Journal of Computers Vol. 30 No. 1, 2019, pp. 206-222
doi:10.3966/199115992019023001020

The Study of Using Big Data Analysis to Detecting APT Attack

Chung-Hsin Liu[1*], Wei-Hung Chen[2]

[1] Department of Information Engineering and Computer Science, Chinese Culture University, Taipei 111, Taiwan
liu3.gold@msa.hinet.net

[2] Graduate Institute of R&D Master Program in Information Security Industry, Chinese Culture University, Taipei 106, Taiwan
fire.icewayne@gmail.com

Received 30 September 2017; Revised 29 October 2017; Accepted 10 January 2018

Abstract. An advanced persistent threat (APT) is a deliberately slow-moving cyberattack that is applied to quietly compromise interconnected information systems without revealing itself. APTs often use a variety of attack methods to get unauthorized system access initially and then gradually spread throughout the network. In contrast to traditional attacks, they are not used to interrupt services but primarily to steal intellectual property, sensitive internal business and legal documents and other data. Once an attack is successful, then the system timely detection is of paramount importance to mitigate its impact and will prohibit APTs from further spreading. For the early detection APT threat, this study proposes a detection mechanism, using Big Data and Splunk analysis, then using data mining techniques to find malicious IP position. Through the experimental results, decision tree algorithm is used as the best prediction model, and in the predictive model, the detection rate increased to 99%. Finally, this study established an alert system, can achieve real-time threat detection APT effect.

Keywords: APT, big data, Splunk

1 Introduction

Sony Pictures Entertainment on November 24, 2014 was called "peacekeeper" hacker groups APT attack, tens of thousands of employees the data, as well as several unreleased copies of the film have been leaked, this incident has proved that the APT attacks prediction and its importance.

At the end of 2014, Taiwan renowned online game league of legends and the path of exile has also suffered APT attack, caused by Remote Access Trojans (RAT) PlugX variants in Setup appear in the official version of the game, the chain of infection as triggered through the download installer or update the game is legitimate, resulting in player's computer suffered Trojan intrusion.

Because APT is a customized, targeted attack, simple pattern analysis and signature-based protection mechanism can't be fully effective defenses. APT may use digital signatures to bypass the white list of security devices directly, bypass the sandbox / virtual environment by infiltrating a zero-day exploit or using encrypted code. According to the statistics report, APT mail attacks with social engineering are the most [23].

APT has evolved to bypass security mechanisms that are difficult to find with current technologies and require new security technologies to deal with these attacks. New technologies require big data analytics technology [1, 7-9, 11, 16, 29] as the core, integrated defensive technology, central control and accident forecasting technology. Therefore, we propose a big data analytics technology to extract data from multiple sources and resist unknown APT attacks.

* Corresponding Author

2 Related Technology

2.1 Advanced Persistent Threat

Advanced Persistent Threat (APT) [2, 6] is different from traditional attack modes, it is a systematic and planned attacks and targeted approach. APT's features more complex and customized, the "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. [24], often orchestrated by certain staff, aimed at specific targets. It is usually motivated by business or political, for a specific organization or country, and remain high for a long time hidden. Advanced is highlighted by the use of sophisticated malicious software and technology to take advantage of loopholes in the system, and avoid anti-virus software. Soon after the invasion, the characteristics of high because of its low profile and hide, for continuous la-tent viruses can attack without being noticed.

The "persistent" process is an external force will continue to monitor specific target, in that time, hackers will make confidential data collection and analysis efforts, and then slowly invading infection network system to the entire company or organization, and finally enabling data to be exported will be collected, and from which to get data. Threat the people involved in the planning of the attacks.

2.2 Advanced Penetration Attacks (APT) Detection and Defense

According to a trend micro TrendLabs study, 91% of targeted attacks using e-mail as the starting point of entry. In addition, the Ponemon Institute study shows 78% of targeted e-mail attacks using malware embedded in an attachment. It can be seen that through email is the attacker's minimum resistance and bypass existing security defenses [15, 19].

2.3 Big Data in the Application of Network Security

Big data is the process of analyzing large amounts of data from thousands of sources including a blog, a malicious IP location, email, information from the other attacks, in order to recognize patterns or anomalies, analyze trends, and final description organization to identify, isolate and neutralize APT attack [4-5, 13-14].

Meanwhile, big data analytics in the cloud can also be used as a centralized, APT attacks are detected immediately updated in another company to another company, even if they are in completely different industries in the world. Finally, from traditional antivirus software to dynamically under the data analysis of the evolution of cloud computing, prevention has changed dramatically for APT: emphasis on detection and response, rather than a focus on prevention.

2.4 Splunk Cloud Technology

Splunk [28] is applied to the machine data engine. It will collect all the IT systems and infrastructure (physical, virtual and cloud) the machine data, and indexes to use. Splunk Cloud provides the following capabilities:

Data collection. Splunk Cloud provides several options for sending data from a variety of sources to your Splunk Cloud deployment.

Ingestion. Splunk Cloud prepares incoming data for searching.

Storage. Your data is stored in a manner that is optimized for the cloud. You can configure data retention according to your auditing and compliance requirements.

Search. Your users can correlate data, visualize results, generate reports and alerts, and more.

Apps and premium solutions. Access to certain pre-configured dashboards, reports, data inputs, and saved searches that provide domain-specific solutions.

3 Research Methods

3.1 Experimental Flowchart

This experimental flowchart as Fig. 1, first set up two computer host in Taiwan, one attack computer is C&C Server, another was suffered APT success invasion of computer. Then began collection the log archives of hacked computer, using statistics analysis and data mining method for integrated analysis, to analyze obviously and the implied information and defined this class attack of sample and features.

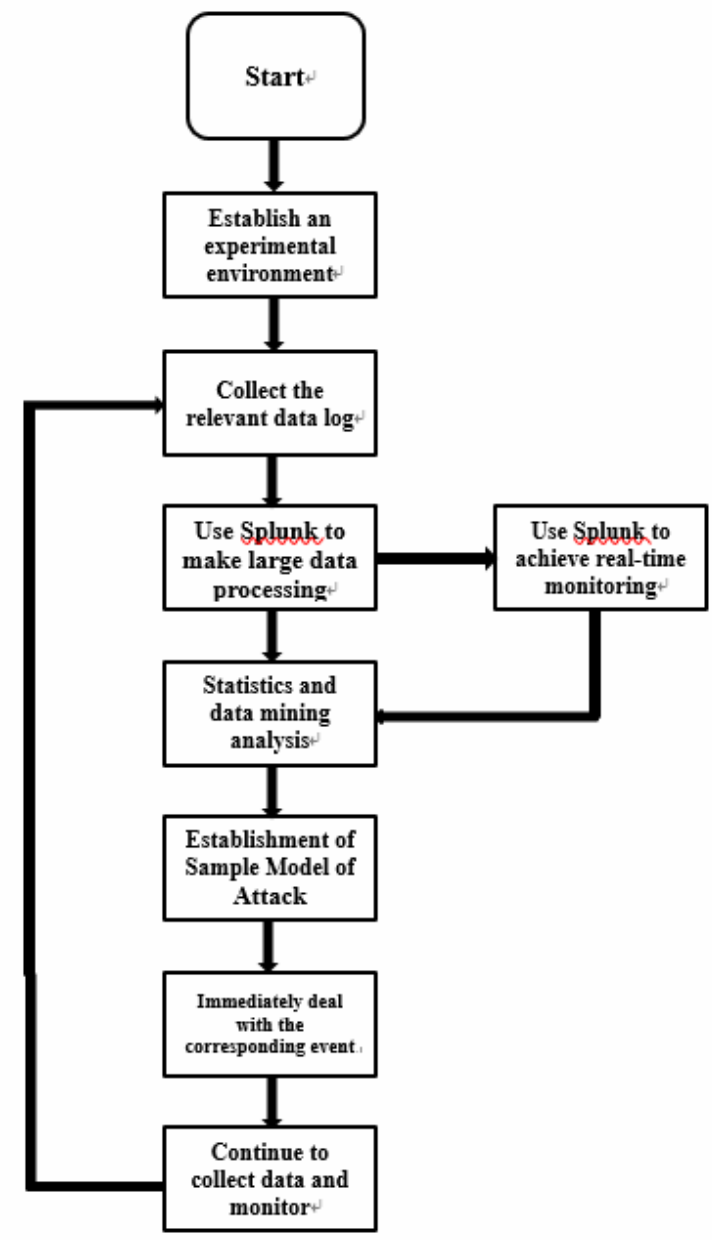

Fig. 1. Experimental flowchart

4 Experimental Simulation and Data Collection

4.1 Research Tools

Hardware and software equipment used in this study are as follows:

Attack computer: Intel Core i7-2620M 8G RAM
OS: Windows 7
Victim computer: Intel Core2 Duo 1G RAM
OS: Windows XP SP3
Use Software: Splunk, SAS
APT attack program: Poison Ivy [22]

4.2 Simulated Attack Environment

First we set up a victim notebook computer at Chinese Culture University laboratory, another C&C Server is installed on the home computer, using 100M non-fixed IP, using the floating IP. C&C Server IP no matter how changes can correct for victim computers online, the architecture is shown in Fig. 2.

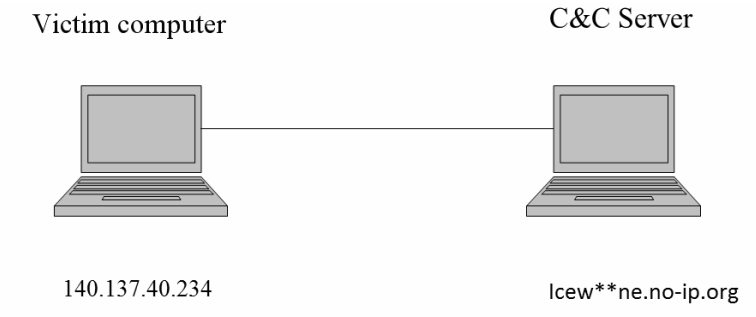

Fig. 2. APT simulated architecture

Attacker uses APT attack software Poison Ivy produces an attached file named .exe. Use the method of Exploit to put the virus into a common word file. And then use the social engineering traps, the word file using e-mail sent to the victim computer. When the victim computer to open this word file, the virus will follow the opening, and the victim did not know. Fig. 3 shows the execution of the Poison Ivy APT attack software.

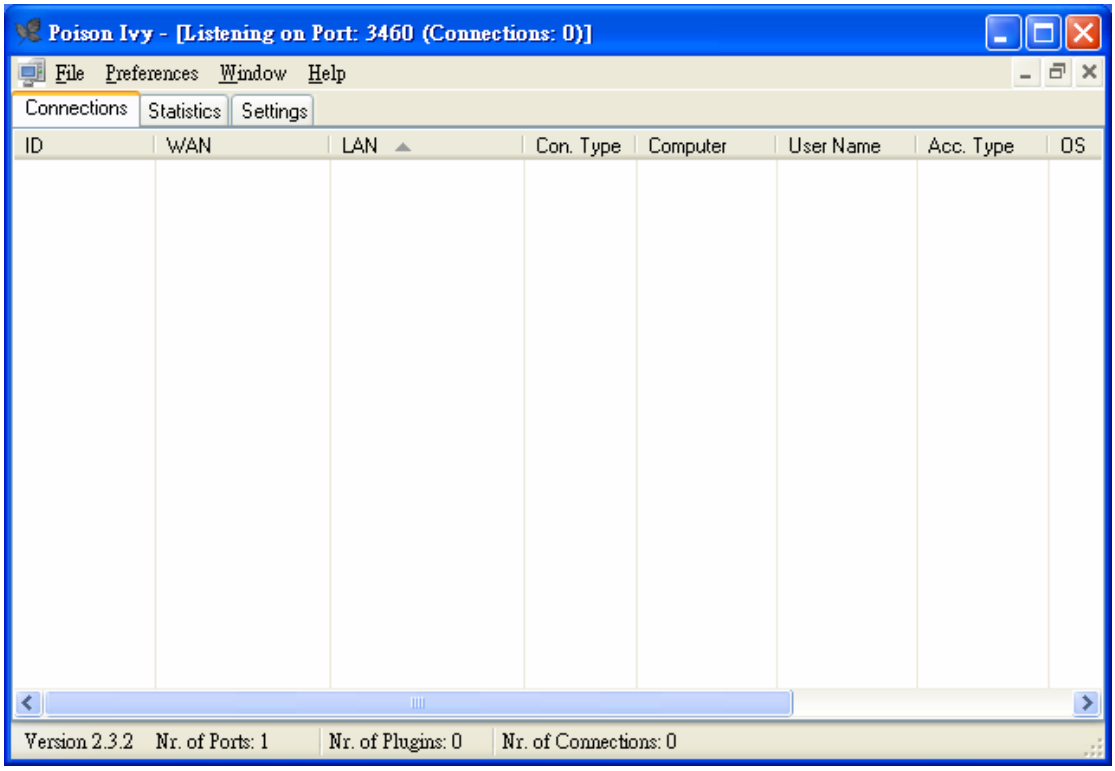

Fig. 3. Poison Ivy

When the victim computer boot and connected to the network, it will automatically connect to attack the computer, as shown in Fig. 4.

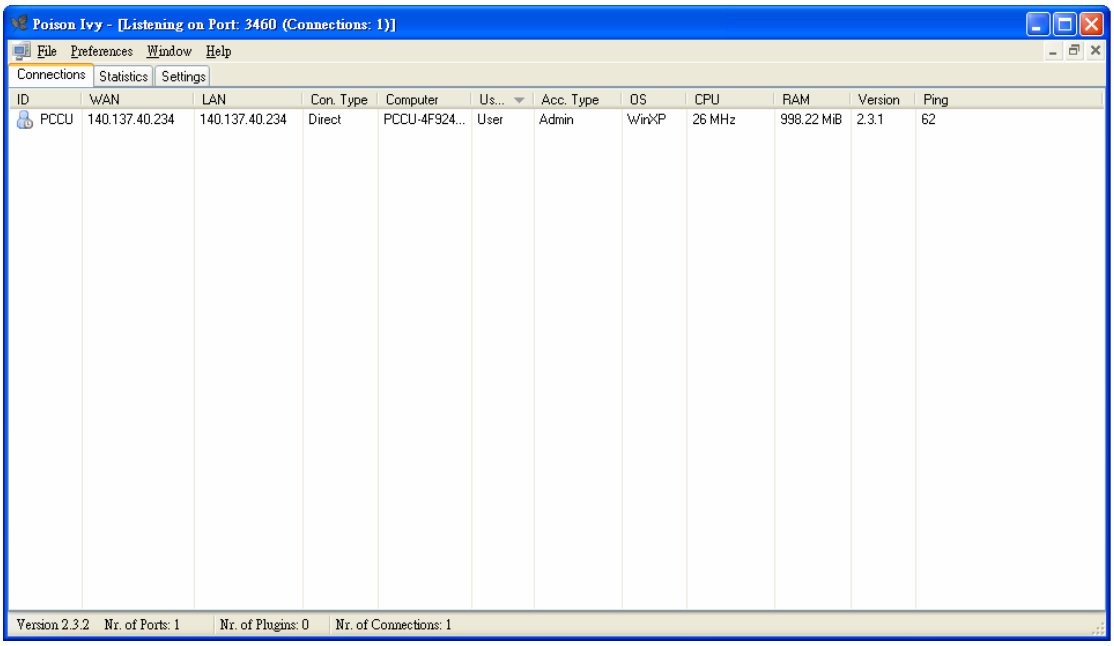

Fig. 4. Victim computer connection C & C Server screen

Fig. 4 shows the victim's IP, computer name, OS system, CPU, RAM and so on. Click the victim computer icon, you can see all the victim computer complete information.

Fig. 5 shows the victim's computer's full details, Fig. 6 shows the program in progress, services, recording for keylogger, Fig. 7 shows the victim's screen, and direct control of the victim.

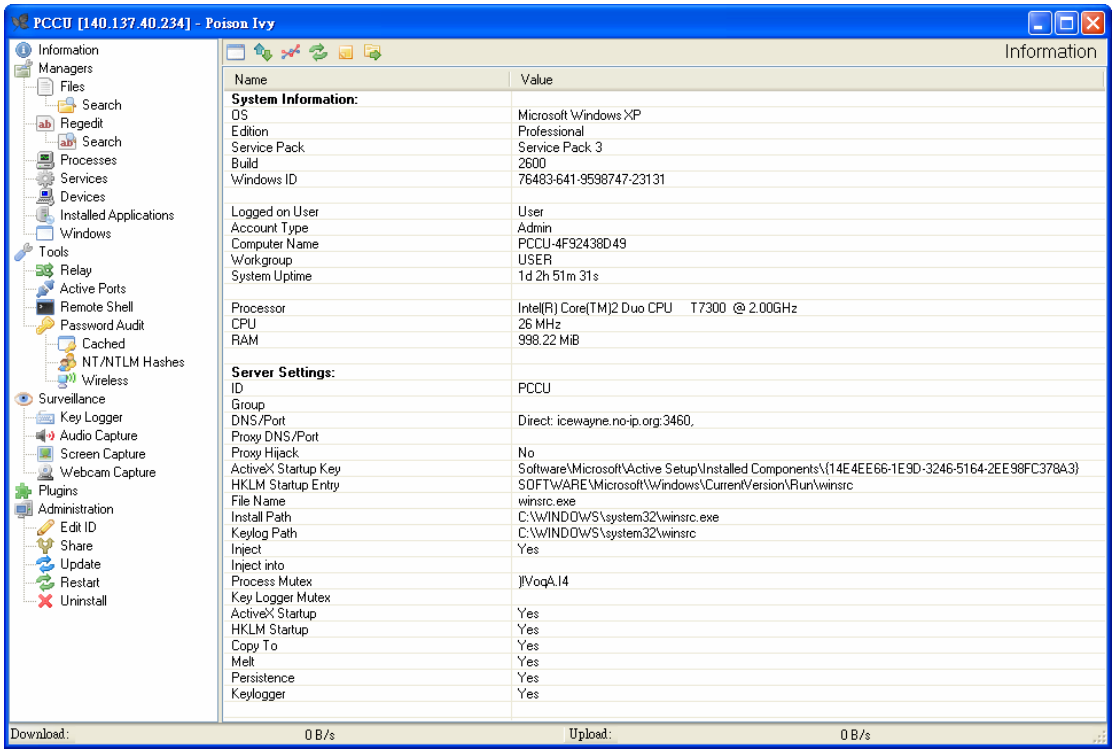

Fig. 5. Victim computer's full computer information

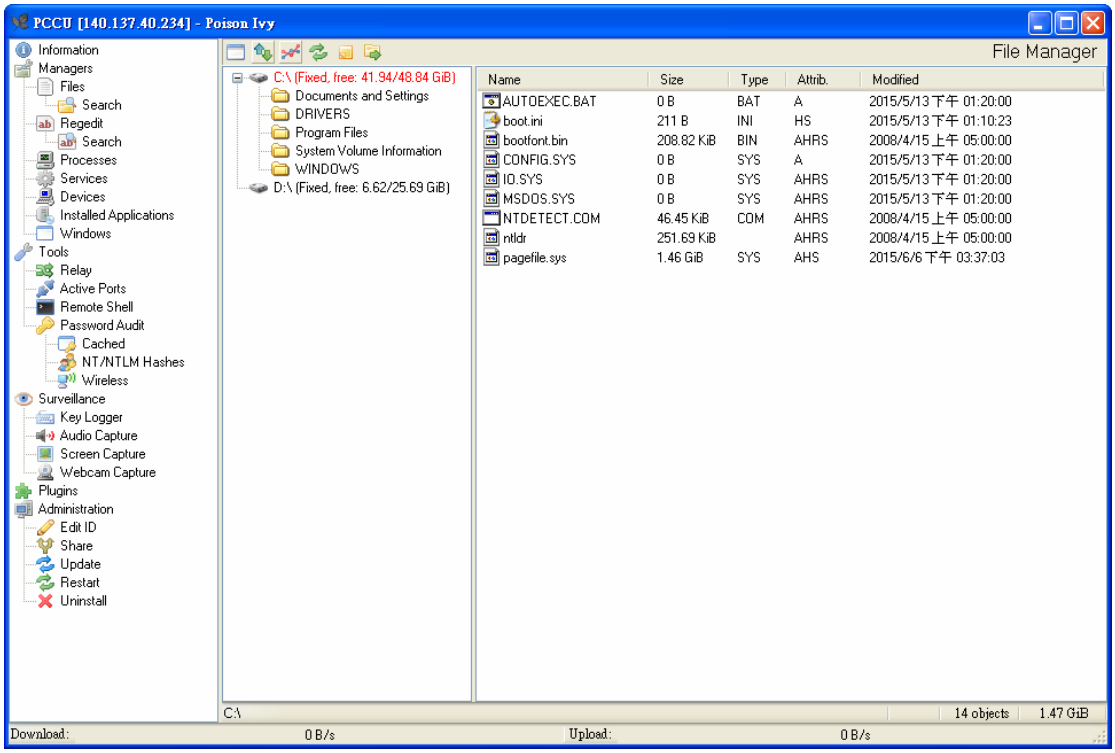

Fig. 6. Victim computer files can be uploaded or downloaded

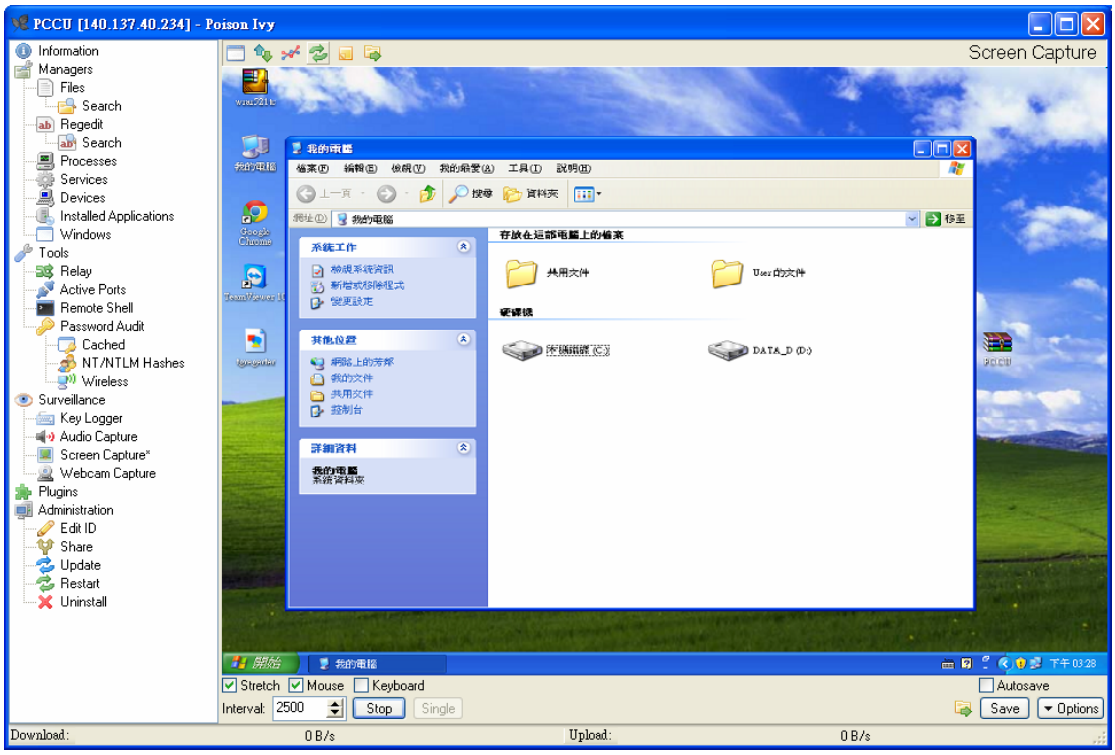

Fig. 7. Monitor the victim's computer screen and control

4.3 Use Splunk to Collect the Firewall log

Established the attack environment, we began collection victim computer of firewall log 14 days total 6,610,297 of data, as Fig. 8 shows. We using no-IP and non-fixed IP of set, created six APT of online to

C&C Server of IP, using Splunk processing, then find its suspicious of IP, as Fig. 9 for time within destination IP of online number.

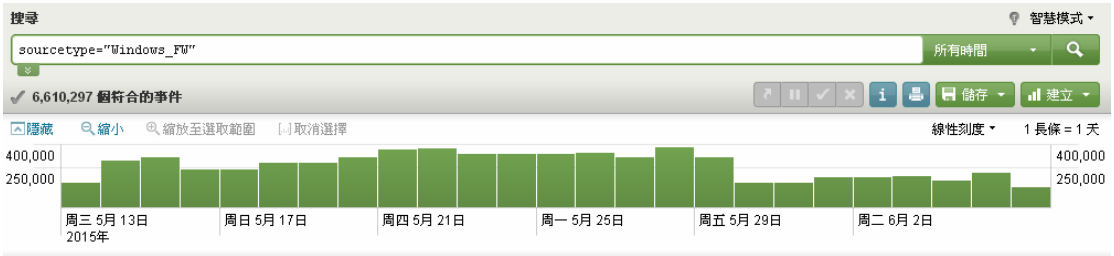

Fig. 8. Firewall log data

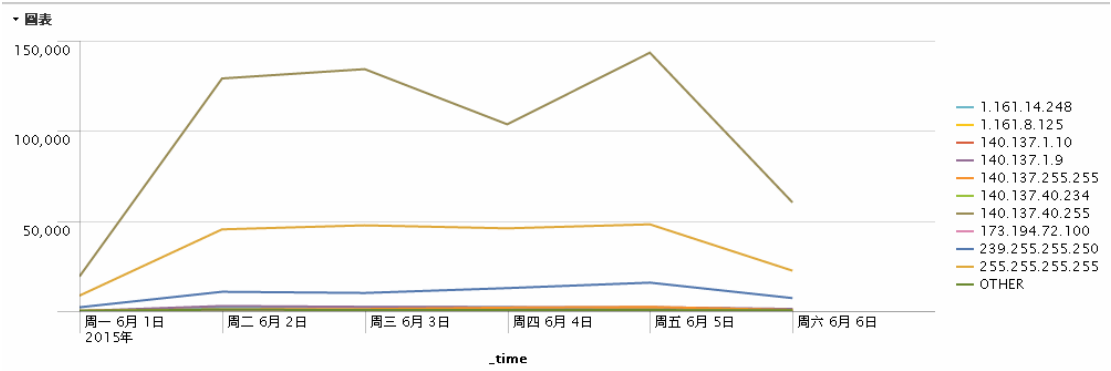

Fig. 9. The number of destination IP connections in time

Due to characteristic of APT, affected computers will be fixed with the C&C Server online. We observed a daily fixed-frequency IP as the same online, after entering the commands in the Splunk, the result shows in the following Table 1 and Fig. 10.

Table 1. Splunk suspected APT produce tables

	dst_ip			
	dist_ip	count	avg(gap)	var(gap)
1	1.161.14.248	6727	48.239964	363062.769769
2	1.1618.125	1671	40.472455	385.390193
3	1.161.8.39	1642	70.200488	1447087.211610
4	1.171.32.116	59.24	52.316900	429284.600841
5	1.171.138.124	12	2039.090909	17863267.890909
6	1.34.136.210	2	1142.000000	0.000000
7	5.135.104.98	1		
8	8.8.4.4	1598	758.351910	313748043.814678
9	8.8.8.8	10794	112.210507	42555482.431220
10	14.063.136	2	141.000000	0.000000
11	23.253.21.117	4	0.666667	0.333333
12	23.41.130.127	3	144.500000	31000.500000
13	23.41.130.230	2	438.000000	0.000000
14	23.41.133.163	38	51750.162162	32754009020.584087
15	23.41.134.165	5	56.500000	1974.333333
16	23.41.141.49	4	134.333333	18504.333333
17	23.48130.72	2	37.000000	0.000000
18	23.48.136.57	2	99.000000	0.000000
19	23.53.75.62	2	61.000000	0.000000
20	23.67.162.110	3	31.200000	412.700000

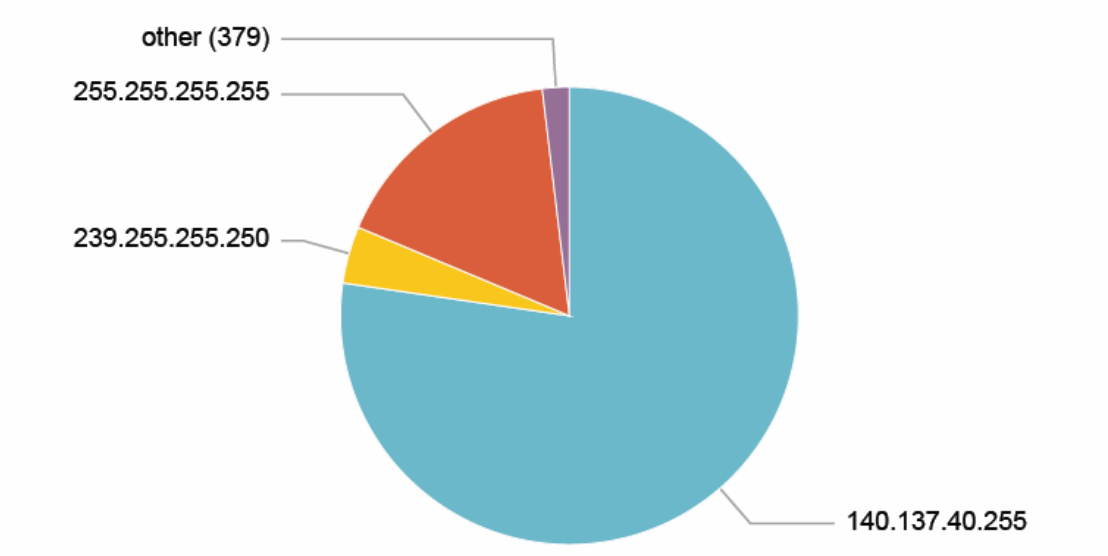

Fig. 10. Splunk produces a pie chart of suspected APT

In Fig. 11, dst_ip is the destination IP, count is the number of time the IP connection, avg (gap) is the average time to connect to the IP, var (gap) of Splunk are calculated variation value. From Splunk Technology handbook, we had known that the lower the number the more suspicious.

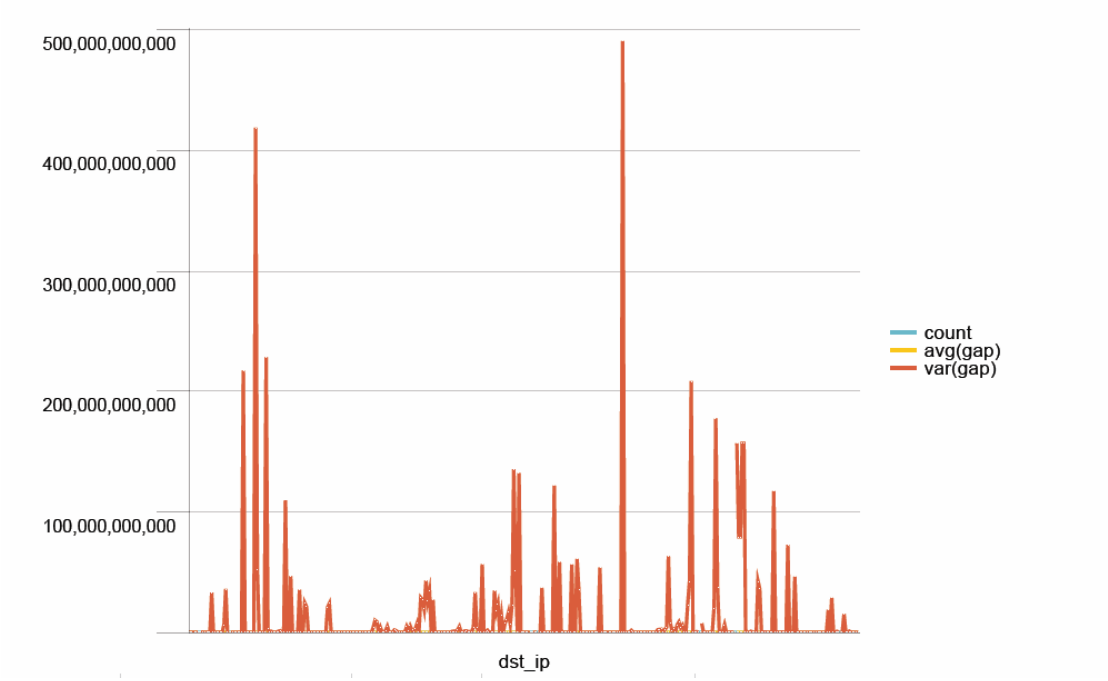

Fig. 11. Splunk generates a line chart of suspected APT

When we collected data through a firewall log to Splunk do big data processing, we got 271 suspicious IP data. Due to substantially reduce the amount of data to be processed, and Splunk can do follow-up treatment of direct export CSV format files.

4 SAS for Data Analysis

4.1 SAS Model Compare

After passing through the Splunk for big data processing, data exported from Splunk in order. This study analyzed using SAS statistical analysis software, first derived Splunk data into SAS EG storing SAS EM

format that can be read, and then into the SAS EM, first need to build a prediction model of APT, and work flow as Fig. 12.

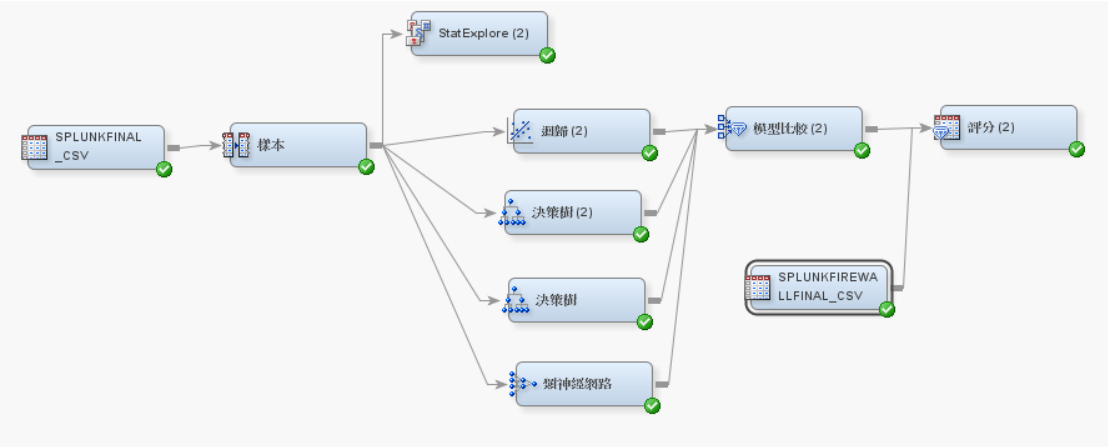

Fig. 12. SAS working flow chart

By the work flow chart, we use regression analysis, CHAID decision tree CART decision trees and neural network the four methods of data mining models. Tree refers to the CART decision trees, Tree2 is CHAID decision trees, and SAS is more suitable for the data that can be compared through SAS models, and numerical tables following figure graphically [3, 10, 17, 20, 21, 27].

In the following Fig. 13 for ROC diagram, ROC curve, closer to the upper-left corner of the better, it can be found the decision tree in figure is greater than the regression analysis and neural networks.

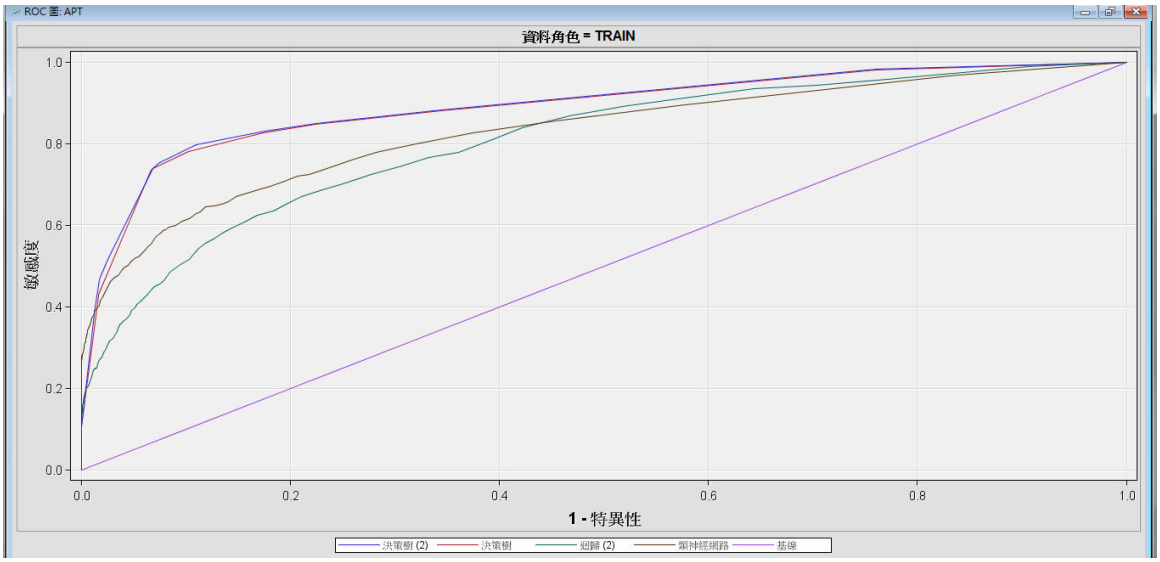

Fig. 13. The ROC diagram [12]

In the following Fig. 14 for Error classification ratio comparison, decision trees can be found in the figure the lowest error rate, and CART decision trees of the lowest rates of misclassification, this is competition important data.

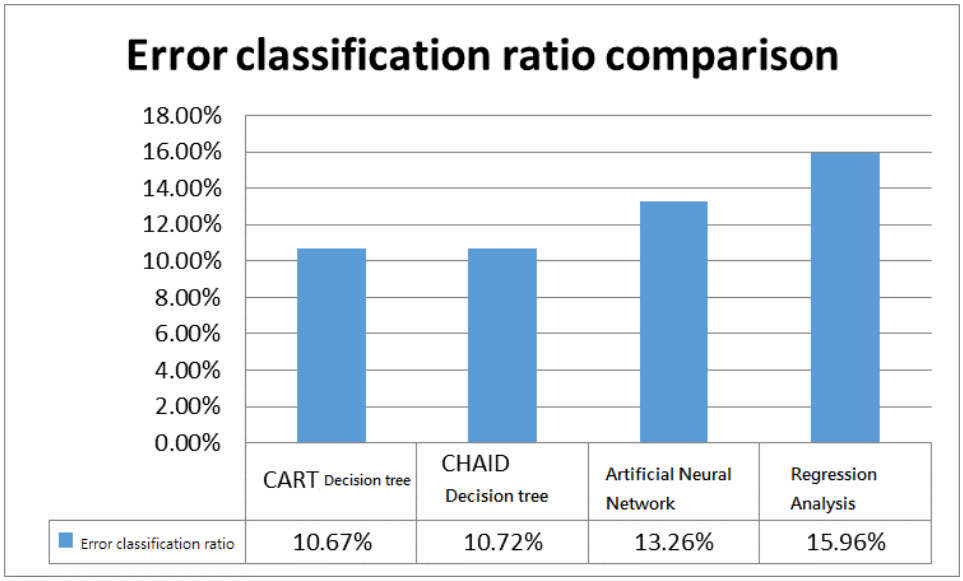

Fig. 14. Error classification ratio comparison chart

In Fig. 15 below for the maximum absolute error comparison, we can see from the figure, the neural network is the lowest value, followed by the decision tree.

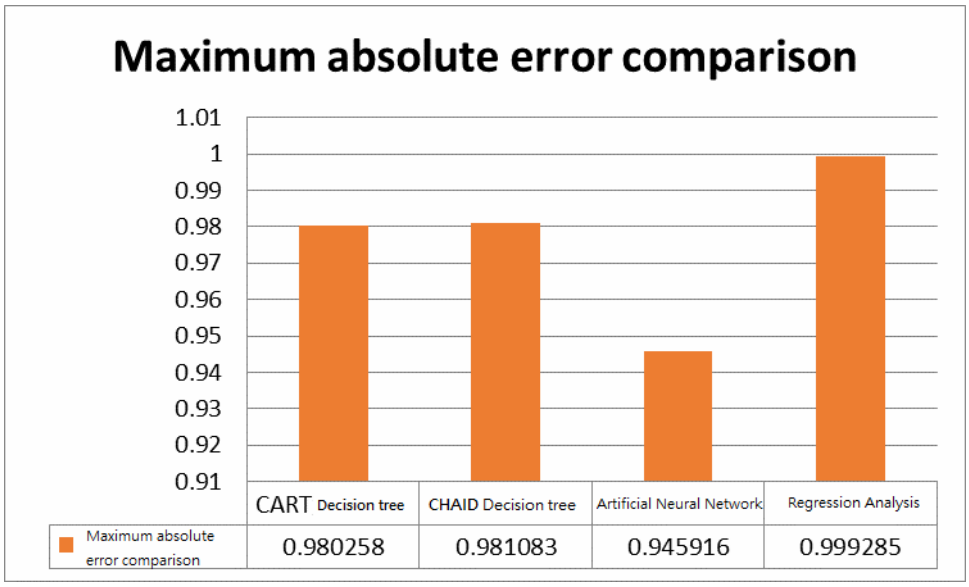

Fig. 15. Maximum absolute error comparison graph

In the following Fig. 16 for compare sum of squares error, two methods of decision tree that is better than the other two algorithms.

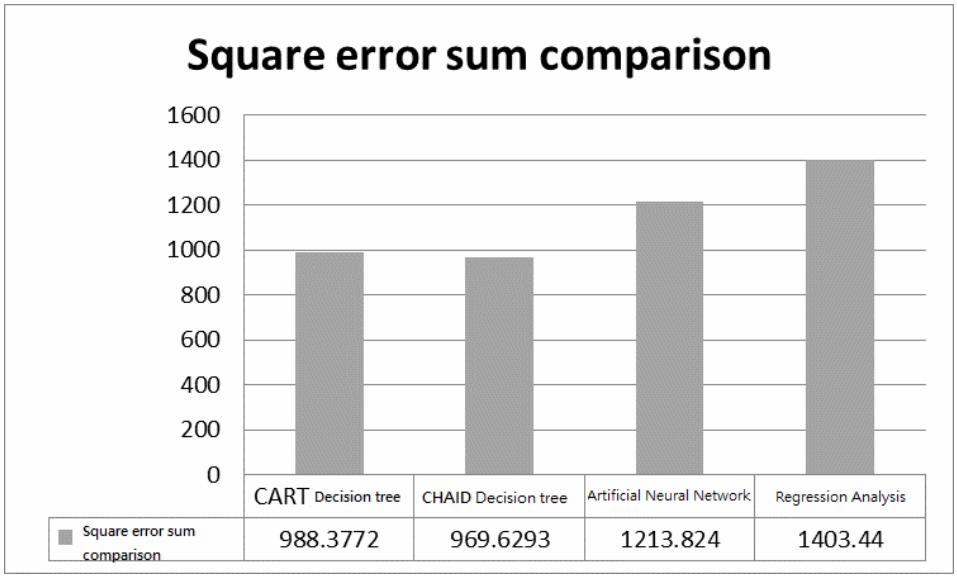

Fig. 16. Square error sum comparison graph

In Fig. 17 below, the mean squared error is compared, and on average, the decision tree is still better than the other two. The CHAID decision tree is slightly better than the CART decision tree.

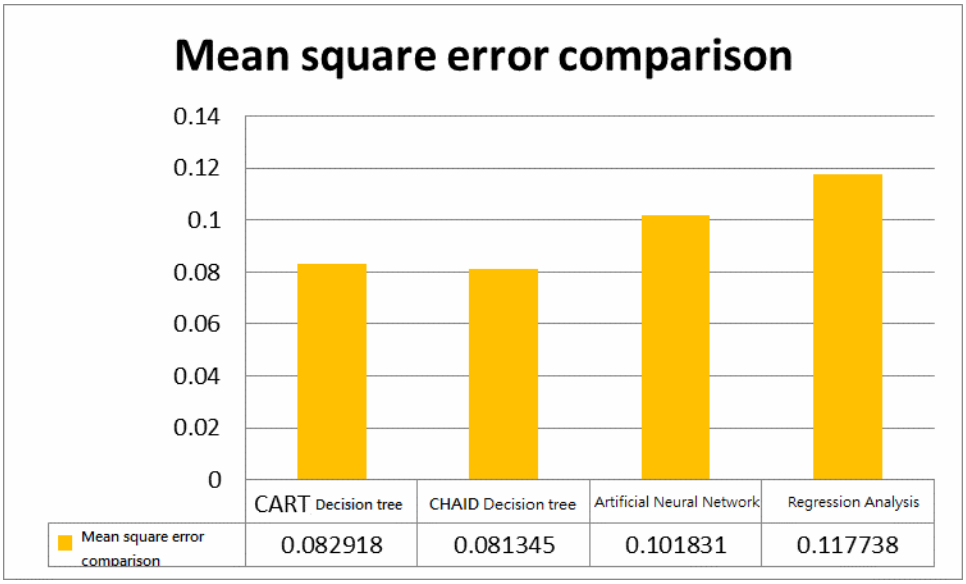

Fig. 17. Mean square error comparison graph

In the root mean square error of Fig. 18 below, the decision tree is still better than the other methods.

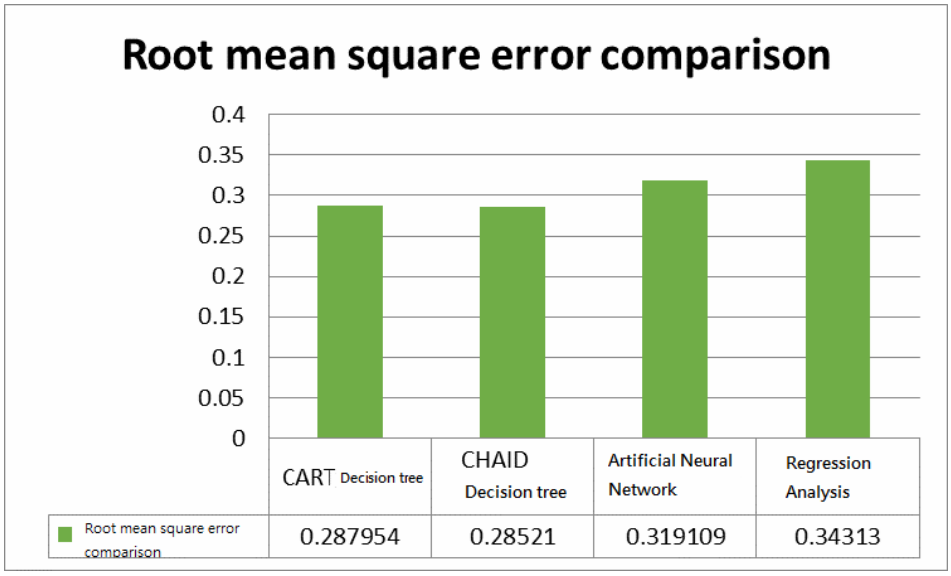

Fig. 18. Root mean square error comparison graph

Gini indices (Gini index) is the Gini coefficient multiply 100 times expressed as a percentage. If the Gini coefficient is "1", the minimum is equal to "0". Indicating a numerical absolute uneven distribution, while the latter represents the absolute value on average, but the two only in theory. Therefore, the actual value of the Gini coefficient between only 0~1. Gini coefficient is smaller numerical distribution is average, Gini coefficient, the greater the value the more uneven distribution. In this study for the prediction model, so there's no need to allocate on average, Gini coefficient, the greater the better. In the following Fig. 19, CHAID decision trees are slightly larger than the CART decision trees.

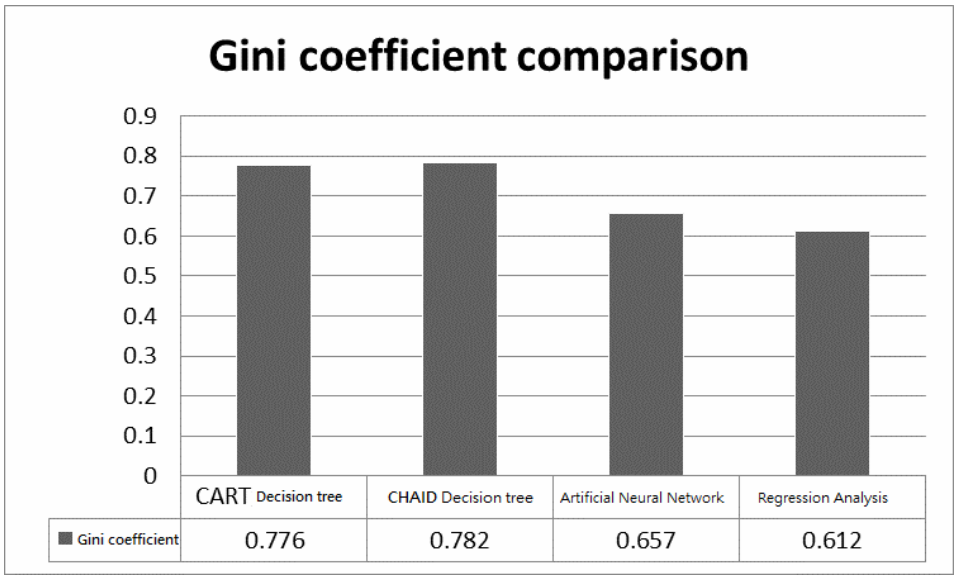

Fig. 19. Gini coefficient comparison chart

From the Fig. 20 compared of four algorithms, two decision trees are superior to regression analysis and artificial neural networks. Although the values are within close proximity of the two decision trees, but in the most important minimum classification error rate, CART decision trees have a minimum classification error rate of 10.67%, lower than other algorithms.

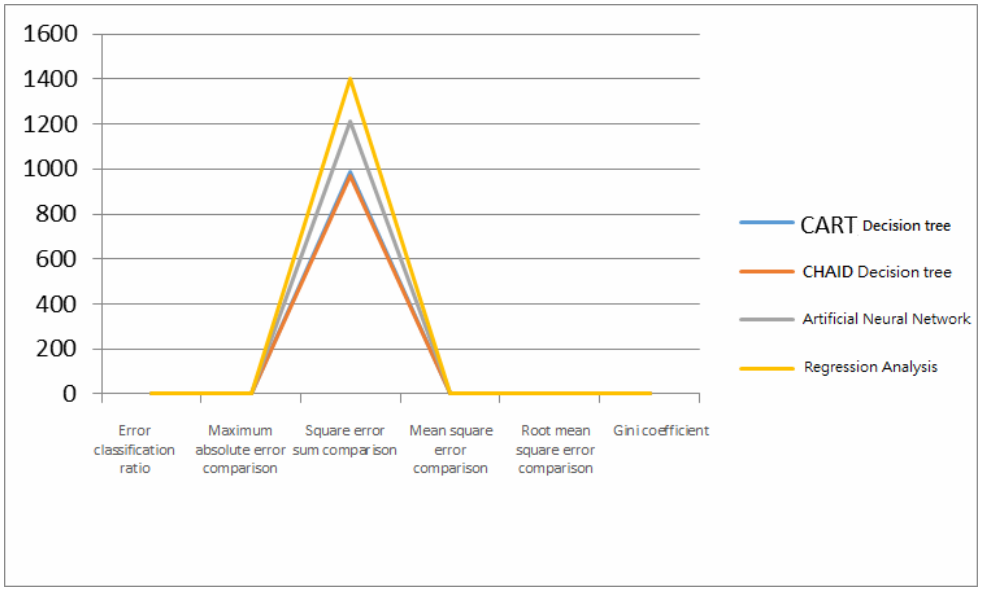

Fig. 20. Comparison of four algorithms

We often hear the decision tree algorithm [26]. This study will compare the CART and CHAID algorithms, as shown in the decision tree of Fig. 21 and Fig. 22. It is clear from Fig. 21 that CHAID has too few nodes and can't be a modeling tree. Therefore, the CART decision tree algorithm is used in this study, as shown in Fig. 22.

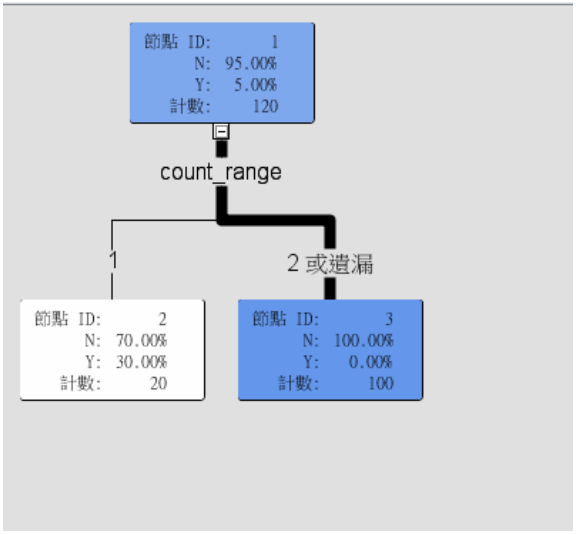

Fig. 21. CHAID decision tree

According to the previous literature, APT has a fixed frequency with the C & C Server connection characteristics. So we observe the count field (The more suspicious the number of connections), var field (Average daily connection frequency) and var (Variance). Fig. 22 shows that when count_range (count greater than or equal to 100 to 1, less than 100 is 2) is greater than 1, and avg_gap (average connection time) is less than 378, var_gap (variance) of greater than 1969690, then have a very high probability of APT in online IP, and called this decision tree for the APT model.

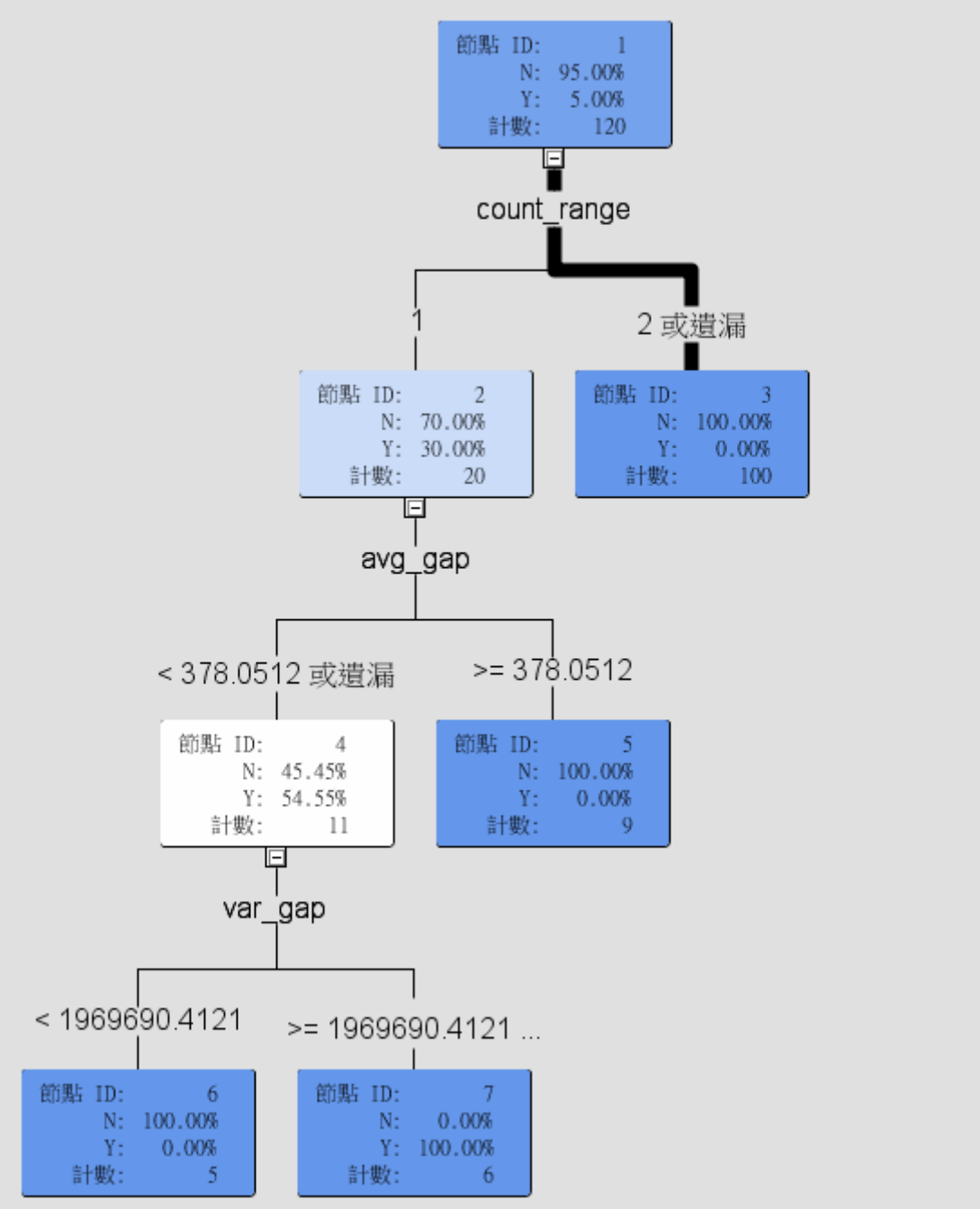

Fig. 22. CART decision tree

4.2 APT Attack Validation

After a prediction model is established, if you want to verify the APT attack, you can collect an unknown APT attack firewall information, through Splunk big data processing, directly into the SAS score, the results shown in Fig. 23.

	dst_ip	count	avg_gap	var_gap	count_range	到: APT	非常聰化到: APT	警告	節點	預測: APT=N	預測: APT=Y	未調整 P: APT=N	未調整 P: APT=Y	b_APT	節點	Probability for level Y of APT	Prob
1	168.95.1.1	2593.0	166.881559	4792290.869	1.0	Y	Y		7.0	0.0	1.0	0.0	1.0	1.0	7.0	1.0	1.0
2	192.168.1.1	2699.0	166.794663	4686303.133	1.0	Y	Y		7.0	0.0	1.0	0.0	1.0	1.0	7.0	1.0	1.0
3	1.34.136.210	1918.0	226.139802	8829502.915	1.0	Y	Y		7.0	0.0	1.0	0.0	1.0	1.0	7.0	1.0	1.0
4	203.69.81.41	2.0	144.0	0.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	19.0	3.0	0.0	1.0
5	94.31.29.154	8.0	22370.14286	3.252159954E9	2.0	N	N		3.0	1.0	0.0	1.0	0.0	19.0	3.0	0.0	1.0
6	54.230.158.195	2.0	133.0	0.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	15.0	3.0	0.0	1.0
7	103.243.222.63	3.0	0.0	0.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	20.0	3.0	0.0	1.0
8	64.233.187.136	18.0	18830.41177	5.471090886E9	2.0	N	N		3.0	1.0	0.0	1.0	0.0	13.0	3.0	0.0	1.0
9	103.243.222.9	2.0	11.0	0.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	11.0	3.0	0.0	1.0
10	64.74.13.21	6.0	112.6	24652.8	2.0	N	N		3.0	1.0	0.0	1.0	0.0	8.0	3.0	0.0	1.0
11	165.254.157.178	1.0	.	.	2.0	N	N		3.0	1.0	0.0	1.0	0.0	8.0	3.0	0.0	1.0
12	203.69.81.98	10.0	6.777778	413.444444	2.0	N	N		3.0	1.0	0.0	1.0	0.0	18.0	3.0	0.0	1.0
13	198.57.30.31	4.0	103.333333	8033.333333	2.0	N	N		3.0	1.0	0.0	1.0	0.0	20.0	3.0	0.0	1.0
14	103.243.222.31	4.0	6.0	108.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	14.0	3.0	0.0	1.0
15	124.108.136.141	24.0	161.652174	492089.9644	2.0	N	N		3.0	1.0	0.0	1.0	0.0	19.0	3.0	0.0	1.0
16	216.137.57.80	4.0	49.333333	1758.333333	2.0	N	N		3.0	1.0	0.0	1.0	0.0	3.0	3.0	0.0	1.0
17	54.225.67.75	8.0	20.857143	1285.142857	2.0	N	N		3.0	1.0	0.0	1.0	0.0	12.0	3.0	0.0	1.0
18	54.165.70.130	2.0	70.0	0.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	16.0	3.0	0.0	1.0
19	74.125.204.93	42.0	10339.65854	1.466959139E9	2.0	N	N		3.0	1.0	0.0	1.0	0.0	7.0	3.0	0.0	1.0
20	54.254.175.95	2.0	130.0	0.0	2.0	N	N		3.0	1.0	0.0	1.0	0.0	14.0	3.0	0.0	1.0

Fig. 23. Detect APT results

From the figure forecast: APT = Y field, 1 refers to the record as APT, “Probability for level Y of APT” This information shows that probability for the record is APT. Among the 493 IP records, there are 3 recorded IPs from which the model is detected, namely “168.95.1.1”, “192.168.1.1”, “1.34.136.210” respectively. Of the three IP records, 168.95.1.1 is Chunghwa Telecom’s DNS and 192.168.1.1 is the Gateway of the intranet. These two data are misjudgments. The remaining 1.34.136.210 is indeed the APT attack IP used to establish the environment. Even so, in the 493 data misjudged two records, the detection rate as high as 99.59%, we can see that the APT detection method provided in this study is correct and feasible.

4.3 The experimental results

After we collect IP log for APT connect to C&C Server, the information will be sent to Splunk, as shown in Fig. 24.

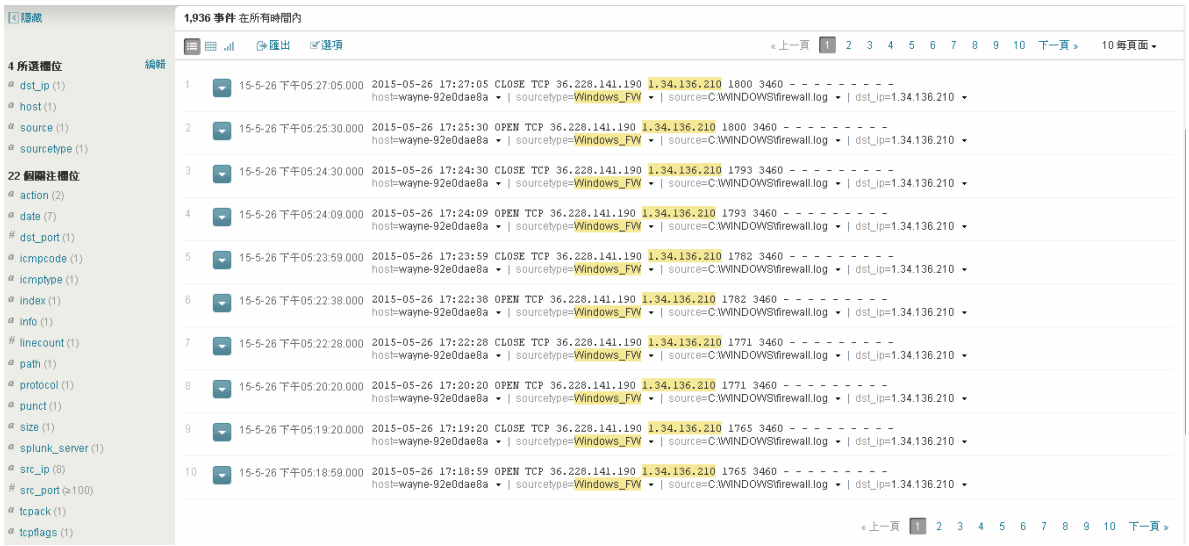

Fig. 24. Splunk network log

The Protocol is TCP and port of APT is 3460, you can use Splunk monitoring TCP 3460 port, real-time monitoring results, and from the APT IP firewall blocking, then step back and analyze the IP packet size, about loss. We Also find out that the IP was made by which computer internal network hosts, reperfusion treatment, such as to the computer immediately. When the APT event occurs again, Splunk may at any time issue a warning, in order to achieve real-time monitoring with real-time effects.

The article [18] also uses APT detection technology, using the MalPEF-er and N-Victims methods, with a detection rate as high as 97%. Our method detection rate reached 99.59%, the detection rate increased by 2.59%.

5 Conclusions and Future Work

This chapter will summarize this research and future research directions. Again, analyzing the logs to prevent APT attacks is necessary. Records and data mining are the most effective ways to deal with big data analytics, making information more valuable, and knowledge models highly relevant.

5.1 Conclusions

The main contribution of the method proposed in this study can be divided into:

Because APT is easy to invade successfully, this research can help the subsequent IP detection after successful APT invasion to find out the host and the loss situation.

Big data processing network log, not only can save time, hardware performance, network resources, but also can simplify too much unnecessary data.

Using data mining and decision trees, you can reduce network-triggered event log data to "behavioral pattern rules." The rule to be summarized directly as a prediction model, experimental verification with high credibility.

5.2 Future Work

APT attack threat, even the best detection technology, there will still be missed. The best defense APT strategy is to have good habits of the Internet, not to download unknown files, is the response to the APT.

In the future development, we hope to improve the detection rate of unknown attacks in the absence of a prediction model so as to achieve a more complete and comprehensive prevention effect. Expect to be able to do all stages of defense against APT attacks in order to achieve more comprehensive results.

References

[1] The Economist, Data, data everywhere. <http://www.economist.com/special-report/2010/02/25/data-data-everywhere>, 2010 (accessed 09.12.12).

[2] C. Tankard, Advanced Persistent threats and how to monitor and deter them, Network Security 8(2011) 16-19.

[3] J.R. Quinlan, Improved use of continuous attributes in C4.5, Journal of Artificial Intelligence Research 4(1996) 77-90.

[4] P. Liu, F.-J. Zhang, GA-LMBP algorithm for supply chain performance evaluation in the big data environment, Journal of Computers 28(5)(2017).

[5] H.-C. Chu, C.-H. Hsu, M.-H. Yin, G.-G. Wang, The digital traces uncovering of generic gmail/Facebook instant messaging sessions via the IE browser as probative evidences, Journal of Computers 28(2)(2017).

[6] I. Jeun, Y. Lee, D. Won, A practical study on advanced persistent threats, in: Proc. Computer Applications for Security, Control and System Engineering, 2012.

[7] S.-W. Ahn, N.-U. Kim, T.-M. Chung, Data analysis system concept for detecting unknown attacks, in: Proc. 16th International Conference on Advanced Communication Technology, 2014.

[8] R. Magoulas, B. Lorica, Introduction to Big Data, Release 2.0, (O'Reilly Media), Sebastopol, 2009.

[9] L. Breiman, J.H. Friedman, R.A. Olshen, C.J. Stone, Classification and Regression Trees, Chapman & Hall, New York, 1984.

[10] G. Kass, An Exploratory technique for investigating large quantities of categorical data, Applied Statistics 29(2)(1980) 119-127.

[11] S. Zeng, Z. Lin, Y. Weng, Data Mining Applications Using SAS Enterprise Miner, Merlin, Taipei, 2012.

[12] W. Huang, Z. Wang, Use R Language to Get through the Large Data of the Meridians, TopTeam Information, Taipei, 2014.

[13] Y.-H. Sha, The defense of DDoS attack by heterogeneous tracers, [thesis] Hsinchu: Chung Hua University, 2010.

[14] W.-K. Lin, A study of government agencies in social engineering exercise based on attacks from malicious email samples: the case of an agency, [thesis] Taoyuan, Taiwan: National Central University, 2014.

[15] H. Chi, A study on the impacts of advanced persistent threat (APT) on corporate information security policy, [thesis] Taipei, Taiwan: Chinese Culture University, 2014.

[16] M.-K. Yang, Internet Hacker's behavior characteristics analysis by decision tree based on attempted to get administration authority, [thesis] New Taipei, Taiwan: Huafan Univetrsity, 2007.

[17] S.-T. Liu, The study on retrospective detection approaches for uncovering potential APT victims, [thesis] Taoyuan, Taiwan: National Central University, 2012.

[18] B. Corson, Stop targeted Email attacks: removing the path of least resistance for attackers. <http://blog.trendmicro.com/stop-targeted-email-attacks-removing-path-least-resistance-attackers/>, 2014 (accessed 23.06.14)

[19] J.R. Quinlan, Induction of decision trees. <http://grc.mnnu.edu.cn/~fmin/ materials/course/roughsets/references/QuinlanJR 1986_InductionOfDecisionTrees.pdf>, 1986.

[20] J.R. Quinlan, C4.5: programs for machine learning. <https://link. springer.com/article/10.1007/BF00993309>, 1993.

[21] FireEye, Inc., Poison Ivy: assess damage and capture information. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf >, 2015 (accessed 15.04.15).

[22] Wiki Zero-day. <http://en.wikipedia.org/wiki/Zero-day_%28computing%29>, 2015 (accessed 15.04.15).

[23] Wiki Advanced persistent threat. <https://en.wikipedia.org/wiki/Advanced_persistent_threat>, 2015 (accessed 15.04.15).

[24] Wiki Exploit. <http://en.wikipedia.org/wiki/Exploit_(computer_security)>, 2015 (accessed 15.04.15).

[25] Y. Huang, From the government, business to individuals are hackers locked APT attack object. <http://www.ithome.com.tw/news/91262>, 2011.

[26] Decision tree for living and learning (3): Using the SAS EM decision tree for CHAID and CART analysis, SAS knowledge+. <http://www.sasresource.com/artical72.html>, 2015 (accessed 15.04.15).

[27] Splunk Inc. <http://zh-hant.splunk.com/>, 2015 (accessed 15.04.15).

[28] Information Security Editorial department, <2014 Asia Pacific Security Forum Post Show Report> APT program duel-DDoS practices are more varied. <https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7830>, 2014.