1. 하드웨어 장치의 악성코드 감염

최근 주요 하드웨어 공급업체의 드라이버 취약점을 악용해 보안 문제의 심각성이 두드러지고 있습니다. 하드웨어 드라이버는 특정 유형의 하드웨어 장치를 제어하여 운영체제와 올바르게 통신하는 데 도움이 되는 소프트웨어 프로그램을 의미합니다. 공격자가 드라이버 취약점을 이용할 경우, 시스템을 손상시킨 후 사이버 공격의 지속성을 유지하는데 가장 핵심적인 역할을 하는 부분이기에 백도어 및 강력한 공격이 지속 가능합니다. 이러한 공격에 따라 그래픽 카드, 네트워크 어댑터, 하드 드라이브 및 기타 장치와 상호 작용하여 장치 내의 악성코드가 네트워크를 통해 저장되고 표시되고 전송된 데이터를 읽고 쓰고 리다이렉션 할 수 있을뿐더러, DoS 또는 랜섬웨어 공격으로 모든 장치가 비활성화될 수도 있습니다.

카스퍼스키 보고서에 따르면, 대기업의 경우 가장 많은 피해를 초래한 보안 사고가 회사 소유 장치 악성코드 감염 사고라고 합니다.

더불어, 사이버 공격자는 조직이 신뢰하는 관리 도구를 공격에 사용하고, 보안 통제를 피해 백업 기능을 마비시키는 등 최단 시간에 최대 피해를 입히는 것을 목표로 함에 따라 자동화된 능동형 공격을 통해 공격을 강화하고 있는 것으로 나타났습니다. 이러한 피해를 막기 위한 가장 필요한 대책은 주요 드라이버 공급 업체에 자체적으로 보안 패치를 권고하는 일입니다. 또한 각 기업들은 개인 장치에 적용되는 정책을 검토하여 엄격한 기업 보안 정책을 도입, 적용할 필요성이 있습니다. 기업 스스로 정보자산을 보호하기 위해서는 이러한 과정과 함께 엄격한 권한 관리가 이루어져야 할 것이며, 사용자에게 적합한 보안 솔루션을 제공해야 합니다. 무엇보다 사이버 보안에 대한 정기적인 트레이닝을 통해 직원들의 보안의식을 높여야 할 것입니다.

2. 랜섬웨어의 지능화

2019년의 경우 다른 종류들의 사이버 위협에 가려져 랜섬웨어 공격이 주춤한 것으로 보였으나, 여전히 랜섬웨어로 인한 피해 사례와 경고가 이어졌습니다. 지난해 역시 새로운 유형의 랜섬웨어가 등장함에 따라 자연스레 2018년과 2019년 상반기 유행하던 갠들크랩(GandCrab)과 아나토바(Anatova) 공격은 감소하고 그 자리를 소르디노키비(Sodinokibi)와 넴티(Nemty)가 대체했습니다. 2019년 4월에 발견된 소르디노키비는 갠드크랩과 유사하게 메일 내부에 정상 파일로 위장한 악성 첨부파일의 열람을 유도, 실행된 랜섬웨어가 사용자의 파일을 암호화하여 복호화에 대한 대가로 가상화폐 요구하는 방식의 공격입니다. 한편 넴티는 지난 8월 말 등장한 신종 랜섬웨어로, 사용자들에게 친숙한 도메인의 피싱 메일을 통해 유포되며 소르디노키비와 함께 2019년 4분기 국내에 최다 유포된 랜섬웨어로 꼽힙니다.

테슬라크립트(TeslaCrypt), 심플로커(SimpleLocker), 워너크라이(WannaCry), 낫페트야(NotPetya), 샘샘(SamSam), 류크(Ryuk) 등 지난 5년 동안 발생한 큰 규모의 랜섬웨어 공격 중에서도 초미의 사건이었던 워너크라이, 낫페트야 랜섬웨어 공격은 대규모 기업의 시스템을 마비시키는 등 전 세계 수많은 기업에 막대한 피해를 입혔습니다. 지난해 이 둘의 활

동은 잠잠해진 듯하였으나 변종은 여전히 확산되고 있으며, 같은 유형의 또 다른 공격이 재개한다면 그 피해는 배가 될 것으로 전문가들은 예측합니다.

최근 기승하는 랜섬웨어는 대부분 특정 표적에 맞춤화되어 있고, 샘샘과 류크같이 정교한 컨트롤러에 의해 실시간 운영되는 공격이 증가하고 있는 추세입니다. 이에 따라 2020년도에도 불특정 다수에게 유포되던 랜섬웨어 공격은 점차 감소하여 영향을 받는 조직의 수가 적어지겠지만, 공격자들은 크게 수익을 낼 수 있을만한 기업을 타깃으로 하여 공격 성공률을 높일 것으로 보입니다. 이제는 랜섬웨어 감염 사례 감소가 피해 금액 감소를 뜻하지 않음을 시사하며 사전 대비책 없이 당하는 기업은 수십억 달러에 달하는 지출을 감행해야 할 것입니다.
랜섬웨어 공격 예방을 위한 가장 기본적인 방어책은 모든 중요 데이터를 사전에 분류하여 검증된 최신 백업을 만들어 유지하는 것입니다.

중요한 파일은 3개의 사본을 최소한 2가지 이상의 백업 방법으로 유지해야 하며, 네트워크가 분리된 공간에의 보관은 필수입니다. 더 나아가서는 1. 조기 패치 및 빈번한 패치 2. 이메일 첨부파일 필터링 및 의심스러운 파일 열람 금지 3. 망 분리 정책 적용 4. 배포 즉시 소프트웨어 업데이트 설치 5. 정기적인 로그 검토를 권장합니다.

3. 클라우드 보안 사고
'공유 경제'의 개념과 함께 클라우드 컴퓨팅은 업무 효율성과 비용 절감이라는 측면에서 기업의 서비스 운영에 관한 고민을 해결해주는 존재로 자리 잡았습니다. 대세에 따라 MS, IBM, 오라클 등 대표적인 글로벌 SW 기업은 모두 클라우드 컴퓨팅 서비스를 제공하고 있으며, 산업 전반에 걸쳐 다양하게 활용됨에 따라 그 중요성은 점차 증가하고 있습니다. 클라우드는 사용이 쉽고 유연하게 적용할 수 있는 만큼 보안에도 취약할 수밖에 없는데요. 기존의 APT 공격뿐 아니라 인증 정보 도용, 구성 오류, 클라우드 자체 취약점 등을 이용한 공격이 다양하게 발생할 가능성이 높기 때문입니다.

클라우드 보안 사고 3대 유형으로는 데이터 유출, 계정 탈취 및 손상, 그리고 자원 착취 및 손상과 같은 형태로 분류됩니다. 이에 많은 IT 기관 및 기업에서는 클라우드 보안 이슈에 대응하기 위한 보고서와 발표를 내놓고 있습니다. 대표적으로 최근 CSA(Cloud Security Alliance)가 <클라우드 컴퓨팅에 대한 12가지 주요 위협: 산업 인사이트 보고서>를 통해 발표한 내용에 따르면, 이들은 문제의 대부분이 기술적 문제보다 기술 외적(사람)인 문제라고 언급했습니다. 순수 기술적인 문제로 불거질 수 있는 보안 문제는 시스템 취약성, 지능형 지속 공격, 분산 서비스 거부 공격이며, 기술 외적인 문제는 주로 불충분한 관리와 부주의, 내부자의 도덕적 해이 등이 주원인으로 파악했습니다.

많은 기업이 비즈니스 인프라를 클라우드로 옮겨감에 따라 공격자의 관심 역시 클라우드 환경에 집중될 것으로 예상하며, 올해도 클라우드 보안에 대한 이슈는 끊이지 않을 것으로 보입니다. 클라우드 도입을 앞둔 기업이 명심해야 할 사항은, 클라우드 서비스 제공사와 이용자 간에 책임 공유 의식이 요구된다는 점입니다. 클라우드 서비스 제공사는 데이터, 스토리

지 등 클라우드 인프라 보안을 책임지고, 이용자는 자체 보안 솔루션 구축을 통해 내부 정보 보안을 직접 관리함으로써 양자간 보안 책임이 분산된다는 개념을 인지해야 한다는 것이 전문가들의 공통된 의견입니다. 이용자는 가상 자원 활용과 보안 서비스 등 클라우드 특성을 고려해 효율적이고 안전한 방식으로 클라우드를 도입해야 하며, 보안 책임을 인식하고 도입에 앞서 자사 클라우드 환경에 맞는 보안 아키텍처를 수립해야 할 것입니다.

4. 애플리케이션 취약점

애플리케이션 취약점 항목으로는 인증, 쿠키 및 세션 관리, 접근통제, 입력값 검증, 부적절한 환경설정, 불필요한 파일 존재, 정보보호 등이 있으며 취약점의 종류만 해도 1,000만 개 이상이라고 합니다. 그중 치명적인 취약점이 1개 이상인 앱의 비율이 20%라고 하니, 수 십에서 수 천 개에 이르는 네트워크, 웹, 모바일, ERP, 클라이언트 서버 애플리케이션을 사용하는 기업들은 현재 그 위험에 노출되어 있는 실정입니다. 최근 웹 애플리케이션 해킹사고는 단순한 웹페이지 변조 수준에서 그칠 뿐만 아니라 이를 이용하여 피싱 사이트로 악용하거나 고객의 정보를 유출하여 악용하는 등의 범죄적인 성향으로 발전하고 있습니다.

이러한 애플리케이션 보안을 위한 대응책으로 자주 소프트웨어를 스캔 및 테스트하는 데브섹옵스(DevSecOps) 방식이 취약점 수정에 소요되는 시간을 줄일 것이며 수시로 앱의 취약점을 스캔 및 테스트하여 심각한 취약점을 먼저 고치는 방법이 효과적이라는 분석이 있습니다. 기능 개선만큼 취약점을 찾아 수정하는 활동이 중요해지고 있는 추세이며, 조직들은 보안 취약점을 찾는데 그치지 않고 이를 수정하는 데 초점을 맞춰 위험이 큰 취약점을 우선시하여 처리할 것을 강조합니다.

5. DDoS 공격

DDoS(Distributed Denial of Service) 공격은 다수의 분산된 컴퓨터를 이용하여 특정 서버 컴퓨터가 처리할 수 있는 용량을 초과하는 정보를 한꺼번에 보내, 과부하로 서버가 다운되거나 정상 접속되지 못하도록 만드는 공격을 뜻하는데요.

2019년 DDoS는 SMB에만 평균13만 8,000달러의 피해를 유발했으며, DDoS 공격을 강화시키고자 혁신하는 공격자들이 늘어나고 있다는 것이 업계의 설명입니다. DDoS 공격의 유형으로는 응용 프로그램 계층 공격, 프로토콜 공격, 볼륨 공격으로 나뉩니다.
최근 들어 5G가 확대되고, IoT 장치 수가 증가함에 따라 국가기관, 군사시설, 에너지만 및 금융업계 등 다양한 영역에의 보안 이슈가 대두되고 있습니다. 5G는 스펙상 백만 단위의 기기가 연결 가능하기 때문에 매우 빠른 속도로 악성코드가 전파되거나, 정반대로 감염된 대량의 기기로부터 기지국이 DDoS 공격을 받을 가능성이 높다는 이유 때문인데요. 현재로서는 이러한 신기술의 상용화 단계이기 때문에 보안 관점, 특히 DDoS 공격에 대한 취약성 존재 가능성을 논의하는 목소리가 커지고 있습니다. 대규모 감염된 사물인터넷 단말의 과도한 접속 요청으로 인한 5G RAN DDoS 공격 위협 등에 부합하는 새로운 안전 기준이 필요함에 따라 보안 업계에 또 다른 과제가 주어졌습니다.