

안랩 온라인 보안 매거진

월간 安

2016. 12

2016 Threat Review

CONTENTS

3 SPECIAL REPORT

2016년을 휩쓴 보안 위협 Top 5
치열한 적자생존 속 '위협의 진화'

6 HOT ISSUE

임베디드 리눅스 기반 사물인터넷 보안위협 동향
IoT 환경 위협하는 '리눅스 악성코드 Top 5'

8 PRODUCT ISSUE

안티랜섬웨어 툴, 탐지 범위 넓히고 삭제 기능 더하고

10 FOCUS IN-DEPTH

애드원드 악성코드의 역습

13 THREAT ANALYSIS

오픈타입 폰트 취약점을 악용한 공격 주의!

15 IT & LIFE

핀테크의 오늘과 내일

17 STATISTICS

2016년 10월 보안 통계 및 이슈

19 AHNLAB NEWS

안랩, '2016 ESG 우수기업' 우수기업상 수상
DDoS 대응 솔루션 '트러스가드 DPX' 매출 크게 성장

2016년을 휩쓴 보안 위협 Top 5

치열한 적자생존 속 '위협의 진화'

“환경에 적응하면서 단순한 것으로부터 복잡한 것으로 진화하며, 경쟁에 적합한 것은 살아남고 그렇지 못한 것은 도태된다” 한 줄로 요약한 다윈의 진화론이다. 2016년 보안 위협 동향도 꼭 이와 같다. 올 한해 보안 위협은 단순한 것에서 복잡다단한 것으로 진화했고, 그들만의 생태계를 통해 공생하면서도 치열한 적자생존 속에서 도태되어 사라지거나 더 강력한 변종으로 나타났다. 변화하는 IT 환경에 우리보다 먼저 적응한 새로운 위협은 현실이 되었다.

안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)가 수집 및 분석한 위협 정보를 중심으로 2016년 주요 위협 동향을 되짚어본다.

전세계를 집어삼킨 랜섬웨어

올 한해 보안 업계뿐만 아니라 뉴스 등 언론을 통해 일반 사용자들 사이에서도 지겨울 정도로 빈번하게 등장한 보안 용어는 바로 ‘랜섬웨어(Ransomware)’다. 더 이상의 설명이 필요 없는 랜섬웨어는 지난 한해 동안 종류와 양이 폭발적으로 증가하면서 전세계적으로 막대한 피해를 입혔다. ASEC에 접수된 비율만 보더라도 연초에는 전체 보안 침해 신고의 15%에 불과하던 것이 11월 말에는 4배 가량 증가해 60% 이상을 차지했다.



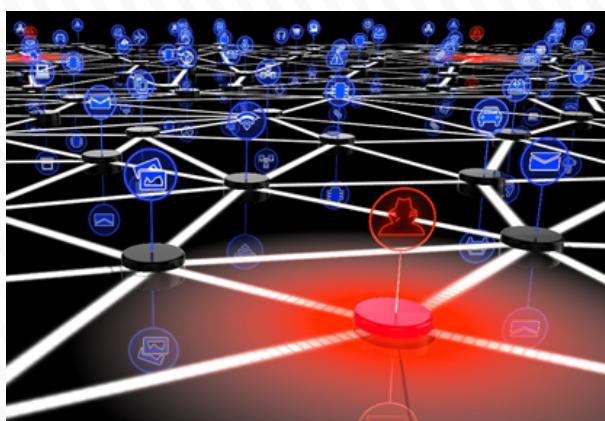
2016년 랜섬웨어의 동향을 자세히 살펴보면, 크고 작은 변화와 소멸을 거듭하며 결과적으로 진화하는 양상을 보이고 있다. 지난 2015년 악명을 떨쳤던 테슬라크립트(TeslaCrypt)가 올해 5월, 돌연 활동 종료를 선언했다. 또 국내에서 피해가 커던 크립트XXX(CryptXXX)도 지난 7월 이후 잠잠해졌다. 반면 스팸 메일을 통해 유포되는 록키(Locky)나 음성으로 감염 사실을 알려주는 케르베르(CERBER)는 지속적으로 업그레이드를 거듭하고 있다. 또 파일뿐만 아니라 MBR(Master Boot Record)까지 암호화해 PC 사용 자체를 방해하는 랜섬웨어도 등장했다.

특히 올해는 랜섬웨어 제작과 유포를 대행해주는 랜섬웨어 서비스, 이른바 RaaS(Ransomware-as-a-Service)가 본격화되면서 랜섬웨어의 전 세계적인 확산에 영향을 끼쳤다. 심지어 다양한 언어를 지원하는 경우도 있다. 대부분의 랜섬웨어는 영어로만 제작되어 있지만, 국내 감염율이 높았던 테슬라크립트나 크립트XXX, 록키, 케르베르 등은 영어 외에도 각국 언어로 서비스를 제공한다.

유포 및 감염 방식 또한 스팸 메일의 첨부 파일부터 드라이브 바이 다운로드(Drive-by-download), 멀버타이징(Malvertising), 최근에는 사회공학기법과 결합하거나 RDP(Remote Desktop Protocol)를 이용하는 등 다양화되고 있다.

이 밖에도 교육 및 연구 목적의 오픈소스인 EDA2, 하든티어(Hidden Tear) 등이 실제 랜섬웨어에 약용되기도 했으며, 크립트XXX나 록키, 페트야(PETYA)와 같은 유명 랜섬웨어를 모방한 사례도 등장했다. 공격자 관점에서 단기간 내에 직접적으로 금전적 이득이 발생한다는 점 때문에 이후로도 랜섬웨어의 증가 추세는 수그려들지 않을 것으로 보인다.

가성비 높은 표적 공격, 경계가 없다



특정한 대상을 선별하여 공격하는 표적 공격(target attack)은 투자 대비 성공률이 높다는 특징 때문에 최근 몇 년간 두렷한 증가세를 나타냈다. 표적 공격은 정치적인 목적과 금전적 목적의 일반 기업을 노린 공격으로 구분할 수 있다.

2016년 2월 미국 국토안보부(DHS) 인사정보 탈취 사건은 러시아의 소행으로 의심되고 있고, 지난 8월 실수로 유출된 것으로 알려진 미국 국가안보국(NSA)의 해킹 툴(Shadow Brokers) 또한 국가간 스파이전과 연관성이 있다. 개인을 대상으로 하는 표적 공격도 대부분 정치적인 목적을 띠고 있다. 주로 홍콩, 미얀마, 시리아, UAE, 카자흐스탄 등의 국가에서 집권당에 반대하는 정치인이나 사회운동가 등을 노린 표적 공격이 발생했다.

일반 기업을 노리는 표적 공격의 단골 메뉴는 개인정보, 즉 개인정보다. 올해도 국내는 물론 야후, 드롭박스 등에서 개인정보 유출 사고가 발생했다. 또 이른바 비즈니스 이메일 스캠(Business email scam)이라 불리는 전통적인 이메일 변조 사기도 유럽과 북미 지역의 기업에 막대한 피해를 입히며 성행 중이다. FBI 집계에 따르면, 이메일 변조 피해 사례는 미국에서만 총 7,000건, 피해액은 약 740만 달러로 확인됐다. 올해 국내에서 발생한 모 기업의 이메일 해킹에 의한 무역대금 240억원 피해 사례의 경우, 사우디 국영 정유업체인 사우디아람코의 이메일 계정이 해킹 당한 것이 원인으로 알려져 있다.

표적 공격은 피해자가 공격 당한 사실을 인지하기까지 오랜 시간이 소요되고, 공격자는 확인하기 어렵거나 짐작만 하는 경우가 대부분이기 때문에 공격의 탐지와 대응이 쉽지 않다. 특히 피해자가 기업 또는 기관 등 조직의 일원일 경우 심각한 피해로 이어질 수 있어 지속적인 주의와 상세한 모니터링이 필요하다.

IoT 악성코드의 선제공격

사물인터넷, 이른바 IoT(Internet of Things) 기술이 발달함에 따라 이와 관련된 위협 또한 진화를 거듭하고 있다. 사물인터넷 기기는 사용성과 저전력의 측면에서 경량화된 임베디드 리눅스(Embedded Linux) 운영체제를 사용한다. 사용자 단말에 사용되는 운영체제를 관리하기 쉽지 않고, 특히 제조사가 영세할 경우 보안까지 신경 쓰기는 쉽지 않은 현실이다. 공격자들은 이 점을 놓치지 않았다.

2016년 9월, 유명 보안 블로그인 크렙스온시큐리티(KrebsOnSecurity)와 호스팅 업체 OVH에 대해 기록적인 규모의 DDoS 공격이 발생했다. 또 지난 10월에는 미국 인터넷 호스팅 서비스업체 딘(Dyn)에 대한 DDoS 공격도 발생했다. 이 공격으로 인해 트위터(Twitter), 뉴욕타임스(The New York Times), 에어비앤비(Airbnb), 페이팔(PayPal), 넷플릭스(Netflix), 사운드클라우드(SoundCloud) 등 다수의 웹사이트에서 접속 장애가 발생했다. 이들 두 공격에는 사물인터넷 악성코드인 미라이(Mirai) 악성코드가 이용된 것으로 확인되었다.

다양한 사물인터넷 기기가 공격에 이용되었으며, 일부 악성코드의 소스코드가 공개되면서 올 한해 동안에만 1만 개 이상의 사물인터넷 관련 악성코드가 발견됐다.

최근 들어 사물인터넷 기기 제조사들도 보안 문제에 대해 관심을 갖기 시작했다. 그러나 사물인터넷 기기는 한번 구입 또는 설치 후 지속적으로 관리하기가 쉽지 않다. 설치 후 대략 5년 정도 사용된다고 가정하면 향후 몇 년 동안은 사물인터넷 기기를 이용한 공격 사례가 꾸준히 발생할 수 있다.

익스플로잇 키의 적자생존, 치열한 취약점 공격

익스플로잇 키(Exploit Kit, 이하 EK)은 취약점을 이용한 악성코드를 대량으로 유포하는 툴로, 랜섬웨어 암시장이 활성화되면서 더욱 활개를 치고 있다. 이와 함께 익스플로잇 키의 치열한 경쟁과 지각 변동이 나타났다.

지난 상반기 랜섬웨어 유포 1순위로 악명을 떨쳤던 앵글러(Angler EK)와 뉴클리어(Nuclear EK)가 활발히 활동하다 갑자기 사라졌고, 앵글러의 자리를 물려받았던 뉴트리노(Neutrino EK) 역시 하반기 들어 활동이 감소했다. 반면 선다운(Sundown EK), 매그니튜드(Magnitude) 등은 지속적으로 활동하고 있다.

익스플로잇 키의 단단계 리다이렉션(Redirection) 기법은 웹사이트 광고 서버를 이용해 랜섬웨어 등 악성코드를 유포하는 멀버타이징(Malvertising) 공격에 주로 이용되고 있다. 다양한 스크립트 형식의 다운로더나 익스플로잇 키를 이용한 랜섬웨어 유포는 현재도 지속적으로 발생하고 있으며, 윈도우 헬프로그램인 파워쉘(Powershell)을 이용한 악성코드도 다수 발견되었다.

또한 익스플로잇 키가 활기를 띠면서 이들이 주로 이용하는 인터넷익스플로러(Internet Explorer, IE), 플래시(Flash), 자바(Java) 등의 취약점을 비롯해 다양한 취약점 공격이 더욱 거세졌다. 특히 문서 파일과 관련된 EPS(Encapsulated PostScript) 취약점과 오픈타입 폰트(Open Type Font) 취약점을 이용한 악성코드 유포도 증가했다. 또, 윈도우(Windows) 운영체제의 정상 기능의 설계상 결함을 이용한 코드 인젝션(injection) 기법의 아톰비밍(AtomBombing)은 모든 버전의 윈도우 운영체제에 영향이 있는 것으로 알려졌다.

모바일 환경에 뿌리내린 루팅 앱

2016년에는 안드로이드 기반의 스마트폰을 루팅(Rooting)하는 악성 앱이 다수 발견되었다. 특히 지난 7월부터 10월까지 3개월간 앤랩이 수집한 루팅 악성 앱의 수가 2016년 상반기 6개월 대비 약 30% 가량 증가했다. 악성 앱이 갈수록 급증하고 있음을 알 수 있다.

악성 앱은 주로 사용자 몰래 앱을 설치하거나 모바일 백신 제품의 탐지 및 삭제를 우회하고, 개인정보를 탈취하거나 광고를 노출하는 등의 악의적인 행위를 위해 루트 권한을 이용한다. 지난 상반기에는 주로 루팅을 통해 광고 행위 또는 사용자 몰래 앱을 설치하는 악성 앱 유형이 주를 이뤘고, 하반기에 들어서며 금융정보 탈취를 목적으로 하는 루팅 앱도 나타났다. 중국에서 제작된 악성 앱들은 대부분 추가적인 앱 설치 또는 광고 노출을 통한 수익을 위해 루트 권한 획득을 시도하는 것으로 확인됐다.



루팅을 시도하는 악성 앱들은 안드로이드 운영체제의 취약점을 이용해 스마트폰의 권한을 획득한다. 상반기에 발견된 악성 앱 갓리스(Godless)는 안드로이드 운영체제 5.1 버전(Lollipop) 이하에서 루트 권한 탈취를 위해 다수의 취약점을 이용했다.

이처럼 안드로이드 운영체제의 취약점을 이용한 악성 앱이 증가함에 따라 구글은 안드로이드 보안 강화를 위해 다각도로 노력을 기울이고 있다. 지난 2015년 스테이지 프라이트(Stage fright) 취약점이 발견된 이후 매달 안드로이드 운영체제 보안 업데이트를 제공하는 한편, 각 스마트폰 제조사들의 업데이트 대응 순위를 공개하고 있다. 또 올해 공개된 안드로이드 운영체제 7.0 버전(Nougat)은 루팅을 통해 시스템 변조를 시도할 경우 부팅 자체를 불가능하게 했다. 문제는, 스마트폰 제조사 또는 단말기의 생산 연도에 따라 보안 업데이트가 제공되지 않는 경우가 있다는 점이다. 따라서 구 버전의 운영체제를 사용하고 있는 스마트폰은 보안에 대해 각별한 주의가 필요하다.

임베디드 리눅스 기반 사물인터넷 보안 위협 동향

IoT 환경 위협하는 ‘리눅스 악성코드 Top 5’

2016년 9월 유명 보안 전문가 브라이언 크렙스의 블로그 크렙스온시큐리티(KrebsOnSecurity)와 프랑스 인터넷 호스팅 업체 OVH에 대해 기록적인 DDoS 공격이 있었다. 이어 2016년 10월 21일 금요일 오전 미국 인터넷 호스팅 서비스업체 딘(Dyn)이 DDoS 공격을 당한 사건이 일어났다. 이로 인해 에어비앤비(Airbnb), 페이팔(PayPal), 넷플릭스(Netflix), 사운드 클라우드(SoundCloud), 트위터(Twitter), 뉴욕타임스(The New York Times) 등 여러 사이트에서 접속 장애가 발생했다. 그리고 이들 공격에는 사물인터넷(Internet of Things, IoT)을 감염시키는 미라이(Mirai)라는 악성코드가 이용되었음이 밝혀진다.

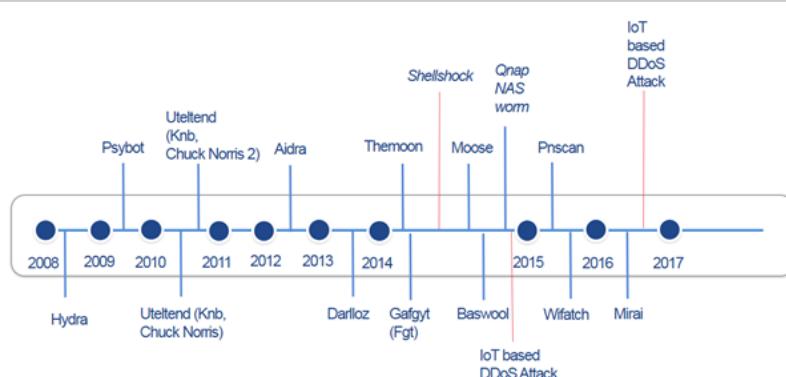
안랩은 월간 ‘안’ 2015년 10월호 ‘IoT 그리고 임베디드 리눅스 악성코드’라는 글에서 사물인터넷 기기를 겨냥한 리눅스 악성코드 제작과 임베디드 리눅스 기반 기기의 보안 문제를 다룬 바 있다.

이번 호에서는 미라이 악성코드를 비롯해 최근 발견된 사물인터넷 관련 리눅스 악성코드에 대해 살펴본다.

현재 여러 운영체제가 IoT의 주도권을 놓고 경쟁하고 있으며 이중 임베디드 리눅스(Embedded Linux)가 많이 사용되고 있다. 우리가 흔히 접할 수 있는 인터넷 공유기, 셋톱 박스, NAS(Network Attached Storage), 디지털 비디오 레코더, IP 카메라 등에 임베디드 리눅스가 이용되고 있다. 이들 시스템은 데스크톱과 비교했을 때는 저성능이지만 다른 IoT 제품보다는 컴퓨터에 가까워 공격자들의 우선 목표가 되고 있다.

이러한 임베디드 리눅스를 겨냥한 악성코드는 2008년 처음 보고되었다. 초기 임베디드 리눅스 악성코드는 MIPS 프로세스를 사용하는 인터넷 공유기만 감염시킬 수 있었지만, 2012년 발견된 에이

드라(Aidra) 웜은 MIPS 외 다양한 프로세스를 지원해 인터넷 공유기뿐 아니라 셋톱 박스 등 다양한 임베디드 리눅스 환경에서 활동할 수 있었다. 많은 임베디드 리눅스 악성코드는 DDoS 공격 기능이 주 목적이지만 2013년 발견된 달로즈(Darlolz)는 비트코인과 같은 가상화폐 채굴이 주목적이다. 2014년 말 리자드 스쿼드(Lizard Squad)란 그룹에서 가프지트(Gafgyt) 변형으로 일으킨 DDoS 공격으로 게임 관련 웹사이트 장애가 발생하기도 했다. 2016년에는 미라이에 의해 9월과 10월 대규모 DDoS 공격이 발생한다. 공격에는 기존 인터넷 공유기뿐 아니라 DVR(Digital Video Recorder), IP 카메라 등의 사물인터넷 기기가 이용되었다.



[그림 1] 주요 임베디드 리눅스 악성코드 타임라인

이 가운데 특정 기기만 감염시키는 악성코드나 지속적으로 변형이 나오지 않는 악성코드를 제외하고 많이 발견되고 있는 악성코드는 에이드라, 달로즈, 가프지트, 피엔스캔, 미라이 등이다. 이들 5 종류 악성코드 발견 현황을 보면 2012년 36개, 2013년 26개, 2014년 348개, 2015년 1,180개, 2016년 9,125개다. 참고로 2016년 통계는 10월 31일까지의 집계로, 연말까지 1만 개 이상의 악성코드가 보고될 것으로 예상된다. 이처럼 임베디드 리눅스 기반 악성코드는 2014년 이후 폭발적인 증가세를 보이고 있다.

	Aidra	Darlloz	Gafgyt	Mirai	Pnscan	Total
2012	36	-	-	-	-	36
2013	19	7	-	-	-	26
2014	98	28	222	-	-	348
2015	87	9	980	-	104	1,180
2016	269	7	8,635	138	76	9,125
Total	509	51	9,837	138	180	10,715

현재 가프지트가 가장 많이 발견되고 있으며, 당분간 가프지트와 미라이가 계속 증가할 것으로 예상된다. 다섯 종류의 악성코드에 대해 간단히 살펴보자.

■ 에이드라(Aidra, Lightaidra)

에이드라는 2012년 2월 최초 발견되었으며 2011년 말 제작되었을 가능성이 높다. 최초의 사물인터넷 악성코드로 볼 수 있다. 기존 임베디드 리눅스 악성코드가 밍스 프로세스를 사용하는 인터넷 공유기만 공격 대상이었다면, 이 악성코드는 밍스 뿐 아니라 암(ARM), 밍셀(MIPSel), 파워PC(PowerPC), 슈퍼H(SuperH) 등의 다양한 프로세스에서도 동작하게 제작되었다. IRC 봇 악성코드로 DDoS 공격 기능을 가지고 있으며 소스코드가 공개되어 다양한 변형이 존재한다. 2014년 발견된 변형에는 경쟁 악성코드인 달로즈 제거 기능이 추가되었다.

■ 달로즈(Darolloz, Zolland)

달로즈는 2013년 10월 발견된 사물 인터넷 월드로 인텔 x86, 밍스, 암, 파워PC 등의 시스템을 감염시킬 수 있다. 다른 악성코드가 주로 DDoS 공격 기능이 있는데 반해 이 악성코드는 비트코인 같은 가상화폐 채굴 기능을 가지고 있다.

■ 가프지트(Gafgyt)

가프지트는 2014년 8월에 존재가 처음 확인되었다. 특히 2014년 말 리자드 스쿼드가 엑스박스 라이브(Xbox Live)와 플레이스테이션 네트워크(PlayStation Network)에 DDoS 공격을 할 때 이용하면서 유명해졌다. 2015년 1월 소스코드가 공개되어 현재 가장 많은 변형이 존재한다.

■ 미라이(Mirai)

미라는 ‘미래’라는 뜻의 일본어로, 2016년 5월 처음 발견되었다. 2016년 10월 초 소스코드가 공개된 후 변형이 증가하고 있다. 2016년 9월 보안 블로그에 기록적인 DDoS 공격과 2016년 10월 호스팅 업체 딘에 대한 DDoS 공격으로 유명해졌다. 미라는 UDP Flood, Syn Flood, ACK Flood, GRE IP Flood 등의 다양한 DDoS 공격 기능을 가지고 있다. 또한 2016년 10월 발견된 변형은 다른 악성코드인 달로즈를 제거하는 기능이 포함되었다.

■ 피엔스캔(Pnscan)

피엔스캔은 2015년 8월 러시아 보안업체 닥터웹(Dr. Web)에

서 발견된 악성코드이다. 암, 밍스, 파워PC 시스템을 감염시키며 HNAP(Home Network Administration Protocol)와 CVE-2013-2678 등의 취약점을 공격한다.

현재까지 임베이드 리눅스 기반 시물인터넷 제품에 감염된 악성코드를 진단·치료할 수 있는 마땅한 방법은 없다. 백신 프로그램이 존재하지 않고 백신 프로그램이 존재해도 제조사 도움이 없으면 프로그램 설치도 어렵다. 따라서 악성코드 감염을 예방하기 위한 노력이 필요하다. 우선 인터넷 공유기나 NAS의 공장 초기화 암호는 반드시 변경해야 한다. 새로운 암호는 숫자와 특수 문자를 섞어서 사용하고 주기적으로 변경하면 가장 좋다. 악성코드에서 Admin, adin1, guest, root, support 등의 계정에 대입해 보는 주요 비밀번호는 다음과 같다([표 2] [그림 2] 참고).

54321	666666	7ujMko0vizxv	7ujMko0admin	00000000
1111	1111111	1234	12345	123456
888888	Admin	Admin1234	anko	Default
dreambox	fucker	ikwb	hi3518	jvbzd
klv123	klv1234	meinsm	Pass	password
realtek	service	system	tech	ubnt
user	vizxv	xc3511	Zte521	Zlxx

[그림 2] 미래 악성코드에 포함된 패스워드 문자열 비교

공격자는 최근 인터넷 공유기 등의 취약점을 찾아 계속 공격하고 있어 제조사에서도 주기적으로 펌웨어 업데이트를 제공하고 있다. 사물인터넷에 대한 다른 취약점 공격도 진행될 것으로 예상되어 인터넷에 연결된 기기는 최신 펌웨어로 업데이트해야 한다. 많은 경우 외부에서 접근할 수 있는 기능을 약용하고 있다. 따라서 꼭 필요한 경우가 아니라면 외부 접근 기능을 해제하고 사용해야 한다.

2014년 이후 임베디드 리눅스 악성코드에 의해 발생한 DDoS 공격으로 세계 여러 나라 정부에서도 문제의 심각성을 느끼기 시작했다. 이러한 기조에 따라 미래창조과학부는 2016년 9월 IoT 기기 생명주기를 기준으로 15가지 보안 요구사항과 기술·관리적 권고사항을 상세히 담은 ‘IoT 공통 보안 가이드’를 발표했다. 따라서 사물인터넷 기기 제조사는 이 가이드를 비롯해 KR-CERT의 ‘공유기 제품 생산 시 적용할 보안 가이드’, OWASP의 ‘IoT 시큐리티 가이드’를 바탕으로 제품을 설계해야 한다.

또한 보안 업체와 협력해 보안 기능을 강화하거나 보안 제품을 탑재할 필요가 있다. 언론을 통한 사물인터넷의 위험성 홍보도 필요하다. 개인과 기업도 사물인터넷 제품을 구매할 때 가격보다 신뢰할 수 있는 제조사에서 보안에 신경 써서 만든 제품을 선택하면 시장 전체적으로 자연스럽게 보안문제에 좀 더 주의를 기울일 것으로 보인다.

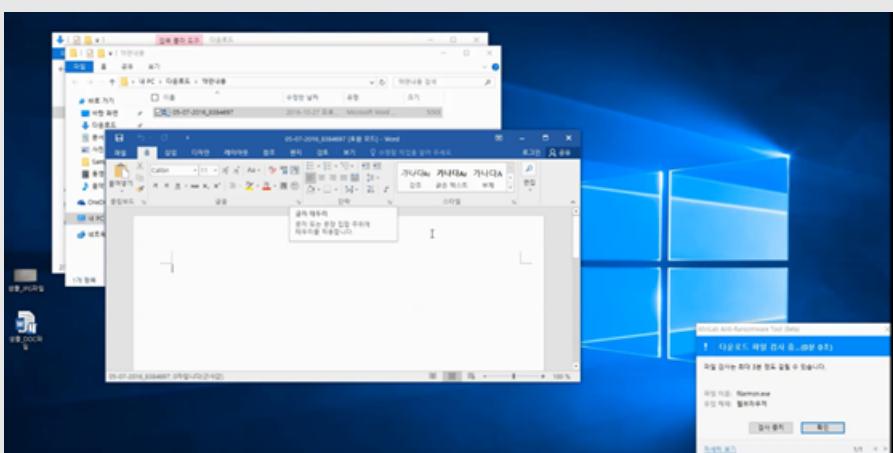
안티랜섬웨어 툴, 탐지 범위 넓히고 삭제 기능 더하고

안랩 안티랜섬웨어 툴 베타버전(AhnLab Anti-Ransomware Tool, 이하 안티랜섬웨어 툴)이 더욱 강력해졌다.

지난 2016년 7월 4일 첫 베타버전이 공개된 안티랜섬웨어 툴은 랜섬웨어 탐지를 위해 가상화 격리 진단이라는 새로운 기술을 적용한 솔루션이다. 출시 이후 사용자들의 의견을 반영하여 성능을 강화하고 안정화를 위한 업그레이드를 지속적으로 진행해왔다. 이러한 과정의 일환으로 지난 10월 31일 이메일 탐지 범위를 확대했으며, 파일 삭제 기능까지 추가했다.

이메일 탐지 범위 확대

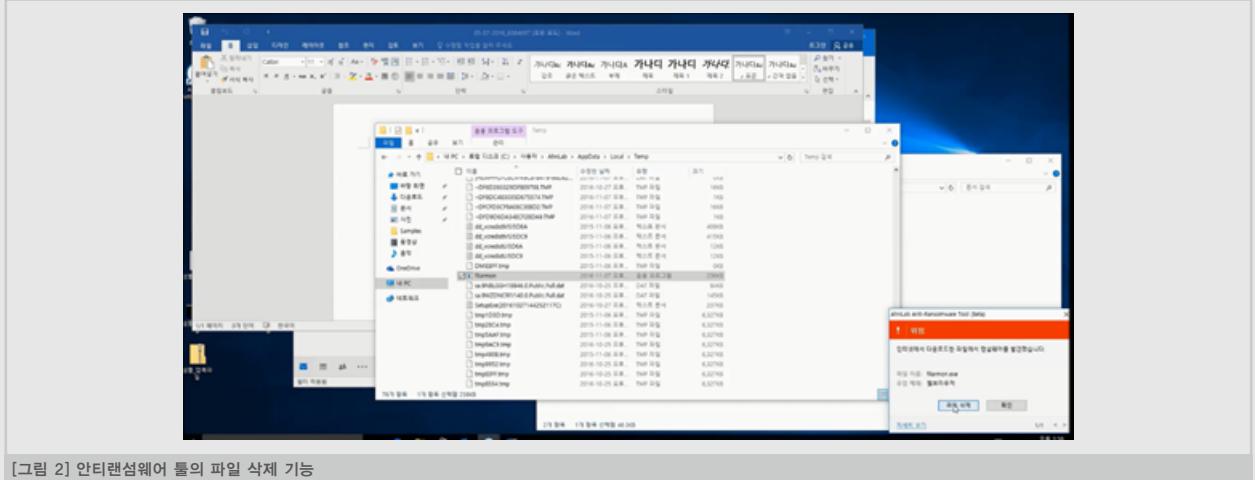
랜섬웨어를 비롯한 악성코드의 유입 경로 중 가장 많은 부분을 차지하는 것은 역시 웹 브라우저와 이메일. 안티랜섬웨어는 기존 버전에서는 웹 브라우저를 대상으로 유입되는 파일(웹 메일 포함)들을 감시했다. 이번 업그레이드에서는 웹 브라우저뿐만 아니라 마이크로소프트(Microsoft, MS) 오피스와 이메일 클라이언트까지 지원 대상에 추가되었다. 안티랜섬웨어 툴이 현재 지원하는 이메일 클라이언트는 아웃룩(Outlook), 아웃룩 익스프레스(Outlook Express), 썬더버드(Thunderbird)다. 이로써 안티랜섬웨어 툴은 웹 브라우저를 이용하는 웹 메일과 이메일 클라이언트를 이용하는 메일 영역까지 안전하게 보호할 수 있게 됐다.



[그림 1] 아웃룩으로부터 유입된 파일 검사

파일 삭제 기능 추가

이번 업그레이드를 통해 앤티랜섬웨어 룰은 랜섬웨어나 악성코드가 발견되면 바로 삭제할 수 있는 기능을 추가했다.



[그림 2] 안티랜섬웨어 툴의 파일 삭제 기능

이 기능은 윈도우(Windows) 휴지통과 연동되는 기능으로 ‘삭제하기’ 버튼 클릭 시 휴지통으로 바로 이동한다. 만약 사용자가 복원을 원하면 휴지통에서 복원할 수도 있다.

현재 베타버전으로 제공되는 안랩 앤티랜섬웨어 룰은 안랩 홈페이지에서 개인, 기업 구분 없이 누구나 무료로 다운로드할 수 있다.

애드윈드 악성코드의 역습

애드윈드(Adwind)는 자바(Java)로 작성된 RAT(Remote Administration Tool)로, 윈도우(Windows)뿐만 아니라 리눅스, 안드로이드 운영체제에서도 동작하는 악성코드다. 최근 애드윈드 악성코드가 백신 프로그램(Anti-virus, AV)의 진단을 회피하는 우회 기법을 탑재하고, 유포 방식 또한 기존의 JAR 파일 형식 외에 워드(Word), PPT 파일 내부에 첨부된 형태 등 화려한(?) 복귀를 꾀하고 있다. 특히 애드윈드 악성코드가 사용자 PC에 유입된 이후 랜섬웨어 등의 악성코드 추가 감염을 유발하는 사례도 발견됐다. 이 글에서는 최신 애드윈드 악성코드 변종을 이용한 공격 사례와 감염 방식을 상세히 살펴본다.

애드윈드류의 악성코드는 지난 2012년에 제작 및 유포된 이후 언리콤(Unrecom), 제이소켓(JSocket), 에일리언스파이(AlienSpy) 등의 변종으로 파생되었다. 2014년 이후 범람하던 애드윈드 3.0(Adwind RAT v3.0)은 2015년 8월을 기점으로 개발 및 서비스가 종료되면서 추가적인 기능 업데이트는 나타나지 않았다. 이후 애드윈드 3.0은 크랙(Crack) 버전으로 생성되는 것이 대다수였으며, 대부분의 백신에서 진단됨에 따라 배포 수가 급격히 감소한 바 있다.

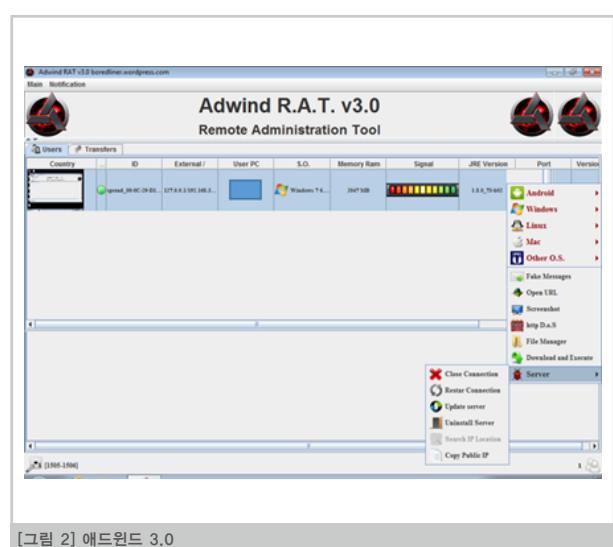


그런데 최근 백신의 진단 우회를 시도하는 애드윈드 변종들이 증가하고 있다. 감염 방식 또한 직접 JAR 파일을 배포하는 방식보다는 주로 OLE에 첨부하여 감염을 유발하는 사례들이 나타나고 있다.

애드윈드 3.0 변종

기존의 애드윈드 3.0 크랙의 경우 Allatori 난독화(Allatori Java obfuscator)되어 있었으나 최근에는 ZKM 난독화된 파일들이 자속적

으로 유포되고 있다. 자바 난독화 부분이 변경되면서 자바 코드 실행을 위해 참조하는 상수 풀(Constant Pool)과 자바 코드가 변경된 것을 확인할 수 있다. 악성코드 제작자의 빌더 소스코드가 유출되어 새로운 형태의 빌더가 제작되었거나, 공격자에 의해 난독화 부분이 변경된 것으로 추정된다.

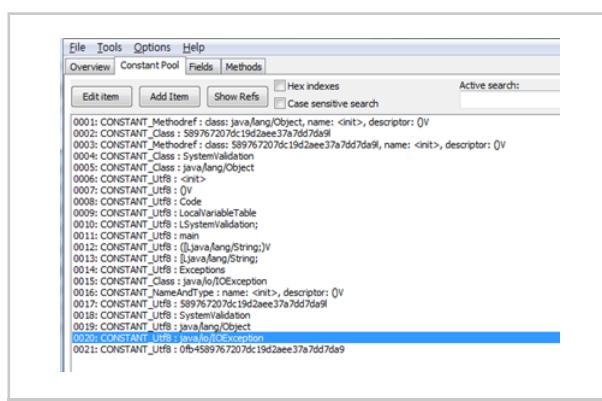


[그림 3], [그림 4], [그림 5]는 각각 애드원드 원형과 변종의 메인 상수 풀(Main-Class Constant Pool)이다(발견 시기 기준).

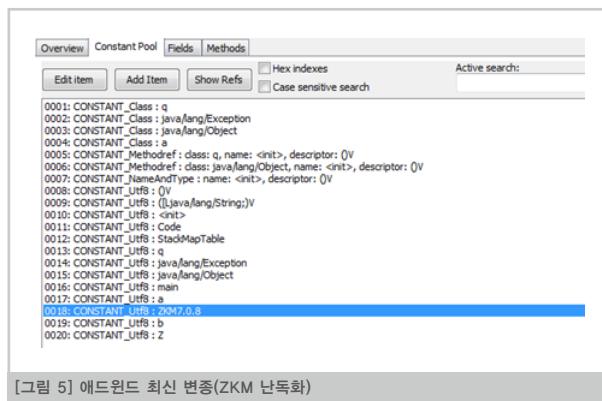
- 애드윈드 3.0 원형 - Allatori
 - 진단 우회를 위한 애드윈드 변형[Allatori] - 문자열 난독화, 클래스[Class] 쪼개기 등
 - 난독화 부분[Obfuscate]이 변경된 애드윈드 - ZKM

Edit item	Add Item	Show Refs	<input checked="" type="checkbox"/> Hex indexes	Active search:	Object filter
			<input type="checkbox"/> Case sensitive search	All Items	
0236: CONSTANT Methodref 1 class: load/ClassLoader, name: ALLATORI_0_DEMO, descriptor: ([Ljava/lang/String;)Ljava/lang/String;					
0237: CONSTANT Uri#L_CACSD;					
0238: CONSTANT Uri#L_CACSD;					
0239: CONSTANT Uri#L_CACSD;					
0240: CONSTANT Uri#L_CACSD;					
0241: CONSTANT Uri#L_JAR!L\$y6YQH1Z,C;					
0242: CONSTANT String: /\$y6YQH1Z,C;					
0243: CONSTANT Uri#L_JAR!L\$y6YQH1Z,C;					
0244: CONSTANT String: /\$y6YQH1Z,C/\$y6YQH1Z,C;					
0245: CONSTANT Uri#L_JAR!L\$y6YQH1Z,C/\$y6YQH1Z,C;					
0246: CONSTANT Uri#L_JAR!L\$y6YQH1Z,C/\$y6YQH1Z,C;					
0247: CONSTANT String: /;					
0248: CONSTANT String: /;					
0249: CONSTANT String: /AAA\$6;					
0250: CONSTANT String: /AAA\$6;					
0251: CONSTANT Uri#L_d;					
0252: CONSTANT Uri#L_d;					
0253: CONSTANT Uri#L_meet;					
0254: CONSTANT Uri#L([Ljava/lang/String;)Ljava/lang/StringBuilder;					
0255: CONSTANT Uri#L([Ljava/lang/String;)Ljava/lang/StringBuilder;					
0256: CONSTANT Methodref 2 class: java/lang/StringBuilder, name: insert, descriptor: ([Ljava/lang/String;)Ljava/lang/StringBuilder;					
0257: CONSTANT Uri#L_ALLATORI_0_DEMO;					
0258: CONSTANT Uri#L_g;					
0259: CONSTANT Uri#L_g;					
0260: CONSTANT Uri#L_f;					
0261: CONSTANT Uri#L_f;					
0262: CONSTANT NameAndType# name: ALLATORI_0_DEMO, descriptor: ([Ljava/lang/String;)Ljava/lang/String;					
0263: CONSTANT NameAndType# name: L, descriptor: [Ljava/util/HashMap;					
0264: CONSTANT NameAndType# name: L, descriptor: [Ljava/util/HashMap;					
0265: CONSTANT NameAndType# name: L, descriptor: [Ljava/util/HashMap;					
0266: CONSTANT NameAndType# name: ALLATORI_0_DEMO, descriptor: [Ljava/lang/String;					

[그림 3] 애드원드 3.0 기본 원형



[그림 4] 백신 진단 우회를 위해 클래스 분할

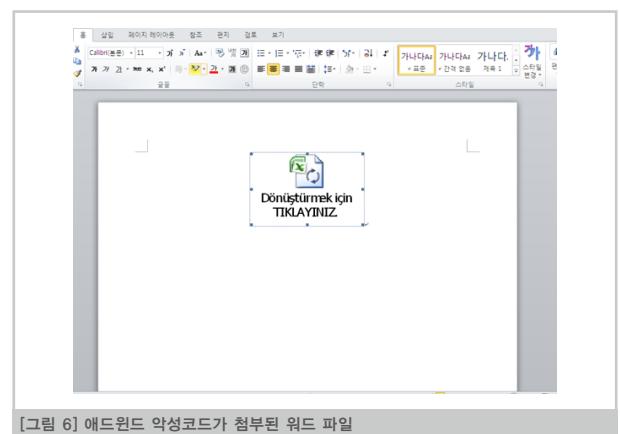


[그림 5] 애드원드 최신 변종(ZKM 난독화)

이메일 첨부 파일 종류별 유포 사례

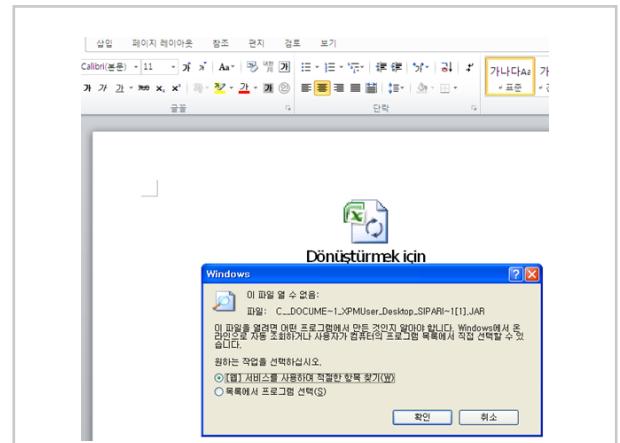
1. 워드 파일

악성코드 제작자는 워드 파일에 애드원드 악성코드를 첨부한 후 이메일로 전송했다. 사용자가 이메일에 첨부된 워드 파일을 열면 [그림 6-1]과 같이 엑셀 아이콘을 가진 문서가 나타난다. 이때 사용자가 별다른 의심없이 이 엑셀 아이콘을 더블 클릭하면 애드원드 악성코드에 감염된다. 즉, 실제 첨부된 파일은 엑셀 파일이 아닌 엑셀 아이콘으로 우주작하고 인더 애드원드 악성코드로 확장자는 '.jar'이다.



[그림 6] 애드윈드 악성코드가 첨부된 워드 파일

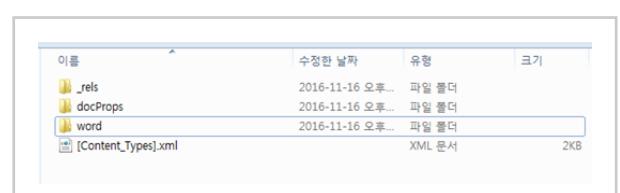
[그림 6]의 엑셀 아이콘을 더블 클릭하면 애드윈드 악성코드가 특정 경로에 생성 및 실행된다. 해당 경로는 제작자가 미리 지정해둔 것이다. 감염 과정이 정상적으로 이뤄지고 나면 공격자는 사용자 PC를 장악할 수 있다.



[그림 7] 엔셀 아이콘 더블 클릭 시 나타나는 환면

OLE 파일의 내부 엔트리(Entry)를 확인해보면, 아래와 같은 경로에 애드윈드 악성코드가 삽입되어 존재한다.

\Word\embeddings\oleObject1 Directory



[그림 8] 워드 루트 디렉터리(WORD ROOT DIRECTORY)



[그림 9]의 oleObject1.bin은 PK 형식을 가진 OLE 객체이며, 내부 엔트리 중 [1]ole10Native에 애드워드를 포함하고 있다

이름	수정한 날짜	유형	크기
[1]Ole10Native~	2016-11-16 오후...	파일 폴더	
[1]CompObj		파일	1KB
[1]Ole		파일	1KB
[1]Ole10Native		파일	67KB
[3]ObjInfo		파일	1KB

[그림 10] 애드윈드를 포함하고 있는 [1]ole10Native

이름	수정한 날짜	유형	크기
[ID]	2016-11-12 오후...	파일	1KB
p.class	2016-11-12 오후...	CLASS 파일	4KB
s	2016-11-12 오후...	파일	59KB
Ujls.class	2016-11-12 오후...	CLASS 파일	6KB

[그림 11] 애드윈드 'ROOT\LOAD DIRECTORY' 클래스 및 복호화 파일

000000 3f 09 01 00 02 00 73 69 70 61 72 69 73 6c 65 72siparisler
000010 2e 6a 61 72 00 43 3a 5c 44 4f 43 55 4d 45 7e 31	.jar C:\DOCUME~1
000020 5c 58 50 4d 55 73 65 72 5c 44 65 73 6b 74 6f 70	\XPMUser\Desktop
000030 03 00 29 00 00 43 2a 5c 44 4f 43 55 4d 45 7e 31	\SIPARI~1\JAR\
000040 31 5c 58 50 4d 55 73 65 72 5c 44 65 73 6b 74 6f	PK.....
000050 70 5c 53 49 50 41 52 49 72 31 2e 4a 41 52 00 ce	p\SIPARI~1 JAR I
000060 08 01 00 50 4b 03 04 14 00 08 08 08 00 72 94 6c	I.....
000070 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK.....
000080 4d 56 54 49 50 41 52 49 72 31 2e 4a 41 52 00 ce	PK.....
000090 00 00 00 02 00 00 00 00 00 00 00 00 50 4b 03 04	PK.....
0000a0 14 00 08 08 00 00 72 94 49 00 00 00 00 00 00 00	PK.....
0000b0 00 00 00 00 00 00 4d 45 54 41 2d 49	META-I
0000c0 4e 46 2f 4d 41 4e 49 46 45 53 54 2e 4d 46 4d 8d	META-I
0000d0	NF\MANIFEST.MF.....

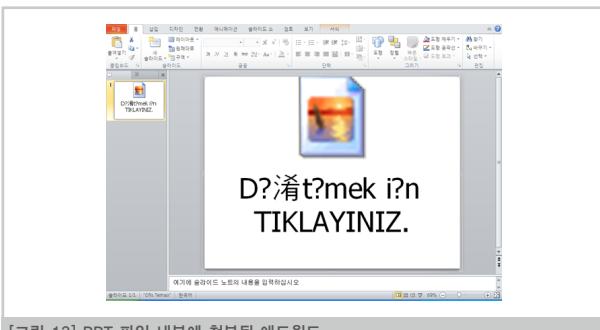
[그림 12] [1]ole10Native 파일 바이너리(BINARY)

[1]ole10Native 내부에는 아래와 같이 애드윈드가 생성 및 실행될 위치가 명시되어 있다.

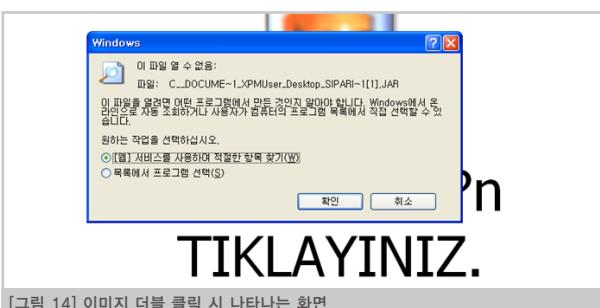
- 생성되는 Jar 파일: siparisler.jar
- 생성되는 Jar 경로: c:\Docume~1\xpmuser\desktop\siparisler.jar

2. PPT 파일

사용자가 이메일에 첨부된 PPT 파일을 열면 특정한 페이지(슬라이드)에 [그림 13]과 같이 그림 파일로 위장한 아이콘이 나타난다. 앞선 사례와 마찬가지로 사용자가 이미지 확인을 위해 해당 아이콘을 더블 클릭하면 첨부되어 있던 애드윈드(*.Jar)가 특정한 경로에 생성 및 실행된다.



[그림 13] PPT 파일 내부에 첨부된 애드윈드



[그림 14] 이미지 더블 클릭 시 나타나는 화면

이때 애드윈드는 앞선 사례와 유사한 위치에 존재하고 있다. 루트 디렉터리는 [그림 15]와 같으며, 첨부된 애드윈드는 아래 경로에 존재한다.

ppt\embeddings\oleObject1\[1]ole10Native

이름	수정한 날짜	유형	크기
[rels]	2016-11-16 오후...	파일 폴더	
docProps	2016-11-16 오후...	파일 폴더	
ppt	2016-11-16 오후...	파일 폴더	
[Content_Types].xml		XML 문서	

[그림 15] PPT 루트 디렉터리

이름	수정한 날짜	유형	크기
oleObject1	2016-11-16 오후...	파일 폴더	
oleObject1.bin		BIN 파일	

[그림 16] ROOT\PPT\EMBEDDINGS

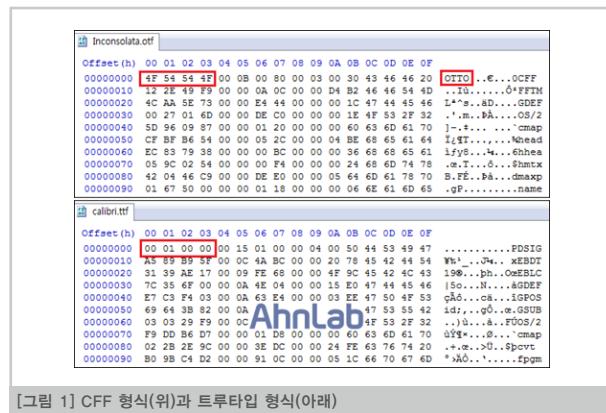
[그림 16]의 oleObject1.bin은 PK 형식을 가진 OLE 객체이며, 내부 엔트리 중 [1]ole10Native0|| 애드윈드를 포함하고 있다.

3 58 01 00 02 00 73 69 70 61 72 69 73 6c 65 72siparisler
2e 6a 61 72 00 43 3a 5c 44 4f 43 55 4d 45 7e 31	.jar C:\DOCUME~1
5c 58 50 4d 55 73 65 72 5c 44 65 73 6b 74 6f 70	\XPMUser\Desktop
5c 53 49 50 41 52 49 72 31 2e 4a 41 52 00 ce	\SIPARI~1\JAR\
03 00 29 00 00 00 43 3a 5c 44 4f 43 55 4d 45 7e 31	I.....
31 5c 58 50 4d 55 73 65 72 5c 44 65 73 6b 74 6f	PK.....
70 5c 53 49 50 41 52 49 72 31 2e 4a 41 52 00 ce	p\SIPARI~1 JAR\
57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK.....
59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK.....
00 60 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 62 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 63 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 64 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 65 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 66 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 67 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 68 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 69 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 6a 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 6b 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 6c 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 6d 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 6e 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 6f 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 70 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 71 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 72 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 73 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 74 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 75 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 76 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 77 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 78 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 79 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 7a 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 7b 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 7c 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 7d 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 7e 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 7f 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 80 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 81 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 82 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 83 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 84 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 85 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 86 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 87 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 88 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 89 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 8a 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 8b 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 8c 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 8d 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 8e 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 8f 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 90 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 91 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 92 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 93 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 94 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 95 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 96 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 97 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 98 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 99 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 9a 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 9b 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 9c 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 9d 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 9e 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 9f 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a0 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a1 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a2 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a3 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a4 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a5 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a6 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a7 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a8 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 a9 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 aa 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 ab 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 ac 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 ad 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 ae 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 af 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b0 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b1 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b2 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b3 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b4 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b5 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b6 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b7 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b8 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 b9 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 ba 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 bb 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 bc 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 bd 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 be 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 bf 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c0 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c1 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c2 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c3 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c4 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c5 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c6 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c7 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c8 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 c9 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 ca 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 cb 61 64 2e 4d 41 4e 49 46 45 53 54 2e 4d 46	META-I
00 cc 61 6	

오픈타입 폰트 취약점을 악용한 공격 주의!

지난 11월 8일, 마이크로소프트(Microsoft)는 오픈타입(OpenType) 폰트(font) 취약점과 관련된 보안 패치를 배포했다. 오픈타입 폰트는 마이크로소프트와 어도비(Adobe)가 함께 개발한 폰트 형식으로, 폰트 구조로 인해 발생한 취약점이 공격의 통로가 될 수 있는 것으로 확인됐다. 오픈타입 폰트에서 취약점이 발생하게 되는 구체적인 과정과 피해 예방을 위한 방법을 살펴보자.

오픈타입 폰트는 ‘*.otf’ 또는 ‘*.ttf’ 형태를 갖는다. 폰트 모양을 결정하는 데이터가 CFF(Compact Font Format) 형식인지 트루타입(TrueType) 형식인지에 따라 폰트 파일의 시작 부분 첫 4 바이트 값이 달라지는데, [그림 1]과 같이 CFF 형식의 오픈타입 폰트는 0x4F54544F('OTTO'), 트루타입 형식의 오픈타입 폰트는 0x000010000의 값을 가진다.

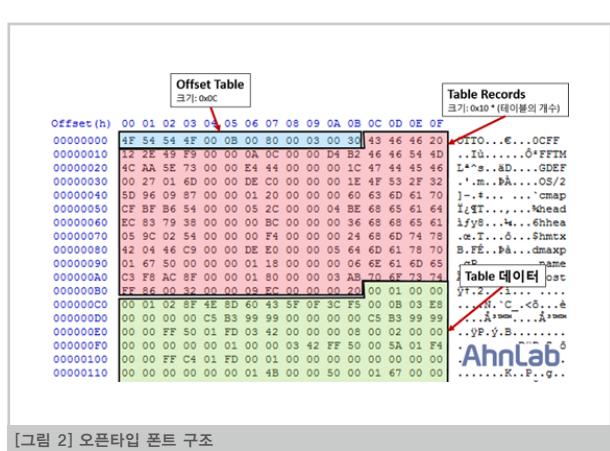


이번에 취약점이 발견된 폰트의 경우, 파일의 첫 4 바이트 값이 ‘OTTO’로 시작되는 CFF 형식의 오픈타입 폰트였다.

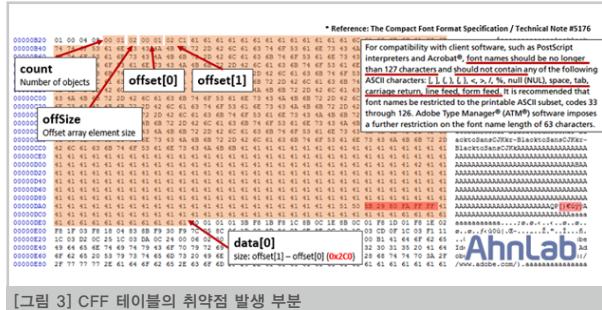
오픈타입 폰트가 어떻게 구성되어 있는지 살펴보자. 오픈타입 폰트는 기본적으로 [그림 2]와 같이 오프셋 테이블(Offset Table)과 테이블 레코드(Table Records)로 구성된다.

코드(Table Record) 및 다수의 테이블 데이터로 구성된다. 오프셋 테이블(크기: 0x0C)에는 폰트의 종류 및 테이블의 개수 정보가 존재한다. 또한, 각 테이블마다 테이블 레코드(크기: 0x10)가 존재하고, 테이블 레코드에는 테이블의 이름, 크기, 시작 위치, 체크섬이 표기되어 있다.

테이블 레코드에 표기된 위치를 따라가면 각각의 테이블 데이터가 존재하는데, 8개의 필수 테이블인 cmap, head, hhea, hmtx, maxp, name, OS/2, post와 더불어 해당 오픈타입 폰트의 종류에 따라 추가 테이블이 존재한다. CFF 형식인 경우에는 CFF, CFF2, VORG 등의 테이블이, 트루타입 형식인 경우에는 cvt, fpgm, glyf, loca 등의 테이블이 추가된다.



취약점이 발견된 폰트는 CFF 형식의 오픈타입 폰트이기 때문에 내부에 CFF 형식의 데이터를 포함하고 있으며, CFF라는 이름의 테이블이 존재한다. 그런데 이 테이블 내부에 어도비에서 정의한 스펙(ADOBTECHNICAL NOTE #5176)을 따르지 않는 구조가 발견되었으며, 이로 인해 취약점이 발생하고 공격자가 임의의 코드를 실행할 수 있는 것으로 확인됐다.



[그림 3] CFF 테이블의 취약점 발생 부분

구체적으로 살펴보면, 4 바이트 크기의 파일 시작 부분(0x010000403) 이후에 네임 인덱스(Name Index)가 등장하는데, 어도비 스펙상 네임 인덱스의 폰트명 길이는 127 바이트 이하여야 정상이다. 하지만 [그림 3]에서 네임 인덱스의 폰트명 크기가 127 바이트를 초과한 0X2C0으로, 어도비 스펙을 따르지 않고 있다.

폰트 파일을 처리하는 윈도우(Windows) 내부 모듈인 ATMFD.DLL에서는 이와 관련하여 폰트명이 127 바이트 이하인지 아닌지 여부를 확인하는 경계 체크 부분이 존재하지 않는 것으로 파악됐다. 이로 인해 해당 영역의 데이터를 복사할 때 초과되는 범위의 데이터까지 함께 복사되는데, 초과된 범위의 데이터가 공격자에 의해 추가된 악성 코드일 수 있는 것이다.

오픈타입 폰트 취약점으로 인한 피해를 예방하기 위해 윈도우(Windows)를 사용하는 모든 사용자는 마이크로소프트에서 배포한 보안 패치(MS16-132, CVE-2016-7256)를 다음 경로에서 다운로드하여 적용할 것을 권장한다.

<https://technet.microsoft.com/ko-kr/library/security/mt674627.aspx>

[표 1] 마이크로소프트 보안 패치 경로

또한 외부로부터 전달된 의심스러운 형태의 폰트 파일(*.otf)이나 문서 파일에 대해서는 가급적 실행하지 않는 것이 좋다.

V3 제품에서는 해당 폰트 취약점 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

〈V3 제품군의 진단명〉

OTF/Cve-2016-7256 (2016.10.29.00)

참고 자료

Microsoft 보안공지 MS16-132: <https://technet.microsoft.com/ko-kr/library/security/ms16-132.aspx>

CVE-2016-7256: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7256>

OpenType Font Specification: <https://www.microsoft.com/typography/otspec/otff.htm>

Compact Font Format Specification: <https://partners.adobe.com/public/developer/en/font/5176.CFF.pdf>

핀테크의 오늘과 내일

한국은행이 최근 발표한 '2016년 3분기 국내 인터넷뱅킹 서비스 이용 현황'을 보면 지난 7~9월 스마트폰뱅킹 이용건수는 하루 평균 5,379만 7천 건으로 집계됐다. 작년 11월 1일 기준 한국 인구가 5,106만 9천명(통계청 인구주택총조사)이라는 점을 고려할 때, 국민 1명이 하루 평균 한 차례 이상 스마트폰뱅킹을 이용한다는 얘기다. 이제 현금의 필요성이 사라지고 있다고 해도 과언이 아닐 만큼 빠르고 간편한 핀테크 시대로 접어든 것이다. 하지만 핀테크가 활성화되기 위해서는 여전히 해결해야 할 과제가 산적해 있다.

핀테크(FinTech)는 '금융(Financial)'과 '기술(Technology)'이 융합된 용어이다. 기존에도 '인터넷뱅킹'이나 '모바일뱅킹' 등의 비슷한 기술이 있었는데, 왜 굳이 핀테크라는 용어를 쓰는 걸까. 인터넷뱅킹이나 모바일뱅킹이 '협의의 기술'이라고 한다면 핀테크는 단순히 결제 서비스가 아닌 송금, 개인 자산관리, 크라우드 펀딩 등 각종 금융 서비스를 아우르는 '광의의 기술'을 의미한다.

핀테크는 뛰어난 접근성과 저비용, 부가가치 창출을 특징으로 한다. IT(Information Technology)나 BT(Bio Technology)보다 확산 속도가 빠르며 인터넷 기반으로 모든 서비스가 제공되기 때문에 투자 비용이 적게 들고 인건비도 절약된다. 또한 빅데이터 수집과 분석으로 새로운 부가 가치 창출이 가능하다는 점이 특징이다.

핀테크 서비스의 특징과 한계

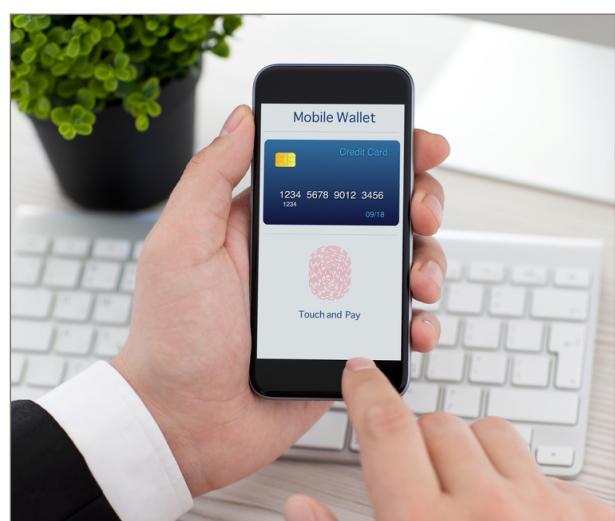
현재 핀테크 서비스는 크게 5가지로 분류된다.

첫째, 결제, 송금, 외환 서비스를 제공하는 '결제·송금 서비스'다. 우리나라의 카카오페이지나 삼성페이, 미국의 페이팔, 중국의 알리페이 등이 대표적이다.

둘째, 은행 전체 업무를 24시간 온라인으로 수행하는 '비대면 금융서비스인 인터넷 전문은행'이다. 우리나라의 카카오뱅크나 K뱅크, 중국의 위어바오 등이 여기에 해당된다.

셋째, 대출이나 투자, 후원 등을 개인과 개인을 연결해 투자를 수행하는 '크라우드 펀딩(Crowd Funding)'이다. 국내의 경우 와이즈나 텁블벅, 미국의 킥스타터나 랜딩클럽 등이 활동 중이다.

넷째, 자산관리 서비스나 세무 서비스, 로보 어드바이저(Robo-Advisor) 서비스와 같은 '금융데이터 분석'이다. 국내에서는 뱅크샐러



드, 미국은 웰스프론트, 민트 등이 대표적이다.

마지막으로 비트코인 결제 서비스나 가상화폐 서비스인 ‘디지털 화폐’다. 세계적으로 비트코인이 가장 유명하며, 국내에는 코빗(Korbit)이라는 디지털 화폐도 있다.

이와 같은 5가지의 핀테크 서비스 가운데 모바일 지급결제 수단으로서의 핀테크가 가장 활발하다. 핀테크의 전통적 강자인 페이팔을 중심으로 애플과 구글 등이 각축전을 벌이고 있는데 애플은 ‘애플페이’를, 구글은 ‘안드로이드페이’를 공개했다. 페이스북도 모바일 결제 시장에 진출했다. 중국 알리바바의 ‘알리페이’의 경우 8억 2천만 명의 회원 수를 자랑한다. 우리나라는 카카오페이를 시작으로 네이버의 라인페이, 삼성의 삼성페이 등이 시장에서 두각을 드러내고 있다.

그러나 국내 핀테크 산업은 여러 가지 규제로 인해 성장에 한계를 드러내고 있다. 미국의 경우 원칙적으로 허용하되 일부만 예외적으로 금지하는 네거티브(Negative) 규제 방식을 채택하고 있는 반면, 우리나라는 기본적으로 금지하고 일부만 예외적으로 허용해 풀어주는 포지티브(Positive) 규제 방식을 채택하고 있다는 점이 가장 큰 문제로 지적된다. 이에 따라 핀테크 분야에서 뛰어난 기술이나 아이디어를 보유하고 있어도 각종 규제로 인해 창업이 쉽지 않아 핀테크 산업의 발전이 더디다는 평가가 나오고 있다. 스마트폰으로 결제나 이체 등을 하면서도 여전히 뒷주머니엔 현금이 든 지갑을 가지고 다녀야 하는 게 현실이다.

보안 이슈 선결돼야…핀테크 활성화를 위한 대책은?

그렇다면 핀테크 산업을 활성화하기 위해 어떻게 해야 할까. 핀테크 전문가들은 기업 진입 규제를 완화하거나 기술 활용 제약 요인을 해소하는 등 국내의 포지티브 규제를 완화해야 한다고 주장한다. 그 일환으로 핀테크 산업의 창업과 성장 촉진, 국민 체감형 핀테크 서비스, 핀테크 인프라 구축 등을 통해 핀테크 산업을 활성화해야 한다고 말한다.

제도적인 규제 못지 않게 핀테크 활성화에 걸림돌이 되는 건 정보유출 및 보안 우려이다. 피싱이나 스미싱 같은 보안 사고가 잇따르면서 우리나라 국민들의 보안에 대한 신뢰도는 바닥 수준이다. 페이팔의 경우 198개국에 1억 4천만 명의 회원을 보유하면서 제1의 핀테크 기업으로 성공한 요인은 철저한 보안 덕분이다. 전세계 20개국에 500여명의 정보유출 방지 전담 인력과 전세계 17개 센터에 7,000여명의 보안 및 리스크 관리 인력을 배치하고 있다.

핀테크에서 보안의 중요성은 아무리 강조해도 지나치지 않다. 금융사고 발생 시 기업의 브랜드 가치는 물론 기업의 존폐 위기까지 발생한다. 인력 못지 않게 보안 인프라와 시스템에 대한 확충도 시급하다. 상대적으로 보안이 취약한 모바일이나 웹상에서 개인 금융정보의 유출 가능성 이 존재하고 기존 보안시스템을 피해 나가는 새로운 금융 사기 및 도용 사기 발생 가능성도 있다. 여기에 다양해지는 핀테크 서비스로 인해 오픈된 채널의 증가에 따른 관리 요소가 증가함에 따라 관리 요소 및 관리 비용의 증가가 발생될 수 있다는 점도 고려해야 한다.

보안 문제를 해결하기 위해서는 관리, 기술, 정책·제도적인 측면에서 다양한 대책을 강구해야 한다. 결제 전반의 기술에 대한 보안대책을 통합 수립하고 전사적 위험관리 전략과 함께 OTP, SMS, 보안 SW, 토큰 등 다양한 인증 수단을 확보함과 동시에 이를 활용해 안전한 거래를 유도해야 한다. 또한 제도적 측면에서 국제 수준에 부합하는 금융보안 인증제를 도입함은 물론 핀테크 투자를 저해하는 각종 규제를 개선해 나가야 한다.

과거의 ‘금융 IT’는 은행에서 IT를 도입하는 것이었다면 핀테크는 IT가 중심이 되어 금융을 융합하는 것으로 이해하면 된다. ‘헤게모니’가 은행에서 IT 기업으로 넘어간 것이다. 다시 말해 IT와 금융의 경계가 사라졌다고 해도 무방하다. 이제는 보다 ‘IT스러운’ 금융을 경험할 일만 남았다.

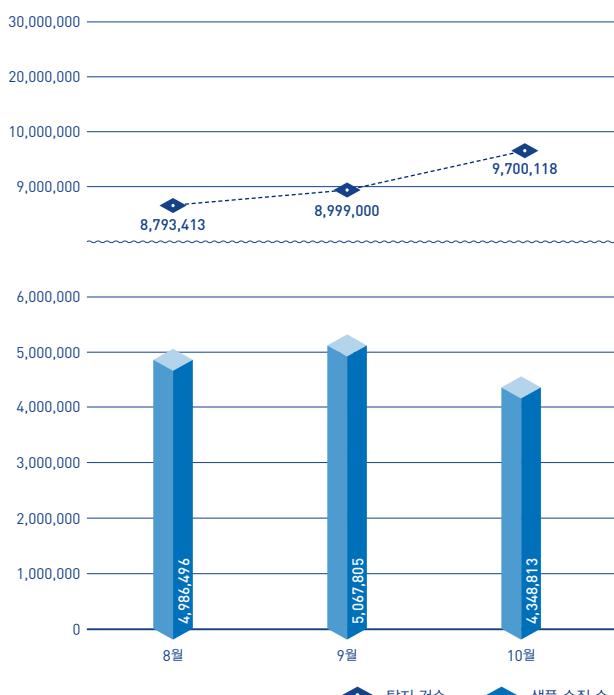
안랩, 10월 악성코드 통계 및 보안 이슈 발표

PC 부팅 방해하는 페트야(PETYA) 랜섬웨어 주의!

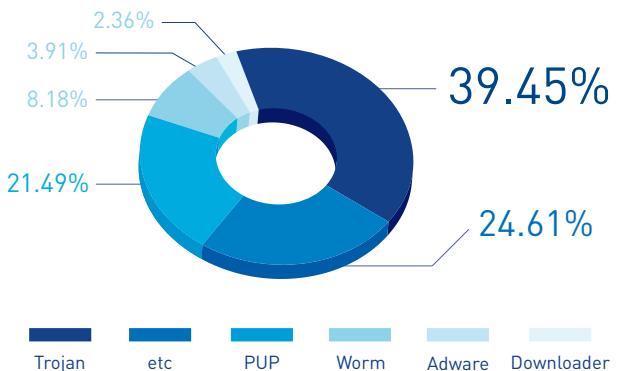
안랩 시큐리티대응센터(이하 ASEC)는 최근 ASEC Report Vol.82를 통해 지난 2016년 10월의 보안 통계 및 이슈를 전했다.

지난 10월의 주요 보안 이슈를 살펴본다.

ASEC이 집계한 바에 따르면, 2016년 10월 한 달간 탐지된 악성코드 수는 970만 118건으로 나타났다. 이는 899만 9,000건에 비해 70만 1,118건 증가한 수치다. 한편 10월에 수집된 악성코드 샘플 수는 434만 8,813건이다.



[그림 2]는 2016년 10월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 39.45%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 21.49%, 웜(Worm)이 8.18%의 비율로 그 뒤를 이었다.



지난 10월 한 달간 탐지된 모바일 악성코드는 39만 3,374건으로 집계됐다.



또한 지난 10월 악성코드 유포지로 도메인은 1,464개, URL은 3,294 개로 집계됐다. 10월의 악성 도메인 및 URL 차단 건수는 총 460만 5,999건이다.

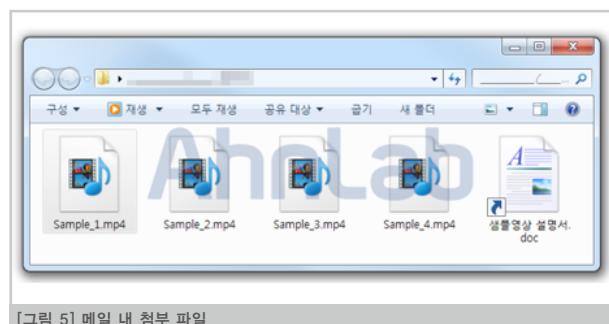


[그림 4] 악성코드 유포 도메인/URL 탐지 및 차단 건수 (2016년 8월~ 2016년 10월)

PC 부팅 방해하는 페트야(PETYA) 랜섬웨어 주의!

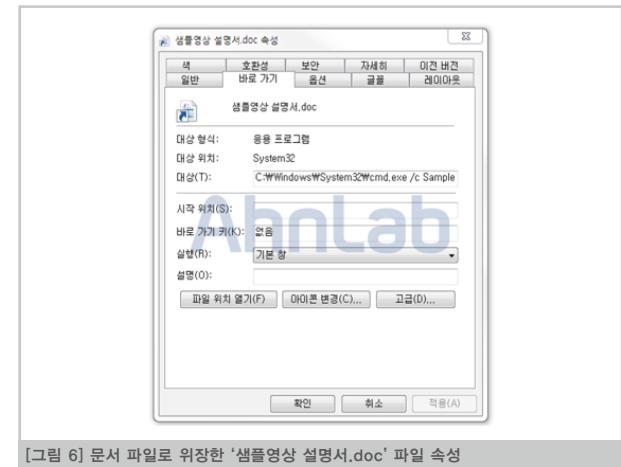
최근 사용자 PC의 정상적인 부팅을 불가능하게 만드는 페트야 랜섬웨어가 ‘스피어 피싱(Spear Phishing)’ 메일을 통해 유포됐다. 페트야 랜섬웨어는 파일을 암호화 대상으로 삼는 기존의 랜섬웨어와 달리 사용자 PC의 MBR(Master Boot Record) 영역 코드 자체를 변조하여, 감염된 이후에는 정상적인 PC 부팅을 불가능하게 하는 것으로 알려져 있다.

이번에 발견된 페트야 랜섬웨어를 유포한 해당 스피어 피싱 메일은 흥보 영상에 대한 의견을 구하는 내용의 메일로 위장하여 수신자가 첨부된 악성 파일을 열어보도록 유도한다. 메일의 첨부 파일을 압축 해제하면 [그림 5]와 같이 *.mp4 형태의 동영상 파일 4개와 *.doc 형태의 문서 파일 1개가 나타난다.



[그림 5] 메일 내 첨부 파일

[그림 6]과 같이 첨부 파일의 속성을 확인하면 ‘샘플영상 설명서.doc’ 파일이 실제로는 문서 파일로 위장한 LNK 형태의 바로가기 파일임을 알 수 있다. 명령 프롬프트를 이용하여 Sample_4.mp4 파일을 실행하도록 설정되어 있다. 마찬가지로 ‘Sample_4.mp4’ 파일 또한 영상 파일로 위장한 *.exe 형태의 실행 파일이다.



[그림 6] 문서 파일로 위장한 ‘샘플영상 설명서.doc’ 파일 속성

최종적으로 실행된 악성 파일은 메모리 내에 DLL 파일을 생성한다. 이 때 시스템 경로인 Program Files(x86) 및 Program Files 폴더의 내부를 탐색하여, 사용자 PC 내 백신 프로그램의 설치 여부도 함께 확인한다.

페트야 랜섬웨어에 감염되면 [그림 7]과 같은 부팅 불가 메시지 화면이 나타나며, MBR과 MFT(Master File Table) 영역을 암호화하여 PC의 정상적인 부팅을 불가능하게 한다. 또한 사용자에게 익명 통신 시스템인 토르 브라우저(Tor Browser)를 이용한 링크 접속을 통해 시스템 복구를 위한 금전을 지불할 것을 요구한다.



V3 제품에서는 페트야 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.DiskWriter (2016.10.04.08)

Trojan/Win32.Mischa (2016.10.06.07)

일단 랜섬웨어에 감염되어 파일이 암호화되면 거의 복구하기 어렵다. 따라서 다른 어떤 악성코드보다 랜섬웨어는 사전 예방이 중요하다. 랜섬웨어 피해 예방을 위해 평소 운영체제 및 주요 프로그램에 최신 보안 업데이트를 적용하고, 중요한 데이터는 주기적으로 백업을 해두는 것이 바람직하다.

안랩, ‘2016 ESG 우수기업’ 우수기업상 수상

안랩이 최근 한국거래소에서 열린 ‘2016 ESG 우수기업’ 시상식에서 ‘우수기업상’을 수상했다. 안랩은 지난해 최우수상 수상에 이어 올해는 우수기업상을 받았다.

‘2016 ESG 우수기업’은 한국기업지배구조원이 매년 한국거래소(KRX) 상장 법인을 대상으로 환경경영(Environment), 사회책임경영(Social), 지배구조(Governance) 부문에 대한 다면적 종합 평가를 실시하여 우수한 기업을 선정하는 방식으로 진행하는 시상식이다. 안랩은 2008년 첫 수상 이래 8회째 ESG 우수기업으로 선정되면서, 사회적 책임 이행 노력 및 지배 구조 개선 성과가 우수한 기업으로서의 명성을 재확인했다.

안랩 권치중 대표는 “안랩은 대표 보안 기업으로서, 앞으로도 경영 활동에 있어 모범 기업이 될 수 있도록 최선을 다하겠다”고 수상 소감을 전했다.

안랩은 이 밖에도 투명 경영 노력을 인정받아 ‘2013 투명회계대상(한국회계학회)’, ‘2013 한국 CFO 대상 회계투명성 부문 대상(한국 CFO협회)’ 등을 수상한 바 있다.



▲ 한국기업지배구조원 조명현 원장(왼쪽)과 안랩 인치범 상무(오른쪽)

DDoS 대응 솔루션 ‘트러스가드 DPX’ 매출 크게 성장

DDoS 대응 솔루션 ‘안랩 트러스가드(TrusGuard) DPX’ 제품군이 금융·포털·통신·공공 등 다양한 분야의 고객사를 다수 확보하며 지난해 3분기 대비 103% 매출을 기록하는 등 큰 성장세를 보이고 있다.

‘안랩 트러스가드 DPX’는 안랩의 독자적인 보안 기술과 인프라가 결합된 DDoS 대응 전용 제품이다. 안랩의 악성코드 분석 시스템과 연동된 신속한 DDoS 공격 대응 프로세스를 제공하여 네트워크의 안정적인 운영을 돋고, 다단계 필터 구조와 자동 학습 정책을 이용해 오탐은 최소화한다.

안랩 네트워크사업부 고광수 상무는 “최근 미국에서 IoT 기기를 악용한 대형 DDoS 사건이 발생한 것처럼 향후 IoT 환경에서의 DDoS 방어는 더욱 중요하다”며, “앞으로도 기술력을 기반으로 게임이나 포털 등 대형 고객사 시장에서 성장을 이어나갈 것”이라고 밝혔다.



▲안랩 트러스가드 DPX

안랩은 장비 외에도 DDoS에 특화된 사전 컨설팅, DDoS 공격 모의 대응 훈련, 보안관제 등 DDoS 대응을 위한 다양한 서비스와 종합적인 프로세스를 제공하고 있다.

발행인 : 권치중

발행처 : 주식회사 안랩

경기도 성남시 분당구 판교역로 220

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

편집인 : 안랩 콘텐츠기획팀

디자인 : 안랩 디자인팀

© 2016 AhnLab, Inc. All rights reserved.

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템
으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입
니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상
표일 수 있습니다. 본 문서에 수록된 정보는 고지없이 변경될 수 있습니다.

<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
© 2016 AhnLab, Inc. All rights reserved.