Security Trend

ASEC REPORT

VOL.63

March, 2015

AhnLab

ASEC REPORT

VOL.63 March, 2015

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.

2015년 3월 보안 동향

Table of Contents

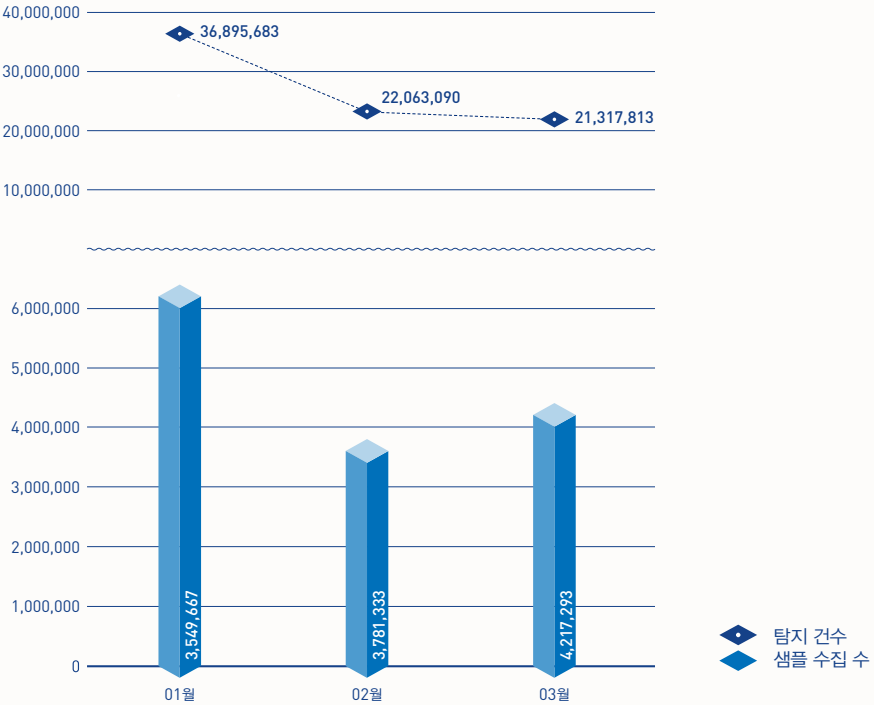
1

보안 통계
STATISTICS

01
악성코드 통계

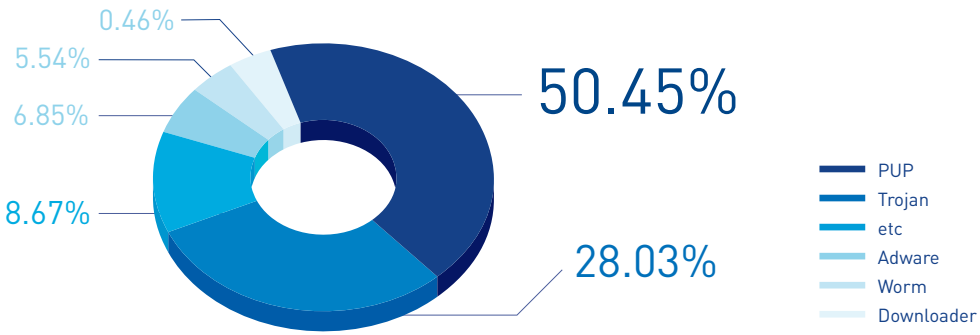
ASEC이 집계한 바에 따르면 2015년 3월 한 달간 탐지된 악성코드 수는 2,131만 7,813건이다. 이는 전월 2,206만 3,090건에 비해 74만 5,277건 감소한 수치다. 한편 3월에 수집된 악성코드 샘플 수는 421만 7,293건이다.

[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 악성코드의 샘플 수를 의미한다.



[그림 1-1] 악성코드 추이(2015년 1월 ~ 2015년 3월)

[그림 1-2]는 2015년 3월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 50.45%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 28.03%, 애드웨어(Adware)가 6.85%로 그 뒤를 이었다.



[그림 1-2] 2015년 3월 주요 악성코드 유형

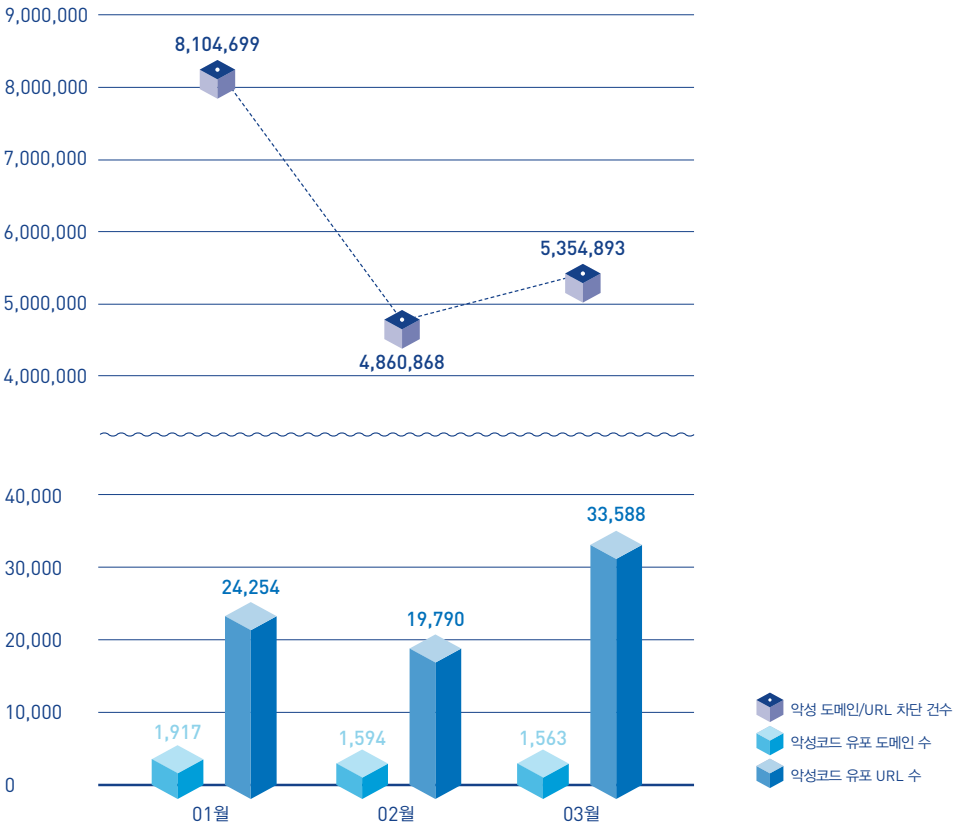
[표 1-1]은 3월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.MyWebSearch가 총 208만 6,933건으로 가장 많이 탐지되었고, PUP/Win32. MicroLab이 163만 2,730건으로 그 뒤를 이었다.

[표 1-1] 2015년 3월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	PUP/Win32.MyWebSearch	2,086,933
2	PUP/Win32.MicroLab	1,632,730
3	PUP/Win32.BrowseFox	1,423,302
4	PUP/Win32.Helper	896,322
5	PUP/Win32.Enumerate	772,126
6	PUP/Win32.SubShop	541,662
7	PUP/Win32.IntClient	516,121
8	PUP/Win32.Generic	514,346
9	PUP/Win32.Gen	405,807
10	PUP/Win32.CloverPlus	398,999

02
웹 통계

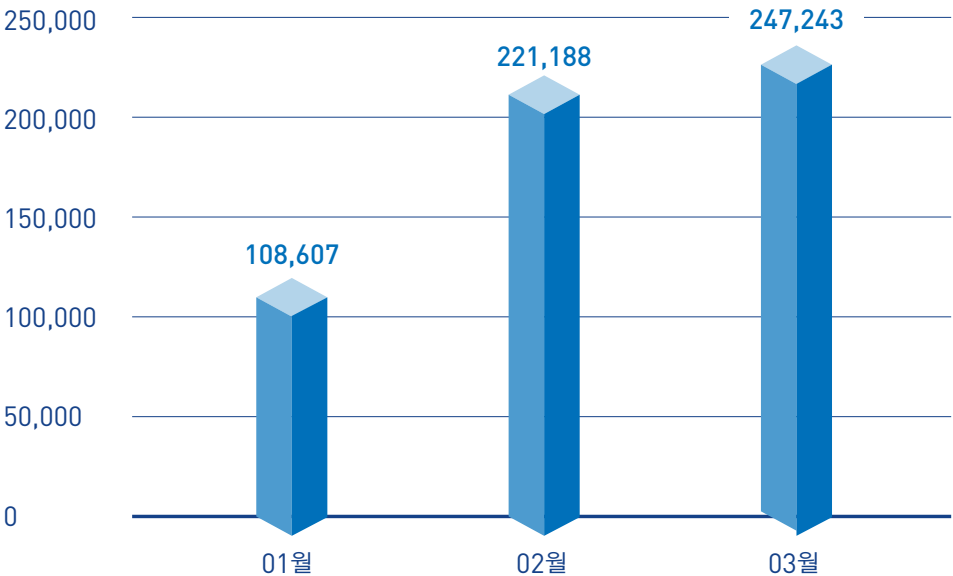
2015년 3월 악성코드 유포지로 악용된 도메인은 1,563개, URL은 3만 3,588개로 집계됐다. 또한 3월의 악성 도메인 및 URL 차단 건수는 총 535만 4,893건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트의 접속을 차단한 수이다.



[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 1월 ~ 2015년 3월)

03
모바일 통계

2015년 3월 한 달간 탐지된 모바일 악성코드는 24만 7,243건으로 집계됐다.



[그림 1-4] 모바일 악성코드 추이(2015년 1월 ~ 2015년 3월)

[표 1-2]는 3월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsReg가 지난 2월보다 3만 2,346건 증가한 15만 2,962건으로 집계됐다.

[표 1-2] 2015년 3월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SMSReg	152,962
2	Android-PUP/Noico	14,083
3	Android-Trojan/FakeInst	12,319
4	Android-PUP/Dowgin	9,480
5	Android-Trojan/AutoSMS	6,176
6	Android-PUP/Airpush	4,041
7	Android-Trojan/Opfake	3,723
8	Android-PUP/Wapx	2,738
9	Android-Trojan/SMSAgent	2,641
10	Android-Trojan/SmsSend	2,152

2

보안 이슈
SECURITY ISSUE

01
다시 돌아온 LSP 변조, 파밍 공격

오래전 '온라인게임핵', '파밍' 악성코드에 사용된 공격 방법이 최근 다시 발견되었다. 이번에 발견된 공격 방법은 LSP(Layered Service Provider) 변조를 이용한 방식과 정상파일을 악용한 방식이다. 두 가지 방식에 대해 알아보자.

1. LSP 변조 방법

관련 악성코드를 다루기 전에 LSP에 대해 알아보면 [그림 2-1]과 같다.

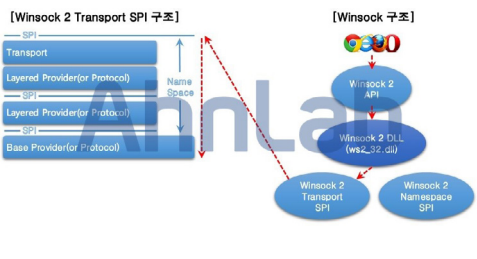


그림 2-1 | Winsock 2 & Winsock 2 Transport SPI 구조

Winsock(Windows Socket API)은 윈도 운영체제 내에서 인터넷 응용프로그램의 입출력 요청을 처리하는 인터페이스이다. 웹 브라우저와 같은 응용프로그램의 명령을 받아 'Winsock 2 DLL'을 거쳐 최종적으로 'Base Provider'와 통신한다.

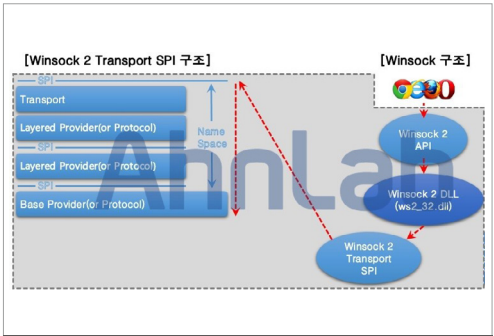


그림 2-2 | LSP(Layered Service Provider) 구조

이러한 통신 과정, LSP는 모든 데이터를 여과 없이 통과하므로 송수신되는 데이터를 모두 감시할 수 있다. LSP를 임의로 삭제할 경우 네트워크가 정상적으로 동작하지 않는다. 또한 레지스트리에 등록 및 설치되므로 LSP의 변조 여부를 인지하기 어렵다.

이번에 발견된 악성코드는 기존의 공격 방법인 'LSP 변조'와 'VPN 터널링' 기법을 사용했다. 악성코드에 감염되면 [표 2-1]과 같이 파일을 생성한다.

표 2-1 | 생성된 파일 경로

[생성 파일]
C:₩WINDOWs₩system32₩v2BSXerv.dll
C:₩WINDOWs₩system32₩twlsp.dll

생성된 파일은 [표 2-2]와 같이 레지스트리에 등록되어 시스템 시작 시 자동으로 실행된다.

표 2-2 | 레지스트리 등록

HKLM₩SYSTEM₩ControlSet001₩Services₩BSXerv₩DisplayName
→"BS Server"

HKLM₩SYSTEM₩ControlSet001₩Services₩BSXerv₩ImagePath
→"%SystemRoot%₩system32₩svchost -k BSXerv"

HKLM₩SYSTEM₩ControlSet001₩Services₩BSXerv₩Parameters₩ServiceDll
→"C:₩WINDOWS₩system32₩v2BSXerv.dll"

이후 시스템의 LSP를 변조한다. 악성코드는 시스템에 저장된 LSP 프로토콜 정보 목록을 모두 삭제한 후 'twlsp.dll' 파일을 추가한다. 그 다음 기존에 저장되어 있는 LSP 프로토콜 정보를 복원시킨다.

표 2-3 | 변조된 LSP 경로

HKLM₩SYSTEM₩ControlSet001₩Services₩WinSock2₩Parameters₩Protocol_Catalog9₩Catalog_Entries₩[숫자]₩PackedCatalogItem
→ *43 3A 5C 57 49 4E 44 4F 57 53 5c 73 79 73 74 65 6d 33 32 5c 74 77 6c 73 70 2e* ...(생략)

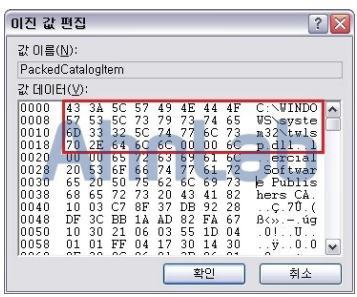


그림 2-3 | 추가된 'twlsp.dll' 파일

악성코드는 사용자가 감염 여부를 인지하지 못하도록 자가 삭제한다. 그리고 svchost.exe 파일을 통해 실행된 'v2BSXerv.dll' 파일로 VPN 정보를 수신하여 연결을 시도한다.

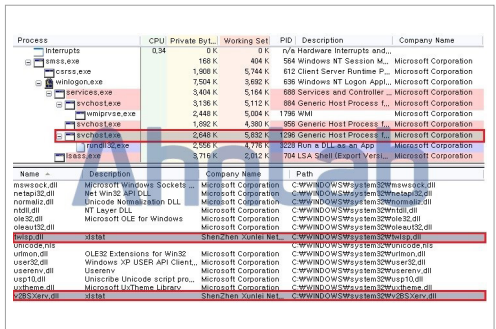


그림 2-4 | 실행 중인 'v2BSXerv.dll' 파일

그림 2-5 | VPN 정보 수신

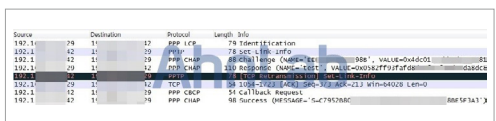


그림 2-6 | VPN 연결 시도

VPN 연결이 완료되면 악성코드는 감염된 시스템에서 사용자가 주요 포털과 은행 사이트에 연결하는지 감시한다. 사용자가 사이트 접속을 시도하면 감염된 악성코드에 의해 파밍 사이트로 연결된다.

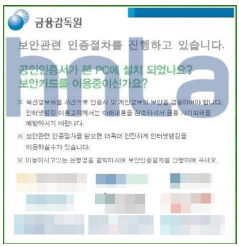


그림 2-7 | 파밍 사이트 화면

[그림 2-7]과 같이 사용자가 파밍 사이트에 접근하면 금융 정보가 탈취된다. 이런 종류의 악성코드는 보안 취약점이 있는 PC에서 웹사이트에 방문만 해도 감염될 수 있다. 따라서 사용자는 악성코드 감염 예방을 위해 응용프로그램의 보안 업데이트를 꼼꼼히 하고 안전한 사이트인지 확인한 후 방문해야 한다.

2. 정상파일(UTIL)을 악용한 파밍 공격

다수의 국내 사이트가 파밍 악성코드 유포에 악용되었다. 악성코드 유포에 이용된 사이트 대부분은 최종적으로 동일한 악성 파일을 내려받도록 조작되어 있었으며, 침해된 사이트 중 일부는 [그림 2-8]과 같다.

그림 2-8 | 침해된 일부 사이트

이번에 발견된 악성코드는 '카이홍 갓모드(Caihong, God Mode)'를 이용한 악성코드와 유포 방법이 유사하다. 공격자는 취약한 사이트에 아이프레임(iframe)을 삽입했으며, 여러 경유지를 거쳐 최종적으로 파밍 악성코드를 내려받도록 유도한다.

그림 2-9 | 악성코드 유포 과정

삽입된 스크립트들은 분석이 어렵게 난독화되어 있었으며, 스크립트 동작이 눈에 보이지 않기 때문에 일반 사용자는 악성코드에 감염된 사실을 인지하기 어렵다.

그림 2-10 | 정상 • 악성 DLL 비교

이번에 발견된 파밍 악성코드의 특징은 악성코드를 실행시키는 과정에서 정상 유틸리티 파일을 이용했다는 점이다. 정상파일이 악성코드 실행에 이용된 것이 이번이 처음은 아니다. 2014년에도 국내에서 잘 알려진 프로그램의 정상파일도 악성코드 실행에 사용되었다.

그림 2-11 | DLL 로드

해당 악성코드는 마우스로 볼륨을 조절하는 유틸리티인 '볼류마우스(Volumouse Utility)'를 통해 악성 행위를 한다. 이는 정상파일이 DLL을 로드하는 과정에서 DLL을 검증하지 않는 설계상의 문제점을 이용한 것이다. Volumouse.exe는 위치기반으로 vlmshlp.dll을 로드하여 실행한다. DLL을 로드하는 과정에서 로드될 파일의 사실 여부를 검증하지 않는다. 따라서 로드될 DLL과 이름만 같다면 설계 시 의도한 파일이 아니어도 문제없이 실행된다.

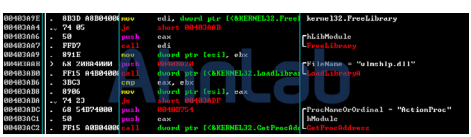


그림 2-12 | 악성 vlmshlp.dll 로드

[그림 2-13]과 같이 로드된 악성 vlmshlp.dll은 svchost.exe를 실행시키고 메모리 변조를 통해 악성 행위를 하는 프로세스로 둔갑시킨다.

그림 2-13 | 변조된 svchost.exe 실행

또한, 메모리 영역의 데이터만 변조했기 때문에 파일 자체는 정상파일이지만 실제 행위는 악성 vlmshlp.dll이 변조한다. 따라서 일반 사용자는 vlmshlp.dll이 악성인지 정상인지 판단하기 어렵다.

최종적으로 변조된 svcshost.exe는 공인인증서 유출, DNS 변조, 맥주소(Mac Address) 유출 등을 통해 파밍 사이트로 접속을 유도하여 사용자 정보를 탈취한다.

그림 2-14 | 파밍 사이트

정상 사이트를 침해한 악성코드 유포는 사이트에 접속하는 모든 사용자를 대상으로 한다. 이러한 공격은 특정 응용프로그램과 운영체제의 취약점을 이용하여 사용자 모르게 악성코드를 감염시킨다. 감염 사실 또한 인지하기 어렵기 때문에 보안 업데이

트나 백신을 사용하지 않으면 무방비 상태로 악성 코드에 노출될 수 있다. 따라서 악성코드를 예방하려면 보안업데이트와 백신을 항상 최신 버전으로 유지해야 한다.

V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Kryptik (2015.03.04.00)
Trojan/Win32.Injector(2015.03.09.03)
Trojan/Win32.Banki(2015.03.10.04)
JS/Redirect(2015.03.10.02)
JS/Exploitkit(2015.03.09.02)

02
주요 기관 노리는 CHM 악성코드

기관을 노린 것으로 추정되는 악성 CHM(Microsoft Compiled HTML Help) 파일이 지속적으로 발견되고 있다. 특히 과거부터 발견된 몇몇 파일들이 서로 비슷한 특징을 가지고 있어 그 연관성을 확인해볼 필요가 있다.

[그림 2-15]와 같이 악성 파일을 실행하면 마이크로소프트 도움말(CHM) 파일과 PDF 파일로 된 청첩장을 확인할 수 있다.

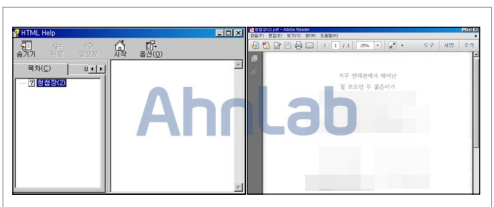


그림 2-15 | CHM 파일(좌)과 PDF 파일(우) 실행 시 나타나는 화면

CHM 파일을 클릭하면 악성 파일이 바로 실행된다. 이는 index.htm에 있는 오브젝트(object) 태그를 이용하여 악성코드를 로드하기 때문이다([그림 2-16]).

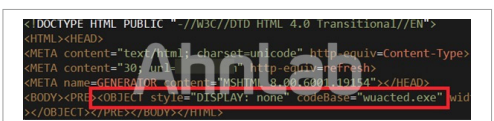


그림 2-16 | 오브젝트 태그를 이용한 악성 파일(wuacted.exe) 실행

해당 악성코드는 여러 스레드(thread)와 이벤트로 동작한다. 각 스레드는 C&C와의 송수신, 악성코드 다운로드, 파일 실행 기능을 갖고 있다. 특히 하드 코딩되어 있는 값들로 HTTP 헤더(header)를 랜덤하게 구성하는 코드가 확인되었다. 하지만 현재 C&C(www.wi****m.com, 17*.**.***.*53:3680)가 정상으로 동작하지 않아 자세한 확인은 이루어지지 않았다. [표 2-4]와 같이 랜덤하게 구성되는 HTTP 헤더의 URL은 존재하지 않는 주소로 확인된다.

표 2-4 | 랜덤하게 구성되는 각 헤더 요소들

HTTP METHOD	HOST	Referer	Connection	Range
GET /ws.mp3	Host: www.vl[redacted].com	Referer: http://89[redacted].mp3.htm	Connection: close	
GET /bws.mp3	Host: www.al[redacted].com	Referer: https://www.n[redacted].com/index.php?act=SF	Connection: keep alive	Range: bytes=256[redacted]4
GET /bws.mp3	Host: www.n[redacted].com	Referer: http://news.n[redacted].com/1FOOQ.html	Connection: continue	

그림 2-17 | 구성된 헤더(요청 페이지는 존재하지 않음)

이러한 형태, 행위와 C&C는 [그림 2-18]과 같이 과거 수집된 몇몇 CHM 악성코드에서도 확인된 바 있다.

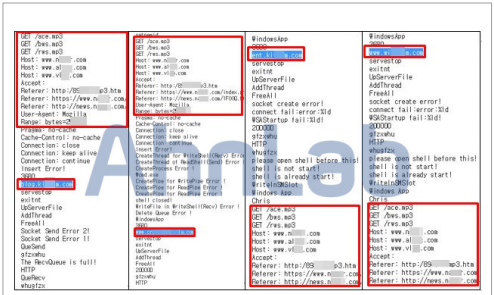


그림 2-18 | 파일 별 바이너리 문자열 비교
(왼쪽부터 2012년 5월, 2013년 4월, 2015년 3월, 2015년 3월)

안랩은 청첩장, 이력서를 비롯하여 '3.20 전용 백신', '국방표준종합정보시스템 공지' 등으로 위장한 CHM을 소개한 바 있다. [표 2-5]는 각 파일의 특징을 간단히 비교한 것이다.

표 2-5 | 파일 비교

수집일	드라퍼 위장	악성파일 로드방식	C&C 도메인	파일명	랜덤 HTTP헤더 조합
2012-05월	청첩장	object 태그	blog.kh[redacted]m.com	arcldrb.exe	o
2013-04월	3.20 전용백신 공지 메일	object 태그	www.cre[redacted]sla.com 119.[redacted]30	wcre.exe	o
2014-10월	국방관련 공지 글업	object 태그	express.kh[redacted]m.com 175.[redacted]63	msupdate.exe	x
2014-12월	-	-	news.kh[redacted]m.com	wuacteld.exe	o
2014-12월	-	-	ent.kh[redacted]m.com	FlashUpdatec.exe	o
2015-03월	청첩장	object 태그	www.wi[redacted]m.com 175.[redacted]53	wuacted.exe	o

[표 2-5]와 같이 로드 방식이나 C&C 도메인의 유사성, 바이너리 문자열 그리고 랜덤 HTTP 헤더 조합 코드의 존재 여부를 비교했을 때 파일 간에는 어느 정도 유사성이 있는 것으로 추정된다. 적당한 시간 간격으로 꾸준히 접수되고 있고 최근까지도 관련 테스트 파일이 수집되었기 때문이다.

이처럼 CHM을 이용한 해킹 시도는 계속되고 있다. 공격 대상 또한 보안, 국방, 외교 등 중요도가 높은 국가 기관일 가능성이 높다. 해당 악성코드가 실행되면 C&C 서버에서 원격 명령을 그대로 실행할 수 있어 감염 시 2차 피해가 우려된다. 이에 사용자의 각별한 주의가 요구된다.

V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Dropper/Rctl (2015.03.17.00)
Trojan/Win32.RCtl (2015.03.20.05)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

오토캐드 악성코드 감염 증상과 예방법

오토캐드 악성코드 감염 증상과 예방법

안랩의 '바이러스 신고센터'에는 간혹 오토캐드(AUTOCAD) 악성코드와 관련된 문의가 접수되고 있다. 오토캐드를 사용하는 기업에서는 악성코드 감염 사실을 바로 알아차리지 못하는 경우가 많다. 이는 오토캐드 악성코드로 자주 발견되는 'LISP(List Processor)' 파일이 다른 프로그램에는 영향을 주지 않고 도면 파일(*.dwg)이 실행될 때 자동으로 로드되어 실행되기 때문이다.

악성코드 제작자는 도면 파일의 명령어 실행을 방해하거나 LISP 파일 유포가 목적인 만큼 일반 PC 사용자는 감염 여부 확인이 어렵다. 이로 인해 어느 정도 시간이 지난 후 다수의 오토캐드 사용자에게 문제가 생긴 후 접수되는 경우가 많다. 이에 오토캐드 악성코드의 감염 증상과 예방법에 대해 알아본다.

오토캐드 악성코드로 발견되는 파일명은 많지만 주로 사용되는 파일명은 [표 3-1]과 같다.

표 3-1 | 오토캐드 악성코드에 주로 사용되는 파일명

acad.lsp, acaddoc.lsp, acadapp.lsp, acadapq.lsp, acadiso.lsp, acad.dvb
acad.fas, acaddoc.fas, acad.vlx, acadiso.lsp, acad.mnl

악성 파일이 있는 폴더의 도면 파일을 실행했을 때 나타나는 증상은 [표 3-2]와 같다.

표 3-2 | 오토캐드 악성코드 감염 시 나타나는 주요 증상

1	모든 도면 폴더 경로에 LISP 파일 생성
2	일부 Command 명령어 사용 불가(EXPLODE, XREF, XBIND 등)
3	알 수 없는 오류 문자열과 알림창
4	시스템 변수 변경(ACADLSPASDOC, FILLMODE 등)
5	LOAD 실패 메시지(acaddoc, acadapp, acadapq)
6	VBA 시스템초기화 중… 실행오류 알림 발생(VBA를 로드하는 중 자동화 오류 발생)
7	오류 : stringp nil
8	도면 파일 실행 시 프로그램 응답 없음 또는 지연(Delay)

[표 3-2]의 오토캐드 악성코드 감염 시 나타나는 주요 증상 중 일부를 살펴보자. 오토캐드 악성코드에 감염되면 [표 3-2]의 1과 같이 모든 도면 폴더 경로에 LISP 파일이 생성된다.

그림 3-1 | 생성되는 LISP 파일

해당 악성 파일은 [AutoCAD폴더\Support\acadapp.lsp] 경로에 자기 자신을 복제한 후 [AutoCAD폴더\Support\acad.lsp] 경로의 파일을 [그림 3-3]과 같이 수정한다.

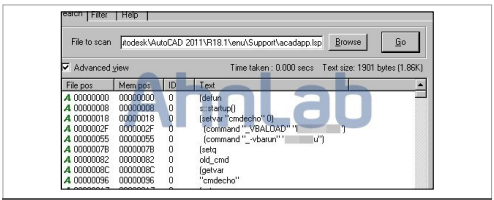


그림 3-2 | acadapp.lsp 파일 내용 중 일부

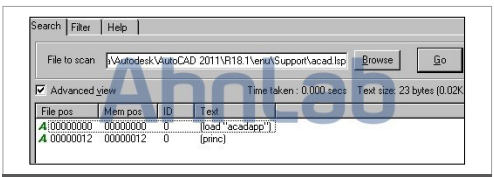


그림 3-3 | acad.lsp 파일 내용

이후 도면 파일 실행 시 [표 3-2]의 7과 같이 '오류 : stringp nil'이라는 메시지가 나타난다.

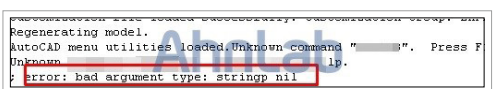


그림 3-4 | stringp nil 오류

또는 [표 3-2]의 6과 같이 'VBA 시스템 초기화 중… 실행오류 알림'이라는 메시지를 출력한다.

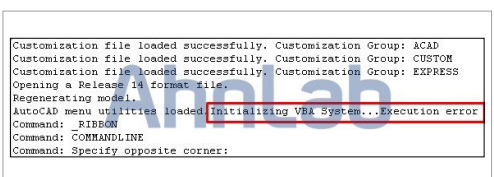


그림 3-5 | VBA 시스템 초기화 중…실행오류

[AutoCAD폴더\Support\acadapp.lsp] 파일 및 다른 폴더의 acad.lsp 파일을 삭제하더라도 [AutoCAD폴더\Support\acad.lsp] 파일의 내용이 수정되지 않으면 [그림 3-6]과 같이 'LOAD 실패([표 3-2]의 5)'가 발생할 수 있다.

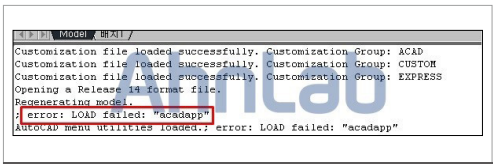


그림 3-6 | 로드 실패

위의 샘플과 비교하여 또 다른 악성 파일인 'acad.fas'에서는 [그림 3-7]과 같은 증상을 확인할 수 있다.

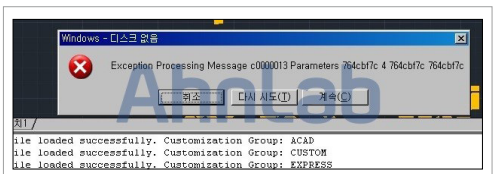


그림 3-7 | '해당 파일과 동일한 폴더에 있는 도면 파일 실행 시 오류 문자열 출력 발생'([표 3-2]의 3)

또한 [표 3-2]의 3과 같이 'ACADLSPASDOC'의 변수 값이 0에서 1로 변경된다.

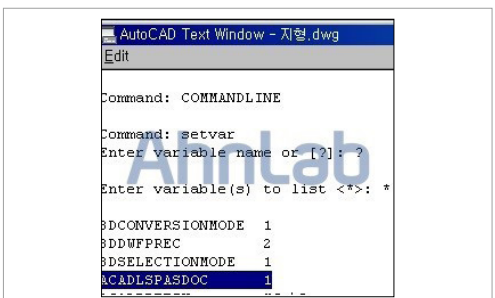


그림 3-8 | 시스템 변수 변경

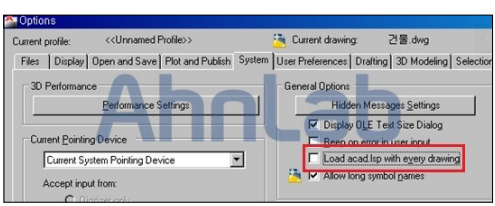
위와 같이 오토캐드 악성코드에 감염되면 도면 파일이 정상으로 실행되지 않거나 특정 명령어가 동작하지 않아 사용자는 불편을 느낀다. 따라서 오토캐드 사용자는 오토캐드 프로그램 실행 시 확인되지 않은 VBA(Visual Basic for Application) 스크립트 실행을 자제하고, 공유 폴더를 사용하지 않는 것이 안전하다. 다수의 기업에서는 업무 편의를 위해 도면 폴더를 공유 폴더로 설정하여 사용하는 경우가 많다. 이는 모든 사용자가 악성코드에 감염될 수 있으므로 공유 폴더를 사용하지 않는 것만으로도 추가 악성코드 감염을 예방할 수 있다.

[오토캐드 악성코드 예방법]

1. 직접 작성하지 않은 LISP 파일이 폴더에 있을 경우, 도면 파일을 실행하기 전 파일 내용을 확인한다(오토캐드 실행 시 자동으로 로드하는 LISP 파일 : acad.lsp, acad.fas, acaddoc.lsp acad.dvb, acaddoc.vlx, acaddoc.fas 등).

2. 악성코드가 자주 사용하는 파일명에 대해 빈 LISP 파일은 '읽기전용' 속성으로 생성한다.

3. 오토캐드 옵션을 조정한다. [모든 도면에 acad.lsp 로드] 체크박스를 해제한다.



4. ACADLSPASDOC 시스템 변수의 값을 0으로 설정한다.
- Command : setvar → ? → * 로 확인 가능

5. *.mnl 파일 또는 사용 중인 *.lsp 파일은 읽기 전용 속성으로 사용한다.

6. 오토캐드 악성코드는 바이러스처럼 전파기능이 있으므로 공유 폴더 사용을 자제한다.

한편, V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

ALS/Bursted

AhnLab

ASEC REPORT

VOL.63
March, 2015

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