최신 사이버 보안위협
사전 탐지·차단 전략

INSEC security

OPSWAT

paloalto NETWORKS

By 바이라인네트워크

SPECIAL REPORT

세상을 위협하는

글로벌 사이버보안 트렌드 6선

미국 실리콘밸리 사이버보안 전문업체인 옵스왓(OPSWAT)의 고태일 최고기술책임자(CTO)는 10월 17일 서울 콘래드 호텔에서 열린 '최신 사이버 보안 위협 사전 탐지 및 차단 전략 세미나'에서 최신 보안 위협 트렌드를 발표했다.

고 CTO가 선정한 보안 위협 트렌드는 ▲국가 지원을 받는 해킹▲빠르게 진화하는 악성코드 ▲공개된 취약점(CVE) 증가 ▲효과적이고 성공적인 악성코드 채널 이메일과 피싱 ▲모든 것의 시작(PUA) ▲컴플라이언스 강화 등이다. 고 CTO의 입을 통해 글로벌 보안 위협 트렌드를 살펴본다.

◀ 글로벌 보안 위협 트렌드에 대해 연설하는 고태일 옵스왓 CTO

01

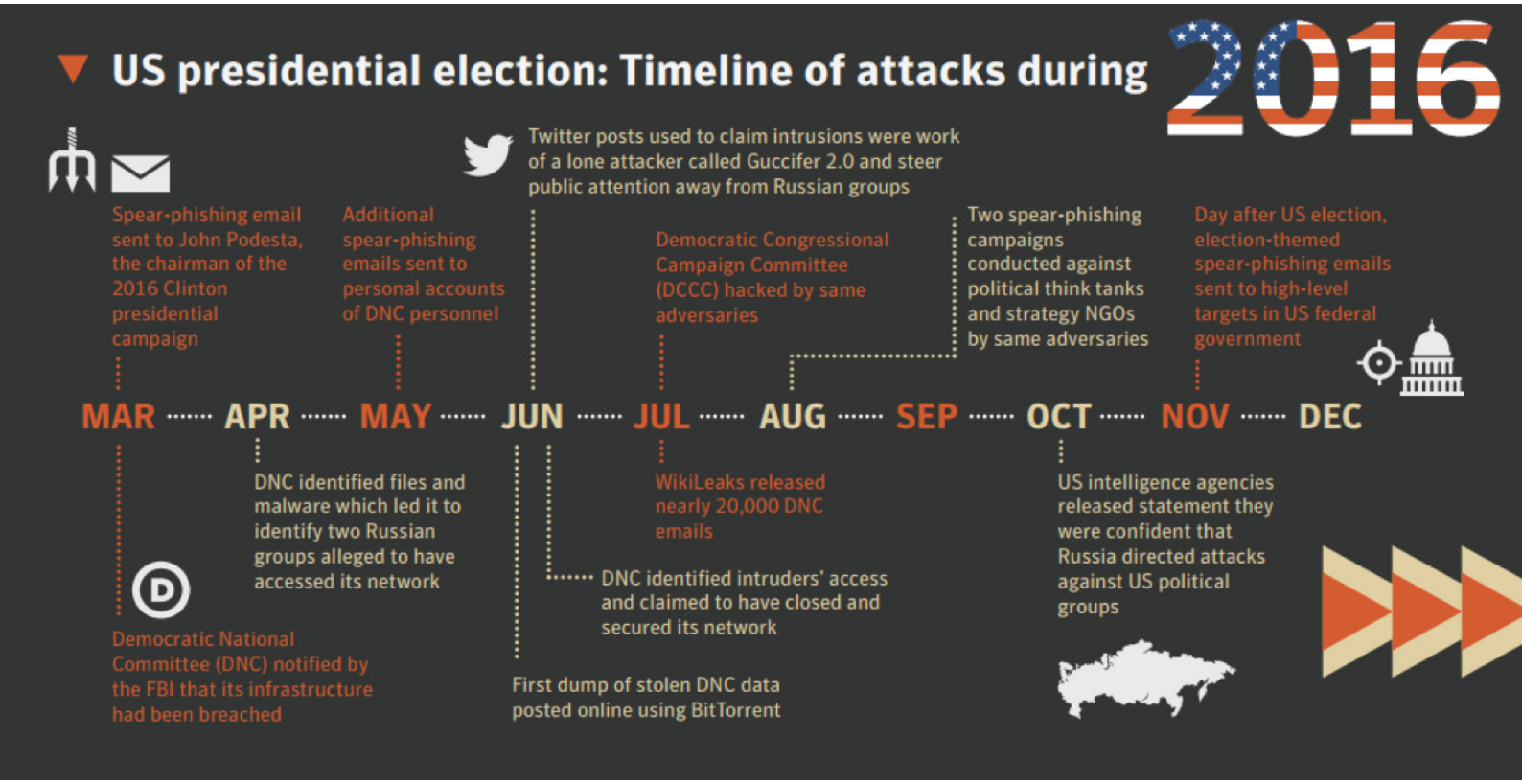
국가 지원을 받는 해킹

2016년 미국 대선에서 러시아가 민주당을 공격했다는 의혹이 있다. 매우 오랜 시간 동안 복잡한 대규모 공격을 해서 미국 대선에 영향을 미치려는 했다는 의혹이다. 한 나라의 대통령을 뽑는 선거가 해킹에 영향을 받는다면, 매우 심각한 일이다.

최근 해킹은 돈을 벌려는 것보다 주요 기반 시설을 공격하고 서비스 중단시키려는 목표를 가진 경우가 많다. 한 국가의 에너지나 물류 등 인프라를 멈추게 할 수 있는 심각한 상태로 바뀌고 있다.

어제 오늘 얘기는 아니다. 이스라엘과 미국은 스턱스넷으로 이란 핵시설 공격했다. 페트야 공격자는 공격 규모에 비해 별로 돈을 못받았다. 돈이 목표가 아니었다. 국가의 지원과 조정을 받는 해킹 늘고 있다.

미국의 Mondelez, Merck, DLA Piper, 우크라이나의 에너지 회사 Kyivenergo, 배송회사 Nova Poshta, 내각 장관들의 컴퓨터, 덴마크의 Maers 등이 대표적이다. 한국에서도 국방부가 해킹 당했다.



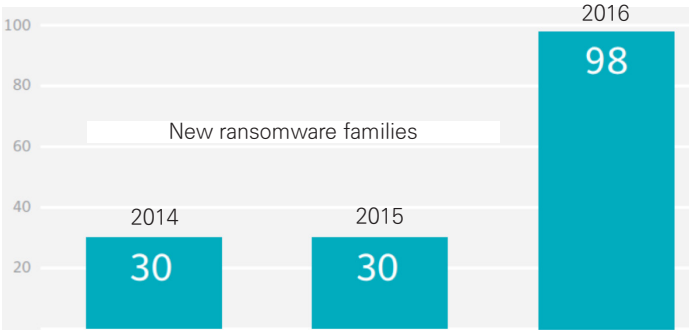
[그림 1] 미국 대선 시 해킹 공격 관련 타임라인 인포그래픽

02

빠르게 진화하는 악성코드

현재 수억개의 멀웨어가 있다. 멀웨어는 단순히 숫자만 많은 것이 아니라 우회기술을 교묘히 쓴다. 샌드박스 우회기술, 디버깅 우회기술, 모니터링 애뮬레이션 우회기술 등 다방면에서 쓰고 있다. 안티바이러스를 우회하는 기술은 너무 잘 알려져 있고. 너무 많은 우회 기술 있다.

가장 우려가 되는 것은 자바스크립트 난독화다. 난독화된 자바스크립트를 원상태로 돌리기 거의 불가능하고 해커를 잡는 것도 어렵다. 난독화하는 툴들이 3000원, 5000원으로 팔리고 있다. 해커들은 별 투자 없이도 악성코드를 만들 수 있다.



[그림 2] 새로운 랜섬웨어의 증가(2014-2016)

아카이브 파일에 악성코드를 심는 것도 늘고 있다. 이 파일은 네트워크 단에서 막지 못한다. 공격자들도 랜섬웨어 트렌드를 따라가고 있다. 2015년 30종에 불과했던 랜섬웨어가 2016년 98개로 늘었다.

03

CVE의 증가

지난 2년 동안 공개적으로 알려진 보안취약점(CVE, Common Vulnerabilities and Exposure)이 엄청 빠르게 증가했다. 공격자들은 게으르지 않다. 예전에는 취약점이 알려진 후 45일이 걸려야 멀웨어가 나왔는데 이제는 15일이면 나온다.

공격은 점점 더 교묘하고 효율적으로 발전했다. 앱을 직접 공격하지 않고 앱이 사용하는 라이브러리를 공격하는 사례가 늘고 있다. 라이브러리를 공격하면 그 라이브러리를 사용하는 엄청나게 많은 앱을 공격하는 효과가 있다. 공격자들도 효율성을 따진다.

문제는 많은 관리자들이 취약점 경고를 무시한다는 것이다. 통계에 따르면 54%의 관리자들이 경고를 무시한다고 한다. 왜냐하면 지금 잘 돌아가니까 일단 나눈다는 이야기를 많이 듣는다. 보안 패치나 업그레이드 하려면 일이 커진다. 스마트폰 운영체제 업그레이드도 잘 안하지 않나. 30분 동안 스마트폰 중단 되는게 불편해서 안 하는 경우가 많다.

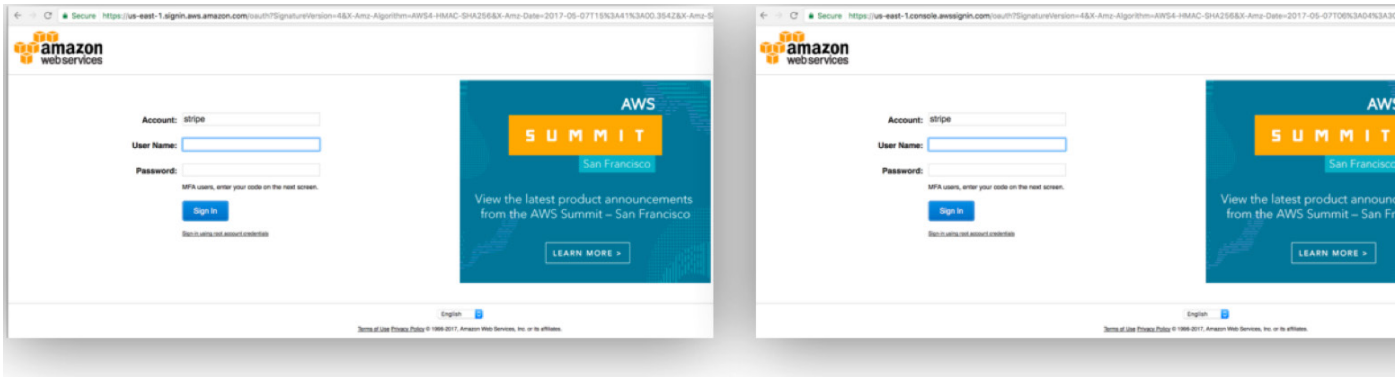
04

효과적이고 성공적인 악성코드 채널, 이메일과 피싱

이메일 중 65%가 광고성 이메일이라고 한다. 그 중 5% 이상이 악성코드를 포함하고 있다. 해커들은 왜 악성코드를 이메일로 보낼까? 악성코드를 보내면 공격대상 회사의 직원 중 누군가 이메일을 열고 링크를 클릭할 확률이 50% 가까이 된다고 한다. 옵스왓도 피싱 테스트를 1주일에 한번씩 하는데 누군가는 클릭을 하더라. 아무리 교육을 해도 클릭하는 사람이 꼭 있다. 그러니까 공격자가 이용한다.

이메일 보안 표준 기술이 나왔는데 적용된 경우가 많지 않다. 세계 기준으로 30% 이하만이 이 표준을 적용했다고 한다.

피싱의 수법도 더 정교하고 복잡해지고 있다. 가짜 아마존웹서비스(AWS) 페이지로 연결하는 피싱, 구글의 Oauth(Open Authorization)를 사용해 계정에 대한 액세스 권한을 부여한 사례가 있다. 피싱 공격자는 머신러닝으로 학습하기도 한다. 학습을 통해 공격기법과 콘텐츠를 바꾸고 진화한다.



[그림 3] 가짜 아마존웹서비스(AWS) 페이지로 연결하는 피싱 수법

05

모든 것의 시작(PUA)

광고성 제휴 프로그램(PUA)은 곧 악성코드라고 보면 된다. PUA의 절반이 악성코드를 배달한다. 무료로 프로그램을 사용하니까 좋다고 생각하는 분들도 있는데, PUA는 막아야 한다. 심각하게 받아들여야 한다. PUA가 악성코드의 시작이다. 보안업체에 왜 PUA를 못 잡냐고 얘기해야 한다. 애드웨어와 멀웨어의 경계는 사라지고 있다.

06

컴플라이언스 강화

2017년 3월 뉴욕 금융권의 사이버보안 규정이 제정됐고, 6월에 중국의 사이버보안법이 나왔다. 특히 유럽 일반데이터보호규정(GPPR, 개인정보보호법)이 내년 5월부터 작동된다. 유럽에서 비즈니스하는 회사, 유럽 직원이 있는 회사에 전부 적용된다.

'멀티스캔'과 '데이터살균(CDR)' 조합, 악성코드 위협 전천후 대응

지금까지 발견된 신규 악성코드의 수는 7억개에 조금 못 미친다. 지난해까지 집계된 신규 악성코드 6억개와 비교한다면 엄청나게 빠른 증가 속도를 보이고 있다. 지난 1년 사이 늘어난 악성코드의 숫자를 일 단위로 나누면 하루 약 30만개의 신종 악성코드가 나오는 셈이다."

김종광 인섹시큐리티 대표는 17일 열린 '최신 사이버 보안위협 사전 탐지·차단 전략' 세미나에서 이같이 강조하면서 "제 아무리 큰 글로벌 보안기업이라도 단일 안티바이러스(백신)에서 7억개의 악성코드 데이터베이스(DB)를 갖고 있는 곳은 없다"고 단언했다.

새롭게 등장하는 수많은 악성코드에 대응하기 위해서는 하나의 백신으로는 역부족이란 얘기다.

많은 사람들이 악성코드를 잡기 위해 백신 프로그램을 설치한다. 그러나 개인이든 기업이든, 설치하는 백신 숫자는 대부분 하나다.

김 대표는 "가장 많이 백신을 업데이트하는 업체도 하루 300여개가 최대"라며 "하루 30만개 발생하는 악성코드 중 29만7000개는 '알려지지 않은 악성코드'와 다름없다"고 설명했다.

그가 내놓은 해결책은 '멀티스캔'(다양한 백신 검사)이다. 하나의 백신으로 모든 악성코드를 잡을 수 없다면, 여러 개의 백신을 쓰면 된다. 하나가 못 잡는 여집합을 다른 백신이 잡는 식이다.

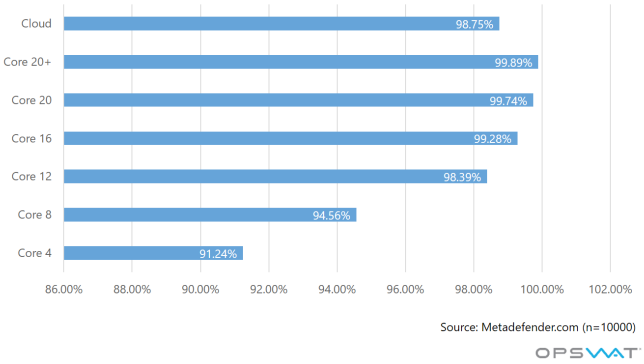
바로 미국 샌프란시스코에 본사를 두고 있는 보안업체 '옵스왓'의 접근법이다.

멀티스캔으로 '알려진 위협' 탐지율·속도 높인다

옵스왓의 대표 제품인 '메타디펜더(Metadefender)'는 30여개 국내외 백신 엔진을 통한 악성코드 검사 기능인 '멀티스캔'을 제공한다. 클라우드를 이용하면 40개까지도 설치할 수 있다. 옵스왓은 백신 수가 많을수록 탐지율이 높아진다고 분석하고 있다.

옵스왓에 따르면, 상위 1만개 악성코드 위협을 대상으로 백신 검사를 실시한 결과 4개 엔진을 사용했을 때는 탐지율이 91.24%였던 반면에 20개 넘는 백신 엔진으로 검사했을 때에는 99.89%의 탐지율을 나타냈다.

특정시점에 '메타디펜더'로 악성코드를 검사해본 결과 43개의 엔진 가운데 4개의 엔진만 즉각 제로데이 위협을 탐지했다. 3일 후에는 17개의 엔진이 위협을 탐지했고, 11일 후에는 23개의 엔진이 위협을 탐지하는 것으로 나타났다.



[그림 1] 백신 엔진이 많아질수록 위협 탐지율이 높아진다는 옵스왓 분석 결과

◀ 메타디펜더의 높은 탐지율을 설명하는 김종광 인섹시큐리티 대표

고태일 옵스왓 본사 최고기술책임자(CTO)는 "백신 엔진을 많이 쓸수록 빠르게 악성코드를 탐지해 대응할 수 있으며, 탐지율도 높아진다는 것을 보여준다"고 말했다.

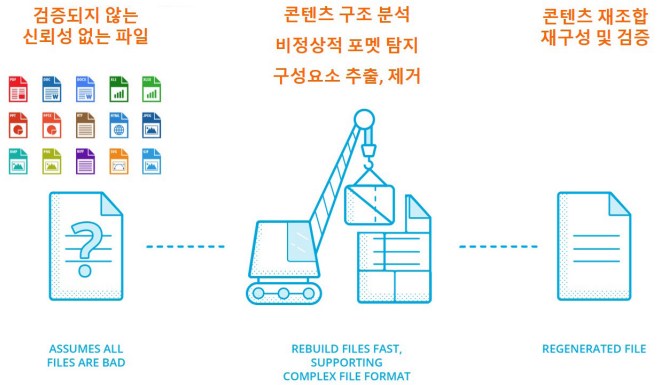
'메타디펜더'는 '멀티백신 스캔' 외에도 CDR(Content Disarm & Reconstruction) 기술을 제공하는 것이 특징이다. 이들 두 가지 기능을 조합해 바로 알려진 악성코드와 알려지지 않은 위협에 모두 대응한다.

문서파일·콘텐츠에 숨겨진 위협 사전 제거하는 'CDR'

옵스왓이 일명 '데이터살균' 기술로 부르는 CDR은 콘텐츠를 분해해 재구성하는 것을 의미한다. 국내에서는 '콘텐츠 무해화', '콘텐츠 악성 정화' 기술이라고 지칭되기도 한다.

고태일 CTO는 이날 세미나에서 CDR 기술을 끓인 물에 비유하면서 "물 안에 독소가 있는지 모르지만 물을 끓여 미리 살균한다"라면서 "CDR은 파일에 있는 잠재적인 모든 위협요소를 제거하는 기술"이라고 설명했다.

CDR은 문서파일이나 콘텐츠에 포함된 악성코드 여부를 분석하지 않는다. 대신에 콘텐츠 구조를 분석해 비정상적인 포맷을 탐지하고 구성요소를 추출한다. 의심스럽거나 승인되지 않은 파일의 구성요소를 추출해 제거함으로써 위협요소를 없앨 수 있다. 해당 요소가 추출·제거한 다음엔 콘텐츠는 안전하게 재조합·재구성된다.



[그림 2] CDR은 문서 파일이나 콘텐츠 구조 분석을 통해 비정상적인 포맷을 탐지하고 구성요소를 추출한다.

이에 따라 CDR 기술은 알려지지 않은 악성코드에 대응할 수 있는 기술로 지목된다.

고 CTO는 "멀티스캐닝은 알려진 악성코드를 탐지하며 데이터살균 기술은 알려지지 않은 악성코드 위협을 미리 제거한다"라면서 "사이버공격 킬체인의 공격코드 제작 단계에서 공격코드를 무력화하는 것에 해당한다. 따라서 간단하지만 효과적인 제로데이 공격 차단 방법"이라고 강조했다.

그에 따르면, 제로데이 위협, 알려진 취약점을 사용한 익스플로잇, 회피 기술을 사용하는 악성코드, 심지어 백신에서 탐지하지 못하는 알려진 악성코드도 알려지지 않은 위협이다.

CDR은 이같은 위협을 포함해 최근 발견된, 한국과 미국의 항공, 국방, 제조 분야를 대상으로 공격하는 '폼북(FormBook)' 악성코드처럼 취약점을 사용하지 않고 문서파일에서 제공하는 기능을 이용하는 경우도 효과적으로 차단할 수 있다.

프로그래밍과 스크립트 콘텐츠를 CDR에서 비활성화 시킬 수 있기 때문이다.

은닉기술(스테가노그래피)을 사용하는 악성코드는 유해한 스크립트를 숨긴 채 심어놔 탐지를 회피하면서 악성코드를 실행시킬 수 있다. CDR은 이같은 스크립트를 미리 제거해 혹시 모를 악성코드 침투를 방지할 수 있다.

이어 고 CTO는 "CDR 기술은 취약점으로 인한 위험을 효율적으로 해결한다"라면서 "취약점 패치와 업데이트를 하지 않더라도 취약점이 무력화되기 때문에 공격할 수 없다"고 설명했다.

HWP 포함 31종 100여개 파일변환 형식 지원

옵스왓 '메타디펜더'는 마이크로소프트(MS) 오피스, 아래아한글(HWP), PDF 등의 문서파일과 HTML, 이미지, XML 등 다양한 콘텐츠 형식을 지원한다.

예를 들어 MS 오피스의 경우 매크로, 임베디드 개체, OLE 개체, 첨부파일, 임베디드 바이너리 파일, 액티브X 컨트롤을 활성화시키는 스크립트, 하이퍼링크 등을 삭제하거나 일부 위험한 개체만 없애는 형태로 바꿀 수 있다.

HTML에서는 스크립트, 프레임, 설명, 이미지, 임베디드 개체, 임베디드 자바 애플릿, 하이퍼링크, HTML 태그 등 악용될 수 있는 개체를 삭제하거나 살균한다.

옵스왓 '메타디펜더' 제품을 국내에 공급하는 김종광 인섹시큐리티 대표는 "옵스왓은 31가지 종류의 원본형식을 100여개 형식으로 변환할 수 있도록 지원한다"며 "국내에서 많이 사용하는 HWP는 물론 가장 많은 수의 파일과 변환 형식을 지원하고 있다"고 강조했다.

이와 함께 김 대표는 "인섹시큐리티는 멀티스캐닝과 CDR, 악성코드 동적분석·행위분석 기능을 제공하는 샌드박스와 이메일 보안 솔루션을 연동해 다양한 경로에서 들어오는 악성코드 탐지율과 차단율을 크게 높이는 동시에 위험수준을 점점 낮출 수 있다"고 덧붙였다. By

“악성코드·익스플로잇, 탐지보다 예방이 중요”

◀ 악성코드와 익스플로잇은 탐지보다 예방이 중요하다는 최원식 팔로알토네트웍스코리아 대표

[그림 1] 익스플로잇은 악성코드가 아니다. 팔로알토네트웍스는 이 둘을 각기 다른 방식으로 대응해야 한다고 지적했다.

사이버보안 기술이 나날이 발전하고 있지만 보안사고는 끊이지 않“치료보다는 예방이 낫습니다. 무언가 일이 일어난 이후에 해결하는 것보다 일이 일어나기 전에 막는 것이 더 좋습니다.”

최원식 팔로알토네트웍스코리아 대표의 말이다. 최 대표는 사용자 환경에서 보안 침해를 방지하려면 5가지의 능력이 있다면서 이같이 말했다. 최 대표가 말한 5가지 능력은 ▲예방에 집중(Prevention Focused) ▲악성코드 예방(Malware Prevention) ▲익스플로잇 공격 예방(Exploit Prevention) ▲예방 자동화(Automated Prevention) ▲지속적인 예방(Persistent Protection)이다.

보안산업계는 사이버공격을 막기 위해 오랫동안 고군분투 했지만 크게 성공적이지 않았다. 엄청난 노력에도 불구하고 전세계는 랜섬웨어 공포에 떨고 있다. 최 대표는 “침해 탐지와 사고 대응이 보안 가치를 제공하지 않는다는 것은 아니지만 예방에 비해 부차적이어야 한다”고 강조했다.

최 대표는 우선 악성코드와 취약점을 구별하지 못하는 오류에서 벗어나야 한다고 설명했다. 이 둘은 명백히 다르기 때문에 각기 다른 방식으로 대응해야 한다고 지적했다.

[그림 2] 팔로알토의 트랩스는 다층적인 방식으로 위협을 예방하도록 설계돼 있다.

악성코드는 자체적으로 실행할 수 있고, 타깃 서버로 이동 가능한 파일이다. 반면 익스플로잇은 악성코드를 집어넣을 수 있는 통로다. 도둑이 유리창문에 구멍을 뚫어 문을 열고 들어온다면, 그 구멍이 익스플로잇이란 게 그의 설명이다.

최 대표는 자사의 엔드포인트 보안 솔루션인 '트랩스'가 공격 예방을 위한 5가지 능력을 모두 보유하고 있으며, 멀웨어와 익스플로잇 모두의 위협에서 벗어날 수 있도록 한다고 강조했다.

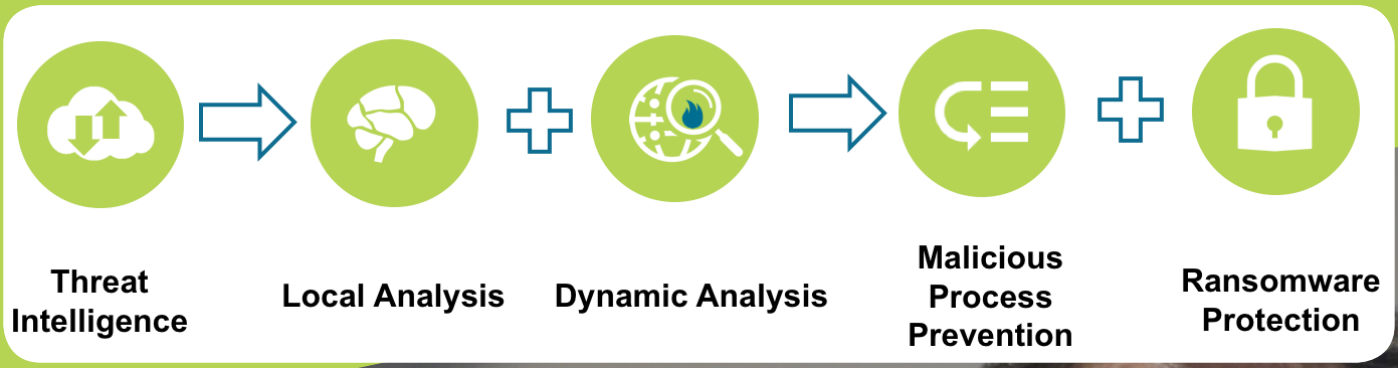
트랩스는 ▲위협 인텔리전스(Threat Intelligence) ▲로컬분석(Local Analysis) ▲동적분석(Dynamic Analysis) ▲악성 프로세스 예방(Malicious Process Prevention) ▲랜섬웨어 보호(Ransomware Protection) 등 다층적 방법으로 멀웨어로부터 예방하도록 설계돼 있다.

특히 알려진 악성코드뿐 아니라 알려지지 않은 멀웨어도 예방할 수 있다고 최 대표는 강조했다. 최 대표에 따르면, 팔로알토네트웍스의 위협 인텔리전스 클라우드에는 매달 2억1500만개의 샘플이 올라온다. 여기에는 알려지지 않은 바이러스가 60~70%를 차지한다.

알려지지 않은 악성코드가 들어오면 로컬분석과 동적분석 시스템으로 넘겨진다. 로컬분석에서는 위협 인텔리전스에서 수집된 샘플을 학습모델(머신러닝)로 악성코드를 찾아낸다. 사인, 스캐닝, 행동분석에 의존하지 않는다. 동적분석은 가상 샌드박스다. 베어메탈 분석 기능을 통해 멀웨어로 의심되는 파일을 실행시켜 어떻게 행동하는지 분석할 수 있다. 샌드박스 우회 기술을 차단할 수 있다.

악성 프로세스 예방은 파일이 아닌 스크립스 형태의 공격을 막아준다. 이는 프로세스를 보고 판단한다. 차일드 프로세스를 모니터링 하고 있다가 적절치 않은 움직임을 할 경우 차단한다.

랜섬웨어 프로텍션은 허니팟 기술을 활용한다. 실제 환경에 시스템을 만들어 파일을 뿌려놓고 랜섬웨어가 암호화시키는지 살펴본다.



[그림 3] 팔로알토의 트랩스는 다층적인 방식으로 위협을 예방하도록 설계돼 있다.

최 대표는 "99%의 멀웨어가 한번 발견된 후에는 변형되는데 기존의 레거시 기술(안티바이러스)은 한계가 있다"면서 "트랩스는 알려지지 않은 멀웨어를 대부분 예방할 수 있다"고 말했다.

최 대표는 트랩스가 익스플로잇도 예방할 수 있다고 설명했다. 최 대표에 따르면, 현재 익스플로잇을 만들 수 있는 기술은 24개 정도다. 이 24개를 다양하게 조합해 공격하는 것이다. 새로운 익스플로잇을 만든다고 해도 완전히 새로운 것을 만드는 것이 아니라 기존의 24개 기술 중 일부를 새로운 것을 조합해서 만든다.

팔로알토네트웍스는 여기에 착안했다. 트랩스는 24개의 익스플로잇 기술을 모니터링하는 방법으로 새로운 익스플로잇까지 예방한다. 이는 트랩스가 제로데이 공격을 막을 수 있다는 것을 의미한다. 제로데이란 취약점이 발견된 후 보안패치가 나오기 전까지의 기간을 말한다. 이용자들은 제로데이 공격에 속수무책일 수밖에 없는데, 트랩스는 이를 막을 수 있다. 새로운 익스플로잇도 24개의 기술 중 일부가 사용됐을 것이기 때문이다. 지난 2017년 마이크로소프트가 자사의 소프트웨어에 취약점이 있다고 인정했는데, 1년 전에 구매한 트랩스로 익스플로잇을 막은 사례가 있다.

이는 안티바이러스(백신)처럼 트랩스를 업데이트 할 필요가 없다는 것도 의미한다. 기존의 24개 기술이 사용됐는지만 보면 되기 때문이다.

최 대표는 "익스플로잇은 마이크로소프트, 어도비, 한글과컴퓨터같은 일반적인 앱을 무기화하기 때문에 대책이 없다"면서 "이를 막기 위해서는 새로운 기술이 필요하고 그것이 바로 트랩스"라고 강조했다. By

▲ 트랩스가 악성코드와 익스플로잇 예방을 위한 최적의 솔루션이라고 강조하는 최원식 팔로알토네트웍스코리아 대표

김종광
인섹시큐리티
대표

위협 인텔리전트 플랫폼, 왜 중요한가

최신 사이버위협의 특징은 글로벌화, 다종화다. 보안이 뚫려 랜섬웨어 악성코드와 다른 위협이 결합된 공격에 의해 보안이 뚫린다면 치러야 할 대가는 엄청나다.

최근 기승을 부리는 랜섬웨어는 단순히 돈을 목표로만 공격하지 않는다. 때로는 서비스 중단을 목표로 한다. 기업의 중요정보가 암호화되고, 심할 경우 서비스 시스템이 완전히 망가진다. 공격의 희생자는 세계 다양한 산업에 걸쳐 있다.

2010년 이란 핵시설, 2015년 우크라이나 전력망, 2017년 미국 핵시설 등을 대상으로 발생하는 사이버공격은 그 규모와 영향력이 엄청나다.

글로벌 보안 기업들은 이에 대항하기 위해 사이버정보 공유·협력체계를 만들고 있는 추세다. 위협의 가짓 수가 엄청난 숫자로 늘어나고, 이를 특정 기업 혼자 막을 수 없다는 공감대가 퍼지고 있다.

협력의 중요성이 강조되고 있는 배경이다. 김종광 인섹시큐리티 대표는 "이제는 일개 기업이 사이버공격을 방어하는데 한계에 도달했다"고 강조하며 '위협 인텔리전트 플랫폼'의 중요성을 역설했다.

김 대표는 "지금 세계 보안 기업은 각종 악성코드를 더 빨리 탐지하기 위한 협약체를 만들어 피드백을 공유하며 활동한다"고 말했다.

이와 비슷한 개념에 착안해, 다양한 보안 솔루션을 유기적으로 연동해 기업 내부로 유입되는 보안위협을 자동으로 판별, 신속하게 대응할 수 있도록 지원하는 보안 플랫폼이 최근 등장했다.

국내 신생 보안업체인 마에스트로네트웍스가 개발한 신개념 위협 인텔리전스 플랫폼인 '마에스트로'다.

마에스트로는 기업 내부로 유입되는 다양한 파일의 악성여부를 자동 분석·검증·차단하는 플랫폼이다. 사내에 구축돼 있는 엔드포인트·네트워크·이메일·웹 보안 솔루션과 연계해 최신 랜섬웨어, 지능형지속위협(APT) 공격코드나 악성코드 등의 위협을 빠르게 판단하고 대응조치를 수행할 수 있도록 특화됐다.

시중에 나와 있는 엔드포인트 보안 솔루션, 네트워크 보안 솔루션, 악성코드 동적분석을 수행하는 샌드박스 등과 연동돼 기업 내부로 들어오는 모든 파일을 진단한다. 이후 악성 파일은 자동 차단하고 정상 파일은 자동 실행하는 기능을 수행한다는 게 김 대표의 설명이다.

김 대표는 "많은 기업, 기관의 정보보호팀은 보통 몇 명 수준의 소수 인원인데 관리해야 할 보안 제품이 너무 많다"라면서 "그 많은 제품과 솔루션을 일일이 대응하기에는 현실적으로 불가능하다"고 지적하기도 했다.

다양한 네트워크 보안 제품에서는 방대한 로그가 쌓인다. 이를 사람이 수동으로 분류하는 대신에 마에스트로 같은 플랫폼이 악성코드와 정상코드를 자동으로 분류하면 업무 생산성과 효율성이 높아진다.

그 점에서 '보안 자동화'를 구현하는 시스템이라고도 할 수 있다.

마에스트로에는 현재 멀티백신, 샌드박스, 도메인과 IP, 이메일 등에 대한 평판 분석 기능과 화이트리스트, 머신러닝, 그리고 안드로이드와 iOS 등 모바일에 대한 취약점 진단기능, APK(Android Package Kit)를 정밀 분석하는 기능 등을 제공한다.

이를 위한 마에스트로 연합군으로 네트워크 보안 솔루션에는 팔로알토, F5, 블루코트, 시스코, 포티넷 등이 있다. 엔드포인트 보안 솔루션은 카본블랙, 팔로알토네트웍스 등이 있다.

마에스트로네트웍스는 기업들이 보다 빠르게 다양한 보안 제품과 통합 운영할 수 있도록 다양한 보안 솔루션을 대상으로 사전 연동 테스트도 마친 상태다.

김 대표는 "각 시스템들의 고유 기능을 통합하고 사용률의 극대화를 위한 시스템 연계가 중요하다"고 재차 강조했다.

마에스트로는 사내 유입된 악성파일 등의 위협 분석 결과와 현황을 한 눈에 살펴볼 수 있는 통합 대시보드와 리포트도 제공한다. By

최신 사이버 보안위협
사전 탐지·차단 전략

바이라인네트워크

발행 | 바이라인네트워크
배포 | https://byline.network/
취재/글 | 이유지 기자 yjlee@byline.network
심재석 기자 shimsky@byline.network
남혜현 기자 smilla@byline.network
문의 | byline@byline.network

Copyright © 2017 BylineNetwork