악성코드의 경유/유포지 위험도 산출에 관한 접근방법

김도훈* · 최동희* · 문진규* · 진종현* · 이태진** · 인 호***

1. 서 론

대규모 네트워크망 관리자 입장 (ISP)에서 산발적이고 예측 불가능한 다양한 악성코드의 출현은 탐지 및 관리(대응) 하는데 있어 많은 어려움이 따른다. 특히, 악성코드를 경유/유포하고 있는 웹페이지들은 그 잠재적 위험이 높고 확산을 유발할 수 있다. 때문에 이러한 위협에 대응하기 위해 다양한 악성코드 유포 및 경유 사이트를 탐지하는 연구가 수행되어져 왔다. 특히, 한국인터넷진흥원에서는 MC-Finder라는 악성코드 탐지 시스템을 개발 운용하면서, 하루에 180만개 이상의 웹 사이트를 분석하고 있다. 하지만, 탐지되는 악성코드 경유/유포 사이트의 관리 및 대응에 있어서는 의사결정, 우선대응 및 인적자원(Human Resource) 등의 한계가 있다.

따라서 관리자 입장에서 효율적으로 대응하기 위해서 악성코드 경유/유포 사이트의 위험도를 산정하여 위험 순위별로 관리 운용하는 것이 중요하다. 또한, 본 논문은 탐지된 악성코드 경유/유포 사이트 정보를 유포지와 경유지별로 잠재적 위험요소를 고려하여 웹사이트 (URL)별로 위험도를 산정하는 것을 목적으로 한다. 특히, 이러한 연구는 악성코드 관련 탐지 및 관리 측면에서 상대적 참조 요인으로 사용할 수 있게 재가공하는데 그 목적이 있다.

게다가, 악성코드 경유/유포 사이트 관리 측면에서 신규 사이트와 기존 악성코드 내포 사이트의 갱신 과정에서 발생할 수 있는 대량의 블랙리스트를 효과적으로 선별 적용 및 관리를 지원한다.

제안 연구의 실험 결과, 해당 사이트의 위험도 측정 관련 표본이 될 수 있는 악성코드 경유/유포 사이트 위험 함수 (Malicious URL Risk Index: MRI) 생성은 추후 악성코드 내포 사이트 관리를 위한 참조 위험 지수로 적극적으로 활용될 것이다.

2. 악성코드 경유/유포 사이트 위험도 분석

본 논문에서는 악성코드 파급 및 확산 위험도 산출 기술 연구에는 두 가지 접근 방법을 제안하고자 한다. 먼저, 악성코드 경유/유포 사이트의 위험도를 산출하는 방법이다.

해당 유포 사이트와 연결되어있는 다른 사이트 간의 상관 분석을 통해서 잠재적 위협 파급력을 분석하여 위험도를 산출한다.

다음은 말단 노드라 할 수 있는 악성코드를 재 유포하는 경유지 사이트의 위험도 예측 연구이다. 이를

※ 교신저자(Corresponding Author) : 인호, 주소 : 서울 성북구 안암동 고려대학교 자연계캠퍼스, 전화 : 02) 3290-3206, FAX : 02) 3291-3206, E-mail : hoh_in@korea.ac.kr
* 국방과학연구소 (E-mail : karmy01@add.re.kr)
** 한국인터넷진흥원 (E-mail : tjlee@kisa.or.kr)
*** 고려대학교

통하여 경유지 사이트의 개별 위험도를 추정한다.

2.1 악성코드 경유/유포 사이트 위험도 개념

기존의 전통적인 IT 자산의 위험도를 측정하는 방법은 해당 시스템의 보안 취약점과 실제 자산의 가치를 고려하여 아래와 같이 측정하게 된다.

$$Risk\ Exposure = Probability(Loss) \times Size(\$) \quad (1)$$

하지만, 이러한 방식의 접근은 네트워크 시스템 자산 분석이 선행이 되어야 하기 때문에 관리자 입장에서는 어려운 작업이다. 특히, 발전하는 네트워크 시스템의 가치를 반영하여야 하기 때문에 매번 자산 규모와 금액을 파악해야 하는 작업이 수반되어야 한다.

또한, 동적으로 변하는 네트워크 환경이나 다양한 네트워크 악성행위에 대해서는 고려하지 않기 때문에 실제 위험의 요소에 대한 직접적인 위험요소를 반영하지 못했다. 무엇보다도 많은 네트워크 보안사고 중 악성코드 경유/유포 사이트를 분석하는데 있어 위험 요소를 정량적으로 반영하는데 한계를 보였다. 따라서 본 연구에서는 위험도 산출을 위한 위험 벡터 개념을 소개하고자 한다.

그림 1에서 보듯이 평면상의 벡터가 두 개의 실수를 나열하여 표시 할 수 있는 바와 같이 3차원 공간내의 벡터에 대해서 직교자표계(直交座標系: rectangular coordinate system)를 도입함으로써 3개의 실수를 나열해서 표시할 수 있다.

공간의 직교좌표계는 원점 O와 이것을 지나서 서로 직교하는 3개의 실수를 나열해서 표시할 수 있다. 공간의 직교좌표계는 원점 O와 이것을 지나서 서로 직교하는 3개의 좌표축(座標軸: coordinate axes) x, y, z를 고정하여 x축, y축, z축의 각각에 양의 방향을 지정해서 단위에 의한 길이를 지정하면 정해진다.

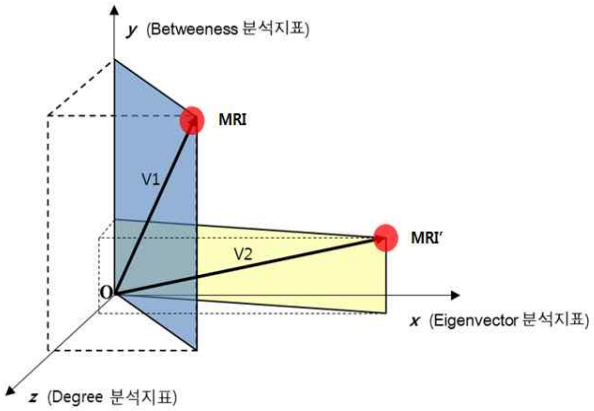


그림 1. 악성코드 경유/유포 사이트의 위험도 산정을 위한 전체 분석 구성도

이처럼, 악성코드 경유/유포사이트의 위험도 산정은 크게 3가지 벡터 (연결, 위세 및 매개 분석값)로 구성이 되어 있으며, 벡터합으로 길이값을 표현한다. 즉, 서로 다른 성질의 벡터값을 길이로 표현하고, 이를 통하여 위험의 크기를 정량화 하는데 그 목적이 있다.

다음은, 탐지된 악성코드 경유/유포 사이트의 위험도 산정을 위해 각 고려 요소에 대한 정의를 하고자 한다.

가. 노드의 연결 중심성 분석
(Degree Centrality Analysis of Nodes)
: 직접 연결된 이웃 노드가 많을수록 연결 중심성이 높아짐. 직접적인 영향력의 크기를 측정

나. 노드의 위세 중심성 분석
(Eigenvector Centrality Analysis of Nodes)
: 다른 노드 간의 최단 경로에 많이 포함된 노드(가장 많이 거치게 되는 노드)가 매개 중심성이 높음. 매개중심성이 높은 노드는 정보 흐름에 대한 통제력을 가지며, 이 노드가 제거될 경우 네트워크 전체연결과 흐름에 큰 영향을 미치게 됨

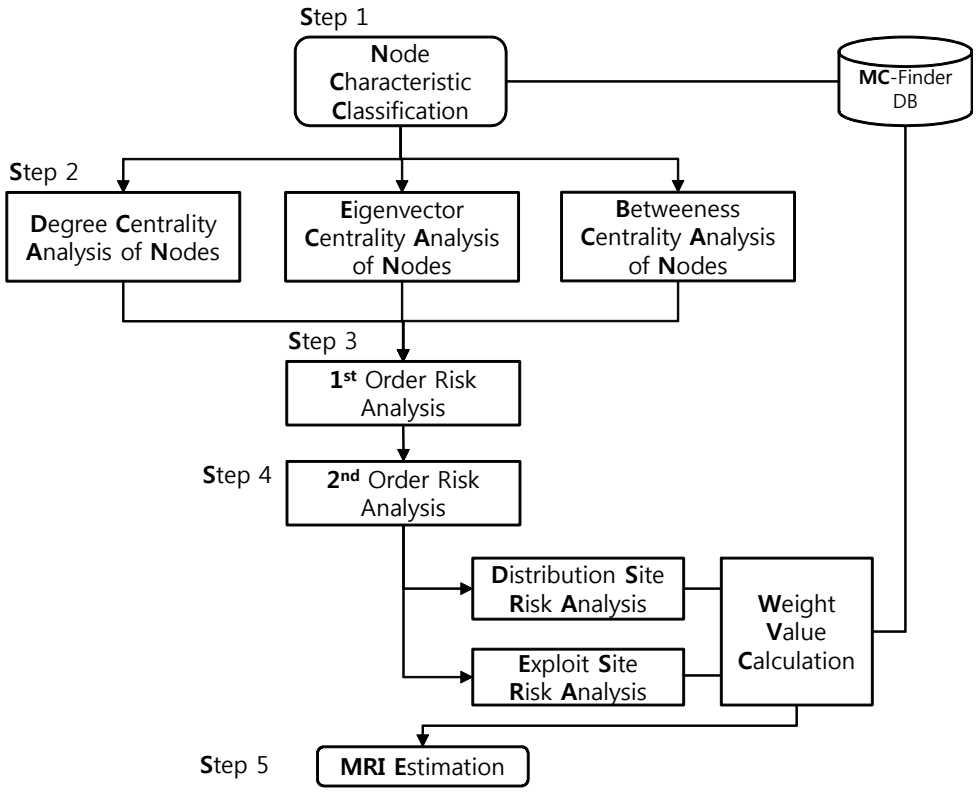


그림 2. 악성코드 경유/유포 사이트의 위험도 산정을 위한 전체 분석 구성도

다. 노드의 매개 중심성 분석
(Betweeness Centrality Analysis of Nodes)
: 한 노드의 위세 중심성은 위세 중심이 높은 이웃들과 많이 연결되어 있을수록 높아짐. 위세 중심성이 높은 노드로부터 어떤 변화가 발생하면, 그로부터 유발되는 파급효과가 큼. (ex: Page-Rank 알고리즘을 응용한 위험도 산정방법)

2.2 악성코드 경유/유포 사이트 위험도(MRI)

악성코드를 경유/유포하고 있는 해당 URL의 위험도 산정하기 위해서는 그림 2와 같은 프로세스를 따른다.

가. Step1 - 노드 성격 분류
(Node Characteristic Classification)
- MC-Finder의 DB에서 생성된 로그로부터 경유지/유포지 정보 분류한다. 그리고 악성코드 경유/유포 사이트의 단위로그에서 시간대별로 탐지 이력을 정렬(Sorting)한 것이다. 아래와 같은 로그 정보를 가지고 기본적인 위험도 산정을 하게 된다.

① 노드의 성격 : 탐지된 감염 사이트가 유포지인지 경유지인지를 판단하는 것으로, 탐지된 악성코드의 링크(최초 감염사이트 정보)가 없을 경우, 유포지로 결정하고, 타 사이트의 URL 링크가 경유/유포되어 있으면, 경유지로 판단한다.

② 악성코드 경유/유포 사이트 정보: 탐지된 악성코드 경유/유포 사이트의 인터넷주소(URL)을 의미하며, 경유지 사이트가 유포지 사이트가 될 수 있다. 즉, 유포지 사이트

가 자체 혹은 타 탐지 시스템에 의거하여 제거가 될 경우, 경우지 사이트가 유포지 사이트로 재 도용되고 이를 토대로 지속적으로 악성코드 유포 사이트로 운용 된다.

③ IP 주소, 국가 코드 및 생존여부: IP 주소를 통하여 기초 정보를 수집하고, 관련서버 위치정보 및 현재 운용 상태를 파악한다. 특히, 해당 경유/유포지 사이트의 생존여부 위험도 산정에 매우 중요한 역할을 하게 되고, 치료 또는 격리가 되어 운용을 하지 않더라도, 취약점 계속적으로 노출되고 있는 한, 앞으로도 재감염이 발생할 수 있음을 예의주시하고 위험도 산정에 반영하여야 한다.

나. Step2 – 노드의 중심도 분석
(Centrality Analysis of Node)

– 크게 3가지 유형으로 각각의 노드를 다음과 같이 분석할 수 있다.

- 노드의 연결 중심성 분석
(Degree Centrality Analysis of Nodes)
- 노드의 위세 중심성 분석
(Eigenvector Centrality Analysis of Nodes)
- 노드의 매개 중심성 분석
(Betweeness Centrality Analysis of Nodes)

① 노드의 연결 중심성 분석
(Degree Centrality Index: DCI)

· 직접 연결된 이웃 노드가 많을수록 연결 중심성이 높아짐. 직접적인 영향력의 크기를 측정함.
· 연결 중심성 분석은 각 노드의 구성 비율로 간단히 계산 가능하다.

degree centrality of node

$$= \frac{\sum(weight\ of\ incident\ link)}{\#\ of\ nodes\ -\ 1} \qquad (2)$$

· 시각 복잡도: O(m)

② 노드의 위세 중심성 분석
(Eigenvector Centrality Index: ECI)

· 노드 N_j가 l_j개의 링크를 포함하고 있다고 가정한다. 만약 이들 링크중 하나가 노드 N_i로 연결이 된다면, N_j는 $1/l_j$의 확률로 N_i로 지나가게 될 것이다. 따라서 최종 위세 중심성 분석 결과는 다음과 같다.

$$ECI = I(N_i) = \sum \frac{I(N_j)}{l_j} \qquad (3)$$

③ 노드의 매개 중심성 분석
(Betweeness Centrality Index: BCI)

· 매개중심성의 측정을 위해서는 한 노드와 다른 노드들 사이에 최단경로 상에 위치하는 정도를 측정한다.
· 상이한 집단 간을 연결하는 노드일수록 매개중심성이 높게 나타나며, 전체 네트워크 내에서 얼마나 다리 역할을 하는지 정도를 나타낼 수 있다.
· 이를 이용해서 분야 간의 정보연계의 역할을 담당하는 매개적 URL를 찾을 수 있다. 노드 i의 매개중심성은 다음의 수식으로 표현된다.
· 수식에서 g_{jk}는 네트워크內 두 노드(j와 k) 사이에 존재하는 최단경로의 경우의 수를 의미하고, $g_{jk}(n_i)$는 두 노드(j와 k)의 최단경로들 중에서 노드 i을 포함하는 경우의 수라고 하면, 최단경로들 중에서 노드 i가 포함될 확률은 $g_{jk}(n_i)/g_{jk}$이라는 것을 의미한다.

$$BCI = C_B(n_i) = \sum_{j<k} g_{jk}(n_i)/g_{jk} \qquad (4)$$

다. Step3 – 1차 위험도 분석
(1^{st} Order Risk Analysis)

Step2에서 산정된 노드 분석 결과를 유클리디언 거리 산정 방법을 고려하여 1차 위험도를 산출 한다. 따라서 1차 위험도 기본적으로 Step 2에서 생성된 값들의 벡터 거리 산정식 으로 계산이 된다.

$$r_1 = \sqrt{DCI^2 + ECI^2 + BCI^2} \quad (5)$$

라. Step4 - 2차 위험도 분석
(2nd Order Risk Analysis)

① 유포지 중심 위험도 분석
(Distribution Site Risk Analysis)

- Step3에서 산정된 1차 위험도 분석 결과를 토대로 가중치(중복감염이력정보, 생존율)를 고려하여 위험도를 산정한다.

유포지 중심 위험도는 기본적으로 Step 3에서 생성된 값들의 벡터값과 각 유포지 노드의 중복감염 이력(I) 그리고, 실제 생존율(S)에 의해 계산이 된다.

* 생존율(S): 감염된 이후 조치 여부
(1년치 정보 기준)

$$\text{치유확률}(S_1) = \frac{\text{생존건수}}{\text{생존건수} + \text{치료건수}},$$

$$\text{실패확률}(S_2) = \frac{\text{치료건수}}{\text{생존건수} + \text{치료건수}} \quad (6)$$

$r_2 = r_1 \times I \times S_1$ (해당노드가치료 되었을경우)
$r_2 = r_1 \times I \times S_2$ (해당노드가치료되지않았을경우)

② 경유지 중심 위험도 분석
(Exploit Site Risk Analysis)

- Step3에서 산정된 1차 위험도 분석 결과를 토대로 가중치(중복감염이력정보, 노출횟수)를 고려하여 위험도를 산정한다. 경유지 중심 위험도는 기본적으로 Step 3에서 생성된 값들의 벡터값과 각 유포지 노드의 중복감염 이력(I) 그리고, 실제 검색사이트 내 노출 횟수(E)에 의해 계산이 된다.

$$r_3 = r_1 \times \left(\frac{2 \times I \times E}{I + E}\right) \quad (6)$$

$$r_3 = r_1 \times I \quad (7)$$

마. Step5 - 최종 위험도 분석
(Malicious URL Risk Index: MRI)

Step4에서 산정된 각각의 위험도를 재차 1차 위험도를 고려하여 최종 위험도를 산정한다. 즉, Step3에서의 1차 위험도와 Step 4에서 계산된 각각의 유포지 / 경유지 위험도 정보를 고려하여 해당 노드 성격에 맞추어 다음과 같이 최종 산출한다.

$$r_{final} = \sqrt{r_1^2 + r_2^2 + r_3^2} \quad (8)$$

3. 적용방안

본 연구의 실험을 위해서는 한국 인터넷 진흥원에서 제공한 MC-Finder의 탐지 로그를 사용했으며, Step1에서 언급한 로그 형태로 가공하여 사용하였다. 다음은 MC-Finder의 시스템 개요이다.

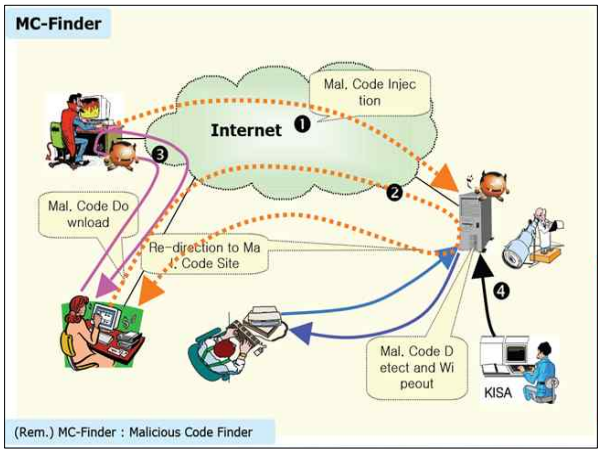


그림. 3 MC-Finder 시스템 개요

그림 3에서와 같이 공격자(해커)는 ①인터넷 상에서 직접 ②악성 유포 서버를 운영하거나 ② 취약한 웹 서버를 ③해킹하여 악성코드를 특정 페이지에 삽입 시킨다. 이때, 해당 웹서버를 이용하는 ④사용자(client)는 본인도 모르게 악성코드가 내포된 유포 및 경유지 사이트를 이용하게 되고, 자동적으로 악성코드를 다운로드 받게 된다. 마지막으로 공격자(해커)는 감염된 서버 및 사용자의 계정 및 각종 정보를 수집하여 악의적인 행위를 수행한다.

따라서 현재 운영 중인 해당 시스템은 지속적으로 180만개 사이트를 탐색하고 크롤링(crawling) 하여 내포된 악성코드를 탐지 후 차단 및 블랙리스트 DB로 구축 운용한다.

4. 분석결과 및 시각화

4.1 분석결과

본 연구는 MC-Finder의 특정 기간 중 운용된 결과를 토대로 분석되어지는 사후 연구로써, 보안 전문가 또는 관리자가 운용업무의 효율성을 극대화시키기 위하여 선 대응 후조치를 할 수 있는 의사결정을 도와주는 방안이다.

이를 토대로 탐지 후, 분석되어지는 악성코드의 URL을 1, 2차 경유지 중심 위험도 분석을 통하여 그림 4와 같은 최종 위험도를 산출 할 수 있다.

그림 4는 탐지되어 있는 악성코드 경유/유포 URL (경유/유포지 모두 포함)을 최종 위험도 기반으로 나열한 것으로 위험도의 크기는 상대적으로 나타낸 것이다. 만약 위험도의 크기를 0에서 1까지 제한을 하게 되면, 최저 위험도는 0으로 고정이 되지만, 최고 위험도에 대한 명확한 기준을 제시하기가 어렵다.

따라서 본 연구에서는 최저 위험도 0에서부터

노드상격	악성 URL	최종 위험도	유포지IP Address	유포지국가	유포지국가코드
유포지	ww.amcia.i	18.38	21	한국	KR
유포지	A%2E%32%	12.85	61.	한국	KR
유포지	p://www.ro	8.21	114.1	한국	KR
유포지	%67%6F%6	5.51	114.1	한국	KR
유포지	104,116,11	2.81	116	한국	KR
유포지	ttp://qh888	1.75	210.1	한국	KR
유포지	ww.wowsh	1.75	211	한국	KR
유포지	ww.housew	1.43	118.	한국	KR
유포지	.baro-ck.co	1.40	121.2	한국	KR
유포지	.swf?	1.33	114.1	한국	KR
유포지	.ksrit.or.kr/	1.21	123.	한국	KR
유포지	9,114,105.	0.84	175	한국	KR
유포지	ww.interba	0.80	218.2	한국	KR
유포지	/www.kra.r	0.64	61.	한국	KR
유포지	wjackey.co	0.52	119.	한국	KR
유포지	ww.ksm.or.	0.48	210.	한국	KR
유포지	ni.co.kr/reti	0.45	211.	한국	KR
경유지	http://r	0.38	180.1	한국	KR
유포지	crm.ofem.c	0.34	211.	한국	KR
유포지	%2E30%2E	0.33	203.	한국	KR
경유지	http://iairc	0.32	211.1	한국	KR
유포지	ttp://jiekef	0.30	118.1	한국	KR
유포지	/www.amci	0.28	119.2	한국	KR
유포지	72%69%70	0.28	211.	한국	KR
유포지	p://www.ge	0.23	121	한국	KR
유포지	earch.nave	0.18	121.2	한국	KR
유포지	p://210.116	0.17	210.	한국	KR
유포지	ttp://173.1	0.17	218	한국	KR
유포지	68 / 8 ,153	0.17	114.1	한국	KR
유포지	p://h.nexpri	0.17	210.1	한국	KR
유포지	http://j5	0.15	175	한국	KR
유포지	33%2E30.6	0.15	211.	한국	KR
경유지	.wsart.net/	0.14	211	한국	KR
유포지	p://lyzbg.33	0.12	121.1	한국	KR
경유지	ttp://www.	0.12	218.	한국	KR
경유지	feucc.com/	0.11	121.	한국	KR
유포지	tp://s19.cn	0.11	180.	홍콩	HK
유포지	%62ee%2E	0.10	211	한국	KR
경유지	http://chc	0.10	121	한국	KR

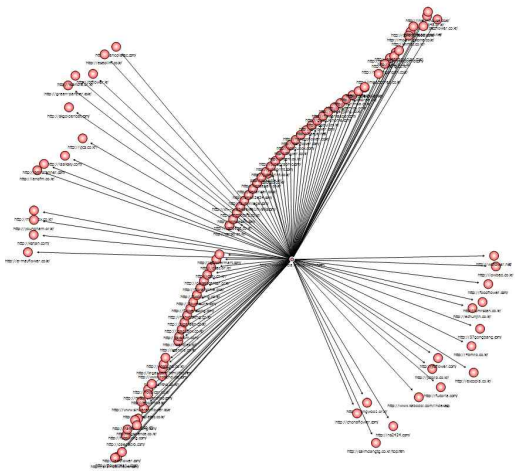
그림. 4 최종 위험도 산출 결과

산정되는 상대적 위험도를 그대로 표기하고 우선순위화를 위한 지표로 활용 한다.

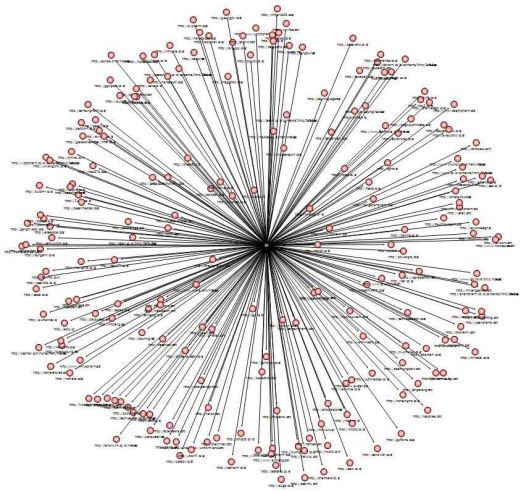
4.2 분석결과에 대한 시각화

본 연구에서 산출된 각 URL의 위험도가 해당 서버의 취약점과 유사한지를 검증을 통해 분석되어져야 한다. 따라서 본 장에서는 산출된 위험도의 실제 취약점 분석을 시도하여 실제 우선순위와 유사한지 또 오차 분석을 통해서 정확도를 검증하고자 한다. 다음은 최종 위험도에서 위험도 1위로 분석된 유포지 사이트와 2위로 분석된 유포지 사이트의 시각화를 한 것이다.

그림 5와 같이 최종 위험도를 고려 해당 경유/유포지 사이트 (1, 2위 기준)를 시각화 하여, 보안 전문가 및 관리자로 하여금 선 대응/후 조치를 위한 의사결정 기준을 제공한다.



1위 유포지 사이트의 네트워크 구성도



2위 유포지 사이트의 네트워크 구성도

그림 5. 유포지 기준 위험도 시각화

5. 결 론

본 논문은 악성코드 경유/유포 사이트 탐지 시스템(MC-Finder)에 의해 산출된 로그정보를 통해 기존적인 1차 위험도를 산출하였다.

이때, 노드의 연결 중심성, 매개 중심성, 위세 중심성을 고려하여 계산하였으며, 노드가 기본적으로 보유하고 있는 잠재적 위험의 정량적인 값이라고 볼 수 있다.

또한, 가중치를 고려하여 유포지 및 경유지 기준 위험도를 산출 하였다. 유포지 기준 위험도는 유포지의 중복 감염이력과 생존확률을 고려하여 위험도를 산정하였다. 그리고 경유지 기준 위험도는 경유지의 중복 감염이력과 경유지 사이트의 노출 횟수를 고려하여 위험도를 산정하였다. 최종적으로 1차 위험도의 결과와 유포지 및 경유지 위험도를 고려하여 최종 위험도를 산출하였다.

따라서 향후에는 웹 페이지 악성코드 탐지 툴과 웹 페이지 취약성 스캐닝 툴들로 부터 생성된 로그를 데이터 마이닝을 통하여 웹 사이트의 보안 심각성을 미리 추정하기 위한 feature model을 연구하고자 한다.

결국, 해당 feature model은 웹 사이트의 위험도를 추정하는데 이용될 수 있기 때문에 기존 악성 코드 탐지 툴에만 의존한 후 대응적 조치(reactive response)에서 발생하는 한계를 넘어선 대비 조치적 (proactive response)인 보안 관리를 도울 수 있도록 한다.

참 고 문 헌

[1] Qingtao Wu Zhiqing Shao., “Network Anomaly Detection UsingTime Series Analysis”, Autonomic and Autonomous Systems and International Conference on Networking and Services, 2005.

[2] Hiroshi Konno, Tomoyuki Koshizuka, Hiroshi Konno, Tomoyuki Koshizuka, “Mean-absolute deviation model”, 2005, 893-900.

[3] J. Franklin and A. Perrig, “An inquiry into the nature and causes of the wealth of internet miscreants,” in Proceedings of the 14th ACM conference on Computer and Communications Security, SESSION: Internet Security, Alexandria, Virginia, 2007, pp. 375 - 388.

[4] A. W. F. Edwards, “Likelihood: An account of the statistical concept of likelihood and its application to scientific inference”, Cambridge University Press (1972). Reprinted in 1992, ex-

panded edition, Johns Hopkins University Press.
[5] Lawrence A. Gordon and Martin P. Loeb, "MANAGING CYBERSECURITY RESOURCES: A Cost-Benefit Analysis," McGraw-Hill, 2006.
[6] Sang-Keun Jang and Proactive Response Research Team / HAURI, "7.7 DDoS Virus Report in Korea & USA", http://www.max-overpro.org/77DDoS.pdf
[7] Peter Gutmann, "The Convergence of Internet Security Threats," http://www.cs.auckland.ac.nz/~pgut001/pubs/blended.pdf
[8] Xiaojie Liu, "An immune method for network security risk evaluation," Evolutionary Computation, 2008.
[9] Lawrence A. Gordon and Martin P. Loeb, "MANAGING CYBERSECURITY RESOURCES: A Cost-Benefit Analysis," McGraw-Hill, 2006.
[10] Paul Judge, Dmitri Aplperovitch, and Weilai Yang, "Understanding and Reversing the Profit Model of Spam (Position Paper)," Fourth Workshop on the Economics of Information Security, March 6, 2005.
[11] Barry W. Boehm, "Software Risk Management: Principles and Practices," January/February 1991, (vol. 8 no. 1).
[12] Howard Anton, "Elementary Linear Algebra 8E," John Wiley & Sons, Inc. 2005.
[13] Siv Hilde Houmb, Virginia N. L. Franqueira and Erlend A. Engum, "Quantifying security risk level from CVSS estimates of frequency and impact," Journal of Systems and Software, Volume 83 Issue 9, September, 2010.
[14] Korea Internet & Security Agency, http://www.kisa.or.kr/main.jsp
[15] Joseph F. Hair, Ronald L. Tatham, Rolph E. Anderson and William Black, "Multivariate Data Analysis," Prentice Hall; 5th edition (March 23, 1998).
[16] Brandes, "A faster algorithm for betweenness centrality," Journal of Mathematical Sociology 25: 163-177, 10.11.2011.
[17] Borgatti, "Centrality and Network Flow," Social Networks 27: 55-71, 2005.
[18] Duijin, M. A., & Vermunt, J. K., "What is special about social network analysis?" Methodology, 2(1), 2-6., 2006.
[19] Freeman, L. C. "The development of social network analysis" Vancouver, Canada: Empirical Press., 2004.
[20] Carrington, j.p., Scott, J. and Wasserman, S. "Models and Methods in Social Network Analysis," Cambridge: Cambridge University Press., 2005.

김 도 훈

- 2005년 고려대학교, 수학/컴퓨터학 학사
- 2007년 고려대학교, 컴퓨터학 석사
- 2012년 고려대학교, 컴퓨터학 박사
- 현 재 국방과학연구소, 선임연구원
- 관심분야: 정보보호, 네트워크보안, 미래인터넷, 상황인지 및 소프트웨어 공학

최 동 희

- 2000년 연세대학교 전산학 학사
- 2004년 서강대학교 컴퓨터학 석사
- 현재 국방과학연구소, 선임연구원
- 관심분야: 정보보호, 웹 서비스 보안

문 진 규

- 1998년 충남대학교 계산통계학과
- 1990년 충남대학교 컴퓨터과학과 이학석사
- 2002년 충남대학교 컴퓨터과학과 이학박사
- 1989년 현재 국방과학연구소 책임연구원
- 관심분야: 정보보호, 데이터베이스, 소프트웨어 공학

진 종 현

- 1982년 동국대학교, 전자계산학 학사
- 1984년 동국대학교, 전자계산학 석사
- 1998년 KAIST/테크노경영대학원, 경영공학 박사수료
- 현재 국방과학연구소, 책임연구원
- 관심분야: 소프트웨어공학, 시스템아키텍처, 네트워크M&S

이 태 진

- 2003년 포항공과대학교 컴퓨터공학과 공학학사
- 2003년 연세대학교 컴퓨터공학과 공학석사
- 현재 한국인터넷 진흥원 책임연구원
- 관심분야: 네트워크 보안, 악성코드 침해대응

인 호

- 1992년 고려대학교 전산학 학사
- 1994년 고려대학교 전산학 석사
- 1998년 University of Southern California (USC), computer science, Ph. D
- 1999년~2003년 Texas A&M University 조교수
- 2003년~현재 고려대학교 교수
- 2004년~현재 San Francisco State University 겸임 교수