Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.93

악성코드 유포 사이트 특성 분석 및 대응방안 연구

김 홍 석,† 김 인 석‡
고려대학교 정보보호대학원

A Study on Characteristic Analysis and Countermeasure of Malicious Web Site

Hong-seok Kim,† In-seok Kim‡
Graduate School of Information Security, Korea University

요 약

최근 드라이브 바이 다운로드 공격 기반의 웹사이트를 통한 랜섬웨어 악성코드 유포로 인해 웹사이트 서비스 마비, 일반 이용자 PC 파일 손상 등의 피해가 발생하고 있다. 따라서 악성코드 경유지 및 유포지 사이트의 현황과 추이 파악을 통해 악성코드 유포의 공격 대상 웹사이트 업종, 유포 시간, 악용되는 어플리케이션 종류, 유포되는 악성코드 유형에 대한 특성을 분석하는 것은 공격자의 공격활동을 예측하고 대응이 가능하다는 점에서 의미가 크다. 본 논문에서는 국내 343만개의 웹사이트를 대상으로 악성코드 유포여부를 점검하여 탐지된 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트별로 어떠한 특징들이 나타나는지를 도출하고, 이에 대한 대응방안을 고찰하고자 한다.

ABSTRACT

Recently, malicious code distribution of ransomware through a web site based on a drive-by-download attack has resulted in service disruptions to the web site and damage to PC files for end users. Therefore, analyzing the characteristics of the target web site industry, distribution time, application type, and type of malicious code that is being exploited can predict and respond to the attacker's attack activities by analyzing the status and trend of malicious code sites. In this paper, we will examine the distribution of malicious codes to 3.43 million websites in Korea to draw out the characteristics of each detected landing site, exploit site, and distribution site, and discuss countermeasures.

Keywords: Malicious web site, Drive by download Attack, Exploit site, Malware

I. 서 론

우리나라 인터넷 이용자수가 2017년 기준 4천 5백만 명이 넘고, 인터넷 이용률은 90%에 육박한다[1]. 인터넷 이용자 및 이용률이 높게 나타남에 따라 인터넷을 통해 악성코드에 감염될 가능성도 높은 실정이다.

악성코드를 유포하는 경로는 웹사이트, 전자메일, SNS, 이동형 저장장치 등 다양하게 존재한다. 그중에서도 웹사이트를 통한 악성코드 유포는 인터넷의 사용이 급격히 증가하면서부터 큰 위협으로 나타나고 있다. 최근에는 웹사이트를 통한 드라이브 바이 다운로드 기반의 랜섬웨어 악성코드 공격으로 인한 피해가 지속적으로 발생하고 있다.

악성코드 전파에 악용되는 악성코드의 경유지 및 유포지의 특성을 잘 파악하고 이해함으로써 공격자의 공격활동을 예측하고 대응이 가능해진다. 본 논문에서는 국내 343만개의 웹사이트를 대상으로 악성코드 유포여부를 점검하여 탐지된 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트별로

Received(11. 06. 2018), Modified(12. 10. 2018), Accepted(01. 22. 2019)
† 주저자, milleniumkhs@kisa.or.kr
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

특징들을 알아보고 이에 대한 대응방안을 고찰하고자 한다.

II. 관련 연구 동향

Fig.1.과 Fig.2.는 한국인터넷진흥원에서 2018년 7월에 발간한 2018년 상반기 악성코드 은닉사이트 동향보고서에 따르면, 악성코드 경유지 사이트는 전년 동기 대비 14% 증가하였으며, 악성코드 유포지 사이트는 전년 동기 대비 33% 증가한 것으로 나타내고 있다[2].

한국인터넷진흥원이 2017년 10월 13일 발표한 자료에 따르면, 2017년 5월12일 워너크라이로 불리는 랜섬웨어 악성코드로 인해 전 세계 150여개국에서 최소 30만대 이상의 컴퓨터 시스템이 피해를 입었다[3]. 이로 인해 우리나라 또한 피해가 발생하였으며, 랜섬웨어 악성코드의 유포는 해킹된 웹사이트의 방문으로 감염된 것으로 파악되고 있다.

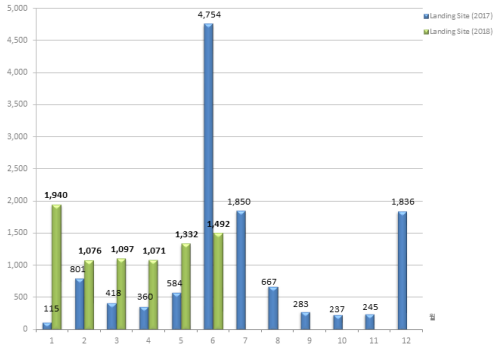

Fig. 1. Landing Site Detect Count (2018)

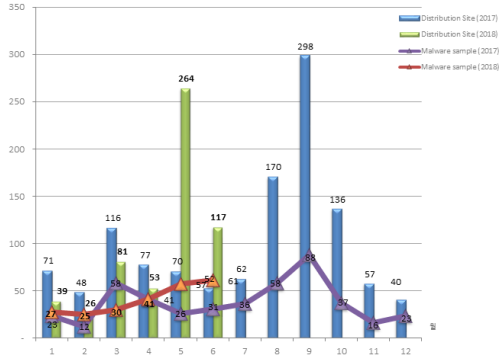

Fig. 2. Distribution Site Detect Count (2018)

일반 이용자가 웹사이트 방문만으로도 악성코드에 감염되는 드라이브 바이 다운로드 공격은 다음과 같은 과정을 통해 이루어지고 있다.

① 일반 이용자는 웹사이트에 접속한다.
② 접속한 웹사이트 페이지 내에는 익스플로잇 사이트 주소를 호출하게 되는 리다이렉트 코드가 삽입되어져 있다.
③ 일반 이용자의 시스템이 취약한 경우, 익스플로잇 코드가 실행되게 된다.
④ 익스플로잇 사이트 페이지 내에는 악성코드 유포지 주소를 호출하게 되는 리다이렉트 코드가 삽입되어져 있다.
⑤ 익스플로잇 코드가 실행됨과 동시에 악성코드 유포지로부터 악성코드를 다운로드 하고 실행되게 된다.

웹사이트 방문만으로도 악성코드에 감염되는 피해 사례가 발생함에 따라, 기존 연구에서는 드라이브 바이 다운로드 형태의 악성코드를 탐지하기 위한 웹크롤러 설계[4]나 자바스크립트 난독화 강도 분석을 통한 악성 의심 사이트 탐지[5] 및 악성코드 유포패턴 분석을 통한 탐지[6] 방법들을 제안하였다.

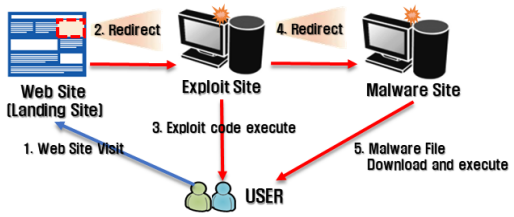

Fig. 3. Drive by Download Attack

III. 악성코드 유포 사이트 현황 및 특성 분석

3.1 악성코드 유포 사이트 분석대상 및 방법

본 논문에서는 국내 343만개 웹사이트를 대상으로 2014년 1월부터 2018년 6월까지 악성코드 유포 여부를 한국인터넷진흥원의 악성코드 탐지 시스템을 통해 정적 분석과 동적 분석으로 탐지된 결과를 이용하였고, 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트로 구분하여 각 사이트별 탐지 현황에 따라 어떤 특징들이 나타나는지 분석하였다.

웹사이트를 점검하기 위해 343만개에 대한 시드(seed) 도메인에 대해서는 한국인터넷진흥원이 보유하고 있는 ccTLD(.kr) 및 한글 도메인(.한국) 2,284,821개와 베리사인(VeriSign)으로부터 제공받은 전 세계 gTLD(generic Top Level Domain) 도메인(.com, .net, .name 등) 160,110,213개 중 국내 소재 IP인 도메인 1,149,708개를 추출하여 점검하였다.

Fig.4.는 악성코드 유포 사이트 탐지하기 위한 시스템 아키텍처를 보여주고 있으며, 웹사이트 점검 시 웹 크롤러를 통한 시그니처(블랙리스트) 기반의 정적 분석과 가상화 환경에서의 윈도우 웹브라우저(internet explorer)를 통해 해당 웹사이트를 직접 방문하도록 하여 악성코드가 자동으로 다운로드 되는지 여부를 확인하는 동적 분석으로 구현하였다.

정적 분석은 동시에 많은 웹사이트를 점검하기 위해 병렬구조의 멀티쓰레드 방식으로 웹 크롤러가 실행된다.

웹 크롤러를 통해 웹사이트 소스코드를 다운로드하여 소스코드 내에 외부 웹사이트나 외부 스크립트를 호출하는 HTML 태그(iframe, script, link) 및 자바 스크립트 태그를 파싱하여 25,221개의 악성사이트 시그니처(블랙리스트)와 비교하였으며, 웹사이트 점검 시 메인 페이지뿐만 아니라 하위 페이지에 대한 최대 깊이 4뎁스까지 설정하여 매일 4회 점검하였다. 하위 페이지의 최대 깊이 설정을 한 것은 웹사이트 점거 시 HTML 태그 및 자바 스크립트 태그를 파싱하여 링크를 추적하는 것이 무한 루프화 되는 것을 방지하기 위함이며, 하위 페이지 깊이가 4뎁스까지 미치지 못하는 웹사이트는 구축되어진 깊이만큼만 점검하고 그 다음의 웹사이트로 이동하여 점검하게 된다.

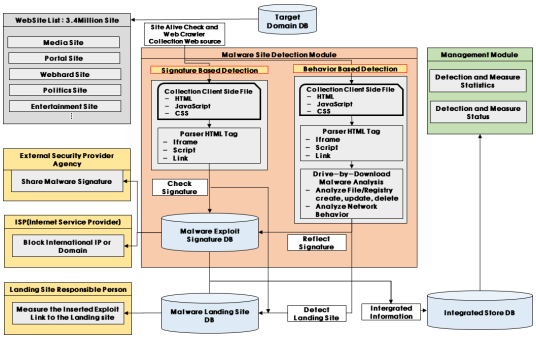

Fig. 4. Architecture of Malicious Web Site Detect

악성사이트 시그니처는 구글의 세이프 브라우징 및 마이크로소프트 윈도우 인터넷 익스플로러의 스마트스크린 필터에 적용되는 악성사이트 정보를 구글 및 마이크로소프트로부터 각각 제공받아 적용하였다. 또한 동적 분석을 통해 탐지된 악성사이트 정보를 정적 분석의 시그니처로 활용하였다.

동적 분석은 윈도우의 가상화 환경에 파일생성・수정・삭제, 레지스트리 생성・수정・삭제, 네트워크 행위를 후킹(hooking)하여 모니터링 할 수 있도록 구축하였으며, 자바, 어도비 플래시 플레이어, 실버라이트가 설치된 상태에서 웹브라우저(internet explorer)로 점검 도메인을 방문하였을 때 가상화 PC에 자동으로 악성코드가 다운로드 되는지를 확인하였다.

악성코드가 자동으로 PC에 다운로드 되는 것은 설치된 자바, 어도비 플래시 플레이어, 인터넷 익스플로러 어플리케이션의 취약점이 익스플로잇 되어 악성코드가 다운로드 되는 것을 의미한다.

3.2 악성코드 유포 사이트 탐지현황

Table 1.은 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트 탐지현황을 나타내며, 악성코드 유포지에서 악성코드 샘플 1개를 유포하기 위해 평균적으로 악성코드 경유지 사이트는 39개, 익스플로잇 사이트는 4개가 악용되었음을 알 수 있다.

악성코드 경유/유포지 특성 및 구조 분석[7] 논문의 분석결과와 비교하였을 때, 악성코드 샘플 1개당 악용되는 익스플로잇 사이트 수는 유사하나 악성코드 경유지 사이트에 대해서는 7.8배 차이가 나는 것을 알 수 있다.

악성코드 경유지 사이트 탐지에서 차이가 발생하는 것은 악성코드 유포 여부를 점검하기 위한 시드

Table 1. Malicious Web Site Detect Count(URL)

Year	Landing Site	Exploit Site	Malware Site
2014	45,120	4,398	813
2015	43,555	4,907	1,077
2016	9,674	2,224	448
2017	12,150	645	445
2018.6.	8,008	42	240
Total	118,507	12,216	3,023

(seed) 도메인에서 약 163만개가 차이가 나며, 점검 방식에 있어서도 본 논문에서는 정적 분석과 동적 분석을 병행하여 점검하는 부분에 있어 차이가 난다고 볼 수 있다. 악성코드 유포 사이트에 대한 좀 더 높은 탐지율을 위해서는 첫째로 시드(seed) 도메인의 양과 점검주기 시간이 중요하다. 점검해야 할 대상의 도메인이 많다는 것은 악성코드를 유포할 수 있는 대상이 많아질 수 있다는 것을 의미하며, 악성코드를 유포하고 있을 시점에 웹사이트를 점검해야 탐지가 될 수 있다. 웹사이트의 점검주기 시간이 길어지면 악성코드를 유포하고 난 이후에 공격자가 추후에 재악용 하려고 악성코드 유포 흔적을 제거한 상태일 때 악성코드 유포 여부를 점검하게 되어 정상적인 사이트로 결과가 나오기 때문에 점검주기 시간을 짧게 가지는 것이 중요하다.

둘째, 점검 방식에서도 동적 분석만을 사용하여 탐지하는 것보다는 정적 분석과 혼용하여 하위 페이지까지 깊이 있게 점검하는 것이 탐지율이 높은 것으로 파악되었다.

3.3 악성코드 경유지 사이트 재악용 현황

Fig.5.는 Table 1.의 악성코드 경유지 사이트의 URL에 대해 도메인 기준으로 재분류하였으며, 분류된 도메인에 대해 얼마나 다시 재악용 되고 있는지 보여 주고 있다. 2014년도에는 경유지 사이트 도메인에 대해 23.9%가 재악용 되어 가장 높게 나타났으며, 그 이후에는 점차 감소하였다. 전체 5년간 평균을 산정하였을 때에는 탐지된 경유지 사이트 도메인에 대해 17.3%가 재악용 된 것으로 파악되었다.

[7]논문에 따르면 2014년 악성코드 경유지 사이트가 2회 이상 탐지된 사이트의 비율을 47%로 나타내고 있다. 본 논문에서 2014년의 재악용 비율과는 23.1%의 차이가 나지만 2014년에 가장 많이 재악용 되었다는 것은 동일하다.

본 논문에서 악성코드 재악용 비율이 낮게 측정되는 이유는 탐지된 악성코드 경유지 사이트에 대한 빠른 조치 대응 여부에 달려 있다. 탐지된 모든 악성코드 경유지 사이트에 대해 웹사이트 관리자에게 메일 및 유선으로 연락하여 악성코드 유포 사실에 대한 정황을 인지시켜 주고 조치하도록 요청한 결과, 웹사이트 관리자는 악성코드 경유지 사이트에 삽입된 악성 스크립트를 삭제 및 근본적인 웹 취약점까지 제거함으로써 공격자의 재악용 빈도가 줄어든다는 것이다.

3.4 악성코드 경유지 사이트 조치시간 분석

악성코드 경유지는 일반 이용자가 제일 처음 접속하게 되는 웹사이트이기 때문에 익스플로잇 사이트로 주소를 호출하게 되는 리다이렉트 코드가 삽입되어져 있기 때문에 단기적으로는 웹 소스내에 리다이렉트 코드를 삭제하여 연결되어지는 링크를 단절시키는 방법을 사용할 수 있지만 공격자가 웹 취약점을 통해 재악용 될 소지가 높으므로 장기적으로는 웹 소스내에 취약점이 존재하는지 유무를 점검하여 제거하는 것이 근본적인 대책이라 할 수 있다. Fig.6.은 악성코드 경유지 사이트에 대해서 리다이렉트 코드를 삭제 또는 웹 소스내에 내포된 웹 취약점을 제거하기까지 소요된 평균 시간을 측정한 결과이다. 2014년부터 2018년까지 조치되기까지의 평균 소요시간을 살펴보면, 2017년에 241시간(10일)으로 가장 짧았고, 2015년에 512시간(21일)으로 가장 길게 나타났다. 5년간에 대해 조치 소요시간을 재계산해 보면 356시간(14일)이 경유지 사이트를 조치하는데 필요로 하는 평균시간으로 분석되었다.

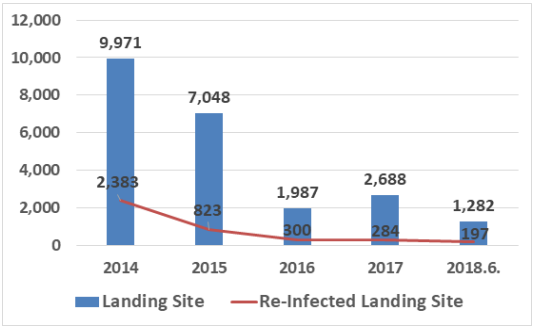

Fig. 5. Re-Infected Landing Site Count (Domain)

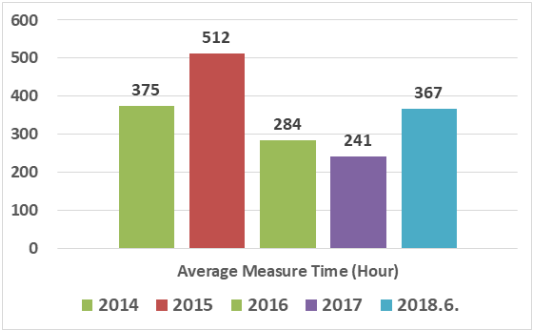

Fig. 6. Landing Site Average Measure Time

악성코드 경유지 사이트 조치 소요시간이 이렇게 길게 나타나는 원인에는 웹사이트를 운영함에 있어 웹사이트 개발자 및 보안 전문가를 보유하고 있지 않거나 웹사이트 운영에 대한 보안인식 부족, 자체적으로 웹 취약점 점검 후 보완조치 시간 등으로 인해 소요시간이 많이 필요로 한 것으로 파악되었다.

3.5 악성코드 경유지 사이트 업종별 분석

2014년부터 2018년 6월까지 탐지된 악성코드 경유지 사이트에 대해 업종별로 분류하였을 때 Fig.7.과 같이 의료 부문이 19%로 가장 높게 나타났으며, 그 이외에도 연구소, 게임웹진 등의 순으로 악성코드 경유지 사이트로 악용된 것으로 확인되었다.

사례기반 악성코드 유포 사이트 특성 분석[8] 논문에서는 2015년 1월 1일부터 2015년 6월 30일까지 탐지된 악성코드 경유지 사이트에 대해 10개의 대분류 업종으로 분류하였으며, 엔터테인먼트 업종이 21.6%로 가장 높게 나타났으며, 교육·연구 부분이 15.8%, 비영리단체 14.6%로 나타난 것으로 제시하고 있다.

본 논문에서는 [8]논문에서 분류한 대분류 10개와는 달리 랭키닷컴 사이트의 카테고리 분류를 기반으로 좀 더 세분화하여 대분류 23개, 중분류 210개, 소분류 1,255개의 업종으로 구분하였으며, 탐지된 악성코드 경유지 사이트에 대해 소분류에 해당하는 업종을 매핑 함으로써, 대분류로만 업종을 분류하였을 때보다 명확히 어떠한 웹사이트들을 대상으로 악성코드 경유지로 악용되고 있는지가 한눈에 파악되었다.

전체 5년간 탐지된 악성코드 경유지 사이트 중 가장 높게 나타난 부문이 피부과(건강/의학) 업종이라는 것은 악성코드 유포로 악용하기 위함과 동시에 의료 관련 개인정보 탈취를 목적으로 공격 타깃이 된 것을 알 수가 있다. 민감한 환자정보와 의료정보가 기록·보관되어 있어, 해킹을 통한 의료정보 탈취는 심각한 사생활 침해까지 발생할 수 있어 높은 보안성이 요구된다.

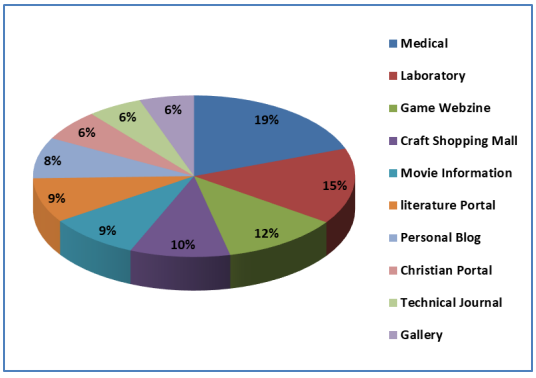

Fig. 7. Landing Site Industrial Classification TOP10

3.6 악성코드 경유지 사이트 요일별 · 시간대별 분석

어느 요일에 가장 많이 익스플로잇 사이트로 연결되어지는 악성코드 경유지 사이트가 탐지되는지 요일별로 분류하였을 때 Fig.8.과 같이 토요일부터 월요일 동안에 탐지가 많이 되었으며, 그중에서도 월요일이 전체 대비 17%로 가장 높게 나타났다. 이는 일반 이용자가 주말에는 개인적 용도로써, 월요일에는 업무적 용도 등으로 웹사이트 접속이 가장 빈번히 발생할 것으로 생각되며, 공격자는 일반 이용자 PC에 대해 악성코드 감염 성공률을 높이기 위한 활동으로 볼 수 있다.

[8]논문에서는 가장 악성코드 경유지 사이트 감염이 가장 높은 요일을 월요일(19.19%), 가장 감염이 적은 요일을 일요일(9.7%)로 제시하여 악성코드 감염은 주말에 더 자주 발생할 것이라는 가설을 기각하고 있으나, 본 논문에서의 요일별 통계의 경우, 일요일의 경우도 평일과 유사하게 높은 비율을 점유하고 있으며, 주말인 토요일과 일요일을 합하였을 경우, 30%에 육박한다. 따라서 사례기반 악성코드 유포 사이트 특성 분석 논문에서 제시한 주말에 악성코드 감염이 자주 발생하지 않는다는 것과는 상반되는 것을 알 수 있다.

Fig.8.에서 본 것처럼 요일별로는 주말과 월요일에 탐지가 많이 되었다면 시간대별로는 Fig.9.와 같이 18시부터 21시 사이에 악성코드 경유지 사이트가 가장 많이 탐지되었다. 즉, 토요일에서 월요일까지

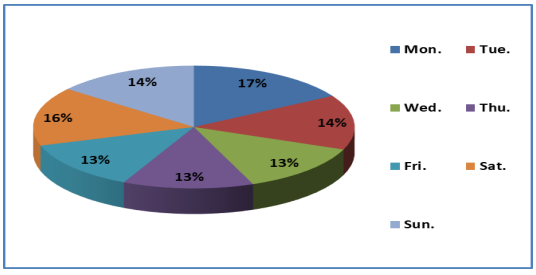

Fig. 8. Landing Site Day Classification

18시부터 21시 사이에 악성코드 경유지 사이트로 악용이 많이 되고 있는 결과가 도출되었다.

〔4〕논문에서는 2016년 6월 1일부터 2016년 9월 30일까지 웹 크롤러 시스템을 통해 데이터를 수집한 결과를 제시하고 있으나, 시간대별로는 상세히 분류되지 않았다.

악성코드 경유지 사이트 탐지가 가장 많은 요일별 통계뿐만 아니라 요일은 상이하지만 동일 시간대에 동일한 웹사이트를 통해 악성코드를 유포하는지 또는 동일 공격자가 동일 시간대에 공격하는지를 알기 위해서는 시간대별 분석이 중요하다고 할 수 있다.

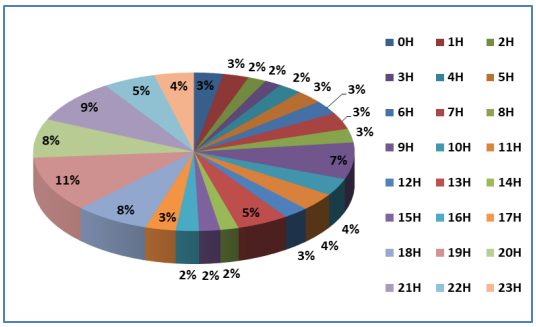

Fig. 9. Landing Site Time Classification

3.7 악성코드 취약점 및 어플리케이션별 취약점 현황

드라이브 바이 다운로드 공격과정 중 악성코드 경유지 사이트내에 삽입된 리다이렉트 코드로 인해 익스플로잇 사이트로 연결되어지게 되는데, 익스플로잇 사이트에서는 일반 이용자 PC를 악성코드에 감염시키기 위한 취약점 공격코드들로 구성되어져 있다.

Fig.10.의 경우, 2014년부터 2018년 6월까지 탐지된 익스플로잇 사이트에 대한 취약점 공격코드들을 분석한 결과, 총 34개의 취약점들이 사용되었음

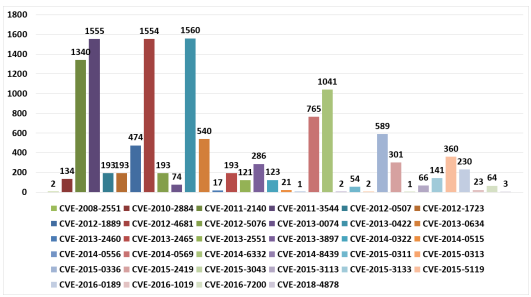

Fig. 10. Exploit Site Vulnerability

을 알 수 있었으며, 이런 취약점들은 단독으로 사용되기 보다는 악성코드 감염 성공률을 높이기 위해 취약점을 복합적으로 사용하였다. Table 1.에서 본 것처럼 악성코드 샘플 1개를 유포하기 위해 익스플로잇 사이트는 평균적으로 4개가 악용되었으며, 34개의 취약점을 복합적으로 사용하여 매년 평균 2,715개의 익스플로잇 사이트를 발생시킨 것으로 확인되었다.

웹 기반 악성코드 유포공격의 특성 분석〔9〕 논문에서는 악용된 취약점 공격코드, 타깃 대상에 대해서만 제시하였으나, 본 논문에서는 익스플로잇 사이트에서 악성코드를 감염시키기 위한 취약점 공격코드들이 얼마나 사용되고 있는지와 2014년부터 2018년까지 계속 악용되고 있는 취약점 공격코드들을 분석하였다.

악성코드 유포에 악용되는 취약점 공격코드는 최신 취약점 CVE-2018-4878(adobe flash player)을 사용하기도 하지만 이전의 취약점도 지속적으로 같이 사용되고 있는 것을 알 수 있다. 특히 2016년 이전의 취약점들 중에서 CVE-2011-2140(adobe flash player), CVE-2011-3544(java), CVE-2012-4681(java), CVE-2013-0422(java), CVE-2014-0569(adobe flash player), CVE-2015-2419(internet explorer), CVE-2015-3133(adobe flash player) 취약점은 현재에도 계속 익스플로잇 사이트에서 악용되고 있다.

Fig.11.은 Fig.10.의 익스플로잇 사이트의 취약점 정보들에 대해 어플리케이션별로 분류한 결과이며, 자바(java) 관련 취약점이 45%로 가장 높게 나타났으며, 그 이외에도 어도비 플래시 플레이어(adobe flash player) 취약점이 33%, 인터넷 익스플로러(internet explorer) 취약점이 9% 순으

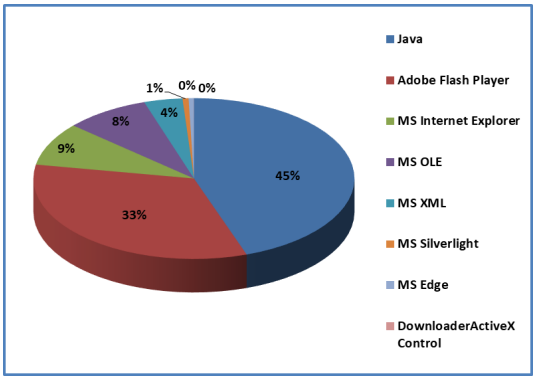

Fig. 11. Exploit Site Application Vulnerability

로 파악되었다.

이처럼 3가지 어플리케이션만 하더라도 전체의 87%에 해당하는 것으로 일반 이용자 PC에서 자바, 어도비 플래시 플레이어, 인터넷 익스플로러에 대한 주기적인 업데이트만 이루어진다면 악성코드에 감염되는 것을 예방할 수 있을 것이다. 어플리케이션에 대한 취약점이 익스플로잇 되지 않는다면 악성코드가 다운로드 및 실행이 되지 않기 때문이다. 업데이트의 중요성이 여기서 나타난다고 볼 수 있다.

3.8 악성코드 유형별 현황

악성코드 유포지 사이트는 드라이브 바이 다운로드 공격의 가장 마지막 단계인 악성코드의 다운로드 및 실행되어 설치되는 단계이다. 악성코드 유형별로 분류하는 가장 큰 목적은 공격자의 최종적인 의도를 파악할 수 있기 때문이다. 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트를 통해 최종적으로 악성코드를 일반 이용자 PC에 설치하게 되고, 설치된 악성코드의 기능에 따라 PC내의 공인인증서 탈취를 위한 목적, 원격제어를 위한 목적, PC내 저장된 게임계정 탈취를 위한 목적 등 다양하게 나타날 수 있다.

Table 1.에서 본 것처럼 2014년부터 2018년 6월까지 탐지된 악성코드 샘플의 수는 총 3,023개이며 이에 대한 악성코드 기능별로 분류한 결과는 아래 Fig.12.와 같다. 금융정보 탈취 악성코드가 55%로 가장 많았으며, 그 이외에도 드롭퍼 7%, 원격제어 7%, 파밍 6% 순으로 나타났다.

이용자 PC내의 공인인증서 탈취 등 금융정보 탈취 악성코드는 2014년부터 매년 지속적으로 유포되어져 왔으며, 전체 대비 비율이 가장 높게 나타난 것

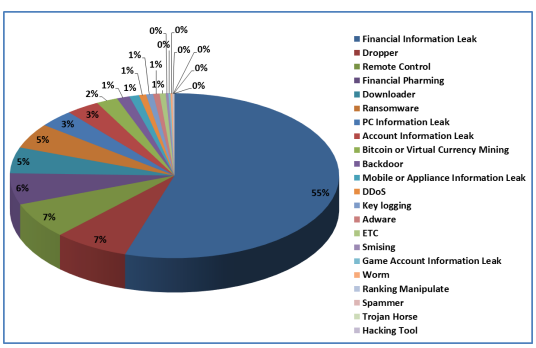

Fig. 12. Malware Type Classification

으로 파악되었다.

2014년에는 이용자가 사용하는 PC에 대한 PC정보나 계정정보를 탈취를 위한 악성코드가 유포되었다. PC정보를 탈취하기 위한 것은 이용자들이 사용하고 있는 PC 환경을 파악하기 위한 것이다. 이용자 PC에 어떠한 어플리케이션이 설치되어져 있는지 파악하여 익스플로잇 사이트에서 악용할 취약점 공격코드를 선별하기 위한 용도와 이용자 PC에 설치된 악성코드가 이용자가 잘 인지하지 못하도록 하거나 백신에 탐지되지 않도록 하기 위해 PC 환경을 파악하여 추후 악성코드를 제작할 때 반영하기 위한 목적으로 볼 수 있다.

또한, 2015년에는 랜섬웨어 악성코드가 처음 유포되었으며, 전체 대비 5%를 차지하고 있다. 2017년부터는 우리나라에 가상통화에 대한 사회적 열풍이 나타남에 따라 2017년과 2018년에 가상통화 채굴 악성코드가 본격적으로 유포되었으며, 전체 대비 2%에 불과하지만 앞으로도 지속적으로 유포될 것으로 예상된다.

이처럼 공격자는 금전적으로 이익이 되거나 사회적으로 이슈가 되는 곳을 타깃으로 하여 악성코드를 제작하여 유포하고 있는 것을 알 수가 있다.

3.9 악성코드 명령제어 서버 네트워크 통신현황

악성코드 유포지 사이트로부터 수집된 악성코드 샘플에 대한 기능별 유형 분류는 Fig.12.에서 살펴보았다. Fig.13.은 Fig.12.의 악성코드 기능이 동작할 때, 외부의 명령제어 서버와의 네트워크 통신이 발생하는 것에 대해 국가별로 분류한 결과를 나타낸 것이다. 악성코드가 외부 도메인 또는 IP에 대해 가장 많이 네트워크 통신이 발생한 국가는 미국으로 60%로 가장 높게 나타났다. 그 이외에도 홍콩 13%, 한국 9%, 중국 7% 순으로 나타났으며, 한국도 명령제어 서버와의 네트워크 통신의 발생이 미국을 제외한다면 높은 비율을 차지하고 있는 것으로 파악되었다.

명령제어 서버와 네트워크 통신을 한다는 것은 공격자가 지속적으로 추가적인 조종을 하기 위한 목적을 가지고 있다는 것을 의미한다. 악성코드 유형으로 보았을 때에는 정보유출 악성코드에 대한 정보 유출지, 원격제어 악성코드, DDoS 악성코드가 여기에 해당한다고 볼 수 있다.

[4]논문에서는 일별 유포되는 악성코드 통계만을

보여주고 있으며, [8]논문에서는 수집된 악성코드 샘플에 대한 유형별 분류 결과만을 제시하고 있어, 악성코드 기능 이외에 상세 분석이 부족한 것으로 나타났다.

악성코드 분석 시 행위에 대한 기능뿐만 아니라 외부 네트워크와의 통신이 발생하는지 유무를 파악함으로써 공격자가 일회성의 악성코드를 유포하기 위한 목적인지 아니면 지속적으로 조종을 하기 위한 목적인지 알 수 가 있다.

Fig.13.에서 명령제어 서버의 네트워크 통신이 한국으로 나타나는 부분에 대해서는 두 가지의 측면으로 생각해 볼 수 있다.

첫째, 공격자가 국내에 있는 서버를 해킹하여 명령 조종지의 서버로 악용하고 있는 경우이다. 공격자의 공격 근원지를 한 번 더 숨김으로써 추적을 회피하기 위한 의도로 볼 수 있다. 즉, 공격자의 공격 근원지를 파악하기 위해서는 명령 조종지로 악용되고 있는 서버를 분석하여 공격자의 침입 흔적을 찾아야만 알 수 있게 되는 것이다.

둘째, 공격자가 직접 국내에 서버를 임차하여 명령 조정지 서버로 활용하고 있는 경우이다. 웹호스팅을 통한 서버 임차 시 서비스 신청 및 결제 절차 과정의 소홀함을 이용하여 쉽게 서비스를 이용하고 있다는 점이다. 따라서 서버 웹호스팅 서비스 신청 과정에 있어 사용자 인증 및 확인절차와 사용 목적을 명확히 확인한 후에 서비스를 제공해 주어야 한다.

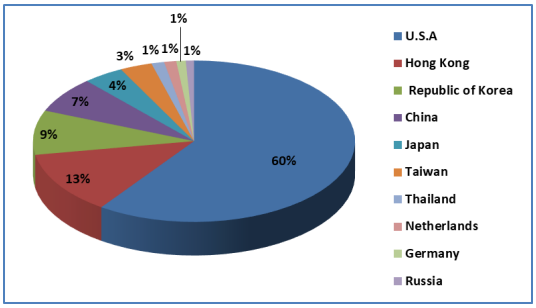

Fig. 13. Malware Network Communication Nation TOP10

IV. 악성코드 유포 사이트에 의한 피해손실 측정

일반 이용자가 악성코드 경유지 사이트를 접속하였을 때, 악성코드에 무조건 감염되는 것은 아니다. 일반 이용자의 PC환경의 취약성 정도에 따라 악성코드 감염여부가 결정되어지기 때문이다. 악성코드 경유지 사이트는 악성코드 유포지까지 연결되어지는 최초 접속 사이트이기 때문에 신속한 탐지와 함께 조치 대응이 필요하다. 그렇다면 악성코드 경유지 사이트를 통해 악성코드를 유포하는 것이 얼마나 많은 피해손실을 발생시키는지 알아보고자 한다.

Table 2. Infected PC Calculation

Year	Landing Site (Domain)	Daily Average Visit site Count	Average Rate of Infection (100,000)	Infected PC Count
2014	9,971	51,780,450	9.2	4,764.80
2015	7,048	39,131,418	9.2	3,600.09
2016	1,987	37,552,192	9.2	3,455.80
2017	2,688	16,572,269	9.2	1,525.65
2018.6.	1,282	1,803,437	9.2	166.92

악성코드 감염률과 악성코드 경유지 사이트에 대한 일평균 접속자수를 산정하기 위해, 마이크로소프트 인텔리전스 보고서와 랭키닷컴 사이트의 일평균 방문자수의 정보를 활용하여 Table 2.와 같이 악성코드 감염 PC 수를 산정하였다. 2017년 1분기 Microsoft Security Intelligence Report(Volume 22)에 따르면, 한국의 악성코드 평균 감염률을 9.2%로 측정하고 있다[10]. 이 수치는 마이크로소프트에서 10만대의 PC를 표본으로 하였을 때의 악성코드 감염 수치이다.

일반 이용자 PC 1대당 손실비용을 산출하기 위해, 2014년 카드3사 정보유출 사건에서는 1인당 10만원 지급[11], 2015년 홈플러스 개인정보 유출 사건에서는 5~20만원 지급[12]을 고려하였을 때, 정보유출 사건에 대한 손해배상 금액 10만원을 적용하여 손실비용을 적용하여 산정하였다. 2014년부터

Table 3. Loss Cost Calculation

Year	Infected PC Count	Loss Cost Per PC	Loss Cost
2014	4,764	100,000	476,380,140
2015	3,600	100,000	360,009,046
2016	3,455	100,000	345,480,166
2017	1,525	100,000	152,464,875
2018.6.	166	100,000	16,591,620
Total			1,350,925,847

2018년 6월까지 손실비용을 산정한 결과, Table 3.에서처럼 총 13억 5천만원의 피해손실 비용이 발생하였다. 이는 악성코드 경유지 사이트에 대한 탐지 및 조치 대응을 함으로써, 13억 5천만원의 피해손실이 발생하는 것을 예방할 수 있음을 알 수 있다.

V. 대응 방안에 대한 고찰

악성코드 유포 사이트로 인한 피해손실이 큰 만큼 악성코드 유포 사이트에 대한 대응이 필요하다. 본 논문에서는 각 구간별 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트로 나누어 앞서 도출한 악성코드 유포현황과 특징을 근거로 대응방안을 고찰하고자 한다.

첫째, 악성코드 경유지 사이트 중 가장 많이 타깃이 되고 있는 의료 부문의 웹사이트에 대해 각별히 신경 써야 한다. 의료 관련 웹사이트의 경우 민감한 환자정보와 의료정보가 기록·보관되어 있어, 해킹을 통한 의료정보 탈취는 인명사고로도 이어질 수 있으며, 심각한 사생활 침해까지 발생할 수 있어 높은 보안성이 요구된다. 의료정보가 중요한 만큼 정보보호 관리체계를 도입 및 운영하기 위한 노력이 필요함에 따라 2016년 6월 2일부터 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의해 세입이 1천500억 이상인 의료법상 상급종합병원은 정보보호관리체계(ISMS) 인증을 받도록 의무화하고 있다. 중소규모의 병원은 고객 정보관리, 영업 및 예약관리 등을 위한 웹사이트를 자체 인력으로 운영하기 어렵다면 클라우드 인프라와 아웃소싱을 활용하여 개발보안을 준수할 수 있도록 하고, 주기적으로 어플리케이션 보안 진단을 받아야 한다. 악성코드 경유지로의 재악용을 예방하기 위해서는 웹사이트 관리자의 정보보호의 중요성을 인식하고 있어야 하며, 악성코드 경유지로 악용되었을 때 얼마나 빠른 시간 내에 침해사실을 인지하고 조치하느냐가 중요하다. 운영하는 웹사이트에 대해 특히 월요일과 18시 이후의 저녁시간에는 외부 침입이나 공격시도에 대해 모니터링이 필요하며, 시스템의 이상 징후에 대해 SMS나 메일 등의 알람 서비스 체계를 갖추어야 한다. 악성코드 경유지에 삽입된 악성 스크립트만을 단순히 삭제하기보다는 웹 취약점을 찾아 패치 및 수정 보완하여야 한다. 앞서 악성코드 경유지 사이트 조치시간 분석에서 악성코드 경유지 사이트를 조치하는데 평균 14일이 소요되는 것으로 나타났다. 14일 동안에는 악성코드를 계속 유포하고 될 수 있기 때문에 조치 소요시간을 단축시키는 방법이 필요하다. 자체적으로 웹사이트 개발자 및 보안 전문가를 보유하고 있다면 조치 대응이 빨리 이루어지겠지만 그렇지 않다면 웹호스팅 업체를 통해 네트워크 회선 및 콘텐츠 저장 공간의 임대뿐만 아니라 웹사이트에 대한 보호 및 대응조치까지 서비스에 포함시켜 위탁 운영을 하도록 하는 것을 권고한다. 또는 한국인터넷진흥원에 웹사이트에 대한 침해사고 사실에 대한 신고접수 후, 침해사고 상세 원인분석을 무료로 기술지원 받는 것도 한 가지 방법이다.

둘째, 익스플로잇 사이트의 경우, 공격자는 웹 익스플로잇툴킷을 사용하여 취약점 공격코드를 파일로 생성하여 익스플로잇 사이트의 웹서버에 업로드 하므로, 웹사이트 관리자는 운영하는 웹서버 내의 디렉토리 또는 파일이 신규로 추가 생성 되었는지 확인해보는 것이 중요하다. 그러므로 해킹되기 이전에 정상적으로 운영 중인 웹서버의 디렉토리 및 파일에 대해 해시(Hash)값을 추출하여 주기적으로 1시간 또는 1일 단위로 비교 검증함으로써 위변조 유무를 확인하는 방법을 제안한다.

셋째, 악성코드 유포지 사이트의 경우, 악성코드 경유지 사이트나 익스플로잇 사이트와는 달리 최종적인 악성코드 샘플을 다운로드 하기 위한 사이트로 악용되는 곳이다. 따라서, 웹서버 내에 서버 사이드의 언어 파일이 아닌 이용자 PC에서 실행 가능한 PE(Portable Executable) 파일이 존재하는지를 점검해 보면 된다. PE 파일에는 실행계열(EXE, SCR), 라이브러리 계열(DLL, OCX, CPL, DRV), 드라이버 계열(SYS, VXD)이 있으며, 여기에 해당하는 확장자 파일이 웹서버 내에 존재하는지를 자동화된 스크립트를 작성하여 주기적으로 1시간 또는 1일 단위로 점검하는 방법을 제안한다.

그 이외에도 웹사이트 운영에 있어 일반적인 보안관리 사항으로는 불필요하거나 미사용 계정에 대한 파악, 주기적인 계정 패스워드 변경, 개발자 PC와 웹사이트 운영 서버와의 분리, 서버 접근권한 설정, 서버의 불필요한 서비스 제거, 서버의 자격증명 기억 금지, 서버의 자원파악, 네트워크 공유 금지, 내부 접근 접점 유무 파악 등의 보안 관리가 필요하다.

일반 이용자들에 대한 예방수칙은 바이러스 백신의 설치 및 최신 버전 업데이트, 설치된 어플리케이션에 대한 최신 버전 업데이트, PC 내부에 중요한 금융정보 파일, 문서 파일, 계정정보 파일 등은 저장하지 않는 것을 권장하며, 저장을 해야 한다면 암호

를 걸어두고, 다른 저장매체에 백업해 두어야 한다.

VI. 결 론

본 연구에서는 국내 343만개 웹사이트를 대상으로 정적 분석 및 동적 분석을 통해 2014년 1월부터 2018년 6월까지 탐지된 결과를 기반으로 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트로 구분하여 각 구간별로 어떤 현황이 나타나는지 분석해 보았다. 악성코드 경유지 사이트에서는 탐지된 경유지 사이트 도메인에 대해 평균 17.3%가 재악용 되고 있었으며, 탐지 이후에 조치하는데 까지 356시간(14일)이 소요되었다. 공격자로부터 가장 많이 타깃이 된 업종은 피부과(건강/의학) 부문으로 19%로 파악되었다. 일주일 중 월요일이 감염이 높은 요일이었으며, 시간대로는 18시~21시경이 가장 위험한 시간대로 분석되었다.

익스플로잇 사이트에서는 2014년 1월부터 2018년 6월까지 총 34개의 취약점 공격코드가 사용되었다. 매년 평균 2,715개의 익스플로잇 사이트가 발생되는 것으로 파악되었으며, 악성코드 샘플 1개를 유포하기 위해 익스플로잇 사이트는 평균 4개가 사용되는 것으로 나타났다. 또한, 취약점 공격 코드에 대해 어플리케이션별로 분류한 결과 자바(java) 관련 취약점이 45%로 가장 많이 악용되었다.

악성코드 유포지 사이트에서 악성코드 유형으로 금융정보 탈취 악성코드가 55%로 가장 많았으며, 그 이외에도 드롭퍼 7%, 원격제어 7%, 파밍 6% 순으로 나타났다. 악성코드 기능이 동작할 때 미국이외부의 명령제어 서버와의 네트워크 통신이 가장 빈번히 발생하는 것으로 확인되었다.

악성코드 경유지 사이트는 악성코드 유포에 최초로 이용자가 접속되는 구간이기 때문에 악성코드 경유지 사이트에 대한 탐지 및 조치 대응이 중요하다고 할 수 있다. 따라서 2014년 1월부터 2018년 6월까지 악성코드 경유지 사이트에 대한 손실비용을 산정한 결과 총 13억 5천만원의 피해손실 비용이 발생한 것을 파악할 수 있었다.

현재에도 드라이브 바이 다운로드 기반의 웹사이트 악성코드 유포는 계속 되고 있으며, 신규 취약점을 악용하거나 신규 및 변종의 악성코드가 유포됨에 따라 이를 탐지하고 모니터링 하는 기술에 대한 연구가 꾸준히 진행되어야 할 것이다.

본 논문에서는 국내 343만개 웹사이트의 도메인에 대해 이름순으로 순차대로 점검을 하였지만, 향후에는 머신러닝 기술을 도입하여 악성코드 경유지 사이트, 익스플로잇 사이트, 악성코드 유포지 사이트에 대해 기존에 탐지된 이력이 있거나 신규 생성된 도메인 및 악성으로 의심되는 도메인에 대해 점검 우선순위를 자동 조정하여 모니터링 하는 방안을 지속적으로 연구할 예정이다.

References

[1] Korea Internet & Security Agency, "Internet Statistics Information System," https://isis.kisa.or.kr/statistics/?pageId=020201

[2] Korea Internet & Security Agency, "2018 Malicious Site Detect Trend Report," https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=27428&queryString=cGFnZT0xJnNvcnRfY29kZT0mc2VhcmNoX3NvcnQ9dGl0bGVfbmFtZSZzZWFyY2hfd29yZD0=

[3] Korea Internet & Security Agency, "WannaCry Analysis Special Report," https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=26747

[4] Yoo Donghyun, "Web Crawler Design for Collection of Malwares Distributed for Drive by download Attacks," Master's thesis, Soonchunhyang University, 2017

[5] Byung-Ik Kim and Joo-Hyung Oh and Chae-tae Im and Hyun-Chul Jung, "Suspicious Malicious We Site Detection with Strength Analysis of a Javascript Obfuscation," KR Patent, KR101060639B1, 2011

[6] Korea Internet & Security Agency, "Study on Spreading Pattern Analysis Method of Malicious code Hidden in Hongpage," KISA-WP-2010-0037, 2010

[7] Han Young-Il and Lee Tae-Jin and Park Hea-Ryong, "Structural and characteristic analysis of malware network," Proceedings of Symposium

of the Korean Institute of communications and Information Sciences, pp. 1000-1002, 2014
〔8〕 Noh MyoungSun, "A Case-based Characterization of Malware Spreading Sites", Doctor's thesis,Chonnam National University, 2016
〔9〕 Yu Dae-Hun and Kim. Ji-Sang and Jo. Hye-Seon and Park. Hae-Ryong, "Characteristics Analysis of Malicious Code spread attack based on Web," The Journal of The Korean Institute of Communication Sciences, 31(5), pp. 15-19, 2014
〔10〕 Microsoft, "Microsoft Security Intelligence Report," http://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf
〔11〕 News1Korea, "Last judgment of personal information leakage case by credit card 3 company 100 thousand won in total per person," http://news1.kr/articles/?2731638
〔12〕 Chosunbiz, "law, Homeplus, and personal information leakage customers," http://news.chosun.com/site/data/html_dir/2018/01/18/2018011801507.html

〈저자소개〉

김 홍 석 (Hong-seok Kim) 정회원
2009년: 영남대학교 컴퓨터공학과 학사
2010년~현재: 한국인터넷진흥원 선임연구원
2017년~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 악성코드 분석, 침해사고대응

김 인 석 (In-seok Kim) 정회원
1973년: 홍익대학교 전자계산학과(학사)
2003년: 동국대학교 국제정보대학원(석사)
2008년: 고려대학교 정보경영공학전문대학원(박사)
2009년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT 감사, 전자금융법규