위협 예측

McAfee 연구소

사이버 스파이 활동

사이버 스파이 활동의 발생 빈도는 앞으로도 계속 증가할 전망입니다.

인텔리전스 데이터 수집

사이버 스파이들은 더욱 은밀한 정보 수집자로 변모하게 될 것입니다.

지능화된 사이버 범죄는 빠르고 민첩한 공격에서 인텔리전스 데이터 수집으로 그 추세가 바뀔 것입니다.

금전 탈취

새로운 사이버 스파이들은 금전을 탈취하고 상대를 교란시킬 방법을 찾을 것입니다.

2013년에 사이버 스파이 활동으로 인한 사고는 511건을 기록했는데, 이 중 데이터 유출로 확인된 것이 306건에 달했습니다.[1]

사이버 스파이 행위자의 유형.[2]

87% 국가 산하 기관

11% 범죄 조직

1% 경쟁업체

1% 전직 직원

사물 인터넷(IoT: Internet of Things)

인터넷에 연결되는 개체 수의 급증, 취약한 보안 환경, IoT 기기 대상의 데이터 중요성 증대 등으로 인해 IoT 기기에 대한 공격이 급속하게 증가할 것으로 전망됩니다.

500억 대에 육박하는 기기 수

2019년이면 전 세계적으로 인터넷에 연결된 기기의 수가 500억 대를 넘어설 것으로 전망[3]

IoT 기기

IoT 기기에 대한 공격이 이미 일반화되어 있습니다.

- IP 카메라.
- 스마트 미터.
- 의료 기기.
- SCADA 기기.

HP가 최근 실시한 테스트에서 IoT 기기의 보안 상태에 대해 경각심을 불러일으킬 만한 통계 결과가 확인되었습니다. 널리 사용되고 있는 10대의 기기를 대상으로 테스트를 한 결과입니다.[4]

70% 보안 취약점 노출

25 홈 네트워크에 위협이 되는 보안 취약점이나 위험이 각 기기에서 발견

80% 복잡한 암호 구성 요구조건을 충족하지 못함

90% 최소 1건의 개인 정보 수집

70% 계정 목록을 통해 유효 계정을 식별하는 공격 허용

개인 정보 보호

정부와 기업이 개인 정보에 대한 공정한 액세스 권한 문제로 씨름하고 있는 상황에서 개인 정보 보호가 앞으로도 여전히 위협을 받을 것입니다.

1억 1천만 명이 개인 정보 노출을 경험

작년 한 해 1억 1천만에 달하는 미국인들(**미국 성인의 약 50%에 해당**)이 어떤 형태로든 **개인 정보의 노출을 경험했다고 합니다.**[5]

암호

시대에 뒤쳐진 역할 기반 시스템 및 **암호 체계는 제대로 보안 기능을 수행하지 못하고** 악의적인 목적을 가진 침입자에 의해 공격을 당할 수 있습니다.

규정

개인 정보 보호 규칙 및 규정의 범위가 계속해서 확대될 것으로 보입니다.

생체인식기술

생체인식기술과 컨텍스트 기반의 ID는 중요한 혁신 분야로 부상할 것으로 보이며, **공격의 존재 여부와 의도를 가장 잘 보여주는 지표**가 될 것입니다.

랜섬웨어(ransomware)

랜섬웨어는 전파 방식, 암호화, 표적 설정 등에서 그 수법이 날로 진화하고 있습니다.

200만 개의 샘플

McAfee 연구소 zoo에 수집된 랜섬웨어 샘플의 총 개수가 **2014년 3분기에 200만 개**를 넘어섰습니다.

클라우드 기반의 스토리지

랜섬웨어는 클라우드 기반의 스토리지 서비스에 가입한 단말 기기들을 표적으로 **로그인한 사용자의 저장된 증명서를 이용해서** 클라우드에 백업되는 데이터에 침투하고자 시도합니다.

255,000 달러 금전 탈취

McAfee연구소는 단 한 차례의 CryptoLocker 랜섬웨어 공격으로 **한 달 만에 255,000 달러**의 금전 탈취가 발생한다는 사실을 발견했습니다.

모바일 공간

랜섬웨어 공격은 **클라우드에 백업되는 데이터를 표적으로** 모바일 공간에서 반복될 것으로 보입니다.

모바일 공격

신종 기술로 공격 범위가 확대되고 있으며 불완전한 앱 스토어 보안으로 모바일 공격이 빠른 속도로 증가할 것으로 보입니다.

온라인 결제

모바일 기기에서의 **온라인 결제를 위해 NFC(Near-Field Communication)가 채택되면서** 사이버 절도가 증가할 것으로 보입니다.

가상 화폐

모바일 기기를 표적으로 삼아 **가상 화폐를 이용해 "몸값"을 지불하도록 요구하는** 랜섬웨어 공격이 증가할 것으로 보입니다.

악성광고(malvertising)

신뢰할 수 없는 앱 스토어가 "악성광고"를 통한 **모바일 악성코드 전파의 주요 근원지가 될 것으로 보입니다.**

모바일 악성코드 키트

악성코드 세대 키트와 소스 코드를 쉽게 이용할 수 있게 되면서 **모바일 기기를 표적으로 하는 사이버 범죄가 용이해질 것으로 보입니다.**

모바일 악성코드 샘플은 올해 3분기에만 16% 증가했고, 작년 한 해 동안 112% 증가했습니다.

16% 2014년 3분기

112% 2013년 4분기– 2014년 3분기

모바일 악성코드 샘플의 총 개수가 2014년 3분기에 500만 개를 넘었습니다.

비 윈도우즈 기반 악성코드 공격 확산

Shellshock 취약점으로 인해 비 윈도우즈 기반 악성코드 공격이 확산되고 있으며, 이러한 추세는 앞으로도 계속될 것으로 보입니다.

22,487건에 육박하는 IP 주소 공격

Shellshock 취약점을 악용한 IP 주소 공격은 발표 후 4일만에 **총 22,487의 발생 건수를 기록했습니다.**[6]

Shellshock

데이터를 탈취하고, 데이터를 볼모로 금전을 요구하며, 스팸봇을 활용하는 등 Shellshock을 악용한 공격이 증가할 것으로 보입니다.

기기

라우터, TV, 산업용 컨트롤러, 비행 시스템 및 기타 중요 인프라 같은 기기들은 Shellshock 취약점을 내포하고 있을 수 있습니다.

위험성

Shellshock은 국가 취약성 데이터베이스(NVD: National Vulnerability Database)가 평가한 보안 심각도에서 **10점 만점**을 받았습니다.[7]

자세한 내용은 2014년 11월에 발표된 위협 보고서(Threats Report)의 "McAfee 연구소 2015년 보안 위협 전망"을 참조하시기 바랍니다.

보고서의 전문은 www.mcafee.com/November2014ThreatsReport에서 확인할 수 있습니다.

intel Security

McAfee는 현재 인텔시큐리티(Intel Security)에 통합되어 있습니다.

1 Verizon 2014 Data Breach Investigations Report (DBIR).
2 Verizon 2014 Data Breach Investigations Report (DBIR).
3 BI Intelligence, IDC 및 Intel의 조사 결과를 토대로 한 McAfee 보고서
4 HP의 사물 인터넷 연구 조사.
5 USA Today.
6 Akamai Security.
7 국가 취약성 데이터베이스(NVD: National Vulnerability Database).