EXECUTIVE SUMMARY

서론

시만텍은 2015년에 4억 3천만 개 이상의 고유한 신종 악성 코드를 발견했으며, 이는 전년 대비 36% 증가한 것입니다. 하지만 가장 주목할 점은 이러한 통계가 더 이상 놀랍지 않다는 것입니다. 오프라인 세상과 온라인 세상의 구분이 점차 모호해지는 가운데 사이버 범죄는 이제 우리 일상의 일부가 되었습니다. 기업과 정부가 공격을 받았다는 뉴스가 심심찮게 헤드라인을 장식하는 가운데 우리는 어느새 사이버 보안 위협의 엄청난 규모와 갈수록 빨라지는 속도에 둔감하게 되었습니다.

대부분의 보안 위협 보고서는 보안 위협 환경을 피상적으로 다루지만 시만텍 인터넷 보안 위협 보고서(ISTR)는 광범위한 시만텍 데이터를 바탕으로 표적 공격, 스마트폰 보안 위협, 소셜 미디어 스캠, 사물 인터넷(IoT) 취약점뿐 아니라 공격자의 전술, 동기, 행위까지 다각적으로 조명합니다. 이처럼 종합적인 관점으로 보안 위협 환경을 살펴본 결과 2015년에는 특히 아래 8가지 현상과 동향에 주목할 필요가 있습니다.

사이버 범죄 집단의 전문화

2015년은 사이버 범죄 집단이 더욱 전문화되어 하나의 기업처럼 움직이는 양상이 두드러진 해였습니다. 사이버 범죄자들은 기업과 개인 사용자를 대상으로 한 공격의 효율성을 높이기 위해 베스트 프랙티스를 채택하고 한층 전문적인 비즈니스로 만들어가고 있는 것으로 나타났습니다. 전문 사이버 범죄 집단은 방대한 리소스와 고급 인력을 보유하고 있으며, 일반 기업처럼 일정한 업무 시간을 준수하고 주말과 휴일에는 활동을 하지 않는 등 효율적인 비즈니스 형태를 띠고 있는 것으로 조사됐습니다.

제로데이 취약점 54개로 사상 최다, 악성코드 매일 118만개 발생

지능적인 공격 집단들이 지금까지 알려지지 않은 브라우저 및 웹 사이트 플러그인의 결함을 이용하여 계속 이익을 얻고 있습니다.

2015년 한 해 동안 발견된 제로데이 취약점은 2014년 24개 대비 125% 늘어난 54개로 두 배 이상 크게 증가하며 사상 최다를 기록했습니다. 다시 말해 2015년에는 (평균적으로) 매주 1개의 새로운 제로데이 취약점이 모습을 드러낸 셈입니다. 2013년에는 제로데이 취약점 수가 23개로 그 전해의 2배였습니다. 2014년에는 24개로 큰 변화가 없었기 때문에 정체기에 들어선 것으로 여겨지기도 했지만, 그 견해는 오래가지 못했습니다. 2015년에 제로데이 공격이 크게 증가한 것은 이 공격 수법이 수익성 표적 공격에서 중요한 역할을 하고 있음을 재차 확인해주는 셈입니다.

이러한 취약점의 가치를 생각한다면 수요를 해결하기 위한 시장이 발달한 것도 놀랍지 않습니다. 사실상 제로데이 취약점은 발견되는 속도로 미루어볼 때 이미 하나의 상품으로 자리잡은 듯합니다. 표적 공격 그룹은 취약점이 공개적으로 확인될 때까지 최대한 이용했다가 새로 발견된 취약점으로 갈아탑니다. 2015년에는 해킹팀(The Hacking Team)의 포트폴리오에 적어도 6가지의 제로데이 공격이 포함되어 있다는 사실이 밝혀지면서 이 분야에서 전문화가 이루어지고 있다는 분석을 뒷받침했습니다.

취약점은 어떤 소프트웨어 유형으로도 나타날 수 있지만 표적 공격자가 가장 선호하는 것은 널리 사용되는 소프트웨어입니다. 물론 이러한 취약점 대다수는 수많은 개인 사용자와 전문가가 일상적으로 사용하는 Internet Explorer, Adobe Flash와 같은 소프트웨어에서 발견됩니다. 2015년에 가장 많이 익스플로잇 공격의 대상이 된 제로데이 취약점 5개 중 4개는 Adobe Flash에서 발견되었습니다. 제로데이 취약점은 발견되는 즉시 사이버 범죄 툴킷에 추가되어 공격에 이용됩니다. 이 단계에서는 패치가 제공되지 않았거나 패치를 적용할 만큼 신속한 조치가 수행되지 않은 경우 수백만 명이 공격을 받고 수십만 명이 감염됩니다.

2015년에는 5억 건 이상의 개인 정보가 유출되거나 사라짐

데이터 유출 사고의 건수를 공개하지 않는 기업이 어느 때보다 많아졌습니다.

2015년을 마무리하는 시점에 공개적으로 보고된 것 중 최대 규모의 데이터 유출 사고가 발생했습니다. 자그마치 1억 9,100만 개의 정보가 유출된 것입니다. 가장 큰 규모의 초대형 보안 사고였지만 그렇다고 유일한 사건은 아닙니다. 2015년에 한 번에 1천만 건 이상의 개인 정보가 유출된 대형 보안 사고가 9차례나 발생, 사상 최다를 기록했습니다.

이러한 사고를 통해 유출된 것으로 보고된 개인 정보는 2014년 대비 23% 증가한 4억 2,900만 개였습니다. 하지만 이러한 수치에 가려진 더 중요한 사실이 있습니다. 2015년에는 발생한 보안 사고를 완전히 공개하지 않는 기업이 늘어난 것입니다. 실제로 유출된 기록 건수를 보고하지 않은 기업이 85%나 증가하면서 이와 같이 보고되지 않은 사고에 대한 보수적인 추정치로도 유출된 기록 수는 5억 건을 웃돌 것으로 예상됩니다.

이렇듯 기업들이 보안 사고의 중요 세부 사항을 공개하지 않는 추세는 매우 우려할 만합니다. 보안에서는 투명성이 관건이기 때문입니다. 보안 업계에서 각종 데이터 공유 이니셔티브가 진행되면서 보안 제품 및 환경을 강화하는 데 도움이 되고 있지만 이러한 데이터 중 일부는 수집하기 더 어려워지고 있습니다.

ISTR

Internet Security Threat Report

Executive Summary

Volume 21, Published April 2016

Symantec.

인기 웹 사이트의 4개 중 3개가 중대한 보안 취약점을 보유하고 있어 모두를 위험에 빠뜨리고 있음

여전히 웹 관리자는 최신 버전의 패치를 적용하는 데 어려움을 겪습니다.

2015년에는 매일 1백만 회 이상의 웹 공격이 발생했습니다. 많은 이들이 잘 알려진 합법적인 웹 사이트만 찾는다면 온라인 범죄로부터 안전할 것이라 생각합니다. 사실 그렇지 않습니다. 사이버 범죄자들은 끊임없이 합법적인 웹 사이트의 취약점을 노리면서 사용자를 감염시킵니다. 웹 사이트 관리자가 웹 사이트를 제대로 보호하지 못하는 상황이기 때문입니다. 실제로 합법적인 웹 사이트 중 75% 가량이 취약점에 대한 패치가 적용되지 않은 상태입니다. 또한 합법적인 웹 사이트 중 16%는 '심각한' 취약점을 갖고 있습니다. 결국 사이버 범죄자가 비교적 수월하게 사이트에 접근하고 조정하면서 목적을 달성할 수 있습니다. 이제는 웹 사이트 관리자들이 보다 적극적인 보안 대비가 필요할 것 입니다.

2015년에는 소수 집중형 표적 공격이 55% 증가

사이버 공격자들이 대기업을 상대로 장기적 전략을 펼치고 있습니다.

2015년에는 이미 공격의 표적이 되었던 정부 기관이나 금융 기관이 1년을 통틀어 3차례 이상 다시 공격을 받는 경우가 많았습니다. 종합적으로 볼 때 사이버 공격을 경험한 대기업에서 평균 3.6회 공격이 성공한 것으로 나타났습니다.

지난 5년 동안에는 직원 수 250명 미만의 기업을 노리는 공격이 꾸준히 증가했습니다. 2015년에 전체 공격의 43%가 소기업을 표적으로 삼은 것을 볼 때 모든 규모의 기업이 위험에 처해 있는 것입니다.

Fortune지 500대 기업과 정부 기관에서만 지적 재산 유출이 발생하는 것이 아닙니다. 동네 세탁업체도 표적이 될 수 있습니다. 실제로 직원 수가 35명인 기업이 경쟁사의 사이버 공격에 피해를 입은 적도 있습니다. 경쟁사는 2년 동안이나 발견되지 않은 채로 이 업체의 네트워크에 침투하여 고객 및 가격 정보를 훔쳐 내 이용했습니다. 모든 기업이 표적 공격에 취약할 수 있다는 분명한 경고입니다. 실제로 2015년에는 기업의 직원을 노리는 스피어피싱 캠페인이 55% 증가했습니다. 영리적 목적으로만 움직이는 공격자는 정부가 후원하는 공격자 못지않게 뛰어난 기술과 체계적인 조직을 갖출 수 있습니다. 가령 Butterfly 조직은 정보를 빼내 주식 조작에 이용하기도합니다.

2015년에 크립토 랜섬웨어 35% 증가

사이버 범죄자들이 기업과 개인의 중요 데이터를 볼모로 잡는 수단으로 암호화를 사용하고 있습니다.

랜섬웨어가 계속 진화하고 있습니다. 지난해에는 상대적으로 더 적은 피해를 일으키는 로커 유형(Locker-Style)의 랜섬웨어(시스템 화면 잠금)를 밀어내고 암호화 랜섬웨어(파일 암호화)가 기세를 떨쳤습니다. 암호화 유형의 랜섬웨어는 2015년에 35%나 증가했습니다. 수익성이 뛰어난 공격 유형인 랜섬웨어는 앞으로도 PC 사용자를 공략하겠지만, 네트워크에 연결되는 모든 장치가 랜섬웨어에 장악되어 돈을 지불하라는 요구를 받을 수 있습니다. 2015년에 랜섬웨어는 새로운 표적을 찾아내고 공격 범위를 PC뿐 아니라 스마트폰, Mac, Linux 시스템으로 확대했습니다. 시만텍도 2015년에 스마트 워치 및 TV에 대한 PoC(Proof-of-Concept) 공격 시연을 감행한 바 있습니다.

시만텍, 2015년에 1억 건에 달하는 기술 지원 위장 소비자 사기 스캠(scam) 차단

피해자가 직접 전화를 걸게 만든 후 갈취하는 사이버 사기가 증가하고 있습니다.

이렇듯 랜섬웨어는 보안 위협으로 성장을 계속하겠지만 발생할 수 있는 보안 위협은 그뿐만이 아닙니다. 생활의 더 많은 부분이 온라인에서 이루어짐에 따라 공격자는 피해자를 속일 새로운 방법을 찾고 있습니다. 2010년에 시만텍이 처음 보고했던 기술 지원 위장 사기는 이를 의심하지 않는 피해자와 통화하면서 피해자를 속여 공격자에게 직접 전화하게 만드는 수준까지 진화했습니다. 공격자는 중대한 오류 또는 문제가 발생했다는 팝업으로 피해자를 속여 콜센터로 전화를 걸게 합니다. 전화를 걸면 "기술 지원 담당자"라는 사람이 피해자에게 불필요한 서비스를 판매하려고 시도합니다. 시만텍은 2015년에 이러한 유형의 공격을 1억 차례나 차단한 바 있습니다.

공격자들은 온라인에서 훔쳐낸 것을 영리적으로 이용할 방법을 끊임없이 모색하고 있습니다. 지난해에는 Netflix가 여러 국가에 새롭게 진출하면서 공격자들의 주목을 받았습니다. 시만텍 연구 팀은 합법적인 Netflix 계정의 로그인 및 암호가 암시장에서 거래되고 있음을 밝혀냈습니다. 이러한 계정 액세스 정보는 피싱 또는 악성 코드를 통해 훔쳐낸 것이었습니다. 물론 계정 액세스 정보를 암시장에서 되파는 것이 결코 새로운 현상은 아닙니다. 시만텍은 유출된 호텔 회원 명단, 항공사 상용 고객, 게임 계정을 판매한다는 광고를 암시장에서 심심찮게 발견하고 있습니다.

모바일 보안 빨간불, 다음 타깃은 IoT 기기

2015년 발견된 신규 모바일 취약점은 528개로 전년 대비 214%의 증가세를 기록, 사이버 범죄의 새로운 타깃으로 모바일이 주목받고 있음을 보여줬습니다. 누적 안드로이드 악성 코드 수는 2014년 9,839개에서 40%가 늘어 지난 해 1만3,783개를 기록했습니다. 아이폰과 아이패드는 비교적 보안 위협이 낮다고 여겨져 왔는데, 2015년에는 상황이 달라졌습니다. 2015년 한 해에만 총 9개의 iOS 악성 코드가 발견되었는데, 이전까지 발견된 iOS 악성 코드를 모두 합쳐도 4개였던 것과 비교하면 현저히 증가한 것입니다. 특히 악성 코드 'XcodeGhost'는 이전 사례와 달리 탈옥하지 않은 기기라도 감염될 수 있음을 보여줘 새로운 위협을 경고했습니다. 한편, 인터넷 연결 기기들의 급증에 따라 스마트TV, 커넥티드카, 스마트홈 기기, 의료장비 등 IoT(Internet of Things) 기기들과 관련된 보안이 새로운 이슈로 떠오를 것으로 예상됩니다.