Journal of Engineering and Applied Sciences 13 (Special Issue 2): 2872-2877, 2018
ISSN: 1816-949X

Case Study of Application of Integrated Control and Management System Based on Inter-Collaboration Against Cyber Threat

[1]Kyuil Kim, [1]Wonhyuk Lee, [1]Buseung Cho, [1]Dongkyun Kim and [2]Hyungwoo Park
[1]Department of KREONET Operation and Service Division,
Korea Institute of Science Technology Information (KISTI), Korea
[2]Department of KREONET Center, Daejeon, Korea Institute of Science Technology Information (KISTI),Korea

Abstract: Internet is the most prominent means of communication and information sharing in our lives at present. However, the incidences of internet abuses such as cyber-attacks have increased steadily. Defense system protecting against cyber-attacks tend to be able to respond adequately to well-known attacks rather than unknown ones. However, security managers overseeing computer systems find it very difficult to gain access to comprehensive information protection systems and lack the knowledge that they need in order to respond to new types of cyber-attacks effectively. We propose an expeditious and precise response mechanism which we describe through a case study of the application of an integrated control and management system. This system can help participating institutions cope with cyber threat occurring in KREONET well as within hosts and their own resource. We also present security mechanisms that respond efficiently to future cyber threats using statistical analysis based on data collected by our system. Therefore, we performed statistical analysis on incidences of cyber-attacks that occurred in KREONET from April 1st to July 31st, 2017 and could provide prompt and correct response to help in the prevention of malware and ransomware.

Key words: Cyber-attacks, ISP CERTs, inter-collaboration, hacking, cyber threat, cyber

INTRODUCTION

Today, most people communicate social media more often than spending time face-to-face. For example, 30 billion contents is shard using Facebook and about 67% of global consumers actively access online banking their mobile phones. The internet has also to the proliferation of new technologies such as IoT, AI, big data which IT environments need to work with. However, incidences of cyber-attacks are on the rise. Such attacks negatively impact a lot of people. In particular, cyber-terrorism destroys the information systems of a government and thus hampers a country's functioning is threatening our cyber space. Recently, cyber security systems have been responding to cyber threats through sources such as ISP CERTs and security center for each field. However, they continue to remain exposed to several cyber-attack's because they operate independently. The security managers of an organization need to respond to upon sources such as ISP CERTs and security monitoring centers because it is difficult for them to personally oversee all the server, PCs and related devices in their own institutions. Consequently, to perform these duties effectively, these managers require comprehensive technical, administrative and physical information on protective measures rather than having to defend network security with incomplete information that does not address all vulnerabilities. However, management organizations are too numerous to respond intensively based on security monitoring. Therefore, institutions cannot defend themselves adequately against even well-known attacks and great damage has occurred in the past.

We developed an integrated control and management system that collates and shares all detected security events in sources such as ISP CERTs and security monitoring center to enhance collaboration and solve problems jointly. Our system integrates detected events transmitted from several source removes duplicate information about the same events and notifies relevant organizations in real time. Thus several institutions are provided with detailed security monitoring through single medium. We also present countermeasures for a cyber threat using statistical analysis based on the integrated control and management system in KREONET environment. KREONET refer to Korea Research

Corresponding Author: Buseung Cho, Department of KREONET Operation and Service Division, (KISTI), 245 Daehanno, Yuseong, 306-806 Daejeon, Korea

Environment Open NETwork. It provides global research assistance, so that, R and D and collaboration is possible anytime, anywhere. KREONET provides information security services through CERT-KREONET and carries out activities that provide advanced security and prevention of attacks to minimize the damage caused by hacking. We performed statistical analysis for the security type, event and port from April 1st to July 31st, 2017 in KREONET and could provide prompt and correct response to help in the prevention of malware and ransomware.

During that time, there were 365 cases of responses to cyber-attacks of which about 82.2% (i.e., 300) were of the worm type, a malicious program that replicates itself repeatedly and spreads over a network rapidly, disrupting computer systems and harming the network. TCP 80 was involved in 230 incidents, i.e., 68% of the time. This result demonstrates that the attack occurs through connections to the web. In terms of attack events, mass-sql injection accounts for 50.5%, i.e., 171 counts. This attack involves the fraudulent transmission of login information to third-party system when users log on to a web page after the attacker inserts the malignant code on to the target web page.

Literature review: Recently, IT technology is leading the fourth industrial revolution based on converging and open science. For example, fusion research has resulted in new technologies such as AI, IoT and block-chain. In addition, security fields (Ko *et al*., 2014; Settanni *et al*., 2017; Ghafir *et al*., 2016; Gandhi *et al*., 2011; Svoboda *et al*., 2015; Moosavi *et al*., 2015) have published valuable research. However, security concerns are not share institutions tend to prefer a closed environment owing to the sensitive security issues because they handle critical user information. Therefore, hacking attacks have harmed institutions considerably. Institutions are limited by the fact that they have many systems protected by different security measures but they cannot protect all these resources because of low budgets and limited manpower. Similarly, ISP CERTs and security centers do not intensive monitoring for any particular institution because they multiple clients.

Though security information of each institution is sensitive, they must mutually share security events that they detect. Currently, institutions do not individually transfer relevant information to ISP CERTs and security centers. In this study, we demonstrate the advantage obtained through inter-collaboration between institutions as compared to when individual institutions hide their sources. We then propose the techniques that respond to cyber threats based on our inter-collaboration management system.

MATERIALS AND METHODS

Realization of integrated control and management system Security system of KREONET: In this study, we provide the definition and construction of our system to protect the secure information source based on KREONET shown in Fig. 1. KREONET operates 17 local network centers and built IDS (Intrusion Detection System) to detect real-time cyber threats. KREONET also collaborates with internal and external CERTs, ISP and security center to address cyber-attacks. The security system of KREONET unifies the management structure to quickly and accurately respond to cyber threats and helps other security organizations to collaborate. Inter-collaboration includes the RBL (Real-time Blocking List), block domain and cyber threat trends. Our system responds more effectively to cyber-attacks and supports backbone network control during DDOS and other large scale attacks. Integrated control and management system conducts intuitive monitoring using the dashboard for real-time progress status and statistical analysis.

Functioning of integrated control and management system: We illustrate the functioning of the integrated control and management system in Fig. 2. Our system unifies and automatizes threat management processes (registration, notice, response) for inter-collaboration in ISP CERTs and security monitoring centers. Integrated control and management system consists of the (global) threat management, network control support, RBL, security information sharing, statistics and dashboard.

Global management: It rapidly and effectively supports the necessary registration, notice and response when it transfers cyber-attacks detected in internal and external ISP CERTs and other sources to our system. Its main parameters are detection date, detection time, security event type, departure IP, port, destination IP and port. It can confirm not only the progresses for the registration and response of cyber-attack but also relevant history for the status of actions.

Network control support: It provides international common countermeasure (network supporting, verification and control) if it controls the network a large scale cyber-attack (e.g., DDoS). Its primary function is one of supporting control, including control IP, period of occurrence and block supporting reason.

RBL: RBL (Real time Blocking List) provides relevant functionality for RBL registration, notice and response (non-block, block) if ISP CERTs and security center notify

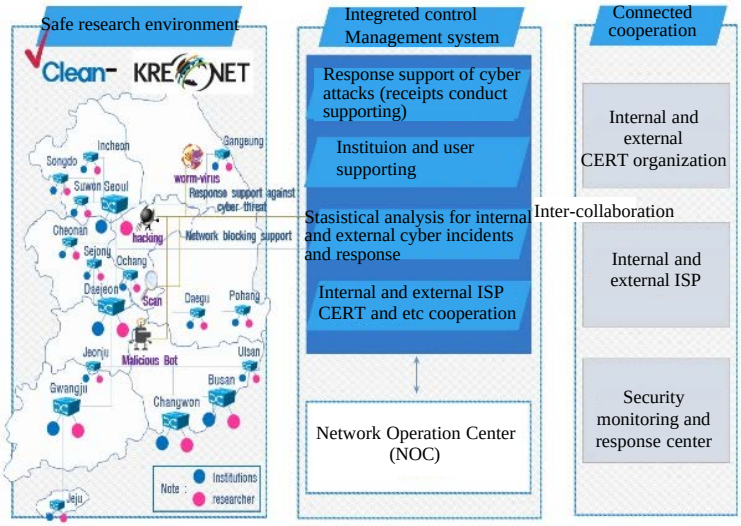

Fig. 1: Security system based on KREONET

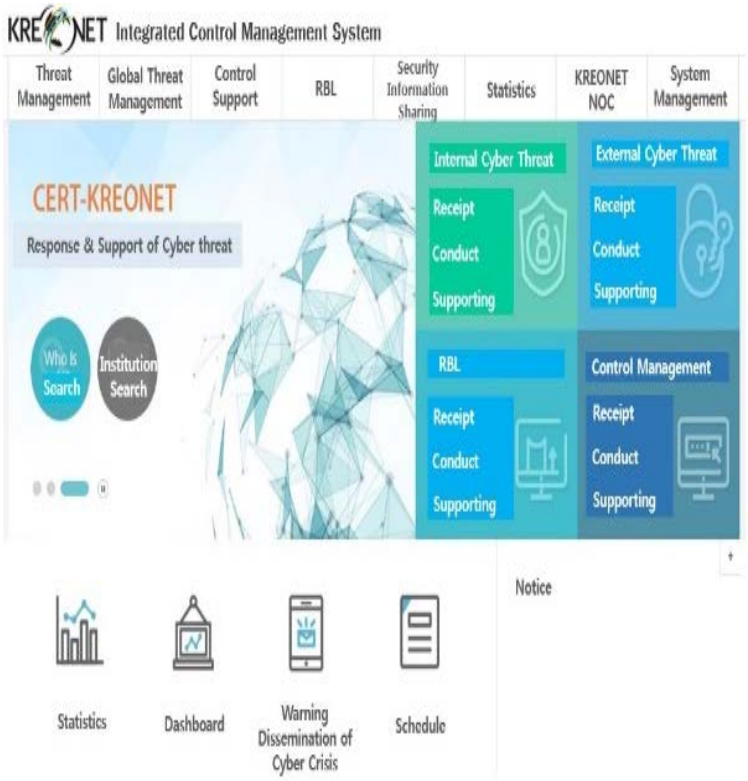

Fig. 2: Existing and proposed model comparison

RBL to local ISP after they detect malignant behavior that infected system transfer, e.g., spam mail which targets the system. RBL requires a rapid response because the client's circuits are blocked if client receive them.

Security information sharing: It shares data such as black IP, malignant URL and code and provides security information to institutions.

Statistics: It analyzes cyber-attacks and the history of control supporting and shows the current situation for

cyber threat. Major parameters include the statistics of attack type, per-port, per-nation, per-event and response history.

Dashboard: It provides modular and complete visualization that intuitively confirms if the incident of global threat, control supporting and RBL has occurred in KREONET.

RESULTS AND DISCUSSION

Statistical analysis of integrated control management system: In this study, we draw cyber threat trends and the associated countermeasures through the statistical analysis of our system. Figure 3 shows the statistical analysis of cyber threat and sensitive information.

We perform statistical analysis for cyber-attacks from April 1st to July 31st, 2017 in KREONET. First, during that time, there were 365 counts of response to cyber-attacks of which about 82.2% (300 counts) was virus as listed in Table 1 worm virus is a malicious program that replicates itself repeatedly and spreads over a network rapidly, disrupting computer systems and harming the network. There were 33 incidences of DDoS attacks which send a large quantity of senseless traffic to the target system. Almost all institutions are exposed to cyber-attacks because they all provide access to web services. Thus, they need a suitable response to cyber crises by collaborating with ISP CERTs and security monitoring centers to protect themselves from DDos attacks. There were 4 counts of homepage forgery attacks which cause damage to the homepage or web page insertion attack using web vulnerabilities. The most recent attack trends have occurred in the drive by download attack that infects a system with malignant code when a user connects to the Internet with the intention of hacking into an organization for economic profit. Therefore, the security manager of each institution requires regular updates on security monitoring their web site in real time. Hop-point misuse also occurred once. This attack involves an attacker

Table 1: Cyber-attack types in KREONET

Security type	April	May	June	July
Worm virus	57	106	72	65
DDos attack	5	6	7	15
Homepage forgery	1	1	1	1
Hop-point misuse	1	-	-	-

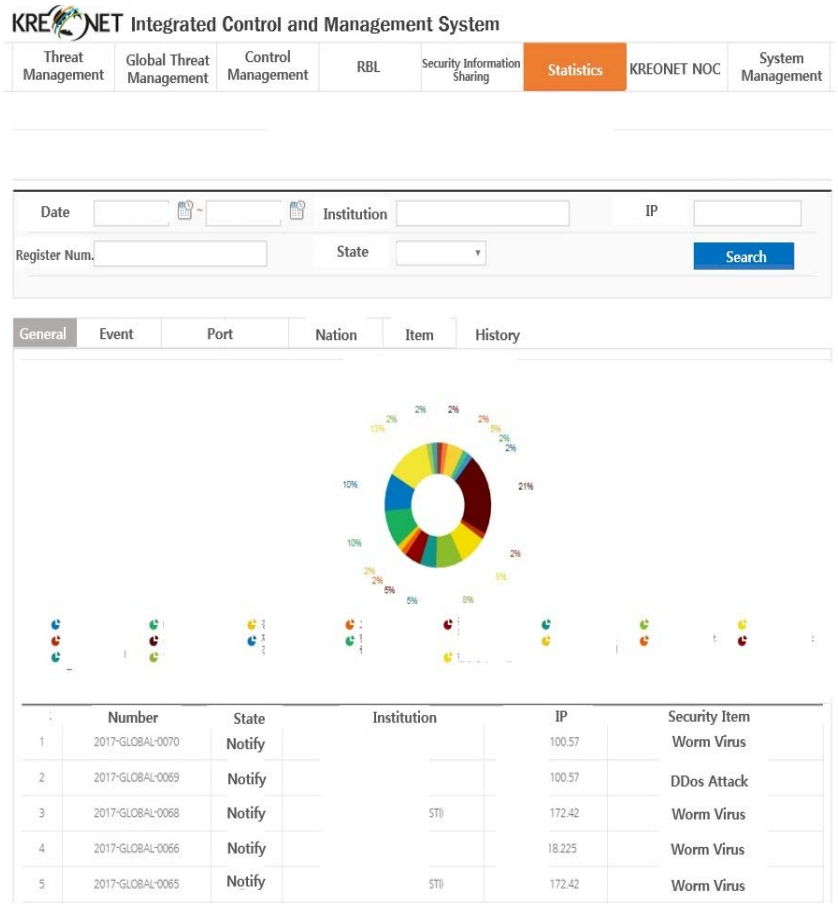

Fig. 3: Process of global treat management

Table 2: Top 5 port cyber-attacks in KREONET

Port	4 months
TCP 80	230
TCP ANY	52
TCP 445	20
TCP 22	5
TCP 23	4

Table 3: Cyber-attack events in KREONET

Security event	April	May	June	July
Mass-SQL	35	66	41	29
Darknet	1	6	11	19
Ransomware	2	19	7	8
Malicious URL	4	2	-	1
TCP SYN flooding	5	-	2	-

attempting the middle-point to attack other sites after hacking. The hacker searches for exposed server information and dominates them after identifying their vulnerability. Therefore, reducing exposure of critical resources is crucial.

In case of the port stats, TCP 80 was 203 counts, i.e., 68% as listed in Table 2. We know that their attack occur frequently because users typically keep the institution homepage open. Second, TCP ANY occurred 52. A hacker targets attacks through various ports. Third, TCP 445 is SMB (Server Message Block) port and a decryption of encrypted files himself after they illegally encrypt important files belonging to a user. TCP 22 is a telnet port and a hacker attempts the remote connection after infecting the target server using this port.

Amongst cyber-attack events, mass SQL occurred 171 times, i.e., 50.5% of the time as listed in Table 3. This event sends a user's login information to third-party server if user checks web page that hacker has inserted malignant code into. Darknet (Ko *et al*., 2014; Lagraa and Francois, 2017) event occurred 37 times and it used unused IP addresses. Darknet does not involve a real system because of the unused IP. Therefore, we regard darknet as an attack action by a hacker. We also observed 37 incidences of ransomware attack (Zavarsky and Lindskog, 2016; Ye *et al*., 2017). This event proliferates around the globe in which users cannot access their own files because it is encrypted by ransomware. Malicious URL is similar to mass SQL event as stated above. TCP SYN flooding massively sends SYN packets to target servers in a short time. Packets lose destination overloads with SYN+ACK packets and consequently, a user cannot connect to infected webpages.

We derived two results through statistical analysis. First, the above statistics is the response result through inter-collaboration of each institution, ISP CERTs and security center and other sources. Therefore, the defense of cyber-attack can be robust when related security organizations cooperate as compared to when individual organizations independently manages security system in single institutions, without collaboration. Secondly, inter-collaboration quickly and correctly establishes the appropriate security monitoring and response environments when an integrated control and management system which does not exchange simply e-Mail is built and utilized.

CONCLUSION

We proposed a case study of application of integrated control and management system based on inter-collaboration against cyber threats. It shares and collates the information related to cyber threats in own organizations, ISP CERTs and security center, certain other resources. Our mechanisms not only an attack response that detects cyber threats throughout the range of our system but also predicted future cyber-attacks and characteristics using statistical analysis. We also realized quick and accurate response system through the unification (notification, conduct and response) of cyber threat occurring in internal and external organizations.

ACKNOWLEDGEMENT

This research was support by "Building and Services of Advanced KREONET Based on Software" Program funded by the Ministry of Science, ICT and Future Planning(K-17-L01-C04)

REFERENCES

Gandhi, R., A. Sharma, W. Mahoney, W. Sousan and Q. Zhu, *et al*., 2011. Dimensions of cyber-attacks: Cultural, social, economic and political. IEEE. Technol. Soc. Mag., 30: 28-38.

Ghafir, I., V. Prenosil, J. Svoboda and M. Hammoudeh, 2016. A survey on network security monitoring system. Proceeding of the IEEE International Conference on Future Internet of Things and Cloud Workshops, August 22-24, 2016, IEEE, Vienna, Austria, ISBN:978-1-5090-3947-0, pp: 77-82.

Ko, S., K. Kim, Y. Lee and J. Song, 2014. A classification method of darknet traffic for advanced security monitoring and response. Lect. Notes Comput. Sci., 8836: 357-364.

Lagraa, S. and J. Francois, 2017. Knowledge discovery of port scans from darknet. Proceedings of the 2017 IFIP-IEEE Symposium on Integrated Network and Service Management (IM), May 8-12, 2017, IEEE, Lisbon, Portugal, ISBN:978-1-5090-5658-3, pp: 935-940.

Moosavi, S.R., T.N. Gia, E. Nigussie, A.M. Rahmani and S. Virtanen *et al*., 2015. Session resumption-based end-to-end security for healthcare internet-of-things. Proceedings of the IEEE International Conference on Computer and Information Technology: Ubiquitous Computing and Communications, Dependable, Autonomic and Secure Computing, Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), October 26-28, 2015, IEEE, Liverpool, England, ISBN:978-1-5090-0154-5, pp: 581-588.

Settanni, G., Y. Shovgenya, F. Skopik, R. Graf and M. Wurzenberger *et al*., 2017. Acquiring cyber threat intelligence through security information correlation. Proceedings of the 3rd IEEE International Conference on Cybernetics (CYBCONF'17), June 21-23, 2017, IEEE, Exeter, UK., ISBN:978-1-5386-2202-5, pp: 1-7.

Svoboda, J., I. Ghafir and V. Prenosil, 2015. Network monitoring approaches: An overview. Intl. J. Adv. Comput. Netw. Secur., 5: 88-93.

Ye, Y., T. Li, D. Adjeroh and S.S. Iyengar, 2017. A survey on malware detection using data mining techniques. ACM. Comput. Surv., Vol. 50, 10.1145/3073559

Zavarsky, P. and D. Lindskog, 2016. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. Procedia Comput. Sci., 94: 465-472.