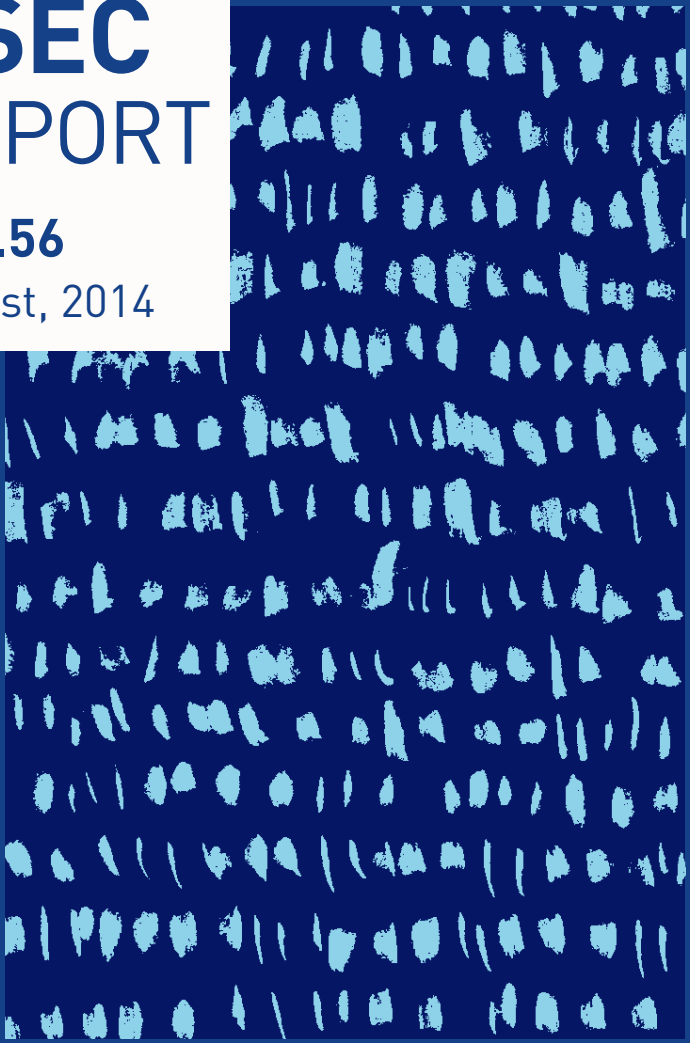
Security Trend

ASEC REPORT

VOL.56

August, 2014



AhnLab

ASEC REPORT

VOL.56 August, 2014

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2014년 8월 보안 동향

Table of Contents

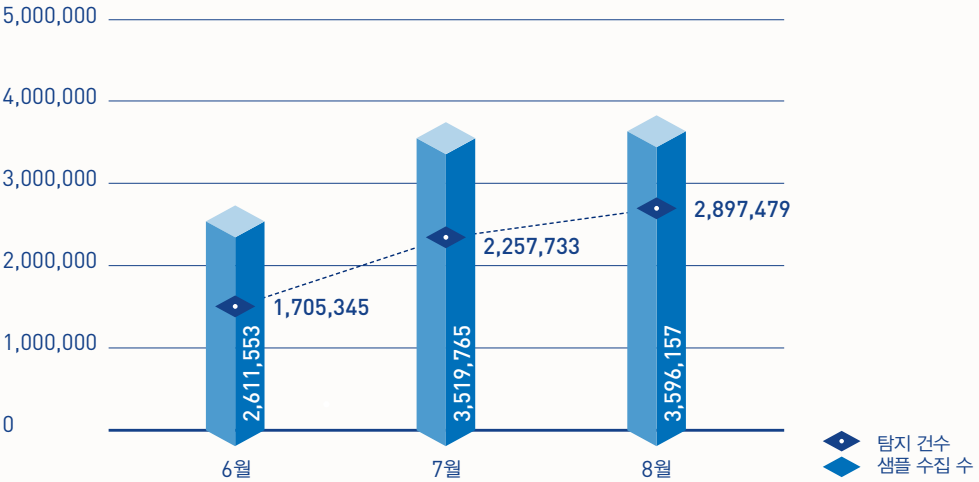
1

보안 통계
STATISTICS

01
악성코드 통계

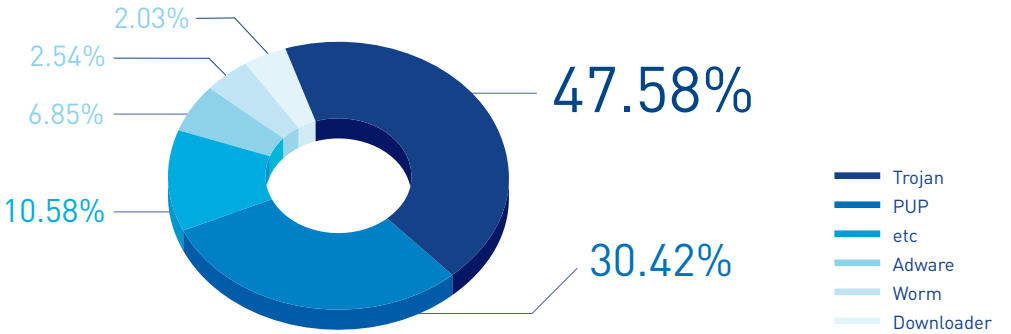
ASEC이 집계한 바에 따르면, 2014년 8월 한달 간 탐지된 악성코드 수는 289만 7,479건으로 나타났다. 이는 전월 225만 7,733건에 비해 63만 9,746건 증가한 수치다. 한편 8월에 수집된 악성코드 샘플 수는 359만 6,157건으로 집계됐다.

[그림 1-1]에서 '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드 샘플 수를 의미한다.



[그림 1-1] 악성코드 추이

[그림 1-2]는 2014년 8월 한달 간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 47.58%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 30.42%, 애드웨어(Adware)가 6.85%로 그 뒤를 이었다.



[그림 1-2] 주요 악성코드 유형

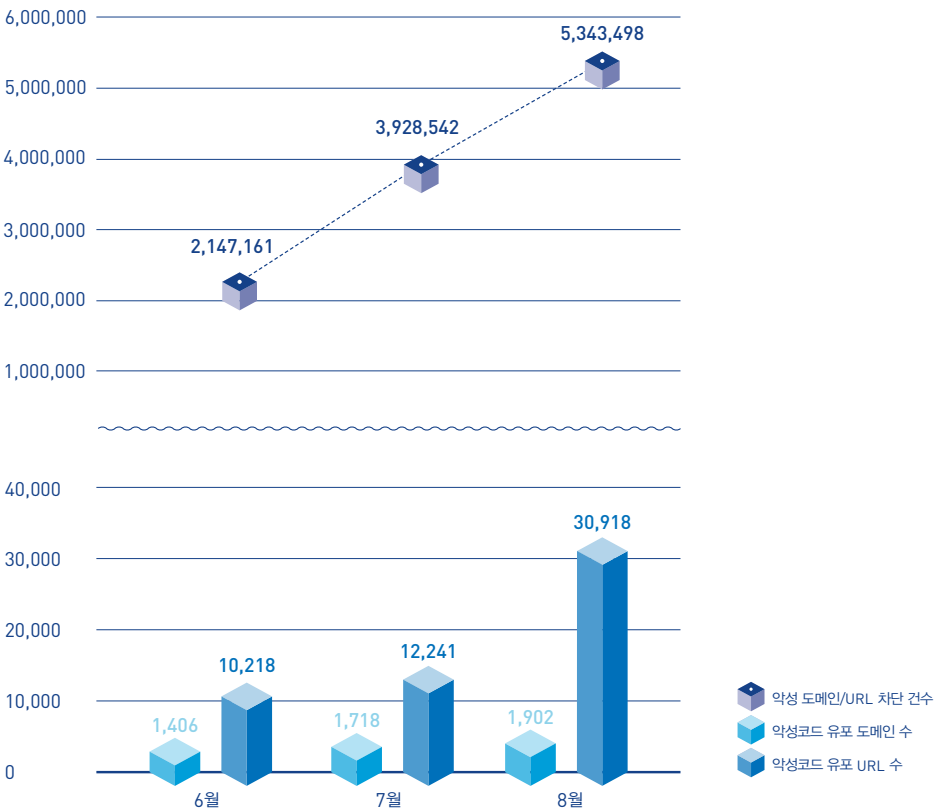
[표 1-1]은 8월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.ADH가 총 14만 5,727건으로 가장 많이 탐지되었고, Trojan/Win32.OnlineGameHack이 11만 6,110건으로 그 뒤를 이었다.

[표 1-1] 악성코드 탐지 최다 10건 (진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.ADH	145,727
2	Malware/Win32.OnlineGameHack	116,110
3	Adware/Win32.SwiftBrowse	108,520
4	Adware/Win32.SearchSuite	106,428
5	Trojan/Win32.Gen	100,588
6	Trojan/Win32.Agent	84,520
7	ASD.Prevention	76,275
8	PUP/Win32.IntClient	69,847
9	Trojan/Win32.Generic	61,433
10	Trojan/Win32. Agent	60,958

02
웹 통계

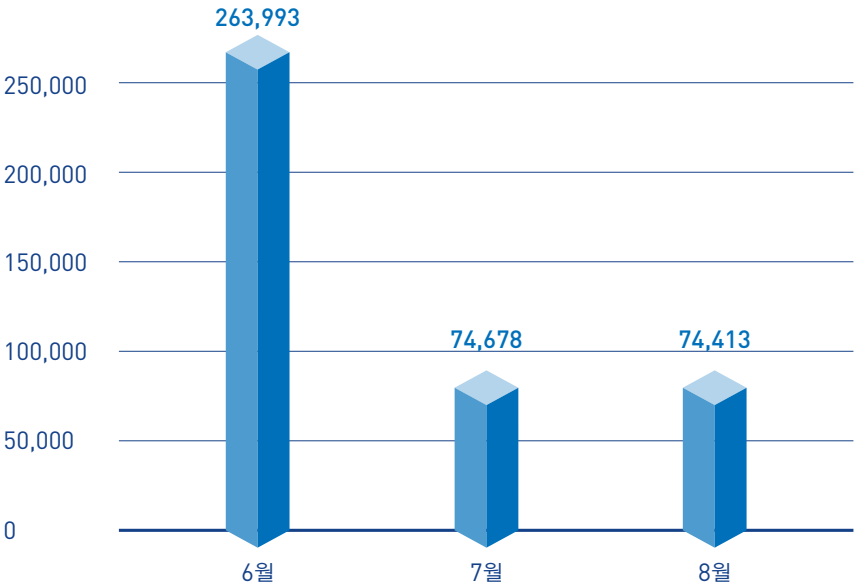
2014년 8월 악성코드 유포지로 악용된 도메인은 1,902개, URL은 3만 918개로 집계됐다. 또한 8월의 악성 도메인 및 URL 차단 건수는 총 534만 3,498건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.



[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수

03
모바일 통계

2014년 8월 한달 간 탐지된 모바일 악성코드는 7만 4,413건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 8월 한달 간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. 안드로이드 애플리케이션에 번들로 설치되어 광고를 노출하는 Android/PUP/Dowgin이 가장 많이 탐지되었다.

[표 1-2] 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/Dowgin	17,160
2	Android-Trojan/FakeInst	15,253
3	Android-Trojan/Opfake	3,889
4	Android-PUP /SMSReg	3,419
5	Android-PUP/ Wapsx	2,408
6	Android-Trojan/ SMSAgent	1,875
7	Android-PUP/ Youmi	1,783
8	Android-Trojan/SMSSend	1,694
9	Android-Trojan/Mseg	1,175
10	Android-PUP/SMSPay	1,078

2

보안 이슈
SECURITY ISSUE

01 사용자 PC 정보를 통계 사이트로 전송하는 악성코드

요즘 개인 정보 유출과 관련된 사건 사고가 증가하고 있는 가운데 개인의 PC 정보를 노린 악성코드가 발견돼 주의가 요구된다. 해당 악성코드는 사용자의 PC 정보를 수집하여 통계 사이트로 전송하고 백신을 무력화시킨다. 통계 사이트로 전송한 정보는 [그림 2-1]과 같이 감염된 PC의 IP 주소와 국적, 감염 일자, 운영체제, 보안 소프트웨어 상태 등이다.

그림 2-1 | 감염 PC 통계 사이트

악성코드가 실행되면 [표 2-1]과 같이 파일이 생성된다.

표 2-1 | 파일 생성 정보

C:₩WINDOWS₩system32₩6to432.dll
C:₩WINDOWS₩system32₩102A[3~4자리 숫자 + 1자리 영문자].tmp
C:₩WINDOWS₩system32₩102B[3~4자리 숫자 + 1자리 영문자].tmp
C:₩WINDOWS₩system32₩6to432
C:₩WINDOWS₩system32₩Vag.tbl
C:₩WINDOWS₩system32₩apci.sep
C:₩WINDOWS₩system32₩ias₩sysprtj.prd

그리고 [표 2-1]에서 생성된 6to432.dll과 Vag.tbl 파일을 서비스에 등록한다.

표 2-2 | 레지스트리 생성 정보

HKLM₩SYSTEM₩ControlSet001₩Services₩6to4₩ImagePath
"%SystemRoot%₩System32₩svchost.exe -k netsvcs"

HKLM₩SYSTEM₩ControlSet001₩Services₩6to4₩Start
0x2 – Auto Load

HKLM₩SYSTEM₩ControlSet001₩Services₩6to4₩Parameters
₩ServiceDll
"C:₩WINDOWS₩system32₩6to432.dll"

HKLM₩SYSTEM₩ControlSet001₩Services₩6to4₩Start
0x2

HKLM₩SYSTEM₩ControlSet001₩Services₩net81390₩ImagePath
"₩??₩C:₩WINDOWS₩system32₩Vag.tbl"

HKLM₩SYSTEM₩ControlSet001₩Services₩net81390₩Start
0x2

dll 파일은 프로세스에 로드되어 실행된다. [그림 2-2]와 같이 svchost.exe에 로드되었음을 확인할 수 있다. 로드된 dll 파일은 특정 사이트에 접근하여 파일을 생성한다.

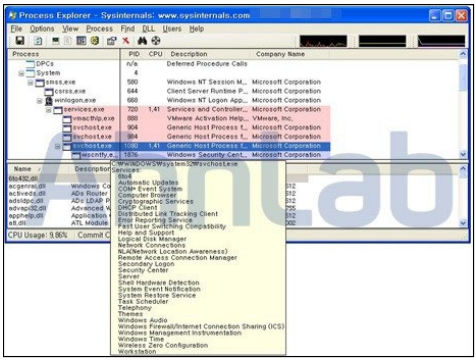


그림 2-2 | svchost.exe에 로드된 6to432.dll 파일

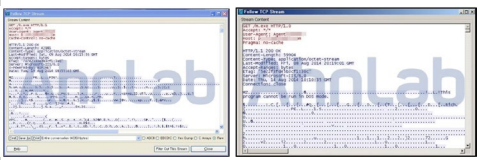


그림 2-3 | 특정 사이트에서 다운로드한 파일_ b.exe(좌)와 m.exe(우)

[그림 2-3]과 같이 m.exe와 b.exe 파일을 다운로드할 때 tmp 파일이 생성된다. 생성된 파일은 [그림 2-4] ①, ②와 같다.

그림 2-4 | 특정 사이트에서 받은 파일_b.exe(좌)와 102A.tmp 파일(우) - ①

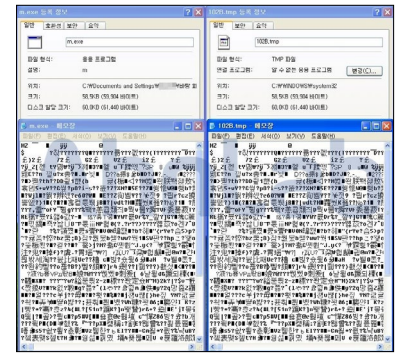


그림 2-4 | 특정 사이트에서 받은 파일_m.exe(좌)와 102B.tmp 파일(우) - ②

102B.tmp 파일은 [그림 2-5]와 같이 사용자의 PC 정보를 탈취하는 파일(Vag.tbl)을 생성한다.

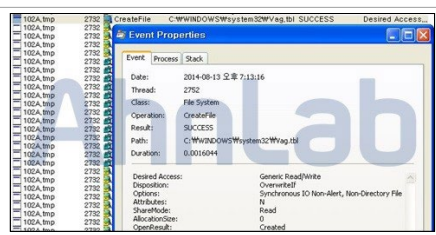


그림 2-5 | 사용자의 PC 정보를 탈취하는 파일 생성

생성된 Vag.tbl 파일의 확장자는 tbl이지만, PE(Portable Executable) 헤더를 확인하면 시스템 드라이버 파일이다. 옵셔널 헤더(Optional Header)의 서브시스템(Subsystem) 값을 통해 파일의 종류(드라이버 파일 / GUI 파일 / CUI 파일)를 확인할 수 있다.

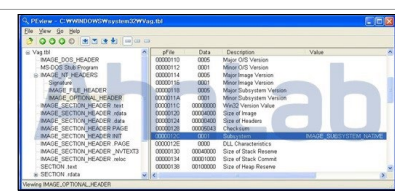


그림 2-6 | Vag.tbl의 파일 종류

Vag.tbl 파일은 서비스에 등록 및 실행되면서 [그림 2-7]과 같이 감염된 PC의 정보를 후킹(hooking)한다. 후킹은 일반적으로 운영체제나 응용 소프트웨어 등의 각종 PC 프로그램에서 소프트웨어 구성 요소 간에 발생하는 함수 호출, 메시지, 이벤트 등을 중간에 바꾸거나 가로채는 명령, 방법, 기술이나 행위를 뜻한다. 공격 대상의 PC 메모리 정보, 키보드 입력 정보 등의 유출 시에도 사용된다.

그림 2-7 | 후킹되는 모습

그림 2-8 | 수집된 정보를 전송하는 과정

유출된 감염 PC의 정보는 [그림 2-8]과 같이 UDP(User Datagram Protocol)를 통해 통계 사이트로 전송된다. 이러한 정보는 추후 악성코드 배포에 악용될 가능성이 높아 주의가 필요하다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.OnlineGameHack (2014.08.12.00)

Backdoor/Win32.Trojan (2014.08.14.00)

Trojan/Win32.Hooker (2014.08.02.01)

Trojan/Win32.Agent (2014.08.13.00)

02 정상 시스템 파일을 변조하는 온라인게임핵

온라인게임핵(OnlineGameHack) 악성코드는 온라인게임 계정을 탈취하여 금전 취득을 목적으로 제작된다. 이 때문에 대부분의 온라인게임 업체는 계정 탈취를 막기 위해 게임 실행 시 별도의 보안 모듈이나 백신으로 보안 사고를 방지한다. 이러한 보안 기술을 회피하기 위해 악성코드 제작자들은 특정 서비스의 로드나 백신의 동작을 방해한다. 이번에 발견된 악성코드도 백신의 동작을 방해하고 윈도 정상 시스템 파일을 변조하여 정상 파일로 위장하였다.

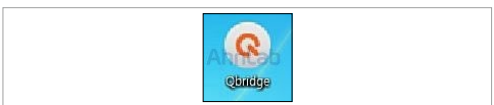


그림 2-9 | 악성코드 아이콘

해당 악성코드를 실행하면 온라인게임 계정을 탈취하는 악성코드와 백신의 동작을 방해하는 악성코드가 생성된다([그림 2-10]).

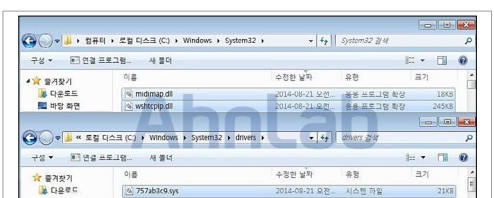


그림 2-10 | 생성된 악성코드

[그림 2-11]과 같이 C:₩Windows₩System32₩drivers 경로에 생성된 [랜덤문자열].sys는 레지스트리에 등록되어 부팅 시 서비스로 자동 실행된다. 이때 드라이버 로드를 방해하여 백신이 정상적으로 동작하지 못하게 한다.

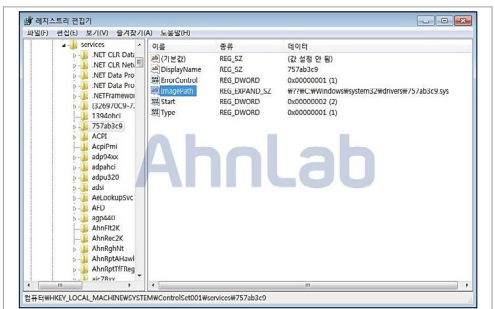


그림 2-11 | 서비스에 등록된 악성코드

해당 악성 파일이 실행되면 서비스 로드를 방해하여 백신이 원활하게 동작하지 않는다. 따라서 백신을 정상적으로 실행시키려면 해당 파일을 직접 삭제하거나 전용 백신으로 치료해야 한다.

악성코드에 의해 생성된 wshtcpip.dll은 윈도 정상 시스템 파일로 보이지만, 정상 파일을 패치(patch)한 악성 파일이다. 파일의 속성 정보를 보면 두 파일

이 다르다. 해당 악성 파일은 정상 프로세스에 로드되어 [그림 2-12]와 같이 온라인게임의 계정 탈취를 시도한다.

그림 2-12 | 계정이 유출된 온라인게임

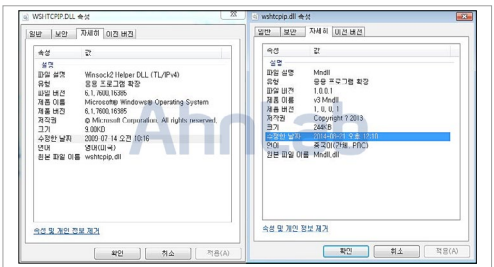


그림 2-13 | 정상 wshtcpip.dll(좌), 변조된 wshtcpip.dll(우)

해당 파일은 윈도 시스템 파일로, 삭제하면 인터넷을 사용할 수 없거나 블루스크린(BSOD) 현상이 나타날 수 있다. Qbridge.exe 파일은 wshtcpip.dll 파일을 변조시키기 위해 해당 파일을 C:₩Windows₩System32 경로에 ws2tcpip.dll이라는 이름으로 복사한다. 그리고 ws2tcpip.dll 파일을 이용하여 정상 파일을 패치한 악성 파일(wshtcpip.dll)을 생성한다. 패치된 악성 파일은 정상 파일의 기능을 그대로 복사하여 시스템 파일의 변조로 인한 오류가 발생하지 않도록 하였다.([그림 2-14]).

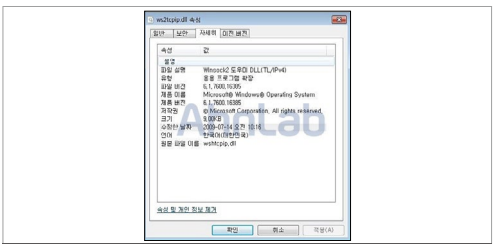


그림 2-14 | 변경된 이름으로 저장된 정상 wshtcpip.dll 파일

해당 악성코드는 안랩에서 제공하는 온라인게임핵 전용 백신으로 변종에 대한 치료도 가능하다.

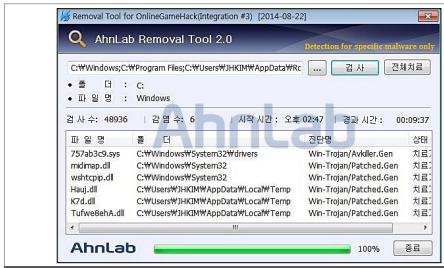


그림 2-15 | 온라인게임핵 전용 백신 실행 화면

전용 백신을 사용할 수 없을 경우 해당 악성코드를 정상 파일로 바꿔주면 치료할 수 있다. C:₩Windows₩winsxs 폴더는 애플리케이션이 필요한 dll 파일의 상세 정보를 별도의 파일로 보관한 후 필요할 때 해당 dll 파일을 선택하여 사용할 수 있는 용도로 쓰인다.

같은 dll 파일이라도 여러 버전이 있다. 프로그램마다 요구 버전이 달라 호환성 유지를 위해 각 버전 별 dll 파일을 C:\Windows\winsxs 폴더에 보관하고 있다. 파일을 수동으로 관리하려면 winsxs 폴더에서 정상 wshtcpip.dll 파일과 midmap.dll 파일을 복사하여 기존 경로(C:₩Windows₩System32)에 복사해주면 된다.

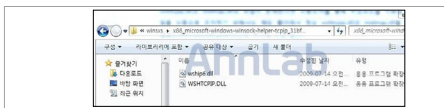


그림 2-16 | winsxs 폴더에 위치한 wshtcpip.dll 파일

온라인게임의 계정 유출은 금전적인 피해로 이어질 수 있어 사용자들의 각별한 주의가 필요하다. 백신을 포함한 응용프로그램을 항상 최신 버전으로 유지하

여 언제 어떻게 일어날지 모르는 보안 위협에 대비해야 한다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Win-Trojan/Onlinegamehack (2014.08.20.00)

Win-Trojan/Onlinegames (2014.08.20.00)

Win-Trojan/Onlinegamehack (2014.08.22.00)

Trojan/Win32.Agent (2014.08.17.00)

3

악성코드 상세분석
ANALYSIS-IN-DEPTH

01 프로그램(PUP) 변조를 통한 악성코드 유포

공격자의 목적은 특정 시스템을 악성코드에 감염시켜 원하는 정보를 탈취하는 것이다. 이때 중요한 것은 "감염 대상 시스템의 사용자가 인지할 수 없도록 악성코드를 감염시킬 수 있는가?"이다. 이를 위해 공격자가 사용할 수 있는 방법은 현재 악성코드의 유포 패턴을 볼 때 [표 3-1]과 같이 정리할 수 있다.

표 3-1 | 악성코드 유포 패턴

1. 해킹된 웹 사이트 + IE, 플래시 플레이어, 자바의 취약점 결함
2. 이메일과 문서 프로그램(MS 오피스, 한글, PDF)의 취약점 결함
3. 정상 응용 프로그램 변조

이번에 살펴볼 사례는 [표 3-1]의 3번으로, "정상적으로 사용하는 응용 프로그램 변조"이다. 분석한 프로그램은 PUP이다.

PUP(Potentially Unwanted Program)란?
공개용 프로그램의 번들이나 블로그, 카페 등을 통해 정상 프로그램처럼 위장하여 배포된다. 하지만 막상 사용자가 무의식적으로 동의를 클릭하면 해당 프로그램 설치 과정에서 광고 프로그램 등이 함께 설치된다. 사용자의 의도와 다르게 주기적으로 광고를 출력하는 등의 불편을 일으키는 프로그램이다.

PUP 업데이트 서버는 외부 공격을 받아 PUP 업데이트 파일은 악성코드로 변조되었고 사용자의 PC에 이미 설치된 PUP는 업데이트 서버로부터 업데이트 파일을 다운로드한 후 실행된다. 이때 다운로드한 파일은 악성코드로 변조되어 사용자의 PC는 악성코드에 감염된다.

위와 같은 방법은 오래 전부터 사용되어 왔다. 지난해 한창 이슈가 되었던 금융권을 대상으로 한 메모리 해킹 악성코드는 변조된 PUP로 사용자의 PC를 감염시키고 금융 정보를 유출하여 금전적인 피해를 일으켰다. 이는 사용자들이 다양한 경로를 통해 프로그램을 다운로드하고 설치하는 과정에서 설치 약관 등을 꼼꼼하게 읽지 않아서이다. 이로 인해 다수의 PUP가 설치되고 설치된 PUP는 자신의 업데이트 서버로부터 업데이트를 다운로드하고 설치하는 과정에서 악성코드에 감염된다.

이번 사례 역시 위에서 언급한 내용과 동일하다. 상당수의 고객이 동일한 악성코드에 감염되었고 수집된 정보를 분석하는 과정에서 해당 PC에 동일한 PUP가 설치되어 실행 중임이 발견되었다.

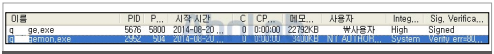


그림 3-1 | 실행 중인 PUP 프로세스

q****ge.exe 파일이 실행되면 [그림 3-2]와 같이 주기적으로 업데이트 서버와 통신하여 버전 정보를 획득한다. 이후 사용자의 PC에 설치된 PUP의 버전보다 상위 버전일 경우 다운로드받도록 되어 있다.

그림 3-2 | 업데이트 서버와 통신 기록

이때 사용자의 PC에 다운로드된 버전의 PUP에 악성코드가 포함되어 있다. 악성코드가 포함된 PUP는 PUP + 악성코드가 하나의 파일에 묶여 있는 구조이다([그림 3-3]).

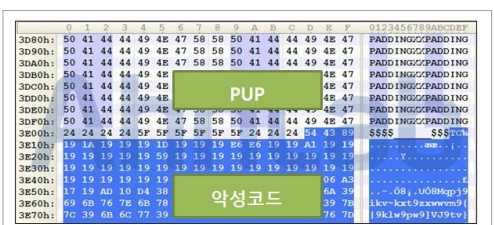


그림 3-3 | 묶여있는 PUP 파일과 악성코드 파일

[그림 3-3]은 "PUP"와 "악성코드"로 표시된 영역이다. 악성코드 영역은 암호화되어 있다. 암호화된 영역은 [그림 3-4]와 같이 복호화 코드를 통해 실행 가능한 파일로 변환된다. 당시 유포되었던 q****ge.exe 파일을 실행하면 복호화를 거친 후 %TEMP%에 악성코드를 생성하고 실행한다.

그림 3-4 | 복호화 코드 부분

[그림 3-5]와 같이 %TEMP%에 생성된 악성코드는 자신의 감염, 유포 경로 등을 추적할 수 없도록 인터넷 접속 기록, 레지스트리 흔적 등을 삭제한다.

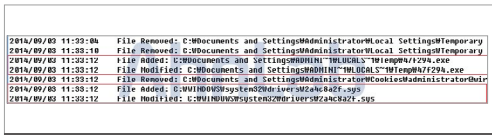


그림 3-5 | 삭제된 기록 정보

[그림 3-6]과 같이 악성코드 실행 시 자신의 흔적을 지우는 기능 때문에 악성코드 파일의 다운로드 기록을 수집하기 어렵다.

그림 3-6 | 다운로드 기록을 삭제하는 부분

[그림 3-7]은 %TEMP%에 생성된 악성코드가 실행되면서 생성한 또 다른 악성코드 내에 있는 문자열이다. 지난해 이슈가 되었던 메모리 해킹은 특정 은행의 인터넷 뱅킹 접속 시 사용자의 금융 정보를 탈취하기 위해 사용한 자바스크립트 패턴과 유사하다. 지난해에는 동일한 기능을 가진 악성코드의 목적은 사용자의 금융 정보 탈취였다. 그러나 은행권에서 보안을 강화하면서 사용자의 금융 정보 탈취가 어려워지자 유사한 기능을 이용하여 특정 온라인게임 사용자의 계정 정보 추출을 시도한 것으로 보인다.

그림 3-7 | 계정 정보를 추출하는 자바스크립트 정보

[그림 3-8]과 같이 인터넷 익스플로러가 실행될 때마다 특정 사이트로 접속하여 변종 악성코드를 다운로드하도록 시도한다.

그림 3-8 | 변종 악성코드 다운로드

표 3-2 | 네트워크 연결 정보

c****t.q*****e.c*.*r : 2**.1*1.3.*6
n**.ou***b.c*m : 2**.1**.2*.1*0

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Agent (2014.08.17.00)

Trojan/Win32.Banki (2014.08.18.03)

AhnLab

ASEC REPORT

VOL.56
August, 2014

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 UX디자인팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000
F. 031-722-8901