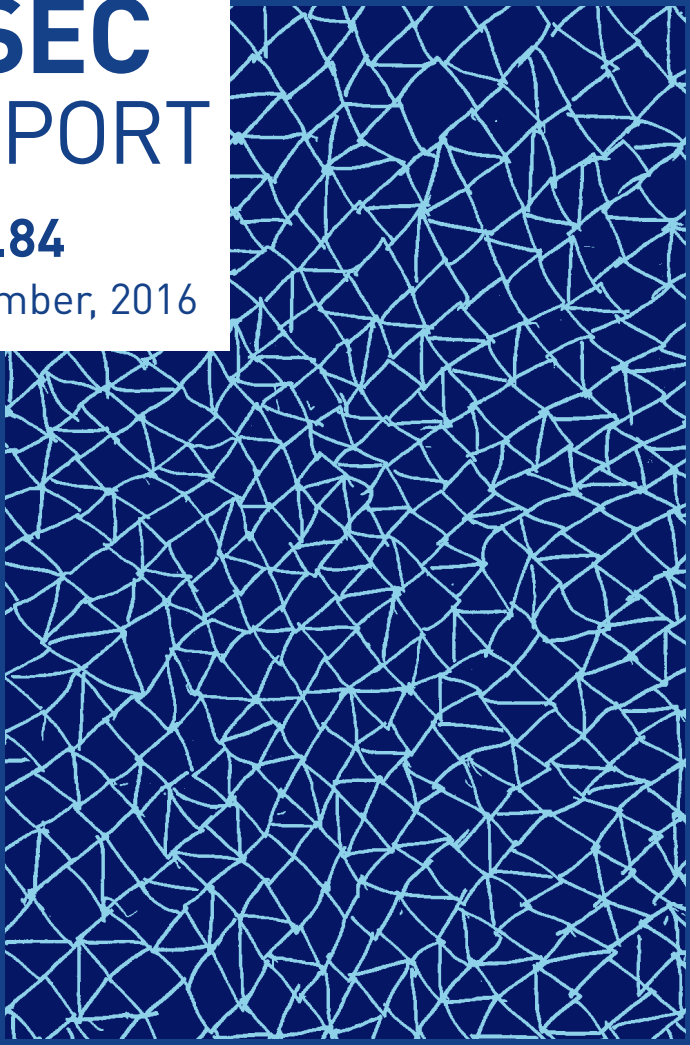
Security Trend

ASEC REPORT

VOL.84

December, 2016



AhnLab

ASEC REPORT

VOL.84 December, 2016

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.

2016년 12월 보안 동향

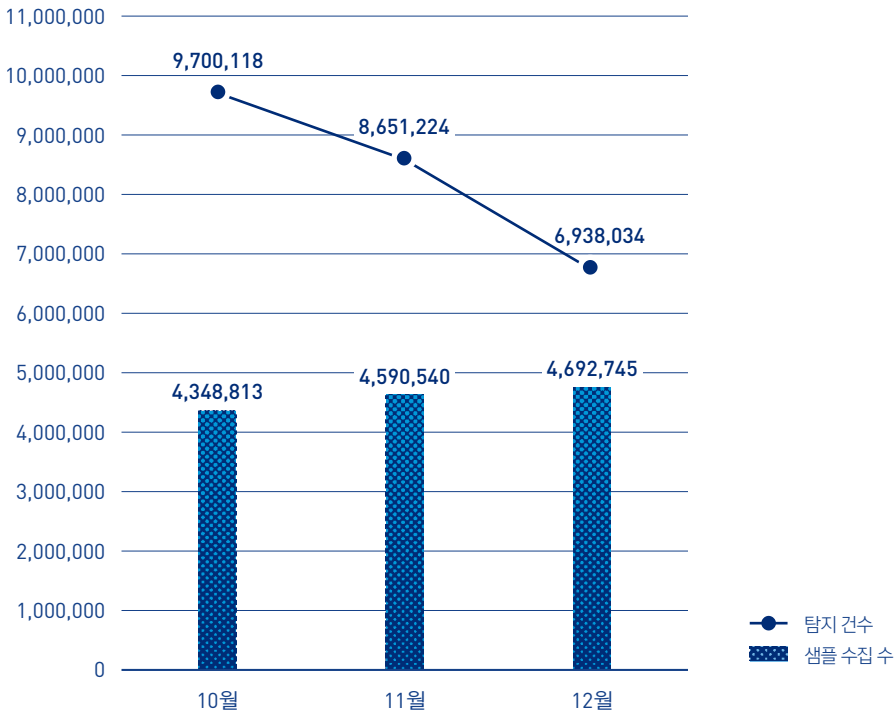
Table of Contents

1

보안 통계
STATISTICS

01 악성코드 통계

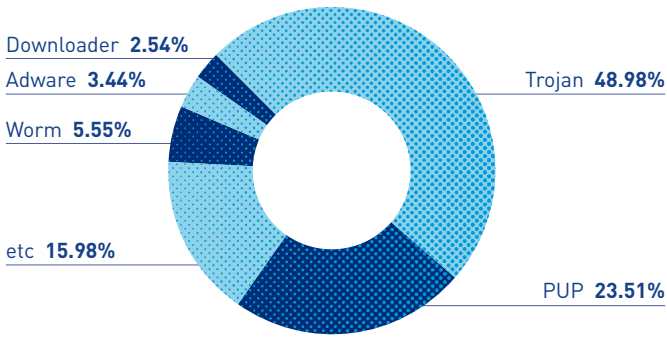
ASEC이 집계한 바에 따르면, 2016년 12월 한 달간 탐지된 악성코드 수는 693만 8,034건으로 나타났다. 이는 전월 865만 1,224건에 비해 171만 3,190건 감소한 수치다. 한편 12월에 수집된 악성코드 샘플 수는 469만 2,745건이다.



[그림 1-1] 악성코드 추이(2016년 10월~2016년 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 2016년 12월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 48.98%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 23.51%, 웜(Worm)이 5.55%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 12월 주요 악성코드 유형

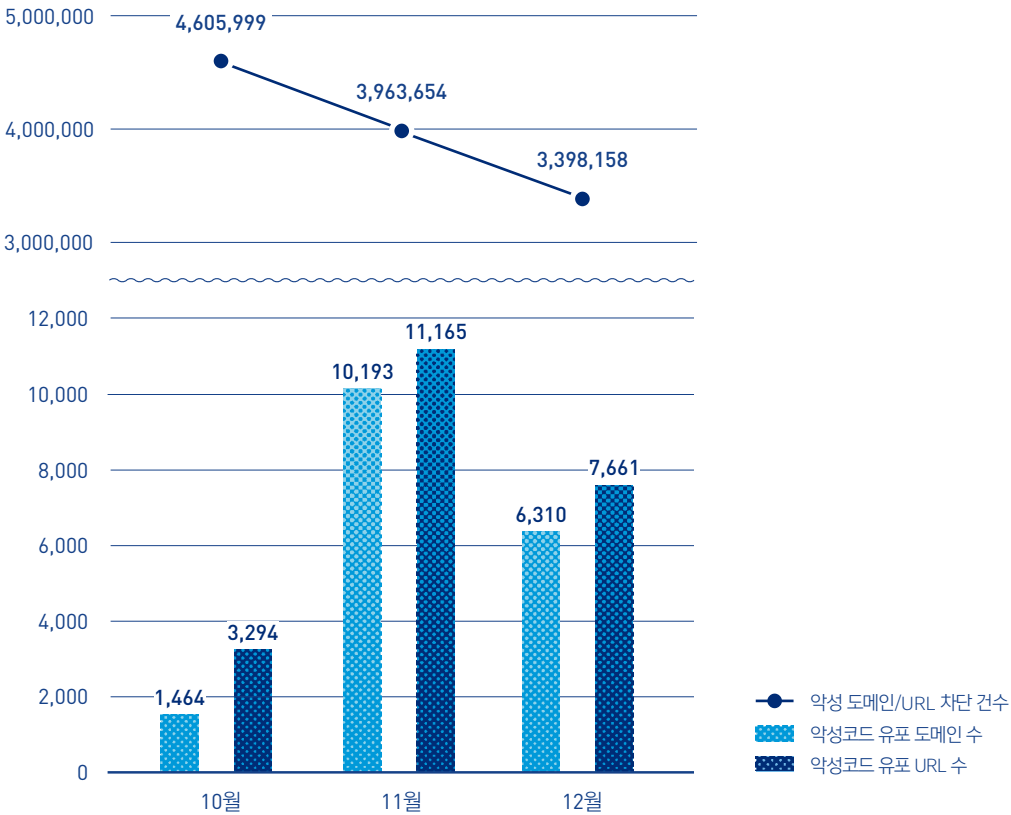
[표 1-1]은 12월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Worm/Win32.IRCBot이 총 31만 7,192로 가장 많이 탐지되었고, Trojan/Win32.Starter가 27만 7,706건으로 그 뒤를 이었다.

[표 1-1] 2016년 12월 주요 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Worm/Win32.IRCBot	317,192
2	Trojan/Win32.Starter	277,706
3	Trojan/Win32.Banki	159,981
4	Malware/Win32.Generic	154,620
5	Unwanted/Win32.HackTool	115,199
6	Trojan/Win32.Cerber	104,462
7	Trojan/Win32.Downloader	91,232
8	Trojan/Win32.Agent	80,939
9	Trojan/Win32.Nitol	74,782
10	Trojan/Win32.Neshta	69,072

02
웹 통계

2016년 12월에 악성코드 유포지로 악용된 도메인은 6,310개, URL은 7,661개로 집계됐다([그림 1-3]). 또한 12월의 악성 도메인 및 URL 차단 건수는 총 339만 8,158건이다.

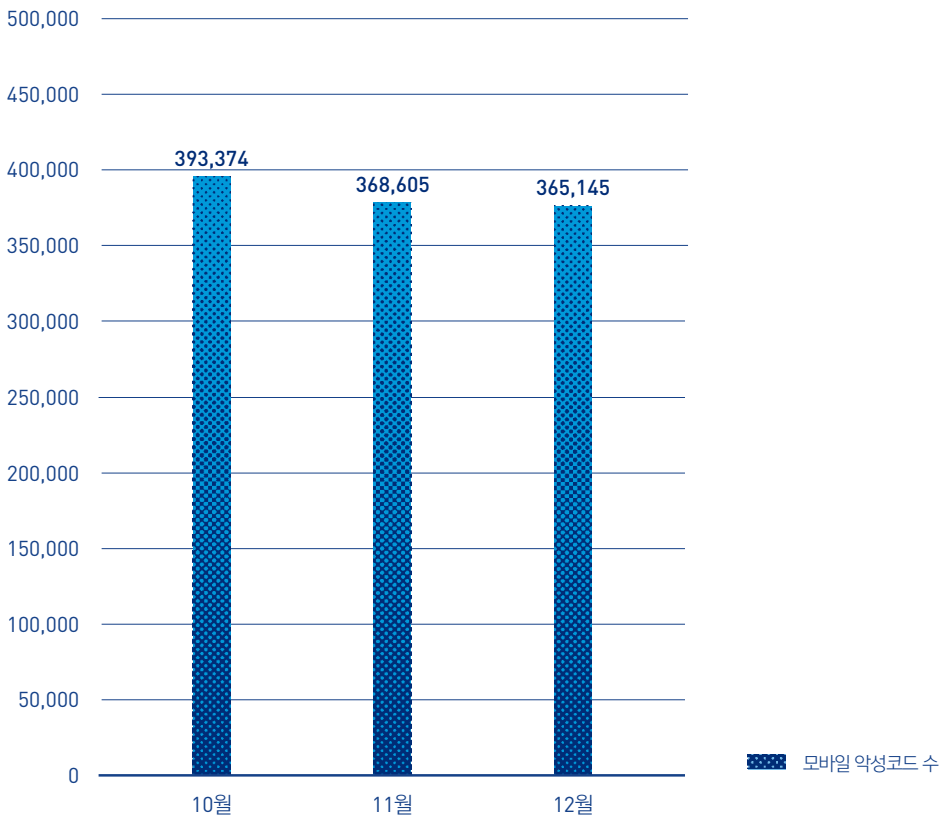


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 10월~2016년 12월)

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

03
모바일 통계

2016년 12월 한 달간 탐지된 모바일 악성코드는 36만 5,145건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이

[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] 2016년 12월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	57,515
2	Android-PUP/Baogifter	34,831
3	Android-PUP/Shedun	31,098
4	Android-Trojan/SmsSpy	25,744
5	Android-PUP/SmsReg	18,214
6	Android-PUP/Agent	18,192
7	Android-Trojan/Jimo	15,891
8	Android-Trojan/SmsSend	14,143
9	Android-Trojan/Agent	12,704
10	Android-Trojan/Slocker	12,050

2

보안 이슈
SECURITY ISSUE

01 개인 블로그를 통해 유포되는 악성코드 주의!

개인 블로그를 이용해 악성코드를 유포하는 사례가 지속적으로 발견되고 있다. 특히 유명 포털 사이트의 서비스로 운영되는 블로그의 경우, 포털 검색을 통해 유입된 다수의 사용자가 피해를 입을 수 있어 주의가 요구된다.

그림 2-1 | 악성 파일을 유포한 블로그

[그림 2-1]은 최근 악성 파일을 유포한 블로그 게시물이다.

그림 2-2 | 악성 파일 다운로드 유도

[그림 2-2]와 같이 언뜻 보면 최신 가요 관련 포스팅 같지만, 음원 공유를 빌미로 악성코드를 포함한 파일을 유포하고 있다. 음악 파일은 'mp3'나 'wav' 확장자를 갖는 것이 일반적이다. 하지만 해당 파일은 실행 가능한 'exe' 확장자를 갖고 있으며, 실행 시 [그림 2-3]과 같은 화면이 나타난다.

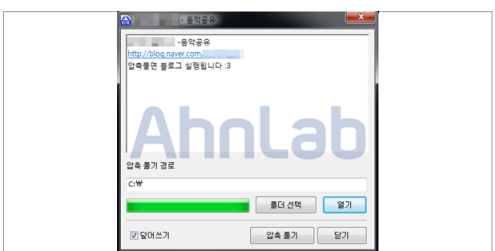


그림 2-3 | 악성파일 실행 화면

압축 풀기 클릭 시 사용자가 지정한 경로에 음원 파일이 생성되지만, 사용자 모르게 로컬 드라이브와 system32 폴더에 각각 악성코드가 생성되어 동작한다.

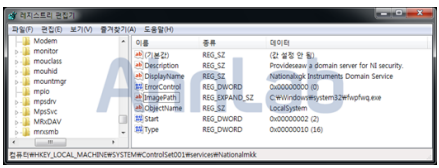


그림 2-4 | 서비스에 등록된 악성코드

이렇게 생성된 악성코드는 'Nationalxgk Instruments Domain Service'라는 이름으로 서비스에 등록되어 자동 실행되며, 방화벽 정책을 해제한 후 C&C 서버와의 연결을 시도한다.

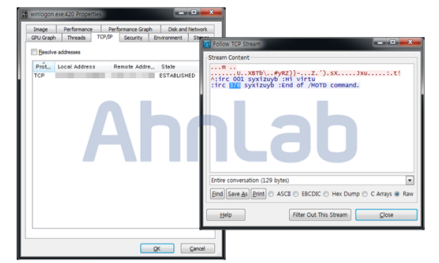


그림 2-5 | C&C 서버와 통신

C&C 서버와 연결되면 IRC를 통해 공격자로부터 명령을 전달 받아 악성 행위를 수행하게 된다.

누구나 접할 수 있는 블로그마저 악성코드 유포에 악용되고 있는 만큼, 출처가 불분명한 파일의 다운로드 및 실행에 주의하는 습관이 필요하다. 블로그 외에도 토렌트와 같은 파일 공유 사이트를 통해 악성코드가 왕왕 유포되고 있는 바, 인터넷에서 파일을 다운로드할 때는 파일의 확장자가 받은 파일과 무관한 파일은 아닌지 반드시 확인해야 한다. 또한 악성코드 감염 예방과 올바른 인터넷 문화를 위해 가급적 불법 다운로드는 지양하고 정식으로 유통되는 곳에서 파일을 다운로드하길 권장한다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Dropper/Win32.Agent (2016.12.28.04)

Trojan/Win32.Scar (2016.11.21.07)

02 njRAT를 활용한 백도어 악성코드

RAT(Remote Access Tool)는 원격 제어 툴로, 악성코드 제작자들이 많이 활용하는 것 중 하나다. 2015년에 유행했었던 njRAT을 활용한 악성코드가 다시 발견되어 사용자들의 주의가 필요하다.

해당 악성코드는 특정 사이트를 통해 유포되었으며, [그림 2-6]과 같다.

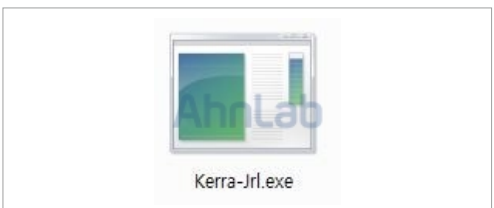


그림 2-6 | njRAT을 활용한 백도어 악성코드

악성코드 실행 시 [표 2-1]과 같이 svhost.exe로 자가 복제와 동시에 실행된다.

표 2-1 | Temp 및 시작 프로그램 경로에 생성된 악성코드

C:\Users\[사용자계정]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\aede67dbcafe22407c4b0dbfe6bbae94.exe C:\Users\[사용자계정]\AppData\Local\Temp\svhost.exe

컴퓨터를 다시 시작해도 악성코드가 실행될 수 있도록 %temp% 경로에 생성된 svhost.exe를 [그림 2-7]과 같이 시작프로그램에 등록한다.

그림 2-7 | 시작 프로그램에 등록된 악성코드

실행된 악성코드는 [그림 2-8]과 같은 정보를 C&C 서버로 전송한다.

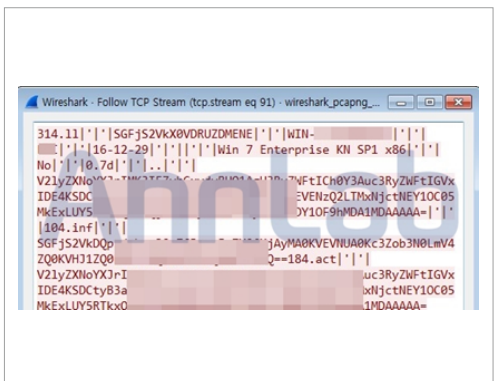


그림 2-8 | C&C 서버에 전송하는 정보

일부 데이터는 base64로 암호화되어 있다. 악성코드의 바이너리 및 전송 데이터를 분석한 결과, [표 2-2]와 같은 정보를 전송하는 것이 확인됐다.

표 2-2 | 유출하는 데이터 정보 리스트

1. 컴퓨터 이름
2. 사용자 이름
3. OS 정보
4. njRAT 버전(악성코드 내 하드코딩되어 있음)
5. CAM 유무
6. 실행 중인 프로세스 정보 등등

실행된 svhost.exe는 특정 포트를 통해 C&C 서버와 통신하기 위해 연결되어 있다.

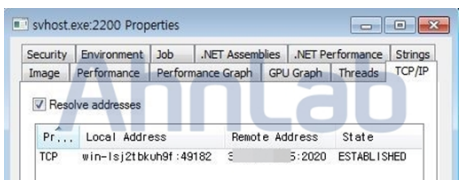


그림 2-9 | C&C 서버와 연결 중인 악성코드

공격자의 명령에 따라 악성 행위를 수행할 것으로 보이나, 분석 당시에는 별다른 동작을 하지 않았다.

대부분의 악성코드는 취약한 웹 사이트를 통해 유포되고 있다. 최신 버전이 아닌 소프트웨어를 사용하는 경우, 취약점을 이용한 악성코드에 감염될 가능성이 높다. 그렇기 때문에 반드시 사용하는 소프트웨어 및 백신 제품을 최신 버전으로 유지하고, 업무상 필요하지 않은 사이트에 접근하지 않는 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Win-Trojan/Zbot.24064 (2016.12.20.07)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

파일과 MBR을 동시에 암호화하는
골든아이 랜섬웨어

파일과 MBR을 동시에 암호화하는 골든아이 랜섬웨어

2016년 3월과 5월에 발견됐던 페트야(Petya), 미샤(Mischa) 랜섬웨어의 변형인 골든아이(GoldenEye) 랜섬웨어가 등장했다. 페트야 랜섬웨어는 MBR만 암호화하고 미샤 랜섬웨어는 파일과 MBR 중 선택적으로 암호화를 진행하는데, 이번에 발견된 골든아이 랜섬웨어는 파일과 MBR을 동시에 암호화하기 때문에 더욱 주의해야 한다.

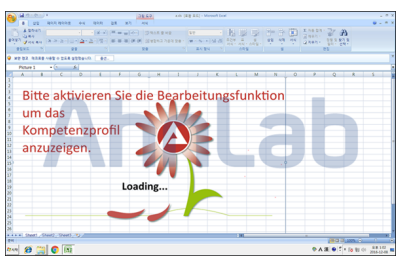


그림 3-1 | 악성 매크로를 포함하고 있는 엑셀 파일

골든아이 랜섬웨어는 독일어를 사용하는 사람들을 주 타깃으로 하여 가짜 이력서로 위장한 스팸 메일을 통해 유포되었다. 해당 스팸 메일에는 가짜 이력서 PDF 파일과 악성 매크로를 포함한 엑셀 파일이 포함되어 있다. 엑셀 파일을 열면 독일어 문장과 함께 매크로를 사용할 수 없다는 메시지가 출력된다. 해당 독일어는 자세한 내용을 확인하기 위해 매크로 실행 기능을 활성화하라는 내용이다. 매크로 실행 기능을 활성화하면, 악성 매크로가 실행되면서 랜섬웨어 감염이 진행된다. 해당 매크로가 실행되면 [표 3-1]과 같이 파일을 생성한 다음 실행한다.

표 3-1 | 악성 매크로 실행 시 생성되는 실행 파일 경로

C:\Users\사용자계정\AppData\Local\Temp\radA3ACA.exe
C:\Users\사용자계정\AppData\Roaming\{db864363-a5b3-4623-a8cf-fa919cd7b079}\java.exe

```
var fso = new ActiveXObject('Scripting.FileSystemObject');
var tmp_path = fso.GetSpecialFolder(2) + '\\' + fso.GetTempName();
tmp_path = tmp_path.replace('.tmp', '.exe');
var stream = new ActiveXObject('ADODB.Stream');
stream.Open();
stream.Type = 1;
stream.Position = 0;
var xmlObj = new ActiveXObject('MSXml2.DOMDocument');
var docElement = xmlObj.createElement('Base64Data');
docElement.dataType = 'bin.base64';
docElement.text = '';
docElement.text =
'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
m9nnmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAA83tKNeL+83n1/vN
v3m+/vN54v73egL+83uNUct55v7ze41Rz3nm/vN7aeHXeeb+83tp4cN55v7zeUmljaHi/vN4A
L3KwFEAAAAAAAAAAOAAAgELAQsAAPgCAAAmAQAAAAAAJMQAAAAQAAAAEAMAAABAAAAQAAAAAg
```

그림 3-2 | 실행 파일을 생성하고 나서 실행되는 악성 매크로

해당 실행 파일이 실행되면 먼저 랜섬 노트를 생성하고 파일 암호화를 진행한다. 랜섬 노트는 [표 3-2] 경로에 생성된다. 주로 사용자 계정, 바탕화면, 다운로드, 내 문서 경로와 공용 계정 경로다. 랜섬 노트는 골든아이 랜섬웨어의 감염 사실을 알려주고, 복구 결제를 위한 토르(Tor) 홈페이지 주소를 안내한다.

표 3-2 | 생성된 실행 파일에 의해 생성되는 랜섬 노트 경로

C:\Users\사용자계정\YOUR_FILES_ARE_ENCRYPTED.TXT C:\Users\사용자계정\Desktop\YOUR_FILES_ARE_ENCRYPTED.TXT C:\Users\사용자계정\Downloads\YOUR_FILES_ARE_ENCRYPTED.TXT C:\Users\사용자계정\Documents\YOUR_FILES_ARE_ENCRYPTED.TXT C:\Users\Public\YOUR_FILES_ARE_ENCRYPTED.TXT

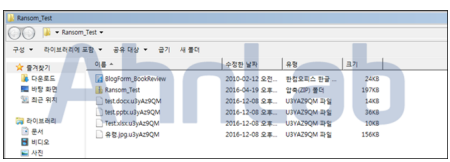


그림 3-3 | 골든아이 랜섬웨어의 랜섬 노트

랜섬 노트 생성을 마치면 암호화를 진행한다. 암호화가 완료되면 무작위 8글자의 확장명을 기존 파일 확장명 뒤에 추가한다. 파일명이 'a.doc'라면 'a.doc.u3yAz9QM'과 같이 변경된다.

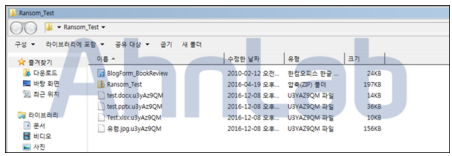


그림 3-4 | 골든아이 랜섬웨어 감염 시 암호화 이후 추가되는 확장명

골든아이 랜섬웨어는 기존 랜섬웨어와 달리 파일 암호화에서 멈추지 않는다. 파일 암호화가 완료되면 C:\ 경로를 수정하는데, MBR 영역 암호화를 위한 프로그램을 준비하는 것으로 보인다. PC를 재부팅하면 정상적인 윈도우(Windows) 로고가 표시되지 않고, 하드디스크의 오류를 수정하는 프로그램인 CHKDSK가 하드디스크를 수리하는 화면이 출력된다. 그러나 이것은 골든아이 랜섬웨어에 의해 생성된 가짜 프로그램이다. 하드디스크를 수리하는 것처럼 표시되지만, 실제로는 부팅과 각 파티션 영역의 정보를 담고 있는 MBR 암호화 과정을 진행한다.

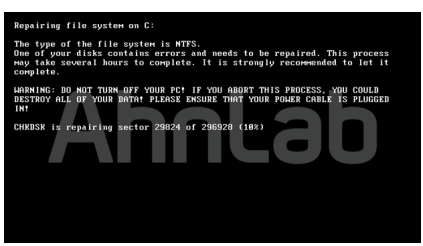


그림 3-5 | CHKDSK 파일로 위장한 MBR 암호화 과정

MBR 암호화가 완료되면 페트야 랜섬웨어와 미샤 랜섬웨어에서 익숙하게 봐왔던 해골 이미지가 출력된다. 기존 페트야 랜섬웨어가 빨간색과 흰색, 미샤 랜섬웨어가 녹색과 검은색의 조합이었다면 골든아이 랜섬웨어는 이름과 어울리는 노란색과 검은색의 조합이다.

그림 3-6 | MBR 암호화 완료 후 출력되는 해골 이미지

또한 이전에 TXT 파일로 생성된 랜섬 노트와 동일한 내용을 확인할 수 있다.

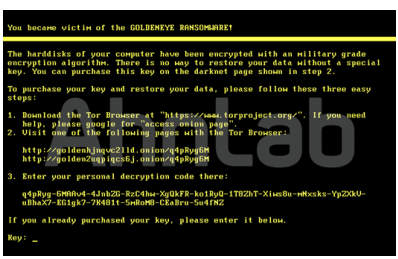


그림 3-7 | MBR 암호화 완료 후 출력되는 랜섬 노트

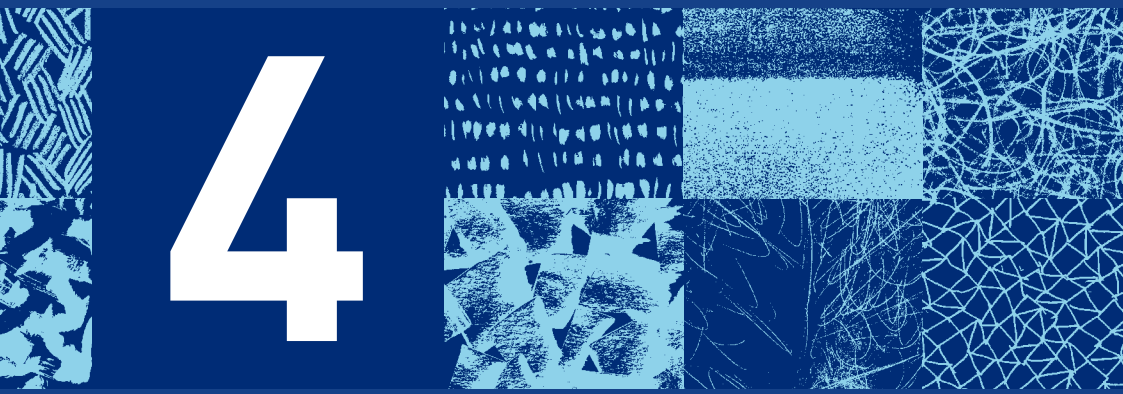
골든아이 랜섬웨어는 페트야 랜섬웨어와 미샤 랜섬웨어를 만들었던 야누스 신디케이트(Janus Syndicate)에 의해 제작된 것으로 알려져 있다. 야누스 신디케이트는 유명한 영화 시리즈인 007 시리즈 중 '골든아이(GoldenEye)' 편에 등장하는 범죄 조직의 이름이기도 하다.

스팸 메일을 통하여 유포되는 랜섬웨어는 메일 수신자가 첨부 파일을 실행하도록 유도하기 위해 '요금청구(Payment)', '영수증(Receipt)'과 같이 위장한 제목으로 메일이 발송된다. 따라서 출처가 불분명한 메일의 열람을 자제해야 한다.

V3 제품에서는 골든아이 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Agent (2016.12.07.05)
W97M/Petya (2016.12.08.00)
W97M/Petya (2016.12.09.00)



4

연간 위협 동향

2016 ANNUAL REPORT

01 2016년 보안 위협 결산 Top 5

02 2017년 보안 위협 전망 Top 5

01
2016년 보안 위협 결산 Top 5

01. 전세계를 위협한 랜섬웨어의 진화

올 한 해 보안 업계뿐만 아니라 뉴스 등 언론을 통해 일반 사용자들 사이에서도 지겨울 정도로 빈번하게 등장한 보안 용어는 바로 '랜섬웨어(Ransomware)'다. 더 이상의 설명이 필요 없는 랜섬웨어는 지난 한 해 동안 종류와 양이 폭발적으로 증가하면서 전세계적으로 막대한 피해를 입혔다. ASEC에 접수된 비율만 보더라도 연초에는 전체 보안 침해 신고의 15%에 불과하던 것이 11월 말에는 4배 가량 증가해 60% 이상을 차지했다.

2016년 랜섬웨어의 동향을 자세히 살펴보면, 크고 작은 변화와 소멸을 거듭하며 결과적으로 진화하는 양상을 보인다. 지난 2015년 악명을 떨쳤던 테슬라크립트(TeslaCrypt)가 올해 5월, 돌연 활동 종료를 선언했다. 또 국내에서 피해가 컸던 크립트XXX(CryptXXX)도 지난 7월 이후 잠잠해졌다. 반면 스팸 메일을 통해 유포되는 록키(Locky)나 음성으로 감염 사실을 알려주는 케르베르(CERBER)는 지속적으로 업그레이드를 거듭하고 있다. 또 파일뿐만 아니라 MBR(Master Boot Record)까지 암호화해 PC 사용 자체를 방해하는 랜섬웨어도 등장했다.

올해는 랜섬웨어 제작과 유포를 대행해주는 랜섬웨어 서비스, 이른바 RaaS(Ransomware-as-a-Service)가 본격화되면서 랜섬웨어의 전세계적인 확산에 영향을 끼쳤다. 심지어 다양한 언어를 지원하는 경우도 있다. 대부분의 랜섬웨어는 영어로만 제작되어 있지만, 국내 감염율이 높았던 테슬라크립트나 크립트XXX, 록키, 케르베르 등은 영어 외에도 각국 언어로 서비스를 제공한다.

유포 및 감염 방식 또한 스팸 메일의 첨부 파일부터 드라이브 바이 다운로드(Drive-by-download), 멀버타이징(Malvertising), 최근에는 사회공학기법과 결합하거나 RDP(Remote Desktop Protocol)를 이용하는 등 다양화되고 있다.

02. 가성비 높은 표적 공격, 경계가 없다

특정한 대상을 선별하여 공격하는 표적 공격(target attack)은 투자 대비 성공률이 높다는 특징 때문에 최근 몇 년간 뚜렷한 증가세를 나타냈다. 표적 공격은 정치적인 목적과 금전적 목적의 일반 기업을 노린 공격으로 구분할 수 있다.

2016년 2월 미국 국토안보부 인사정보 탈취 사건은 러시아의 소행으로 의심되고 있고, 지난 8월 실수로 유출된 것으로 알려진 미국 국가안보국(NSA)의 해킹 툴(Shadow Brokers) 또한 국가간 스파이전과 연관성이 있다. 개인을 대상으로 하는 표적 공격도 대부분 정치적인 목적을 띠고 있다. 주로 홍콩, 미얀마, 시리아, UAE, 카자흐스탄 등의 국가에서 집권당에 반대하는 정치인이나 사회운동가 등을 노린 표적 공격이 발생했다.

일반 기업을 노리는 표적 공격의 단골 메뉴는 고객 정보, 즉 개인 정보다. 올해도 국내는 물론 야후, 드롭박스 등에서 개인정보 유출 사고가 발생했다. 또 이른바 비즈니스 이메일 스캠(Business email scam)이라 불리는 전통적인 이메일 변조 사기도 유럽과 북미 지역의 기업에 막대한 피해를 입히며 성행 중이다. FBI 집계에 따르면, 이메일 변조 피해 사례는 미국에서만 총 7,000건, 피해액은 약 740만 달러로 확인됐다. 올해 국내에서 발생한 모 기업의 이메일 해킹에 의한 무역대금 240억원 피해 사례의 경우, 사우디 국영 정유업체인 사우디아람코의 이메일 계정이 해킹 당한 것이 원인으로 알려져 있다.

03. IoT 악성코드의 선제 공격

사물 인터넷, 이른바 IoT(Internet of Things) 기술이 발달함에 따라 이와 관련된 위협 또한 진화를 거듭하고 있다. 사물 인터넷 기기는 사용성과 저전력의 측면에서 경량화된 임베디드 리눅스(Embedded Linux) 운영체제를 사용한다. 사용자 단말에 사용되는 운영체제를 관리하기 쉽지 않고, 특히 제조업체가 영세할 경우 보안까지 신경 쓰기는 쉽지 않은 현실이다. 공격자들은 이 점을 놓치지 않았다.

2016년 9월, 유명 보안 블로그인 크렙스온시큐리티(KrebsOnSecurity)와 호스팅 업체 OVH에 대해 기록적인 규모의 DDoS 공격이 발생했다. 또 지난 10월에는 미국 인터넷 호스팅 서비스업체 딘(Dyn)에 대한 DDoS 공격도 발생했다. 이 공격으로 인해 트위터(Twitter), 뉴욕타임스(The New York Times), 에어비앤비(Airbnb), 페이팔(PayPal), 넷플릭스(Netflix), 사운드클라우드(SoundCloud) 등 다수의 웹사이트에서 접속 장애가 발생했다.

이들 두 공격에는 사물 인터넷 악성코드인 미라이(Mirai) 악성코드가 이용된 것으로 확인되었다. 다양한 사물 인터넷 기기가 공격에 이용되었으며, 일부 악성코드의 소스코드가 공개되면서 올 한해 동안에만 1만개 이상의 사물 인터넷 관련 악성코드가 발견됐다.

04. 익스플로잇 킷의 적자생존, 치열한 취약점 공격

익스플로잇 킷(Exploit Kit, 이하 EK)은 취약점을 이용한 악성코드를 대량으로 유포하는 툴로, 랜섬웨어 암시장이 활성화되면서 더욱 활개를 치고 있다. 이와 함께 익스플로잇 킷의 치열한 경쟁과 지각 변동이 나타났다.

지난 상반기 랜섬웨어 유포 1순위로 악명을 떨쳤던 앵글러(Angler EK)와 뉴클리어(Nuclear EK)가 활발히 활동하다 갑자기 사라졌고, 앵글러의 자리를 물려받았던 뉴트리노(Neutrino EK) 역시 하반기들어 활동이 감소했다. 반면 선다운(Sundown EK), 매그니튜드(Magnitude) 등은 지속적으로 활동하고 있다.

익스플로잇 킷의 다단계 리다이렉션 (Redirection) 기법은 웹사이트 광고 서버를 이용해 랜섬웨어 등 악성코드를 유포하는 멀버타이징(Malvertising) 공격에 주로 이용되고 있다. 다양한 스크립트 형식의 다운로더나 익스플로잇 킷을 이용한 랜섬웨어 유포는 현재도 지속적으로 발생하고 있으며, 윈도우 쉘프로그램인 파워쉘(Powershell)을 이용한 악성코드도 다수 발견되었다.

또한 익스플로잇 킷이 활기를 띠면서 이들이 주로 이용하는 인터넷 익스플로러(Internet Explorer, IE), 플래시(Flash), 자바(Java) 등의 취약점을 비롯해 다양한 취약점 공격이 더욱 거세졌다. 특히 문서 파일과 관련된 EPS(Encapsulated PostScript) 취약점과 오픈 타입 폰트(Open Type Font) 취약점을 이용한 악성코드 유포가 증가했다. 또, 윈도우(Windows) 운영체제의 정상 기능에 대한 설계상 결함을 이용한 코드 인젝션(injection) 기법의 아톰바밍(AtomBombing)은 모든 버전의 윈도우 운영체제에 영향이 있는 것으로 알려져 충격을 주었다.

05. 모바일 환경에 뿌리내린 루팅 앱

2016년에는 안드로이드 기반의 스마트폰을 루팅(Rooting)하는 악성 앱이 다수 발견되었다. 특히 지난 7월부터 10월까지 3개월간 안랩이 수집한 루팅 악성 앱의 수가 2016년 상반기 6개월 대비 약 30% 가량 증가했다. 악성 앱이 갈수록 급증하고 있음을 알 수 있다.

악성 앱은 주로 사용자 몰래 앱을 설치하거나 모바일 백신 제품의 탐지 및 삭제를 우회하고, 개인 정보를 탈취하거나 광고를 노출하는 등의 악의적인 행위를 위해 루트 권한을 이용한다. 지난 상반기에는 주로 루팅을 통해 광고 행위 또는 사용자 몰래 앱을 설치하는 악성 앱 유형이 주를 이뤘고, 하반기에 들어서며 금융 정보 탈취를 목적으로 하는 루팅 앱이 나타났다. 중국에서 제작된 악성 앱들은 대부분 추가적인 앱 설치 또는 광고 노출을 통한 수익을 위해 루트 권한 획득을 시도하는 것으로 확인됐다.

루팅을 시도하는 악성 앱들은 안드로이드 운영체제의 취약점을 이용해 스마트폰의 권한을 획득한다. 상반기에 발견된 악성 앱 갓리스(Godless)는 안드로이드 운영체제 5.1 버전(Lollipop) 이하에서 루트 권한 탈취를 위해 다수의 취약점을 이용했다.

이처럼 안드로이드 운영체제의 취약점을 이용한 악성 앱이 증가함에 따라 구글은 안드로이드 보안 강화를 위해 다각도로 노력을 기울이고 있다. 지난 2015년 스테이지 프라이트(Stage fright) 취약점이 발견된 이후 매달 안드로이드 운영체제 보안 업데이트를 제공하는 한편, 각 스마트폰 제조사들의 업데이트 대응 순위를 공개하고 있다. 또 올해 공개된 안드로이드 운영체제 7.0(Nougat)은 루팅을 통해 시스템 변조를 시도할 경우 부팅 자체를 불가능하게 했다. 문제는, 스마트폰 제조사 또는 단말기의 생산 연도에 따라 보안 업데이트가 제공되지 않는 경우가 있다는 점이다.

02
2017년 보안 위협 전망 Top 5

01. 랜섬웨어, '돈'이 모이는 곳 정조준

지난 2016년 한 해 동안 가파른 성장세를 보였던 랜섬웨어(Ransomware)는 공격자 관점에서 즉각적으로 금전적 이득을 취할 수 있는 유용한 범죄 수단으로 자리잡았다. 특히 기업의 경우, 비즈니스 중단이나 고객 정보와 같은 중요 데이터를 잃을 수 있다는 부담 때문에 결국 몸값(ransom)을 지불하는 사례가 적지 않다. 여기에 랜섬웨어 제작 및 유포의 서비스화(Ransomware as a Service, RaaS) 등 랜섬웨

어 자체가 수요자와 공급자가 유기적으로 활동하는 하나의 시장을 형성하기에 이르렀다.

랜섬웨어의 위협은 올해 더욱 고도화되고 공격 범위도 확장될 전망이다. 금전적 이득이 목적이라면 '돈'이 모이는 곳으로 향하는 것이 당연지사. 지금까지 금전적인 피해를 야기하는 사이버 범죄는 가짜 홈페이지를 통해 사용자 정보를 탈취하는 피싱과 파밍이 주도했지만 이제 랜섬웨어가 그 중심에 있다 해도 과언이 아니다. 또한 스피어 피싱 등과 결합한 랜섬웨어가 나타날 가능성도 높다. 이와 관련해 스피어 피싱 등을 이용해 기업 간 무역 거래 대금을 노리는 범죄 조직이 다년간 활동 중이기 때문에 무역 거래가 빈번한 기업의 경우 각별한 주의가 요구된다.

02. 대중화된 공격 툴을 이용한 사이버 범죄의 고도화 · 가속화

불과 몇 년 전까지만 해도 사이버 공격은 전문적인 IT 지식을 가진 해커 또는 해킹 그룹의 전유물로 여겨졌다. 그러나 최근 사이버 암시장뿐만 아니라 일반 인터넷 상에서도 랜섬웨어 제작 서비스인 RaaS를 비롯해 다양한 스팸 메일 발송 서비스 등을 이용할 수 있어, 전문적인 IT 관련 지식이 없더라도 악성코드를 제작하고 사이버 공격을 시도할 수 있게 됐다. 이렇게 대중화된 사이버 공격이 더 많은 범죄에 악용될 것으로 전망된다. 동시에 사이버 범죄자를 특정인 또는 그룹으로 한정 지을 수 없게 됨에 따라 이에 대한 대응 및 수사 등이 더욱 어려워질 전망이다.

공격자들은 스팸 메일 첨부 파일과 홈페이지 방문 시 자동으로 설치하는 드라이브 바이 다운로드(Drive-by-download) 공격을 지속할 뿐 아니라 소프트웨어 보안 패치를 적용하지 않는 사용자들이 더 많다는 사실에 주목하고 소프트웨어 보안 취약점을 악용하는 익스플로잇 킷을 더욱 적극적으로 활용하는 등 기존 공격 기법의 업그레이드에 주력할 것이다. 지속적으로 증가하는 익스플로잇 킷 기반의 공격에 대비하기 위해 정기적으로 웹사이트 위 · 변조 여부를 확인하고, 특히 웹쉘을 이용한 공격에 각별한 주의를 기울여야 한다.

03. 고도화된 위장술로 내부 침입 및 시스템 장악 시도

2010년 전후로 발생한 기업 해킹은 기업 기밀이나 기업이 보유하고 있는 개인정보를 탈취하기 위한 목적이 대부분이었다. 그러나 최근에는 단순한 정보 유출을 넘어 기업 내부 인프라를 장악하기 위한 공격으로 변화했다. 이를 위해 특히 올해는 기업 및 기관의 내부 인프라에 성공적으로 침입하기 위해 다양한 속임수를 더한 공격 기법이 등장할 것으로 보인다.

이러한 공격을 통해 감염된 시스템을 거점으로 기업 내부 인프라에 침입하여 내부 정보를 수집 및 검색함으로써 시스템 계정 정보를 획득한다. 주요 계정 정보의 수집과 활용을 반복함으로써 내부 관리 시스템 운영에 관련된 권한을 탈취하고 마침내 전체 인프라를 장악한다.

이런 방식으로 특정 기업의 내부 시스템 장악을 장악하면 이를 공격 거점으로 삼아 해당 기업의 서비스 이용에 필요한 정상적인 프로그램으로 위장하여 광범위한 다수의 PC에 악성코드를 설치할 수 있다. 또 이렇게 감염된 PC와 연결된 네트워크상의 다른 시스템을 통해 또 다른 기업의 내부 시스템 장악까지 시도할 수 있어 이 영역에 대한 공격은 여전히 지속될 것으로 보인다.

04. 멈추지 않는 사회기반시설 공격 · 사이버 테러

2017년에는 국내뿐만 아니라 전세계적으로 정치적 · 경제적 이해 관계 대립이 더욱 심화될 전망이다. 국가간 이념적 갈등 또한 깊어져 타국의 기관과 기업을 겨냥한 사이버 테러 역시 사라지지 않을 전망이다.

최근 공격의 대상(target)은 기존의 다수 시민들이 이용하는 온라인 서비스를 겨냥하던 것에서 서비스 종류나 규모에 관계없이 거의 모든 기업과 기관으로 확대되고 있다. 사회기반시설 공격 등 사이버 테러의 배후는 주로 테러 단체이거나 적대적인 관계를 맺고 있는 국가로 추정된다. 공격 동기 또한 금전적 이득보다는 종교적 · 이념적 · 정치적 갈등에서 찾을 수 있다. 특히 사회기반시설 공격이 성공할 경우 사회적 혼란과 공포를 야기함으로써 자신들의 선전 효과를 극대화할 수 있으며, 종교적 · 정치적 갈등은 쉽게 해결되기 어렵기 때문에 사회기반시설 공격은 앞으로도 지속될 전망이다.

대부분의 사회기반시설 내 시스템은 외부 인터넷에 직접적으로 연결되지 않는 망 분리 환경에서 안전하게 운영되고 있다. 그러나 단 하나라도 인터넷망에 연결된 시스템이 존재하거나 인터넷망과 내부망을 연결하는 지점이 존재할 경우 보안 위협으로부터 완벽하게 자유롭다고 할 수 없다. 또 어디에서든 보안에 가장 취약한 지점은 사람이다. 불편함 등을 이유로 보안 정책을 어기는 내부 직원이 있을 수 있다. 공격자들은 이러한 취약점을 찾아내기 위해 다양한 방법을 동원해 지속적으로 공격을 시도하고 있다.

05. Internet of Things vs. Threat of Things

사물 인터넷(Internet of Things, IoT) 기술의 발전과 확산은 더욱 가속화될 전망이다. 문제는 아직 사물 인터넷의 보안 이슈에 대한 인식이 부

족해 보안에 취약한 제품의 판매가 지속될 것이라는 점이다. 그리고 이를 노린 사물 인터넷 악성코드 또한 빠르게 증가할 것으로 예상된다.

실제로 지난 해 미국에서는 미라이(Mirai)라는 악성코드에 감염된 사물 인터넷 기기를 이용한 대규모 DDoS 공격이 발생한 바 있다. 사물 인터넷 기기는 한번 판매 또는 설치되면 사후 관리가 이루어지기 어렵고, 대부분 수년간 초기 상태 그대로 사용된다는 특징이 있다. 사용자 입장에서는 사물 인터넷 기기 제조사가 제공하는 보안 패치를 적용하는 것 외에는 마땅히 방법이 없다. 그러나 현재 대부분의 사물 인터넷 기기 제작 업체는 보안 문제를 고민할 정도의 여유(?)가 없거나 기술력이 부족한 실정이다. 또 사용성의 측면에서 저전력과 저비용이 핵심인 사물 인터넷 기기의 특성상 보안 강화를 위한 기능 추가나 가격을 인상하는 것은 현실적으로 어렵다.

따라서 빠르게 확산되고 있는 사물 인터넷 기기와 관련된 보안 위협을 방지하기 위해서는 제조사뿐만 아니라 보안 업체와 정부 기관의 유기적인 협력이 필요하다. 또 다양한 국가에서 앞다퉈 사물 인터넷 기술과 제품 개발을 서두르고 있어 개별 국가의 규제만으로는 사물 인터넷 기기에 의한 광범위한 보안 위협을 해결하기 어렵다. 각국의 정부와 관련 협회, 제조사의 전방위적인 협업을 통해 사물 인터넷 기기에 대한 최소한의 점검 체계 구축과 실질적으로 적용 가능한 보안 강화 조치 가이드 마련이 시급하다.

AhnLab

ASEC REPORT

VOL.84
December, 2016

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