ACE – Advanced Correlation Engine

The ACE is fed data directly by the ESM at a set time interval. The ACE is able to monitor close to real time data and aggregate events in order to present them as one in the ESM. The correlation rules have been predefined by McAfee but can also be set and altered in the ESM. ASB has set-up a number of correlation rules in order to customize the SIEM to fit the information security goals.

5.2 Use Of Global Threat Intelligence (GTI)

The McAfee GTI framework is a cloud based threat intelligence tool which has the ability to look into multiple types of cyber threats from around the world and allow an organization to make decisions in real time. The data comes in from millions of McAfee products acting in sensors that are deployed across the world in organizations. With every query that is sent, the GTI system is able to learn something new about the subject. This information is combined with other threat vectors such as known malware types to provide a solid worldview of trending threat activity (McAfee, 2010). There are five main types of reputation and categorization services that are implemented as part of GTI. They are:

File Reputation – the GTI system is able to look at a file and rate it based on the likelihood that it is malware. This is done through sensors that are deployed across organizations as well as analysis performed by McAfee researchers and cross-vector intelligence tools from email, web and network threat data. The score that is assigned can be used to block or quarantine a file depending on local policy.

Web Reputation – The GTI system is able to look at a URL, DNS server or web domain and determine the likelihood of the service being a phishing site, being infected with malware or otherwise malicious. After a score is determined, actions can be taken depending on local policy.

Message Reputation – The GTI system is able to determine if an email message is malicious by analysing the message contents many dimensions. It combines this information with spamming

patterns and IP behaviour in order to provide a score based on likelihood of the file being malicious. This allows actions to be taken depending on local policy.

Network Connection Reputation – McAfee is able to collect billions of IP addresses and network ports, using this information the GTI system calculates a reputation score based on port numbers, protocols and connection requests. The score reflects the possibility of the connection type being malicious. This score is then used in local policy to take action against the network connection.

5.3 Use of Third-Party Blacklists

Many organizations maintain and publish blacklists of URLs and IP addresses of known malicious activity. Most of these lists are available online for free to use and implement. The lists generally differ in goals, format and collection methodology. Some lists may target a specific type of malware, whilst others collect a wider variety of data. The lists currently being used and implemented by ASB currently include:

- Dyre – A watch list for a particular type of malware named "Dyre". The malware is used to target users through phishing emails that appear to be from financial institutes. (Kuhn, Mueller, & Kissem, April 2015)

- EmergingThreats - an open source platform more than 10 years old for collecting Suricata and SNORT rules. More than 20,000 active users download the rules daily. Provides a watch list based on input from the user community on a wide set of vulnerabilities. (Emerging Threats, 2015)

- Malc0de – An open source database of URL's and IP addresses that are hosting malicious executable files.

- Palevo – A watch list that tracks a worm known as Palevo which transmits using instant messaging, P2P networks and removable drives such as USB media. (palevotracker.abuse.ch, 2015)

- Zeus Tracker – IP addresses and domain names that contain known command and control servers associated with Zeus crimeware. Zeus tracker offers both bad domain name lists and bad IP address lists. (Andriesse & Bos, April 10, 2014)

6 CURRENT SYSTEM

The SIEM platform provides a number of pre-built sub-systems in order to help security professionals achieve their goals faster and more effectively. The ASB Information Security team has also built several sub-systems in order to serve a single purpose. In this section I will be looking at several of these sus-systems and analysing the information security goals they help achieve.

The two inbound file sub-systems I will be looking into in sections 6.1 and 6.2 are primarily created for malware detection, as seen in the Carbanak case study (Kaspersky Lab HQ, February, 2015) ; one of the key aspects of the attacks was the use of vulnerabilities in MS Office documents and drive by download attacks. By detecting all the incoming files into the ASB Enterprise, we are able to check if potentially malicious files are being downloaded and/or if they are coming in via the means of email.

6.1 INBOUND EXE.

The purpose of the inbound executable subsystem is simply to detect and record all inbound executable files that are coming into the ASB enterprise. This is done by filtering the data type by the unique signature ID that is associated with executable content. The SEM is able to look into the header of the document to detect the file type rather than looking at the extension. This allows detection of files that have been renamed to avoid being captured by low-complexity firewalls.

The general investigation process for the Inbound Exe Subsystem is to filter once more by “source IP”. This allows us to look into the executable files and pick out the files that have potential to be a threat as they originate at a known suspicious or malicious IP address.

From this point forward the processes is largely manual. For data that is coming in via email, the mail content management system must be used to see if the executable did indeed reach the target or if it was blocked at one of the firewalls such as the email security gateway. To support automation of this process, plans are currently in place to integrate mail and web content management logs into the SIEM platform.

6.2 INBOUND OFFICE

The inbound Office sub-system is in nature very similar to the inbound executable. The purpose is to record all inbound office documents that are coming into the ASB enterprise. This again is done by filtering for the unique signature ID that is associated with all office documents.

The general investigation process for the Inbound Office documents is very similar to the Inbound Executable. After the user has filtered down for suspicious or malicious IP’s, we must look into either the mail content

management system or the web proxy/content management system to see if the data was blocked by the firewall before it got to the end user.

The placement of the ASA provides both advantages and disadvantages in data collection. As it is placed above the firewalls, it is able to collect all data that is directed to the ASB Enterprise, this allows a very accurate view of incoming traffic, however as ASB has strict policies in place around office documents, for example, PowerPoint documents are blocked to a degree from going in or out of the system through Email, however the ASA will pick up this activity regardless and feed it into the SEM. This then creates manual work for the user, as they must investigate further to check at what point the file was blocked or if it reached the end user.

6.3 GTI Inbound & Outbound

The GTI Inbound and GTI Outbound sub-systems are based on the Global Threat Intelligence that is gathered by McAfee. Inbound presents all the data that is coming from a known suspicious or malicious IP and Outbound does the opposite.

The GTI dashboards also normalize to two levels. The first level of normalization provides a high level overview of which category an event belongs as seen in Figure 3. The second level provides a much more detailed explanation as to why the particular event was grouped in this way.

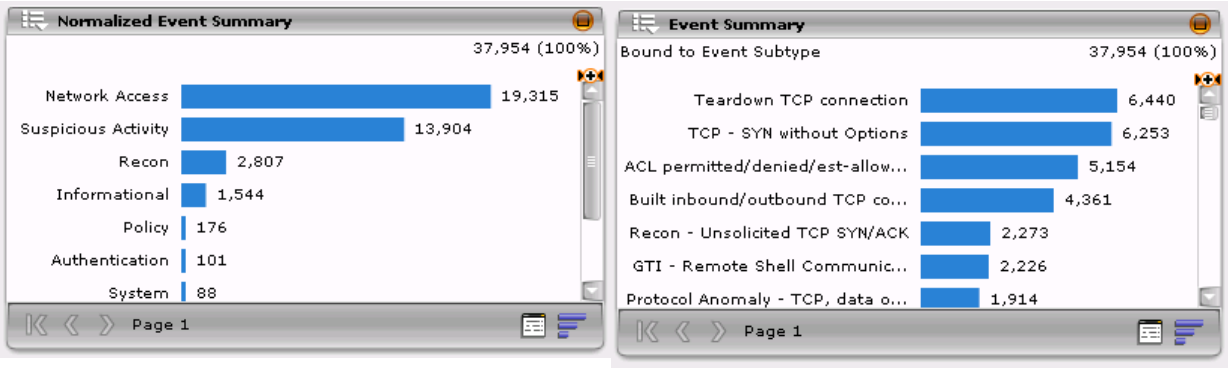

FIGURE 3: MODULES FROM GTI SYSTEM

One of the key issues relating to the GTI dashboards is the reasoning behind why an IP address is flagged as suspicious or malicious and the difference between the two. Speaking to experts at ASB revealed that an IP address may potentially be considered suspicious if it is in the same geolocation as another malicious IP. This has the potential to create false positives.

6.4 Default Summary

The default summary sub-system is the first view a user gets once they have logged into the SEM platform. It is preconfigured by McAfee and at the moment does not provide any real intelligence. This is because it simply displays all the data that is available. As seen in Figure 4, the majority of the pie charts displayed do not give real information, the largest portion of each one is listed as “other” meaning it is uncategorized. There is room for drastic improvement on this system, so that once a user logs onto the SEM they are able to get a clear idea of what is going on in the organization security-wise.

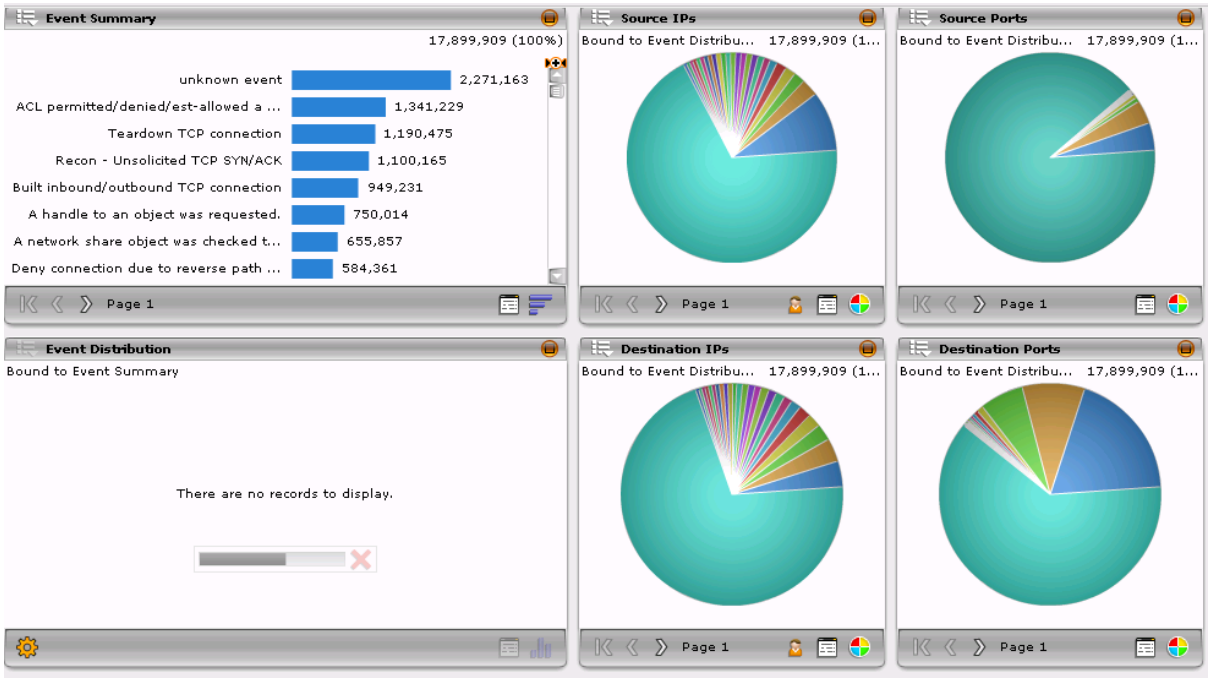

FIGURE 4: DEFAULT SUMMARY SYSTEM

7 SUB-SYSTEM CREATION

7.1 RECREATION OF THE DEFAULT SUMMARY

As previously mentioned, the default summary sub-system is the first view a user gets once they have logged into the SEM platform. My goal for this part of the project will be to recreate this system so that it provides useful information and intelligent to the security professionals using it. The sub-system I create is intended to replace the current default summary and provide an overview of what is going on in the ASB enterprise with a single glance. The newly created sub-system will be called Information Security Summary

In order to do this, I have selected a number of preconfigured dashboards that I believe to be of importance. This selection process was done mostly through speaking to information security experts at ASB Bank and asking them, what sub-systems they used the most and which ones were most underutilised. From this information I created the basic outline as displayed in figure 5.

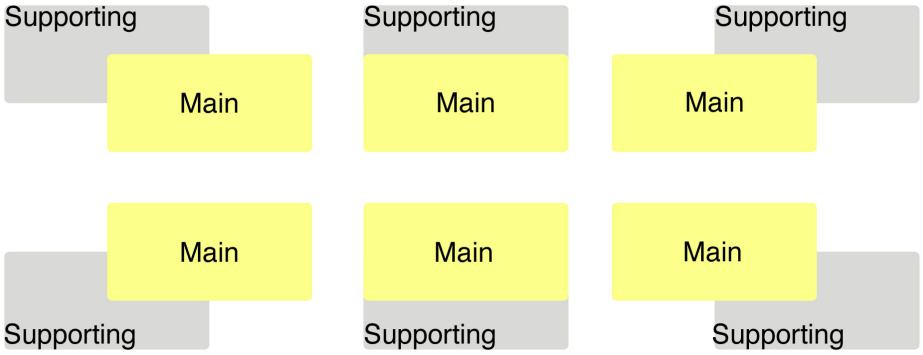

FIGURE 5: OUTLINE OF INFORMATION SECURITY SUMMARY

As all the information required to investigate a particular event cannot fit onto a single system view, my main sus-system will feature six modules, each one relating to a different key issue related to information security. There will also be six other sub-systems providing a mode in-depth view into each module coming from the main sub-system, this idea is visualized in figure 5.

The six modules that will be incorporated into the system are:

- Critical File Issues
- Critical Authentication Issues
- Administrator Access Summary
- Severity of Correlated Events
- Global Threat Intelligence Inbound Data
- Global Threat Intelligence Outbound Data

Each one of these six modules will also have an accompanying sub-system that will allow the user to look into the module in more detail. These sub-systems will initially be taken directly from the current working implementation but in the future have the potential to be expanded and modified as needed.

7.1.1 Version 1.0 of Information Security Summary

FIGURE 6: VERSION 1.0 OF INFORMATION SECURITY SUMMARY SYSTEM

The core of the Information Security subsystem is displayed in Figure 6, as previously stated it contains six main modules. This subsystem was created with the intention of modifying it and enhancing it as the year goes on. The sub-system may also be modified as business requirements change and/or new threats arise. The six current modules are:

Malicious Incoming Files – This module lists potentially malicious files that have been received in the ASB enterprise. It is built from the Malicious File Subsystem that I have created and illustrated in part 7.2

Admin Access Summary – This module counts the special privileges assigned to a new logon for each of the systems that are listed. By viewing this information a security professional may detect an anomaly if one particular system is showing an excess of assigned privileges. There is vast room for

improvement in this module as the data can be cut down to the most critical components so it is easier to view.

Critical Authentication Issues – This module lists issues related to authentication. At the moment, it is taken directly from another preconfigured system, but in the future has potential to look at only critical system authentication or a particular system by customizing the filters that it takes into account.

Average Event Severity – The module looks at the all of the correlated events over the specified time frame. It then displays the average severity of each correlated event. Currently the severity factors for all correlated events are set to 1. Further research needs to go into this module so it is more representative of ASB's Information Security goals.

Incoming Data from Blacklist IP's – This module builds on the preconfigured subsystem of GTI Sourced Threats, it takes the most detailed module from that subsystem and incorporates third party IP watch lists to give a more complete and comprehensive view.

Outgoing Data to Blacklist IP's – This module simply does the opposite to that of its neighbour. It builds upon the GTI destined threats system and incorporates the third party watch lists in the destination IP filter, thus allowing you to see all traffic going to a suspected malicious IP. Due to internal ASB research, I have decides to exclude GTI suspicious IP's from the list of incorporated watch lists as it is believed to not provide the required level of confidence.

7.1.2 Customization of Information Security Summary

Due to the ever-changing landscape of the cyber security world, it is important to keep the information security summary system up-to-date with emerging threats. This vector is already implemented through the use of global threat intelligence and third party IP blacklists but can be taken further by creating custom modules for newly released information related to malicious activity.

An example of such actions would be the creation of a module to combat the Shellshock vulnerability that was discovered in September 2014. IP addresses for those looking to exploit the vulnerability were published and shared online by the Information Security community in efforts to help each other protect themselves from attackers. By incorporating this information into a dynamic watch list that tracks traffic from these incoming IP addresses, we would be able to track and take appropriate action against such attacks.

7.2 Malicious File Subsystem

The Malicious file subsystem is an example of one of the six subsystems that can be built for the main default summary system. For this subsystem, I focussed on the two currently implemented subsystems that were being utilized the most throughout the information security team, the inbound executables and inbound Microsoft Office documents. These two dashboards are very similar in nature as the primary goal of the two is to look at incoming documents.

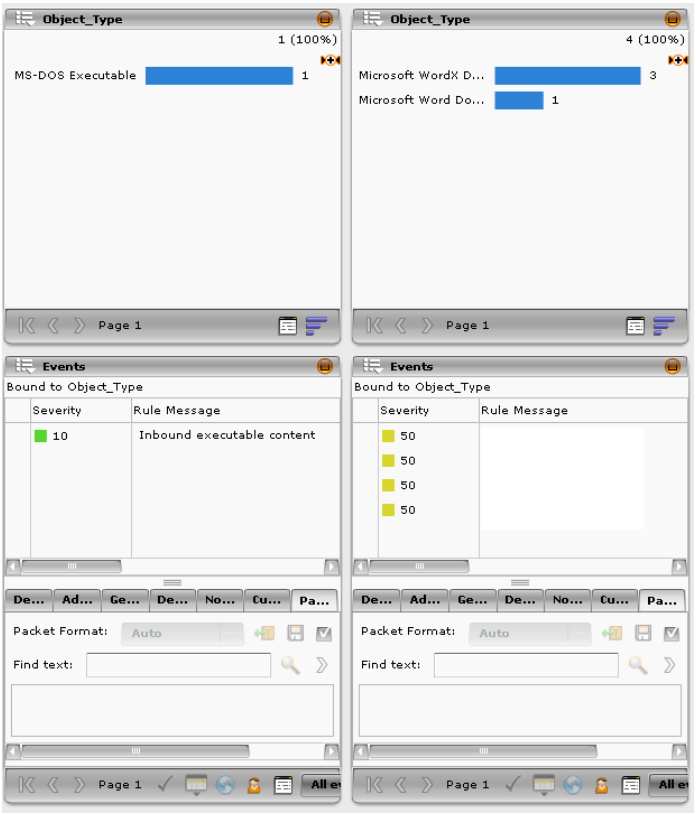

FIGURE 8: MALICIOUS FILE SUBSYSTEM VERSION 1

The first malicious file sub-system that I created is displayed in Figure 8

This system simply takes the most important data from the two systems in question and displays them in an easy to see manner. The two top modules display the incoming file types of question, whilst the bottom two modules display a breakdown of the events in question.

As mentioned previously, one of the key steps in recognizing a malicious incoming file was filtering the data for malicious source IP addresses. This can be done in the SIEM platform by the use of preconfigured watch lists taken from McAfee Global Threat Intelligence and by the use of third party IP blacklists. As this is an important step in both the systems in question it can also be combined into the new system being created.

This idea was implemented as seen in Figure 9:

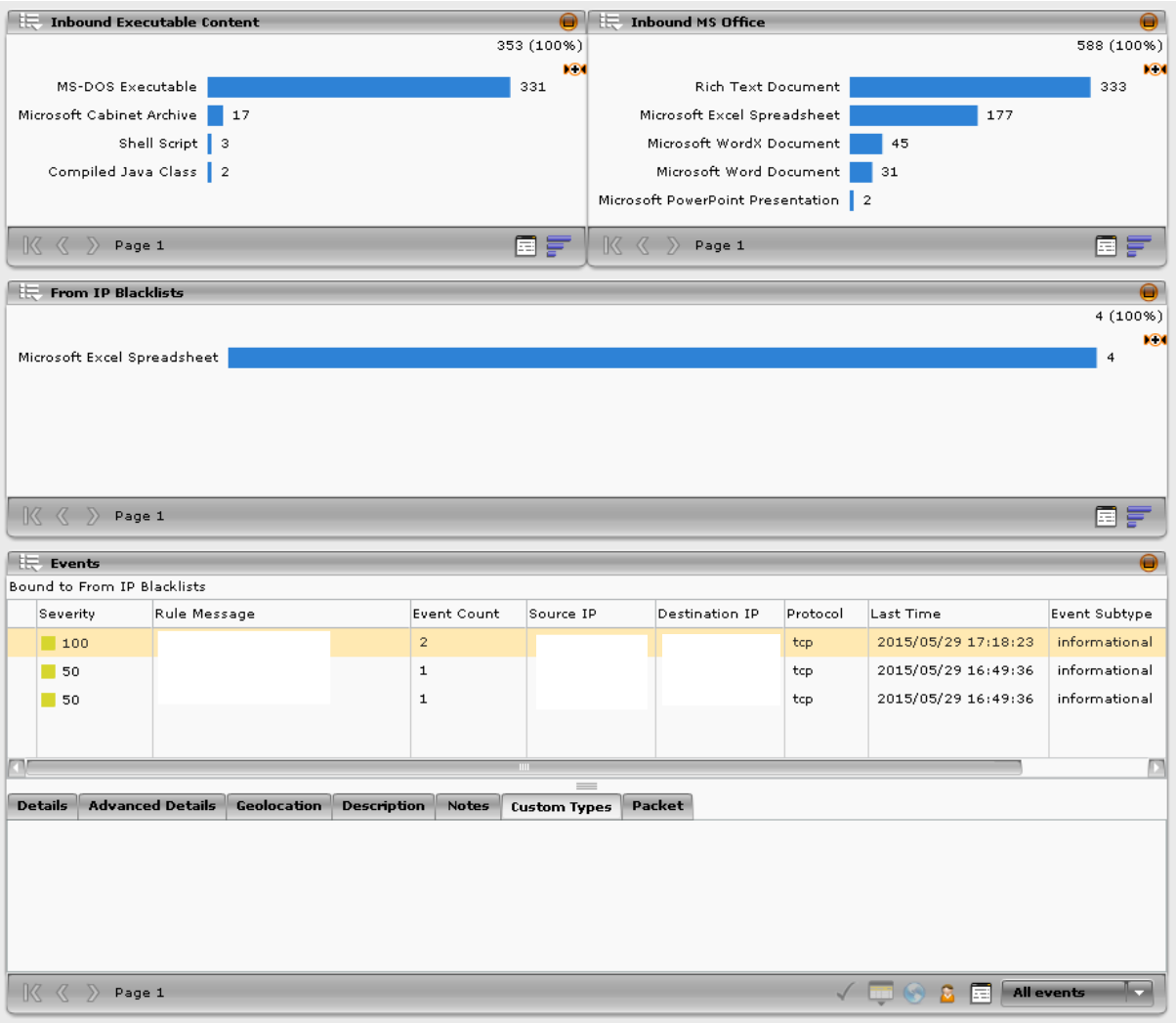

FIGURE 9: MALICIOUS FILE SUBSYSTEM VERSION 2

The figure displays two modules that are identical to the previous version; they are used to display the incoming executables and office documents. The middle module is used to filter the data through the preconfigured watch lists, such as the ones mentioned previously in this report. By automatically filtering down the data to display the most important aspects, the security professional using the system is able to save time and make more effective decisions in time allocation.

As seen in Figure 9, in the specified time frame, there were over 300 inbound executable files and over 500 inbound MS Office files, to go through each and every one of these files to determine if they are coming from a malicious source would be both time consuming and extremely tedious. By using this implementation, the events of concern are listed, so that they may be prioritised. The figure shows there were four incoming files from a malicious source. A drilldown of these events is visible in the bottom module of the system, the user now simply needs to look at the bottom module and is able to further investigate the event.

7.2.1 Detection of Communication with C2 Server

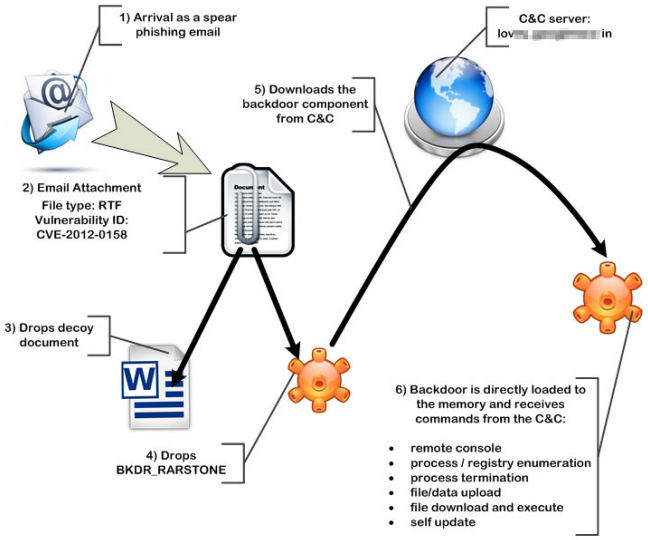

FIGURE 1 MALWARE COMMUNICATION WITH C2 SERVER (TREND MICRO, 2015)

As previously stated and seen in the Carbanak case study, once a malicious file has been downloaded on the targets server, it will install malware and try to communicate back with the C2 (Command and Control) server. (Mezzour, Carly, & Carley, 2015) This process is displayed in figure 10. The lists of malicious IP addresses that are implemented through the use of watch lists in the SEM contain many IP addresses for known C2 servers. In theory, we should be able to look at communications going out to these servers, simply by filtering for destination IP address.

The first step in this process would be to create a list of all the IP addresses that have received content from a malicious IP address, by taking this list and using it as our source IP, we can then filter for a destination IP address which is taken from the preconfigured watch lists. By performing these steps, we should in theory be able to detect if:

1. A user has received a malicious file
2. If the target has communicated back with a malicious IP address.

By doing so, we would be able to see if a machine or particular system in the ASB enterprise has been compromised and escalate the matter accordingly.

However, when trying to implement this procedure, I noticed that the destination IP address that was being displayed was generally not of the host, but that of the Email Security Gateway. This meant that I would not be able to map these to actual machines. The only way to do this would be to first match it to the mail content management system and the web/proxy management system data in order to get the IP address of the targeted host. This in theory should be possible once the mail content management system and web proxy/content management system is integrated into the system, but at the current time can only be done in a manual manner.

8 KEY ISSUES

8.1 FAMILIARITY WITH AND SIZE OF DATASET

The Current SIEM implementation consists of terabytes of data. There is well over a million events that are recorded each day. In order to gather intelligence from the dataset, it is important to understand the underlying logic of the SIEM. It is important to understand the data sources as well the different fields that are presented. This is a crucial step in determining if the data is of use or is simply background noise that can be ignored.

Due to the size of the dataset, performing analysis on historical was very difficult and in some cases impossible. Running queries over a period of over a month and in some cases a week required a waiting period anywhere between five minutes to an uncalculated amount of time. This meant the subsystems I created could at most only look at data for the current or previous day.

8.2 MISSING DATASET

As mentioned previously in my report, the process of adding data into the SIEM platform can at times be very complicated and time consuming if the data is source is not directly supported. The parsing of this data to make it compatible for SIEM is an ongoing process at ASB Bank and is prioritized from most important to least. Currently data from the mail content management system and web proxy/content management system are not implemented in SIEM. When implementing the automatic detection of communication with a C2 server as outlined in 7.3.1 this was a very apparent issue. In order to truly get the full picture of what is happening security wise in the ASB enterprise it is essential to have this data feeding into the SIEM platform and is a prioritised task for the Operational Security team.

8.3 ACCESS PRIVILEGES

Due to the confidential nature of the dataset, my profile for the ASB SIEM platform did not allow full access to all the tools and utilities available. This was done as a security measure by the bank and is common practice throughout corporations. This is a measure that has to be taken in order to be compliant but does pose several challenges as I work through this project.

9 CONCLUSION

The above report is the progress on my goal of enhancing information security intelligence at ASB Bank through the use of their SIEM implementation. The sub-systems I have created will be continued to be monitored throughout the year by both me and members of the Information Security team. This will allow them to be customized and changed as needed to fit the business goals of the bank.

The next phase of this project will involve significant hours of research into current behaviour profiling models and anomaly detection techniques. From this research one or more models will be chosen and incorporated into what best fits the business needs of the bank. The end goal is to provide a working implementation of a behaviour profiling model with supporting subsystems that can be used to identify threats, allowing them to be elevated or mitigated depending on severity.

10 BIBLIOGRAPHY

Andriesse, D., & Bos, H. (April 10, 2014). *An Analysis of the Zeus Peer-to-Peer Protocol .* VU University Amsterdam, Amsterdam.

ASB Bank Limited. (2015). *Our History*. Retrieved from ASB Bank LimitedWebsite: www.asb.co.nz

Cyren. (October 2014). *Internet Threats: Trend Report.* Cyren Limited.

Emerging Threats. (2015). *Emerging Threats Open Source Overwiew*. (Emerging Threats Pro, LLC) Retrieved from Emerging Threats Website: www.emerginghtreats.net

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (n.d.). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Lockheed Martin Corporation.

Kaspersky Lab HQ. (February, 2015). *Carbakan APT: The Great Bank Robbery.* Moscow.

Kuhn, J., Mueller, L., & Kissem, L. (April 2015). *The Dyre Wolf: Attacks on Corporate Banking Accounts.* IBM.

McAfee. (2010). *McAfee Global Threat Intelligence.* McAfee Inc, Santa Clara, CA.

McAfee. (June 2014). *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.* McAfee, Intel Security.

Mezzour, G., Carly, K. M., & Carley, L. R. (2015). *An empirical study of global malware encounters.* Carnegie Mellon University, Pittsburgh, PA .

palevotracker.abuse.ch. (2015). *Palevo Tracker :: Home*. Retrieved from Palevo Tracker Website: https://palevotracker.abuse.ch

Ponemon Institute. (2014). *2014 Global Report on the Cost of.* HP Enterprise Security.

The Associated Press. (2015). *Timeline of the Sony Pictures Entertainment hack*. Retrieved from Phys.org 2003 - 2015, Science X network Website: www.phys.org

Zakir Durumeric, J. K. (n.d.). *The Matter of Heartbleed.* University of Michigan, University of Illinois.