안랩 온라인 보안 매거진

월간 安

2016. 02

Mobile Security

CONTENTS

영화 오블리비언과 C&C 서버

다소 어렵게 느껴지는 오블리비언(Oblivion)이란 단어를 처음 접한 것은 아르헨티나의 유명한 탱고 작곡자 피아졸라의 곡 제목에서였다. '망각'이라는 뜻의 이 단어는 꼭 기억상실증과 관련된 영화에 쓰일 것만 같았다. 그러나 연초의 강추위를 피해 따뜻한 아랫목에서 보기에 적당한 SF 영화의 제목으로 사용되었고, 톰 크루즈가 주인공으로 나와서 지구를 탐험하는 듯한 포스터에서 그 의미를 찾아서 연결해 보기란 쉽지 않을 것 같다.

2013년에 개봉된 영화 오블리비언은 톰 크루즈, 모건 프리먼, 올가 쿠릴렌코가 주연한 영화로, 가까운 미래의 어느 시점에 외계인의 침공 후 폐허가 되어버린 지구를 순찰하는 임무를 맡은 주인공인 잭 하퍼의 이야기이다.

49번 지역을 할당 받아서 순찰 임무를 맡은 주인공은 다른 지역은 방사능이 심해서 들어갈 수 없다는 지침 하에 구름 위에 떠 있는 49번 센터에 복귀하여 정기적인 보고를 하는 임무를 가지고 있었다. 파견 기간을 다 채워야 중앙 센터로 복귀할 수 있기 때문에, 49번 센터의 담당자와 파트너가 되어서 주기적인 임무만을 수행할 뿐이었다.

이렇게 하나의 지휘센터와 순찰 임무가 연결되어서 명령을 내리고 정보를 전달 받아서 다음 임무를 주고 받는 관계는 악성코드의 일종인 트로이목마(Trojan)가 중앙 관제 센터 역할을 하는 C&C(Command and Control) 서버와 연결되어서 명령을 수행하는 체계와 동일하다. C&C 서버의 명령에 따라서 해당 시스템의 정보를 수집하고, 정보를 C&C 서버로 전송하며, 다음의 명령에 따라서 파일을 다운로드하거나 시스템을 감염시키는 2차적인 행동을 하게 된다.

▲오블리비언 공식 포스터

차이라면 C&C 서버는 많은 양의 트로이목마를 뿌리고 조정하는데, 영화에서 49번 센터의 잭 하퍼는 오직 49번 센터의 명령과 관리를 받는다는 점이다.

영화 속에서 하퍼는 정기적으로 맡은 지역을 돌아다니다가 정체불명의 우주선을 발견하게 된다. 그 후 자신을 알고 있는 여자 주인공을 만나게 되면서 혼란스러워 하던 중 지하조직의 리더와 조우하게 되면서 더 큰 혼란 속으로 빠져들게 된다. 지하조직의 이야기대로 자신이 기억을 잃어버린 채로 중앙 센터에 있는 컴퓨터의 명령을 받고 있다는 것을 깨달은 뒤에야 자신의 과거를 되돌리기 위해서 싸우게 되는데, 결국 52번 센터만 좋은 일을 하게 된다.

영화 '오블리비언'을 보안으로 풀어서 이야기하다 보니 얼마 전 상영했던 '스타워즈 – 깨어난 포스'의 자쿠 행성이 생각나기도 하고, 아이유의 모던 타임즈(Modern Times) 앨범에 있는 '오블리비아테(Obliviate)'란 노래가 떠오르기도 한다. 우리가 과거에 무심코 설치했던 프로그램과 다운로드한 파일들을 잊어버리고 있는 사이에 망각 속을 뚫고서 시스템 장애를 일으키거나 랜섬웨어를 불러올 수 있으니, 잊어버리지 말고 시스템을 점검하는 습관을 들이는 것이 좋겠다.

안랩, 새로워진 'V3 모바일 시큐리티' 출시

고도화되는 모바일 위협, 해답은?

모바일 위협으로 인한 피해가 지속적으로 늘고 있는 가운데 안랩이 최근 새로운 모바일 보안 솔루션 AhnLab V3 Mobile Security(이하 'V3 모바일 시큐리티')를 출시해 이목이 집중되고 있다. 1월 28일 서비스를 시작한 이 제품은 다수의 글로벌 테스트 기관에서 최고의 성적을 거둔 V3 Mobile 엔진을 기반으로 세계 수준의 강력한 안티바이러스 성능을 제공한다. 또한 프라이버시 보호 기능과 원터치 보안 점검 기능 등이 더해져 사용자의 편의성과 보안성을 모두 만족시킬 제품으로 기대되고 있다.

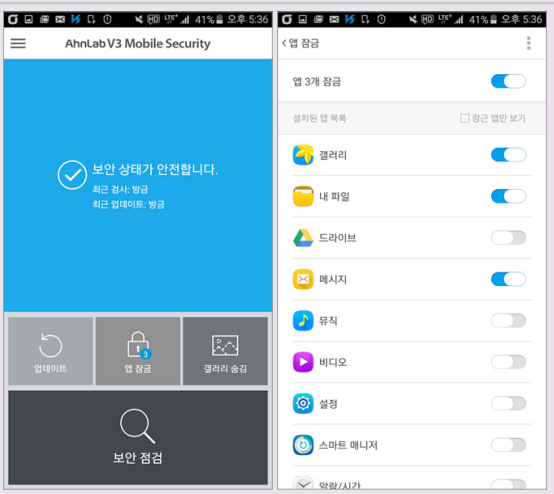
스미싱에 이어 최근에는 악성 앱을 이용한 모바일 랜섬웨어가 등장하는 등 모바일 위협이 날로 고도화되고 있다. 한국인터넷진흥원이 발표한 '2015년 모바일 보안 기획조사'에 따르면 스마트폰 사용자 중 87.7%는 모바일 보안에 관심이 있는 것으로 조사됐다. 이 같은 높은 관심에도 불구하고 모바일 보안이 어렵다고 응답한 비율이 73.6%로 높게 나타났다. 악성코드, 스미싱, 개인정보 유출 등 모바일 보안 위험은 알고 있으면서도 모바일 기기를 보호하는 방법에 어려움을 느끼고 있다는 방증이다. 이는 곧 안심하고 사용할 수 있는 간편하고 쉬운 보안 솔루션이 절실하다는 의미이기도 하다.

[그림 1] 모바일 보안 관심 및 체감 난이도
(단위 %, *출처: 한국인터넷진흥원 '2015 모바일 보안 기획조사')

'V3', 모바일 환경에서도 명불허전

전 세계적으로 안드로이드(Android) 기반의 모바일 위협이 증가하고 있는 가운데 국내 모바일 환경은 안드로이드 운영체제를 기반으로 하고 있다 해도 과언이 아니다. 미래창조과학부의 '2015년 하반기 국내 인터넷 이용환경 현황조사'에 따르면 안드로이드 기반의 스마트폰이 84.11%에 달하는 것으로 나타났다.

이처럼 안드로이드 중심의 국내 모바일 환경과 사용자의 보안에 대한 심리적 거리감을 해소할 수 있는 모바일 보안 솔루션이 바로 'V3 모바일 시큐리티'다. 안랩은 더욱 안전한 모바일 환경을 구현하기 위해 스마트 모바일 기기와 관련해 발생할 수 있는 다양한 보안 위협은 물론 사용자들의 요구까지 다각도로 분석해 제품에 반영했다.



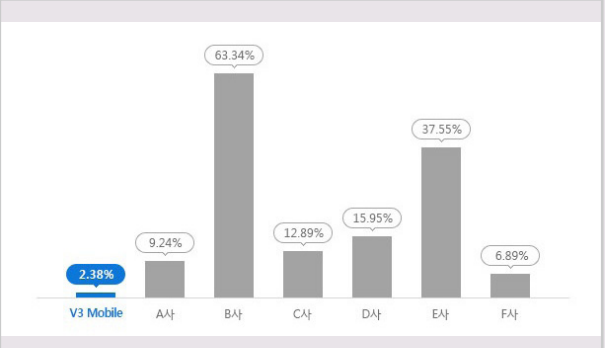
[그림 2] V3 모바일 시큐리티

V3 모바일 시큐리티의 가장 큰 장점은 강력한 안티바이러스 기능이다. V3 모바일 시큐리티는 안드로이드 플랫폼을 공격하는 모바일 악성코드와 사용자 동의 없이 개인정보에 접근해 정보를 유출하는 유해한 악성 프로그램을 탐지한다. 실시간 감시 기능을 통해 앱 설치 시 또는 업데이트 시 앱의 안전성 여부를 검사하며, 설치한 앱에 대한 '빠른검사', 불필요한 앱(Potentially Unwanted Application, PUA) 및 파일 폴더에 대한 '정밀검사' 기능을 제공해 스마트폰을 안전하게 보호한다.

세계가 인정한 강력한 모바일 백신

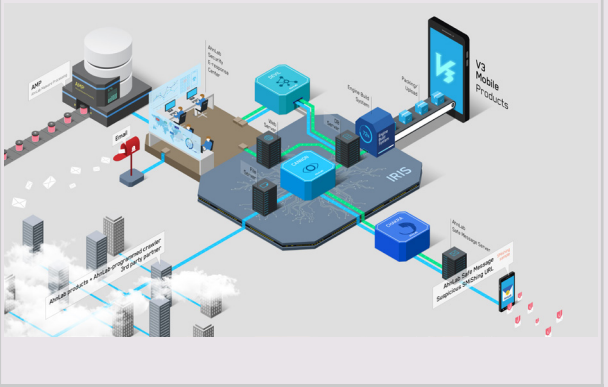
이 같은 V3 모바일 시큐리티의 경쟁력은 이미 글로벌 시장에서도 정평이 나있다. 안랩의 V3 모바일 엔진은 국내에서 유일하게 AV-TEST가 모바일 분야 테스트를 시작한 2013년 이래 매회 빠짐없이 참가해 18회 연속 인증을 획득했다. 또한 2014년부터 지난해 9월까지 진행된 테스트 중 9회에 걸쳐 100%의 악성코드 진단율을 기록하기도 했다.

보안 검사 시 배터리 소모, 단말 속도에 미치는 영향 등을 평가하는 사용성(Usability) 부문에서도 테스트에 참가한 25개 보안 제품의 평균 CPU 사용률 22.86% 대비 10분의 1에 불과한 2.38%를 기록하는 등 압도적인 성적으로 1위를 차지했다.



[그림 3] 주요 모바일 보안 솔루션의 보안 검사 시 CPU 사용률 (*출처: AV-TEST, 2015.09)

이처럼 V3 모바일 시큐리티가 세계적으로 인정받을 수 있는 힘은 바로 안랩의 20여 년의 모바일 위협 대응 노하우와 독자적인 모바일 위협 대응 프로세스에 있다. 안랩은 자사 악성코드 분석가와 그들의 노하우가 적용된 자동화 시스템을 통해 모바일 악성코드 수집부터 엔진 룰 반영까지 채 20분도 걸리지 않는다. 특히 최근 개발한 DEVIL(DEx VIsualLizer) 시스템은 모바일 앱의 라이프사이클(Life cycle)을 그래프 형태로 보여주는 애널라이저(Analyzer)로, 이를 통해 악성 앱의 컴포넌트들의 연관 관계를 파악하고 악성 행위를 진단할 수 있다. 또한 안드로이드 파일에 특화된 '캐쉬앤핑거프린트 기법'을 이용해 진단 속도 향상을 이뤄내 AV-Comparatives 및 AV-TEST에서 세계 최상위권 성적을 기록하며 기술력을 인정받고 있다.



[그림 4] 안랩 모바일 위협 대응 프로세스

쉽고 편리한 프라이버시 보호, 원터치 보안 점검 기능 더해

V3 모바일 시큐리티의 또 다른 강점 중 하나는 프라이버시 보호 기능이다. 보안코드를 이용해 선택적으로 앱을 잠글 수 있는 '앱 잠금' 기능과 갤러리 내의 사진과 동영상 파일을 숨겨 프라이버시 노출을 방지할 수 있다.

또한 '개인정보보호 도우미' 기능을 통해 기기 관리자의 권한이나 오디오 녹음, 결제 유발, 단말 위치 정보 사용, 사용자의 연락처 접근 등 기기에 설치된 솔루션이 요구하는 권한을 사용자에게 안내함으로써 사용자가 무심코 지나칠 수 있는 개인정보의 유출 위험을 사전에 방지한다.

또한 '원터치(One-Touch) 보안 점검' 기능을 이용해 OS 변조 여부나 기기의 루팅 여부, 알 수 없는 소스 허용 여부, 화면 잠금 사용 여부 등을 쉽게 확인할 수 있다. 이 밖에도 엔진 업데이트와 함께 웹 브라우저의 접속 기록, 클립보드 기록, 캐시 데이터를 삭제하는 기능도 있다. V3 모바일 시큐리티를 사용하는 것만으로도 스마트폰 보안 걱정을 덜 수 있는 이유가 바로 여기에 있다.

세계적으로 인정받은 안랩의 모바일 위협 대응 기술이 총망라된 V3 모바일 시큐리티는 사용자의 스마트폰을 안전하게 보호할 뿐만 아니라 더욱 안전하고 편리한 모바일 보안 환경을 구축하는데도 크게 기여할 것으로 기대된다.

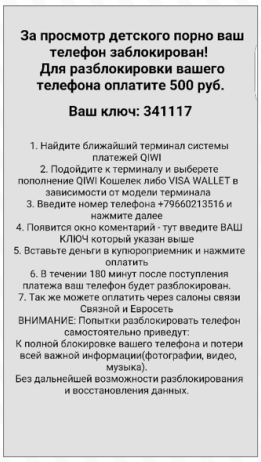
유포 방법에서 예방까지 '모바일 랜섬웨어의 모든 것'

모바일까지 눈독 들이는 랜섬웨어를 막아라!

2015년 보안 업계의 화두는 단연 '랜섬웨어'였다. 안랩을 비롯한 많은 보안 업체들은 2016년에도 랜섬웨어의 광풍이 지속될 것으로 전망하고 있다. 특히, 스마트폰 사용자를 대상으로 한 모바일 랜섬웨어도 주의 대상이다. 다행이 아직까지 국내에서는 모바일 랜섬웨어 감염이 확인된 바 없다. 그러나 PC 랜섬웨어도 해외에서 활발히 활동하다 한국에 등장했다. 모바일 랜섬웨어도 현재 급격한 증가 추세를 보이고 있으므로, 이에 대한 주의와 관심이 필요하다.

이 글에서는 모바일 랜섬웨어의 유포 방법, 특징, 수동 제거 방법, 예방법에 대해 자세히 살펴본다.

어느 날 갑자기 스마트폰이 잠겨버려 더 이상 아무것도 할 수 없게 되는 일을 상상해본 적이 있는가? 스마트폰의 잠금 화면 비밀번호를 잃어버려서가 아니다. 스마트폰이 고장 난 것은 더더욱 아니다. 스마트폰을 대상으로 하는 랜섬웨어에 감염됐을때 일어날 수 있는 일이다.

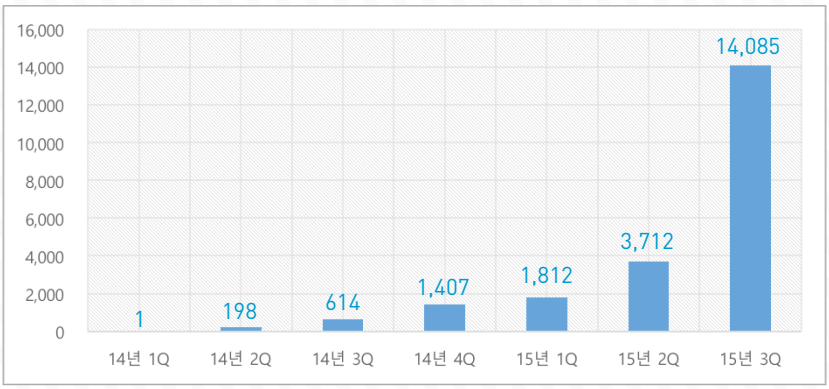


[그림 1] 랜섬웨어에 감염된 스마트폰

모바일 랜섬웨어에 감염되면 스마트폰을 이용하는데 큰 제한이 생기거나 제거하기 전까지 스마트폰을 사용하지 못하게 될 수 있다. 랜섬웨어에 따라 스마트폰에 저장된 파일을 암호화하거나 삭제해버리기도 한다. 대부분의 랜섬웨어는 스마트폰의 '기기 관리자'로 등록되고 삭제를 방지하는 기능들을 포함하고 있어 제거도 어렵다. 심지어 스마트폰을 공장 초기화해야만 치료가 가능한 경우도 있다.

이처럼 랜섬웨어에 감염되면 지금 내 손에 스마트폰이 쥐어져 있음에도 불구하고 랜섬웨어 혹은 해커에게 스마트폰과 내 정보를 고스란히 인질로 내주는 꼴이 된다.

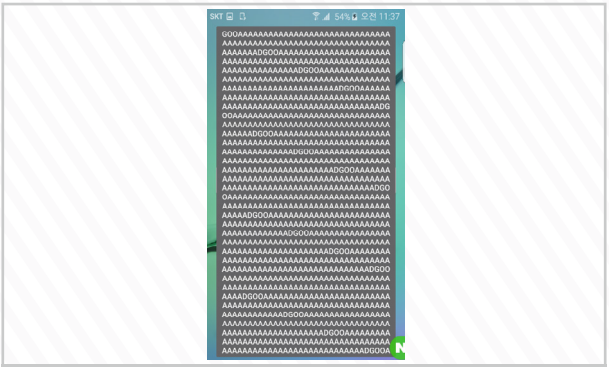
최근 전 세계적으로 PC 기반 랜섬웨어가 많이 유포되어 많은 피해가 발생하고 있는데 모바일 역시 랜섬웨어의 주요 타깃이 되고 있다. 최근 통계를 보면, 2015년 3분기까지 발견된 모바일 랜섬웨어는 2014년 대비 약 8.8배 증가했다.



[그림 2] 모바일 랜섬웨어 연간 통계

현재까지 모바일 랜섬웨어는 PC 기반 랜섬웨어와 달리 한국을 대상으로 하는 것은 보고된 바가 없고 주로 동유럽권 국가와 중국 등을 대상으로만 활동하고 있다. 그러나 한국에서만 사용되는 앱의 아이콘을 도용하고 화면을 점유해 스마트폰을 사용할 수 없게 만드는 'Android-Trojan/Blocker'가 발견된 바가 있고 화면 잠금에 이어 금전을 요구하면 바로 랜섬웨어가 되는 것이므로 국내 또한 모바일 랜섬웨어 안전지대라 할 수 없다.

[그림 3] Android-Trojan/Blocker 아이콘


[그림 4] Android-Trojan/Blocker 감염 화면

갈수록 증가하는 모바일 랜섬웨어 위협에 대응하기 위해 랜섬웨어가 어떤 방법으로 유포되는지 알아보고 최근까지 발견된 모바일 랜섬웨어를 유형별로 자세히 살펴보자. 또한, 랜섬웨어에 감염되었을 경우 대처하기 위한 수동 제거 방법과 랜섬웨어 피해 예방법을 알아보도록 한다.

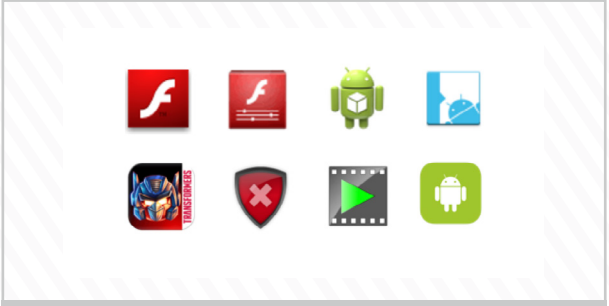
모바일 랜섬웨어 유포 방법

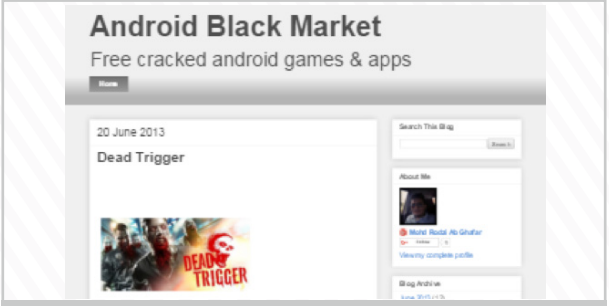
현재까지 한국을 대상으로 하는 모바일 랜섬웨어는 보고된 바 없으며 주로 동유럽, 영어권 국가, 중국 등의 국가에서 피해가 발생하고 있다. 하지만 아직까지 국내 모바일 랜섬웨어 위협이 뚜렷하게 없다고 해서 안심할 건 아니다. 유포 자체가 인터넷이나 SMS 등으로 이뤄지기 때문에 사실 인터넷에 연결된 누구라도 피해자가 될 수 있다. 지금부터 알려진 모바일 랜섬웨어 유포 방법에 대해 좀 더 자세히 알아보자.

1. 성인물 사이트를 통한 다운로드

성인물 사이트는 모바일 랜섬웨어 유포에 흔히 사용된다. 공격자는 성인물 사이트에서 성인 앱을 위장한 모바일 랜섬웨어 다운로드를 유도한다. 앱이 자동으로 설치되지는 않으며 다운로드 된 APK 파일을 터치할 경우 앱 설치 화면으로 넘어간다. 설치 완료와 동시에 기기 관리자 권한 획득을 시도하며, 이후에 바로 랜섬웨어 기능을 시작한다.

2. 블랙마켓을 통한 다운로드


[그림 5] 모바일 랜섬웨어가 애용하는 아이콘



[그림 6] 안드로이드 블랙 마켓

[그림 5]는 모바일 랜섬웨어가 주로 위장하는 앱의 아이콘을 나타낸 것이다. 어도비 플래시 플레이어, 안티바이러스 앱, 유명 게임 아이콘, 비디오 플레이어, 안드로이드 시스템 아이콘 등을 주로 이용한다. 공격자는 이런 사용자 접근성이 높은 앱으로 위장한 랜섬웨어를 블랙마켓에 업로드한 뒤 다운로드를 유도한다.

3. SMS/MMS를 이용한 피싱

플래시 플레이어 업데이트 또는 금융기관 등을 사칭하며 랜섬웨어 다운로드 링크를 포함한 SMS나 MMS를 유포한다. 다운로드 링크를 클릭하면 자동으로 다운로드 되며 마찬가지로 다운로드한 파일을 터치하면 설치가 시작된다.

지금까지 모바일 랜섬웨어가 유포되는 방법을 살펴보았다. 다양한 랜섬웨어가 발견되었으나 유포 방법은 기존 악성앱이 사용하는 방식과 크게 다르지 않으며, 대상을 랜섬웨어로 좁혀 보면 오히려 유사한 점들이 많다. 특히 성인앱을 위장한 유포 방법은 모바일 랜섬웨어에서 두드러지게 나타난다.

이제부터 모바일 랜섬웨어의 유형을 살펴보며 어떤 방법으로 스마트폰을 사용 불가능하게 만드는지, 어떤 방법으로 사용자를 속이고 협박하는지 자세히 알아보도록 하자.

모바일 랜섬웨어의 유형별 기능 및 특징

1. 심플락(Android-Trojan/Simplelock)

심플락(Android-Trojan/Simplelock)은 사용자의 스마트폰을 사용 불가능 상태로 만들고 사용자를 협박해 몸값을 요구하는 랜섬웨어다. 포르노 앱을 사칭해 설치를 유도하며 설치된 이후에는 사용자를 협박해 돈을 요구하는 화면을 계속해서 단말에 표시해 사용자의 스마트폰 사용을 방해한다. 설치 시 [그림 7]과 같이 안드로이드 시스템 관련 권한을 요구한다.

[그림 7] Android-Trojan/Simplelock 설치 시 요구 권한

[그림 8] Android-Trojan/Simplelock 실행 화면

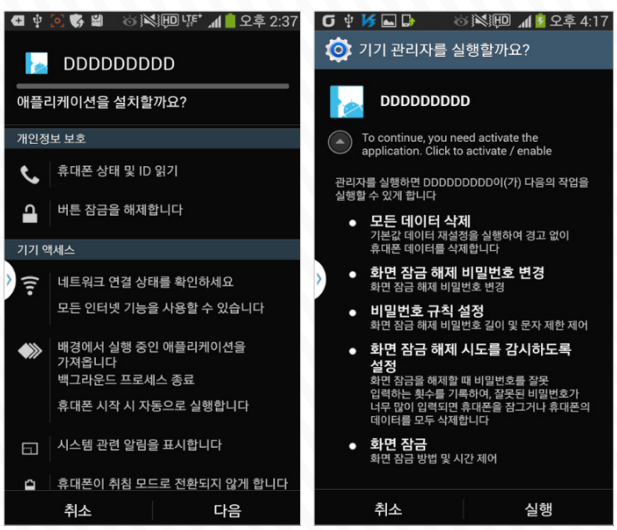
설치 후 실행하면 [그림 8]과 같이 아동 포르노를 시청했다는 내용으로 사용자를 협박하고 이를 해결하기 위해서는 500루블을 보낼 것을 요구한다. 사용자를 협박하는 화면을 항상 화면의 최상단에 표시되어 모든 화면을 가려 버리기 때문에 다른 앱을 실행하거나 메시지 확인 등을 할 수 없어 스마트폰을 정상적으로 사용할 수 없게 된다.

2. 슬로커(Android-Trojan/Slocker)

슬로커(Android-Trojan/Slocker)는 심플락과 마찬가지로 사용자의 스마트폰을 사용 불가능 상태로 만들고 사용자의 스마트폰에 음란물이 발견됐다고 협박해 금전을 요구하는 랜섬웨어다.

설치 과정을 살펴보면 [그림 9(좌)]와 같이 안드로이드 시스템에 관련된 권한을 다수 요구하는 것을 알 수 있다.

설치가 완료되면 [그림 9(우)]와 같은 기기 관리자 권한을 요구한다. 즉, 화면을 잠그거나 최대 잠금 시간을 조정할 수 있는 안드로이드 시스템 보안과 관련된 권한을 요구한다.



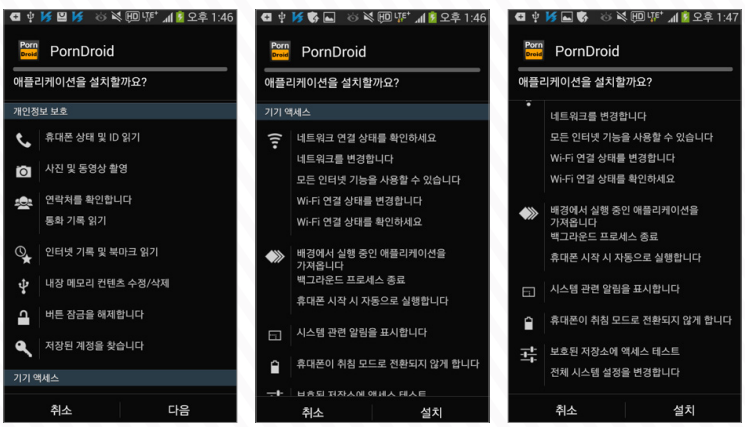
[그림 9] Android-Trojan/Slocker 설치 시 요구 권한(좌) / 기기 관리자 권한 요구(우)

실행하면 [그림 10]과 같이 음란물을 시청했다며 잠금 상태를 해제하려면 36시간 이내 500루블을 지불하라는 러시아로 된 안내문이 나온다. 이때 공격자는 안드로이드 창 속성을 설정하는 플래그(flags)와 포맷(format) 등을 조정하여 항상 가장 위에 보이도록 설정한다. 따라서 다른 앱의 화면을 모두 가려 스마트폰을 정상적으로 사용할 수 없게 된다.

[그림 10] Android-Trojan/Slocker 실행 화면

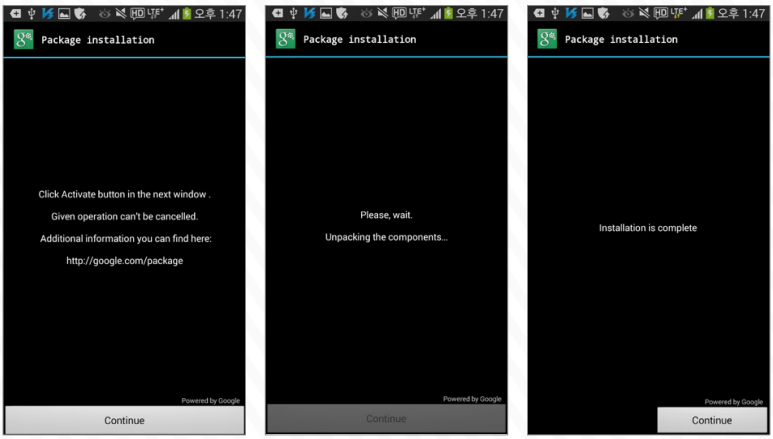
3. 콜러(Android-Trojan/Koler)

콜러(Android-Trojan/Koler)는 포르노 앱을 사칭하는 랜섬웨어다. 설치 후 잠금 화면 비밀번호를 무작위로 설정하는 점과 전면 카메라를 사용하여 사진을 찍은 다음 협박에 이용하는 점이 특징이다. 다른 랜섬웨어와 마찬가지로 스마트폰을 사용 불가능 상태로 만들고 금전을 요구한다. 설치과정을 살펴보면 [그림 11]과 같이 다수의 시스템 관련 권한을 요구한다.



[그림 11] Android-Trojan/Koler 설치 시 요구 권한

특히 스마트폰에 저장된 개인정보와 시스템 정보를 사용할 수 있는 권한도 요구하는 것을 확인할 수 있다.
실행하면 [그림 12]와 같이 설치 과정의 한 부분인 것처럼 사용자를 속이고 기기 관리자 권한을 획득한다.



[그림 12] 기기 관리자 권한 획득을 위한 가짜 창

이렇게 기기 관리자 권한을 획득하면 [그림 13]과 같이 미국 연방 수사국(Federal Bureau of Investigation, FBI)을 사칭하며 음란물이 스마트폰 내부에서 발견되었다고 보여주고, 이를 해결하고 스마트폰 잠금을 해제하기 위해서는 페이팔(PayPal)을 통해 500달러를 송금하라고 협박한다.

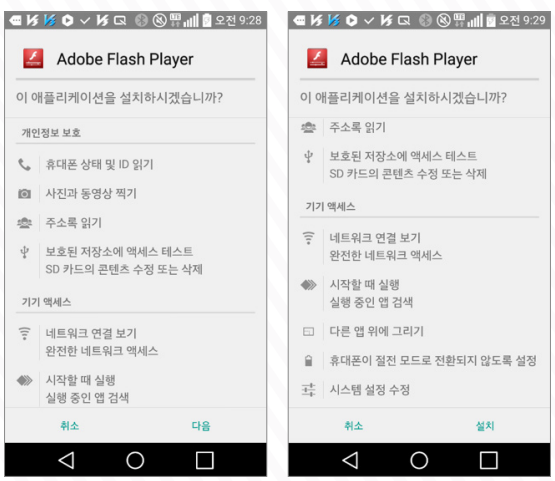
[그림 13] Android-Trojan/Koler 실행 화면

특히, 사용자의 스마트폰 카메라를 이용하여 현재 사용자의 모습을 사진으로 찍어 보여주고 불법적인 콘텐츠 및 사용 기록을 확보했다고 안내하여 사용자의 불안감을 극대화 시킨다.

또한 공격자는 코드를 이용하여 스마트폰의 기본 잠금 화면 비밀번호를 임의의 숫자로 변경하고 현재 보이는 화면을 항상 가장 위에 나타나도록 하여 스마트폰을 정상적으로 사용할 수 없도록 만든다.

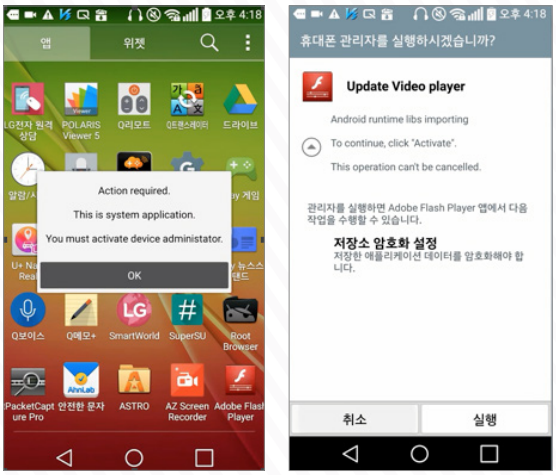
4. 크로세이트(Android-Trojan/Crosate)

크로세이트(Android-Trojan/Crosate)는 주로 어도비 플래시 플레이어를 사칭하여 설치를 유도하는 것이 특징이다. 다른 랜섬웨어와 마찬자기로 스마트폰을 사용 불가능 상태로 만들고 협박하여 몸값을 요구하는 기능이 있다. 설치 시 [그림 14]와 같은 권한을 요구한다.



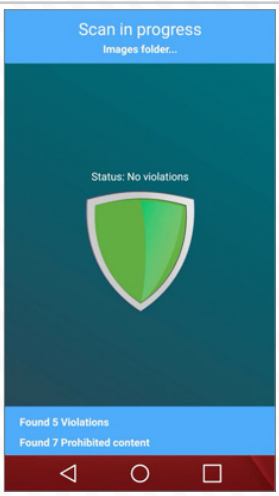
[그림 14] Android-Trojan/Crosate 설치 시 요구 권한

실행하면 [그림 15]와 같이 앱을 정상적으로 사용하기 위해 관리자 권한이 반드시 필요한 것처럼 안내하며 관리자 권한 획득을 시도한다. 특히 OK 버튼 외의 다른 영역은 터치되지 않는다. 기기 관리자 등록 취소 버튼을 눌러도 다시 창을 띄우기 때문에 기기 관리자를 등록하지 않아도 스마트폰을 정상적으로 사용할 수 없다.

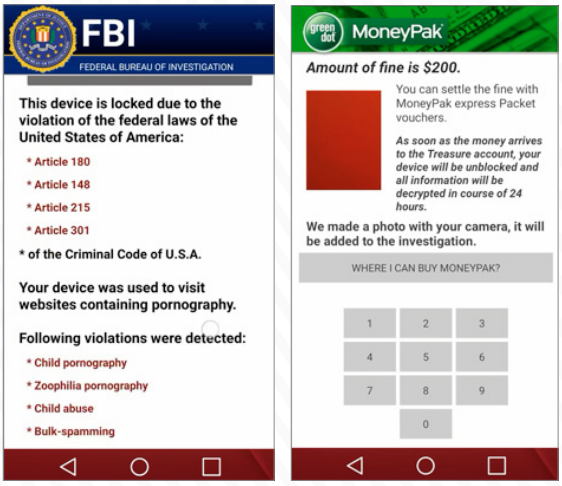


[그림 15] 기기 관리자 권한 요구

관리자 권한을 획득하면 [그림 16]과 같이 스마트폰을 검사하는 듯한 창을 띄우고 몇 가지 위반 사항과 금지된 콘텐츠를 찾았다고 화면에 표시한다. 잠시 후 [그림 17]처럼 미국 연방 수사국을 사칭하여 특정 법률을 위반했다며 스마트폰에서 찾은 위반 사항을 보여주며 머니팩(MoneyPak, 해외에서 사용되는 전자화폐)을 통하여 벌금 200달러를 보내라고 협박한다.

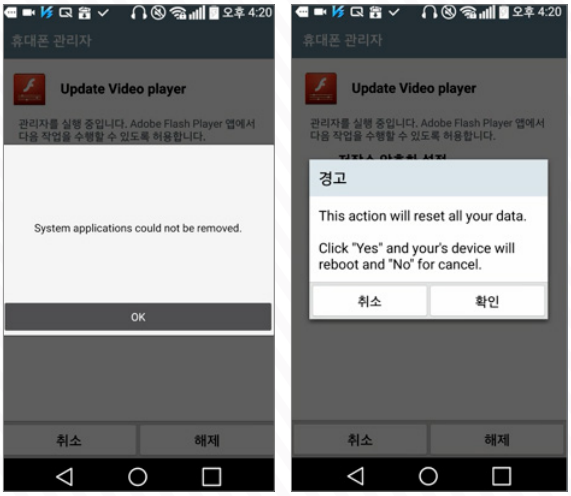


[그림 16] 스마트폰 검사 위장



[그림 17] FBI를 사칭하며 벌금 200달러 송금 요구

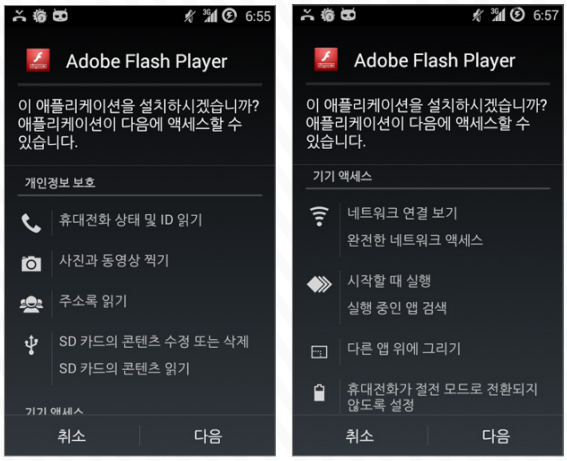
삭제하기 위해 기기 관리자 해제를 진행하면 [그림 18]과 같이 스마트폰의 모든 데이터가 삭제된다고 경고하며 삭제를 방해한다.



[그림 18] 기기 관리자 해제 방해

5. 에스브이팽(Android-Trojan/Svpeng)

에스브이팽(Android-Trojan/Svpeng)은 특정 앱 동작 시 가짜 정보 입력창을 팝업시켜 정보를 탈취하는 악성앱으로 랜섬웨어는 아니다. 하지만 기기 관리자 등록을 요구할 때 나타나는 화면과 해제를 방해하는 기능이 먼저 살펴보았던 크록세이트(Android-Trojan/Crosate)와 매우 유사하다. 다른 랜섬웨어와 유사하게 [그림 19]와 같이 많은 권한을 요구한다.

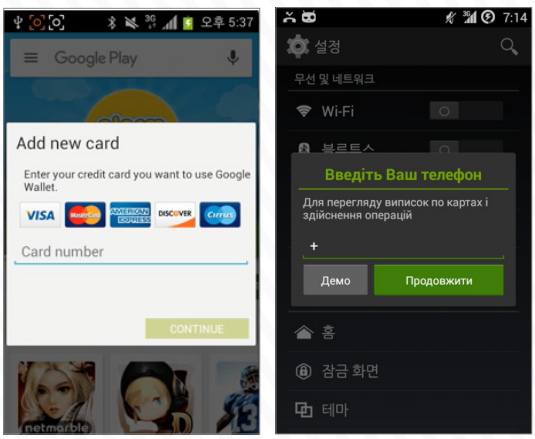


[그림 19] Android-Trojan/Svpeng 설치 시 요구 권한

실행하면 [그림 20]과 같이 앱을 정상적으로 실행하는데 꼭 필요한 것처럼 사용자를 속여 기기 관리자 권한을 요구한다. OK 버튼 외의 다른 공간은 터치되지 않는다. 기기 관리자 등록 취소 버튼을 눌러도 다시 창을 띄우기 때문에 기기 관리자를 등록하지 않으면 스마트폰을 사용할 수 없다. 실행 후에는 자신을 실행할 수 있는 아이콘을 숨겨 존재 사실을 은폐한다.

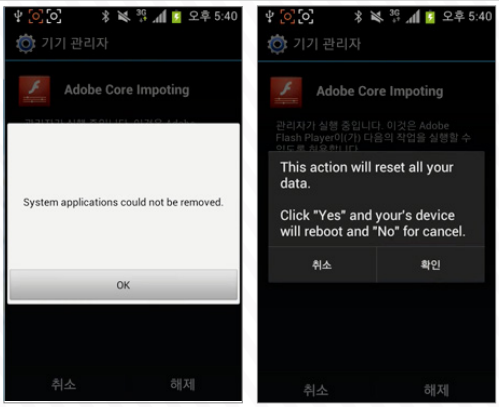
[그림 20] 관리자 권한 요구

공격자는 코드를 이용해 통해 [그림 21]과 같이 현재 동작 중인 최상위 앱이 구글의 플레이스토어인 경우 구글 플레이스토어 가짜 결제 창을 실행시킨다. 우크라이나 금융 앱이 실행되어 있을 경우에는 해당 금융 앱을 통해 결제할 때 필요한 정보를 입력받을 수 있는 가짜 창을 실행시킨다.



[그림 21] 구글플레이 사칭(좌) / 우크라이나 금융앱 privatbank 사칭(우)

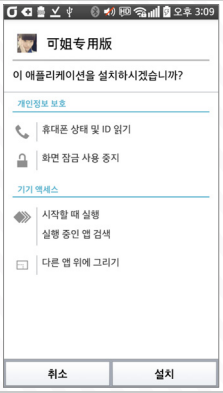
사용자가 삭제를 위해 기기 관리자 등록을 해제하려고 하면 시스템 앱은 제거될 수 없다는 안내 창을 보여주거나 스마트폰의 모든 데이터가 초기화된다고 협박하는 등 다양한 방법을 통해 이를 방해한다([그림 22] 참조).



[그림 22] 기기 관리자 해제 방해

6. 지모(Android-Trojan/Jimo)

지모(Android-Trojan/Jimo)는 금전적인 요구는 하지 않기 때문에 랜섬웨어는 아니지만 랜섬웨어처럼 화면을 잠궈 정상적인 사용을 방해하는 락커류의 악성앱이다. 설치 시 [그림 23]과 같은 권한을 요구하며 락커류에 꼭 필요한 "다른 앱 위에 그리기" 권한을 요구한다.



[그림 23] Android-Trojan/Jimo 설치 시 요구 권한

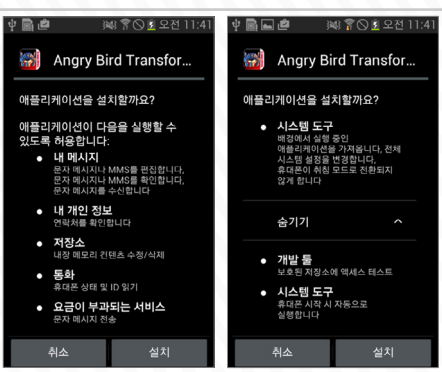
[그림 24] Android-Trojan/Jimo 실행 화면

실행되면 [그림 24]와 같이 아래 버튼을 1,000번 클릭하라는 지시 내용과 함께 화면 중앙에 버튼이 나타난다. 화면상의 버튼 외 다른 부분은 터치가 불가능하다. 1,000번을 클릭하면 터치는 할 수 있게 되지만 화면을 껐다 켜거나 홈 버튼을 누르면 재동작하여 1,000번을 클릭하라는 메시지가 다시 나타난다.

7. 와이프락커(Android-Trojan/WipeLocker)

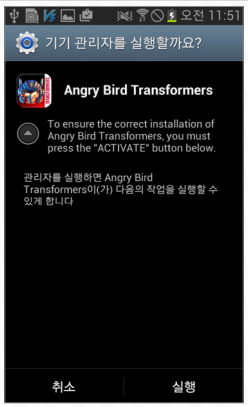
와이프락커(Android-Trojan/WipeLocker)는 금전적 요구는 하지 않는 락커류의 악성앱이다. 스마트폰에 저장된 모든 데이터를 삭제하여 정상적으로 스마트폰을 사용할 수 없게 만든다.

유명한 게임 등을 사칭하여 사용자의 설치를 유도하는데 [그림 25]와 같이 SMS/MMS에 관한 권한과 내장 메모리 데이터에 접근하여 수정하고 삭제할 수 있는 권한을 요구한다.



[그림 25] Android-Trojan/WipeLocker 설치 시 요구 권한

실행 시 [그림 26]과 같이 정상적인 설치를 보장하기 위해서는 기기 관리자 권한이 필요하다고 주장하며 해당 기기 관리자 권한을 얻을 때까지 지속적으로 권한을 요구하는 창을 실행시킨다.



[그림 26] 기기 관리자 권한 요구

기기 관리자 권한을 얻은 후에는 스마트폰에서 접근할 수 있는 저장소를 검색하여 검색된 모든 파일을 삭제한다. 이렇게 삭제되는 데이터 중에는 그 동안 사용자의 사진이나 동영상 데이터는 물론, 앱에서 생성한 각종 데이터도 포함된다. 또한 사용자의 개인정보도 외부로 유출한다.

지금까지 랜섬웨어, 락커류 악성앱의 기능과 특징을 살펴보았다. 모바일 랜섬웨어는 기기 관리자 권한을 요구하며, 이는 기기 관리자에 등록하여 삭제를 어렵게 하기 위함으로 분석된다.

랜섬웨어 삭제 방법

랜섬웨어가 스마트폰에 설치되어 기기 관리자 권한을 얻은 경우 설치된 악성앱이 기기 관리자 권한으로 화면으로 들어가는 것을 방해하기 때문에 일반적인 방법으로는 랜섬웨어를 삭제할 수 없다. 이런 유형의 악성앱이 스마트폰에 설치된 후 백신에 탐지되더라도 정상적인 삭제를 위해서는 기기 관리자를 해제해야 하는데, 설치된 악성앱이 기기 관리자 접근을 방해하기 때문에 정상적인 삭제가 어렵다. 백신에 의해 탐지되더라도 기기 관리자를 해제할 수 없어 삭제를 할 수 없는 경우에는 수동으로 악성앱을 삭제해야 한다.

이 글에서는 랜섬웨어와 같이 일반적인 방법으로 삭제가 어려운 악성앱을 삭제하는 방법을 알아본다.

1. 안전모드를 이용한 악성앱 삭제

악성앱을 삭제하는 손쉬운 방법은 스마트폰을 안전모드로 부팅한 후 삭제하는 것이다. 안드로이드 스마트폰을 안전모드로 부팅하는 방법은 제조사와 스마트폰 모델별로 다를 수 있으나 일반적으로 안드로이드 4.1 젤리빈 이상의 버전에서는 2가지 방법을 이용해 안전모드 부팅을 할 수 있다.

[그림 27] 켜진 상태에서 안전모드 부팅 방법

두 번째는 종료된 스마트폰을 부팅하는 동안 볼륨 낮추는 버튼을 길게 누르는 방법이다. 이 방법을 이용해 안전모드로 진입할 수 있다. 부팅 후에는 [그림 28]과 같이 화면 왼쪽 아래에 안전모드라는 표시가 나타나며 런처에 서드파티(3rd-party) 앱(다운로드 받은 앱)의 아이콘이 회색으로 보이거나 버전에 따라 아이콘이 보이지 않는다. 이때는 아이콘을 터치해 앱을 실행하려해도 실행되지 않는다.

[그림 28] 안전모드

안드로이드 스마트폰의 안전모드는 최소한의 드라이버를 이용해 시스템을 구성한 후 부팅하는 윈도우에서의 안전모드와 유사하다. 안전모드로 부팅된 경우 애플리케이션 중 서드파티 앱을 사용하지 않도록 하고 시스템을 부팅하기 때문에 많은 경우 기기 관리자를 해제하고 악성코드 삭제를 삭제할 수 있다.

2. 안전모드에서도 동작하는 악성앱 삭제

일부 악성코드는 안전모드로 부팅하더라도 기기 관리자 해제를 방해한다. 이런 악성앱을 삭제하기 위해서는 악성앱의 패키지명을 확인해 'adb[1]'로 실행 중인 악성앱을 강제 종료하고 삭제해야 한다. adb를 스마트폰에 연결하기 위해 드라이버를 설치하고 스마트폰의 설정을 변경하는 방법은 이 글에서는 다루지 않는다.

2.1 악성앱 패키지명 확인

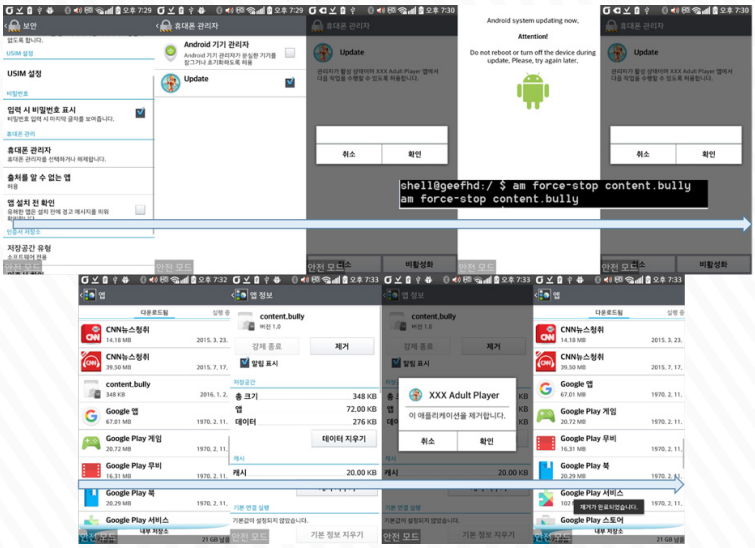
실행중인 악성코드를 종료하기 위해서는 adb shell 명령인 'am force-stop'을 이용해야 한다. 'am force-stop'은 패키지명을 활용해야 하기 때문에 먼저 악성앱의 패키지명을 알아야 하는데 패키지명은 백신의 진단 결과나 'pm list-packages' 명령을 이용해 확인할 수 있다.

[그림 29] V3의 악성앱 진단 결과

[그림 29]에 표시된 경로를 보면 "/data/app/content.bully-1.apk"에서 파일 경로인 "/data/app/"와 "-1.apk"를 제외한 "content.bully"가 진단된 악성앱의 패키지 명이다.

2.2 실행 중인 악성앱 프로세스 종료

adb shell 명령 중 'am force-stop [패키지명]' 명령은 실행 중인 프로세스를 종료한다. 이 명령을 이용하면 기기 관리자 해제 창 접근 시 악성앱이 화면을 가리더라도 악성앱의 프로세스를 종료시킬 수 있어 기기 관리자를 해제할 수 있다. 설정 → 앱 정보에 접근할 때도 악성앱이 화면을 가릴 수 있지만 이때에도 동일하게 'am force-stop [패키지명]' 명령을 이용해 프로세스를 종료하면 설치된 악성앱을 제거할 수 있다.



[그림 30] 실행 중인 악성앱 프로세스 종료 후 삭제

[1] http://developer.android.com/intl/ko/tools/help/adb.html

[2] http://developer.android.com/intl/ko/tools/help/shell.html#shellcommands

2.3 루팅된 스마트폰에서 악성앱 제거

일부 악성앱은 화면을 기기 관리자 접근 시 화면을 가리는 방법이 아닌 홈 화면 호출 방법을 사용한다. 이 경우는 실행 중인 악성앱의 프로세스를 종료하더라도 기기 관리자 화면으로 접근할 수 없기 때문에 루트 권한을 이용해 제거해야 한다. 루팅은 안드로이드 운영체제를 탑재한 모바일 기기에서 관리자 권한을 획득하는 것을 말하는데, 루팅을 통해 슈퍼 유저 권한을 획득하면 안드로이드의 파일 시스템에 접근할 수 있으므로 안드로이드 패키지 매니저를 통하지 않고 설치된 악성앱을 삭제할 수 있다. 루팅된 스마트폰에서 악성앱을 제거하기 위해서는 먼저 악성앱 패키지명을 확인해야 한다. 악성앱 패키지명을 확인했다면 adb shell에서 'su' 명령을 이용해 루트 권한을 획득하고 사용자의 앱이 설치된 /data/app 경로로 이동한다. (/data/app 경로는 루트권한이 없다면 접근할 수 없기 때문에 루트 권한이 필요하다.) /data/app 디렉터리에서 패키지명을 포함하는 apk 파일을 검색하고 검색된 파일을 삭제하면 악성앱을 제거할 수 있다.

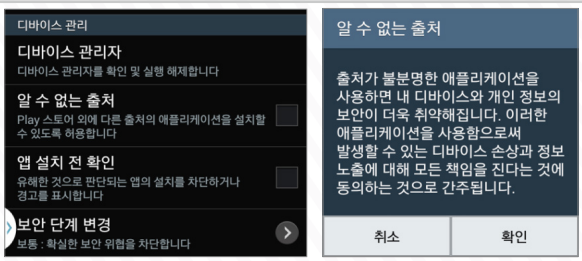
제거된 스마트폰에서는 여전히 악성앱이 동작하지만 재부팅 후에는 삭제된 악성앱이 동작하지 않는다.

모바일 랜섬웨어 피해 예방법

모바일 랜섬웨어를 비롯한 악성앱이 설치되고 피해가 발생한 후에 복구하는 것은 많은 노력과 시간이 필요하다. 더욱이 랜섬웨어의 경우 한 번 설치되면 제거하기 어렵고 데이터를 암호화하는 경우 중요한 데이터를 잃을 수도 있다. 가장 좋은 방법은 안전한 스마트폰 환경을 만들어 악성앱이 설치되지 않도록 미리 예방하는 것이다. 랜섬웨어에 감염되는 것을 예방할 수 있는 몇 가지 방법을 살펴보자.

1. 알 수 없는 출처 설정 확인

알 수 없는 출처의 앱을 설치하는 것을 주의해야 한다. 안드로이드는 공식 마켓이 아닌 다른 경로를 통해서도 앱을 설치하는 것이 가능하다. 하지만 대부분의 악성앱들은 공식 마켓이 아닌 경로를 통해 배포되고 있다. 스미싱 문자를 통해 URL 접속을 유도해 설치되는 경우나 피싱 사이트를 통해 다운로드하는 경우도 있다. 또 신뢰할 수 있는 마켓이 아닌 블랙 마켓에서 다운받을 경우 악성앱이 포함되어 있을 가능성이 매우 크다. 이러한 위험을 방지하기 위해서는 공식 마켓인 구글 플레이 스토어 등을 통해서만 앱을 설치하는 것이 안전하다. 구글 플레이 스토어에서는 잠재적으로 위험한 앱을 차단하기 위한 검토를 거치고 앱을 등록하고 있다. 구글 플레이스 스토어를 통해서만 앱을 설치하려면 [그림 31]과 같이 스마트폰의 설정에서 '알 수 없는 출처' 설정을 통해 플레이 스토어 외 출처에서 앱이 설치되는 것을 방지할 수 있다.



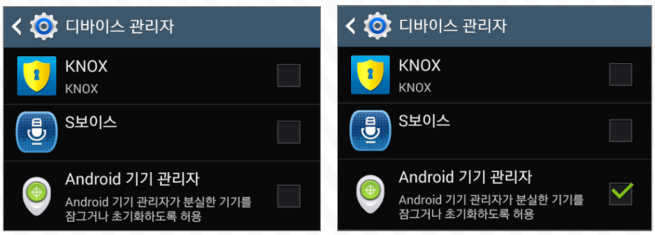
[그림 31] 알 수 없는 출처 설정 화면

2. 성인 콘텐츠 앱 주의

성인 콘텐츠 앱을 설치할 때는 신중해야 한다. 많은 악성앱이 음란물을 이용해 다운로드 및 설치를 유도하고 있는 만큼 모바일 랜섬웨어도 성인 콘텐츠를 활용하고 있다. 해외에서 발견되는 모바일 랜섬웨어 중 상당수 앱이 포르노 앱을 사칭하고 있다. 포르노 앱인 것처럼 위장하여 설치를 유도하거나 앱을 다운로드하여 설치하면, 불법적인 음란물을 소장하거나 시청하여 법을 위반했다고 협박하며 금전을 요구하기도 한다. 음란물이 앱을 설치하도록 유도하는 것뿐만 아니라 금액을 요구하는 랜섬웨어 행위에 활용되고 있다.

3. 기기 관리자 권한 등록 주의

앱을 기기 관리자에 등록하는 것을 조심해야 한다. 앱이 기기 관리자에 등록되면 스마트폰 보안과 관련된 작업, 원격 초기화, 네트워크 설정 등을 할 수 있게 된다. 기기 관리자에 등록된 앱은 관리자 등록을 해제하기 전까지 제거되지 않기 때문에 많은 모바일 랜섬웨어 앱들이 보안에 관한 권한과 제거 방지를 목적으로 기기 관리자 등록을 요구한다. 랜섬웨어들은 기기 관리자 권한 해제 이벤트를 수신하여 기기 관리자 권한 해제 자체를 방해하기 때문에 안전모드를 통한 제거도 어렵게 하는 방식을 사용하고 있다. 그러므로 앱 설치 후 기기 관리자 등록을 요구하는 앱의 경우 세심한 주의를 가지고 안전성이 보장되고 신뢰할 수 있는 경우에만 설정을 하는 것이 바람직하다.



[그림 32] 기기 관리자 관리 화면

4. 최신 업데이트 유지

안드로이드 운영체제 및 보안 앱의 최신 업데이트를 유지해야 한다. 스마트폰의 개체 수가 늘어남에 따라 스마트폰 보안에 관심이 높아지고 스마트폰 및 모바일 운영체제에 대한 취약점이 많이 발견되고 있다. 악성앱 개발자들이 이러한 취약점을 활용하는 것을 방지하기 위해서는 취약점이 패치된 최신 업데이트를 유지해야 한다. 또 새로운 유형의 모바일 랜섬웨어를 차단하거나 새로운 보안 기술을 스마트폰에 적용하기 위해서는 모바일 보안 앱의 버전을 최신으로 유지하여 안전한 스마트폰 환경을 만들어야 한다.

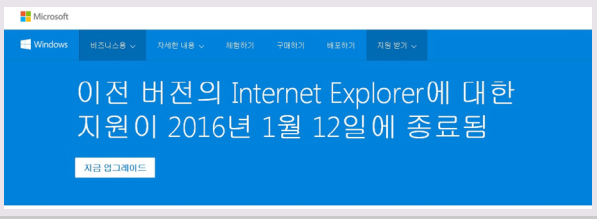
지금까지 모바일 랜섬웨어에 대해 자세히 살펴보았다. 모바일 랜섬웨어에 감염되면 스마트폰 이용이 제한되고 데이터가 손실되는 피해를 볼 수 있다. 더욱이 모바일 랜섬웨어는 제거하기가 어렵다는 문제가 있다. 이러한 모바일 랜섬웨어를 유형별로 자세히 살펴봄으로써 동작 방식 및 기능을 이해할 수 있었다. 아직 한국을 대상으로 하는 모바일 랜섬웨어는 확인된 바 없지만 조만간 나타날 가능성은 매우 높다. 국내에 모바일 랜섬웨어가 등장한다면 현재 해외에서 활동하는 랜섬웨어가 유포되는 방식과 유사하게 나타날 수 있다. 그러므로 앞에서 살펴본 유포 방법을 바탕으로 세심한 주의를 기울여야 한다. 만약 모바일 랜섬웨어에 감염되었을 경우에는 수동 제거 방법을 따라 대처해야 한다. 하지만 가장 중요한 것은 모바일 랜섬웨어가 설치되지 않도록 예방하는 것이다. PC 랜섬웨어도 해외에서 활발히 활동하다 한국에 등장했다. 모바일 랜섬웨어도 현재 급격한 증가 추세를 보인다. 모바일 랜섬웨어의 피해자가 '나 자신'이 될 수 있는 만큼 많은 주의와 관심이 필요하다.

MS 구버전 IE 지원 종료에 따른 이슈 점검

구버전 IE 지원 중단, 기업의 고민은?

마이크로소프트(Microsoft, 이하 MS)가 2016년 1월 12일을 기점으로 구버전 인터넷 익스플로러(Internet Explorer, 이하 IE)에 대한 기술 지원 및 보안 업데이트를 중단했다. 즉, 이후로는 최신 버전이 아닌 구버전의 IE에서 새로운 취약점이 발견되더라도 이에 대한 패치는 제공되지 않는다는 것. 국내의 경우 개인 사용자뿐만 아니라 기업에서도 대고객 웹 서비스 및 사내 인트라넷 등과 관련해 구버전 IE 사용 비율이 높은 편이다. 이에 보안에 대한 우려와 함께 업무 생산성 측면에서도 기업의 고민이 늘고 있다.

MS는 자사 OS 및 소프트웨어의 최신 보안 취약점을 해결하기 위해 정기적으로 보안 패치를 제공하고 있다. 대부분의 악성코드가 프로그램의 취약점을 이용하고 있기 때문에, 최신 보안 패치 적용은 매우 중요한 보안 수칙 중 하나다. MS의 구버전 IE 지원 중단이 최근 화두가 된 까닭이 바로 이것이다. 구버전 IE 브라우저를 계속 사용하다가는 심각한 보안 위협이 발생할 수 있기 때문이다.



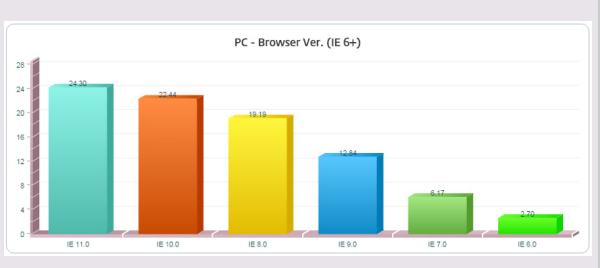
[그림 1] MS의 구버전 IE 지원 종료 안내 (*출처: Microsoft 홈페이지)

대고객 서비스 사이트는 당장 어쩌나

MS의 가장 최신 브라우저 버전은 IE11이다. 그러나 아직까지 상당수의 국내 웹 사이트 및 웹 서비스는 구버전 IE 중심이다. 지난 2014년 말 국제 웹표준 기구 W3C가 HTML5를 웹 표준으로 선정함에 따라 국내에서도 지난 2015년부터 주요 업체를 중심으로 HTML5와 호환되는 IE9를 이용한 웹 환경으로 개선을 서둘렀으나 여전히 상당수의 웹 서비스는 구버전 IE 환경에 종속되어 있다.

따라서 최신 버전의 IE를 사용하는 고객이 이러한 웹 서비스 사이트에 접속할 경우 정상적으로 서비스를 이용하기 어렵다. IE 11부터는 웹 표준 기술이 상당수 적용되어 있기 때문에 액티브X 등과 같은 비표준 기술을 사용해 만든 기능은 제대로 작동하지 않거나 제대로 화면에 표시되지 않기 때문이다. 기존에 이용하던 기능들이 최신 버전인 IE11에서 정상적으로 동작하지 않을 경우 고객 불만이 급증할 우려가 있다.

반면 당장 대고객 웹 서비스를 최신 버전을 기준으로 개편하더라도 고객의 불편을 야기할 수 있다. 여전히 국내 개인 사용자들의 상당수가 구버전의 IE를 사용하고 있기 때문이다. 한국인터넷진흥원(KISA)이 국내 인터넷 이용환경을 분석한 통계자료에 따르면 2015년 상반기 IE 이용자는 87.64%에 달한다. 문제는 이 가운데 IE 11을 사용하는 비율은 24.3%에 불과하다는 것. 즉, 최신 IE 브라우저를 사용하고 있는 사람은 10명 중 3명도 채 되지 않는다. 나머지 구버전 IE 사용자들이 최신 버전으로 업데이트하지 않는 한 대고객 서비스 사이트 개편이 오히려 사용자의 불만을 야기하는 역풍을 맞을 수도 있다는 것이 일부 업체들의 고민이다.



[그림 2] MS의 구버전 IE 지원 종료 안내 (*출처: 한국인터넷진흥원)

이 밖에도 미처 관련 개발 인력이나 예산을 책정하지 못한 기업도 적지 않다. 또 웹 서비스의 지원 브라우저를 변경할 때는 해당 브라우저 상에서 모든 기능이 정상적으로 작동하는지 일일이 호환성을 확인하는 테스트 기간이 필요하다. 따라서 당분간 웹 서비스 지원 환경을 구버전 IE로 유지할 수 밖에 없는 경우도 있어 호환성 이슈와 함께 당분간 사용자들의 혼란과 불편이 우려된다.

'인트라넷, 너마저'…사내 시스템 호환성 이슈 '복병'까지

구버전 IE 지원 중단 및 최신 버전 사용 이슈는 기업의 업무 생산성에 더 큰 영향을 끼칠 것으로 보인다. 상당수 기업에서는 인트라넷 등 업무 프로그램과의 호환성을 이유로 구버전의 IE를 사용하고 있기 때문이다. 최근 미래창조과학부가 발표한 '2015년 하반기 국내 인터넷 이용환경 현황 조사'에 따르면 국내 기업에서 구버전 IE를 사용하는 비율은 약 50.34%로, 절반 이상의 기업에서 구버전 IE를 이용하는 것으로 나타났다.

	IE10	IE9	IE8	IE7	IE6
Windows XP	0.00%	0.00%	7.24%	0.42%	0.83%
Windows VISTA	0.00%	0.33%	0.14%	0.17%	0.00%
Windows 7	8.02%	11.98%	7.44%	1.66%	0.00%
Windows 8	21.08%	0.00%	0.00%	0.16%	0.00%
합계	29.10%	12.31%	14.82%	2.41%	0.83%

[표 1] 국내 지원 중단 IE 점유율
(*출처: 미래창조과학부, '2015년 하반기 국내 인터넷 이용환경 현황 조사')

브라우저를 업그레이드하려면 연동되는 사내 업무 시스템에 대한 개발 및 점검 작업이 함께 이루어져야 한다. 그러나 대고객 웹 서비스와 달리 사내 업무 시스템 개편을 고려한 예산 책정이나 인력 배분을 해둔 업체는 그리 많지 않다. 따라서 사내 업무 시스템의 개편 착수부터 점검이 마무리되는 시점까지 한동안 기업 내 구버전 IE 사용에 따른 보안 위협이 우려되고 있다.

구버전 IE 보안 대응 자구책 마련, 쉽지 않아

그런데 구버전 IE를 사용하면 정말 위험할까? 결론부터 말하자면 꼭 그런 것만은 아니다. 구버전 IE를 쓰는 PC에 대해 당장 사이버 공격이 급증하거나 장애가 발생하지는 않는다. 다만 구버전 IE의 신규 보안 취약점이 확인될 경우 이를 이용한 공격에 노출될 가능성이 높아진다는 것이다. 또한 신규 보안 취약점에 대한 패치가 제공되지 않기 때문에 구버전 IE 사용자 및 사용 기업에서는 발생 가능한 보안 침해 사고에 대해 자구책을 마련해두어야 한다는 부담이 따른다.

한편 모든 운영체제에서 IE11을 사용해야만 하는 것은 아니다. 특수 시스템용 OS 등 기술 지원 일정이 남아있는 일부 OS에서는 IE11이 아닌 다른 버전의 IE를 최신 브라우저로 지원하고 있기 때문이다. 윈도우 비스타 SP2(Windows Vista SP2)는 IE9까지, 윈도우 7과 윈도우 8.1의 경우 IE11을 최신 브라우저로 지원한다. 하지만 윈도우 비스타 SP2의 IE9에 대한 지원도 2017년 4월 11일까지만 받을 수 있어 그 이후에는 최신 버전으로 업그레이드해야 한다. 이 밖에도 ▲윈도우임베디드 스탠더드 2009 ▲윈도우임베디드 POSReady 2009 등의 환경에서는 IE8을, ▲윈도우비스타SP2 ▲윈도우서버2008R2 ▲윈도우서버2008 IA64 이용 시에는 IE9를, ▲윈도우서버2012 ▲윈도우임베디드8 스탠더드 환경에서는 IE10을 지원한다.

그러나 이들 OS 및 IE에 대한 지원도 멀지 않은 시점에 종료될 수 있기 때문에 사전에 현재 사용 중인 IE에 대한 기술 지원 및 보안 업데이트 가능 여부를 확인해두는 것이 바람직하다. 또한 부득이하게 당분간 구버전 IE를 사용해야 하는 상황이라면 예전에 제공되었던 보안 업데이트를 빠짐없이 적용해 기존 취약점을 이용한 공격에 대한 최소한의 대비를 하는 것도 필요하다.

2016년 알아야 할 의료기관 개인정보보호 10가지

2011년 3월 29일 제정돼 곧 다섯 돌을 앞두고 있는 개인정보보호법이지만 의료기관의 개인정보보호에 대한 인식은 다른 산업군에 비해 미흡한 상황이다. 지난 2015년 12월 31일, 의료법 시행규칙이 입법 예고됨에 따라 의료기관의 개인정보보호 및 보호조치에 대한 이해가 반드시 필요한 시점이다. 이에 이 글에서는 지난 2015년 2월에 발행된 '의료분야 개인정보보호 가이드라인'을 중심으로 의료기관에서 간과하기 쉬운 개인정보보호 법령 기준에 대해 짚어본다.

한국보건사회연구원(이하 보사연)이 발표한 2013년 보고서에 따르면 일정 규모 이상의 병원급은 어느 정도 법 기준에 따른 개인정보 보호조치가 이루어지고 있지만, 실제 국민들이 흔히 찾는 의원급 의료기관에서는 보호조치에 대한 이해가 부족한 것으로 나타났다.

구 분		병원급		의원급	
		조치함	모르겠음	조치함	모르겠음
정보시스템 관리	업무권한 관리	83.8%	6.7%	31.4%	31.4%
	접속 기록 생성 및 보관	53.3%	16.2%	15.2%	40.0%
보안 조치	백신설치 및 업데이트	92.4%	3.8%	82.9%	4.8%
	고유식별정보 암호화	59.0%	10.5%	19.2%	36.5%
	기록물의 안전한 장소 보관	74.3%	10.5%	37.1%	10.5%

[표 1] 의료기관의 개인정보보호 현황 (*출처: 2013년 한국보건사회연구원 연구보고서)

게다가 지난해 말 시행된 의료기관 개인정보보호 자율점검 결과에 따른 보완 조치를 수행해야 하기 때문에 이제 의료기관의 개인정보보호는 더 이상 피할 수 없는 문제가 되었다. 이와 관련해 올해 의료기관에서는 적어도 다음의 10가지 사항에 대해서는 알아두는 것이 바람직하다.

1. 전자의무기록의 관리 보존에 대한 기준이 강화되는 대신 외부업체 위탁이 가능하게 된다. (예정)

현행 의료법 시행규칙 제16조에 따르면 전자의무기록의 보관은 의료 기관 내로 제한되며 기록의 생성 및 보관, 이력관리에 필요한 장비, 복제/저장에 필요한 백업 장비를 갖추도록 규정하고 있다. 그러나 정보보호와 IT 관리 수준이 떨어지는 의료기관이 자체적으로 관리할 경우에 오히려 정보보호가 제대로 되지 않을 위험이 높다는 지적에 따라 일정 기준을 충족하는 외부업체 또는 원격지에 관리•보관할 수 있도록 의료법 시행규칙을 개정하고 정보보호를 위한 필수 시설과 장비에 대한 조항이 신설되었다.

현행	개정
1. 전자의무기록의 생성 및 보관을 위하여 필요한 기능을 갖춘 장비 2. 전자의무기록의 이력관리를 위하여 필요한 장비 3. 전자의무기록의 복제 · 저장에 필요한 백업 장비	1. 전자의무기록의 생성 및 보관을 위하여 필요한 기능을 갖춘 장비 2. 전자의무기록의 이력관리를 위하여 필요한 장비 3. 전자의무기록의 복제 · 저장에 필요한 백업 장비 4. 네트워크 및 시스템 보안에 관한 설비 · 장비 5. 물리적 보관장소를 별도로 두고 있는 경우 그 장소의 통제 설비

[표 2] 의료법 시행규칙 개정안 일부

전자의무기록을 의료기관 자체에서 관리하지 않고 외부기관에 위탁하려하는 경우에는 해당 업체가 필수적인 정보보호 시설과 장비를 갖추고 있어야만 하며 의료기관은 지자체장(시장/군수, 구청장)에게 안전한 관리 보존을 위한 계획서를 제출하도록 함으로써 절차적 보완을 하고 있다.

〈의료기관 외부의 전자시스템에서 전자의무기록을 관리 보존하고자 할 경우 갖추어야 할 필수 시설 및 장비〉

1. 전자의무기록의 생성 및 보관을 위하여 필요한 기능을 갖춘 장비
2. 전자의무기록의 이력관리를 위하여 필요한 장비
3. 전자의무기록의 복제 · 저장에 필요한 백업 장비
4. 네트워크 및 시스템 보안에 관한 설비 및 장비
5. 전자시스템 운영에 필요한 장비
6. 별도의 출입통제구역의 설치와 그 장소의 통제 및 감시를 위한 설비
7. 재해예방에 관한 설비

2. 개인정보 처리 업무를 위탁할 때는 반드시 다음 내용이 포함된 문서에 의하여야 한다.

전자의무기록을 의료기관 자체에서 관리하고 있다 하더라도 소프트웨어나 컴퓨터 시스템의 개발 유지 보수를 위해서는 타 업체가 시스템에 저장된 환자의 자료에 접근하는 경우가 있을 수 있다. 또한 전화 예약, 주차 관리, 환자 식이 및 배식, 진료비 수납/환급, 환자 이송 등 의료기관의 여러 업무를 타 업체에 위탁하는 일도 있을 텐데, 이 경우 반드시 개인정보 처리 위탁에 따른 필수 조항을 수록하여 문서화하도록 개인정보보호법은 규정하고 있다. 위반 시 최대 1천만 원의 과태료가 부과된다.

위탁업체에 대해 유의해야 할 사항은 개인정보 처리에 대해선 수탁업체가 법 위반으로 인한 사고를 일으키면 업무를 위탁한 의료기관에서 법적 책임을 함께 지도록 되어 있다는 사실이다. 법에서는 '수탁업체를 위탁자의 직원으로 본다'고 되어 있다. 이러한 관리 책임에 대한 최소한의 이행 사항이 계약 시 필수 문서 확보와 수탁자에 대한 주기적인 교육 점검이라고 보아야 할 것이다.

〈개인정보 처리 위탁 계약서 기재사항〉

① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

② 개인정보의 기술적 • 관리적 보호조치에 관한 사항

③ 위탁업무의 목적 및 범위

④ 재위탁 제한에 관한 사항

⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항

⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항

⑦ 법 제26조제2항에 따른 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

3. 모든 의료기관은 "개인정보처리방침"을 수립하고 공개해야 한다.

개인정보처리방침은 의료기관의 규모와 관계없이 개인정보를 취급하는 모든 조직이 수립하고 공개해야만 하는 법적 의무사항이다. 위반 시 최대 1천만 원의 과태료가 부과된다.

흔한 오해 중 하나가 의원이나 병원은 홈페이지가 없기 때문에 개인정보처리방침이 없어도 된다고 생각하는 것이다. 이는 절대 그렇지 않다. 개인정보처리방침은 개인정보처리에 대한 기본 사항을 이용자(환자)에게 공개함으로써 정보주체의 개인정보 자기결정권을 보장하는 관리적 보호조치 사항이기 때문이다. 개인정보처리방침은 아래와 같은 사항을 필수로 포함하고 있어야 하며, 공개 방법은 ▲홈페이지가 있는 경우에는 홈페이지 메인 화면의 눈에 띄기 쉬운 위치(보통 하단 중앙)에 게시하거나 ▲인쇄물 형태로 병원 내 이용자가 쉽게 열람할 수 있는 위치에 비치, 또는 ▲우편물로 이용자에게 발송하는 방법 등을 선택할 수 있다.

〈 개인정보처리방침 필수 기재사항 〉

① 개인정보의 처리 목적

② 개인정보의 처리 및 보유 기간

③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)

④ 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)

⑤ 정보주체의 권리 • 의무 및 그 행사방법에 관한 사항

⑥ 처리하는 개인정보의 항목

⑦ 개인정보의 파기에 관한 사항

⑧ 개인정보 보호책임자에 관한 사항

⑨ 개인정보 처리방침의 변경에 관한 사항

⑩ 개인정보의 안전성 확보조치에 관한 사항

〈 개인정보처리방침 선택 기재사항 〉

① 정보주체의 권익침해에 대한 구제방법

② 개인정보의 열람청구를 접수 • 처리하는 부서

4. 의료기록이라 하더라도 일정 기간 후엔 파기하는 것이 원칙이다.

'의료기록이므로 삭제할 수 없습니다!'

의료기관 담당자들에게서 간혹 듣게 되는 단호한 주장이다. 그러나 의료법 시행규칙 제15조에서 "의료기관의 개설자 또는 관리자는 진료에 관한 기록을 다음 각 호에 정하는 기간 동안 보존하여야 한다. 다만, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 다음 각 호에 정하는 기간의 범위에서 그 기간을 연장하여 보존할 수 있다.〈개정 2015.5.29.〉"고 밝히고 있다. 즉, 법적 보관기간이 지나면 의료기록 또한 파기하는 것이 원칙이며, 진료상 필요 시에만 1회에 한정하여 연장이 가능하다. 따라서 의료기록이라 할지라도 '영구보관'이란 없다고 보는 것이 옳을 것이다. 이때 주의할 점은 자료의 파기는 전산시스템뿐만 아니라 직원의 PC에서도 동일한 기준이 적용되어야 한다는 것이다.

종 류	보존기간
환자명부	5 년
진료기록부	10 년
처방전	2 년
수술기록	10 년
검사소견기록	5 년
방사선사진 및 그 소견서	5 년
간호기록부	5 년
조산기록부	5 년
진단서 등의 부본	3 년

[표 3] 의료기관의 개인정보 종류별 보존 기관

5. 경찰이 의료기록을 달라고 하면 주어야 하나? 이런 경우에만 허용된다!

경찰이 범죄 수사 등을 이유로 의료기록에 대한 열람을 요청하는 경우가 있다. 관행적으로 협조 차원에서 단순 방문이나 전화 연락만 있어도 이를 제공하는 의료기관이 적지 않았다. 그러나 개인정보보호법은 물론이고 의료법에서도 의료기록의 열람 제공은 '법에서 규정한 특별한 조건'에만 가능하다. 경찰이 요청할 경우, 의료법 제21조에 근거하여 형사소송법 제106조, 제215조, 제218조에 따른 압수 • 수색영장에 의하여 해당 환자의 개인정보를 압수하는 경우에만 제공이 가능하며, 다른 기관의 정보요구에 대해서도 법적 근거가 명확한 경우에만 환자의 동의 없이 제공할 수 있다.

6. 병원을 양도 • 양수한 경우, 이전 사실을 의료기록의 정보주체들에게 반드시 알려야 한다.

평소 다니던 의원을 찾아가면 의원 이름은 그대로인데 의료진이 싹 바뀐 경우를 간혹 경험한다. 알고 보니 이전 원장이 의원을 새로운 원장에게 팔고 다른 곳으로 옮겼다고 한다. 사업자가 바뀐 양도 • 양수가 이루어진 것이다. 이 경우 개인정보보호법(제27조)은 개인정보의 이전 사실에 대하여 정보주체(의료기관에 기록 보존되어 있는 환자)에게 통보를 해야 할 의무가 있다. 일차적인 통보 책임은 사업을 넘기는 양도자에게 있으며, 양도자가 의무를 이행하지 않을 경우 양수자 또한 통보의 책임이 있다. 이 또한 위반 시 최대 1천만 원의 과태료가 부과된다.

〈의료기관 양도 양수 시 등록 환자에게 통보해야 할 사항〉

① 개인정보를 이전하려는 사실

② 개인정보를 이전받는 자(영업양수자 등)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처

③ 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

7. 전산시스템 ID를 간호사들이 함께 이용하는 일은 절대 금지

규모가 큰 병원에서는 간호사 별로 전산시스템의 사용자 계정을 등록하여 사용하는 게 일반적이지만, 작은 의원에서는 1대의 컴퓨터에서 특정 ID로 로그인한 상태로 여러 간호사가 환자 정보를 조회하거나 입력하는 등 업무를 처리하는 경우가 있다. 바쁜 의원의 현실을 생각하면 십분 이해가 되는 일이지만, 법적 기준으로 보자면 위반 사항이고 정보보호 관점에서도 볼 때도 심각한 문제가 된다. 정보 유출과 같은 보안 사고가 발생하면 빨리 해결하기 위해선 어떤 계정의 사용자가 어떤 행위를 했는지 추적하는 일이 필수적인데 하나의 계정을 여러 사람이 사용한다면 그런 추적이 매우 곤란하기 때문이다. 전문 용어로, '추적성 확보'가 안 되는 상황이다. 이러한 이유로 개인정보의 안전성 확보조치 기준도 개인정보취급자 계정의 공유 사용을 엄격하게 금지하고 있으며 위반 시에는 최대 3천만 원 이하의 과태료를 부과할 수 있도록 하고 있다.

〈개인정보의 안전성 확보조치 기준 제4조〉

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

7. 상시 근로자가 5명 이상이라면 내부관리계획을 수립해야 한다.

병원이든 의원이든 환자의 정보를 취급하는 근로자 수가 4명을 넘으면 개인정보 내부관리 계획을 수립해야만 한다. 개인정보 내부관리 계획이란 개인정보 보호에 대한 지침 또는 말 그대로 계획이라고 보면 되는데, 이 계획을 수립하는 것 자체가 개인정보의 안전성 확보조치 기준에 해당된다. '내부관리계획'란 타이틀로 문서 표지를 작성하고 내용으로는 다음 사항에 대해 검토하고 기록하여 책임자(개인정보책임자를 별도로 지정하지 않은 경우에는 의료기관의 최고경영자) 승인을 받은 후 보관하고 있으면 된다.

〈내부관리 계획의 필수 기재사항〉

① 개인정보 보호책임자의 지정에 관한 사항

② 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항

③ 개인정보의 안전성 확보에 관한 사항

④ 개인정보취급자에 대한 교육에 관한 사항

⑤ 그 밖에 개인정보 보호를 위하여 필요한 사항

8. 진료실에 CCTV가 있을 경우, 반드시 동의를 받아야 한다.

CCTV에 촬영된 개인의 영상 정보는 법으로 보호받아야 할 개인정보이다. 개인정보보호법에 따르면 일반적으로 공개된 장소에 설치된 CCTV에 대해서는 안내판을 설치하여 CCTV 운영 사실을 공개하기만 하면 된다. 그러나 진료실은 의료인과 환자만이 출입할 수 있으므로 불특정 다수가 출입할 수 있는 공개된 장소라고 보지 않는다. 따라서 진료실에 CCTV 등 영상정보처리기기를 설치하여 촬영하기 위해서는 이곳에 출입하는 모든 사람의 동의를 받아야만 녹화할 수 있다. 동의를 받은 경우에도 개인의 사생활 침해가 최소화되도록 녹화만 할 수 있을 뿐, 녹음은 할 수 없다. 녹음 금지 위반 시, 3년 이하의 징역 또는 3천만 원 이하의 벌금이 부과된다.

9. PC에 저장된 고유식별정보도 반드시 암호화해야 한다.

의료기관의 개인정보처리시스템으로는 병원정보시스템, OCS(Order Communication System, 처방전달시스템), EMR(Electronic Medical Record, 전자의무기록), PACS(Picture Archiving Communication System), LIS(Lab Information System, 임상병리시스템), 건강검진시스템 등을 들 수 있다. 이런 시스템에 저장되는 개인정보 중 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등 4가지 정보는 '고유식별정보'로 분류되어 반드시 암호화를 하도록 규정하고 있다. 실제로 이 부분은 규모가 있는 병원의 시스템에서는 암호화가 잘 되어 있는 편이다.

반면, 담당자의 PC에 저장된 고유식별정보는 암호화가 미흡한 경우가 많다. 암호화를 해야 한다는 인식 자체가 없거나 암호화 솔루션이 있어도 업무 편의성을 이유로 해제시켜 놓고 쓰는 경우도 있다. 개인정보의 안전성확보 조치기준은 PC에 저장되는 고유식별정보에 대한 암호화를 요구하고 있으며 최근엔 APT 공격 등 사내 PC를 통한 보안 침해 및 정보 유출 위험이 높아지고 있어 각별한 주의가 필요하다. PC 내 고유식별정보를 암호화하기 위해 DRM(Digital Rights Management)이나 암호화 솔루션을 사용하지 않더라도 엑셀과 같은 문서 편집 솔루션에 내장된 패스워드 설정 기능을 이용해도 무방하다.

〈개인정보의 안전성 확보조치 기준 제6조〉

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

10. 개인정보가 유출되면 반드시 정보주체(의료기록에 수록된 환자 등)에게 알려야만 한다.

법에서 규정한 개인정보가 유출된 상황은 다음과 같다.

〈개인정보 유출의 법적 정의〉

"개인정보 유출"이란 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용하는 것을 말하고, 개인정보 유출은 다음의 경우 가운데 어느 하나에 해당하여야 함.

① 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난 당한 경우

② 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

③ 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

④ 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우를 말함

해킹 등 사이버 공격에 의한 보안 침해 사고가 아니더라도 내부자의 실수에 의하여 개인정보가 수록된 파일 또는 종이문서가 권한이 없는 사람에게 잘못 전달될 수 있다. 이 경우에도 유출된 정보의 당사자에게 서면, 전자우편, 전화, SMS 등을 이용해 유출 사실에 대한 통지를 반드시 해야 한다는 의미이다. 위반 시 3천만 원 이하의 과태료가 부과된다.

개인정보 유출 발생 시, 정보주체에게 통지해야 할 사항은 아래와 같다. 또한 유출 건수가 10,000건을 넘는 경우에는 정보주체에게 통지하고 조치 결과를 5일 이내에 행정자치부장관 또는 전문기관(한국정보화진흥원, 한국인터넷진흥원) 중 하나에 신고해야 한다.

〈개인정보 유출시 통지 사항〉

① 유출된 개인정보의 항목

② 유출된 시점과 그 경위

③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

④ 개인정보처리자의 대응조치 및 피해 구제절차

⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

멀버타이징을 이용한 악성코드 분석

랜섬웨어가 이용하는 멀버타이징 기법 … 도대체 어떻길래?

안랩은 2015년 12월 월간 '안'의 '랜섬웨어, 알아야 막을 수 있다'를 통해 랜섬웨어가 증가하는 이유로 악성코드 제작자들이 유포지를 제대로 파악할 수 없도록 '멀버타이징(Malvertising)' 수법을 사용하기 때문이라고 설명한 바 있다. 멀버타이징을 이용한 방법은 불특정 다수를 대상으로 악성코드를 감염시킬 수 있어서 최근 많이 이용된다. 실제로 2015년 9월 말부터 국내에 증가하기 시작한 랜섬웨어의 주된 유포 방법으로 확인되었다.

이 글에서는 멀버타이징 애드웨어인 '에오레조(PUP/Win32.EoRezo)'를 통해 멀버타이징 기법이 어떻게 악성코드를 감염시키는지 알아보자.

멀버타이징(Malvertising)은 악성 프로그램을 뜻하는 멀웨어(Malware) 혹은 '악의적인'이라는 뜻의 멀리셔스(Malicious)와 광고 활동을 뜻하는 애드버타이징(Advertising)의 합성어다. 멀버타이징은 광고 서비스의 정상적인 네트워크를 이용하여 악성코드를 유포 및 감염시키는 방법을 말한다.

악성코드 제작자는 그럴 듯한 도메인 이름으로 위장된 광고 웹 사이트를 제작 후 광고 서비스에 이를 광고한다. 그리고 사용자가 해당 웹 사이트를 접속했을 때 취약한 페이지로 리다이렉트 되도록 설정해 둔다. 그 이후에 정상 웹 사이트로 이동한다.

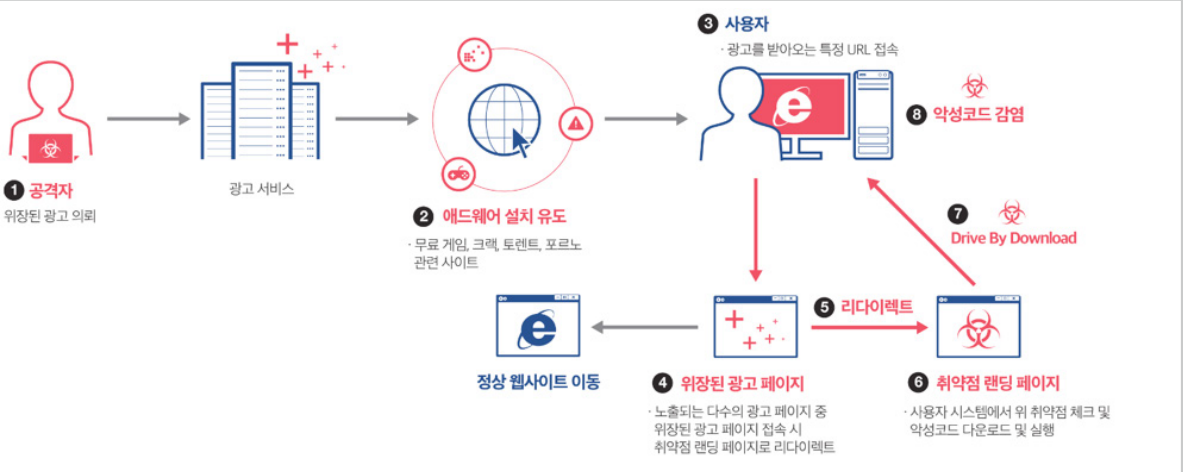
광고 서비스를 하는 업체는 일반적으로 사용자들에게 광고를 많이 노출하기 위해서 애드웨어를 사용하거나, 동적으로 광고를 받아 올 수 있는 특정 매개변수(Parameter)를 갖는 URL을 제공하기도 한다. 참고로 애드웨어(Adware)는 광고(advertisement)와 소프트웨어(software)의 합성어로 인터넷에 접속할 때마다 자동으로 활성화되는 광고 프로그램의 종류를 말한다.

이 글에서 소개하는 멀버타이징 애드웨어인 에오레조(PUP/Win32.EoRezo)는 동적으로 광고를 받아 올 수 있는 특정 매개변수를 갖는 URL 을 인코딩하여 내부적으로 가지고 있으며, 다음과 같은 웹 사이트에서 팝업을 통한 설치 또는 크랙 파일, 무료 게임 파일로 위장하여 설치를 유도한다.

– 토렌트 관련 사이트
– 크랙 관련 사이트
– 음란물 관련 사이트
– 무료 게임 사이트
– 무료 동영상 플레이어 다운로드 유도 사이트
– 허위 플래시 플레이어 다운로드 유도 사이트

멀버타이징 감염 방법

본격적으로 애드웨어 멀버타이징을 이용한 악성코드 감염 방법을 자세히 살펴보자.



[그림 1] 애드웨어 멀버타이징(Malvertising)을 이용한 악성코드 감염 방법

멀버타이징으로 악성코드에 감염되는 경우는 크게 2가지이다. 첫 번째, 웹 서핑 시 웹 브라우저의 팝업으로 보여지는 광고 사이트에 노출되는 경우이다. 두 번째, 사용자 시스템에 설치된 멀버타이징 애드웨어가 사용된 경우이다. 후자의 경우, 사용자가 웹 서핑을 하지 않아도 설치된 애드웨어가 불규칙하게 웹 브라우저를 자동 실행한 후 광고를 받아 오는 특정 매개변수를 갖는 URL로 접속하여 광고를 보여준다.

웹 사이트가 정상적인 광고 웹 사이트라면 이런 자동 실행이 문제가 되지 않을 수 있다. 하지만 보안이 취약한 웹 브라우저이거나 플래시 플레이어(Flash Player), 아크로뱃 리더(Acrobat Reader), 실버라이트(Silverlight), 자바(Java)가 설치된 경우라면 상황이 다르다. 사용자 의도와 상관 없이 애드웨어를 통해 취약점이 있는 웹 사이트로 리다이렉트된 후 앞서 열거한 웹 애플리케이션 플러그인 취약점을 이용하여 악성코드에 감염이 될 수 있다.

멀버타이징 애드웨어를 이용한 악성코드 감염 과정을 정리하면 다음과 같다.

① 공격자는 광고 서비스 업체에 위장 광고 의뢰

② 일부 웹 사이트를 애드웨어 배포지로 활용

– 예: 토렌트, 크랙, 음란물, 무료 게임, 무료 동영상 플레이어 다운로드 유도, 허위 플래시 플레이어 다운로드 유도 사이트

③ 사용자 웹 사이트 접속 시 애드웨어 설치 유도

④ 애드웨어에 의한 불특정 광고 사이트 접속

⑤ 위장된 광고 페이지 접속 시 취약한 사이트로 리다이렉트

– 이후 알려진 정상 사이트로 이동

⑥ 사용자 PC에서 애플리케이션 취약점 체크

– 예: 실버라이트, 아크로뱃 리더, 인터넷 익스플로러, 자바, 플래시 플레이어

⑦ 취약점이 확인되면 악성코드 다운로드 실행

⑧ 사용자 PC 감염

이러한 공격 뒤에는 '익스플로잇 킷(Exploit Kit, EK)'이라는 악성코드를 제작, 관리, 유포를 자동화할 수 있는 도구가 있으며 최근 공격에는 앵글러(Angler) EK, 리그(Rig) EK, 매그니튜드(Magnitude) 등이 주로 사용되고 있다.

애드웨어 주요 기능 요약

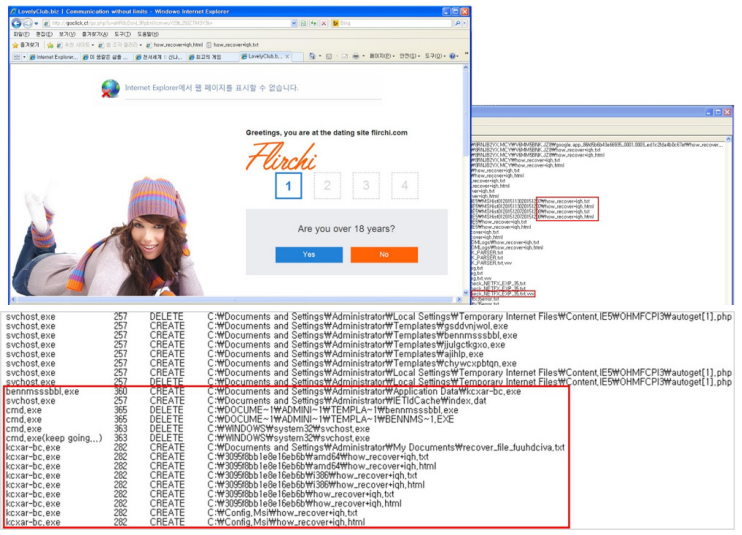
에오레조의 주요 기능을 살펴보자. 에오레조는 %appdata% 하위 경로에 특정 폴더와 파일을 생성한다. 파일에는 프로그램 설치 시간에 대한 내용이 담겨 있으며, 해당 정보를 가지고 추후 특정 IP로 접속을 시도한다. 실행 시 특정 조건이 성립하면 사용자 PC의 기본 브라우저를 통해 광고를 받아 오는 특정 매개변수를 갖는 URL에 접속을 시도하는데 요약하면 다음과 같다.

URL은 애드웨어 내부에 암호화되어 있으며 복호화 후 접속하기 위해 ShellExecute API를 호출하여 사용자 PC의 기본 브라우저를 실행한다. 이 행위는 특정한 규칙에 의해 이루어지며, 이 규칙은 time64 함수를 사용하여 특정 값들과 비교하는 방법을 사용한다. 이후 특정 값들과 비교하는 반복 루틴을 수행하면서 time64 함수의 리턴값이 내부적으로 정의된 특정값보다 크거나 같을 경우, ShellExecute API를 호출하여 웹 브라우저를 자동 실행한다. 접속 조건(시간, 횟수)이 일정하지 않기 때문에 사용자들은 애드웨어에 의한 접속 여부를 알아채기 어렵다.

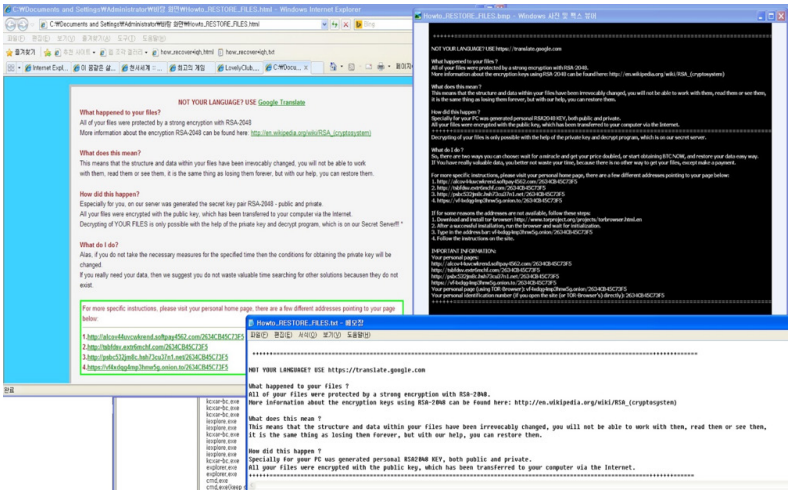
감염 사례

다운로드 실행 방식에 의한 '테슬라크립트' 랜섬웨어 감염 사례

[그림 2]는 실제 애드웨어가 접속하는 URL 중 취약한 광고 사이트에서 악성코드가 다운로드 실행(Drive-by-Download)이 이뤄지는 모습이다. 다운로드된 악성코드는 사용자 PC의 파일을 암호화하는 랜섬웨어로, 최근에도 꾸준히 변형이 나오고 있는 테슬라크립트(Teslacrypt)이다.



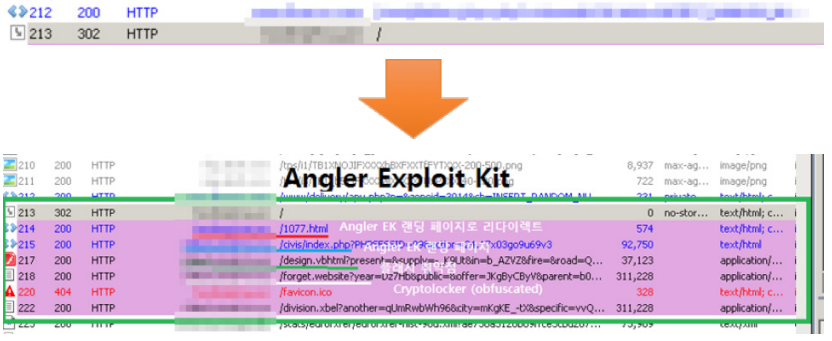
[그림 2] 취약한 사이트로부터 다운로드 실행(Drive-by-Download)으로 감염시키는 악성코드



[그림 3] 테슬라크립트 랜섬웨어에 감염된 모습

앵글러 EK에 의한 크립토락커 감염 사례

공격자에 의해서 제작된 booki*****.pw (이미 제거됨) 웹 사이트는 위에서 언급한 '광고 관련 특정 매개변수_내부 URL' 중 하나로, 광고 서비스 사이트인 www.fh****.com/(특정 매개변수)로부터 받아온다.



[그림 4] Angler Exploit Kit을 이용한 감염 사례

[그림 4] 에서 보듯이 이후 다음 순서대로 진행된다.

① 위장된 광고 웹 사이트 접속

② 취약점 랜딩 페이지로 리다이렉트

③ 랜딩 페이지의 악성 스크립트로부터 타깃 시스템에 플래시 취약점(CVE-2015-8446) 실행

④ 난독화된 크립토락커(Cryptolocker) 바이너리 다운로드 및 실행

지금까지 애드웨어 멀버타이징을 이용하는 악성코드 감염 방식에 대해 알아보았다. 멀버타이징을 이용한 방법은 불특정 다수를 대상으로 감염시킬 수 있고, 웹 사이트(도메인)를 자주 변경하여 유포지를 찾거나 차단하기 어렵게 만든다. 따라서 악성코드에 감염되지 않도록 철저하게 예방하는 것이 중요하다. 악성코드 감염을 막기 위해서는 항상 프로그램 및 백신 프로그램을 최신 업데이트 상태로 유지하는 것이 필요하다. 또한, 멀버타이징 공격은 애드웨어 프로그램으로 인해 사용자가 취약한 광고 사이트에 노출되기가 쉽기 때문에 해당 취약점에 자주 쓰이는 플래시 플레이어, 아크로뱃 리더, 실버라이트, 자바 등 애플리케이션의 업데이트가 필수적이다. 애드웨어를 이용한 멀버타이징은 사용자 개입 없이도 악성코드 감염에 노출될 수 있는 만큼 위에서 언급된 웹 사이트 방문 시 주의가 필요하다.

안랩은 해당 멀버타이징 애드웨어에 대해 V3와 MDS 제품에서 다음과 같은 진단명으로 진단 및 치료 기능을 제공한다.

- PUP/Win32.EoRezo(V3 제품군)
- Win-PUP/EoRezo
- Malware/MDP.Execute

한편 V3 제품군에서는 '악성 사이트 접근 차단' 기능을 통해 위장된 광고 페이지와 랜딩 페이지 등 멀버타이징 관련 사이트에 접속하는 것을 막아준다.

[그림 5] V3 Internet Security 9.0의 악성 사이트 접근 차단 기능

V3 Internet Security 9.0 사용자라면 '악성 사이트 접근 차단' 창 발생 시 '확인' 버튼을 눌러 더 이상 해당 웹 사이트 방문하지 않고 웹 브라우저가 종료되도록 조치하면 된다.

디지털 네이티브의 '신조어' 따라잡기

"캬~! 이 분 최소 사이다!",
"그 사람, 정말 고답이",
"너 정말 엄마랑 빼박캔트!",
"안물안궁!"

분명 한국어 같긴 한데 무슨 뜻인지 모르겠다면 요즘 사람들이 많이 쓰는 신조어에 익숙하지 않은 탓이다. 자녀와의 대화 도중 자녀의 말을 알아듣지 못하는 상황이 여러 번 있었거나, 직장 동료들과의 단체 대화방에서 쓰이는 말이 영 이해가 가지 않는 경험을 한 적 있다면 지금 주목하자.

태어난 순간부터 컴퓨터, 인터넷, 휴대폰과 같은 디지털 환경을 접하고 디지털 기기 사용이 생활화된 세대인 '디지털 네이티브(Digital Native)'. 그들에게 있어 '언어'는 즐거움을 풍요롭게 하기 위한 놀잇감 중 하나다. 이것으로 자신의 감정을 표현하고, 자신의 의견을 나타내기도 하며, 세상의 부조리를 비판하거나 비아냥거리기도 한다.

신조어 중 일부에 대해서는 과도한 줄임말, 한글 파괴와 같은 비판이 뒤따르기도 하지만 이 단어들은 현 세대의 문화와 정서를 반영하고 있다는 점에서 그것을 살펴보는 것만으로도 의미 있는 시간이 될 것이다. 다음에 소개한 단어 중 자신이 뜻을 알고 있는 것이 몇 개인지 세어보는 것도 재미있게 이 글을 읽는 방법 중 하나다.

1. 사이다

답답했던 속이 사이다를 마신 것처럼 시원하고 통쾌하게 풀릴 때 쓰는 감탄사 또는 수식어.

[연관 표현] 고구마, 사이다데이

삶은 계란이나 고구마를 먹다가 목이 막힐 때 사이다를 마시면 쑥 내려가는 경험을 해본 적이 있을 것이다. 이처럼 답답했던 속을 시원하게 해주는 상황에서 쓰는 말이 '사이다'다. 예전에는 사이다가 소화제로도 쓰였다고 하니 틀린 말도 아니다. 인터넷 게시판 등에서 문제가 되는 사안에 대해 조목조목 비판하는 글에 '이 분 최소 사이다!', '완전 사이다!'라는 댓글을 다는 식으로 많이 쓰인다. 일상 생활에서도 활용도가 높은 단어이니 기억해두는 것도 좋다. 11월 11일 빼빼로데이처럼, 4월 2일을 '사이다데이'라고도 한다.

2. 고답이

고구마를 100개 먹은 것처럼 답답한 사람이나 상황을 뜻하는 말.

[연관 표현] 고구마, 고답이병

신조어 '고구마'는 고구마를 먹고 목이 막히는 답답한 상황에서 쓰인다. '고답이'는 여기에서 한발 나아가 '고구마 답답이'의 줄임말이다. 상대의 말을 잘 알아듣지 못하거나 앞뒤가 꽉꽉 막힌 사람을 고답이라고 부른다.

3. 안물안궁

'안 물어봤고 안 궁금해'의 줄임말.

[연관 표현] 안물, 안궁

'안 물어봄'의 줄임말인 '안물'과 '안 궁금하다'의 줄임말인 '안궁'의 합성어다. 현재 대화의 주제와 상관없는 이야기를 꺼내거나 자신의 개인적인 이야기를 쓸 때 보통 글 앞에 말머리로 달아 쓴다. 상대방의 설명을 듣기 싫을 때도 쓸 수 있다. 하지만 무시의 의미도 담겨 있어 상대방이 언짢아 할 수 있다.

4. 복세편살

'복잡한 세상 편하게 살자'의 줄임말.

영화 '신세계'에서 이중구 역을 맡았던 배우 박성웅의 영화 속 대사 중 하나로, 그가 자신의 팬에게 페이스북 메시지로 '복잡한 세상 편하게 살자'라고 보낸 것이 '복세편살'로 줄여져 유행하게 됐다. 날로 힘들고 복잡해지는 세상에 대한 관조적인 태도가 담겨있기도 하다.

5. 사바사

사람 by 사람의 줄임말로, 사람에 따라 다르다는 뜻.

[연관 표현] 케바케

'케이스 바이 케이스(Case by case)'라는 말을 줄여 '케바케'라고 쓰는데, '사바사'는 이 말의 응용어쯤 되겠다.

6. 빼박캔트

빼도 박도 못한다는 뜻.

우리말 '빼도 박도'와 '~할 수 없다'는 뜻의 영어 표현 Can't가 합쳐져 만들어졌다. 이러지도 저러지도 못하는 난처한 상황에서 주로 쓰인다.

7. 트인낭

[격언] '트위터는 인생의 낭비다'라는 말의 줄임말.

영국 프로축구 맨체스터 유나이티드의 알렉스 퍼거슨 감독이 인터뷰 중 트위터에 적절하지 않은 글을 올린 웨인 루니 선수를 언급하며 "왜 그런 것(트위터)에 신경 쓰는지 모르겠다. 차라리 도서관에서 책을 읽어라. 그건 정말 시간 낭비다"라고 말한 데서 유래했다. 이 말이 적절하게 붙고 줄여져 '트인낭'이라는 신조어가 탄생했다. 트위터나 페이스북 등의 SNS에 부적절한 글을 올렸다가는 곤경에 처할 수 있음을 경고하는 의미로 쓰인다.

8. 노오력

노력보다 더 큰 노력이라는 의미로 노력이라는 단어에 '오오', '오오오'를 넣어 '노오오력', '노오오오력' 이런 식으로 응용된다.

[확장 표현] 노오오력, 노오오오력

연애, 결혼, 출산을 포기하는 3포 세대, 3포에 집과 인간관계까지 포기하는 5포 세대, 5포를 넘어 꿈과 희망 그리고 삶의 모든 가치를 포기한 20~30대를 말하는 N포 세대. N포 세대의 좌절을 보고 노력이 부족해서라고 꾸짖는 기성 세대의 충고를 비꼬는 의미에서 만들어진 말이다. 노력보다 더 큰 노력을 해도 사회가 혼란스러워 되지 않는다는 의미를 함축하고 있다.

9. 스테이케이션

'머물다'라는 의미의 영어 표현인 '스테이(stay)'와 휴가를 뜻하는 '배케이션(vacation)'의 합성어

휴가 중에 먼 곳으로 떠나지 않고 집이나 집 근처에서 휴가를 보내는 것을 말한다. 역시 휴가는 집에서 쉬는 게 진리인 것일까? 본래 휴가(休暇)는 쉴 '휴(休)'에 틈 '가(暇)'자를 쓴다.

핵노잼, 생선, 생파, 노답, 버카충 그리고 별다줄까지..

이 밖에 요즘 어린이들이 많이 쓰는 단어들도 있다. '핵노잼'은 '재미없다'는 뜻. '생선'은 '생일 선물', '생파'는 '생일 파티'의 줄임말이다. '노답'은 '답이 없다'는 뜻. '버카충'은 '버스 카드 충전'의 줄임말이다.

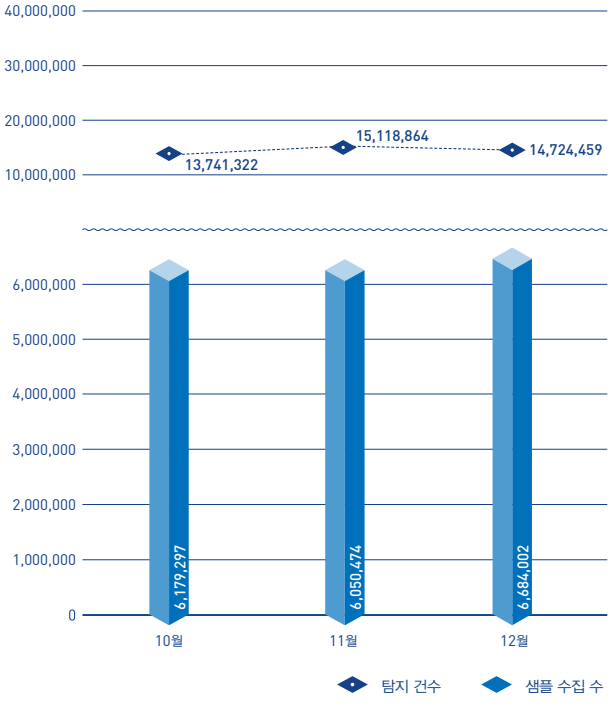
'별다줄'도 신조어인데 '별걸 다 줄인다'는 뜻이다. 신조어 중에는 정말 별걸 다 줄여 쓴다는 생각이 드는 경우가 많은데 그걸 지적하는 말조차도 줄임말이다.

안랩, 12월 악성코드 통계 및 보안 이슈 발표

잇따른 신종 랜섬웨어…'지역화' 양상도 보여

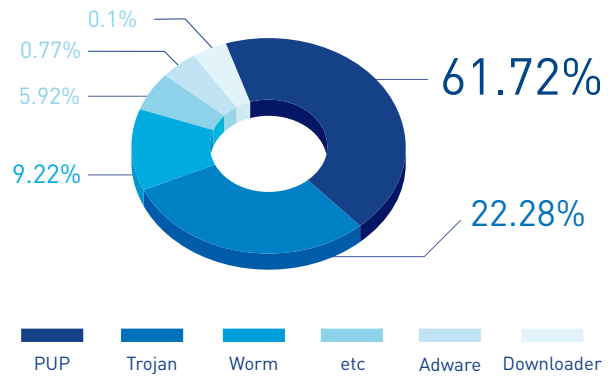
안랩 시큐리티대응센터(ASEC)는 ASEC Report Vol.72를 통해 지난 2015년 12월의 보안 통계 및 이슈를 전했다. 12월의 주요 보안 이슈를 살펴본다.

ASEC이 집계한 바에 따르면, 2015년 12월 한 달간 탐지된 악성코드 수는 1,472만 4,459건으로 나타났다. 이는 전월 1,511만 8,864건에 비해 39만 4,405건 감소한 수치다. 한편 12월에 수집된 악성코드 샘플 수는 668만 4,002건이다.



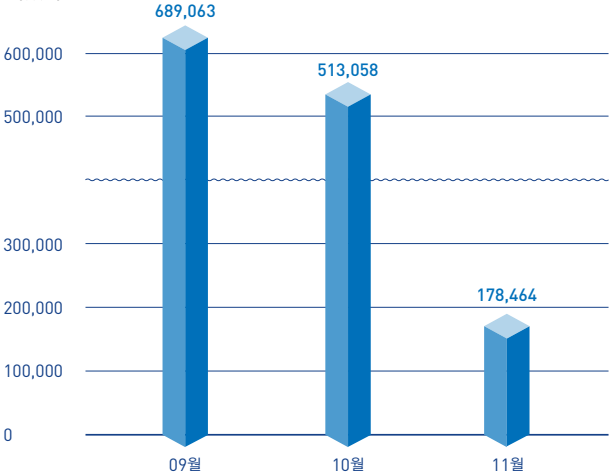
[그림 1] 악성코드 추이(2015년 10월 ~ 2015년 12월)

[그림 2]는 2015년 12월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 61.72%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 22.28%, 웜(Worm)이 9.22%의 비율로 그 뒤를 이었다.



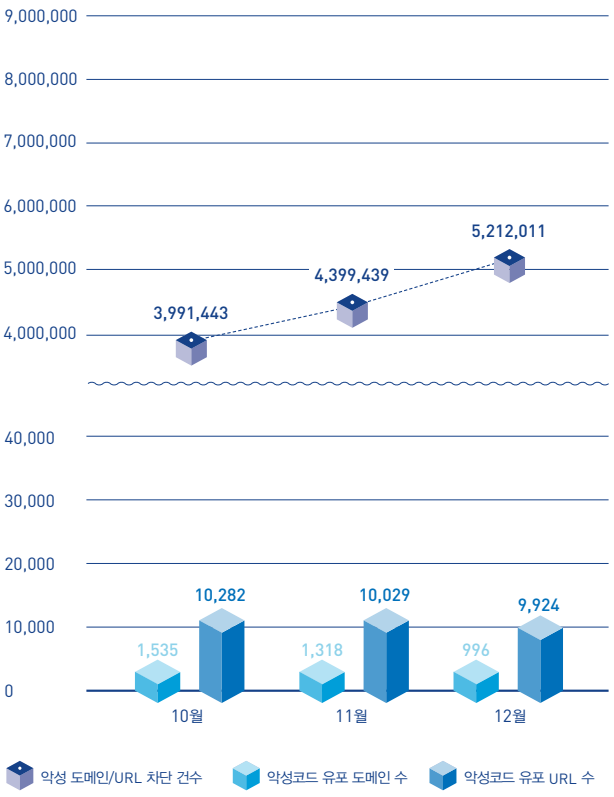
[그림 2] 2015년 12월 주요 악성코드 유형

지난 12월 한 달간 탐지된 모바일 악성코드는 17만 8,464건으로 집계됐다



[그림 3] 모바일 악성코드 추이(2015년 10월 ~ 2015년 12월)

또한 지난 12월 악성코드 유포지로 악용된 도메인은 996개, URL은 9,924개로 집계됐다. 12월의 악성 도메인 및 URL 차단 건수는 총 521만 2,011건이다.



[그림 4] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 10월 ~ 2015년 12월)

신종 랜섬웨어, 파일 유포 협박부터 '지역화'까지

지난 2015년에 전세계적으로 랜섬웨어가 폭발적으로 증가했다. 랜섬웨어는 기술적으로도 고도화되고 있으며, 최근에는 '지역화' 양상까지 보이고 있다. 기존의 랜섬웨어의 금품 요구 메시지는 대부분 영어로 작성되어 있었으나 최근 영어 외의 다른 언어를 사용하는 랜섬웨어가 등장하고 있는 것이다. 일례로 일부 크립토락커(CryptoLocker) 랜섬웨어는 감염 PC의 IP 대역을 확인하여 금품 요구 메시지를 해당 국가의 언어로 출력하기도 한다. 최근에는 러시아어로 제작된, 이른바 '오프라인(Offline)' 랜섬웨어와 유럽 지역 사용자를 노리는 '키메라(Chimera)' 랜섬웨어도 등장했다.

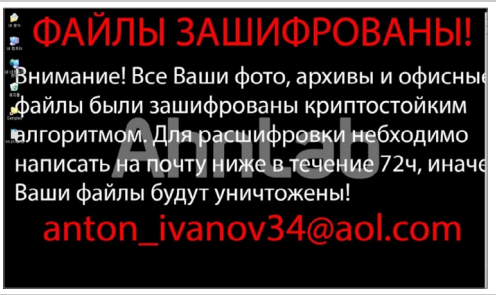
1. 오프라인 랜섬웨어

다른 랜섬웨어와 달리 C&C 서버와의 통신 없이도 감염 PC의 파일을 암호화하는 랜섬웨어가 등장했다. 이런 특징 때문에 '오프라인(Offline) 랜섬웨어'로 명명됐다. 오프라인 랜섬웨어는 일반적인 랜섬웨어와 마찬가지로 RSA 알고리즘을 사용한다. 다만 C&C 서버로부터 키(Key)를 전달받아 파일 암호화를 진행하는 것이 아니라, 감염 시스템의 정보 및 암호화 대상 파일의 데이터를 기반으로 무작위로 키를 생성하여 여러 단계를 거쳐 암호화를 진행한다는 점이 다르다. 즉, C&C 통신을 통해 암호화 키를 받지 않아도 파일 암호화가 진행된다. 오프라인 랜섬웨어는 주로 메일에 첨부된 RAR 압축 파일을 통해 유포되고 있어 사용자의 주의가 필요하다.

[그림 5] 오프라인 랜섬웨어 유포 파일(RAR 파일 압축 해제 후)

[그림 5]는 국내에서 발견된 오프라인 랜섬웨어로, RAR 파일의 압축을 해제한 exe 파일이다. 이 파일이 실행되면 특정 파일을 생성하며 시작프로그램에 리지스트리를 등록한다. 이후 PC별로 무작위로 생성한 아이디 및 감염 시점을 저장하고, 특정한 URL로 'GET' 요청을 수행한다.

암호화가 완료되면 [그림 6]과 같이 러시아어로 작성된 메시지가 담긴 그림 파일을 바탕화면으로 설정한다. 요약하면 '파일이 암호화 되었고, 아래 메일 주소로 72시간 내에 메일을 보내지 않으면 파일이 파괴된다'라는 내용이다. 여기에서 '파일이 파괴된다'는 것은 복호화가 불가능하게 된다는 의미로, 일반적으로 '지불이 확인되면 복구 툴을 주겠다'라는 다른 랜섬웨어들과는 차이를 보인다.



[그림 6] 오프라인 랜섬웨어 감염 화면

2. 키메라(Chimera) 랜섬웨어

최근 독일 등 유럽 국가를 중심으로 키메라(Chimera) 랜섬웨어가 유포되고 있다. 키메라 랜섬웨어가 처음 발견된 2015년 9월 당시에는 독일에서만 피해 사례가 보고되어 여파가 크지 않은 것으로 여겨졌다. 그러나 최근에는 랜섬웨어 유포자를 공모하는 등 그 영향력을 키워나가고 있다.

키메라 랜섬웨어는 다른 랜섬웨어와 마찬가지로 암호화를 하고 나면 비트코인을 입금할 주소를 안내하는 HTML 페이지를 생성한다. 여기에서 특이한 점은 돈을 지불하지 않으면 암호화된 파일을 인터넷에 유포하겠다고 협박한다는 점이다. 그러나 실제로는 협박 내용과는 달리 암호화된 파일을 유출하는 기능은 존재하지 않았다.

[그림 7] 키메라 랜섬웨어 감염 화면

키메라 랜섬웨어는 암호화 대상인 확장자의 종류가 상당히 많은 것으로 확인되었다. 심지어 Windows 구동에 필요한 boot.ini, system.ini 파일도 암호화한다. 키메라 랜섬웨어에 의해 암호화된 파일은 확장자 뒤에 '.crypt'가 붙는다.

[키메라 랜섬웨어의 암호화 대상 파일 확장자]

*.jpg, *.jpeg, *.vmx, *.txt, *.xml, *.xsl, *.vbs, *.ini, *.conf, *.config, *.msg, *.key, *.htm, *.html, .class, .java,.cs,

.asp, *.aspx, *.php, *.jsp, *.bak, *.dat, *.pst, *.eml, *.sql, *.js, *.jar, *.py, *.db, *.bay, *.png, *.bmp, *.gif, *.zip,

.rar, *.bin, *.ptx, *.wav, *.ram, *.mkv, *.doc, *.docx, *.rtf, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *swf, etc.

이처럼 키메라 랜섬웨어의 광범위한 암호화 때문에 일부 운영체제에서는 "Windows 실행에 필요한 파일이 알 수 없는 버전으로 교체되었다. 시스템 안정성을 유지하려면 원본 버전으로 복원해야 한다"는 메시지가 나타나는 경우도 있다.

랜섬웨어 감염 화면의 html 소스코드를 확인해보면, 아래 그림과 같이 키메라 랜섬웨어 제작자는 공모자를 모집하고 있다. P2P 형식의 암호화 메일 시스템인 비트 메시지(BitMessage)를 이용해 연락을 취하라는 내용으로, 이는 추적을 피하기 위한 것으로 보인다.

[그림 8] 공모자를 모집하는 키메라 랜섬웨어 제작자

한편 V3 제품에서는 이들 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

〈V3 제품군의 진단명〉

Trojan/Win32.MDA (2015.12.01.04)

Trojan/Win32.Chimera (2015.11.10.07)

랜섬웨어는 최근 침해된 웹사이트를 통해서 유포되는 경우가 대부분이지만, 여전히 스팸 메일을 이용한 랜섬웨어 감염도 이뤄지고 있다. 특히 지속적으로 다양한 랜섬웨어 변종이 나타나고 있어 사용자의 각별한 주의가 필요하다.

안랩, SW 공인 파트너사 대상 ‘안랩 파트너 데이’ 개최

안랩은 지난 1월 27일 양재동 엘타워에서 공공/교육/기업 분야의 SW 공인 파트너사를 초청해 ‘안랩 파트너 데이 2016’을 개최했다.

이 행사에서 안랩은 ‘Partner, Connected’라는 주제 하에 최신 IT 환경에서의 보안 전략을 파트너와 공유하고, 안랩의 사업 전략 및 파트너 지원 프로그램을 소개했다.

먼저 안랩 이호웅 연구소장이 클라우드, BYOD, 빅데이터, 사물인터넷(IoT), O2O(Online to Offline) 등 IT 최신 트렌드를 설명하며 변화하는 IT 환경에 대응하는 R&D 방향 및 보안 전략에 대해 발표했다.

EP(엔드포인트플랫폼)사업 총괄 강석균 전무는 2016년 EP사업부 사업계획을 발표하며 1등 보안 플랫폼 기업으로 도약하기 위해 ▲파트너 동반 성장 ▲제품 경쟁력 강화 ▲신규 시장 확대 등을 진행할 계획이라고 밝혔다. 이어서 EP영업본부 배민 본부장이 안정된 파트너 체계 유지와 신규시장 확대, 소통 강화 등 파트너 프로그램 전략을 소개했다. EP기술지원본부 임영선 본부장은 파트너 케어 다각화, 협업 모델 활성화, 기술지원 효율화 등 다양한 관점의 파트너 지원 방안을 소개했다.

안랩 권치중 대표는 “안랩은 올해 파트너사와 함께 현장의 목소리를 경청하고 해결방안을 함께 고민하며 파트너사와 동반 성장 할 수 있는 미래를 만들어 나가겠다”라고 말했다.

안랩, ‘아마존 웹서비스 고객을 위한 원격보안관제 서비스’ 개시

안랩이 아마존 웹 서비스(Amazon Web Service, 이하 AWS) 이용 고객의 클라우드 서버의 보안을 원격으로 관리해주는 ‘AWS 고객을 위한 원격보안관제 서비스’를 개시했다.

AWS는 서비스 제공업체, 즉 아마존과 고객 간 관리 영역을 나누어 운영 책임을 분산하는 구조이다. 즉, 데이터 센터, 컴퓨팅, 스토리지, 데이터베이스 등 AWS 자체 관리영역과 고객 데이터, 네트워크 및 방화벽, 애플리케이션 관리 등 고객 관리 영역으로 나눠져 있다.

안랩의 ‘AWS 고객을 위한 원격보안관제 서비스’는 AWS를 이용하는 고객이 직접 수행해야 하는 서비스 관리 영역 중 네트워크 및 방화벽 보안을 안랩의 침해대응(CERT) 전문 인력이 원격으로 모니터링 및 관리해주는 서비스다.

안랩의 전문 관제 인력을 통해 ▲고객의 클라우드 서버 상시 모니터링 ▲클라우드 환경 내 보안 솔루션 운영 및 보안 위협 분석 ▲고객에 최적화된 보안 정책 설정 및 운영 등 AWS 서비스 이용에 필요한 보안 서비스를 제공한다.

이 서비스로 AWS 서비스 이용 고객은 높은 전문성이 필요한 보안 영역에 대한 직접 관리 부담을 줄이고, 전문 인력이 제공하는 수준 높은 보안관제 서비스 및 보안 위협에 대한 추가 정보도 제공받을 수 있다.

또한, 고객이 현재 보안 현황을 실시간으로 확인할 수 있도록 데이터 시각화 대시보드를 제공하고, 정기/비정기 관제 보고서로 최신 보안 동향, 탐지 이벤트 분석 등 보안 인텔리전스(Security Intelligence)를 제공한다. 이를 통해 고객 스스로 보안 수준을 판단하고, 위협 정보를 활용해 더욱 강력하고 효과적인 보안관리를 수행할 수 있다.

안랩 서비스사업부의 방인구 상무는 “안랩은 아마존과 공식 파트너를 맺고 보안 서비스를 제공하는 클라우드 보안 관제의 퍼스트무버(First Mover)”라며 “안랩의 침해대응 노하우와 보안관제에 대한 전문성을 바탕으로 새로운 IT 환경에서도 안정적인 보안관제 서비스를 제공할 수 있도록 노력하겠다”고 말했다.

발행인 : 권치중
발행처 : 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000 F. 031-722-8901
편집인 : 안랩 콘텐츠기획팀
디자인 : 안랩 디자인팀

http://www.ahnlab.com

http://blog.ahnlab.com

http://twitter.com/ahnlab_man

AhnLab

경기도 성남시 분당구 판교역로 220

T. 031-722-8000 F. 031-722-8901