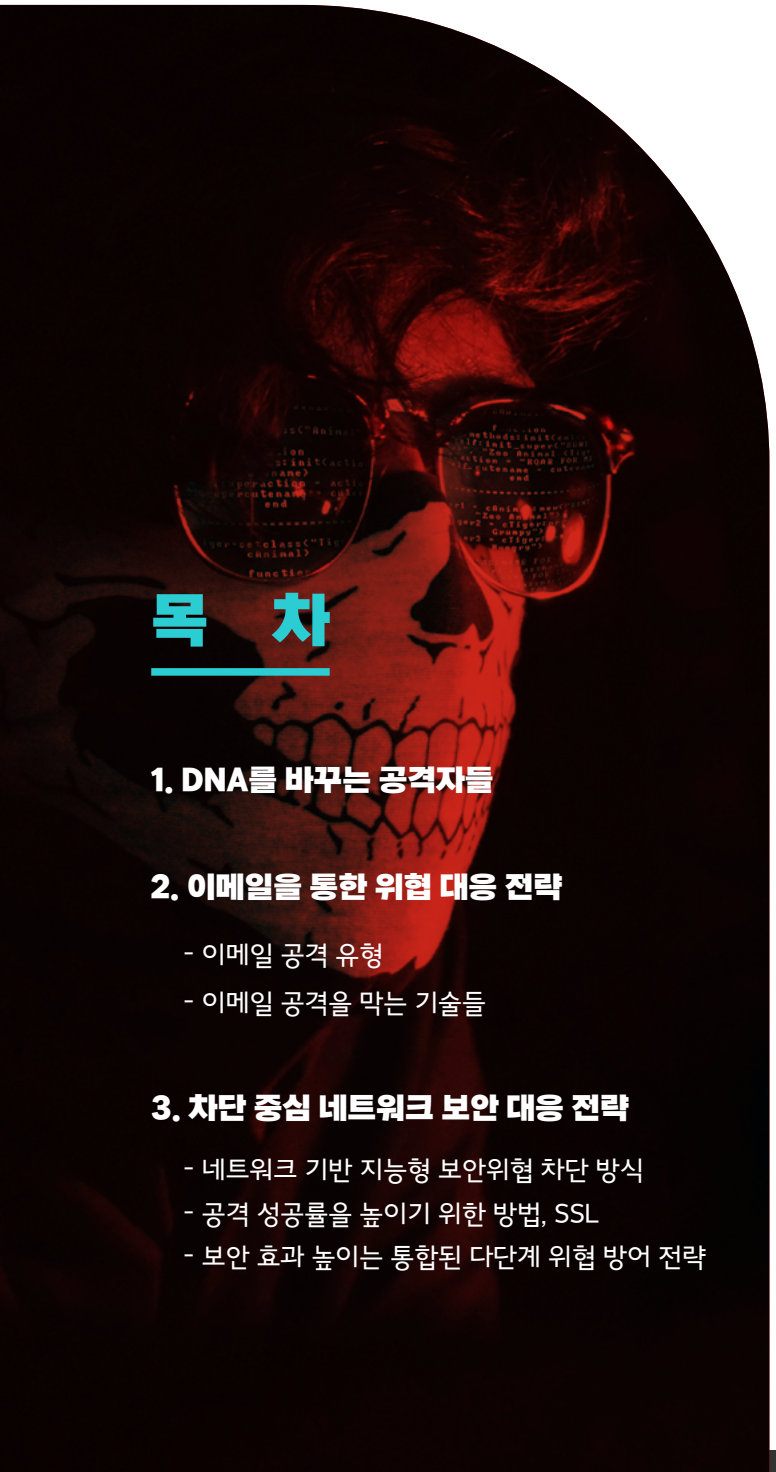
FORTINET

공격자 DNA를 고려한
방어자 중심 전략

special report
Byline Network

공격자 DNA를 고려한

방어자 중심 전략



목 차

더운 여름, 초등학생 자녀를 둔 어느 단란한 가족이 휴가를 보내기 위해 바닷가로 놀러갔다. 해수욕을 즐기기 위해 옷을 갈아입고 곧바로 바다로 향했다. 그런데 아이가 해변 모래사장에서 갑자기 바닷물에 들어가기를 거부하는 일이 발생했다. '해파리'가 무섭다는 이유였다. 얼마전 유튜브에 서 해파리 영상을 보더니, 과도한 공포가 생겨버린 탓이다.

바닷물 속의 조그만 부유물만 보여도 해파리 같다면서 무서워했다. 해파리가 아니라고 말했지만, 이 공포를 쉽사리 걷어내지 못했다.

부모는 즉시 인터넷을 뒤져 해파리 사진과 영상을 찾아 보여줬다. 현재 보이는 부유물들이 해파리가 아닌 것을 확인시켜줬다. 또 해파리를 막기 위한 안전 펜스가 쳐져 있고, 해수욕장 관리요원들이 상시 감시하고 있다는 것을 설명해주며 공포를 최소화하기 위해 노력하자, 아이는 비로소 천천히 발을 물에 담갔다.

사실 이 아이의 공포는 아주 근거 없는 것은 아니다. 바닷가에서 해파리에 쏘이는 피해 사례가 종종 발생한다. 그러나 해파리가 무서워서 여름에 바다로 놀러가는 것을 포기할 수는 없다. 해파리가 어떻게 생겼는지 언제 어느 지역에 많이 출몰하는지 제대로 조사 연구하고 대책을 마련해 관리체계를 강화하면 피서객들이 해파리로 인한 공포에서 벗어나 휴가를 즐길 수 있을 것이다.

악성 해커의 지능형 위협에 대한 조직의 공포도 이와 마찬가지다. 디지털 전환이 가속화될수록, 위협의 범위와 규모가 커지고, 공격 기술이 발전할수록 침해사고에 대한 공포는 커진다. 언론에서는 연일 국내외에서 발생하는

침해사고가 보도된다. 어느 회사는 이메일 사기로 수백억원의 매출이 사라졌고, 어느 회사는 디도스(DDoS) 공격이나 파괴적 악성코드로 비즈니스 인프라가 멈추고 서비스가 중단됐다. 다른 회사는 중요 데이터를 인질로 잡은 랜섬웨어 공격자들의 요구에 굴복해 큰 금액의 뒷돈(암호화폐)을 줬다는 소식이 심심치 않게 전해진다. 공격자들은 점점 지능화되고 있고 은밀하고 정교한 수법을 사용하고 있다며 공포를 부추긴다. 공격자가 오랜 시간을 들여서라도 맘먹고 내부 네트워크에 침입해 원하는 것을 얻으려 한다면 결국 뚫릴 수밖에 없다는 인식도 생겨났다. 실제로 방어자는 시시각각 발생하는 수많은 공격 시도를 막아내더라도 단 한 번만 뚫리면 심각한 피해를 입을 수 있는 '비대칭' 전력 상황에 처해있는 실정이다.

그러나 침해사고가 일어날까 무섭다고 디지털 전환을 멈출 수는 없다. 초등학생 아이가 해파리가 어떻게 생겼는지 공부한 후에 바닷물에 발을 담글 수 있었던 것처럼, 조직도 공격자를 알아야 한다. 공격자 DNA를 고려해야 효과적인 방어 전략을 세울 수 있다. 공격자들의 동향과 기법을 알아야 침해사고에 대한 막연한 공포 없이 디지털 전환 속도를 높일 수 있다. 사실 발생하는 공격의 대부분은 이미 알려진 위협을 이용한다. 공격자가 지능화되고 있다지만 실제로 발견된 지 오래된 취약점과 오래된 악성코드에 당하기도 한다.

DNA를 바꾸는 공격자들

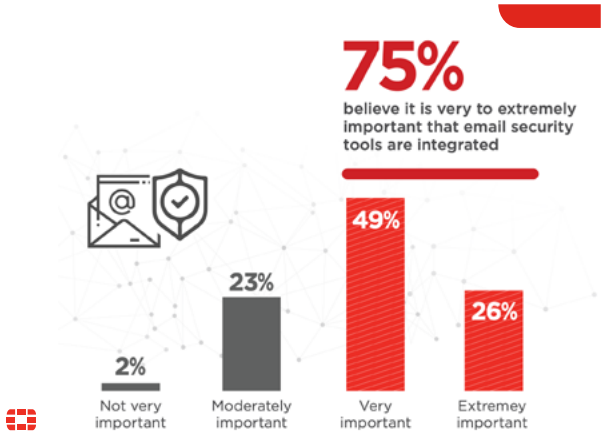
인터넷 초창기 공격자들은 악성코드 실행파일을 이메일 첨부 파일로 보냈다. 하지만 현재 이같은 방법의 공격은 거의 통하지 않는다. 대부분의 조직이 이를 막는 보안 솔루션을 가지고 있기 때문이다.

이제 공격자는 이렇게 단순한 유형의 공격만 하는 것이 아니다. 공격자는 계속 DNA를 바꾸고 있다. 조직에서 방어책을 마련하면 공격자도 이를 우회할 방법을 찾으려는 것이다. 해킹 기술이 진화하고 있지만 모든 공격이 다 지능화된 것은 아니다. 사실 발생하는 공격의 대부분은 이미 알려진 위협을 이용한다. 공격자가 지능화되고 있다지만 실제로 발견된 지 오래된 취약점과 오래된 악성코드에 당하기도 한다. 공격하는 경로도 과거와 크게 다르지 않다.

다만 바뀌고 있는 공격자의 DNA를 고려해 방어자 중심 전략을 세워나간다면 침해사고 위협에서 벗어날 수 있을 것이다.

지능형지속위협(APT, Advanced Persistent Threat)은 공격자들이 흔하게 사용하는 위협이다. 조직 내부망 침투를 위한 다양한 공격 경로와 전략·기술·절차(TTP)를 모두 동원한다. 최근에는 랜섬웨어, 디도스, 정보 유출 공격을 결합시켜 피해 확산을 통해 사회적 문제로 대두되기도 했다. 하지만 APT 역시 많은 사례와 정보 공유를 통해 이제는 대처할 수 있는 위협이 됐다. 이제는 APT에 대한 공포에 떨기 보다는 발견됐던 다양한 유형의 공격 사례를 학습하고, 그에 대처할 수 있는 방어전략을 마련하는 것이 중요하다. 이런 APT 공격을 막기 위한 솔루션으로 지능형위협보호(ATP)가 있다.

APT의 공격 경로는 크게 이메일과 네트워크로 구분된다. 이를 막기 위한 ATP 솔루션의 기능도 크게 이메일 방어와 네트워크 방어로 나뉜다.



[그림 1] 이메일 보안을 중요하게 생각한다 (출처: 사이버 시큐리티 2022)

이메일을 통한 대응전략

이메일은 공격자들이 가장 주목하는 채널이다. 이메일은 다른 채널에 비해 상대적으로 보호 장치가 많지 않기 때문이다. 특히 사용자의 심리를 이용하거나 부주의한 지점을 파고드는 것이 공격의 포인트다.

이메일 공격 유형

1 알려진 악성코드 불특정 다수 배포

공격자들은 공격할 대상을 특정하지 않고 알려진 악성코드를 불특정 다수에게 배포할 때가 있다. 첨부파일을 통해 악성코드를 배포하기도 하고, 이메일의 링크를 클릭하면 악성코드가 설치되도록 하는 방식을 취하기도 한다. 사실 어느정도 체계가 갖춰진 조직이라면 알려진 악성코드 공격에 피해를 입지는 않는다. 백신과 같은 기존의 보안 솔루션들이 알려진 악성코드를 차단하기 때문이다. 그러나 기본적인 보안조치도 취하지 않은 가정의 PC는 이같은 공격에도 좀비PC가 되거나 랜섬웨어에 감염될 수 있다.

2 스피어피싱

스피어피싱은 특정인을 겨냥한 공격을 의미한다. 공격자는 이메일 수신자의 지인으로 위장해서 악성코드가 삽입된 첨부파일이나 악성코드 링크를 송신한다. 스피어피싱 공격의 경우 대부분 알려지지 않은 악성코드를 사용한다. 공격자들은 기존 악성코드를 변조한 후 백신 솔루션에서 필터링이 되는지 여부를 체크해가면서 공격을 준비한다. 이런 공격들은 시그니처로 차단이 되지 않기 때문에 행위분석을 통해 피해를 막아야 한다.

3 사기메일

금융감독원의 2020년 발표에 따르면 국내에서 2600건의 사기메일 공격이 있었고, 피해금액은 1370억원에 달했다. 사기 메일의 특징은 기계적으로는 위협임을 알기 어렵다는 점이다. 예를 들어 공격자들은 회사 내 계약 관련 담당자에게 계약이 취소됐다는 내용의 제목으로 메일을 보낸다.

겉으로 볼 때는 평범한 비즈니스 이메일이다. 계약이 취소됐다는 소식을 들은 이용자는 당연히 첨부파일을 열어볼 것이다. 이용자가 첨부파일을 여는 순간 악성코드에 감염될 수 있다. 과거에는 직접 실행파일을 첨부해서 눈치 빠른 이용자가 위협을 감지할 수라도 있었는데, 이제는 PDF 문서 내에 숨겨놓는 경우가 많다. 이용자가 PDF 뷰어 등의 응용프로그램을 실행하게 되면 이게 트리거가 돼서 오브젝트 형태로 숨겨져 있던 악성코드가 실행된다. 또는 송금계좌가 바뀌었다는 사기 이메일을 보내서 송금을 유도하기도 한다.

4 매크로공격

전세계적으로 악명을 떨친 이모텟 공격이라고 있다. 일각에서는 사상 최악의 멀웨어라고 표현하기도 한다. 일반적으로 이모텟은 악성 매크로에 여러가지 URL을 심어놓고 파일을 전송할 때 암호화해서 보낸다. 암호화 덕분에 여러가지 보안장비를 우회할 수 있고, 사용자들이 암호화를 풀고 매크로를 실행할 때 포함된 URL을 통해 악성파일이 다운로드 된다.

5 아웃바운드

일반적으로 공격을 막는다는 표현을 들으면 외부에서 조직 안으로 침입하는 것만 생각을 하게 된다. 그러나 때로는 조직 내부의 감염된 매체가 외부로 악성 이메일을 발송하는 경우도 있다. 인바운드 공격과 함께 아웃바운드도 막아야 하는 대상이다. 특히 최근 모 식품회사 일본 지사에서는 사내에 감염된 PC를 통해 직원으로 위장해 악성코드가 배포돼 문제가 됐던 적이 있다.

지난 해 한 공공기관에서는 외부 심사위원에게 보낸 이메일에 포함된 개인정보가 유출되는 사례가 있었다. 이 심사위원의 이메일이 악성코드에 감염돼 있었던 것이다. 외부의 개인 이메일로 회사의 정보가 담긴 이메일을 보낼 때가 있는데, 아무런 악의가 없는 행동이지만 결과적으로 내부 정보를 유출하는 경우가 생긴다.

이메일 공격을 막는 기술들

01 샌드박스를 통한 알려지지 않은 위협 대응

샌드박스는 가장 널리 사용되는 이메일 보안 방안이다. 이메일 수신자가 URL을 클릭하거나 첨부파일을 내려 받았을 경우 해당 URL이나 첨부파일을 샌드박스로 전송, 그곳에서 안전성 여부를 테스트하는 방식이다. 샌드박스는 보안 분야에서는 다소 고전적인 기술이지만, 이메일 보안을 위해서는 여전히 유용하고 필수적인 보안방법이라고 볼 수 있다.

02 CDR(Content Disarm & Reconstruction, 콘텐츠 무해화)

최근에는 공격자들이 실행파일을 직접 첨부하지 않고, 일반적인 문서 내에 숨겨서 전송하는 경우가 많다. 이메일 수신자가 첨부파일을 열면 그제서야 매크로를 통해 악성행위들이 일어나거나, 첨부파일 내의 URL을 통해 악성코드를 배포하는 방식이다.

이처럼 정해진 형태가 아닌 첨부파일을 모두 제거하거나 URL의 하이퍼링크를 삭제해서, 이용자가 이메일을 열면 순수 텍스트만 보게 할 수도 있다. 첨부파일에 매크로가 들어있으면 차단이 되는 방식을 택하기도 한다. 이런 기술을 CDR이라고 부른다.

물론 이런 경우 일부 이용자가 불편을 겪을 수도 있다. 예를 들어 엑셀에서 매크로를 꼭 써야하는 업무가 존재한다. 하지만 매크로 기능이 필요한 직원은 소수에 불과하다. 이런 경우 정해진 소수만 매크로를 허용하고, 나머지는 모두 삭제하는 방식을 택하기도 한다.

03 BEC(Business Email Compromise, 사기 이메일) 탐지

BEC는 겉으로 볼 때는 100% 정상적인 이메일이다. BEC 공격은 악성코드를 사용하지 않고 사회공학적인 방법을 사용하기 때문에 일반적인 보안 소프트웨어로는 감지되지 않는다. 거래처를 위장해 가짜 송장을 보내거나, CEO를 가장해 계좌변경을 요구하는 식이다. 겉으로는 매우 정상적인 이메일인데 결과적으로는 엉뚱한 가상계좌에 송금을 하는 기업들이 적지 않았다. 수신자가 송신자를 주의 깊게 보지 않으면 알아채기 어렵다.

BEC를 탐지하기 위해서는 발신자를 분석해야 한다. 발신자가 주로 위변조 되는 이메일 주소가 아닌지 모니터링 하고, 신규 이메일 주소나 새로운 패턴의 이메일이 수신됐을 때는 혹시 BEC가 아닌지 다시 한번 확인하는 프로세스를 만들어야 한다.

04 URL 클릭 보호

일부 공격은 시간차 공격을 하기도 한다. 기업들이 샌드박스 등의 보안장비를 통해 URL을 검증하는 것을 역이용하는 방식이다. 샌드박스는 이메일이 메일서버에 수신되면 안전한 장비에서 URL을 클릭해보고 악성코드를 배포하는지 여부를 살펴본다. 이때 이상이 없으면 사용자의 수신함에 이메일을 보내주고, 사용자는 의심없이 URL을 클릭한다.

그러나 시간차 공격은 일정 시간 이후에 작동하는 경우가 있다. 샌드박스에서 테스트할 때는 정상적인 URL이었는데, 이용자가 클릭할 때는 악성코드를 배포하는 웹페이지로 변하는 것이다. 이런 부분 역시 탐지하는 것이 쉽지 않다.

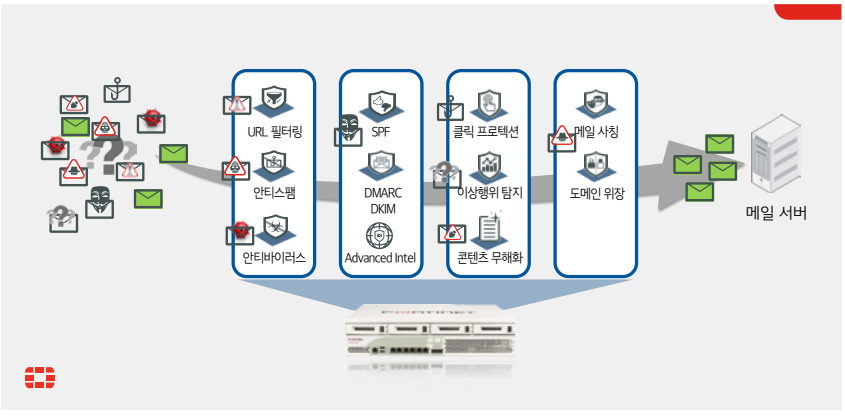
이를 막기 위한 기술로는 이용자가 URL을 클릭하는 순간 그 웹사이트를 열지 않고, 다시 한번 보안장비로 이동해 URL의 위협검사를 실시하는 방법이 있다. 1차적으로 샌드박스를 통과한 URL이라고 하더라도 이용자가 클릭할 때 다시 검사를 하기 때문에 시간차 공격도 막을 수 있다.

05 데이터 유출 탐지

밖으로 내보내는 이메일에 혹시 조직 내부의 영업기밀이나 중요한 문서가 포함돼 있지 않은지 탐지하는 기술이다. 조직이 외부로 나가지 않도록 중요 문서를 등록해 놓고 아웃바운드 이메일에 첨부된 문서가 중요 문서로 등록된 것인지 아닌지 매칭한다. 또는 정규식을 이용해서 고객의 개인정보나 금융정보 등이 외부로 나가지 않도록 차단할 수도 있다.

이메일은 가장 흔하게 사용되는 비즈니스 커뮤니케이션 채널이기 때문에 공격자의 타깃이 되기 쉽다. 반면 모든 부서가 사용하기 때문에 일관된 보안 정책을 적용하기도 쉽지 않다. 일부 부서는 모든 URL과 첨부파일을 없애버리는 극단적인 정책이 필요하기도 하고 일부 부서는 매크로를 허용해야 하는 상황도 있다. 이 때문에 이메일 보안 솔루션은 이런 다양한 요구에 맞게 정책설정을 할 수 있어야 한다.

이메일 공격은 워낙 보편적인 방법이고 위협적이기 때문에 필요에 따라 이메일 보안 솔루션이 계속 늘어나는 경우도 있다. 하지만 여러 개의 보안 솔루션을 사용할 경우 보안정책을 관리하는 것이 어려워진다. 이 때문에 이메일 보안을 위해 통합위협관리(UTM) 보안 솔루션을 활용하는 것이 비용으로나 보안성 면에서도 합리적이라고 볼 수 있다.



차단 중심 네트워크 보안 대응 전략

조직의 내부 네트워크로 유입되는 사이버공격의 양이 엄청나게 많아지면서 탐지되는 이벤트와 로그를 자동 분석해 효과적으로 차단해야 할 필요성이 커지고 있다. 실제로 발생한 보안 사고를 분석해보면, 운용 중인 보안 솔루션에서 위협을 탐지했음에도 대량의 고객정보가 유출되는 피해를 입는 사례가 꽤 많이 있다. 여러 보안 솔루션을 운용하고 있고, 보안 장비가 위협을 탐지했음에도 피해를 막지 못한다면 보안체계가 제대로 작동한다고 볼 수 없다. 보안 투자는 많이 했는데 침해사고는 피하지 못하는 형국이다.

위협이 지능화되면서 네트워크단에서 대응하는 방식도 변화하고 있다. 대표적인 네트워크 차단 시스템인 방화벽은 차세대 방화벽으로 진화하면서 애플리케이션(앱) 제어, URL 필터링, 안티바이러스 등의 기능을 모두 지원해 위협 대응 범위와 기능이 보다 넓어졌다.

네트워크 기반 지능형 보안위협 차단 방식

네트워크 보안 솔루션이 위협을 차단하는 방식을 살펴보면, 과거에는 시그니처와 매칭되는 위협들을 인라인으로 설치된 장비에서 탐지 즉시 실시간 차단하는 방식을 많이 활용했다. 방화벽, 침입방지시스템(IPS), 바이러스월(안티바이러스) 등이 대표적이다. 시간이 가면서 신·변종 악성코드가 출몰하고 점차 시그니처 기반 차단 방식의 한계가 노출되면서 APT를 가상 행위 기반 위협 분석솔루션(샌드박스)과 연동해 차단하는 방식이 등장했다. 바로 ATP 솔루션이다.

샌드박스는 가상 환경에서 의심스러운 파일의 위협 여부를 분석하는데 보통 1분에서 3분이 소요된다. 분석 결과가 나올 때까지는 네트워크 트래픽을 보낼 수 없기 때문에 자칫 웹서비스가 느려지거나 중단될 수 있다. 그 이유로 샌드박스는 인라인 설치가 가능하지만 대부분 미러링 형태로 구성하고 있다. 위협을 탐지한 뒤 차단하기 위해 인라인으로 설치돼 있는 웹 프록시(보안 웹 게이트웨이)나 방화벽(네트워크 보안 게이트웨이) 장비와 연동하는 방법을 활용하고 있다.

예를 들어, 포티넷의 네트워크 보안(차세대 방화벽) 장비인 '포티게이트(ForiGate)'는 방화벽, 가상사설망(VPN), 앱 제어, IPS, 안티바이러스, URL 필터링, 샌드박스 분석 등의 기능이 모두 지원되는 ATP 솔루션이다. 네트워크를 통과하는 모든 L2~L7 트래픽을 검사한다. 통합 네트워크 보안 솔루션에서 제공되는 안티바이스(AV)·IPS·웹방화벽·SSL 검사 등으로 1차 필터링을 거친 후, 의심스러운 파일을 샌드박스로 보내 분석한 결과를 토대로 시그니처를 생성·업데이트해 자동 차단한다.

이 과정에서 최초의 의심스러운 트래픽은 통과될 수밖에 없다. 위협으로 판별된 뒤 업데이트가 완료되면, 이후 침입하는 동일한 위협은 실시간 차단하게 된다.

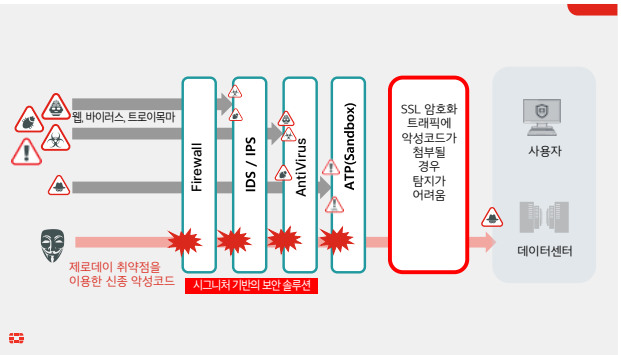
샌드박스에서 'TCP-리셋(Reset)' 기능을 사용해 자체적으로 위협 차단 기능을 수행할 수도 있다. 샌드박스와 네트워크 차단 솔루션을 상호 호환성이 부족한 여러 제조사의 이기종 보안 제품으로 운영할 경우에 활용할 수 있다. 이 방식은 실제 세션이 연결돼 있을 때 'TCP-리셋' 패킷을 보내 세션을 끊어 위협 유입을 차단하는 효과를 가져올 수 있다. 특정 웹사이트에서 악성코드 다운로드를 시도하거나 외부의 명령제어(C&C) 시스템 접속을 시도할 경우 세션을 바로 끊어버릴 수 있다. 하지만 이 경우도 네트워크 구조가 복잡한 경우 리셋 패킷이 제대로 도달하지 못할 수 있고, 보안 장비의 리소스가 많이 사용될 경우 우선순위가 떨어져 리셋 수행이 뒤늦게 이뤄질 수 있다는 한계가 있다.

공격 성공률을 높이기 위한 방법, SSL

사이버위협이 다양화, 지능화되면서 사용되는 보안 솔루션의 수도 많아졌다. 공격자들은 이들 솔루션에 의한 탐지를 우회하기 위해 최근 들어 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 암호화를 흔하게 사용하고 있다. APT 공격 트래픽의 80%, 전체 네트워크 트래픽의 50%가 SSL 트래픽이라는 조사결과도 있다.

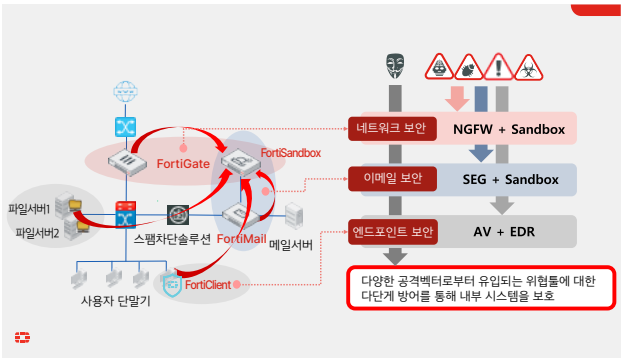
시그니처 기반 보안 솔루션으로 차단할 수 있는 알려진 악성코드가 SSL 암호화 트래픽에 첨부될 경우 SSL 복호화 기술이 탑재되지 않은 네트워크 보안 솔루션으로는 악성코드 탐지가 불가능하다.

이로 인해 SSL 가시성 솔루션 수요도 크게 증가했다. SSL 트래픽 복호화에는 많은 시스템 자원이 소요되기 때문에 보안 장비에 SSL 복호화 기능이 탑재된 경우 성능 저하 현상이 발생할 수 있어 이를 고려해 대책을 마련해야 한다.



보안 효과 높이는 통합된 다단계 위협 방어 전략

공격자들은 엔드포인트, 이메일, 네트워크, 클라우드 등 다양한 공격 경로를 이용한다. 사물인터넷(IoT)과 클라우드, 원격·재택근무 환경 확대로 인해 보호해야 할 범위도 계속 넓어지고 있다. 조직은 엔드포인트 보안, 이메일 보안, 네트워크 보안, 클라우드 보안 등 점점 확대되는 모든 영역을 지원하는 다양한 개별 보안 솔루션을 운영하고 있다.



이같은 환경은 오히려 보안 복잡성을 높이고 운영관리 부담만 커져 보안 효과를 떨어뜨릴 수 있다. 한정된 보안 인력으로 수많은 보안 솔루션에 접속해 이벤트와 로그를 확인하고 분석해 치명적인 위협을 가려내고 차단 정책을 적용하는 것이 쉬운 일은 아니다. 공격자는 이러한 운영환경에서 생겨나는 크고 작은 허점을 파고든다.

보안 위협대응 수준은 높이고 보안 복잡성은 단순화하면서 보안담당자들의 운영관리 부담을 덜어줄 수 있는 방법으로 포티넷은 다단계 위협 방어가 가능한 통합된 접근방식을 제시한다. 바로 '포티넷 시큐리티 패브릭(Security Fabric)' 아키텍처가 구현하는 방식이다.

시큐리티 패브릭은 차세대방화벽과 웹과 이메일 보안, AV, 엔드포인트 위협 탐지대응(EDR)과 샌드박스 등 모든 포티넷 제품군을 서로 연계해 모든 경로에 설치된 제품에서 탐지·분석한 위협 인텔리전스 정보를 서로 공유해 자동 대응하는 통합보안 아키텍처이다.

각각의 보안 솔루션에서 분석된 정보를 보안담당자가 일일이 개별 솔루션에 접속해 위협 차단 정책을 적용하지 않더라도 조직의 인프라 환경 내에 있는 모든 보안 솔루션에 '자동 업데이트, 자동 차단'이 가능한 환경을 구성할 수 있다.

포티넷 시큐리티 패브릭에서 핵심 역할을 하는 '포티게이트'는 단일 플랫폼에서 다양한 보안 기능을 제공하고 중앙집중식 보안관리도 수행해 조직의 보안운영을 간소화할 수 있도록 지원한다. BN

FORTINET 포티넷코리아
서울특별시 강남구 영동대로 325 에스타워(구 해암빌딩) 14/15층 T. 080-559-8989 E. kr-callcenter@fortinet.com W. https://www.fortinet.com/kr
페이스북. https://www.facebook.com/Fortinet 링크드인. https://www.linkedin.com/company/fortinet/
유튜브. https://www.youtube.com/channel/UCAoOBpYtHFaCkmCRPmNsnHA

Byline Network 바이라인네트워크
서울특별시 마포구 토정로5길 30 2층
전화: 02-761-1928 이메일: byline@byline.network 취재/글 : 이유지 기자 yjlee@byline.network