보고

# McAfee® Labs 2014년도 위협 예측

# 목차

### 1: 모바일 악성 프로그램은 2014년 전반적인 악성 프로그램 "시장"에서 기술 혁신과 공격의 양 측면에서 모두 성장 동인이 될 것입니다.

2013년, 거의 Android 플랫폼만 목표로 삼았던 새로운 모바일 악성 프로그램의 성장 속도는 PC를 목표로 한 새로운 악성 프로그램의 성장 속도보다 훨씬 높았습니다. 보고된 지난 두 분기 동안 새로운 PC 악성 프로그램 성장은 거의 변화가 없었으나 새로운 Android 샘플은 33% 증가했습니다.

McAfee Labs는 2014년에도 이 동향이 지속될 것으로 예상하고 있으며 주목해야 할 것은 새로운 모바일 공격의 성장 속도만이 아닙니다. Android를 목표로 하는 완전히 새로운 공격 유형도 나타날 것으로 예상됩니다. 장치의 중요 데이터를 암호화하여 그에 대한 "몸값"을 요구하는 모바일 장치를 목표로 하는 최초의 실질적인 랜섬웨어가 등장할 가능성이 높습니다. 피해자가 기존 통화나 가상 통화(비트코인 등)로 가해자에게 지불할 경우에만 정보를 놓아주는 것입니다. 모바일에서 등장할 것으로 예상되는 다른 새로운 전술로는 이제 많은 장치에 탑재된 근거리 통신 기능의 취약성을 이용하여 정상적인 앱이 들키지 않고 데이터를 도용하게 만드는 공격이 있습니다.

모바일 장치에 대한 공격은 기업 인프라도 목표로 삼을 것입니다. 이러한 공격은 이제 보편화된 BYOD(bring-your-own-device) 현상과 모바일 보안 기술의 상대적인 미숙함 때문에 가능합니다. 사용자가 자신도 모르게 다운로드한 악성 프로그램이 기업 내부로 침투하여 기밀 데이터를 빼내게 됩니다. 그렇다고 BYOD가 사라지지는 않기 때문에 기업이 포괄적인 장치 관리 정책과 솔루션을 확립하여 피해를 입지 않도록 해야 합니다.

### 2: 가상 통화는 전 세계 악성 랜섬웨어 공격을 더욱 가속할 것입니다.

피해자 장치의 데이터를 암호화하는 랜섬웨어 공격이 등장한 것은 꽤 오래전의 일입니다. 하지만 지금까지 이러한 공격은 가해자가 이용하는 지불 처리 업체에 대한 법적인 조치로 쉽게 차단되었습니다.


CryptoLocker 대화 상자.

가상 통화의 이용률 증가는 경제 활동을 촉진하지만 사이버 범죄자가 피해자로부터 돈을 갈취하기에 이상적인 규제되지 않는 익명의 지불 인프라를 제공하는 셈입니다. CryptoLocker와 같은 공격이 많은 수익을 보장하는 한 앞으로도 계속 확산될 것으로 생각됩니다. 또한 기업을 대상으로 하여 주요 기업 데이터를 암호화하는 새로운 랜섬웨어 공격도 예상됩니다.

개인에게나 기업에게나 다행인 것은 랜섬웨어의 페이로드는 고유하지만 배포 메커니즘(스팸, 다운로드 및 감염된 앱)은 그렇지 않다는 점입니다. 악성 프로그램 방지(엔드포인트 및 네트워크 모두) 시스템을 최신으로 유지하는 소비자와 기업은 이러한 위협으로부터 상대적으로 안전합니다. 개인이나 기업이 구현한 효과적인 백업 시스템 또한 랜섬웨어의 부정적인 영향 대부분을 차단할 것입니다.

### 3: 스파이와 스파이가 맞서는 사이버 범죄의 세계에서는 범죄 집단과 국가 단체가 식별과 차단이 매우 어려운 새로운 은폐형 공격을 이용할 것입니다.

정보 보안 솔루션만큼 이를 우회하려는 사이버 범죄 커뮤니티의 노력도 정교해졌습니다. 진화한 우회 기술을 사용하는 공격이 기업 데이터 보안 전쟁의 최전선에 설 것입니다. 2014년에 사이버 범죄자들이 널리 채택할 것으로 예상되는 인기 우회 기술은 보호되지 않는 장치에 실행 중임이 확인되지 않으면 완전히 배포하지 않는 sandbox 인식 공격을 사용하는 것입니다.

2014년에 더욱 발전하고 배포될 다른 인기 있는 공격 기술로는 정상적인 응용 프로그램이 악성 프로그램이 되는 return-oriented 프로그래밍 공격, 목표를 전복시킨 후 흔적을 지우는 자가 삭제 악성 프로그램, 공공 및 민간 인프라를 손상시킬 가능성이 있는 전용 산업 제어 시스템에 대한 진화한 공격이 있습니다.

특히 2014년 소치 동계 올림픽(2월)과 브라질 FIFA 월드컵(6월~7월) 전후에는 정치적인 동기의 공격이 증가할 것입니다. 핵티비스트 역시 이러한 행사를 이용하려고 할 것입니다.

기업 IT 조직은 글로벌 사이버 범죄 집단에 의해 즉시 뚫릴 수 있는 보안 조치에 완전히 의존하지 않도록 이러한 새로운 전술에 대응해야 합니다.

### 4: 2014년 말에는 "소셜 공격"이 보편화될 것입니다.

소셜 플랫폼 공격은 Facebook, Twitter, LinkedIn, Instagram 등의 대규모 사용자 기반을 이용하는 공격입니다. 이들 대부분은 Koobface처럼 레거시 악성 프로그램의 전략을 흉내내며 소셜 플랫폼을 그 수단으로 활용할 뿐입니다. 하지만 2014년에는 소셜 플랫폼의 고유한 특징을 활용하여 광고 타겟팅 또는 가상 또는 실제 세계 범죄에 활용할 수 있는 사용자 연락처, 위치 또는 비즈니스 활동에 관한 데이터를 제공하는 공격도 등장할 것입니다.

가장 일반적인 플랫폼 공격 중 하나는 사용자 자격 증명을 도용한 후 이를 알지 못하는 친구나 동료로부터 개인 데이터를 빼내는 것입니다. Facebook, Google, Yahoo 등의 사용자로부터 2백만 건의 암호를 빼돌린 Pony 봇넷[1]은 빙산의 일각에 불과합니다. Facebook은 자체적으로 월간 활성 사용자(MAU) 계정 5,000만~1억개가 복제되고 등록된 MAU 중 최대 1,400만개가 "원하지 않는 계정"인 것으로 추산하고 있습니다. 최근 Stratecast 연구에 따르면 소셜 미디어 사용자의 22%가 보안 관련 사고를 경험했습니다.[2]

공기업과 사기업 모두 소셜 플랫폼을 사용하여 직접적으로 또는 제3자를 통해 간접적으로 경쟁업체와 라이벌에 대한 "정찰 공격"을 수행할 것입니다. 2013년에는 공공 부문 및 민간 부문의 유명한 선도업체가 이런 공격의 목표가 되었습니다. 2014년에는 이러한 공격의 빈도와 범위가 확대될 것으로 예상됩니다.

2014년에 증가할 것으로 예상되는 다른 소셜 공격 형태는 사용자가 개인 정보 또는 인증 자격 증명을 드러내게 만드는 "가짜 플래그" 공격입니다. 사용자의 암호를 재설정하라는 "긴급" 요청을 제시하는 방법이 가장 많이 쓰일 것입니다. 그런 다음 사용자 이름과 암호 자격 증명을 도용하고 사용자의 계정을 이용하여 사용자와 연락처에 대한 개인 정보를 수집합니다.

소셜 플랫폼과 가짜 플래그 공격을 모두 차단하려면 직원의 소셜 미디어 플랫폼 이용으로 중요한 데이터 침해가 발생하지 않도록 보장하기 위한 개인과 기업 정책 및 솔루션을 통해 경계를 강화해야 합니다.

### 5: 새로운 PC 및 서버 공격은 운영 체제 위와 아래의 취약성을 목표로 삼을 것입니다.

대부분의 사이버 범죄 집단은 모바일 장치로 주의를 돌리지만 여전히 PC와 서버 플랫폼을 목표로 삼는 곳도 있을 것입니다. 하지만 2014년에 새로 등장할 공격은 운영 체제를 공격할 뿐만 아니라 OS 위와 아래의 취약성도 공격할 것입니다.

2014년의 새로운 PC 공격 중 다수는 상호 작용, 개인화 및 프로그래머를 위한 풍부한 기능으로 웹 사이트에 활력을 불어넣을 HTML5의 취약성을 노릴 것입니다. 하지만 HTML5는 몇 가지 새로운 공격 표면을 노출하기도 합니다. 이미 HTML5를 사용하여 사용자의 브라우저 기록을 모니터링함으로써 맞춤 광고를 향상시키는 방법이 증명되었습니다. 대부분의 HTML5 기반 응용 프로그램이 모바일 장치에 맞게 설계되었기 때문에 브라우저 sandbox를 무력화하고 공격자가 장치와 서비스에 직접 액세스할 수 있게 하는 공격이 등장할 것입니다. 또한 많은 기업들이 HTML5 기반 기업 응용 프로그램을 구축할 것입니다. 이러한 응용 프로그램에서 사용하는 데이터가 유출되지 않도록 시작부터 새로운 시스템에 보안을 내장해야 합니다.

사이버 범죄자는 운영 체제 아래의 스토리지 스택은 물론 BIOS까지 취약성을 찾아 공격할 것입니다. 기업 환경에서 이러한 하위 수준 공격을 완화하려면 운영 체제 수준 아래에서도 작동하는 하드웨어 지원 보안 조치를 실시해야 합니다.

### 6: 위협 환경의 진화로 인해 감지 및 성능 요구 사항을 충족하기 위한 빅데이터 보안 분석 채택이 요구될 것입니다.

역사적으로 대부분의 정보 보안 솔루션은 악성 페이로드 식별(블랙리스트) 또는 유효한 응용 프로그램 추적(화이트리스트)에 의존해왔습니다. 현재 정보 보안 담당자들이 직면한 과제는 "회색" 페이로드를 식별하고 적절히 처리하는 것입니다. 이를 위해서는 여러 개의 보안 기술을 강력한 위협-평판 서비스를 통해 조화롭게 적용해야 합니다.

위협 평판 서비스는 악성 프로그램, 악성 웹 사이트, 스팸 및 네트워크 공격의 감지에 있어 이미 그 가치를 증명했습니다. 2014년에는 보안 공급업체가 지금보다 은폐 위협 및 진화한 영구적인 위협을 더욱 빠르고 정확하게 식별할 수 있는 새로운 위협 평판 서비스와 분석 도구를 추가할 것입니다. 빅데이터 분석은 보안 담당자가 미션 크리티컬 비즈니스 프로세스를 중단시킬 수 있는 정교한 고급 우회 기술 공격과 진화한 영구적인 위협을 파악할 수 있게 할 것입니다.

### 7: 클라우드 기반 기업 응용 프로그램의 배포로 사이버 범죄자가 새로운 공격 표면을 이용할 수 있게 될 것입니다.

20세기 초에 100개의 은행을 턴 Willie Sutton은 은행을 턴 이유가 "돈이 있는 곳이기 때문"이라고 말한 것으로 알려져 있습니다.[3] 21세기의 사이버 범죄 집단은 클라우드 기반 응용 프로그램 및 데이터 저장소를 목표로 삼을 것입니다. 그 곳에 데이터가 있기 때문입니다. 이는 IT가 기업 보안 정책에 대해 평가하지 않은 비즈니스 응용 프로그램을 통해 이루어질 수 있습니다. 최근 보고서에 따르면 비즈니스 사용자의 80% 이상이 기업 IT의 지식이나 지원 없이 클라우드 응용 프로그램을 사용한다고 합니다.[4]

클라우드 기반 응용 프로그램은 매력적인 기능과 경제적 이점을 제공하지만 모든 데이터 센터에서 발견되는 보편화된 하이퍼바이저, 클라우드 서비스의 멀티테넌트 통신 인프라, 대규모 클라우드 서비스 프로비저닝 및 모니터링에 사용되는 관리 인프라와 같이 가해자에게 전혀 새로운 공격 표면을 다수 노출시키기도 합니다. 기업 보안 담당자의 문제는 기업 응용 프로그램이 클라우드로 옮겨질 때 조직이 보안 프로파일에 대한 가시성과 제어를 잃는다는 것입니다.

이렇게 기업 보안 경계에 대한 직접적인 제어를 잃으면 보안 책임자와 관리자가 클라우드 공급자의 사용자 계약 및 운영 절차에 따라 보안 정책이 확립되고 진화하는 위협 환경에 맞게 꾸준히 업그레이드되는지 확인해야 하는 부담이 크게 증가합니다. 대기업은 클라우드 공급자가 기업의 보안 태세와 일관된 보안 정책을 확립하도록 요구할 수 있는 충분한 힘을 가지고 있을 수 있습니다. 하지만 소규모 클라우드 기반 서비스 소비자는 그렇지 않기 때문에 공급자의 모호한 사용자 계약을 신중하게 검토해야 합니다. 보안과 데이터 소유권에 관련되어 있기 때문입니다. 새로운 클라우드 서비스는 반드시 보호해야 하는 데이터 보안 보장에 필요한 장치와 대응 조치를 포함하는 수준으로 서비스가 성숙할 때까지는 새로운 공격 표면을 노출할 것입니다.

## 작성자 정보

본 보고서는 Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky 및 Chong Xu가 준비하고 작성한 것입니다.

## McAfee Labs 소개

McAfee Labs는 위협 연구, 위협 인텔리전스 및 사이버 보안 사고 리더십에 대한 세계 최초의 소스입니다. 500명의 연구원으로 이루어진 McAfee Labs 팀은 파일, 웹, 메시지 및 네트워크라는 주요 위협 벡터에 걸쳐 수백만 개의 센서로부터 위협 데이터를 수집합니다. 그런 다음 교차 벡터 위협 상관 관계 분석을 수행하고 클라우드 기반 McAfee Global Threat Intelligence 서비스를 통해 긴밀히 통합된 McAfee 엔드포인트 및 네트워크 보안 제품으로 실시간 위협 인텔리전스를 제공합니다. McAfee Labs는 또한 DeepSAFE, 응용 프로그램 프로파일링, 그레이리스트 관리와 같은 핵심 위협 감지 기술을 개발하여 업계에서 가장 폭넓은 보안 제품 포트폴리오로 통합합니다.

## McAfee 정보

Intel Corporation(NASDAQ: INTC)의 자회사인 McAfee는 비즈니스, 공공 부문 및 가정 사용자가 인터넷의 혜택을 안전하게 경험할 수 있게 지원합니다. McAfee는 시스템, 네트워크 및 모바일 장치를 위한 사전 예방적이고 검증된 보안 솔루션과 서비스를 제공합니다. McAfee는 선구적인 Security Connected 전략, 혁신적인 하드웨어 향상 보안 접근 방식, 그리고 고유한 글로벌 위협 인텔리전스 네트워크를 통해 고객을 안전하게 지키는 데 전념하고 있습니다.
http://www.mcafee.com/kr

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords
[2] Stratecast, *"The Hidden Truth Behind Shadow IT."* (그림자 IT(Shadow IT)의 숨겨진 진실.) 2013년 11월. http://www.mcafee.com/kr/resources/reports/rp-six-trends-security.pdf
[3] Sutton는 그가 한 말로 널리 알려져 있는 말을 실제로는 하지 않았고 은행을 턴 이유는 단지 "재미있었기 때문"이라고 했습니다.
[4] Stratecast, *"The Hidden Truth Behind Shadow IT."* (그림자 IT(Shadow IT)의 숨겨진 진실.) 2013년 11월. http://www.mcafee.com/kr/resources/reports/rp-six-trends-security.pdf

McAfee
An Intel Company

한국맥아피(주)
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.mcafee.com/kr


60756rpt_threats-predictions_1213_fnl_ETMG