
알약 월간 보안동향 보고서.

2015년 11월



알약 11월 보안동향보고서

CONTENTS

Part1 10월의 악성코드 통계

악성코드 통계
허니팟/트래픽 분석
스팸 메일 분석
스미싱 분석

Part2 악성코드 이슈 분석

개요
상세 분석
결론

Part3 보안 이슈 돋보기

10월의 보안 이슈
10월의 취약점 이슈

Part4 해외 보안 동향

영미권
중국
일본

10월의 총평

올 초부터 꾸준히 증가해오던 랜섬웨어의 위협이 본격적으로 현실화되기 시작하였습니다.

2015년 3월경 CryptoFortress, CryptoWall 3.0을 시작으로, 4월에는 한글로 작성된 금전요구 메시지를 최초로 띄우기 시작한 CryptOLocker가 사용자들이 많이 방문하는 웹사이트를 변조하여 DBD형태로 유포되었으며, 5월이후에도 조금씩 그 피해사례가 증가하기 시작하여 9월경부터 본격적으로 국내에서 랜섬웨어 유포사례가 급증하고 있습니다. Windows OS 사용자를 노린 랜섬웨어 뿐만 아니라, 안드로이드OS 사용자를 노린 랜섬웨어, 최근에는 리눅스OS 사용자를 노린 랜섬웨어까지 등장하고 있는 추세입니다.

랜섬웨어는 일단 감염되면, 타겟을 삼은 모든 파일에 대해 암호화를 진행하며 공격자 서버에 존재하는 복호화키 정보가 없으면 원상복구가 거의 불가능하므로, 중요자료에 대한 주기적 백업이 가장 중요합니다. 또한 랜섬웨어는 사용자 시스템상의 OS와 SW의 취약점을 이용하여 유포되는 경우가 많으므로, 사용중인 OS와 SW의 보안취약점을 최신업데이트를 통해 패치하고 취약점을 이용한 공격을 사전에 차단할 수 있는 취약점 방어 솔루션을 사용하시는 것이 가장 효과적인예방방법 중 하나입니다. 또한, 해외스트리밍 사이트 또는 블로그/웹사이트/이메일의 첨부파일 등을 통해 랜섬웨어가 유포되는 경우도 많으므로 신뢰하기 어려운 사이트에서의 파일 다운로드 및 실행은 각별한 주의가 필요합니다.

Part1. 10월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸 메일 분석

스미싱 분석

1.악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 순위이다.

2015년 10월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2,3위를 차지했던 악성코드들이 변동 없이 순위를 유지하였다.

악성 애드웨어들은 8,9월에 이어 10월에도 역시 리스트에 많이 올라온 것이 특이사항이며, 전체 감염자수는 소폭 증가하였다. 호스트파일을 변조하는 악성코드 수치가 크게 증가한 것도 주목할 만한 부분이다.

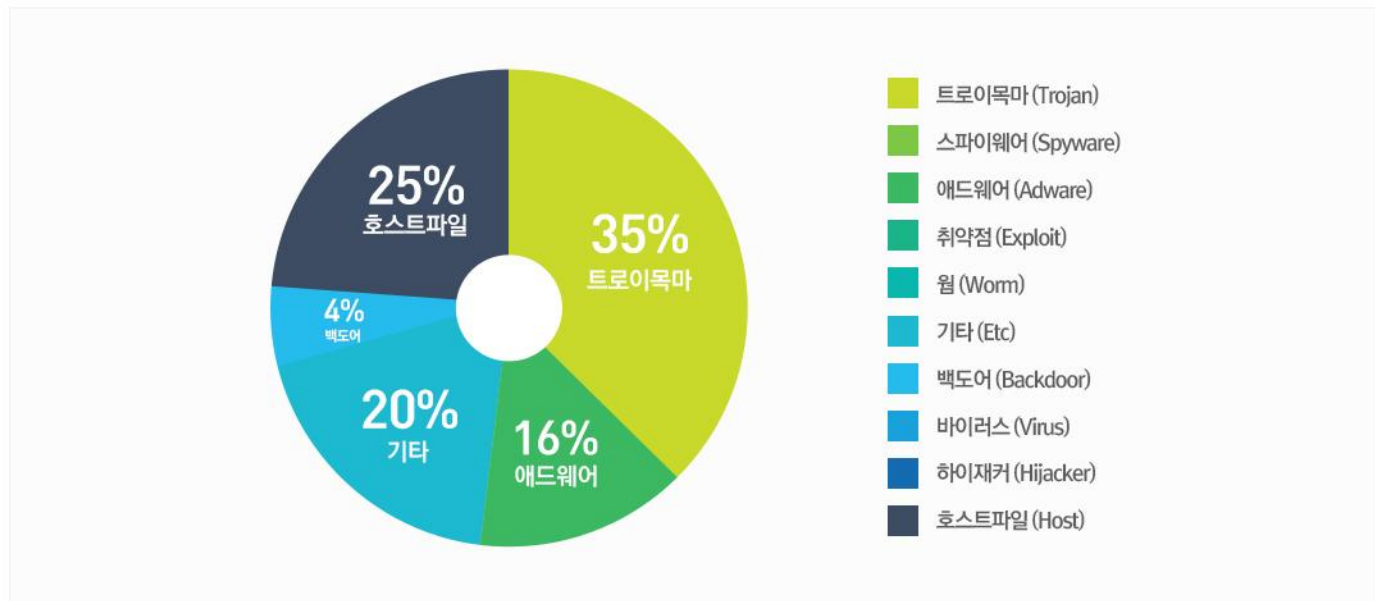
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.Suspicious.NTZ	Etc	1173
2	-	Misc.Keygen	Trojan	783
3	-	Misc.HackTool.WinActivator	Trojan	632
4	NEW	Gen:Adware.BrowseFox.1	Adware	412
5	NEW	Gen:Variant.Adware.Zusy.164797	Trojan	383
6	↓ 2	Adware.Kraddare.295936	Adware	306
7	-	Misc.Agent.126672	Trojan	251
8	↓ 2	Backdoor.Agent.com32	Backdoor	250
9	↑ 6	Hosts.www.nate.com	Host	248
10	-	Hosts.www.daum.com	Host	248
11	↑ 1	Hosts.www.naver.com	Host	248
12	-	Hosts.www.zum.com	Host	247
13	NEW	Hosts.www.gmarket.com	Host	247
14	NEW	Hosts.www.kjbank.com	Host	247
15	↓ 10	Adware.OpenShopper.J	Adware	245

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 10월 01일 ~ 2015년 10월 31일

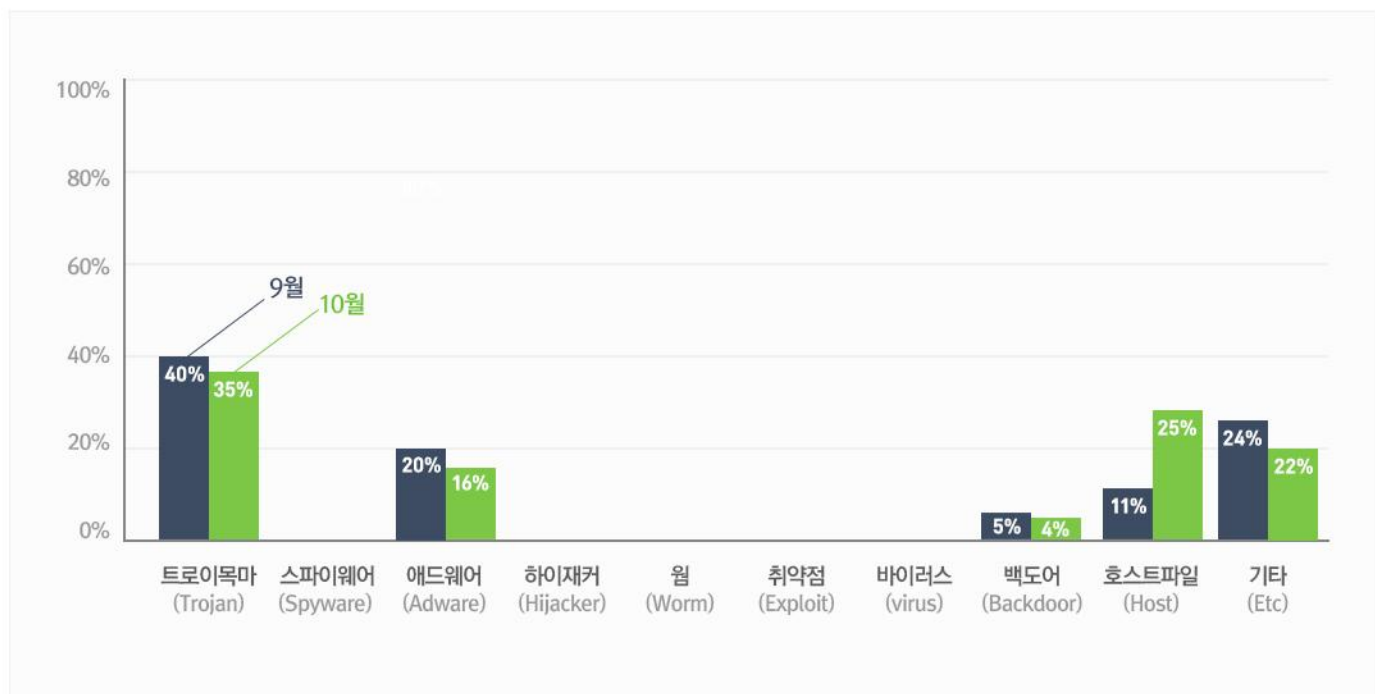
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 35%를 차지했으며 호스트파일(Host)유형이 25%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

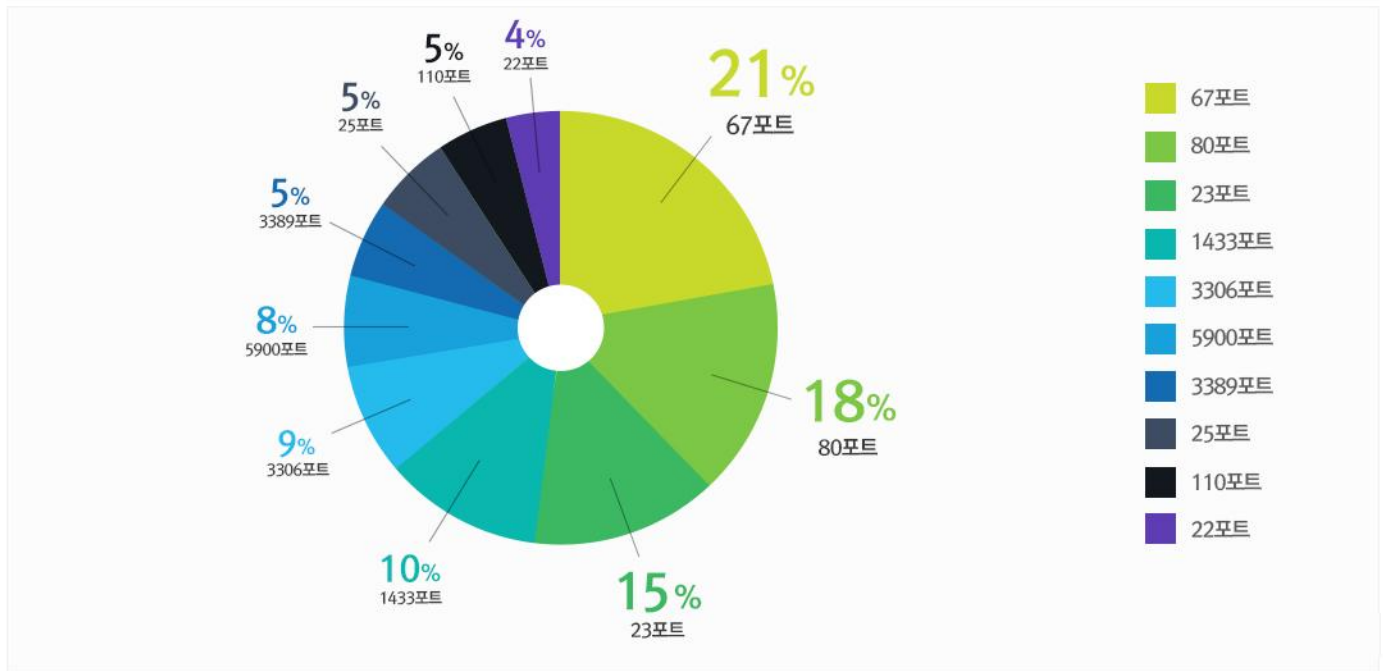
10월에는 지난 9월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율은 소폭 감소했으며 호스트파일 변조와 관련된 호스트파일(Host)유형의 악성코드의 비중이 2배 넘게 증가하였다.



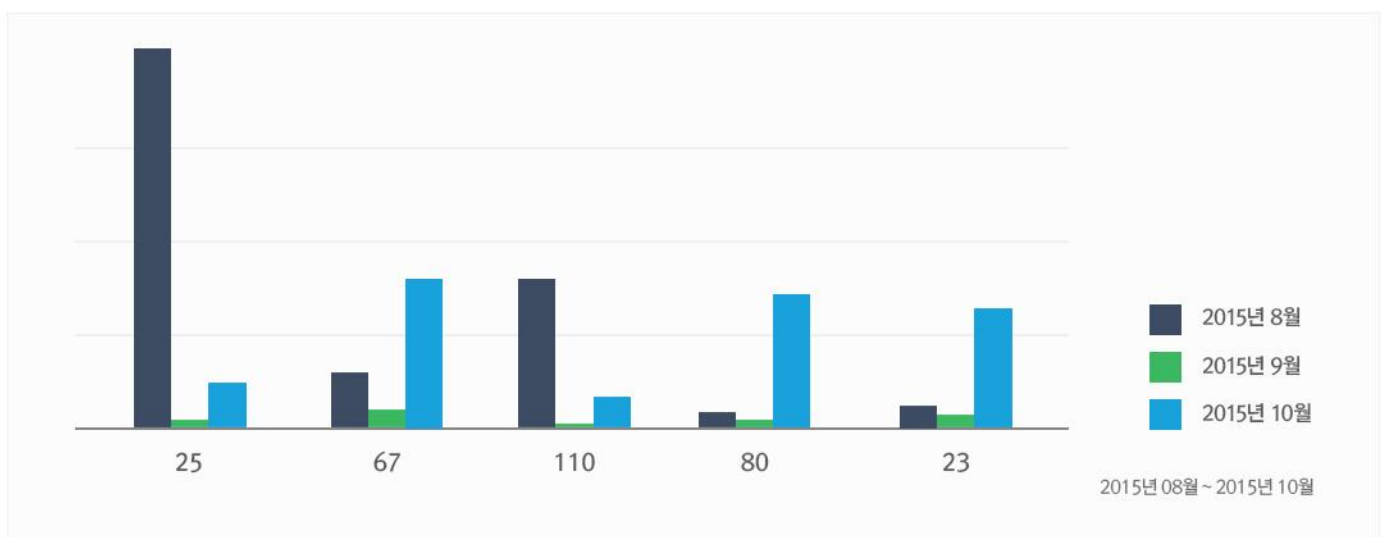
2.허니팟/트래픽 분석

10월의 상위 Top 10 포트

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

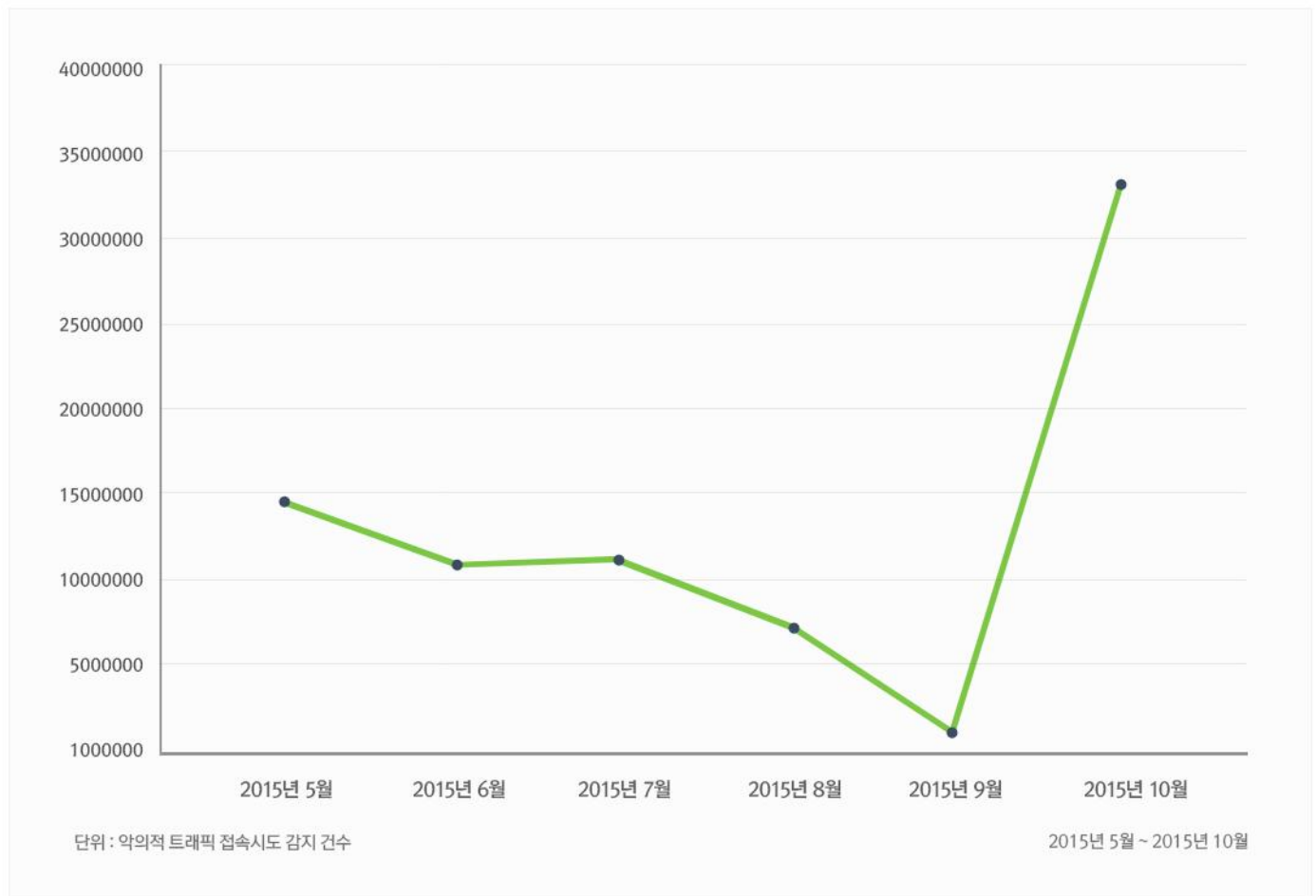


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치

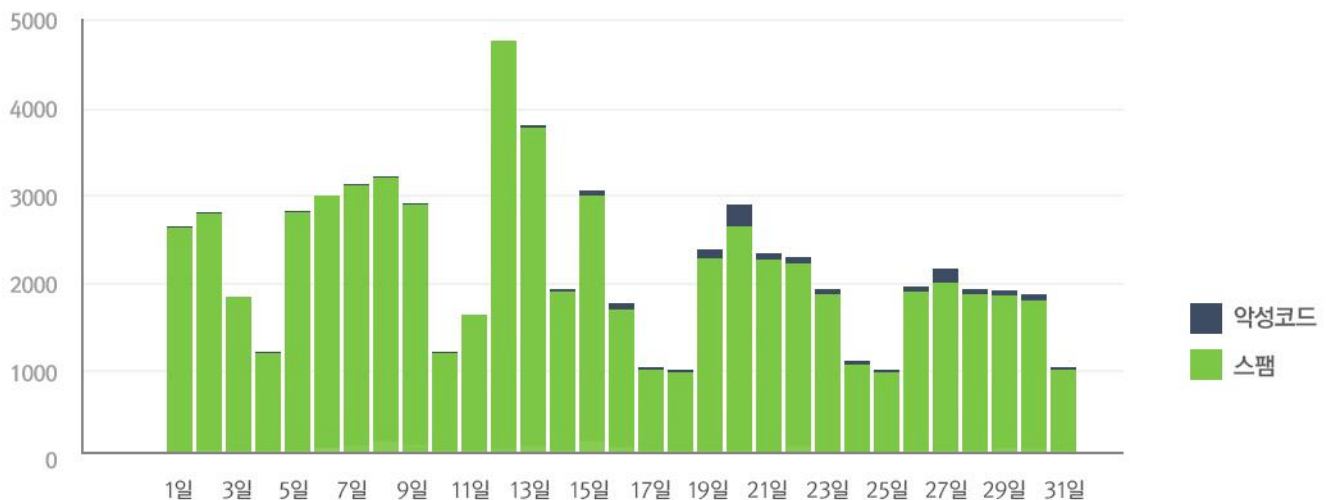


3. 스팸메일 및 악성코드가 포함된 메일 분석

일별 스팸 메일 및 악성코드 포함 메일 통계 현황

일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다. 2015년 10월의 경우 2015년 9월에 비해 스팸메일 유입수치는 10%가량 감소하였고 반면, 메일에 첨부된 악성코드수치는 약 10배 가량 증가하였다.

10월에 가장 많이 발견된 메일에 포함된 악성코드는 W32/HEURISTIC-300!ELDORADO이다. 해당 악성코드는 이메일에 첨부되어 주로 유포되는, 트로이목마 악성코드이며, 공격자가 의도한 악의적인 시도를 진행하며, 악성코드 추가 파일을 사용자 모르게 다운로드 하여 실행시키는 악성코드이다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2015년 10월 01일 ~ 2015년 10월 31일
총 신고 건수	8,794건

키워드별 신고 내역

키워드	신고 건수	비율
택배	742	8.44%
결혼	359	4.08%
등기	61	0.69%
보안	55	0.63%
공유	39	0.44%
민방위	24	0.27%
입학	22	0.25%
본인확인	19	0.22%
위반	16	0.18%
돌잔치	8	0.09%

스미싱 신고추이

지난달 스미싱 신고 건수 8,041건 대비 이번 달 8,794건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 753건 증가했다. 이번 달에는 결혼 관련 스미싱은 감소하였고, 택배 관련 스미싱이 증가했다. 새롭게 본인확인 관련 스미싱이 등장했다.

알약이 뽑은 10월 주목할만한 스미싱

특이문자

순위	문자내용
1	새로운 게임자문 재미고 자극 게임 기다리고있습니다
2	[학부모님!확인해주세요
3	제가 내일 결혼하는데 시간 있으세요?저의명함 확인

다수문자

순위	문자내용
1	[Web발신] 고객님의 요청하신물품 배송운송장~주소확인.
2	여러분♡♡우리들 결혼합니다 꼭참석하시어축하해주세요.
3	(경찰청)등기 발송하였으나 (부재중)하였습니다.내용조회
4	[Web발신] NCOTP 가 보안에 취약합니 주소에 연결 하셔서확인하세요
5	[Box] 은정님이 공유한 동영상이 도착하였습니다
6	[소집명령] 훈련 일시를 확인하세요.
7	cms_(통지서) 도착했어요~
8	본인확인 인증번호[592585]를 화면에 입력해주세요.
9	교통법 위반사건 2014형 제330-33510 기소내용본문
10	[등기 발송하였으나[전달 불가]부재 중 하였습니다(내용확인)

Part2. 10월의 악성코드 이슈 분석

개요

상세분석

- 유포과정

- 분석정보

결론

자극적인 문구로 이용자를 유혹하는 악성코드 분석 보고서

1. 개요

불법적으로 운영하는 사행성 도박사이트들이 소셜네트워크서비스(SNS)나 각종 인터넷 방송에서 광고하는 모습을 쉽게 발견할 수 있다. 이러한 사이트는 누구나 돈을 쉽게 벌 수 있다는 등 갖가지 허위문구로 이용자들을 현혹하고 있는 것이 다반사이다.

이런 가운데 2015년 11월 초 “불법토토사이트운영진정보 (1).rar” 파일명의 악성파일이 발견되었다. 마치 사설도박 사이트의 운영진 및 회원들의 명단처럼 위장하고 있지만, 실제로는 악의적인 파일들이 압축파일 내부에 다수 포함되어 있었다.

더불어 해당 압축파일에는 사설 도박사이트 회원정보로 위장한 위장파일과 중국 유흥업소 운영진의 단체 사진처럼 위장한 파일들도 포함되어 있다.

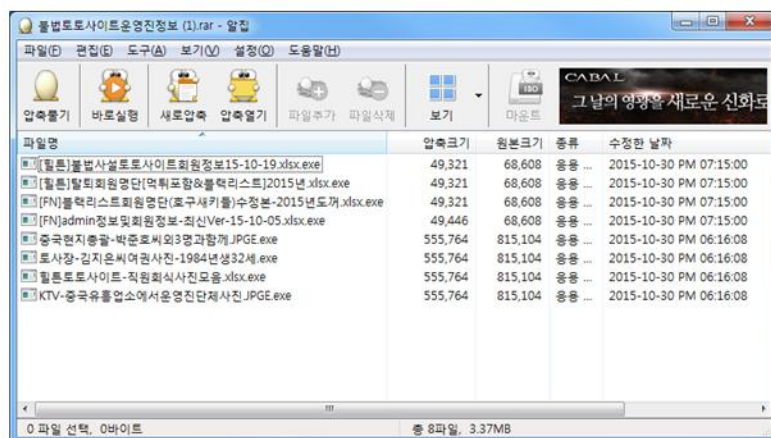
인터넷으로 운영되는 불법 사설 도박사이트는 아직까지 근절되지 않고 있으며, 독버섯처럼 확산되고 있고, 사행성 게임 늪에 빠진 많은 사람들은 피해를 호소하고 있기도 하다.

이런 가운데 사설 도박사이트의 운영진 및 회원정보처럼 위장한 악성파일도 발견되고 있어, 이용자들은 이런 사이버 미끼에 현혹되어 예기치 못한 피해를 입지 않도록 각별한 주의가 필요하다.

2. 상세분석

“불법토토사이트운영진정보 (1).rar” 파일의 화면

파일정보



[그림 1] 불법토토사이트운영진정보로 위장한 압축파일 화면

-유포과정

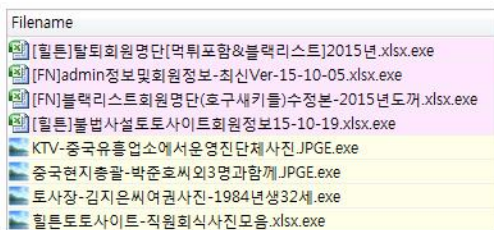
현재 정확한 유포과정은 확인되고 있지 않지만, RAR 압축파일에 호기심을 유발할 수 있는 다수의 파일이 포함되어있고, 마치 문서(XLS)나 사진(JPGE)파일처럼 위장하고 있다.

공격자는 압축파일 형태로 배포했을 가능성도 있고, 개별적으로 하나씩 배포해 악용했을 가능성도 존재한다.

-분석정보

RAR 압축파일 내부에는 총 8개의 파일이 포함되어 있는데, 모두 악성파일이다.

8개의 파일 중에 4개는 회원정보 명단으로 위장한 파일이고, 나머지 4개는 사진으로 위장한 파일이다.



[그림 2] 압축파일 내부에 포함된 중복파일 화면

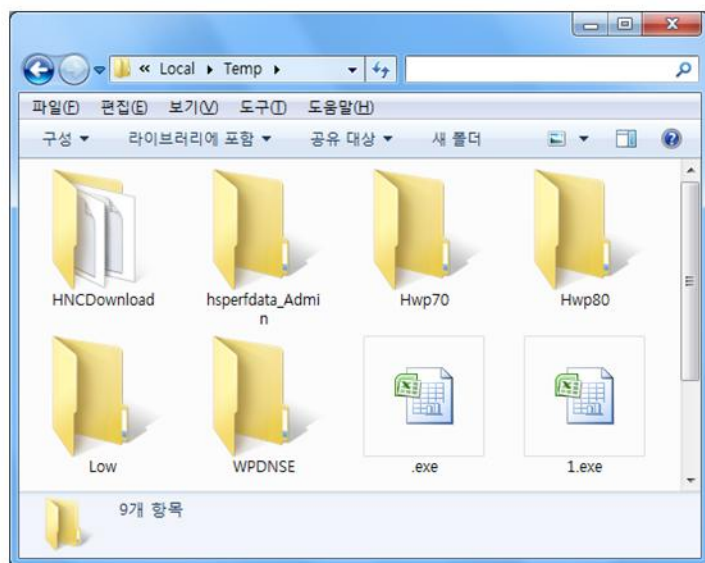
아래 4개의 파일은 모두 파일명만 동일한 악성파일로 2중 확장명(xlsx.exe)을 사용해서 실행파일(EXE)이 엑셀문서(XLS)파일처럼 보이도록 하고 있다. 또한, 치밀하게 아이콘도 함께 위장되어 있다.

- [힐튼]탈퇴회원명단[먹튀포함&블랙리스트]2015년.xlsx.exe
- [FN]admin정보및회원정보-최신Ver-15-10-05.xlsx.exe
- [FN]블랙리스트회원명단(호구새키들)수정본-2015년도꺼.xlsx.exe
- [힐튼]불법사설토토사이트회원정보15-10-19.xlsx.exe

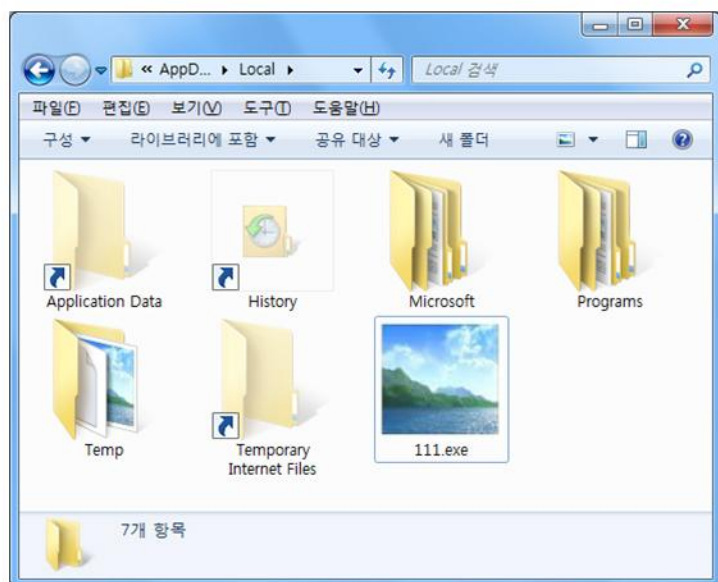
다음 4개의 파일도 위의 4개의 파일과 파일명만 다른 동일 악성파일로 모두 이미지 파일처럼 아이콘을 위장하고 있다. 이 파일 중 일부는 2중 확장명으로 위장하고 있고, 일부는 실행파일을 그대로 포함하고 있다.

- KTV-중국유흥업소에서운영진단체사진.JPGE.exe
- 중국현지총괄-박준호씨외3명과함께.JPGE.exe
- 토사장-김지은씨여권사진-1984년생32세.exe
- 힐튼토토사이트-직원회식사진모음.xlsx.exe

해당 악성파일들은 모두 유사한 형태로 제작되어 있으며, 실행되면 복사본(.exe, 1.exe, 111.exe)을 임시폴더(Temp)에 생성해서 작동한다.



[그림 3] 엑셀 파일로 위장한 파일화면



[그림 4] 이미지 파일로 위장한 파일화면

임시폴더에 생성된 악성파일 복사본들은 아이콘 리소스가 실제 엑셀문서 파일과 이미지 파일처럼 치밀하게 조작되어 있기 때문에 이용자는 육안상 단순 임시파일로 오해할 수 있게 된다. 공격자는 이러한 위장수법을 통해 악성파일이 오랜 기간 은밀히 잠복하고 생존을 유지할 수 있게 제작했다.

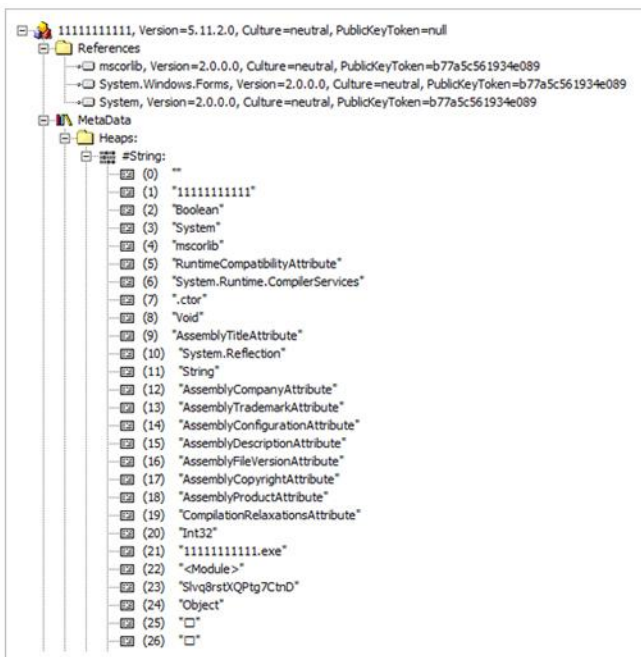
악성파일들은 모두 2015년 10월 30일 제작되었는데, Time Data Stamp 코드를 비교해 보면 몇 십분 사이에 변종을 제작한 것을 확인할 수 있다.

pFile	Data	Description	Value
00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
00000086	0003	Number of Sections	
00000088	56335178	Time Date Stamp	2015/10/30 11:16:08 UTC
0000008C	00000000	Pointer to Symbol Table	
00000090	00000000	Number of Symbols	
00000094	00E0	Size of Optional Header	
00000096	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

pFile	Data	Description	Value
00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
00000086	0003	Number of Sections	
00000088	56335A62	Time Date Stamp	2015/10/30 11:54:10 UTC
0000008C	00000000	Pointer to Symbol Table	
00000090	00000000	Number of Symbols	
00000094	00E0	Size of Optional Header	
00000096	010E	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0004		IMAGE_FILE_LINE_NUMS_STRIPPED
	0008		IMAGE_FILE_LOCAL_SYMS_STRIPPED
	0100		IMAGE_FILE_32BIT_MACHINE

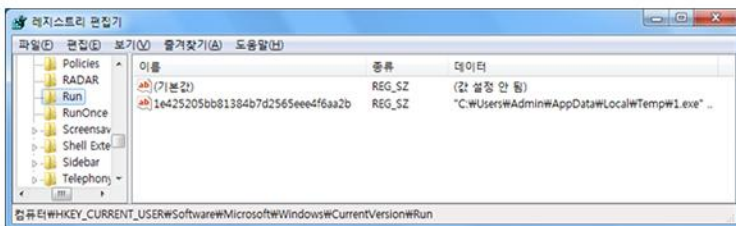
[그림 5] 악성파일 제작 날짜하면

또한, 악성파일은 .NET 프로그램으로 개발되어 있어, 이용자 컴퓨터에 .NET Framework 프로그램이 설치되어 있어야 정상적으로 감염이 된다.



[그림 6] .NET 개발 코드 화면

.NET 프로그래밍으로 악성파일이 제작된 경우 이용자 환경에 따라 악성파일에 노출되지 않을 확률도 높은 편에 속한다. 그렇기 때문에 공격자는 제한적인 범위 내에서만 공격을 성공할 수 있다.



[그림 7] 레지스트리 등록 화면

악성파일은 레지스트리 Run 부분에 자신을 등록해 컴퓨터가 재부팅시 자동으로 실행되도록 만들었기 때문에 컴퓨터가 새로 시작할 때마다 악성모듈이 자동으로 동작하게 된다.

```
// Segment type: Pure data
a111_exe:                                // DATA XREF: CaptainBri__Main+36fo
                                         // CaptainBri__Main+53fo ...
    unicode <#111.exe>,0
aNurNoisrevtner:                        // DATA XREF: CaptainBri__Main:loc_72fo
    unicode <nuR#noisreUtnerruC#swodniW#tfosorcit#werawtfos>,0
asc_106E:                                // DATA XREF: CaptainBri__Main+7Dfo
    unicode <>,0
aRes:                                    // DATA XREF: CaptainBri__Main+9Ffo
    unicode <res>,0
aLjpursyrashull:                        // DATA XREF: CaptainBri__Main+B2fo
    unicode <LJPurSYrasHULL>,0
aXer9ron7pxdco0:                        // DATA XREF: CaptainBri__Main+C1fo
    unicode <Xer9ron7pxDco0mbQptNl45HaMguCGWKbLZmbYFHhdJYezqDNkin7Ag3iT>,0
```

[그림 8] 레지스트리 분석 화면

이러한 유형의 악성파일은 특정 호스트로 접속을 시도할 수 있으며, 외부 공격자의 명령에 따라 추가적인 피해를 입게 될 수 있어 주의가 필요하다.

공격자들은 이용자들이 쉽게 현혹될 수 있는 문서나 사진파일로 위장하는 고전적인 수법을 아주 오랜 기간 꾸준히 사용하고 있다.

이러한 유형은 매우 단순한 공격기법에 속하지만 보안위협에 노출되는 순간 자신도 모르게 다양한 침해사고를 입을 수 있으므로, 인터넷을 통해 접하는 파일들은 보다 세심한 주의를 거친 후에 실행하는 노력이 필요하다.

3. 결론

사이버 범죄자들은 자극적인 문구나 흥미를 유발할 수 있는 내용으로 불특정다수의 인터넷 이용자들을 꾸준히 유혹하고 있다.

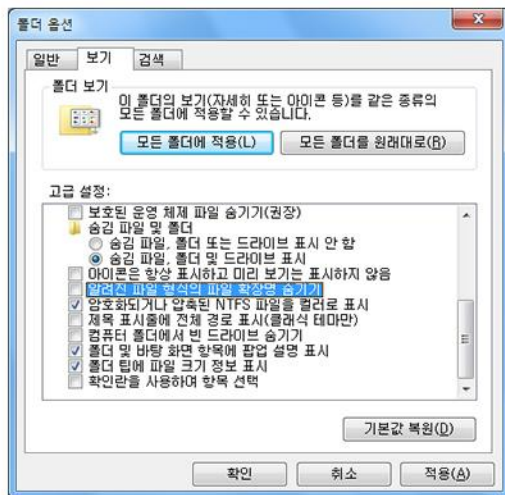
공격방식은 갈수록 다양화, 지능화되고 있기 때문에 각별한 주의가 필요하다.

따라서 이용자들은 평소 출처가 불명확한 파일은 절대로 실행하지 않는 보안습관이 필요하다.

아울러 이번 사례처럼 2중 확장명(xlsx.exe, JPG.exe 등)으로 위장한 파일의 형태를 보다 쉽게 육안으로 식별하기 위해 Windows 운영체제의 폴더옵션에서 “알려진 파일 형식의 파일 확장명 숨기기” 설정 기능을 해제해 두는 것도 좋은 방법이다.

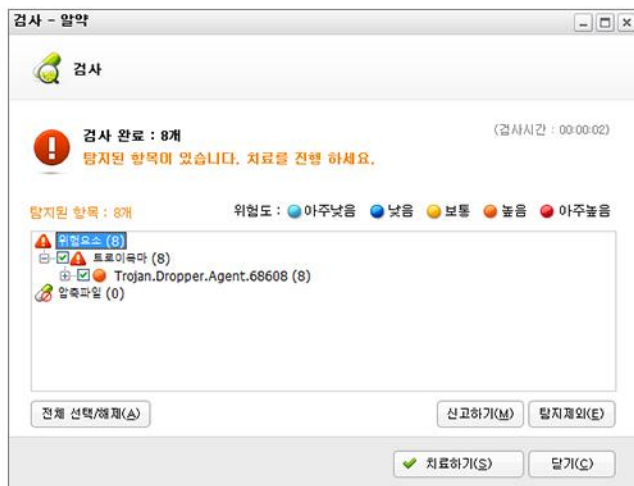
또한, 아이콘과 확장명이 정확하게 일치하는지 꼼꼼하게 비교한 후 실행하는 것도 알려지지 않은 악성파일에 노출될 가능성을 최소화하는 것 중에 하나이다.

이런 보안위험들은 쉽고 간단한 보안습관으로도 사전에 충분히 예방할 수 있는 경우가 있으므로, 스스로 개인 보안에 세심하게 신경을 쓴다면 보다 안전한 컴퓨터환경을 유지할 수 있을 것이다.



[그림 9] 폴더 옵션 설정화면

해당 악성파일들은 알약 제품에서 “Trojan.GenericKD.2837516”, “Trojan.Dropper.Agent.68608” 등으로 치료가 가능하므로, 알약 제품을 항상 최신버전으로 업데이트하고, 실시간 감시기능을 항상 켜두어 악성코드에 대비해야 한다. 더불어 알약과 함께 알약 익스플로잇 쉴드 제품을 함께 설치하면 행위기반의 다양한 보안위험도 사전방어가 가능하다.



[그림 10] 알약으로 탐지되는 화면

Part3. 보안 이슈 돋보기

10월의 보안이슈

10월의 취약점

10월의 보안 이슈

알약이 뽑은 TOP 이슈

- '삭제불가' 중국발 안드로이드 해킹 발견

유명 안드로이드 앱으로 가장해 감염되면 영구히 삭제되지 않으면서 안드로이드폰을 완전히 장악하는 중국발 해킹이 발견되었다. 공격그룹은 유명 앱에 악성코드를 심어 배포하였으며, 사용자가 스마트폰에 악성 앱을 내려받으면 악성코드가 특정 URL에 접속하여 사용자 스마트폰으로 루팅 앱을 내려받아 루팅작업을 하며, 루트권한 획득 후 쉘 스크립트를 시행하여 루트 백도어를 삽입하여 악성 앱을 제거할 수 없다.

- 국내 백신 무력화하는 APT 공격그룹 실체 드러나

국내 안티바이러스(백신)를 무력화하는 백도어를 활용하는 지능형지속위협(APT) 공격 실체가 드러났다. 이 해킹그룹의 이름은 '원티'로 주로 게임사를 포함한 소프트웨어 기업을 대상으로 산업 사이버스파이 활동을 전개해온 사이버범죄조직이다. 또한 HD루트 플랫폼을 사용한 백도어 중에는 국내 백신제품을 무력화 하는 기능을 포함하고 있으며, 이는 한국 기업을 대상으로 한 공격을 벌이기 위해 개발된 기능으로 추정된다.

- 뽐뿌, 해킹 사고 이후에도 보안에 계속 허점

휴대전화 등을 거래하는 온라인 커뮤니티인 '뽐뿌'가 해킹되면서 190만명의 개인정보가 유출돼 원인 조사를 진행 중인 와중에도 보안에 계속 허점을 드러내고 있는 것으로 나타났다. 이에 뽐뿌 운영진은 타인 계정을 이용한 활동에 대해 실시간 모니터링을 통해 활동을 제한하는 한편 문제 현황을 확인하고 있다. 현재까지 추가 침입 등에 대한 문제 정황은 확인되지 않고 있다"며 "9월 11일 기준 6주간 미접속자에 대한 사전차단 조치가 진행됐다. 사건 이후 비변 미변경 계정에 대한 사안으로 판단되고 있다"고 밝혔다. 하지만 운영진의 공지와는 달리 해커가 해킹 사건이 일어난 지난달 11일 이후에 가입한 회원 아이디로도 글을 작성한 정황이 포착됐다.

- 해외 메신저 업데이트 프로그램으로 위장한 악성코드 발견

해외 유명 메신저 업데이트 프로그램으로 위장해 파밍 공격을 시도하는 악성코드가 발견됐다. 해당 악성코드는 드라이브 바이 다운로드(Drive-by-Download) 방식으로 불특정 다수를 대상으로 유포됐다. 해당 악성코드에 감염된 경우, PC 공인인증서 경로 파일이 전송돼 DNS 서버와 인터넷 시작 페이지 변조(파밍)로 금융정보 탈취를 시도해 금전 피해를 유발할 수 있다.

- 정부 홈페이지 일시 장애... 디도스 공격 의심

보안당국에 따르면 이날 오후 7시께 여성가족부와 정부통합전산센터 홈페이지에 잠시 접속장애 현상이 발생했다. 보안당국 관계자는 "오늘 오후 잠시 두 사이트 접속에 장애가 발생한 것은 사실"이라면서 "몇 초간 접속이 계속 끊기는 현상이 계속됐으나 서버가 다운돼 아예 접속이 차단된 수준은 아니었다"고 밝혔다. 정부는 이번 사고가 특정 사이트에 의도적으로 접속을 집중해 해당 사이트를 마비시키는 디도스(DDos·분산서비스 거부) 공격 수법으로 보고 조사를 벌이고 있다.

- 법원 "구글, 한국 이용자 정보 제공 내역 공개하라"

구글이 미국 정보기관 등에 넘긴 국내 이용자의 정보 내역을 공개해야 한다는 1심 판결이 나왔다. 서울중앙지법 민사합의22부는 16일 국내 인권활동가 6명이 미국 구글 본사와 구글코리아를 상대로 "개인정보 제3자 제공 내역을 공개하라"며 낸 소송에서 원고 일부 승소로 판결했다. 이들은 지난해 2월 구글이 미 국가안보국(NSA)의 프리즘(PRISM) 프로그램에 사용자 정보를 제공했고 이에 따라 자신들의 개인정보와 이메일(Gmail) 사용 내용이 넘어갔을 가능성이 있다며 정보공개 내역을 밝히라고 구글에 요구했다.

- 제2의 뽐뿌사태 막아라...정부, 내년 커뮤니티사이트 보안점검

정부가 지난 9월 발생한 휴대폰 온라인 커뮤니티 '뽐뿌' 해킹과 같은 사태가 재발하지 않도록 온라인으로 정보가 공유되는 커뮤니티 사이트에 대한 보안점검을 내년 상반기에 시행한다. 사이버안전 대진단은 사고가 발생하면 대응에 나서는 기존의 '사후·사고시 점검'을 '사전·상시점검' 태세로 바꿔 통신기반시설과 포털, 쇼핑몰 등에 대한 사이버보안 체계를 미리 점검하는 것으로, 지난 3월 400여개 시설을 대상으로 처음 실시했고 매년 상반기 지속적으로 실시한다.

10월의 취약점 이슈

Microsoft 10월 정기 보안 업데이트

- Internet Explorer용 누적 보안 업데이트(3096441)

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

- Microsoft Edge용 누적 보안 업데이트(3096448)

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

- 원격 코드 실행을 해결하기 위한 JScript 및 VBScript에 대한 보안 업데이트(3089659)

이 보안 업데이트는 Microsoft Windows의 VBScript 및 JScript 스크립팅 엔진의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 공격자가 Internet Explorer를 통해 취약성을 악용하도록 디자인된 특수 제작된 웹 사이트를 호스트(또는 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스트하는 웹 사이트나 공격에 노출된 웹 사이트 이용)한 다음 사용자가 이 웹 사이트를 보도록 유도하는 경우 원격 코드 실행을 허용할 수 있습니다. 또한 공격자는 사용자가 특수 제작된 웹 사이트로 이동하도록 IE 렌더링 엔진을 사용하는 Microsoft Office 문서 또는 응용 프로그램에 "초기화하기 안전"이라고 표시된 ActiveX 컨트롤을 포함시킬 수 있습니다.

- 원격 코드 실행을 해결하기 위한 Windows Shell에 대한 보안 업데이트(3096443)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 사용자가 Windows에서 특수 제작된 도구 모음 개체를 열거나 공격자가 사용자에게 특수 제작된 콘텐츠를 온라인으로 보도록 유도하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

- 원격 코드 실행을 해결하기 위한 Microsoft Office에 대한 보안 업데이트(3096440)

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

- 권한 상승을 해결하기 위한 Windows 커널에 대한 보안 업데이트(3096447)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 이러한 취약성 중 더 위험한 취약성으로 인해 공격자가 영향받는 시스템에 로그인하여 특수 제작된 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다.

- 해결법

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

한글 : <http://technet.microsoft.com/ko-kr/library/security/ms15-Oct>

영문 : <https://technet.microsoft.com/en-us/library/security/ms15-Oct>

VMware(ESXi, vCenter Server) 보안 업데이트 권고

VMware ESXi와 vCenter Server의 취약점을 해결한 보안 업데이트를 공지

- 상세정보

VMware ESXi OpenSLP 및 vCenter Server JMX RMI 원격 코드 실행을 이용한 피해가 발생할 수 있어 이용자들은 최신버전으로 업데이트 권고

- 해결법

vCenter Server 사용자

- 홈페이지 직접 설치: <https://www.vmware.com/go/download-vsphere> 링크에서 해당 버전을 다운로드하여 업데이트 진행

ESXi 사용자

- 홈페이지 직접 설치: <https://www.vmware.com/patchmgr/findPatch.portal#sthash.dUkCrU0Z.dpuf>

링크에서 해당 버전을 다운로드하여 업데이트 진행

- 참고사이트

<http://www.vmware.com/security/advisories/VMSA-2015-0007.html>

<https://www.7elements.co.uk/resources/blog/cve-2015-2342-remote-code-execution-within-vmware-vcenter/>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe사는 Adobe Flash Player에서 발생하는 6개의 신규취약점을 해결한 보안 업데이트를 발표

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

- 상세정보

임의코드 실행으로 이어질 수 있는 type confusion 취약점(CVE-2015-7645, CVE-2015-7647, CVE-2015-7648)

정보노출과 same-origin 정책을 우회할 수 있는 취약점(CVE-2015-7628)

Flash broker API에 심층 방어 기능 포함(CVE-2015-5569)

임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2015-7629, CVE-2015-7631, CVE-2015-7643, CVE-2015-7644)

임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점 (CVE-2015-7632)

임의코드 실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, CVE-2015-7634)

영향 받는 소프트웨어

- Adobe Flash Player 19.0.0.207 및 이전 버전

- Adobe Flash Player Extended Support Release 18.0.0.252 및 이전버전

- Adobe Flash Player for Google Chrome 19.0.0.207 및 이전 버전(CVE-2015-7852)

- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 19.0.0.207 및 이전 버전

- Adobe Flash Player for Internet Explorer 10 and Internet Explorer 11 19.0.0.207 및 이전 버전

- Adobe Flash Player Linux 11.2.202.535 및 이전 버전

- Adobe Air Desktop Runtime 19.0.0.190 및 이전 버전

- 해결법

Adobe Flash Player desktop runtime 사용자는 Adobe Flash Player 19.0.0.226 버전으로 업데이트 적용

- Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동업데이트를 이용하여 업그레이드

Adobe Flash Player Extended Support Release 사용자는 18.0.0.255 버전으로 업데이트 적용

리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.540 버전으로 업데이트 적용

구글 크롬 및 윈도우 8.x, 10 버전의 인터넷 익스플로러 10, 11, EDGE에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용

- 참고사이트

<https://helpx.adobe.com/security/products/flash-player/apsb15-27.html>

<https://helpx.adobe.com/security/products/flash-player/apsb15-25.html>

2015년 10월 Oracle Critical Patch Update 권고

Oracle Critical Patch Update(CPU)는 Oracle사의 제품을 대상으로 다수의 보안 패치를 발표하는 주요 수단

Oracle CPU 발표 이후, 관련 공격코드의 출현으로 인한 피해가 예상되는 바 Oracle 제품의 다중 취약점에 대한 패치를 권고

- 상세정보

2015년 10월 Oracle CPU에서는 Oracle 자사 제품의 보안취약점 154개에 대한 패치를 발표

해당 소프트웨어

- Oracle Database Server, version(s) 11.2.0.4, 12.1.0.1, 12.1.0.2

- Mobile Server, version(s) 10.3.0.3, 11.3.0.2, 12.1.0.0

- Oracle Access Manager, version(s) 11.1.2.2, 11.1.2.3

- Oracle Business Intelligence Enterprise Edition, version(s) 11.1.1.7, 11.1.1.9

- Oracle Endeca Server, version(s) 7.3.0.0, 7.4.0.0, 7.5.1.1, 7.6.1.0.0

- Oracle Enterprise Data Quality, version(s) 8.1, 9.0, 11.1.1.7.4, 12.1.3.0.0

- Oracle Exalogic Infrastructure, version(s) EECS 2.0.6.2.3

- Oracle Fusion Middleware, version(s) 10.1.3.5, 11.1.1.7, 11.1.1.8, 11.1.1.9, 11.1.2.1, 11.1.2.2, 11.1.2.3, 12.1.2.0, 12.1.3.0

- Oracle GlassFish Server, version(s) 3.0.1, 3.1.2

- Oracle HTTP Server, version(s) 10.1.3.5, 11.1.1.7, 11.1.1.9, 12.1.2.0, 12.1.3.0

- Oracle Identity Manager, version(s) 11.1.1.7, 11.1.2.2, 11.1.2.3

- Oracle JDeveloper, version(s) 11.1.2.4.0, 12.1.2.0.0, 12.1.3.0.0

- Oracle Mobile Security Suite, version(s) MSS 3.0

- Oracle Outside In Technology, version(s) 8.5.0, 8.5.1, 8.5.2

- Oracle Traffic Director, version(s) 11.1.1.7.0, 11.1.1.9.0

- Oracle WebCenter Content, version(s) 10.1.3.5.1- Oracle WebCenter Sites, version(s) 7.6.2, 11.1.1.6.1, 11.1.1.8.0

- Hyperion Installation Technology, version(s) 11.1.2.3

- Enterprise Manager Base Platform, version(s) 12.1.0.4, 12.1.0.5

- Enterprise Manager Ops Center, version(s) 12.1.0.1, 12.2.2

- OSS Support Tools, version(s) prior to 8.8.15.7.15

- Oracle E-Business Suite, version(s) 11.5.10.2, 12.0.6, 12.1.3, 12.2.3, 12.2.4

- Oracle Agile Engineering Data Management, version(s) 6.1.2.2, 6.1.3.0, 6.2.0.0

- Oracle Agile PLM, version(s) 9.3.3, 9.3.4
- Oracle Configurator, version(s) 12.0.6, 12.1.3, 12.2.3, 12.2.4
- Oracle Transportation Management, version(s) 6.1, 6.2
- PeopleSoft Enterprise FIN Expenses, version(s) 9.2
- PeopleSoft Enterprise FSCM, version(s) 9.2
- PeopleSoft Enterprise HCM, version(s) 9.2
- PeopleSoft Enterprise HCM Talent Acquisition Management, version(s) 9.2
- PeopleSoft Enterprise PeopleTools, version(s) 8.53, 8.54
- Siebel Applications, version(s) IP2014, IP2015
- Oracle Fusion Applications, version(s) 11.1.2 through 11.1.9
- Oracle Utilities Work and Asset Management, version(s) 1.9.1.1.2
- Oracle Communications Convergence, version(s) 2.0, 3.0.1
- Oracle Communications Diameter Signaling Router (DSR), version(s) 4.1.6 and prior, 5.1.0 and prior, 6.0.2 and prior, 7.1.0 and prior
- Oracle Communications LSMS, version(s) 13.1
- Oracle Communications Messaging Server, version(s) 7.0.5, 8.0
- Oracle Communications Performance Intelligence Center Software, version(s) 9.0.3 and prior, 10.1.5 and prior
- Oracle Communications Policy Management, version(s) 9.9.0 and prior, 10.5.0 and prior, 11.5.0 and prior, 12.1.0 and prior
- Oracle Communications Tekelec HLR Router, version(s) 4.0.0
- Oracle Communications User Data Repository, version(s) 10.2.0 and prior
- Oracle Retail Back Office, version(s) 12.0, 12.0IN, 13.0, 13.1, 13.2, 13.3, 13.4, 14.0., RM2.0
- Oracle Retail Central Office, version(s) 12.0, 12.0IN, 13.0, 13.1, 13.2, 13.3, 13.4, 14.0., RM2.0
- Oracle Retail Open Commerce Platform, version(s) 3.0
- Oracle Retail Returns Management, version(s) 12.0, 12.0IN, 13.0, 13.1, 13.2, 13.3, 13.4, 14.0., RM2.0
- Oracle Java SE, version(s) 6u101, 7u85, 8u60
- Oracle Java SE Embedded, version(s) 8u51
- Oracle JavaFX, version(s) 2.2.85
- Oracle JRockit, version(s) R28.3.7
- Fujitsu M10-1, M10-4, M10-4S Servers, version(s) prior to XCP 2271
- Integrated Lights Out Manager (iLOM), version(s) 3.0, 3.1, 3.2
- Solaris, version(s) 10, 11.2
- Oracle FS1-2 Flash Storage System, version(s) 6.1, 6.2, 6.3
- Oracle VM VirtualBox, version(s) prior to 4.0.34, prior to 4.1.42, prior to 4.2.34, prior to 4.3.32, prior to 5.0.8
- MySQL Enterprise Monitor, version(s) 2.3.20 and prior, 3.0.22 and prior
- MySQL Server, version(s) 5.5.45 and prior, 5.6.26 and prior

- 해결법

해결방안으로서 “Oracle Critical Patch Update Advisory – October 2015” 문서를 검토하고 벤더사 및 유지보수업체와 협의/검토 후 패치적용 요망
JAVA SE 사용자는 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나, Java 자동업데이트 설정을 권고

- 참고사이트

<http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html>
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
http://www.java.com/ko/download/help/java_update.xml

NTP 다중 취약점 보안 업데이트 권고

NTP(Network Time Protocol)에서 발생한 원격코드실행 등 총 13개의 취약점을 보완한 보안 업데이트를 발표
공격자는 취약점에 영향 받는 시스템에 악의적인 명령어 실행 등의 피해를 발생시킬 수 있으므로 해결방안에 따라 최신버전으로
업데이트 권고

- 상세정보

- crypto-NAK을 통해 인증을 우회하는 취약점(CVE-2015-7871)
- decodenetnum()함수에서 위조된 값에 대해 FAIL 반환하는 대신 오류 값을 발생하는 취약점(CVE-2015-7855)
- 패스워드 길이 처리하는 과정에서 발생하는 메모리 손상 취약점(CVE-2015-7854)
- refclock 드라이버에서 부적절한 데이터 길이로 인해 발생하는 버퍼오버플로우 취약점(CVE-2015-7853)
- ntpq atoascii()함수에서 발생하는 메모리 손상 취약점(CVE-2015-7852)
- saveconfig에서 발생하는 디렉토리 접근 취약점(CVE-2015-7851)
- NTP의 원격 구성 기능에서 발생하는 DoS 취약점(CVE-2015-7850)
- tursed key에서 발생하는 use-after-free 취약점(CVE-2015-7849)
- 조작된 패킷에 의해 7 loop counter를 처리할 때, 발생할 수 있는 Out-Of-Bounds 취약점(CVE-2015-7848)
- CRYPTO-ASSOC에서 발생하는 메모리 손상 취약점(CVE-2015-7701)
- "pidfile"과 "driftfile"만 허용 가능한 디렉토리 접근 취약점(CVE-2015-7703)
- timestamp 유효성 검사를 하는 클라이언트에서 발생할 수 있는 DoS 취약점(CVE-2015-7704, CVE-2015-7705)
- autokey 데이터 패킷 길이 체크 시 발생하는 취약점(CVE-2015-7691, CVE-2015-7692, CVE-2015-7702)
- Oracle Agile PLM, version(s) 9.3.3, 9.3.4

- 해결법

- 해당 취약점에 영향 받는 사용자는 아래 공식 업데이트 사이트에 방문하여 NTP 4.2.8p4버전으로 보안 업데이트 적용
- 공식 업데이트 사이트: <http://support.ntp.org/bin/view/Main/SoftwareDownloads>

- 참고사이트

- <http://support.ntp.org/bin/view/Main/SecurityNotice>
<http://www.ntp.org/downloads.html>

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

애플, 생산성 소프트웨어 패치; 모질라, 파이어폭스 보안 패치 진행

Apple Patches Productivity Software; Mozilla Updates Firefox with Security Fix

지난 목요일, 애플이 Keynote, Pages, Numbers, iWork 생산성 소프트웨어의 취약점 다수를 패치하였다.

가장 심각한 보안 취약점은 공격자가 Yosemite 10.10.4 및 이후 버전을 사용하는 OS X 컴퓨터 및 iOS 8.4 및 이후 버전을 사용하는 모바일 기기에서 코드를 실행하도록 허용하는 것이다.

Keynote 6.6, Pages 5.6, Numbers 3.6, iOS용 iWork 2.6이 익스플로잇을 포함한 문서를 파싱할 때 악용될 수 있는 다수 입력 승인 취약점(multiple input validation vulnerabilities)을 가지고 있었다. 애플은 위 프로그램에서 악성 문서를 열면 유저의 정보 도난으로 이어질 수 있다고 말했다. 이 문제는 입력 승인을 개선하는 것으로 해결되었다.

또한 Keynote에서는 악용이 가능한 메모리 충돌 취약점이 있었고, Pages와 Numbers에는 어플리케이션 충돌이 발생하며 결국 공격자가 해당 기기에서 코드를 실행할 수 있게 되는 취약점이 발견 되었다.

Pages에 존재하는 또 다른 메모리 충돌 취약점 또한 Pages를 충돌하게 하여 공격자가 그들이 원하는 코드를 실행할 수 있었다. 애플은 이를 메모리 처리를 개선하는 방식으로 해결하였다.

지난 목요일, 모질라에서도 Firefox 41.0.2를 발표했다.

업데이트된 버전의 브라우저는 “높음”으로 분류 되었던 cross-origin 제한 우회 취약점이 수정되었다.

모질라는 공지를 통해 파이어폭스의 fetch() API가 cross-origin 리소스 공유 내역을 제대로 실행하지 못했다고 밝혔다. 그 결과로, 공격자는 다른 origin으로부터 프라이빗 데이터에 접근할 수 있는 악성 웹페이지를 호스팅하는 것이 가능했다. 애플 보안 팀은 해당 취약점이 iOS 8.4.1에서 이미 수정 된 상태라고 밝혔다.

출처:

<https://threatpost.com/apple-patches-productivity-software-mozilla-updates-firefox-with-security-fix/115081/>

워드프레스 보안: 브루트포스 증폭 공격, 수천 개의 블로그 노려

WordPress Security: Brute Force Amplification Attack Targeting Thousand of Blogs

Sucuri의 연구원들이 워드프레스의 빌트인 XML-RPC 기능에 브루트 포스 증폭 공격을 가해 어드민 크리덴셜을 해킹해낼 수 있는 방법을 발견해냈다.

XML-RPC는 인터넷을 통한 컴퓨터간의 데이터 교환에 사용할 수 있는 가장 간단한 프로토콜 중 하나다. 이는 system.multicall 메소드를 사용하여 어플리케이션이 하나의 HTTP 요청으로 다수의 명령어를 실행할 수 있도록 한다.

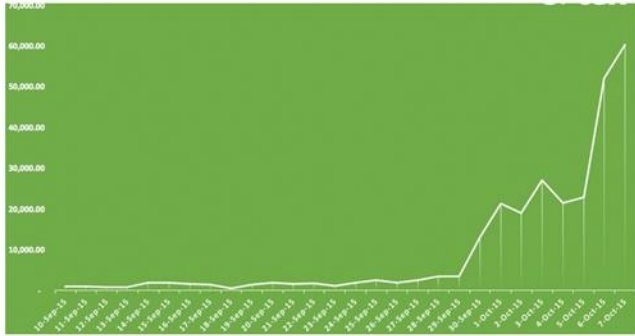
워드프레스와 드루팔을 포함한 다수의 CMS(Content Management System: 콘텐츠 관리 시스템)에서 XML-RPC를 지원한다.

하지만, 탐지를 피하고 하나의 HTTP 요청을 통해 수백 번의 패스워드를 시도하는 방법으로 브루트포싱 공격을 증폭시키기 위해 이 메소드가 악용 되고 있다.

- 증폭된 브루트포싱 공격

로그인 페이지에서 수천 개의 계정 및 패스워드 조합을 실행해보는 대신, (이는 IP 차단 등을 통해 쉽게 블록될 수 있다.) 공격자들은 system.multicall 메소드와 함께 XML-RPC 프로토콜을 사용하여 아래의 행동을 할 수 있다:

- 일반적인 브루트포싱 완화 제품에 탐지 되지 않는다.
- 수십만 개의 계정 패스워드 조합을 3, 4개의 XML-RPC 요청을 통해 시도한다



Sucuri는 이 타입의 공격이 지난 달 초에 시작 되었으며, 이달 초부터 하루에 60,000회 가량으로 증가하였다고 밝혔다.

- XML-RPC를 통한 브루트포싱 증폭 공격 예방법

이러한 위협으로부터 자신을 보호하려면, 단순히 XML-RPC의 접근을 모두 차단하면 된다.

xmlrpc.php를 사용하는 플러그인을 사용 중이 아닐 경우, 리네이밍 또는 삭제하면 된다. 하지만 JetPack과 같은 플러그인을 사용 중이라면, xmlrpc.php를 삭제할 경우 당신의 웹사이트의 일부 기능이 망가질 수 있다.

따라서, 웹마스터들은 WAF(웹 어플리케이션 방화벽)을 사용하는 XML-RPC system.multicall을 블록해야 할 것이다.

출처 : <http://thehackernews.com/2015/10/WordPress-BruteForce-Amplification.html>

스마트 TV, 스마트폰, 태블릿 탈옥 행위, 이제는 합법적으로 가능해져

It's Now Legal to Jailbreak Smart TV, Smartphone Or Tablet

EFF(Electronic frontier Foundation, 전자 프런티어 재단)이 미국 저작권 관리 사무소(DMCA)에서 진행하는 입법 절차에 참여한 결과 미 의회 도서관이 차의 소프트웨어를 고객이 직접 수리하거나 수정하는 것을 허락했을 뿐만 아니라 기기 잠금 해제, 탈옥, 재편집을 위해 영상물의 일부 추출 등을 허가하였다. 이로 인해 소비자들은

- DVD나 블루레이 디스크, 온라인 스트리밍 서비스의 영상물 일부를 추출하여 재편집(remix)에 활용할 수 있게 되었다.
- 구매한 폰, 태블릿, 스마트워치를 탈옥시키고 써드 파티 소스를 통한 OS 및 어플리케이션을 실행할 수 있게 되었다.
- 퍼블리셔가 더 이상 서비스 하지 않는 비디오 게임을 변경할 수 있게 되었다.

출처 : <http://thehackernews.com/2015/10/jailbreak-phones.html>

2. 중국

자동으로 앱을 내려받는 새로운 안드로이드 악성코드 GhostPush

新型安卓病毒GhostPush来袭: 自动下载安装应用

중국의 국가악성코드대응센터는 최근 a.expense.DhostPush.a라는 안드로이드 악성코드가 급속도로 전파되고 있어 사용자들의 주의가 필요하다고 하였다. 이 악성코드는 전파형 악성코드로, 휴대폰을 키면 자동으로 실행되며, 자동으로 다른 앱을 내려받고 시스템에 몰래 설치한다. 이 모든 과정은 사용자가 모르게 진행되며, 각종 사용자 정보를 해커 서버로 전송한다. 또한 끊임없이 다른 앱을 내려받기 때문에, 모바일 데이터를 낭비하게 되며, 정상적으로 지워지지도 않는다.

분석결과, 이 악성앱은 사용자 휴대폰에 설치된 후에 기기관리자 권한을 획득하여 사용자의 동의 없이 folder DB에 있는 정보들을 해커의 서버로 전송한다. 현재 국가악성코드대응센터에서는 해당 악성코드를 치료할 수 있는 백신을 배포 중에 있다.

출처 : <http://www.ithome.com/html/android/183018.htm>

많은 네티즌들이 Wangyi이메일이 해킹당해 계정정보가 유출되었다고 하였다.

大量网友称网易邮箱被破解: 绑定账号遭泄露

10월 17일 저녁부터 많은 네티즌들이 wangyi 이메일이 해킹을 당해 이메일 정보가 유출되었다고 밝혔다. 사용자들은 wangyi 계정을 다른 홈페이지 계정들과 연동시켜 놓아 다른 계정들도 함께 해킹 당했을 것으로 추측된다. 또한 많은 iPhone 사용자들은 자신의 Wangyi 계정과 연동된 Apple ID가 등록된 휴대폰이 잠겼으며, 데이터가 모두 삭제되었다고 주장했다. 이 사건에 대하여 애플 사용자가 추적을 해 본 결과, 이와 같은 현상은 10월 15일에 집중해서 발생하였으며, 사용자 대부분은 wangyi 이메일을 사용하고 있는 것으로 나타났다. 네티즌들은 wangyi의 DB가 해킹을 당한 것이 아닌가라고 추측하였으며, 웨이보 인기 검색어에는 "wangyi이메일" "wangyi DB 유출" 등이 순위권에 올라와 있다. Apple ID 뿐만 아니라 wangyi 계정과 연동된 파일 공유 사이트 계정들도 모두 유출된 것으로 추측되고 있다.

이러한 사건에 대하여 wangyi그룹은 공식 발표를 하였으며, 내용은 아래와 같다.

"금일 wangyi이메일 DB유출과 관련하여 유언비어가 퍼져 사용자들을 불안에 떨게 하였는데, 이는 모두 사실이 아니다. wangyi이메일은 중국 내에서 가장 뛰어난 기술을 보유하고 있으며, 이메일 시스템 영역에서 중국 내 유일하게 중국 최고 보안등급인 EAL3+ 인증을 받았다. 뿐만 아니라 끊임없이 이메일 보안 기술 영역에 대하여 연구를 진행하고 있으며, 높은 보안성과 앞선 기술로 모든 중국 사용자들에게 더 나은 서비스를 제공하기 노력하고 있다. 이번에 DB유출 이슈와 관련하여 보안점검을 실시한 결과, DB유출 징후가 포착되지 않았다. 계정이 유출된 일부 사용자들은 다른 홈페이지와 wangyi 이메일의 계정정보를 동일하게 사용하여 유출된 것 같다"고 하였다

公告

今日谣传网易邮箱出现数据泄露，引起用户恐慌。网易邮箱团队现郑重声明，此报道不实。

网易邮箱拥有国内最高等级，同时也是邮件系统领域唯一的最高级别的安全证书 EAL3+，是最值得信赖的帐号系统之一。同时，网易邮箱在安全技术领域持续升级，保持在安全技术领域的领先地位，为广大用户邮件系统安全保驾护航。本次事件经严密的技术排查，网易邮箱不存在自身数据泄露问题。此次事件，是由于部分用户在其他网站使用了和网易邮箱相同的帐号密码，其他网站的帐号信息泄露，被不法分子利用，侥幸尝试登录网易邮箱造成。

网易邮箱团队提醒广大用户，在互联网上，不建议在安全级别较低的普通网站使用与个人邮箱、金融支付等高安全需求平台相同的帐号密码体系。避免在普通网站的帐号信息泄露后，影响到您在高安全需求平台的帐号安全。

网易邮箱运营 18 年，产品安全是我们的立足之本，我们也将一直为追求最极致的安全服务而努力。在成长的道路上，我们非常欢迎广大用户给予反馈和建议，网易邮箱团队将认真聆听采纳。但对任何恶意中伤的不实报道，网易公司将保留追究法律责任的权利。



——网易邮箱团队

由橘子便签发送 via Smartisan Notes

출처 : <http://www.163.com/html/it/183005.htm>

3. 일본

88개의 금융기관을 노리는 악성코드 – 가짜 금융청사이트에서 정보사취

88の金融機関を狙うマルウェア – 偽金融庁サイトで情報詐取

일본국내의 온라인뱅킹 이용자를 표적으로 한 새로운 악성코드 ‘Win32/Brolux.A’가 확인되었다. 88개의 일본국내 금융기관을 대상으로 하고 있어, 금융청을 가장한 피싱페이지로 유도, 계정정보를 탈취하고 있었다..



[유도처인 피싱페이지 (화면 : ESET)]

이 악성코드를 검지한 ESET에 따르면 이번의 감염활동에서는 기지(口知)의 취약성 2건을 악용하였다. 하나는 이탈리아의 보안기업 Hacking Team에서 유출한 ‘Adobe Flash Player’의 ‘CVE-2015-5119’였다. 게다가 2014년에 수정된 ‘Internet Explorer’의 취약성 ‘CVE-2014-6332’를 이용하고 있었다.

‘CVE-2015-5119’는 이미 익스플로잇 킷에 장착되는 등 악용이 확산되고 있다. 그러나 이 회사의 분석으로는 이번 공격에 익스플로잇 킷은 사용되지 않고 해석도 용이했다고 한다. 동영상파일을 가장한 익스프로잇은 악질적인 어덜트사이트 ‘dmmm.jp’에서 배포되고 있었다. 다운로드된 트로이의 목마 ‘Win32/Brolux.A’는 ‘Internet Explorer’ ‘Chrome’ ‘Firefox’에서 열람되는 페이지의 URL이나 제목 등을 감시한다. 금융기관의 페이지로 접속했을 때에 금융청이나 검찰청의 페이지로 보이게 한 피싱페이지로 유도한다.

문제의 피싱페이지는 도메인 ‘fas-go-jp-security.kensatsutyo.com’에서 발신했다. 온라인뱅킹을 노린 범죄가 늘어나고 있다는 등으로 설명하고 금융기관에서 보안 레벨업을 실행하고 있다는 등의 설명으로 속이는 내용이었다.

온라인뱅킹에서 이용하는 ‘질문’이나 ‘암호’외에 계좌번호, 비밀번호, 제2비밀번호, 메일주소, 메일의 패스워드 등을 송신시키려고 한다. 유도처인 피싱 사이트에는 일부 중국어에 의한 기재가 있었던 점 등 악성코드의 서명에는 중국기업으로 발행된 전자증명서가 이용되고 있었다고 한다. 과거에 한국의 온라인뱅킹을 노린 공격과의 유사점도 있다고 이 회사는 지적하고 있다.

이 회사는 악용되고 있는 취약성은 기지(口知)의 것이며, 최신 소프트웨어라면 막을 수 있다고 설명한다. 또한 온라인뱅킹에 새로운 콘텐츠가 추가된 것처럼 보이는 경우, 경계하는 것이 중요하다고 어드바이스하고 있다.

출처 : <http://www.security-next.com/063408>

수상한 친구신청에 주의, 기업에서 확산의 우려도

不審な友達申請に注意、企業で拡散の恐れも

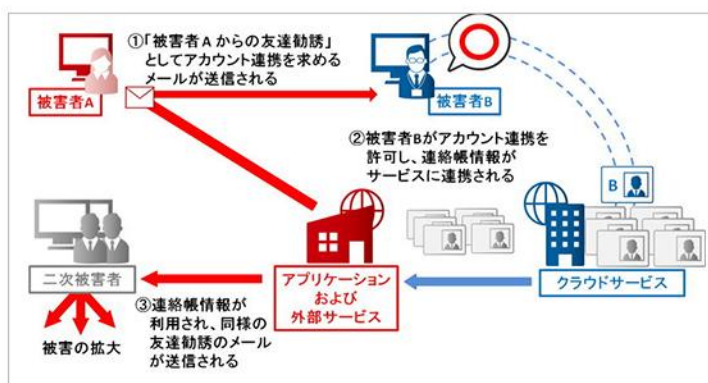
정보처리추진기구(IPA)는 10월28일, 해외SNS에서 송신된 친구 리퀘스트에 관한 주의를 호소했다. 승인해버리면 유저의 이름으로 Google에 등록된 메일주소로 초대메일이 송신되어버린다고 해서 특히 Google Apps를 이용해서 독자 도메인의 메일을 이용하는 조직에서는 영향이 우려된다고 한다.

IPA에서는 이 종류의 상담이 5월경부터 와서 10월은 23일 현재 39건으로 급증했다고 한다. JPCERT 코디네이션센터(JPCERT/CC)에 따르면, 같은 날 현재 18개의 조직이 이 문제에 대해서 정보를 공개하고 있다고 한다.

친구 리퀘스트의 메일은 넷서비스의 연계기능을 이용하여 해외의 SNS에서 송신되고 있는 것으로 보인다. SNS에서의 메일이 요구하는 서비스연계를 허가해버리면 유저가 등록하고 있는 Google의 연락처로 접속을 허가해 버린다.



[친구 리퀘스트의 예 (IPA에서)]

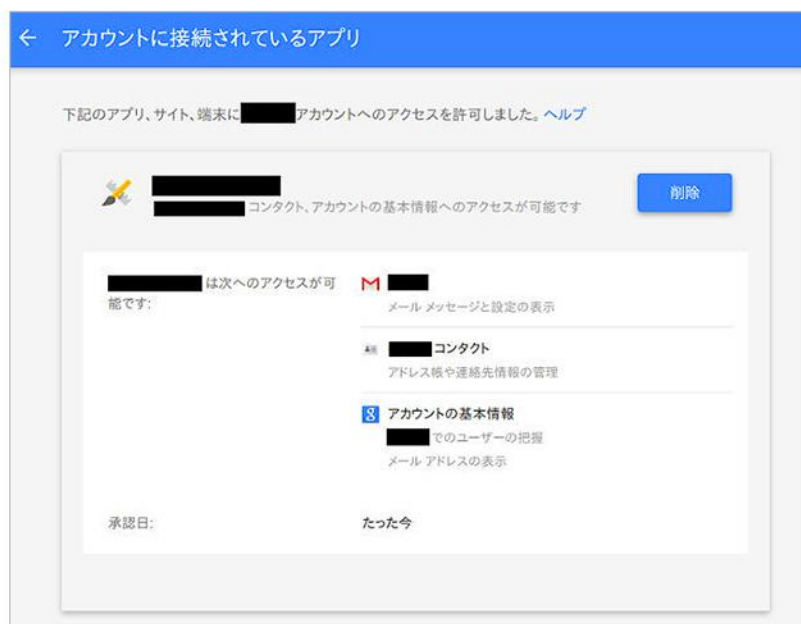


[피해발생까지의 흐름 (JPCERT/CC에서)]

정보처리추진기구(IPA)는 10월28일, 해외SNS에서 송신된 친구 리퀘스트에 관한 주의를 호소했다. 승인해버리면 유저의 이름으로 Google에 등록된 메일주소로 초대메일이 송신되어버린다고 해서 특히 Google Apps를 이용해서 독자 도메인의 메일을 이용하는 조직에서는 영향이 우려된다고 한다.

IPA에서는 이 종류의 상담이 5월경부터 와서 10월은 23일 현재 39건으로 급증했다고 한다. JPCERT 코디네이션센터(JPCERT/CC)에 따르면, 같은 날 현재 18개의 조직이 이 문제에 대해서 정보를 공개하고 있다고 한다.

친구 리퀘스트의 메일은 넷서비스의 연계기능을 이용하여 해외의 SNS에서 송신되고 있는 것으로 보인다. SNS에서의 메일이 요구하는 서비스연계를 허가해버리면 유저가 등록하고 있는 Google의 연락처로 접속을 허가해 버린다.



[서비스 연계의 관리화면 (JPCERT/CC에서)]

출처 : <http://www.itmedia.co.jp/enterprise/articles/1510/28/news122.html>

Apple ID의 사인 인(sign in)을 요구하는 가짜 사이트, 일본에서도 10월 들어서 보고가 급증

Apple IDのサインインを求める偽サイト、日本でも10月に入って報告が急増

Apple ID의 사취(詐取)를 목적으로 한 피싱 사이트의 보고가 늘어나고 있다고 해서 피싱대책협의회가 28일 긴급정보를 냈다.



[Apple ID의 피싱사이트 (피싱대책협의회 긴급정보에서 화면)]

Apple의 사이트를 가장한 이 피싱사이트는 Apple ID의 계정정보의 확인과 업데이트를 위해서라고 하며 Apple ID와 패스워드 입력을 독촉하는 것이다. 해외에서 증가경향에 있으며, 일본에서도 수 년 전부터 보고가 있었다고 한다. 이것이 올해 10월에 들어 보고가 급증했다. 피싱대책협의회에 들어온 보고건수는 4월 이후 1개월에 4~5건 정도였던 것이 10월은 45건으로 증가하고 있다. (10월29일 시점)

피싱대책협의회에서는 이미 10월2일 시점에서 일본어에 의한 Apple ID의 피싱사이트에 대해서 긴급정보를 내고 있었지만 이번에 다시 주의를 호소한 모양새다.

피싱대책협의회에서는 Apple ID가 사취되면 아래와 같은 피해를 입는 경우가 있다고 해서 Apple ID의 피싱사이트에서는 절대 정보를 입력하지 않도록 주의를 촉구하는 동시에 만일 정보를 입력한 경우는 신속하게 Apple 등에 상담하도록 요구하고 있다.

iCloud서비스에 보존되어 있는 iPhone의 백업데이터 등에 부정 접속된다.

백업데이터(메모 등)에 금융기관 등의 로그인 ID와 패스워드 등이 포함되어 있는 경우, 부정송금의 피해를 입는 경우가 있다.

iPhone상, 혹은 iCloud서비스에 보존되어 있는 연락처와 메일데이터가 삭제된다.

메일주소가 탈취되어서 진짜를 가장한 메일이 송신된다.

Apple Store서비스에 있어서 금전적인 피해(크레디트카드 피해)가 발생한다.

또한 복수 서비스에서 같은 패스워드를 계속 돌려서 사용하고 있으면, 백업데이터를 바탕으로 다른 서비스(웹 메일과 SNS 등)에 부정으로 접속되는 등의 피해도 발생한다고 하며 같은 패스워드를 돌려서 사용하지 않을 것을 권고하고 있다.

출처 : http://internet.watch.impress.co.jp/docs/news/20151029_728171.html

알약 11월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr