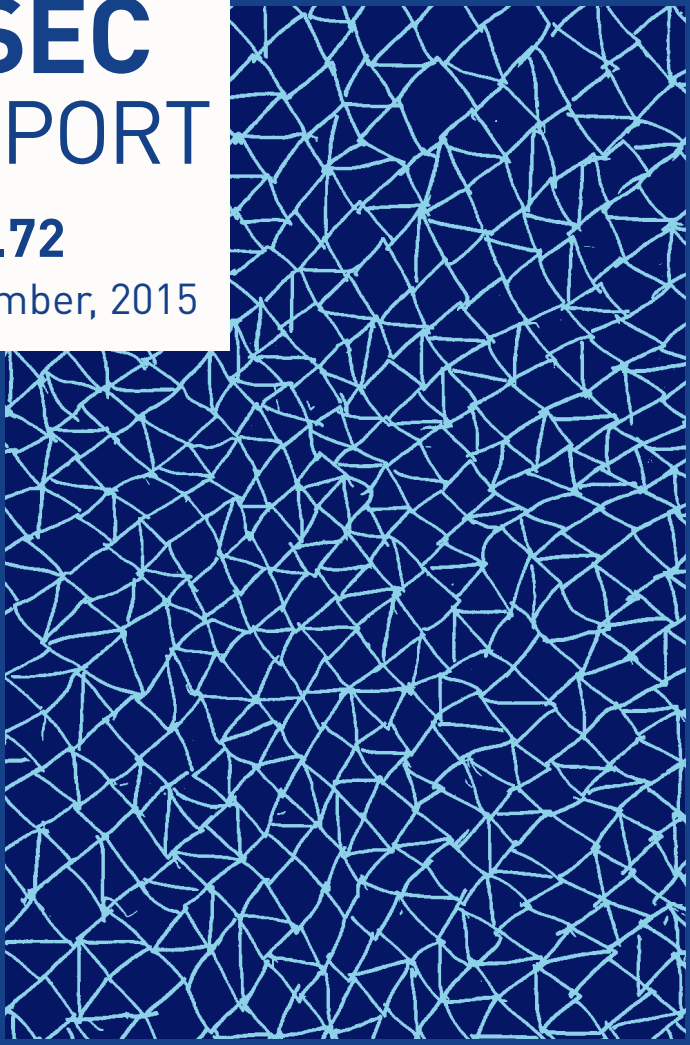
Security Trend

ASEC REPORT

VOL.72

December, 2015



AhnLab

ASEC REPORT

VOL.72 December, 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 12월 보안 동향

Table of Contents

1 보안 통계 STATISTICS

- **01** 악성코드 통계 4
- **02** 웹 통계 6
- **03** 모바일 통계 7

2 보안 이슈 SECURITY ISSUE

- **01** 랜섬웨어의 지역화: '오프라인(Offline)', '키메라(Chimera)' 10
- **02** 중국을 겨냥한 온라인 게임 계정 탈취 악성코드 14

3 악성코드 상세 분석 ANALYSIS IN-DEPTH

- LNK 악성코드 17

4 연간 위협 동향 2015 ANNUAL REPORT

- **01** 2015년 보안 위협 결산 20
- **02** 2016년 보안 위협 전망 23

1

보안 통계
STATISTICS

01 악성코드 통계

02 웹 통계

03 모바일 통계

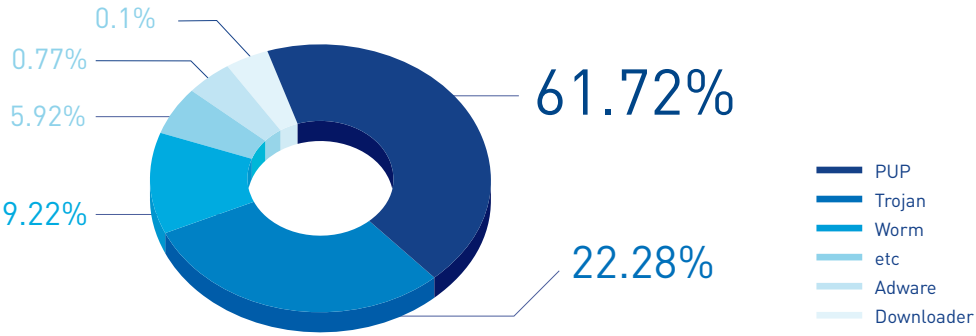
01 악성코드 통계

ASEC이 집계한 바에 따르면, 2015년 12월 한 달간 탐지된 악성코드 수는 1,472만 4,459건으로 나타났다. 이는 전월 1,511만 8,864건에 비해 39만 4,405건 감소한 수치다. 한편 12월에 수집된 악성코드 샘플 수는 668만 4,002건이다.

[그림 1-1] 악성코드 추이(2015년 10월 ~ 2015년 12월)

* '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 2015년 12월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 61.72%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 22.28%, 웜(Worm)이 9.22%의 비율로 그 뒤를 이었다.



[그림 1-2] 주요 악성코드 유형

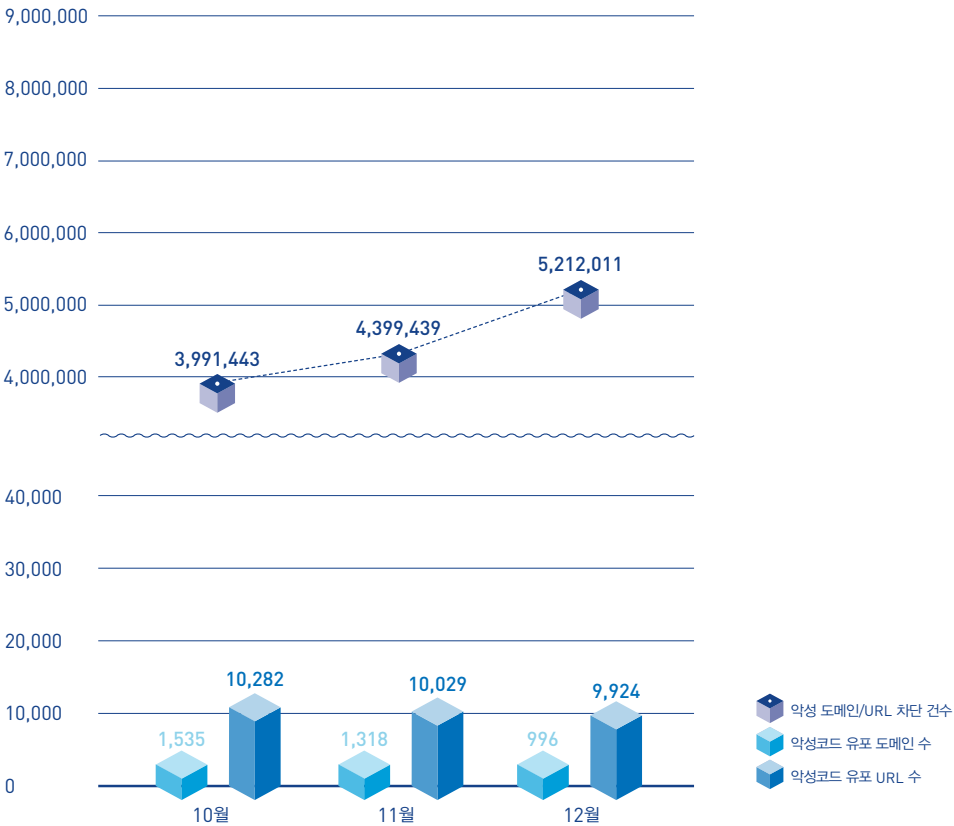
[표 1-1]은 12월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/SWF.Agent가 총 19만 6,608건으로 가장 많이 탐지되었고, Trojan/Win32.Starter가 19만 1,120건으로 그 뒤를 이었다.

[표 1-1] 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/SWF.Agent	196,608
2	Trojan/Win32.Starter	191,120
3	Malware/Win32.Generic	141,225
4	Trojan/Win32.Agent	117,330
5	Trojan/Win32.Gen	85,034
6	Trojan/Win32.Neshta	84,827
7	Unwanted/Win32.Exploit	71,726
8	HackTool/Win32.Crack	68,159
9	Unwanted/Win32.HackTool	67,421
10	Trojan/Win32.Teslacrypt	65,017

02
웹 통계

2015년 12월에 악성코드 유포지로 악용된 도메인은 996건, URL은 9,924건으로 집계됐다([그림 1-3]). 또한 12월의 악성 도메인 및 URL 차단 건수는 총 521만 2,011건이다.

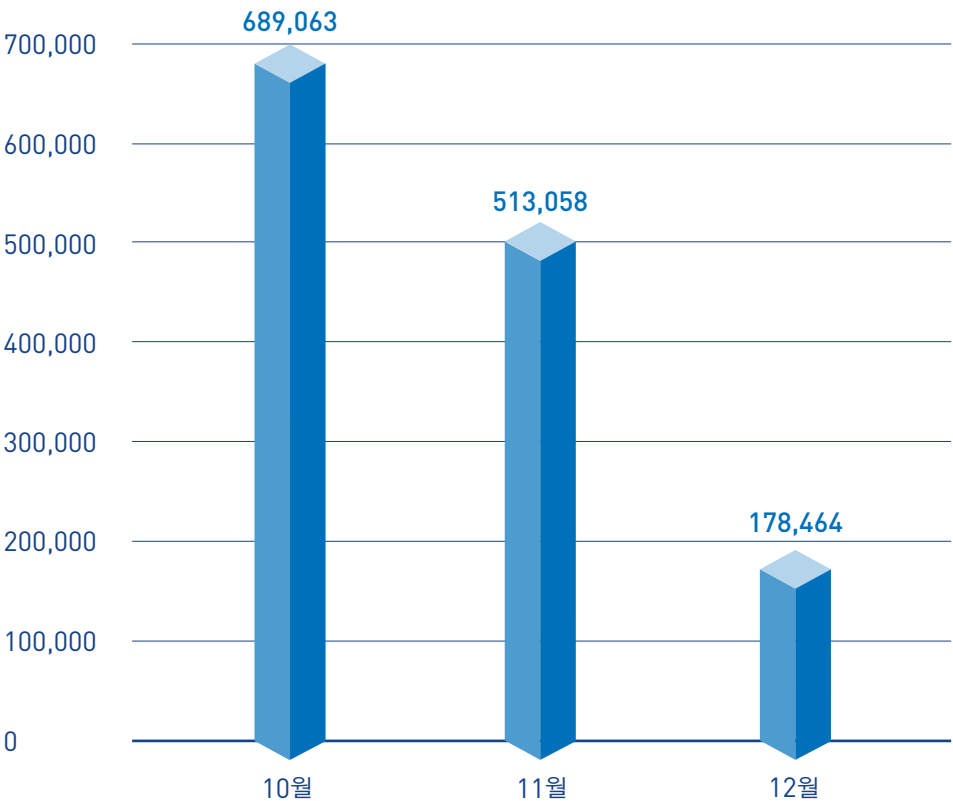


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 10월 ~ 2015년 12월)

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

03
모바일 통계

2015년 12월 한 달간 탐지된 모바일 악성코드는 17만 8,464건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이(2015년 10월 ~ 2015년 12월)

[표 1-2]는 12월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2015년 12월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	25,847
2	Android-Trojan/FakeInst	25,382
3	Android-PUP/Noico	23,665
4	Android-PUP/SmsReg	22,146
5	Android-Trojan/Opfake	7,331
6	Android-Trojan/SMSAgent	6,888
7	Android-PUP/Dowgin	5,378
8	Android-Trojan/SmsSend	4,769
9	Android-Trojan/Slocker	3,933
10	Android-Trojan/SmsSpy	3,493

2

보안 이슈
SECURITY ISSUE

01 랜섬웨어의 지역화: '오프라인(Offline)', '키메라(Chimera)'

02 중국을 겨냥한 온라인 게임 계정 탈취 악성코드

01 랜섬웨어의 지역화: '오프라인(Offline)', '키메라(Chimera)'

지난 2015년, 전 세계적으로 급증한 랜섬웨어가 최근에는 '지역화' 양상까지 보이고 있다. 기존 랜섬웨어의 감염 후 메시지들은 대부분 영어로 작성된 경우가 많았으나, 최근 발견된 일부 랜섬웨어는 감염 PC의 IP 대역을 확인하여 해당 국가의 언어로 메시지를 출력하기도 한다. 이처럼 지역화하는 랜섬웨어의 추세에 따라, 최근에는 러시아어로 제작된 '오프라인(Offline) 랜섬웨어'와 유럽 지역 사용자를 노리는 '키메라(Chimera) 랜섬웨어'가 등장했다.

1. 오프라인 랜섬웨어

오프라인 랜섬웨어는 대부분의 랜섬웨어가 사용하는 RSA 알고리즘을 사용한다. 다만 차이점은 C&C로부터 키(Key)를 전달받아 파일을 암호화하는 것이 아니라, 감염 시스템의 정보 및 암호화 대상 파일의 데이터를 기반으로 무작위로 키를 생성하여 여러 단계를 거쳐 암호화를 진행한다는 점이다. 즉, 암호화 키를 전송받기 위한 C&C 통신이 이뤄지지 않더라도 파일 암호화가 진행된다. 이러한 암호화 과정상의 특징 때문에 '오프라인 랜섬웨어'로 불리고 있다.

오프라인 랜섬웨어는 주로 해외에서 유포되고 있는 것으로 추정되었으나, 최근 국내에서도 메일에 첨부된 RAR 압축 파일을 통해 유포되는 것으로 확인되어 주의를 요한다.

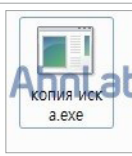


그림 2-1 | 오프라인 랜섬웨어 유포 파일(RAR 파일 압축 해제 후)

RAR 파일을 압축 해제하면 [그림 2-1]과 같이 exe 파일을 확인할 수 있으며, 해당 exe 파일을 실행하면 다음과 같이 자가 복제한 파일을 생성하고 시작 프로그램에 레지스트리를 등록한다.

표 2-1 | 생성 파일 목록

파일 생성
C:\Program Files\1C\копия иска.exe (자가복제) %TEMP%\1C\копия иска.exe (자가복제)

표 2-2 | 레지스트리 등록(시작 프로그램)

시작프로그램 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pr - C:\Program Files\1C\копия иска.exe

이후 별도 파일을 생성하여 PC별로 무작위로 생성한 아이디 및 감염 시점을 저장하고, 아래 URL로 'GET' 요청을 수행한다.

표 2-3 | 추가 파일 생성 및 URL 접속

파일 생성
C:\Program Files\1C\[랜덤파일명]
URL 접속
www.res********a.co.uk/********/in**all/in**.**p

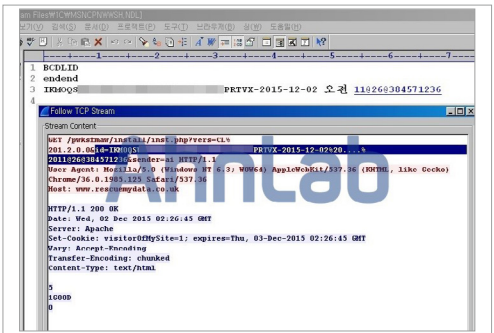


그림 2-2 | 생성된 파일(위) / URL 접속(아래)

로 작성된 메시지를 바탕화면으로 설정한다. 해당 메시지는 '너의 파일이 암호화되었고, 아래 메일 주소로 72시간 이내에 메일을 보내지 않으면 파일을 복호화 할 수 없다' 라는 의미가 담겨있다. 이 점 또한 일반적인 랜섬웨어가 비트코인 주소를 안내하고 '지불이 확인되면 복구 툴을 주겠다'라는 메시지를 보여주는 것과는 다른 오프라인 랜섬웨어만의 특징인 것을 알 수 있다.

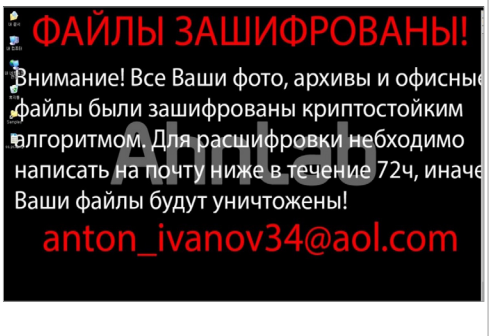


그림 2-3 | 변경된 바탕화면(감염 안내 메시지)

최종적으로 암호화된 파일은 파일명이 [표 2-4]와 같이 변경된다.

표 2-4 | 암호화된 파일명 규칙 및 예시

파일 암호화
[폴더경로]\email-[제작자 메일 주소].ver-[랜섬웨어 버전].id-[PC별 랜덤 생성 아이디]-[감염 시점].random name-[랜덤파일명].cbf
Ex) email-anton_ivanov34@aol.com.ver-CL 1.2.0.0.id-******UWY*****KLNPRTU*****GIKLO**TVX-2015-12-02 오전 11@26@384571236.randomname-FIJMOQRUVXZBDFHILNOQSUWYABEFHJ.LNP.cbf

암호화가 완료된 후에는 [그림 2-3]과 같이 러시아어

2. 키메라 랜섬웨어

러시아어로 된 감염 메시지를 출력하는 오프라인 랜섬웨어에 이어, 최근 독일을 포함한 몇몇 유럽 국가에서는 키메라(Chimera) 랜섬웨어가 유포되고 있다. 2015년 9월에 처음 발견된 키메라 랜섬웨어는 등장 초기에는 독일에서만 피해 사례가 보고되었으며, 감염 메시지 또한 독일어로 작성되어 독일을 타깃으로 한 신종 랜섬웨어로 인식되었다. 그러나 최근에 발견된 키메라 랜섬웨어의 경우, [그림 2-4]와 같이 오른쪽 상단에 영국 및 독일 국기 그림을 클릭하면 각각 영어와 독일어로 메시지를 출력하는 것으로 보아 점차 그 영향력을 키워나가는 것으로 파악된다.

그림 2-4 | 키메라(Chimera) 랜섬웨어

키메라 랜섬웨어는 다른 랜섬웨어와 유사하게 파일 암호화가 완료되면 감염 사실 및 비트 코인을 입금할 주소를 안내하는 HTML 페이지를 생성하는데, 여기서 특이한 점은 돈을 지불하지 않으면 암호화된 파일을 인터넷에 유포하겠다고 협박한다는 점이다.

(If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name)

하지만 협박 내용과는 다르게 실제로 암호화된 파일을 유출하는 기능은 존재하지 않았다.

또한 [표 2-5]와 같이 암호화 대상 파일의 확장자 종류가 많은 것으로 확인된다. 심지어 Windows 구동에 필요한 boot.ini, system.ini 파일도 암호화한다.

표 2-5 | 암호화 대상 파일 확장자

암호화 대상 파일 확장자
*.jpg, *.jpeg, *.vmx, *.txt, *.xml, *.xsl, *.vbs, *.ini, *.conf, *.config, *.msg, *.key, *.htm, *.html, .class, .java,.cs, .asp, *.aspx, *.php, *.jsp, *.bak, *.dat, *.pst, *.eml, *.sql, *.js, *.jar, *.py, *.db, *.bay, *.png, *.bmp, *.gif, *.zip, .rar, *.bin, *.ptx, *.wav, *.ram, *.mkv, *.doc, *.docx, *.rtf, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *swf, etc.

키메라 랜섬웨어에 감염되면 암호화 대상 파일 확장자 뒤에 '.crypt'가 붙으며, 이러한 광범위한 파일 확장자에 대한 암호화로 인해 일부 운영체제에서는 [그림 2-5]와 같은 경고창을 발생시키기도 한다.

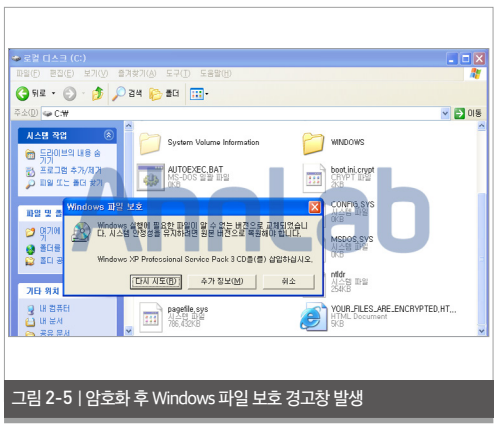


그림 2-5 | 암호화 후 Windows 파일 보호 경고창 발생

한편, 감염을 알리는 안내 페이지 하단 내용에 따라 페이지의 소스 코드를 확인해보면, [그림 2-6]과 같이 키메라 랜섬웨어 제작자는 공모자를 모집하고 있다. P2P 형식의 암호화 메일 시스템인 비트 메시지(BitMessage)를 이용해 연락을 취하라는 내용이며, 이는 추적을 피하기 위한 우회 방법으로 보인다.

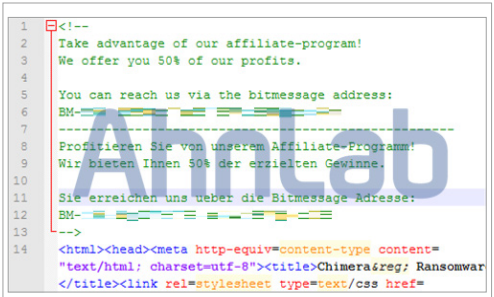


그림 2-6 | 공모자를 모집하는 키메라 랜섬웨어 제작자

현재 국내에 유포되는 랜섬웨어는 주로 침해된 웹사이트를 통해서 유포되는 사례가 많지만, 여전히 스팸 메일을 통한 랜섬웨어 감염도 이뤄지고 있으므로 이에 대한 사용자의 주의가 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.MDA (2015.12.01.04)
Trojan/Win32.Chimera (2015.11.10.07)

02
중국을 겨냥한 온라인 게임 계정 탈취 악성코드

온라인 게임 시장의 성장과 함께 게임 계정을 노리는 악성코드도 꾸준히 발견되고 있다. 게임 아이템 거래는 국내에서만 연간 1조 5,000억원대의 규모로, 활발한 거래량을 보이고 있기 때문에 악성코드 제작자들의 계정 유출 시도가 계속되고 있다. 최근에는 국내뿐만 아니라 중국 온라인 게임 시장의 규모가 점차 커지면서 중국 온라인 게임 사용자를 타깃으로 유포되는 악성코드가 발견되었다.

해당 악성코드는 중국의 한 도박 사이트를 통해 처음으로 배포되었으며, 최초 감염 시 정상 유틸리티 프로그램을 통해 주요 브라우저의 시작 페이지를 [그림 2-7]의 포털 사이트로 고정시킨다.

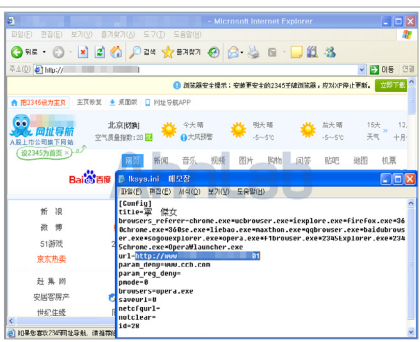


그림 2-7 | 변경된 시작 페이지와 유틸리티 설정 파일

유틸리티의 설정 파일이 [그림2-7]과 같이 지정되어 있으면 브라우저에서 설정한 시작 페이지와 무관하게 유틸리티에서 지정한 특정 사이트로 연결된다. 이렇게 사용자의 의도와는 무관한 페이지로 연결함으로써 브라우저 이용 시 불편함을 초래한다.

이후 악성코드는 GET 방식을 통해 C&C IP로 감염 PC의 운영체제 정보, MAC 주소, 컴퓨터 이름과 같은 사용자의 시스템 정보를 유출한다.

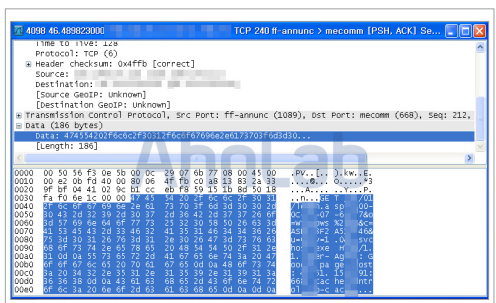


그림 2-8 | 사용자 정보 전송

이후 C&C로부터 추가 악성 파일의 다운로드 경로가 명시된 TXT 파일을 주기적으로 받아온다. 추가 다운로드 경로는 해당 TXT 파일에 의해 언제든지 변경될 수 있기 때문에 TXT 파일 내부 IP를 통한 차단은 불가능하다.

표 2-6 | 추가 악성 파일 경로

파일 생성
svchost.exe||http://1.**.**.239:777/IE-32.exe DNF.exe||http://42.**.***.191:668/down/DNF.exe LolClient.exe||http://42.**.***.191:668/down/LolClient.exe crossfire.exe||http://42.**.***.191:668/down/crossfire.exe cstrike-online.exe||http://42.**.***.191:668/down/cstrike-online.exe MapleStory.exe||http://42.**.***.191:668/down/MapleStory.exe Game.exe||http://42.**.***.191:668/down/Game.exe wow.exe||http://42.**.***.191:668/down/wow.exe wow-64.exe||http://42.**.***.191:668/down/wow-64.exe ... (중략) mir2.dat||http://42.**.***.191:668/down/7.exe mir1.dat||http://42.**.***.191:668/down/7.exe iexplore.exe||http://42.**.***.191:668/down/iexplore.exe

[표 2-6]의 내부 파일명은 중국에서 흥행 중인 주요 온라인 게임들의 실행 파일명과 일치하며, 국내에서 개발된 게임도 다수 포함되어 있다. 악성코드는 이 목록을 참고하여 실행 중인 프로세스명과 TXT 파일의 첫 번째 필드 값이 같을 경우, 실행 중인 정상 프로세스를 종료하고 동일한 파일명의 악성코드를 실행한다. 이는 계정 탈취를 위해 특정 게임에 맞는 악성코드를 실행하기 위함으로 추정된다.

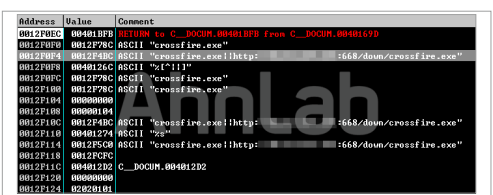


그림 2-9 | 게임 프로세스명과 비교하여 추가 악성 파일 생성

이렇게 설치된 악성코드는 각 게임에 맞는 방법으로 계정 탈취를 시도하며, 공통적으로 C&C로 연결해 공격자의 명령을 기다리게 된다.

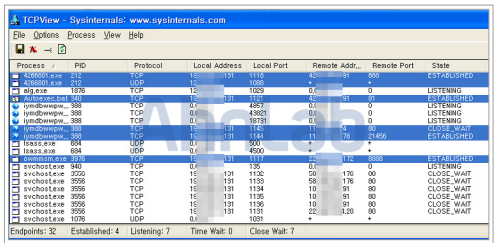


그림 2-10 | C&C 연결

온라인 게임 아이템은 인터넷상으로 편리하게 거래가 가능하고 시장이 충분히 활성화되어 있기 때문에 악성코드 제작자에게는 좋은 먹잇감일 것이다. 따라서 이를 사전에 방지하기 위해서는 현재 사용하고 있는 백신을 항상 최신 버전으로 유지하고, 게임과 관련된 불법 프로그램은 악성코드와 연관이 있을 확률이 높기 때문에 가급적 사용하지 않는 것이 좋다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Malware/Win32.Generic (2015.12.03.00)
Backdoor/Win32.Farfli (2015.12.02.02)
Adware/Win32.Agent.R169696 (2015.12.03.01)
Dropper/Win32.Crypter (2015.11.24.05)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

LNK 악성코드

LNK 악성코드

안랩에서는 이전에도 ASEC Report를 통해 LNK 악성코드에 대해 소개한 적이 있다. 여전히 LNK 악성코드 관련 사례가 지속적으로 발견되고 있는 만큼 사용자로 하여금 더욱 주의를 요한다. LNK 악성코드에 대해 다시 살펴보자.

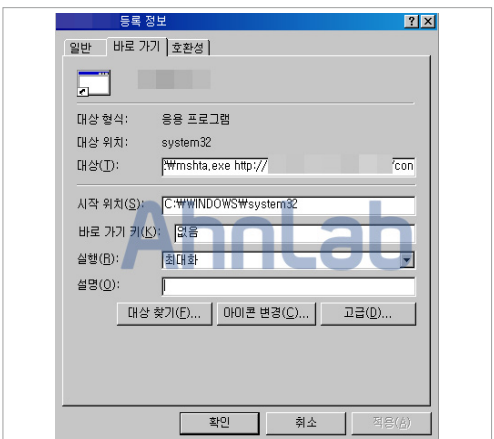


그림 3-1 | 파일 정보

LNK 악성코드를 실행하면 Windows 정상 파일인 mshta.exe를 이용하여 특정 웹사이트에 접근하고 결과적으로 '%TEMP%SysErrCheck.vbs' 경로에 악성 VBS를 생성하게 된다.

일반적으로 악성코드는 실행 시 사용자에게 정상적인 문서를 보여줌으로써 사용자가 악성 파일임을 눈치채지 못하게 한다. LNK 악성코드 또한 악성 VBS가 실행되면 정상적인 문서 파일을 받아와 사용자에게 보여줌으로써 사용자를 안심시킨다. 이러한 정상 문서들은 이미 감염된 다른 PC에서 유출되어 공격에 사용된다.

악성 VBS 파일은 정상 문서와 함께 의심스러운 그림 파일도 함께 다운받아 오는데, [그림 3-2]를 보면 그림 파일에 악성 코드가 숨겨져 있음을 알 수 있다.

그림 3-2 | 그림 파일에 숨겨져 있는 악성코드 복호화 전(위)/ 복호화 후(아래)

VBS 파일에서 그림 파일의 특정 지점으로 이동한 후 0x55로 XOR하여 악성코드를 복호화한 다음 파일을 생성하고 실행한다. 이 악성코드는 단지 추가 악성코드를 다운로드하고 실행하기 위한 다운로더이며, [표 3-1]의 동작을 한다.

표 3-1 | 다운로더 행위

1. http://CNC서버주소/update2014.php 와의 통신으로 서버가 살아 있는지 확인
2. http://CNC서버주소/download2014.htm에서 인코딩되어 있는 악성 파일을 받아 옴
3. 2.의 결과에 따라 다음 주소에 요청을 남김으로써 서버에 기록
3-1. 다운로드 성공 시 http://CNC서버주소/DownLoadSuccess.php 접속
3-2. 추가 파일 다운로드 실패 시 http://CNC서버주소/DownLoadFail.php 접속
3-3. 다운로드 받았으나 PE 복구 실패 시 http://CNC서버주소/ExeFail.php

download2014.htm에서 받아오는 파일은 인코딩되어 있는데, base64로 디코딩한 후 0x19로 XOR하면 정상적인 PE 형태로 복호화된다.

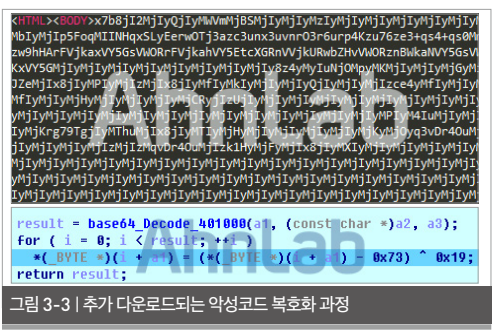


그림 3-3 | 추가 다운로드되는 악성코드 복호화 과정

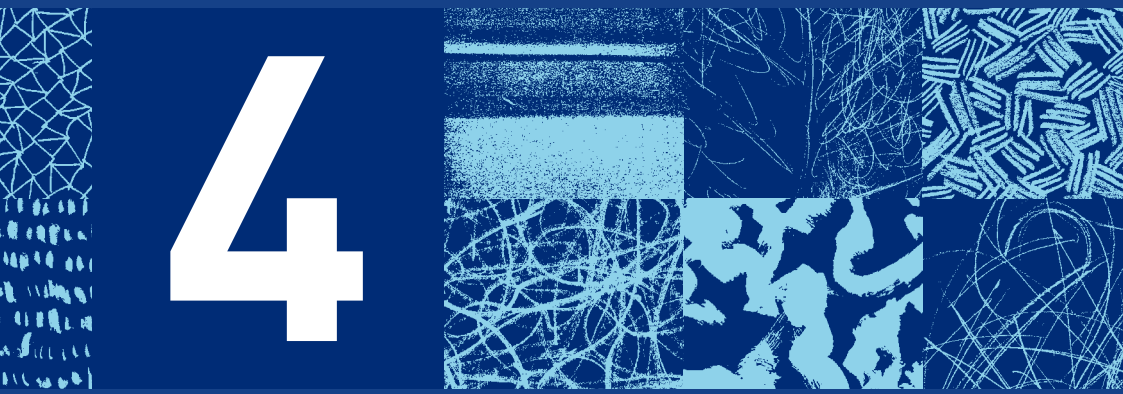
다운로드된 추가 악성코드는 '%Temp%[랜덤숫자]_res.tmp'에 저장된 후 파일의 시간 정보를 특정 시간으로 변경하고 시작 프로그램 경로로 이동되어 Windows가 다시 시작할 때 실행된다. 해당 악성코드는 컴퓨터 정보 수집, 파일 다운로드, 업로드, 추가 파일 실행 등의 기능을 하는 백도어(Backdoor) 역할을 수행하며 사용자의 컴퓨터를 장악한다.

이러한 악성코드에 대비하려면 확인되지 않은 첨부파일은 함부로 실행하지 않아야 하며, 주기적인 정밀 검사를 수행하고 백신을 최신 버전으로 유지하는 것이 중요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

LNK/Downloader (2015.12.03.08)
VBS/Downloader (2015.12.03.08)
Trojan/Win32.Lnkdoor (2015.12.05.00)



4

연간 위협 동향

2015 ANNUAL REPORT

01 2015년을 뒤흔든 보안 위협 Top 5

02 2016년 보안 위협 전망

01
2015년 보안 위협 결산

2015년을 뒤흔든 보안 위협 Top 5

1. 깨어난 랜섬웨어의 광풍

랜섬웨어는 국내뿐만 아니라 전 세계적으로 보안 분야의 가장 큰 이슈였다. 북미 지역 및 유럽 등을 중심으로 폭발적인 증가 추세를 보인 가운데, 국내에서는 지난 2015년 4월 국내 유명 커뮤니티 사이트를 통해 한글화된 크립토락커가 대량 유포된 때를 기점으로 랜섬웨어가 급격하게 증가하고 있다.

기존에는 주로 문서 파일(doc, ppt 등)과 이미지 파일(jpeg 등)을 암호화했으나 최근에는 실행 파일(exe)을 포함한 140여 개의 확장자가 암호화 대상이 되었다. 또한, 데이터를 암호화하는 방식에서 더 나아가 화면 잠금을 통해 PC 구동 자체를 불가능하게 하는 랜섬웨어도 등장했다.

랜섬웨어의 '지역화' 양상도 나타났다. 북미와 유럽 지역에서는 비트크립트(BitCrypt)와 코인볼트(CoinValut)가, 러시아 및 터키 등 동유럽 지역에서는 트롤데시(TrolDesh) 등의 랜섬웨어가 큰 피해를 입혔다. 반면 국내에서는 크립토락커, 크립토월(CryptoWall), 테슬라크립트(TaslaCrypt), 나부커(Nabucur) 등의 랜섬웨어 감염 빈도가 높았다.

2. 결국은 '돈', 계속되는 금융 정보 위협

2015년에도 금융 정보를 노린 악성코드가 기승을 부렸다. 전 세계 1,000여 개 은행과 기업을 노리며 악명을 떨쳤던 다이어(Dyre) 악성코드가 올해 초 국내 은행을 공격 대상에 포함해 국내 금융 업계를 긴장시켰다. 최근에는 Windows 10과 엣지 브라우저(Edge Browser) 등 최신 운영체제와 브라우저에서도 정보를 탈취하는 등 더욱 진화하는 양상을 보인다. 파밍(Pharming) 사이트로 사용자를 유도해 금융 정보를 탈취하는 뱅키(Banki)류의 악성코드도 2015년 하반기에는 유포 방식을 바꾸는 등 여전히 기승을 부리고 있다.

금융 정보를 탈취하는 악성코드의 공격 대상은 은행만이 아니다. POS(Point of Sale) 시스템을 통해 카드 정보를 유출하는 POS 악성코드가 2015년 들어 다시 증가하기 시작한 것이다. 체리피커(Cherry Picker), 모드포스(ModPOS) 등이 2015년 등장한 대표적인 POS 악성코드다. POS 악성코드의 위험성은 지난 2013년 말 해외 대형 마트에서 대규모 카드 정보 유출 사건이 발생하면서 수면 위로 떠올랐다. 국내에서도 POS 단말기를 통한 카드 정보 유출 및 이에 따른 금전적 피해가 발생하며 POS 위협이 나날이 심화되고 있다.

3. 웹 익스플로잇 툴킷의 역습

랜섬웨어를 비롯해 2015년을 뒤흔든 수많은 보안 위협의 뒤에는 웹 익스플로잇 툴킷(Web Exploit ToolKit)이 있었다. 게다가 이전보다 훨씬 정교한 방식으로 존재감을 드러내고 있다.

'웹 익스플로잇 툴킷'은 다수의 취약점을 악용해 사용자 PC에 악성코드를 감염시키기 위한 공격 도구로, 공격자들은 이를 이용해 악성코드를 손쉽게 제작하고 유포한다. 2015년에 맹위를 떨친 대표적인 웹 익스플로잇 툴킷은 '앵글러(Angler) 툴킷'이다. 지난 4월 국내 유명 커뮤니티에서 유포된 랜섬웨어 공격의 배후에도 바로 이 앵글러 툴킷이 있었다.

공격자들은 웹 익스플로잇 툴킷을 이용한 악성코드의 유포 경로 추적을 더욱 어렵게 만들기 위해 다양한 블로그 제작툴이나 콘텐츠 관리 시스템 등을 이용하거나 동적 콘텐츠를 생성하는 광고 사이트를 악성코드 배포에 이용하는 방식인 '멀버타이징(Malvertising)' 기법을 이용하기도 했다. 또한 백신의 탐지를 우회하려는 시도도 더욱 정교화되어 웹 익스플로잇 툴킷은 더욱 심각한 위협으로 자리잡았다.

4. 애드웨어, 모바일 환경으로 영역 확장

과다한 광고 노출 등으로 사용자 불편을 야기하는 '애드웨어(adware)'가 모바일 환경으로 영역을 확장했다.

2015년 발견된 모바일 애드웨어 수가 전년 대비 약 2.5배가량 증가했다. 모바일 애드웨어는 개인 정보 수집, 과도한 광고 노출, 앱 바꿔치기 등 스마트폰 이용의 불편함을 넘어 악의적인 행위로 피해를 야기하고 있다. 특히 최신 모바일 애드웨어는 다른 앱을 사칭하거나 루트 권한을 획득해 삭제를 방해하는 등 한층 교묘해진 수법으로 스마트폰 사용자를 노리고 있다.

그 밖에 2015년 모바일 위협은 전년과 비슷하거나 다소 감소하는 추세를 보였다. 2012년 이후 매년 2배 이상 급증세를 보이던 모바일 뱅킹 악성코드는 전년도와 비슷한 수를 유지했고, 모바일 악성코드의 유포 방법으로 이용되던 스미싱은 2015년 하반기 들어 감소 추세를 보였다. 이는 미래부, KISA(Korea Internet & Security Agency, 한국인터넷진흥원), 경찰청 등 관련 기관의 적극적인 스미싱 메시지 및 네트워크 차단 노력, 보안 업체 및 이동통신사 등 민간업체들의 이용자 보호 조치, 언론 보도 및 캠페인을 통한 국민 보안 의식 증진 등에 의한 결과로 풀이된다.

5. 공유기, IoT 등 '연결'을 노리는 위협의 대두

2014년에 이어 2015년 초부터 국내 유명 제작사의 유 • 무선 공유기의 취약점을 노린 해킹 시도가 지속적으로 발견됐다. 공유기의 취약점을 이용해 관리 권한을 획득하면 공유기와 연결된 모바일 기기나 PC를 동시에 공격할 수 있어 위험도가 높다.

네트워크에 연결된 기기에 대한 보안 위협은 공유기뿐 아니라 사물 인터넷까지 공격 범위를 확장하고 있다. 최근 각종 웨어러블 기기(Wearable device) 등 개인용 사물 인터넷 기기(Internet of Things)가 증가함에 따라 이들 기기의 보안에 대한 우려도 커지고 있다. 대표적인 사물 인터넷 기기인 IP 카메라, NAS(Network Attached Storage), CCTV 등

은 일반 컴퓨터와 유사한 운영체제를 가지고 있어 공격자들이 쉽게 접근할 수 있다. 특히 이러한 기기들은 네트워크에 항상 연결되어 있는 반면 아직 마땅한 보안 대책은 없는 형편이다. 인터넷 공유기나 사물 인터넷 관련 기기 등 항상 '연결'된 상태의 기기를 안전하게 이용하려면 각 제조사에서 제공하는 펌웨어 업데이트나 관리 비밀번호 수시 변경 등의 사용자 노력이 중요하다.

02
2016년 보안 위협 전망

2016년을 장악할 보안 위협 Top 5

1. 랜섬웨어의 지속적인 고도화

랜섬웨어 위협은 2016년에 더욱 거세질 전망이다. 랜섬웨어의 암호화 대상 확대, 화면 잠금 등 사용자의 조치를 방해하는 기능 추가 등 지속적인 진화가 예상된다. 특히 안랩을 비롯한 보안 업체들이 랜섬웨어 진단 및 차단 기능을 강화함에 따라 보안 제품의 탐지를 우회하거나 방해하는 등의 고도화된 랜섬웨어가 등장할 것으로 예측된다.

모바일 랜섬웨어가 국내에 상륙할 가능성도 점쳐진

다. 아직 국내에서는 모바일 랜섬웨어 감염이 확인된 바 없으며, 대부분의 모바일 랜섬웨어는 영어로 제작되어 있다. 그러나 PC 랜섬웨어가 그랬듯, 향후 한글화된 모바일 랜섬웨어가 등장해 국내 스마트폰 사용자들에게 막대한 피해를 준다 해도 전혀 이상할 것이 없다. 모바일 랜섬웨어가 국내 스마트폰 사용자를 노리기 시작하면 지난 2014년 사회적 화두가 됐던 스미싱 악성코드와는 비교할 수 없을 정도의 피해를 야기할 수도 있다.

한편 안드로이드를 대상으로 하는 랜섬웨어 수는 2014년 2,220건에서 2015년 27,845건으로, 1년새 12배가 넘게 증가했다. 2016년에도 모바일 랜섬웨어 변형은 계속해서 증가할 것으로 보인다.

2. 사라지지 않는 사이버 테러 및 국가 기반 시설 위협

지난 2015년 연말 발생한 '파리 테러' 사건은 전 세계를 충격으로 몰아넣었다. 종교적 • 이념적 갈등에 따른 국가 간의 대립은 사이버 세계에서도 별반 다르지 않다. 과거에는 테러가 물리적인 파괴에 국한됐던 것에 반해 최근 인터넷을 통한 테러리스트들의 이념 선전 및 정보 수집, 적대국 도 • 감청과 정보 유출 등의 테러는 이미 사이버 환경에 깊숙이 침투해 있다.

일반 대중에게 공포감을 조성하는 것이 테러의 목적이라는 점에서 국가 기반 시설을 노린 고도화된 지능형 위협인 APT(Advanced Persistent Threat)의 가능성도 배제할 수 없다. 물론 국가 기반 시설은 다수의 보안 시스템으로 겹겹이 보호되고 있을 뿐만 아니라 대부분 직접 인터넷에 연결하지 않는 것을 원칙으로 폐쇄망 환경에서 운영되고 있어 비교적 위협에 노출될 가능성이 작다. 그러나 이란 부셰르 핵발전소의 스턱스넷(Stuxnet) 감염, 일본 핵 발전소 정보 유출 사건, 그리고 최근의 미국 뉴욕 댐 통제 시스템 보안 침해 등 국가기반 시설을 노린 사이버 공격 사례가 국내 • 외에 지속적으로 발생하고 있다. 정치적 갈등과 장기적인 세계 경기 침체의 영향으로 국제 정세가 급변함에 따라 국가 기반 시설 보안의 중요성도 더욱 강조된다.

3. 웹 브라우저부터 클라우드와 가상 환경까지 노리는 취약점 공격

2016년에는 인기 있는 소프트웨어의 취약점을 활용한 공격이 더욱 기승을 부릴 것으로 보인다.

마이크로소프트(Microsoft)는 2016년 1월 12일을 기점으로 자사 웹 브라우저인 인터넷 익스플로러(Internet Explorer, 이하 IE)의 최신 버전을 제외한 이전 버전에 대한 지원을 종료하겠다고 밝혔다. 즉, 최신 버전이 아닌 구 버전의 IE에서 새로운 취약점이 발견되더라도 2016년 1월 12일 이후에는 해당 취약점에 대한 패치가 제공되지 않기 때문에, 이를 노린 공격이 증가할 것으로 예상된다.

지난해에는 국내에서 많이 사용 중인 문서 편집 프로그램이나 기타 프로그램의 취약점도 다수 발견됐다. 대중적인 소프트웨어의 신규 취약점을 이용한 공격은 비교적 사용자의 의심을 쉽게 피할 수 있어 앞으로도 주요 공격 방식으로 사용될 것이 분명하다. 2016년에는 단순 취약점 보고를 넘어 취약점 이용 공격으로

인한 구체적인 피해 사례가 발생할 것으로 예상된다.

또한 2015년에는 가상 환경 시스템에서 발생 가능한 '베놈(VENOM, Virtualized Environment Neglected Operations Manipulation)' 취약점을 비롯해 특정 가상화 솔루션의 임의 코드 실행 취약점 등이 발견됐다. 최근 다수의 국내 기업에서 클라우드 또는 가상화 인프라 도입을 검토함에 따라 이들 환경에 대한 보안 위협도 구체화될 것으로 보인다.

4. 사물인터넷(IoT), 스마트홈을 둘러싼 위협의 현실화

IT 기술과 기기가 빠른 속도로 발전함에 따라 이제 사이버 위협의 범위는 PC를 벗어나 광범위하게 확대되고 있다. 사실상 컴퓨터와 성능과 기능 면에서 큰 차이가 없는 사물인터넷 기기가 속속 등장하는 등 인터넷에 연결되는 기기가 늘어날수록 새로운 사이버 위협 또한 계속해서 증가할 전망이다.

일반 가정에서도 흔히 볼 수 있는 무선공유기를 비롯해 가정용 전원 컨트롤, 난방 제품 제어시스템 등 스마트홈 기술이 발전하면서 이에 대한 보안 위협의 고려가 시급하다. 이 밖에도 현재 각국에서 유효성 검증과 관련 법제 마련이 한창인 드론(Drone)이나 인터넷에 연결되어 구동되는 자동차(Connected Car), 이른바 스마트카에 대한 위협 또한 머지않아 현실화될 전망이다.

5. 새로운 금융 환경을 노리는 위협의 등장

금융 정보, 금융 시스템은 언제나 사이버 위협의 핵심 타깃이었으며, 금융 환경이 온라인화될수록 위협의 정도 또한 심화되었다. 2016년에는 인터넷 전문 은행이 출범함에 따라 이를 둘러싼 보안 위협이 증가할 전망이다.

인터넷 전문 은행은 오프라인 영업점이 존재하지 않기 때문에 본인 확인 시 비대면 실명 확인이 필수불가결하다. 이에 실명 확인 절차부터 중요한 보안 이슈로 떠오르고 있다. 또한, 스마트폰을 이용한 모바일 거래 위협에 대한 우려도 크다. 인터넷 전문 은행이 출범하면 스마트폰을 이용한 모바일 거래가 많아질 수밖에 없다. 지난 몇 년간 소액 결제나 뱅쿤 등 모바일 악성코드를 통한 금융 정보 탈취 피해가 빈번하게 발생하고 있으며 스마트폰 사용자를 노린 파밍 공격 등도 증가하고 있는 만큼, 인터넷 전문 은행 도입과 관련해 모바일 금융 거래의 보안 강화가 시급한 시점이다.

AhnLab

ASEC REPORT

VOL.72
December, 2015

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