

Received November 19, 2019, accepted December 15, 2019, date of publication December 18, 2019, date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960552

Potential Risk Analysis Method for Malware Distribution Networks

DOHOON KIM^{id}, (Member, IEEE)

Department of Computer Science, Kyonggi University, Suwon-si 16227, South Korea

e-mail: karmy01@kgu.ac.kr

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. NRF-2018R1C1B5044713).

ABSTRACT In this study, the structural characteristics of malware distribution networks (MDNs) were examined and the network centrality of the relationships between websites containing malware, infection sites, intermediate connection sites, and initial connection sites were analyzed. The core malware sites within MDNs that contribute to the success of cyberattacks were identified, and the overall risk of the MDNs, which changes dynamically, was examined quantitatively to predict additional attacks. As such, real-time security events occurring in the information security systems of target organizations were collected and analyzed, and different types of security intelligence were assessed to recreate various MDNs. In addition, the risk levels of malicious URLs, IPs, etc. in MDNs were analyzed continuously over time, and a model suitable for predicting potential attack times was developed. The developed model identified the characteristics of potential future cyberattacks based on the analyzed initial MDN risk level, as well as the connectivity of and malware associated with the MDN, which change over time, thereby maintaining an average prediction accuracy of 94.9% over one week.

INDEX TERMS Advanced persistent threat, information security, malware distribution network, network centrality analysis, risk assessment.

I. INTRODUCTION

Recently, intelligent cyberattacks (advanced persistent threats (APTs)) [1], have become continuous, targeted, and specialized. In response to these threats, various information security solutions are being developed, and research and development projects are being conducted. However, it is still difficult for decision-makers, such as directors of computer emergency response teams and information security solution operators, to determine the importance of numerous malware sites and malware types that are detected or the order of priority for related event processing, such as blocking [2]. In addition, inserting blocking policies unilaterally without an order of priority results in false positives, false negatives, and system malfunctions in information security solutions.

Conventionally, decision-making has been in the form of qualitative decisions by cybersecurity experts or generalized decisions by information security systems; consequently, various problems have occurred, including poor judgment, inadequate management, difficulty in determining risk weights,

and limitations in information processing capabilities. Furthermore, in the case of risks from malware sites and malware, different information security solutions and information security experts have different standards for making decisions. Thus, it is necessary to develop a standardized process for assessing the quantitative risks of malware sites and malware, as well as the potential risks of malware distribution networks (MDNs), which are composed of malware sites and malware, to achieve objective decision-making. A network centrality analysis (NCA) method is proposed herein for calculating the potential risks of malware sites and MDNs. Our proposed NCA model supports multidimensional analysis of the relationship between nodes.

This allows the relationship between various nodes (malicious sites, malware) to be analyzed in depth by centrality analysis for degree, betweenness, and eigenvector. The final risk level of the MDN is determined through a linear combination of various computational results such as the self-risk of malicious code, the possibility of propagation, and proximity to malicious sites. Thus, the complex redirection relationships of MDNs are identified and the magnitude of the risk is determined quantitatively.

The associate editor coordinating the review of this manuscript and approving it for publication was Liehuang Zhu^{id}.

Furthermore, changes in the risks of attacker groups within MDNs are described and the prediction of potential attack times is addressed by calculating the accumulated MDN risk, measuring risk changes based on a timeline, and determining the overall cyber threat level.

Ultimately, the model proposed in this paper provides a structured understanding of the various Landing Sites, Hopping Sites, and Distribution Sites related to the core malicious sites in terms of the Computer Emergency Response Team (CERT) mission. It avoids the simple prevention policies of identified malicious sites and identifies various malware associated with core malicious sites that have potential risks. The model enables an active response system against possible APT attacks as organizations are multidimensionally aware of cyber threats. In addition, it can produce critical threat information that may be used to establish an active APT attack defense strategy.

The remainder of this paper is organized as follows. Section II describes the structural characteristics of MDNs and the differences between this study and previous studies. Section III introduces the proposed quantitative risk calculation model for malware sites and malware (referred to as the potential risk analysis method for malware distribution sites, PRiAM), as well as the accumulated MDN risk and attack time prediction method—in which PRiAM is used for each MDN. Section IV describes the experimental environments employed to analyze various MDN configuration scenarios and presents the actual experimental results, evaluations of accumulated MDN risks, and attack predictions. Finally, Section V summarizes the conclusions and topics requiring additional research.

II. BACKGROUND AND RELATED WORK

A. MALWARE DISTRIBUTION NETWORK (MDN)

MDNs are intelligent malicious networks that are built by attackers to perform persistent cyberattacks on unspecified users or selected organizations. Specifically, MDNs are composed of various types of malicious URLs containing malware (including landing sites, exploit sites, hopping sites, and distribution sites) that have mutually dependent relationships [3], and they are normally in an attack posture that is determined by the strategy of the attacker.

Fig. 1 shows how the malware in an MDN infects or is disseminated to internet users through various types of URLs, which is the basis for research on calculating risk levels.

As shown in Fig. 1, the malware infection process starts with the Internet user (a) connecting directly to a distribution site (b). The attacker then induces an advanced infection by redirecting the user [2] to a landing site (e), which is an initial malware dissemination site, through several intermediate hopping sites (c) or exploit sites (d) via the distribution site, which is the initially accessed site; subsequently, the malware is downloaded.

The attacker creates an advanced MDN in advance to infect normal Internet users with malware and to attempt various secondary cyberattacks (such as seizing personal information, disabling systems, and attacking other hosts). Therefore, in this study, multidimensional quantitative analysis was performed on the various malware infection cases that occur in such an MDN. In addition, objective qualitative analysis of the potential cyber threats that can occur in the future was conducted.

B. RELATED WORK

Most studies on malware site analysis involve i) assessment and detection of the direct distribution of malware from the URL, as in the case of a distribution site, or ii) investigation of redirection from an exploit site to a landing site (e).

Typical examples of studies in the first group are those involving analysis of malware URLs or web content based on static characteristics such as URL lexical patterns, HTML page content (malware), JavaScript features, and host attributes [4]–[11], followed by classification of cyber threats through machine learning or data mining. In addition, studies have been conducted in which sandbox-based virtual machines were used to detect abnormal API calls in the target content that perform malicious behaviors (such as file creation, registry changes, host file tampering, and backdoor installation). Furthermore, many studies involved the detection of malicious iFrame injection [12]–[14] through browser vulnerabilities. This process is considered the basic malicious behavior that is employed to create MDNs.

Studies of the second type can reveal the volumes or sizes of MDNs based on number of redirections occurring between malware sites. Therefore, it is necessary to consider the agents through which redirections occur. First, studies have been conducted in which redirections to distribution sites were analyzed by identifying search poisoning events [15].

In this case, redirection occurs automatically and is not based on the search queries of normal users. In addition,

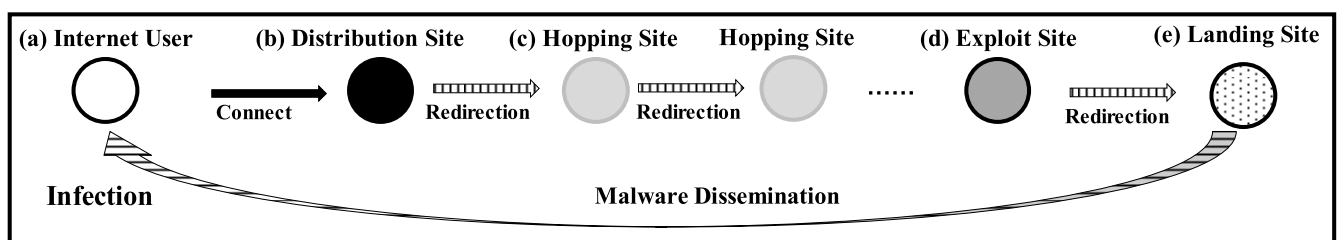


FIGURE 1. Malware infection process on an MDN.

redirections created by users who click on malicious URLs published on social networks such as Twitter [16] have been focused on. Finally, malware is downloaded when redirection is started by various malicious banner advertisements [17] that are included in web pages.

Studies have also been conducted involving structural analysis of the MDN. Chuang *et al.* [18] analyzed the traffic of a particular organization by visualizing and analyzing the behavior of malicious sites and connection attempts. However, their proposed analysis method focused only on visualization and did not perform quantitative analyses of the various connectivity threats in the graph analysis. Our proposed model can improve the effectiveness of CERT control systems by integrating various network analyses of each malicious site and malicious code to quantitatively reproduce the new risk index.

Peryt *et al.* [19] analyzed both the topology structure of a malicious site that distributed malicious code directly and that of the MDN, which includes sub-networks. However, visual representations do not reflect the various changing architectural characteristics of MDNs. In contrast, our method provides quantitative figures to predict future cyber threats through continuous tracking of the cumulative rate of change in MDN based on a specific timeline.

Wang *et al.* [20] proposed a system that detects landing sites distributing malicious code inside the MDN. Their proposed system conducts continuous observation using honeypots and is able to track and manage the mutations of MDNs based on landing pages. However, as the main purpose is searching for malicious sites, it is limited to inferring an attacker's intelligent attack strategy. In contrast, our proposed method continuously analyzes MDNs managed by groups of attackers and quantitatively analyzes potential threats to establish an intelligent intrusive response system.

Whereas existing studies are focused on detecting malware sites that constitute MDNs, our approaches are focused on performing reconfiguration with MDN risk levels through network centrality analysis of various forms of security intelligence (malware DNSs, IPs, C&Cs, URLs, etc.) collected by the information security systems of the target organizations. In addition, in this study, the overall MDN risk level was determined according to the distance between malware sites, involvement of malware or lack thereof, and the risk level of the malware.

Finally, MDN risk levels undergo various changes over time, and can thus be used to create defensive strategies that minimize or prevent damage to organizations by predicting when secondary and tertiary attacks will occur.

III. PROPOSED MODEL

A. POTENTIAL RISK ANALYSIS METHOD (PRiAM)

To assess the risk level of an MDN, it is necessary to analyze the form and structural characteristics of that MDN and perform multidimensional analysis considering the effect of malware that are connected to the MDN sites. Hence, threat

information was collected and the centrality of an MDN was analyzed based on the collected intelligence, as shown in Fig. 2.

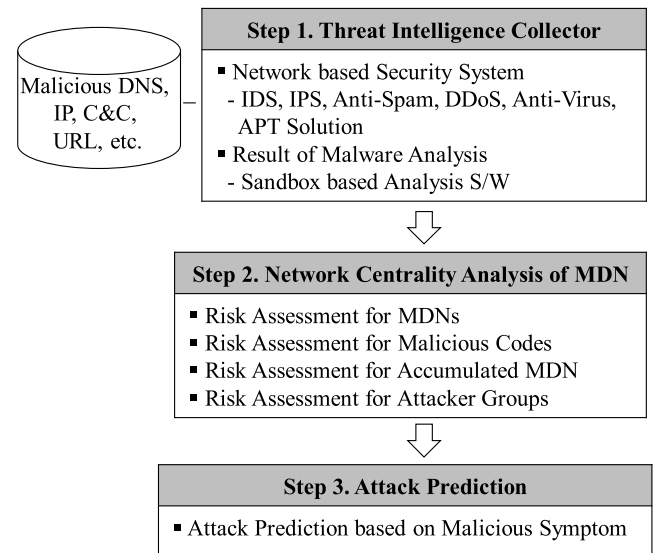


FIGURE 2. Potential risk analysis process for MDN.

In this study, the risk levels of the core component URLs of the MDN (landing, exploit, hopping, and distribution sites) as well as those of each piece of malware, were calculated, and the ultimate risk level of the MDN group was assessed quantitatively. In addition, the MDN processed in this manner was defined as a single attack group, and the extent to which the risk level changed over time was observed to analyze the future potential risk.

B. NETWORK CENTRALITY ANALYSIS OF MDN

To assess the risk level of a dynamically changing MDN, it is necessary to analyze the risk of each malware site. Hence, an optimal analysis theory was selected from among the network centrality analysis theories listed below. (Herein, the connections between nodes in malware sites are called links.)

1) DEGREE CENTRALITY ANALYSIS

This analysis method involves measuring neighbor nodes that are directly linked and is suitable for measuring direct influence. When directionality exists between nodes or networks, in/out degree centrality is measured. Nodes that have numerous links are important nodes. In MDNs, these nodes are important for continuously disseminating malware through directly linked neighbors; however, because global search methods are required to find MDNs in large networks such as the Internet, this method is limited.

$$C_D(i) = \frac{k_i}{N-1} (= \frac{\sum_j A_{ij}}{N-1}) \quad (1)$$

where

N : Overall system size (number of nodes),

A_{ij} : Adjacency matrix

- $A_{ij} = 1$: If a link exists between nodes i and j
- $A_{ij} = 0$: If link exists between nodes i and j
- k_i : Number of links of node i
- d_{ij} : Shortest distance between nodes i and j

a: BETWEENNESS CENTRALITY ANALYSIS

This analysis method involves measuring the frequency at which links between nodes are passed through. It is suitable for measuring the control that occurs during information transfer. In this analysis method, it is assumed that information moves along the shortest distance. However, when malware is disseminated by an MDN, it is disseminated not via the shortest path, but rather via all reachable paths. Therefore, this analysis method is not suitable for an MDN, in which all paths must be considered.

$$C_B(i) = \frac{\sum_j \sum_k g_{jk}(i)/g_{jk}}{(N - 1)(N - 2)} \quad (2)$$

where

g_{jk} : Number of paths that have the shortest distance between nodes j and k

$g_{jk}(i)$: Number of paths that passes through node i among the paths that have the shortest distance between nodes j and k

b: EIGENVECTOR CENTRALITY ANALYSIS

This analysis method involves measuring the sum of centrality of directly linked neighbor nodes. Therefore, it is assumed that nodes with high centrality have a high capacity for dissemination, and an intuitive phenomenon is defined in which neighbor nodes that are linked to important nodes have high importance. As such, a method of assessing risk as proportional to the centrality (risk) of nearby neighbors is necessary. To reflect the assumption that risk decreases as distance increases, it is necessary to define an advanced concept of centrality (risk). Consequently, this analysis method is considered suitable for determining the risk of an entire MDN because the risk of linked URLs increases as the risk of the malware or the importance of the landing site increases.

$$C_E(i) = \frac{1}{\lambda} \sum_j A_{ij} C_{E_j} \quad (3)$$

where

λ : Largest eigenvalue of the adjacency matrix

c: CLOSENESS CENTRALITY ANALYSIS

This analysis method involves measuring the link distances between all nodes in an MDN. It is suitable for calculating the immediacy of the influence between nodes. Therefore, when this analysis method is used, it is necessary to consider the risk levels of the actual malware and the malware site according to distance. The precondition that the initial source (malware) and target (first hopping site) are fixed, but not all possible paths are fixed, must be satisfied. However, because this method is not suitable when dissemination is performed

through redirection by intermediate connection sites (hopping sites) when the distance is large, only the definition for risk between malware and malware sites with a primary link relationship is considered herein.

$$C_C(i) = \frac{N - 1}{\sum_j d_{ij}} \quad (4)$$

C. RISK ASSESSMENT FOR MDNs

Importantly, risk is assessed for each malware site because the degree of risk differs according to the network location of the malware site (malicious URLs) and the related malware that exists within the MDN. More specifically, quantified analysis results regarding risk, which changes because the risk level of an MDN varies according to the intentions of the attacker, are used as data that serve as the basis for various decision-making and intelligent response capabilities. Therefore, to analyze the risk of each malware site quantitatively, the following basis for calculations was defined in this study.

1) To understand the various link relationships between a certain malware site (exploit / hopping / landing site) and the malware, it is necessary to perform centrality closeness analysis. This must be achieved based on multiple scenarios. First, as shown in Fig. 3(a), the risk increases according to the closeness of the link relationship between the hopping site and the landing site that contains the malware. Further, as shown in Fig. 3(b), the risk increases according to the direct and indirect connections between URLs and multiple malware items. The changes in risk of the malware [21] are used as factors for determining the overall scale of the risk.

2) As depicted in Fig. 4(a), the analysis considers closeness to the landing site, from which the initial malware download occurs, and the risk of the landing site itself. Further, the risk of the malware sites that disseminate malware through the landing site (hopping/exploit sites) increases with the number of visitors, as illustrated in Fig. 4(b), because malware sites that contain malware dissemination paths to multiple landing sites have high risks. Ultimately, if the two cases above are combined and analyzed, the dissemination of malware becomes more definite and risk increases near the landing site.

3) As shown in Fig. 5(a), the risk increases with the risk of the malware itself that is directly or indirectly linked to the malware site (hopping/exploit site). Therefore, the risk of the MDN is determined according to the malware category. As illustrated in Fig. 5(b), the risk of the overall MDN is determined because the importance of the landing site varies according to the number of visitors, that is, the risk of linked URLs increases with the risk of the malware itself or the importance of the landing site. Using this information, it is possible to assess the centrality eigenvector, which describes networks from the perspective of expansion and dissemination centrality.

4) As shown in (5) and (6), the distance between the malware and landing site and the number of malware and

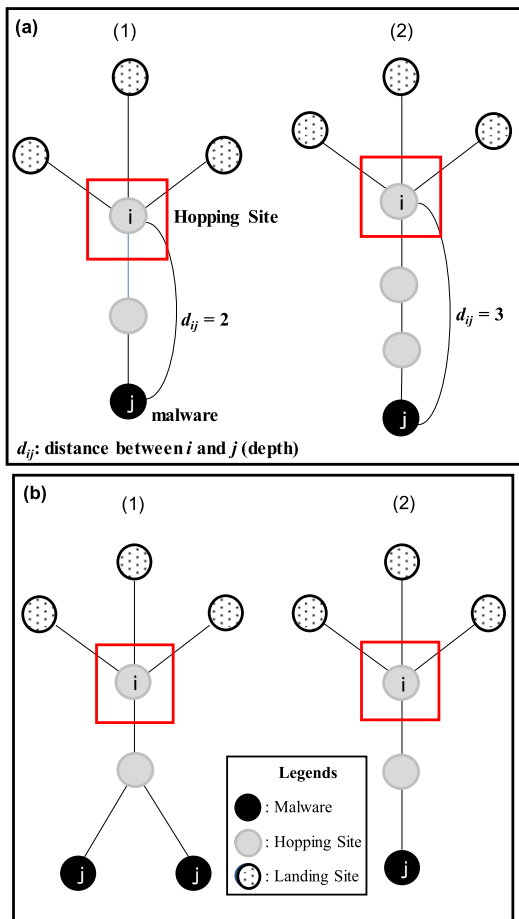


FIGURE 3. Analysis of closeness with malware and risk of malware itself.

landing sites are factors that determine the risk of the MDN, which is assessed through closeness centrality analysis. When defining risk as the inverse of distance, the risk decreases as the distance increases. To compensate for this behavior, an exponential function is used as a control parameter to represent the risk in the form of a monotonic decrease with respect to distance. As shown in (7), the risk of the malware itself and the importance of the landing site according to the number of visitors are factors that determine the risk of the MDN. This is assessed through eigenvector centrality analysis, which obtains the centrality of expansion and dissemination. Therefore, using a formula that simultaneously applies both the aforementioned closeness and eigenvector centrality $C_M(i)$ is the risk based on the closeness to the malware and the dissemination of the malware risk itself.

$$C_M(i) = \sum_{j \in \{Malware\}} M(j) \cdot \lambda^{[d_{ij}-1]} \quad (5)$$

where

- d_{ij} : Depth between nodes i and j
- λ : Control parameter of decrease rate
- $M(j)$: Risk index of malware
- $V(j)$: Risk index of the landing site, which is based on the number of visitors

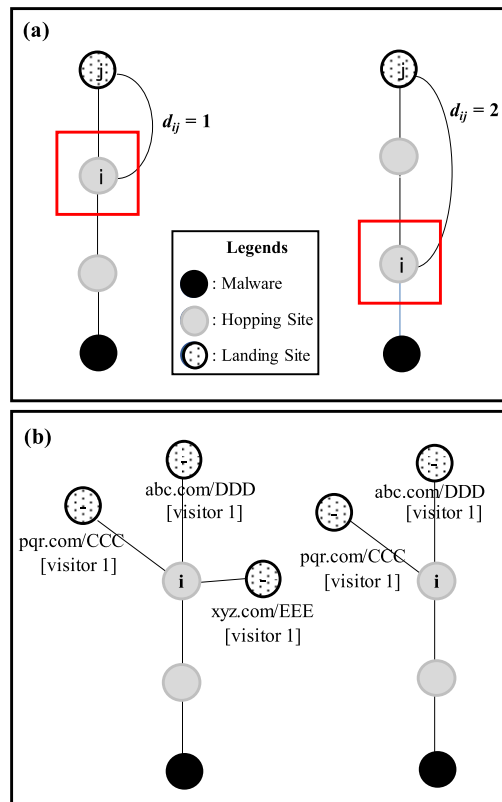


FIGURE 4. Analysis of closeness to landing site and risk of the landing site.

$C_L(i)$ is the risk that is based on closeness to the landing site (user access site) and risk dissemination of the landing site; it is expressed as follows:

$$C_L(i) = \sum_{j \in \{LandingSites\}} V(j) \cdot \lambda^{[d_{ij}-1]} \quad (6)$$

Equation (7) defines the overall ultimate risk index of the URL, which is assessed via $C_M(i)$ from (1) and $C_L(i)$ from (2).

$$C_{URL}(i) = \alpha \cdot \sum_{j \in \{Malware\}} M(j) \cdot \lambda^{[d_{ij}-1]} + (1 - \alpha) \cdot \sum_{j \in \{LandingSites\}} V(j) \cdot \lambda^{[d_{ij}-1]} \quad (7)$$

where $0 \leq \alpha \leq 1$

As shown in (7), $C_{URL}(i)$ reflects the malware-caused risk $C_M(i)$ in the URL risk index as α approaches one. $C_L(i)$, which is the risk caused by the linked landing site, is reflected in the malware site risk index as α approaches zero. When $\alpha = 1$, only the malware-caused risk $C_M(i)$ is reflected in the malware site risk index. When $\alpha = 0$, only $C_L(i)$, which is the risk caused by the landing site, is reflected in the malware site risk index.

However, the final MDN risk value is not normalized, because it varies according to the characteristics of the surrounding nodes, even if the malware site has the same risk. Consequently, it is difficult to determine the threshold index of the risk. Here, the threshold index is the value that distinguishes whether a node has a risk above a certain value.

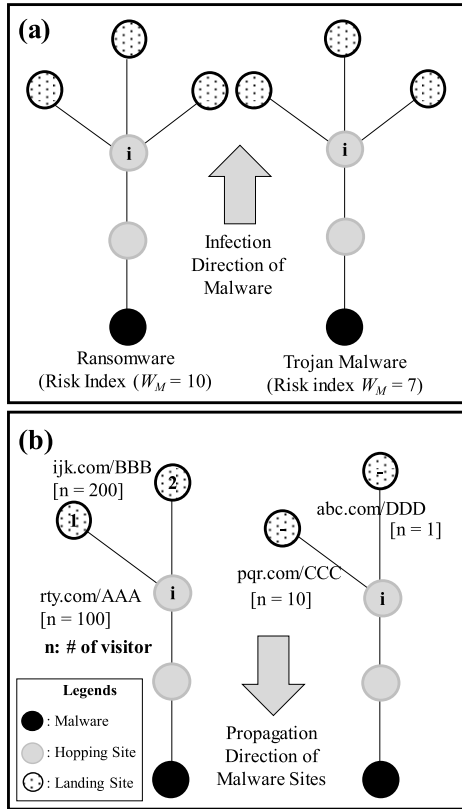


FIGURE 5. Analysis of risk dissemination of the malware itself and importance of the landing site.

In other words, when the risk is unilaterally normalized to a value between zero and one, it is difficult to reflect subtle changes in the actual risk value. However, the actual rate of increase of the risk can be depicted by expressing it as a relative value rather than limiting it to an absolute value.

D. RISK ASSESSMENT FOR MALICIOUS CODES

Because the overall risk of an MDN changes according to the changes in risk caused by the malware type (such as viruses, worms, trojans, ransomware, ad/spyware, hybrids, and exotic forms), $M(j)$ [18], which is the risk according to the initial malware type classification and analysis, is expressed as a quantitative value (between zero and one); i.e., the risk of the malware itself is assessed.

In addition, as shown in (6), if the closeness to the user access site (landing site) and the risk of the landing site are considered, the risk of the malware sites (hopping / exploit sites) that disseminate through the landing site increases the number of visitors to the landing site increases or the importance of the site increase. Furthermore, the risk of malware that contains dissemination paths through multiple landing sites is large; risk dissemination becomes more definite as one approach the landing sites, and the risk becomes higher. Therefore, the final malware risk formula is as follows:

$$C_{MAL}(i) = \alpha \cdot M(j) + (1 - \alpha) \cdot C_L(i) \quad (8)$$

where $0 \leq \alpha \leq 1$

Equation (8) shows that as α approaches one, the malware-caused risk is reflected more in the URL risk index, and as α approaches zero, the risk caused by the linked landing site is reflected more in the URL risk index. When $\alpha = 1$, only the risk of the malware itself is reflected in the initial malware risk, and when $\alpha = 0$, only the risk caused by the landing site is reflected in the initial malware risk.

E. RISK ASSESSMENT FOR ACCUMULATED MDN

In Section III.D, different methods of employing the risks of various malware within an MDN in risk calculations and those of measuring the initial MDN risk were discussed. Calculating the initial risk of an MDN is important; however, changes occur in the MDN over time owing to several reasons, as shown in Fig. 6(a).

The initial MDN properties change variously as URLs (landing sites, exploit sites, hopping sites, and distribution sites) are created, shut down, or modified. Currently, only the MDN characteristics and exploit types can be determine based on the types of connections between URLs.

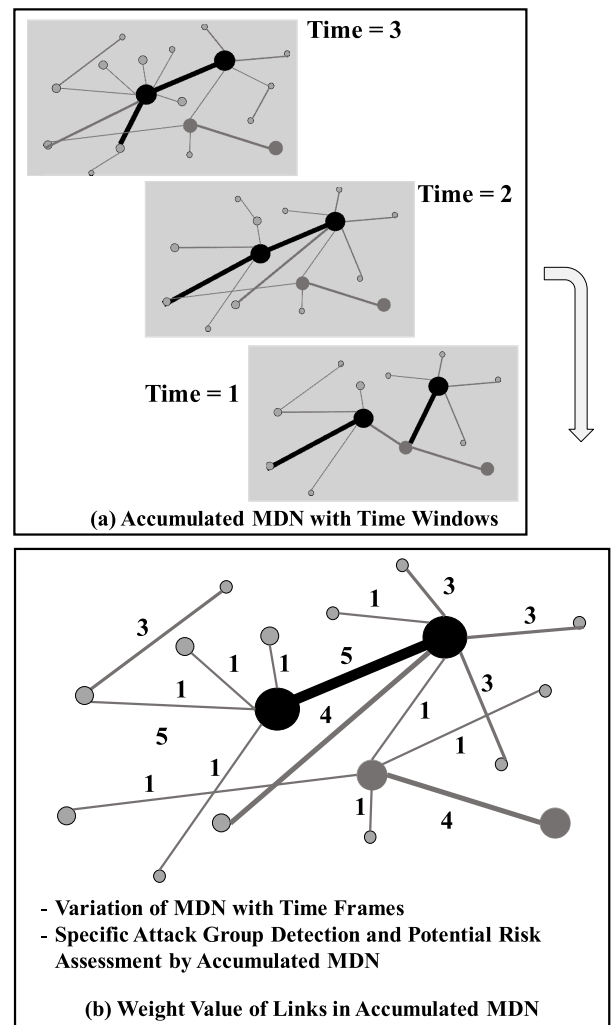


FIGURE 6. Accumulated MDN.

Therefore, limitations exist in performing various additional analyses, such as analyses of future MDN trends and predictions.

As such, it is necessary to examine the overall characteristics of an MDN by analyzing the accumulated MDN characteristics, which incorporate the characteristics of both current and past MDNs. This necessity originates from the fact that the overall MDN changes according to variations in web pages (frames) over time. Therefore, by observing the changes and continuously measuring the accumulated (merged) changes, certain attacker groups that cannot be determined currently can be detected, and potential threats can be predicted and assigned with various meanings.

Moreover, constant readiness for APT attacks can be maintained and intelligent defensive measures established. For this type of MDN, weights must be assigned to the link information between URLs, as shown in Fig. 6(b). Thus, it is possible to maintain the most recent MDN information, which better reflects the current information, if larger link weights are assigned as one approach to the current time and the time period in which link connectivity exists during the overall accumulation period. For the weights, d_{ij} in (5) and (6) is defined as the link strength.

F. RISK ASSESSMENT FOR ATTACKER GROUPS

To distinguish between specific attack groups in the accumulated MDN described above, attacker differentiation analysis is performed through component analysis, which is a typical cohesive subtype of social network analysis. Here, the maximum group that is connected without interruption from the initial observation time becomes the base of a component. Therefore, the following are assumed.

- The malware within the same component is assumed to be from the same attacker. That is, the malware in an MDN comprising a single component is considered to be from the same attacker.
- A single attacker is assumed if the IP bandwidth is the same. Malware in the same IP bandwidth is assumed to be from the same attacker based on the fact that the same C&C server is used.

The risk for each attack group that is assessed based on the assumptions above exhibits the following characteristics.

- The sum of risks of the landing sites within the same attacker group is assessed.
- The landing sites are accessed, and infection occurs.
- The risk of a user being infected with malware increases with the landing site risk.
- Landing site risk reflects malware risk.

Therefore, the risk of each attack group is assessed as in (9):

$$C_{Att}(i - th \text{ component}) = \sum_{\substack{j \in \{LandingSites \\ \text{in } i-th \text{ component}\}}} C_{URL}(j) \quad (9)$$

where the *i-th component* is the network group that is expected to be the same attacker via the component analysis described above. Because the degree of threat changes over

time according to the specific attacker groups observed, it is necessary to specify the following causes and perform a trend analysis.

- The risk of the MDN increases with the number of malware items.
- The risk of the MDN increases with the number of distribution sites.

The following processes are required to perform this type of prediction analysis:

- Measure the changes in statistical values and compare with those on the previous day.
- Assume that changes between variables are independent.
- Measure the *Mahalanobis distance* [22].

The *Mahalanobis distance* is obtained because it quantifies how rarely the initial measurement value occurs or how abnormal it is, and the distance from the mean is expressed in terms of multiples of the standard deviation. Thus, it is concluded that additional actual cyberattacks will occur if an abnormal increase in risk is detected.

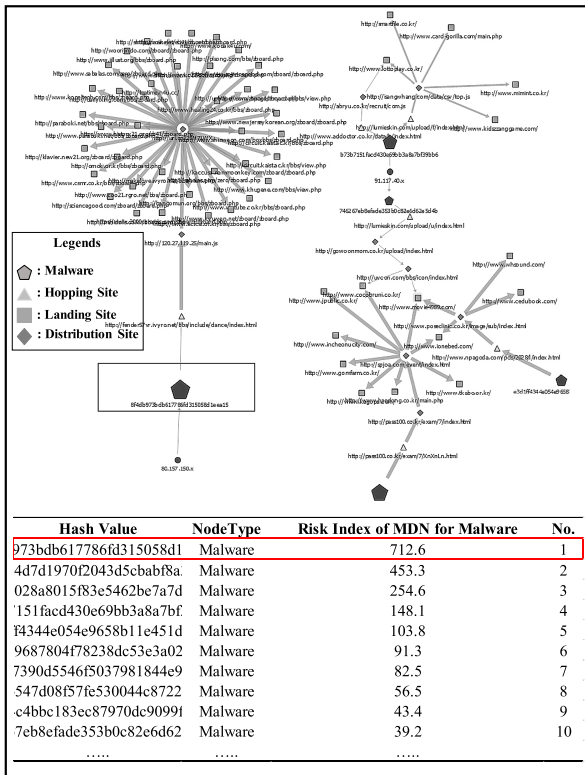
IV. EXPERIMENT AND RESULTS

A. BUILDING THE EXPERIMENTAL ENVIRONMENT

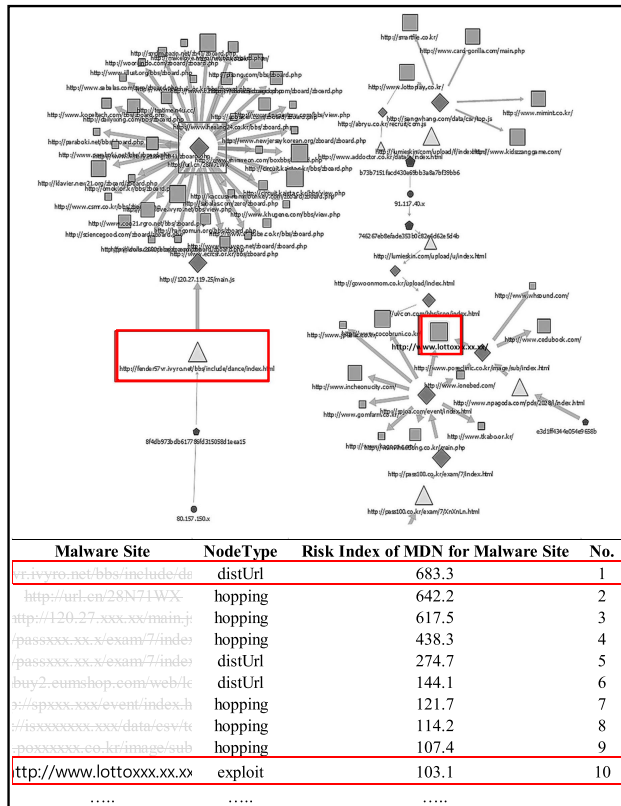
To test and verify the proposed model, reverse analysis was performed on security event information generated by certain organizations. For example, common civil, administrative, and military organizations have their own information security systems (IDSs; IPS, anti-spam, anti-virus, DDoS, APT solutions, etc.) based on various networks. Each system collects data related to external links (malicious DNSs, IPs, C&Cs, URLs, etc.), which constitute secondary analysis results obtained by analyzing the malware collected from the systems being monitored (servers or PCs), as well as primary analysis results (malicious DNSs, IPs, C&Cs, URLs, etc.) regarding the in/out network traffic that is generated by the organization. Therefore, the experiment started with this information and an MDN centered on the target organization was created.

Various forms of risk were assessed, and the degree of threat exposure, which changes over time, was observed to predict how the forms of attack would change. An information security system, such as those built by typical organizations was established, and various types of malware intelligence were collected for approximately one year. Fig. 7 presents an outline of the overall configuration and infrastructure for the experiments.

To create an environment similar to the service environments operated by actual organizations, an open source-based information security environment was created, as shown in Fig. 7. For the purpose of the experimentation in this study, it was composed of security solutions that can be built within the enterprise. Above all, it is structured around open source software to faithfully collect information about threat intelligence. As such, analysis was conducted only on datasets for which the initial cyber threat information collection was



(a)



(b)

FIGURE 8. (a) (ex) Top risk index of MDN based on malicious codes. (b) (ex) Top risk index of MDN based on malware sites.

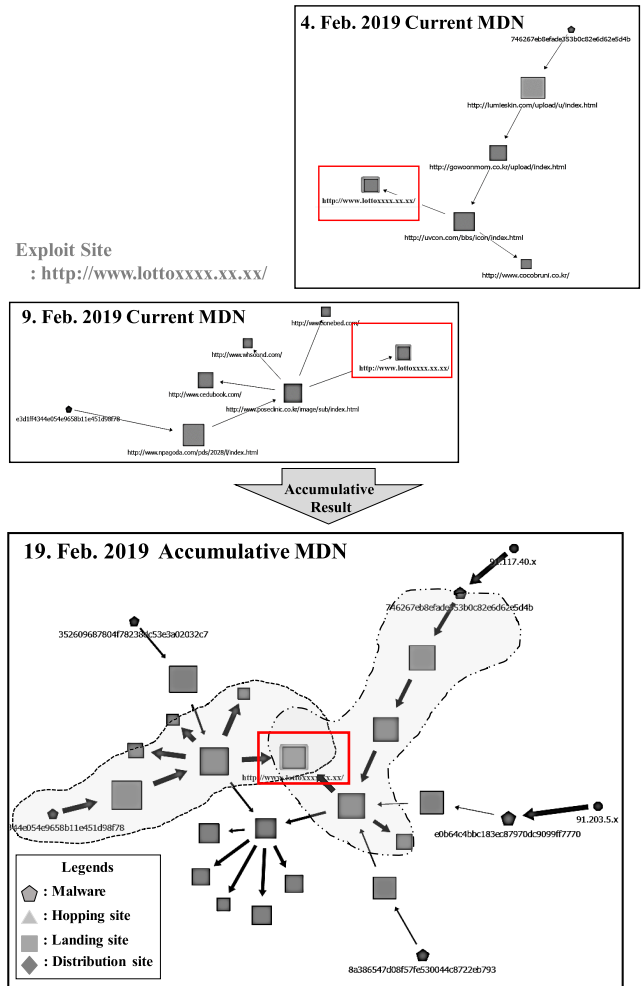


FIGURE 9. (ex) Final accumulated malware distribution network.

MDN values of the site up until February 9, an actual risk occurs in the MDN on February 9.

Therefore, it is concluded that a certain attack group is infecting the MDN (<http://www.lottoxxx.xx.xx>) and using it to perform cyberattacks continuously, as shown in Fig. 10.

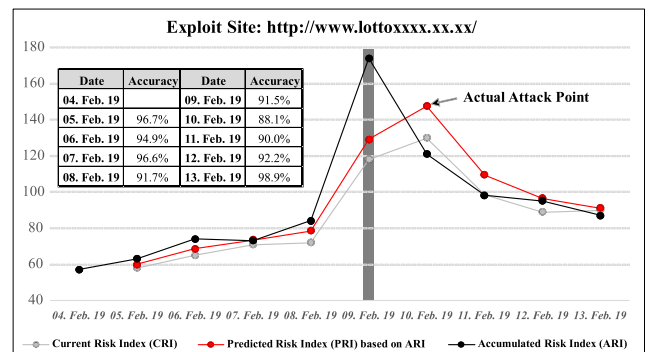


FIGURE 10. Accumulated risk index of top attacker group.

On February 9, 2019, the accumulated risk increases slightly. Consequently, it is determined that the attack group will perform actual attack behaviors via the target site starting on that day. Because the accumulated risk increases by a small amount on February 9, 2019, the actual risk (current risk index, CRI) peaks on February 10 when the attack actually occurs. Additionally, the predicted index risk (PRI), which predicts this attack, increases simultaneously. Ultimately, the actual main attack point can be predicted one day earlier via the accumulated risk.

Time series analysis was also performed based on the accumulated risk index (ARI). The results show that the calculated PRI was 147.5 on February 10. The CRI for the actual day is 130, indicating a high prediction rate with an accuracy of 88.1% at that time. Here, the CRI value is the result of calculating $C_{MAL}(i)$ in (8). The ARI is the result of calculating $C_{Att}(i)$ in (9). The PRI is the time series analysis result of the ARI. Overall, the comparison between the PRI and the CRI of the observed MDN during the same period reveals an average prediction accuracy of approximately 94.9%, as shown in Table 4.

TABLE 4. Information on URLs in MDN.

Date	Current Risk Index (CRI)	Predicted Risk Index (PRI)	Accuracy between CRI and PRI	Accumulated Risk Index (ARI)
04-Feb-19	-	-	-	57
05-Feb-19	58	60	96.7%	63
06-Feb-19	65	68.5	94.9%	74
07-Feb-19	71	73.5	96.6%	73
08-Feb-19	72	78.5	91.7%	84
09-Feb-19	118	129	91.5%	174
10-Feb-19	130	147.5	88.1%	121
11-Feb-19	98.5	109.5	90.0%	98
12-Feb-19	89	96.5	92.2%	95
13-Feb-19	90	91	98.9%	87

In addition, the accuracy of the predicted PRIs increases without distortion because the relative ARI of the attack group over time is incorporated without any normalization process, and the changes in the ARI can be understood intuitively.

C. THREATS TO VALIDITY

In this study, a method of analyzing the risk of MDNs by attacker groups observed in APT attacks that target specific organizations was developed. Accordingly, we performed network centrality analysis based on the associations between local security events (IDS, IPS, anti-spam, anti-virus, DDoS, APT detection solutions, etc.) and global intelligence. The following threats to validity have been identified.

- The estimated risk of the MDN is a quantitative value limited to the perspective of the victim organization, which possibly prevents observations in other organizations.

- If an attacker continues to generate various redirect paths, the risk of observed MDNs may be reduced. However, an attacker can create many malicious sites that can limit

the use of malicious codes. In the future, we will continue to observe the rate of change of an attacker's MDN volume to analyze the relationship with newly created redirect sites. In addition, we will analyze the malicious codes and strains frequently used by groups of attackers to identify their relationships.

- A comparative analysis was performed, focusing on the proposed study and research in similar fields. However, it is difficult to make quantitative comparisons with related studies owing to differences in the experimental environments. The proposed research method adopts a variety of application methods—such as multidimensional network analysis methodologies and malicious code analysis methods—not used in previous studies. As such, this study demonstrates a novel analysis method as well as presenting results of MDN analysis.

- Nevertheless, this risk assessment method, which is specific to the target organization, can be considered an integral approach for intelligent threat responses to APT attacks.

V. CONCLUSION

In this study, the structural characteristics of MDNs, which are created by attackers to target multiple unspecified organizations or specific organizations, were examined and network modeling (group analysis) was performed to model the relationships between websites that contain malware (landing sites), infection sites (exploit sites), intermediate connection sites (hopping sites), and initial connection sites (distribution sites). Subsequently, the risk levels of various MDNs were assessed.

In addition, the ARIs of exploit sites, which are directly related to cyberattacks, were calculated and time series analysis was performed to obtain the PRI. The PRI was then compared to the actual CRI, and a high prediction accuracy was obtained. In terms of active cyber defense, the method developed in this study can be used to perform multidimensional risk-based analyses on various security threat intelligence data, establish active defense strategies for APT attacks, and implement aggressive intrusion responses.

In future studies, continuous machine learning of attack patterns (static and dynamic analyses of new/variant malware and the connections between URLs) that are used to classify attack groups based on MDNs and malware analysis results will be conducted. Additional studies will also be performed to analyze attacker-centered networks and establish active defense strategies for cyberattacks that are based on various malicious behaviors.

REFERENCES

- [1] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proc. IEEE Conf. Comput. Commun.*, Hong Kong, Apr./May 2015, pp. 747–755.
- [2] R. K. Baggett and B. K. Simpkins, *Homeland Security and Critical Infrastructure Protection*, 2nd ed. New York, NY, USA: Praeger, 2018.
- [3] D. Kim, D. Choi, and J. Jin, "Method for detecting core malware sites related to biomedical information systems," *Comput. Math. Methods Med.*, Feb. 2015, Art. no. 756842, doi: 10.1155/2015/756842.

- [4] T. Matsunaka, J. Urakawa, and A. Kubota, "Detecting and preventing drive-by download attack via participative monitoring of the web," in *Proc. 8th Asia Joint Conf. Inf. Secur.*, Tokyo, Japan, 2013, pp. 48–55, doi: 10.1109/ASIAJCS.2013.15.
- [5] P. Likarish, E. Jung, and I. Jo, "Obfuscated malicious javascript detection using classification techniques," in *Proc. 4th Int. Conf. Malicious Unwanted Softw.*, Montreal, QC, Canada, 2009.
- [6] C. Seifert, I. Welch, and P. Komisarczuk, "Identification of malicious Web pages with static heuristics," in *Proc. Australas. Telecom. Network. Appl. Conf.*, Adelaide, SA, Australia, 2008.
- [7] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Learning to detect malicious URLs," *ACM Trans. Intell. Syst. Tech.*, vol. 2, no. 3, p. 30, 2011.
- [8] Y. Fukushima, Y. Hori, and K. Sakurai, "Proactive blacklisting for malicious Web sites by reputation evaluation based on domain and IP address registration," in *Proc. IEEE 10th Int. Conf. Trust Secur. Privacy Comput. Commun.*, Washington, DC, USA, Nov. 2011, pp. 352–361.
- [9] J. Zhang, C. Seifert, J. W. Stokes, and W. Lee, "ARROW: GenerAting SignatuRes to detect DRive-By DOWNloads," in *Proc. Int. World Wide Web Conf.*, Hyderabad, India, 2011, pp. 187–196.
- [10] D. Canali, M. Cova, G. Vigna, and C. Kruegel, "Prophiler: A fast filter for the large-scale detection of malicious Web pages," in *Proc. Int. World Wide Web Conf.*, Hyderabad, India, 2011.
- [11] M. Hasan and Z. Balbahaith, "Detection of drive-by download attacks using machine learning approach," *Int. J. Inf. Secur. Privacy*, vol. 11, no. 4, pp. 1–13, 2017.
- [12] N. Provos, M. Panayiotis, M. A. Rajab, and F. Monrose, "All your iFRAMEs point to us," in *Proc. USENIX Secur. Symp.*, 2008, pp. 1–15.
- [13] Z. Gardezi, *Still Getting Served: A Look at Recent Malvertising Campaigns Involving Exploit Kits*. Accessed: Oct. 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/03/still_getting_served.html
- [14] K. Sen, S. Kalasapur, T. Brutch, and S. Gibbs, "Jalangi: A selective record-replay and dynamic analysis framework for JavaScript," in *Proc. 9th Joint Mtg. Found. Softw. Eng.*, Saint Petersburg, Russia, 2013, pp. 488–498.
- [15] L. Lu, R. Perdisci, and W. Lee, "Surf: Detecting and measuring search poisoning," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, Chicago, IL, USA, 2011, pp. 467–476.
- [16] L. Lu, R. Perdisci, and W. Lee, "WarningBird: Detecting suspicious URLs in Twitter stream," in *Proc. NDSS Symp.*, San Diego, CA, USA, 2012.
- [17] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang, "Knowing your enemy: Understanding and detecting malicious Web advertising," in *Proc. ACM Conf. Comput. Commun. Secur.*, Raleigh, NC, USA, 2012.
- [18] T.-H. Chuang, S.-Y. Huang, Albert B. Jeng, Hahn-Ming Lee, and C.-H. Mao, "Ziffersystem: A novel malware distribution detection system," in *Proc. IEEE Conf. Dependable Secure Comput.*, Aug. 2017, pp. 509–515.
- [19] S. Peryt, J. Morales, W. Casey, A. Volkman, B. Mishra, and Y. Cai, "Visualizing a malware distribution network," in *Proc. IEEE Symp. Vis. Cyber Secur.*, Oct. 2016, pp. 1–4.
- [20] G. Wang, J. Stokes, C. Herley, and D. Felstead, "Detecting malicious landing pages in malware distribution networks," in *Proc. Dependable Syst. Netw. (DSN) Conf.*, 2013.
- [21] A. Walker, M. Amjad, and S. Sengupta, "Cuckoo's malware threat scoring and classification: Friend or foe?" in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf.*, Las Vegas, NV, USA, Jan. 2019, pp. 678–684.
- [22] R. McCollum, D. Brown, S. B. O'Shea, W. Reith, J. Rabulan, and G. Melrose, "Multidimensional risk analysis: MRISK," Langley Research Center, NASA, Hampton, VA, USA, Tech. Rep. 20150018915, Sep. 2015.
- [23] GitHub. (2019). *Gatekeeper*. [Online]. Available: <https://github.com/AltraMayor/gatekeeper>
- [24] Suricata. (2019). *Open Information Security Foundation*. [Online]. Available: <https://suricata-ids.org/>
- [25] Trustwave. (2019). *ModSecurity 3.0*. [Online]. Available: <https://modsecurity.org/>
- [26] GitHub. (2019). *MailScanner*. [Online]. Available: <https://github.com/MailScanner/v5>
- [27] (2019). *Open-Xchange*. [Online]. Available: <https://www.open-xchange.com/>
- [28] Stichting Cuckoo Foundation. (2019). *Cuckoo Sandbox*. [Online]. Available: <https://cuckoosandbox.org/>
- [29] (2019). *Virustotal*. [Online]. Available: <https://www.virustotal.com/gui/home/upload>
- [30] (2019). *Malwares.com*. [Online]. Available: <https://www.malwares.com/>
- [31] (2019). *Malware-Traffic-Analysis.net*. [Online]. Available: <https://www.malware-traffic-analysis.net/>
- [32] Secrepo.com. (2019). [Online]. Available: <http://www.secrepo.com/>

• • •