IDG
STRATEGIC
MARKETING SERVICES

CISCO

IDG Tech Focus

2017년에도 지속될 랜섬웨어 위협에 대응하는 기업 보안 전략

연초가 되면 상당히 많은 보안 전망 보고서가 쏟아져 나온다. 수많은 예측 가운데 100% 공통된 점이 있는데, 사이버 공격은 더 진화할 것이고, 기업은 더 많은 위협에 처해진다는 것이다. 무엇보다 100% 방어란 불가능하다는 인식이 확산되고 우리가 현재 처한 보안 상황이 예상보다 심각하다는 것을 깨닫는 것이 중요하다. 2017년 보안 현실을 짚어보고, 이에 맞는 차세대 보안 전략과 효과적인 랜섬웨어 방어 방안을 알아보자.

Tech Trends

"랜섬웨어, 위협 인터넷, 그리고 드웰 시간은 증가한다" 2017년 보안 전망

"랜섬웨어에 당했다" 기업에서 할 수 있는 대응 전략 2가지

Solution

2017년 국내 보안 현실과 랜섬웨어에 대응하는 다단계 방어 전략

Tech Trends

"랜섬웨어, 위협 인터넷, 그리고 드웰 시간은 증가한다" 2017년 보안 전망

Sharon Florentine | CIO

"2016년이 나빴다고 생각한다면 안전 벨트를 매라! 더 나쁠 한 해를 앞두고 있기 때문이다."

W-2 스캔과 워드프레스(WordPress) 취약점에서부터 랜섬웨어와 비즈니스 이메일 침해, DDoS 공격, 미국 대통령 선거 해킹에 이르기까지 2016년은 사이버 보안의 '지옥' 같은 한 해였다. 하지만 이것이 끝이 아니다. 2017년은 조금이라도 나아질 것이라고 믿을 근거가 단 한 가지도 없기 때문이다. 오히려 훨씬 더 나빠질 소지가 많다. 사이버 범죄자들이 소셜 엔지니어링 공격에 더 박차를 가하고, 악성코드를 전달하고, 취약한 데이터베이스를 해킹하고, 기업 네트워크 내부로 침입하고, 개인 사용자를 표적으로 삼을 새로운 방법들을 찾고 있기 때문이다. 이에 보안업체 봄가(Bomgar)의 CEO 매트 더크스와 사이버 애드APT(Cyber adAPT) CTO 스콧 밀리스와 함께 2017년 전망에 대해 논의했다.

1. 비밀번호가 강화된다

10월 21일 인터넷에 큰 혼란을 초래했던 DDoS 공격의 빌미를 제공한 원인 가운데 하나는 IoT 장치의 기본 비밀번호를 변경하지 않고 사용했기 때문이다. 더크스는 해커들이 이 점을 악용할 수 있었다고 지적했다.

이 문제가 자사와는 상관없다고 생각하지 말기 바란다. 단순하고 흔하며, 오래된 비밀번호를 사용하는 사용자가 많기 때문이다. 더크스는 2017년에는 기업들이 비밀번호가 얼마나 취약한지 깨닫고 비밀번호 관리 서비스에 관심이 쏠릴 것이라고 내다봤다.

더크스는 "다른 사람의 집을 방문했을 때 라우터를 해킹하는 시범을 보이곤 했다. 몇 달 전 DDoS 공격에 사용된 라우터 같이, 해커들의 수고를 덜어주는 '멍청한' 전용 장치들이 정말 많다"고 말했다. 사이버보안 담당자들은 취약한 비밀번호를 이용하는 '관행'이 개선되지 않아 핵심 인프라, 연결된 시스템, 원격 액세스 시스템, 장치 보안에 계속 애를 먹을 것이다.

그런데 외부 위협만 문제가 되는 것은 아니다. 비밀번호 관리를 개선해 내부 위협 또한 경감해야 한다. 이를 위한 가장 좋은 방법은 사용자가 모르는 비밀번호를 생성해 저장하고, 정기적으로 인증과 순환을 반복하는 솔루션을 도입하는 것이다.

더크스는 "우리는 이를 크리덴셜 금고(Credential Vaults)라고 부른다. 사용자가 자신의 비밀번호를 모르는 것이 이상적이다. 금고가 이를 자동으로 생성, 순환, 매주 변경하는 방식이다. 해커들은 원래 게으르다. 또 해야 할 일이 있다. 일을 어렵게 만들면 에너지를 투자하지 않아도 되는 다른 표적을 찾을 것이다"고 말했다.

2. 권한 있는 사용자가 중시된다

해커는 고수준의 액세스를 원한다. 이에 IT 담당자, CEO, 개발업체 등 특권 사용자(Privileged User)를 표적으로 삼는다. 기업과 기관은 비즈니스에 아주 중요한 시스템, 애플리케이션, 데이터에 보안을 적용한다. 그러나 이제 이런 예방책만 가지고 위협을 방지하기 어렵다.

2017년부터는, 사이버 보안에 앞선 기업들을 중심으로 시스템은 물론 특권 사용자를 보호하는 것을 중시할 전망이다. 특권 사용자를 파악하고, 이들의 액세스를 모니터하고, 불필요한 액세스를 차단하게 된다.

더크스는 "사용자와 협력업체에 대해 VPN에 유지시켜도 문제가 없다고 말하는 고객이 있는데, 이들이 실제 액세스하는 대상을 모르고 있다. 특권 사용자는 '엘리베이터'처럼 역할에 따라 특정 층에만 도착하도록 관리해야 한다. 이런 관리 방법은 특히 악의적인 의도를 갖고 있는 이가 있을 때 도움이 된다. 유효한 비밀번호가 있어도, 1층과 7층만 이용할 수 있는 권한이라면, 6층을 눌렀을 때 시스템이 이를 차단하고 통보한다"고 말했다.

이런 문제들을 해결하기 위해 조직들은 다양한 위험을 광범위하게 교육하고 훈련시켜야 한다. 특히 액세스를 위해 프라이버시와 개인 데이터를 포기하고, 서드파티 서비스 공급자와 애플리케이션 개발자가 보안을 책임져 줄 것이라고 믿는 모바일 인력이 증가하고 있다는 점에서 중요한 부분이다.

더크스는 "젊은 디지털 세대들은 앱 액세스, 연결성, 정보 액세스를 위해 개인 정보와 데이터를 포기하는 경향이 있다. 이는 쉽게 악용될 수 있는 부분들이다. 또한 이 세대들은 앱 개발자와 서비스 공급자가 자신을 안전하게 보호해 줄 것이라고 믿는다. 아주 위험한 생각이다. 여기에 더해, 사이버 보안 역량과 인재가 부족하고, 모바일 인력과 앱 중심 환경이 확산되고 있어 해킹이 더욱 정교해지고, 피해가 커진다. 이로 인해 상황이 개선되기 전에 더 악화될 것으로 보인다"고 말했다.

3. 보안에 대한 책임 회피가 증가한다

더크스는 "고객들과 이야기를 나누면서 정말 두려운 트렌드 한 가지를 발견했다. 고객들은 '공격을 받는 것은 시간 문제라고 생각한다. 그런데 두 손을 놓고 공격받게 된다'라고 하는데, 이는 아주 무서운 얘기다"고 말했다.

IoT와 함께 보안 솔루션 공급자에 대한 의존도가 높아지면서 공격이 발생했을 때 기업들이 책임을 지거나, 공격 원인을 설명할 수 없게 될 수도 있다. 누

가 기술 보안, 유지관리, 패치를 책임진 것일까? 아직 패치를 하지 못한 내부 시스템에 연결된 제품이 있는 경우 더 위험하다. IT의 전통적인 관리 범위를 벗어나있어 간과되는 IoT 장치들이 많다. 위협에 노출되어 있다는 의미다.

더크스는 "IoT와 자동화, 클라우드가 통합되면서, 다양한 기술 요소들의 보안을 책임질 주체가 불명확해졌다. IoT 장치 제조업체가 책임져야 할까? 보안 솔루션 공급자? 내부 IT 부서? 아니면 개별 사용자? 가장 안전하지 못한 장치 또는 주체가 보안 수준을 결정하는 법이다"고 말했다.

보안 계층이 겹겹이 형성되어 있는 상황에서 사고가 발생한 경우에는 책임 소재 문제가 대두된다. 서로 책임을 미루게 되는 것이다. 이를 해결하는 방법은 IT와 비즈니스 리더들이 열린 대화를 통해 잠재적인 위협, 보안 옵션, 도전과제와 제약을 이해하는 것이다.

더크스는 "CSO, CISO, 심지어는 CIO 등 보안을 책임진 사람들이 자신이 해야 할 일을 해도 존재감이 없기 때문에 문제가 발생한다. 좋은 정책, 절차, 보안 대책이 있을 때 IT에 운용을 맡기는 때가 많다. 그러나 비즈니스 필요사항, 예산, 요구사항을 이해하지 못해 제대로 실행이 되지 않았다면, 전혀 도움을 주지 못한 것이나 다름없다"고 말했다.

4. 랜섬웨어가 걷잡을 수 없이 확산된다

시만텍 시큐리티 대응팀이 발표한 '2016년 인터넷 보안 위협 보고서(2016 Internet Security Threat Report)'에 따르면, 2016년 1월 1일 이후 매일 평균 4,000건의 랜섬웨어 공격이 발생했다. 지난 해보다 약 300%가 증가한 수치다.

사이버 애드APT의 스콧 밀리스는 랜섬웨어 위협 경감에 경상비용이 적게 드는 방화벽, 안티바이러스 솔루션, 침입 방지 기술을 이용하는 기업들이 많다. 그러나 이들 도구로는 불충분하다. 침해 관련 통계는 탐지와 사고 대응을 강화해야 한다는 점을 보여준다.

공격자들은 데이터를 탈취하기 위해 조직의 중요한 직책이나 개인을 표적으로 소셜 엔지니어링, 소셜 네트워크를 이용하고 있다. 포괄적인 보안 교육이 훨씬 더 중요해진 것이다. 밀리스는 "보안 정책과 기술은 랜섬웨어가 침입 경로를 고려하지 않는다. 또 탐지의 문제도 있다. 일부 공격자는 조직 내부 환경에 몇 달 동안 은닉해 있다. 그러다가 수평 이동을 시작한다. 그런데 네트워크, 엔드포인트, 데이터 보안 시스템, 프로세스들이 고립되어 있어 이런 지능형 공격을 방어, 탐지, 대응하지 못한다"고 지적했다.

또한 조직이 최상의 보안 방법을 찾지 못한 새로운 공격 표면들이 존재한다. IaaS, SaaS, IoT를 예로 들 수 있다.

5. '드웰 시간'이 개선되지 않는다

드웰 시간(Dwell Times)이란 공격이 성공했을 때 피해자가 이를 발견하기까지 걸리는 시간이다. 밀리스에 따르면, 2017년에도 이 드웰 시간이 전혀 개선되지 않을 전망이다. 일부 극단적인 경우에는 드웰 시간이 2년까지 치솟고, 1건의 침해가 기업에 수백 만 달러의 피해를 초래할 수도 있다.

밀리스는 "드웰 시간이 이렇게 긴 이유는 무엇일까? 내 생각으로는 간단하다. 진짜 공격 활동에 초점을 맞추고 있지 않기 때문"이라고 말했다. '악성코드 시대'가 도래하면서, 기업과 보안업체, 개인이 사이버 범죄자들을 몰아내는 것에 집중했다. 그리고 전체 산업이 2가지에 초점을 맞추게 됐다.

첫째 다단계 방어(Defense-in-depth)다. 방어 계층을 겹겹이 형성해 외부 침입을 어렵게 만드는 방법이다.

둘째 '악성코드 탐지(식별)'이다. 악성코드를 100% 감지하도록 노력을 경주하는 방법이다. 대응 기술과 복구 능력이 개선되면서 피해자들이 아주 빠르게 피해를 복구할 수 있게 됐다. 그러나 이런 기술들은 드웰 시간을 줄이는데 도움을 주지 못한다. 대응 팀이 우연히 악성 동작을 발견할 때나 가능하다.

현재 보안 담당자들은 네트워크 장치 로그 파일을 이용, 공격 시도가 있었는지, 공격이 성공했는지 알려주는 단서를 찾는다. 그러나 수 많은 데이터를 저장해 처리하는데 많은 비용이 초래되며, 비효율적이다.

밀리스는 "막대한 데이터 저장과 광범위한 분석 엔진에 대한 필요성이 새로운 SIEM(Security Information and Event Management) 시장을 만들었다. SIEM은 사고 조사자들에게 아주 유용한 사후 포렌직 도구이지만, 진행 중인 공격을 효과적으로 탐지하지 못한다. 현재 일부 보안 업체들이 원래 네트워크 트래픽을 분석, 공격 지표를 찾는 제품을 개발하고 있다. 엔드포인트 또는 기기 방어 체계를 뚫거나, 우회한 즉시, 가능한 빨리 공격자를 찾을 수 있다면 드웰 시간을 크게 줄일 수 있다"고 설명했다.

6. 모바일이 공격 진입점이 되는 사례가 증가한다

밀리스는 2017년에는 모바일 기기로 인한 대규모 기업 침해 사고가 최소한 한건 이상 발생할 것이라고 전망했다. 포네몬 연구소(Ponemon Institute) 보고서에 따르면, 모바일 데이터 침해가 한 기업에 초래하는 경제적 위험이 최대 2,640만 달러에 달할 수 있다. 또 직원들이 자신의 모바일 기기로 회사의 요주의 비밀 정보를 이용하면서 데이터 침해 사고가 발생했다고 대답한 비율이 67%에 달했다.

밀리스에 따르면, 기존 사이버 보안 전략으로는 효과적으로 대처할 수 없을 정도로 사람과 모바일 기기의 이동 범위가 넓고, 속도가 빠르다. 여기에 사용자

의 기기 선택 권한이 커지면서 위협이 더 크게 증가했다.

밀리스는 "업무, 개인 서비스를 제한 없이 안전하게 이용하는 동시에 프라이버시도 보호할 수 있다고 생각하는 사용자가 많다. 또 사용자 경험을 높이기 위해 보안을 우회해도, 보안 침해 사고는 자신의 책임이 아니라고 믿는 사람들이 많다. 기업 보안 전략을 도입할 때, CISO, CIO, CEO들은 이를 까다로운 당면 과제로 인식한다. SSL을 통해 이메일과 캘린더 데이터를 전달하는 방법으로는 해결할 수 없는 과제다"고 말했다.

모바일 결제도 문제가 될 전망이다. 마스터카드의 '셀피 페이(selfie pay)'와 인텔의 '트루 키(True Key)'는 빙산의 일각에 불과하다. 개별 사용자가 생체인식 데이터를 다른 금융 데이터, 개인 데이터처럼 주의를 기울여 다뤄야 한다는 점을 인식해야 한다. 결국 교육과 훈련으로 귀결되는 문제다.

밀리스는 "담배처럼 공용 와이파이 액세스 공급자에게 의무적으로 위험을 고지하도록 만드는 것이 좋은 방법이 될 수 있다. '경고: 공용 인터넷 연결은 안전하지 않습니다. 범죄자가 전송되는 정보를 엿보거나, 수집하거나, 훔쳐 귀하의 자산, 신원, 개인 정보를 탈취할 수 있습니다.' 이런 경고문을 고지하도록 만드는 것이다"고 말했다.

7. 위협의 인터넷(Internet of Threats)?

IoT 취약점과 공격이 증가하고, 여러 다양한 보안 도구를 표준화 할 필요성이 높아질 전망이다. 2016년 데프콘(DefCon)에 참석한 해커들은 21개 제조업체의 23개 장치에서 47개의 새로운 취약점을 발견했다. 또한 2016년 10월에는 트위터, 넷플릭스, 영국 정부 등 주요 글로벌 웹사이트가 안전하지 못한 IoT 기기들을 동원한 미라이(Mirai) 봇넷으로부터 DDoS 공격을 받았다.

더크스는 "IoT의 영향력 증가에 대한 증가로 '스마트 장치'에 관심이 집중되어 있다. 그러나 연결된 기기는 스스로 스마트 기기가 되지는 못한다. 연결된 사물은 단순성을 유지하기 위해 '발사 후 망각형'의 형태를 갖는 경우가 많다. 또 이번 미라이 봇넷 공격에 악용된 라우터처럼, 우리가 계속 주의를 기울이지 못하는 내장 기능과 도구들이 있다. 즉 '멍청한' 기기들이 가장 큰 인터넷에 연결되어 있다는 사실을 잊어버리고, 여기에 주의를 기울이지 않는 때가 많다"고 지적했다.

이는 소형 가정용 전자 제품, 커넥티드 홈, 커넥티드 카에만 국한된 문제가 아니다. 또 다른 형태의 DDoS 공격이 발생할 가능성도 있다. 전력 그리드, 항공 시스템, 철도 시스템 등 대규모 인프라에 대한 공격이 발생한다면 더 심각한 문제가 초래될 수 있다.

더크스는 "인터넷에 연결된 샤워기가 제 멋대로 찬물, 더운물을 쏟아내는 등의 문제는 걱정하지 않는다. 2017년에는 전력 그리드나 철도 등 교통망에 해킹 사고가 발생할 확률도 있기 때문이다. '멍청한' IoT 기기들이 존재하는 장소이기 때문이다. 1950~60년대 기술이 핵심 인프라 시스템을 지원하고 있다. 안전과는 거리가 먼 기술들이다"고 지적했다. 밀리스는 "인식 문제가 있다. 보통 사람

들은 이들 시스템을 점차 사용이 증가하고 있는 IoT 기기와는 다른 기기로 생각한다. 그런데 휴대폰조차 이 범주에 포함될 수 있다"고 설명했다.

그러나 생각할 점이 있다. 스마트폰은 지금 주변에 가장 많은 인터넷 기기다. 그리고 미래에는 IoT 기기들이 규모 면에서 가장 많은 수를 차지하게 될 것이다.

일부 조직들은 현명하게 트렌드에 앞서 나가고 있다. 휴대폰이 지금 직면한 것과 동일한 문제들을 해결하려 노력하는 것이다. 그러나 대부분의 조직이 예방(방지)에 초점이 맞춰져 있으며 모든 기기/연결 기술들이 침해될 수 있다고 생각한다. 드웰 시간을 줄이고, IoT 보안을 철저히 해야 한다. 이를 위해서는 불가피한 침해 사고가 발생했을 때, 가능한 빨리 높은 신뢰도로 이를 파악하는 능력을 갖춰야 한다. ITWORLD

Tech Trends

"랜섬웨어에 당했다" 기업에서 할 수 있는 대응 전략 2가지

Jonathan Hassell | CIO

기업들이 데이터를 도난 당하고 볼모로 잡히면서 점차 사이버 범죄자들의 대가 지불 요구에 굴복하고 있다. 결국 최선의 방어는 적절한 공격이다.

새벽 5시에 긴급한 전화를 받고 잠에서 깨어났다. 무엇인가 회사의 네트워크를 장악하고 모든 데이터를 암호화했으며, 이를 되찾을 수 있는 유일한 방법은 익명의 제 3자에게 비트코인을 이용해 상당 금액을 지불하는 것이다. 다소 할리우드 영화처럼 들릴 수도 있지만 이것이 현실이며 전 세계적으로 여러 랜섬웨어 변종 때문에 조직들이 당하고 있는 일이다.

2016년 뉴스에 많이 회자됐던 여러 건의 랜섬웨어 사건들은 공공 및 사회 서비스에 필수적인 대형 조직들이 랜섬웨어 공격을 받으면서 피해 규모와 수가 증가하는 양상을 보여주고 있다.

- BBC는 미국 캘리포니아에 위치한 CVMCDV(Chino Valley Medical Center and Desert Valley) 병원이 랜섬웨어에 감염되었다고 보도했다. 이 병원의 소유주 PHS(Prime Healthcare Services)는 "병원 시스템에 상당한 혼란이 있었다"고 밝혔다.
- HPMC(Hollywood Presbyterian Medical Center)는 랜섬웨어 발생 후 내부적인 긴급 상황을 선언했다. 궁극적으로 이 병원은 컴퓨터에 액세스하기 위해 1만 7,000달러 이상의 대가를 비트코인으로 지불하기로 결정했다. 처음에는 370만 달러의 대가를 요구했기 때문에 병원의 입장에서는 꽤나 괜찮은 협상 결과였다.
- 미국 켄터키에 위치한 병원인 MH(Methodist Hospital)는 최근 랜섬웨어 공격을 받았다. 이번에는 랜섬웨어의 압박이 확인되었다. 크립토록커(Cryptolocker)의 새로운 변종인 록키(Locky)는 해당 병원의 네트워크의 방어 체계에 침투해 내부 네트워크 전체뿐만이 아니라 기타 여러 시스템에 확산되었다고 CNBC가 보도했다. 공격자들은 1,600달러의 대가를 요구했다. 아스 테크니카(Ars Technica)의 또 다른 보도에서는 이 병원의 변호사의 말을 인용했다. "절대적으로 필요한 경우가 아니라면 대가를 지불하지 않을 것으로 생각된다."

이렇듯 기업의 랜섬웨어 피해 사례들이 확산되고 있다. 일반적으로 랜섬웨어는 송장 또는 운송장 또는 기타 무해한 것으로 보이는 이메일 첨부 파일로 전달된다. 일단 파일을 열면 랜섬웨어는 사용자 상호작용이나 알림 없이 가능한 모

든 파일을 조용히 암호화하기 시작한다. 이런 악랄한 조치가 끝나면 사용자에게 복호화 대가의 금액과 지불 방법 등에 관한 정보를 제공한다.

크립토록커의 첫 번째 버전은 네트워크 드라이브의 데이터에 영향을 끼칠만큼 스마트하지 못했고 기기에 로컬 상태로 저장되어 있는 파일에만 암호화를 적용했다. 경우에 따라서는 무효화될 수도 있었지만 데이터의 대부분을 네트워크 드라이브와 SAN 또는 NAS에 저장하는 대기업이나 중견 기업들에게는 다행이었다.

하지만 안타깝게도 더 이상 그렇지 못하다. 왜냐하면 랜섬웨어가 거듭 진화 과정을 거쳐 대부분의 변종이 네트워크 드라이브와 UNC 경로를 통해 이동해 해당 악성코드를 실행하는 사용자 계정에 부여된 권한의 수준으로 접근할 수 있는 모든 것을 암호화하기 때문이다. 최근 랜섬웨어에 관한 보도에서 알 수 있듯이 그 결과는 한 기업을 아수라장으로 만들 수 있다.

랜섬웨어 대응 전략

랜섬웨어의 해결책으로는 단순한 것과 복잡한 것 2가지가 있다. 사실 3가지가 있지만 대가를 지불한다고 해서 무조건 해결된다는 보장이 없기 때문에 해결책이라 생각하지 않으며, 공격과 침략이 점차 성공을 거두게 되면서 몸값이 지속적으로 상승할 것이다.

– 정기적이고 일관된 백업과 검증된 복원

랜섬웨어 공격 때문에 망했다는 느낌이 들지 않는 유일한 방법은 일관되고 정기적인 백업 및 복원 절차를 통해 유효성을 검증한 최신 백업을 확보해 대가를 지불하지 않는 것이다.

그리고 나서 엄격한 모니터링과 적절한 파일 및 폴더 권한 설정을 통해 공격을 신속하게 탐지한 후 백업에서 암호화된 데이터를 복원할 수 있다. 많은 전문가가 파일 모니터링으로 한 동안 따로 수정하지 않은 다수의 파일이 순서대로 변경되는 상황을 탐지하는데 성공한 것으로 보고되고 있다. 이 덕분에 초기에 감염된 데이터만 잠재적으로 되돌릴 수 없는 암호화의 위험에 처하게 된다.

– 애플리케이션 화이트리스트(Whitelist) 작성

기본적으로 랜섬웨어 공격과 침입 또는 이와 관련된 기타 악성코드 침입을 방어하는 확실한 방법은 애플리케이션 화이트리스트를 작성하는 것이다. 화이트리스트에는 시스템에서 실행할 수 있도록 허용된 것으로 간주하는 애플리케이션에 대한 컴퓨팅 검사 및 기타 “디지털 지문”이 수반되며, 기본적으로 모든 것을 차단하고 코드가 실행되지 못하도록 방지한다.

화이트리스트에 미리 등록되어 있지 않은 공격은 원천적으로 실행될 수 없기 때문에 이 접근방식으로 현재의 위협으로부터 보호할 뿐 아니라 미래의 악성코드를 예방할 수 있다. 엔드포인트 보안을 잘 유지하고 있다 하더라도 알려진 건

전한 애플리케이션에 대한 목록을 확보하고 나머지 모든 것을 차단하는 것이 보안에서는 중요한 구성이 될 것이다.

하지만 여기에 문제가 있다. 모든 사용자들이 정기적으로 사용하는 애플리케이션과 그 변종 버전 및 패치 수준을 보면 프로그램이 수천 개쯤 될 것이며, 윈도우 안에서 내장 소프트웨어 화이트리스트 기능을 이용하려면 이 모든 것을 위한 서명(Signature)을 생성해야 한다. 모든 것을 일일이 생성해야 한다. 자동화된 솔루션이 있지만 라이선스 비용과 관리 시간을 줄여야 한다.

마지막으로 화이트리스트 작성의 경우 사용자 수용 인자가 있다. 사용자는 브라우저 플러그인을 포함해 사전에 허용하지 않은 그 어떤 것도 다운로드할 수 없게 된다. 여기에는 IT 직원들에게 인기가 있는 퓨티(PuTTY)와 같은 사소한 프로그램이나 많은 지식 노동자가 간단한 메모 작성을 위해 다운로드 하는 훌륭한 텍스트 편집기인 노트패드+(Notepad+) 등도 포함된다(이런 프로그램들은 모두 설치가 필요없는 단독 실행 가능 파일이며 시스템 사이에서 이동할 수 있기 때문에 메모리 스틱 또는 USB 저장장치를 통해 동료들 사이에서 자유롭게 공유하는 경우가 많다).

자신과 자사의 IT 팀은 초기의 화이트리스트 정의를 수립할 뿐 아니라 새로운 패치로 디지털 서명이 변경되고 직원들이 새로운 프로그램을 요청하며 추가적인 서비스가 온라인으로 제공될 때에도 지속적으로 유지할 준비가 되어 있는가? 엄청난 작업량이 되겠지만 시스템에서 랜섬웨어의 위협을 없애는 방법 가운데 가장 간단한 방법이기 때문에 핵 옵션(nuclear option)이라고 부르고 싶다. ITWORLD

Solution

2017년 국내 보안 현실과 랜섬웨어에 대응하는 다단계 방어 전략

이성철 이사 | 시스코 코리아 보안 사업부

지금까지의 경계선 중심 보안으로는 진화하는 위협을 막을 수 없다. 성벽을 쌓고 망루 위에서 공격자들이 공격할 때만을 기다리는 보안은 이제 끝이 난 것이다. 이에 따라 가트너는 공격자의 공격 패턴에 따른 심층적 보안을 설파하고 있다. 사이버 보안 분야에서 100% 방어를 장담할 수 없게 된 것은 언제부터인지, 그리고 이런 보안 현실에서 기업들이 갖춰야 할 보안 전략은 무엇인지 살펴보자.

APT 등장으로 100% 방어는 끝났다

수년 전, APT의 등장으로 인해 사이버 보안은 새로운 국면으로 접어들게 됐다. APT는 그 이름만으로도 논란이 많았다.

APT는 DDoS와 같은 특정 공격 방법이 아니며, 웜 바이러스와 같은 불특정 대상을 표적으로 하는 것이 아니고, 공격 형태도 특정된 것이 아니다. 사이버 공격의 피해 사례들을 분석해 본 결과, 기존 사이버 공격과는 다른 형태를 가진 공격들의 공통 분모를 정리해 놓은 것이다. APT는 특정 대상에 대해 교묘하고 지능적인 방법으로 지속적으로 침입을 시도하고 침입 이후 특정 목적을 몰래 달성하는 사이버 공격 행위를 의미한다.

APT 공격이 양산화된 최근에는 방법적인 것보다는 지속적으로 침입을 시도하고 아무도 모르게 목적을 달성한다는 점에 초점을 맞추고 있다. 최근 해킹 사례에서 보듯이 공격자의 침입 경로는 공격 대상의 가장 취약한 부분이었다. 굳이 지능적인 방법을 사용하지 않아도 기업들이 속수무책으로 당하게 된 이유에는 사용자의 취약한 보안 인식을 포함해 여러 가지가 있다.

효율적인 보안을 거론하는 이유

솔루션 측면에서 본다면, 지금까지 기업들은 수많은 포인트 보안 솔루션들을 도입, 사용하고 있는데, 문제는 이를 제대로 활용하지 못한다는 점이다. 사이버 보안 사고가 발생하면 유행처럼 해당 솔루션을 도입하지만 이를 100% 활용하는 기업은 그리 많지 않다.

사실 이는 국내 기업만의 문제가 아니다. 포천 500대 기업이 도입한 보안 제품의 수는 평균 48~50개에 이른다. 이는 한 기업이 48개의 콘솔과 수십 곳의

보안 솔루션 업체와 함께 한다는 의미이기도 하다.

사고가 발생하면 피해 기업은 수많은 보안업체와 함께 사고 원인과 대책들을 분석하고 조치를 취해야 하는 커다란 문제에 봉착했다. 매니지드 보안 서비스 업체와 계약을 맺고 있더라도 해당 담당자가 수많은 업체와 접촉해야 하는 현실은 변함이 없다. 특히 보안업체들은 사고 원인을 분석하는 것보다 자사의 솔루션이 잘못 없음을 입증하는데 초점을 맞춘다. 그래서 사고 대책은커녕 원인 분석조차 힘들어진다.

이런 경우 기업 보안 담당자와 관제 담당자가 원인 분석, 조치, 재발 방지책 등을 내놓게 되는데, 대부분 합의 중재안을 제시하게 된다. 결국 사고에 대한 진정한 원인 분석과 조치를 취할 수 없다.

이와 함께 어떤 기업도 보안에 대해 무한정의 예산과 자원을 투자하는 경우는 없다. 보안 관리자 입장에서는 한정된 예산과 자원으로 다양하고도 끊임없는 공격들을 방어해야 하는 상황이기 때문에 가장 효율적인 방어 전략을 구현하는 것이 당면 과제가 됐다.

보안 제품 선정을 위한 보안 담당자의 선택 기준

국내 보안 현실은 전세계 보안 상황과는 괴리가 있다. 우선 기업에서 보안 솔루션을 도입하는 것부터 문제가 있다. 기업에서 보안 제품을 도입할 때 보안 업체 간 BMT를 실시하게 된다. 이때 사용하는 테스트 계측기가 있는데, 보통 특정 공격 패턴을 넣어 이를 막으면 O, 못 막으면 X로 판정한다.

문제는 각 보안업체가 데이터 규모별로 최적화되어 있는, 해당 계측기에 맞는 BMT용 머신을 갖고 참여한다는 점이다. 해당 기업의 실제 환경이나, 적어도 실제 환경에 준하는 환경에서 위협이 되는 공격을 탐지하고 차단하는 것이 아니라 계측기에 최적화된 BMT를 하는 셈이다. 상황이 그렇다보니 BMT 점수가 해당 제품의 성능이 아니라는 것을 모두들 잘 알고 있으며, 이로 인해 기업에서는 솔루션을 선택하는데 다른 요소가 많이 개입된다.

앞으로 기업들이 IoT 기기들을 도입, 확장하면 엄청난 양의 데이터와 로그 기록들이 발생하게 되는데, 실제 위협에 초점을 맞춰 보안 솔루션을 준비하지 않으면 엄청난 문제에 직면하게 될 것은 자명하다. 기업 보안 담당자들이 자사에 도움이 될 수 있는 보안 솔루션을 도입하기 위해서는 다음과 같은 사항을 체크해야 한다.

- 실시간 위협 분석 시스템을 보유하고 있는가
- 실제 환경, 실제 환경에 준하는 환경에서 실행되는 제품을 구매하고 있는가
- 실제적으로 위협을 차단하는 솔루션을 구매하고 있는가, 아니면 예산에 맞는 제품을 구매하고 있는가
- 입찰 기준이 최저가 기준인가, 보안 효과 기준인가

2%를 막기 위한 샌드박스의 등장과 한계

일반적으로 침입의 98%는 기존의 시그니처 기반 보안 솔루션으로도 충분히 막을 수 있다. 하지만 알려지지 않은 악성코드, 의심스러운 파일을 통한 공격에는 허점을 보일 수밖에 없는데, 이를 해결하고자 등장한 것이 샌드박스다.

기존에 알려지지 않은 파일들, 의심스러운 파일들을 샌드박스 내에서 우선 실행한다는 개념이 처음 등장했을 때에는 굉장히 혁신적이고 파괴적인 기술이었다. 샌드박스의 초기 형태는 기업 내에 들어오는 의심스러운 파일들을 모두 샌드박스에 넣어 실행, 분석해보는 것이었다. 이런 방식은 공격 수가 그리 많지 않았던 초기 APT 상황에서는 충분히 가능했다. 하지만 트래픽은 기하급수적으로 증가하고 의심스러운 파일 수가 폭증한 시점에서는 그리 효율적인 방법이 되지 못했다.

샌드박스는 일종의 클라우드 방식으로 전세계 고객들을 대상으로 패턴 데이터를 주고받음으로써 최신 정보를 신속하게 제공한다는 게 장점이었다.

문제는 오탐이나 과탐이 많다는 것이다. 특히 주요 샌드박스 솔루션들은 탐지 이후 필요한 조치나 실행은 모두 백신업체에게 맡겼다. 또한 샌드박스는 파일을 분석하는 시점에서 해당 파일이 악성코드인지, 정상파일인지를 파악한다. 정상 판정 이후 해당 파일들을 추적하는 기능이 없다는 한계가 있었다.

이런 점을 악용해 특정 시점에서만 탐지하는 샌드박스를 회피하고자 일정 시간동안 동작을 중지한 후, 본 서버에서만 작동하는 샌드박스 우회 악성코드가 등장했다. 이후 우회하는 악성코드에 대한 보완점을 가미한 샌드박스가 출시되고 있지만, 또 이를 뛰어넘는 공격 방법이 나타나고 있다. 결국 한 솔루션으로는 APT를 위시한 최근 사이버 위협을 막을 수 없다는 점을 시사하고 있다.

샌드박스 이후의 시대, 지속적 분석과 회귀적 보안

현재 침투 이후 파일을 추적하기 위해서는 포렌식 솔루션이 필요하다. RSA 포렌식 장비의 기본적인 작동 원리는 샌드박스와 동일한데, 이 장비는 기본적으로 네트워크 단에 들어오는 모든 파일을 스토리지에 담는다. 스토리지에 저장된 데이터를 정규화하고 분석하는데 소요되는 시간이 턱없이 길다. 최소 준비하는 데만 2주가 걸리며, 정밀 분석을 하려면 2개월이 걸린다. 그래서 포렌식은 사전, 실시간 탐지 방어라기보다는 사후 분석 솔루션으로 이용되는 것이다. 이러한 한계를 극복하기 위해 등장한 것이 지속적 분석과 회귀적 보안이다.

지속적 분석과 회귀적 보안은 파일이 네트워크로 들어온 후에는 파일 성향에 관계없이 지속적으로 활동을 감시하고 분석하고 기록한

다. 이후 악의적인 행동이 포착되면 보안 팀에 악성코드의 출처, 상주 위치, 활동에 대해 알리는 회귀적 알림을 보낸다. 그러면 사용자는 클릭 몇 번으로 악성코드를 억제하고 치료할 수 있다.

전체적으로 제시되는 것은 네트워크 각 단계에서 탐지와 차단, 조치를 취해야 한다는 다단계 방어 전략이다. 시스코의 경우, DNS에서부터 파이어월, IPS, 엔드포인트에 이르기까지 각 단계에서 클라우드 상의 샌드박스(탈로스(Talos) 실시간 위협 분석 시스템)를 통해 하루에 150TB 용량을 분석하는 실시간 위협 분석 시스템을 보유하고 있다. 특히 DNS 단계에서는 IP를 기반으로 차단하는데, C2 서버와 통신하는 에이전트를 화이트리스팅 방식으로 차단하게 되어 원천적으로 봉쇄할 수 있다. 파이어월이나 IPS, 이메일 차단 솔루션, 엔드포인트에서도 각 단계의 방식대로 공격을 차단한다.

랜섬웨어 대응 방안, 다단계 방어 전략

사실 랜섬웨어는 주된 침입 경로가 웹과 이메일이다. 침입 방법이나 형태에 있어서는 기존 악성코드와 별다른 차이가 없다. 하지만 랜섬웨어의 선구자 격인 크립토록커(CryptoLocker)와 크립토월(CryptoWall)이 강력한 파일 암호화를 사용하기 시작하면서 악성코드의 효력을 완전히 새로운 차원으로 끌어올렸다. 침입 이후 파일들을 암호화시켜 이를 푸는 대가를 비트코인으로 지불하라고 요구하는 것인데, 이 범죄 시장이 엄청나게 확산되고 있는 실정이다.

그런데 기존 악성코드를 막는 보안 장비를 갖추고도 랜섬웨어를 막지 못하는 이유는 무엇일까? 기존 보안 장비들은 일반적으로 98% 위협에 초점을 맞추고 있어 1~2%의 진화하는 위협을 막을 수 있는 방안이 없다.

진화하는 위협을 막기 위해서는 앞서 설명했던 DNS에서부터 파이어월, IPS, 이메일 솔루션, 그리고 엔드포인트 보안까지 다단계 방어 전략이 필요하다. 그러나 이런 전략에도 불구하고 100% 막지 못하는 상황이 발생한다. 공격 후 조치가 필요한 이유가 바로 이 때문이다. 100% 막을 수 없다면 피해를 최소화하는 방안이 중요하다.

'해킹은 일어날 수 밖에 없다'는 것을 전제로 가트너가 제시한 보안 전략은 공격자의 모든 행동, 즉 공격 전, 공격 중, 공격 후의 프로세스 전 과정에서 지속적으로 탐지, 확인, 추적, 분석, 치료하자는 '엔드 투 엔드 킬 체인(Kill Chain)' 개념이다. 공격 전, 중, 후 기업에서 필요한 보안 기능은 다음과 같다.

- **공격 전** : 최고의 글로벌 위협 인텔리전스를 이용해 공격을 사전에 방어
- **공격 중** : 인텔리전스, 알려진 파일 시그니처, 동적 파일 분석 기술을 이용해 알려진 악성코드, 정책 위반 파일 유형, 네트워크로 침입을 시도하는 통신 등을 차단하고 가시성 확보를 통해 감염 여부 판단과 감염 원인 추적
- **공격 후** : 1차 방어선을 우회하는 위협에 대해 파일 및 네트워크 트래픽을 지속적으로 추적, 분석하고, 감염을 차단하고 공격자의 활동과 행동을 가시화

시스코 AMP(Advanced Malware Protection)는 APT와 같은 지속적인 위협 공격에 효과적으로 대응할 수 있는 솔루션으로 전방위적으로 위협을 신속하게 찾아내고 대응하며, 빠르게 복구한다. APT 솔루션인 AMP는 악성 파일과 트래픽이 방어 지점을 통과한 후에도 경계를 늦추지 않고 모든 파일들의 움직임을 기록하고 분석한다. 해당 파일이 악성으로 밝혀질 경우, AMP는 보안 담당자에게 위협에 대한 분석과 그 출처와 현재 위치에서, 무엇을 하고 있는 지에 대한 이력을 알려준다. 또한 기업 내부에서 실행된 모든 파일에서 실행빈도가 가장 낮은 것부터 가장 높은 순으로 표시해 보여줘 표적 공격도 확인할 수 있다. ITWORLD