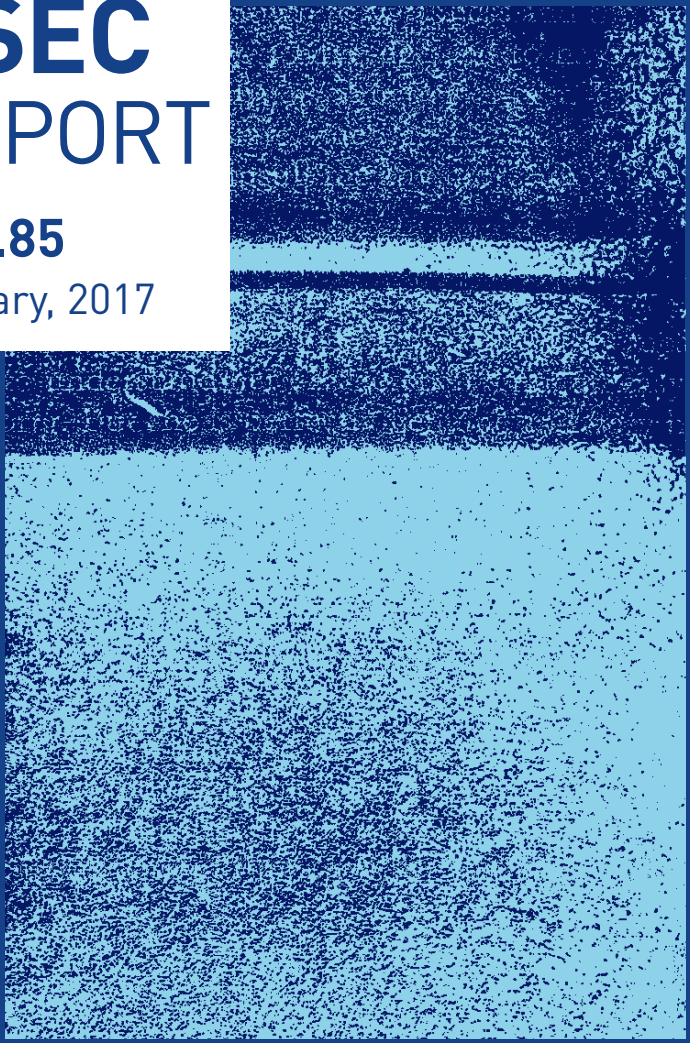
Security Trend

ASEC REPORT

VOL.85

January, 2017



AhnLab

ASEC REPORT

VOL.85 January, 2017

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.

2017년 1월 보안 동향

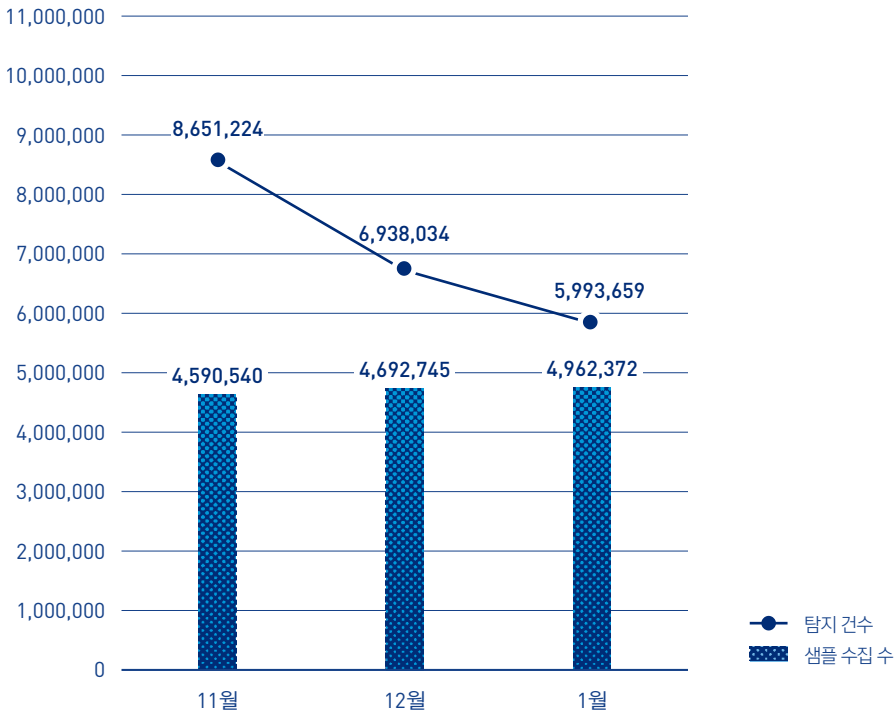
Table of Contents

1

보안 통계
STATISTICS

01
악성코드 통계

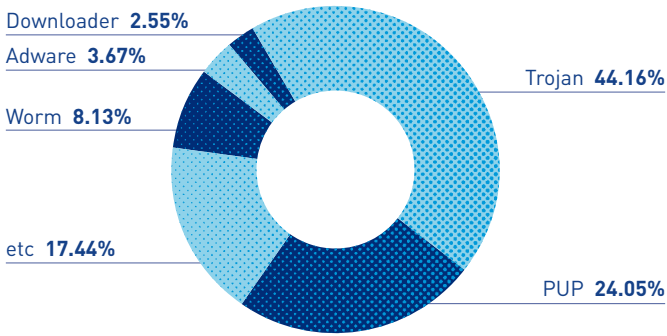
ASEC이 집계한 바에 따르면, 2017년 1월 한 달간 탐지된 악성코드 수는 599만 3,659건으로 나타났다. 이는 전월 693만 8,034건에 비해 94만 4,375건 감소한 수치다. 한편 1월에 수집된 악성코드 샘플 수는 496만 2,372건이다.



[그림 1-1] 악성코드 추이(2016년 11월~2017년 1월)

* '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 1-2]는 2017년 1월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 44.16%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 24.05%로, 웜(Worm)이 8.13%의 비율로 그 뒤를 이었다.



[그림 1-2] 2017년 1월 주요 악성코드 유형

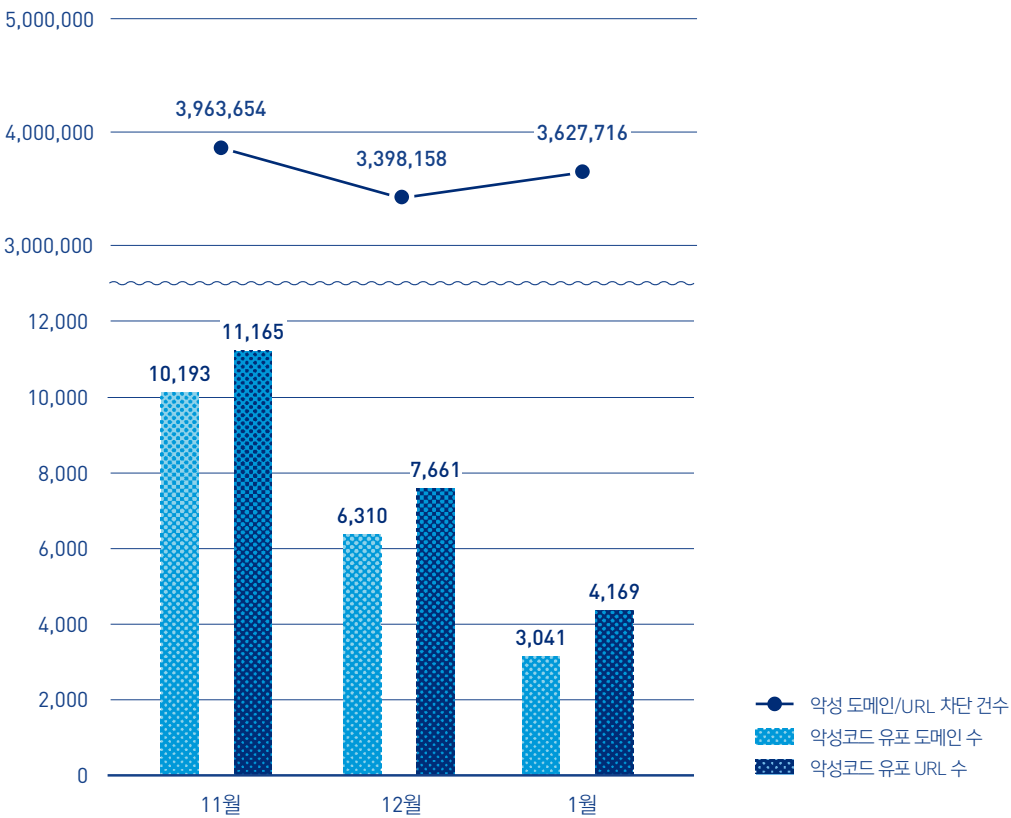
[표 1-1]은 1월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter가 총 18만 8,236건으로 가장 많이 탐지되었고, Trojan/Win32.Banki가 10만 9,737건으로 그 뒤를 이었다.

[표 1-1] 2017년 1월 악성코드 탐지 최다 10건 (진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	188,236
2	Trojan/Win32.Banki	109,737
3	Malware/Win32.Generic	109,532
4	Unwanted/Win32.HackTool	100,074
5	Trojan/Win32.Cerber	83,796
6	Trojan/Win32.Agent	81,853
7	Trojan/Win32.Downloader	70,037
8	Trojan/Win32.Neshta	62,705
9	HackTool/Win32.AutoKMS	58,664
10	Trojan/Win32.Nitol	50,652

02
웹 통계

2017년 1월에 악성코드 유포지로 악용된 도메인은 3,041개, URL은 4,169개로 집계됐다([그림 1-3]). 또한 1월의 악성 도메인 및 URL 차단 건수는 총 362만 7,716건이다.

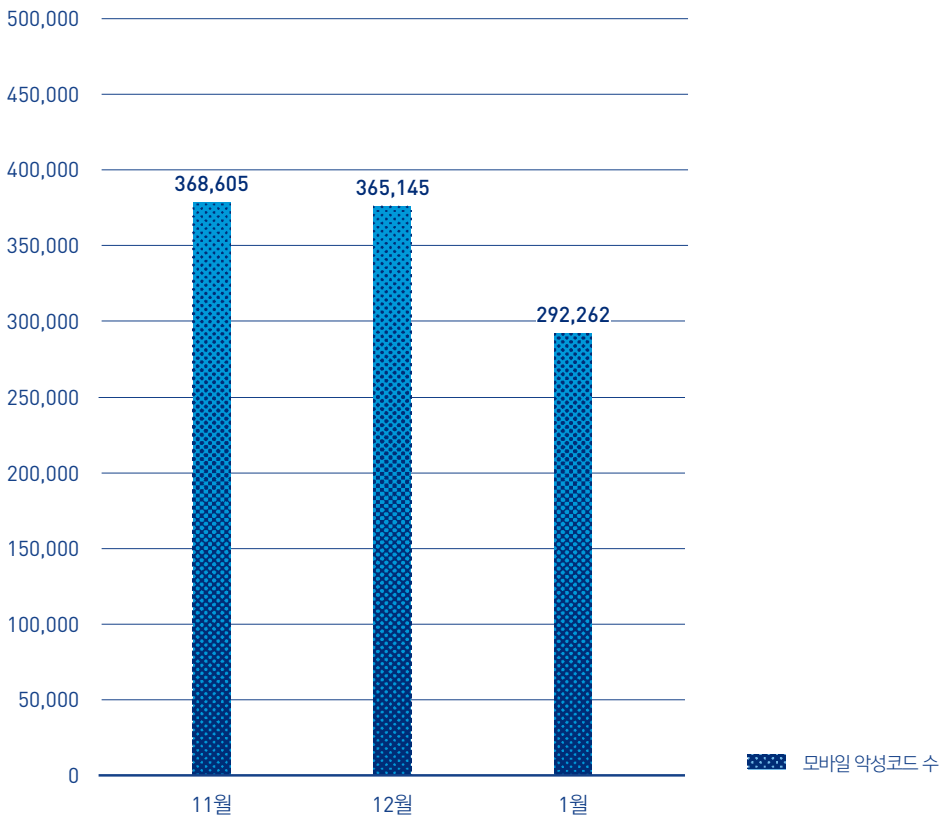


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 11월~2017년 1월)

* '악성 도메인 및 URL 차단 건수'란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03
모바일 통계

2017년 1월 한 달간 탐지된 모바일 악성코드는 29만 2,262건으로 나타났다.

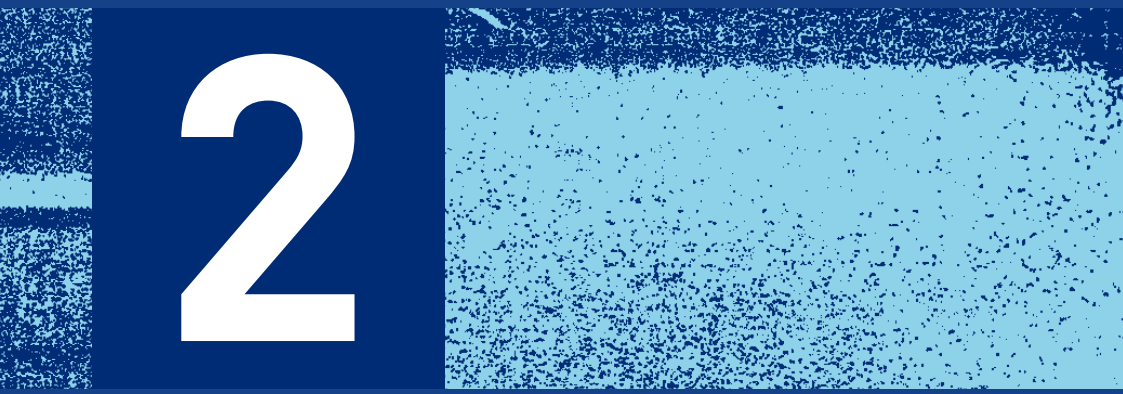


[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 1월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/Shedun이 가장 많이 발견되었다.

[표 1-2] 2017년 1월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/Shedun	61,999
2	Android-PUP/SmsPay	41,759
3	Android-PUP/Agent	23,227
4	Android-Trojan/Jimo	18,024
5	Android-Trojan/Slocker	14,999
6	Android-Trojan/SmsSpy	11,249
7	Android-Trojan/Agent	11,037
8	Android-PUP/SmsReg	7,424
9	Android-Trojan/SmsSend	6,389
10	Android-PUP/Baogifter	6,333



2

보안 이슈
SECURITY ISSUE

01 압축 프로그램으로 위장한 백도어 악성코드 유포

최근 정상 프로그램으로 위장한 백도어(Backdoor) 악성코드가 발견되어 사용자들의 각별한 주의가 필요하다. 공격자들은 주로 사용자들에게 익숙하고 널리 알려진 유명 유틸리티 프로그램이나 동영상 파일 등을 이용하여 악성코드를 유포하는데, 이번에 발견된 백도어 악성코드 역시 국내 유명 압축 프로그램인 것처럼 둔갑해 사용자들을 속이는 전통적인 공격 방식을 통해 유포됐다.

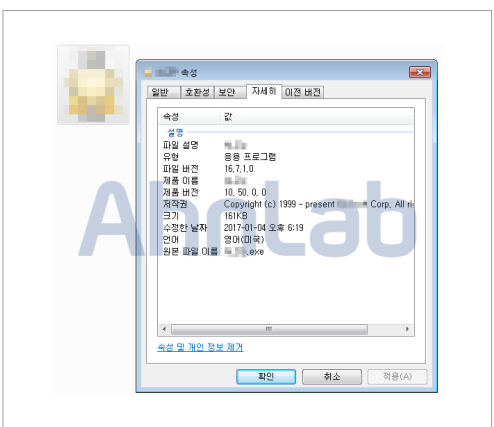


그림 2-1 | 국내 유명 압축 프로그램으로 위장한 악성코드

백도어는 본래 유사 시 장애 해결이나 유지 보수 등의 관리를 위해 시스템에 의도적으로 남겨둔 일종의 보안 허점으로, 악의적으로 이용되는 경우 보안상으로 치명적인 문제를 일으킬 수 있다. 특히 정상적인 로그인 절차를 거치지 않고 트로이목마를 침투시켜 백도어로 이용하는 경우 시스템 침입 여부를 은폐하고, 추후 시스템에 재침입하기 위한 백도어를 추가로 설치하는 등 추가 악성 행위가 가능하기 때문에 위험하다.

그림 2-2 | DEP 우회를 위한 API

이번에 발견된 악성코드는 [그림 2-2]와 같이 윈도우(Windows)의 DEP(Data Execution Prevention, 데이터 실행 방지)를 우회하기 위해 2개의 API를 이용한다. DEP는 프로그램이 동적으로 생성하는 코드의 실행을 막는데, 그

대표적인 예가 악성코드의 특정 메모리에 입력된 쉘코드(Shellcode)다. 따라서 이를 우회하여 악성 행위를 수행하기 위해 API를 이용하는 것이다.

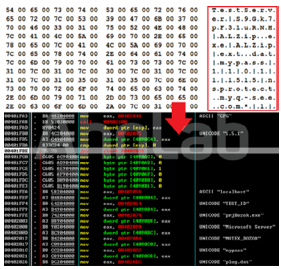


그림 2-3 | RCDATA 내 하드코딩된 문자열

분석 결과 악성코드는 RCDATA 내 특정 하드코딩된 문자열을 읽어 들이며, 해당 문자열에는 악성코드명, 뮤텍스(Mutex), C&C 서버 주소 등과 같은 정보가 포함된 것이 확인됐다. 만일 RCDATA 내 데이터가 존재하지 않으면, [그림2-3]의 유니코드(UNICODE) 값으로 정보를 설정한다.

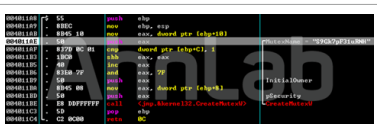


그림 2-4 | 뮤텍스(Mutex) 생성

이후 악성코드는 RCDATA 내 문자열로 [그림 2-4]와 같이 뮤텍스(Mutex)를 생성한 뒤, 특정 값(0B7)과 비교하여 중복 실행될 경우 종료된다.

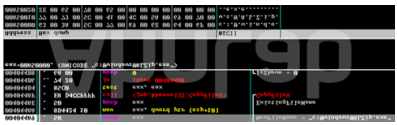


그림 2-5 | C:\Windows 경로 내 자가 복제

또한 [그림 2-5]와 같이 C:\Windows 경로에 자가 복제한 후 악성코드를 실행시키는데, 해당 경로에서 복제 파일을 실행하지 못할 경우에는 추가 경로인 C:\Documents and Settings\Administrator\Application Data에 자가 복제한 후 실행된다.

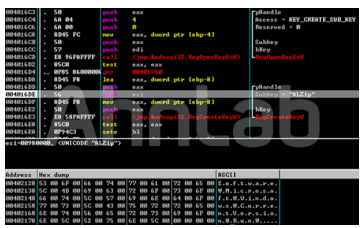


그림 2-6 | 런(Run) 레지스트리 키 등록

이후 악성코드는 [그림 2-6]과 같이 런(Run) 레지스트리 키에 자기 자신을 등록하여 시스템이 시작될 때마다 자동 실행될 수 있도록 한다.

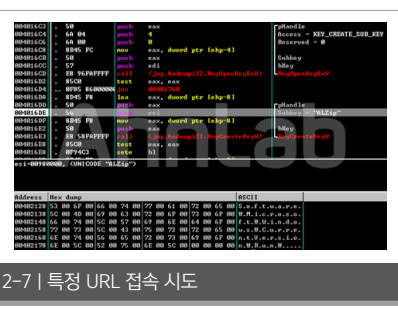


그림 2-7 | 특정 URL 접속 시도

또한 악성코드는 [그림 2-7]과 같이 125.189.58.45:1515의 C&C 서버 주소로 20초마다 통신을 시도한 것이 확인됐다. 분석 당시에는 해당 C&C 서버에 접속이 되지 않았지만, 해당 C&C 서버로부터 추가 명령을 받아 악성 행위를 수행했을 것으로 추정된다.

그림 2-8 | 백도어로부터 탈취되는 정보들

최종적으로 C&C 서버와 접속이 이뤄지면, 공격자는 명령 프롬프트(cmd.exe)를 이용하여 [그림 2-8]과 같이 사용자 시스템 내 다양한 정보들을 탈취할 것으로 보인다.

최근 불법 공유되는 유틸리티 프로그램이나 동영상 파일 등에 악성코드가 첨부되어 유포된 사례가 꾸준히 발견되고 있다. 특히 이번 사례와 같이 대부분의 백도어 악성코드는 의심을 피하기 위해 사용자들에게 익숙한 정상 프로그램으로 위장하므로 주의해야 한다.

악성코드 감염을 예방하기 위해서는 공식적인 경로로 제공되는 프로그램이 아닌 불법 공유되는 프로그램의 이용은 지양하는 것이 바람직하다. 또 파일 다운로드 시 백신의 정밀 검사 기능을 이용해 확인하는 습관이 필요하다. 또한 최신 버전이 아닌 소프트웨어를 사용하는 경우, 취약점을 이용한 악성코드에 감염될 가능성이 높기 때문에 반드시 사용하는 소프트웨어 및 백신 제품을 최신 버전으로 유지하는 등 올바른 사용 습관을 가져야 한다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Bezigate (2017.01.03.06)

02
신용카드 정보 '쏙', 파밍 악성코드 주의보

"보다 안전한 인터넷 뱅킹의 이용을 위하여 인터넷 뱅킹, 스마트 뱅킹, 폰 뱅킹, 이 모든 서비스를 이용하시려면 (개인, 기업) 추가 인증 후 이용이 가능합니다."

해당 메시지는 파밍(Pharming) 악성코드에 감염되었을 때, 위조된 피싱 페이지에서 흔히 볼 수 있는 팝업 메시지다. 파밍 악성코드의 주 목적은 사용자의 공인 인증서와 주요 금융 정보들을 탈취하는 것이기 때문에 공격자들은 주로 은행 사이트를 사칭한 피싱 사이트를 제작하는데, 최근 사용자들의 신용카드 정보를 노려 국내 유명 카드사로 위장한 피싱 사이트가 새롭게 발견되어 각별한 주의가 필요하다.

파밍 악성코드는 주로 사용자가 직접 파일을 실행하는 행위를 하지 않고, 사이트에 접속만 해도 악성코드에 감염되는 '드라이브 바이 다운로드(Drive-by-download) 방식'을 통해 유포되거나, 불필요한 프로그램(Potentially Unwanted Program, PUP)이나 정상 유틸리티 프로그램의 업데이트 모듈을 이용해 유포된다.

이번에 발견된 파밍 악성코드 또한 사용자가 인지할 수 없도록 불필요한 프로그램을 통해 다운로드되는데, 해당 파밍 악성코드가 실행되면 [표 2-1]과 같이 윈도우 운영체제 파일인 mshta.exe를 실행하게 한다.

표 2-1 | 파일 정보

C:\windows\system32\mshta.exe

mshta.exe 파일은 [그림 2-9]의 프로세스 정보에서 확인할 수 있는 것처럼 HTML Application을 실행하는 정상 파일이며, 악성코드는 해당 파일을 실행한 뒤 메모리 영역에 악성코드를 추가로 삽입하여 악성 행위를 수행한다.

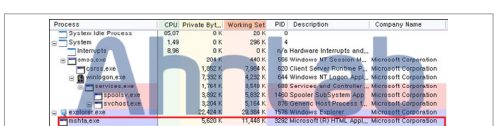


그림 2-9 | 프로세스 정보

이후 공격자의 C&C 서버에 연결을 시도하는데, 해당 C&C 서버의 주소 정보는 [표 2-2]와 같다.

표 2-2 | C&C 서버 정보

67.229.148.198

또한 [표 2-3]과 같이 시작 프로그램에 mshta.exe 파일을 등록하여 시스템이 다시 시작될 때마다 자동으로 실행될 수 있도록 하고, 윈도우 방화벽 예외 정책을 변경하기 위해 레지스트리 정보를 수정한다.

표 2-3 | 시작 프로그램 및 윈도우 방화벽 예외 정책 레지스트리 정보

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\000C293298E5 **->"C:\WINDOWS\system32\mshta.exe"**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Gopp **->"%Temp%\[랜덤 문자열].exe"**
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\1157:TCP **->"1157:TCP:*:Enabled:System"**
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\WINDOWS\system32\mshta.exe **->"C:\WINDOWS\system32\mshta.exe:*:Enabled:Microsoft (R) HTML Application host"**

파밍 악성코드는 [그림 2-10]과 같이 사용자를 위조된 피싱 사이트로 유도하기 위해 먼저 인터넷 익스플로러의 시작 페이지를 국내 주요 포털 사이트로 변경한다. 또한, [인터넷 옵션 > 연결 > 자동 구성 스크립트]에서 항목을 수정하여 사용자가 포털 사이트에 접속할 때 위조된 카드사 페이지로 연결될 수 있도록 조작한다.

그림 2-10 | 피싱 페이지 정보

여기서 눈 여겨 볼 것은 포털 사이트에 나타나는 금융감독원을 사칭한 팝업창이 이전과 다르게 변경된 것이다. 가장 큰 차이점은 [그림 2-11]에 표시된 것처럼 팝업창 하단에 은행 사이트 외에 카드사 사이트가 추가된 것이다.

그림 2-11 | 이전 금융감독원 팝업창(좌)
카드사가 추가된 금융감독원 팝업창(우)

국내 주요 카드사 사이트를 사칭한 피싱 페이지에서는 [그림 2-12]와 같이 사용자의 카드 정보 및 개인 정보 입력을 요구한다.

그림 2-12 | 카드사 사칭 피싱 사이트

최종적으로 사용자가 피싱 사이트에 입력한 정보는 [그림 2-13]과 같이 공격자의 C&C 서버로 전송되어 각종 악성 행위에 이용된다.

그림 2-13 | 네트워크 정보

지난 수 년간 지속적으로 발생하고 있는 파밍 공격은 점점 더 교묘하게 진화하고 있다. 이번 사례에서 확인한 바와 같이 은행 사이트 이외에도 국내 주요 카드사로 위장한 피싱 사이트의 등장으로 사용자들의 피해가 더욱 증가할 것으로 예상되므로 각별히 주의해야 한다.

파밍 공격을 예방하기 위해서는 기본적으로 윈도우 운영체제의 보안 업데이트를 최신으로 설치하여 드라이브 바이 다운로드 유포 방식을 이용한 악성코드에 감염되지 않도록 하며, 출처가 불분명한 사이트에 대해서는 접속에 특히 주의해야 한다. 또한 V3 등 백신 제품의 엔진을 항상 최신 버전으로 유지하는 등의 올바른 습관이 필요하다.

V3 제품에서는 해당 파밍 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Banki (2017.01.12.04)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

랜섬웨어, DDoS 기능을 더하다

랜섬웨어, DDoS 기능을 더하다

2016년에 이어 2017년에도 랜섬웨어 위협은 여전히 계속되고 있다. 랜섬웨어가 지난 한 해 동안 수많은 신・변종 형태로 등장하여 사용자들을 위협한 가운데, 이번에는 DDoS(Distribute Denial of Service, 분산 서비스 거부) 공격 기능이 포함된 랜섬웨어가 발견되어 주의가 필요하다.

해당 랜섬웨어는 닷넷 프레임워크(.NET Framework)를 활용하는 악성코드로, 닷넷 프레임워크 버전이 4.0 미만인 경우에는 실행되지 않고 바로 종료된다. 하지만 버전 조건을 만족하는 경우에는 악성코드가 실행되어, [표 3-1]과 같이 시작 프로그램에 자기 자신을 복사해 시스템이 시작될 때마다 자동으로 실행될 수 있도록 한다.

표 3-1 | 시작 프로그램에 자가 복사

%Programs%\Startup\Djrsqvgah LYXnru.exe %ApplicationData%\SysWin32\files.txt

또한 시스템 내 파일을 파악하여 감염 대상 파일 리스트를 생성하며, [그림 3-1]과 같이 파일 암호화 코드를 통해 해당 리스트에 포함된 파일들의 암호화를 진행한다. 감염 대상 파일 확장자는 [표 3-2]와 같다.

그림 3-1 | 파일 암호화 코드

표 3-2 | 감염 대상 파일 확장자

.aep, .asp, .aspx, .csv, .csx, .doc, .docx, .htm, .html, .jpg, .mdb, .mp3, .pdf, .php, .png, .psd, .sln, .sql, .torrent, .txt

랜섬웨어 악성코드가 실행 상태를 유지하는 경우, 코드 내 하드코딩된 주소(파키스탄 통신 기관)에 지속적인 접근을 시도한다. 이 때 해당 주소에서 받은 데이터를 임시 경로인 Temp를 생성하여 저장한다. 분석 당시에는 해당 URL 접근 시 호스트가 확인되지 않아 파일은 확인되지 않았지만, 실제 패킷을 분석해 보면 [그림 3-2]와 같이 특정 URL 주소에 대한 지속적인 접근이 확인된다.

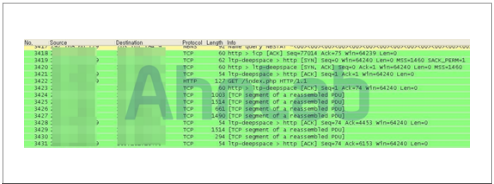


그림 3-2 | 특정 URL 접근 패킷

이번에 발견된 랜섬웨어의 특징은 [그림 3-3]과 같이 다수의 스레드(Thread)를 생성하여 지속적인 접근을 시도하여, 해당 악성코드에 감염되는 사용자가 늘어날수록 하드코딩된 주소를 사용하는 서버에서 많은 수의 패킷이 발생할 수 있다는 점이다. 이와 같은 기능은 DDoS 공격을 유발하여 더 큰 피해를 입힐 것으로 추정된다.

[그림 3-3] 다수의 스레드 생성(좌) 및 특정 URL 접근(우)

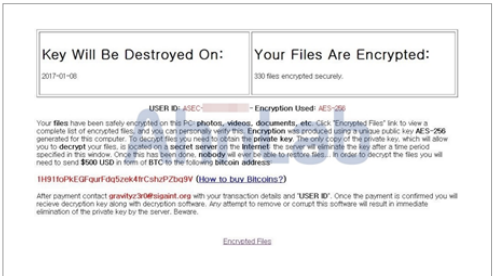
또한 [그림 3-4]의 코드를 분석한 결과, taskmgr의 프로세스 정보를 확인하고 taskmgr을 종료하는 코드가 존재하는데, 이는 작업관리자(taskmgr)의 실행을 방지하여 현재 실행 중인 랜섬웨어 악성코드를 종료하지 못하게 하기 위한 것으로 추정된다.

따라서 랜섬웨어 악성코드가 실행되고 있는 것을 인지한 경우, 작업관리자(taskmgr)가 아닌 명령 프롬프트(cmd.exe), 프로세스 관리 툴 등을 이용하여 해당 악성코드를 종료시켜야 한다.

[그림 3-4] 작업관리자(taskmgr) 프로세스 종료

대부분의 랜섬웨어는 감염 당시 악성 행위가 종료되는 순간 사용자에게 랜섬웨어 감염 메시지를 보여주는 경우가 많다. 그러나 이번에 발견된 랜섬웨어는 시작 프로그램에 자가 복제한 파일이 있을 경우, 랜섬웨어 감염 메시지를 보여주기 때문에, 시스템을 다시 시작했을 때 랜섬웨어 감염 메시지를 확인할 수 있다.

[그림 3-5]의 랜섬웨어 감염 메시지 또한 감염 대상 파일이 있는 경로 전체에 생성하는 것이 아니라, 바탕화면에만 생성하는 점이 일반적인 랜섬웨어와의 차이점이다. 따라서 이번에 발견된 랜섬웨어는 바탕화면에 생성된 랜섬웨어 감염 메시지 파일을 발견하지 못하면 PC 내 파일이 암호화된 사실을 뒤늦게 인식할 것이다.



[그림 3-5] 랜섬웨어 감염 메시지

랜섬웨어는 지난 수 년간 PC 내 파일을 인질로 삼아 몸값을 요구하며 지속적으로 사용자들을 위협해왔다. 그리고 올해 2017년에도 다수의 신・종 랜섬웨어가 발생할 것으로 예측된다. 유포 방식이나 공격 기법이 날로 교묘해지고 있는 랜섬웨어의 피해를 최소화하려면 PC사용자는 ▲스팸 메일(첨부 파일) 실행 자제 ▲중요 파일 별도 백업 습관화 ▲수상한 웹사이트 방문 자제 ▲OS 및 사용 프로그램 업데이트 등의 기본 보안수칙의 실천이 필요하다.

V3 제품에서는 해당 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Crypmodadv (2017.01.05.05)

AhnLab

ASEC REPORT

VOL.85
January, 2017

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

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