PASCON 2018
2018 공공기관·기업 개인정보보호&정보보안 컨퍼런스
Public institution·Affiliated organization Information Security Conference 2018

사이버 보안 전문가들이 말하는

사이버 보안의 "진실 혹은 거짓"

2018. 10. 25

트루컷시큐리티

사이버 보안에 잘못된 정보가 난무하는 이유

- ✓ 보이지 않는다.
- ✓ 일반인들의 접근이 어렵다.
- ✓ 보안기업들이 주도해 왔다.
- ✓ 끊임없이 새로운 용어를 만들어 낸다.

1. 우리도 막는다

최대 60%에 이르는 셀프웨어.

해커에게 무력화된 방어 제품.

Why X

보안 셀프웨어 문제와 이를 중단하는 방법

원문보기 : http://www.itworld.co.kr/howto/108922#csidxdc60daf3b6b8e5097f2a499c85ad18d

1. 30~60%가 셀프웨어라는 조사 결과
2. 2013년 Target은 악성코드 방지에 100만 달러를 지출한 직후 자료유출 사고를 당했다

막는 걸 보면서 뚫는 해커

해커가 앞서고, 보안기업은 뒤따르는 역사의 반복

2. 악성코드를 막는다

코드 자체가 악성인 것은 없다.

악성코드 없는(Malware-less) 공격 급증.

알려진 일부 코드는 막을 수 있다.

Why ▲

2018년 보안과 관련된 가장 중요한 "팩트"와 수치, 통계

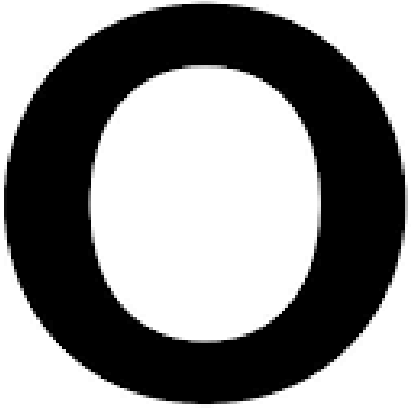
원문보기 : http://www.itworld.co.kr/news/111098#csidxd91a6cb2c59ced98c6401b77a5967f2

2017년 침해 공격의 77%가 파일리스 공격

코드 자체가 악성인 것은 없다

악의적으로 이용되는 프로그램이 있을 뿐이다

3. 엔드포인트에서 막아야 한다



최상의 범죄 예방은

현장에서 범죄 행위를 저지하는 것이다.

4. APT공격을 막는다

막지 못한 공격을 “APT공격”이라고 부른다.

Why X

APT(Advanced Persistent Threat)

원문보기 : http://www.itworld.co.kr/news/95741

새로운 두려움의 대상을 만들어 돈을 벌고자 하는 마케팅 용어에 불과하다고 혹평

전설의 해커 “케빈 미트닉”의 저서 〈네트워크 속의 유령〉

원문보기 : https://librewiki.net/wiki/%EC%BC%80%EB%B9%88%EB%AF%B8%ED%8A%B8%EB%8B%89

자신이 1980년대에 했던 공격과 무슨 차이가 있냐고 비판

5. 인공지능은 만능이다

학습을 하지 못한 인공지능은 빈 깡통에 불과하다.

Why X

진짜 AI vs. '무늬만' AI

원문보기 : http://www.itworld.co.kr/news/109368#csidx17e28b49a8d289fb2942dc32fb0c447

AI 보안제품에 AI가 없다

인공지능에 기대는 건 보안의 답이 될 수 없다

원문보기 : https://www.boannews.com/media/view.asp?idx=71586

알려진 무지 : 인공지능은 모르는 걸 분석할 수 없다

6. 망을 분리했으니 보안제품이 없어도 된다

이론적으로 안전하다.

현실은 이론이 아니다.

7. 클라우드 컴퓨팅을 해서 보안제품이 없어도 된다

보안을 책임져 주는

클라우드 컴퓨팅 제공업체는 없다.

8. 블록체인은 완벽한 보안이다

보안의 3 요소인 기밀성, 무결성, 가용성 중에서

블록체인은 무결성, 가용성이 좋은 기술일 뿐이다.

Why X

보안 기술이자 보안 대상

D G D e e p D i v e | Blockchain Security

1. 가장 약한 링크만큼 강하다 - Chris Wysopal | 베라코드 CTO, 공동 설립자
2. 블록체인 데이터베이스, “그렇게까지 안전하지 않다” - James Kobielus | SiliconAngle Wikibon

51% 공격 현실화

원문보기 : https://www.blockinpress.com/archives/5740

51% 공격 당한 비트코인 골드 - 일부 거래소 수백만 달러 피해

우리가 흔히 들어 온 말들에 대한 오해와 진실

사이버 보안전문가들이 말하는

사이버 보안 **총정리**

01 우리도 막는다 — X

대부분의 보안기업들은 늘 이렇게 말하지만,
보안사고는 지금도 계속되고 있다.

02 악성코드를 막는다 — △

애초에 악성코드라는 것은 없다.
악의적으로 이용되는 코드가 있을 뿐이다.

03 엔드포인트에서 막아야 한다 — O

범죄를 막는 최상의 방법은
현장에서 범죄 행위 자체를 저지하는 것이다.

04 APT공격을 막는다 — X

APT공격은 해킹을 막지 못해 쓰기 시작한 용어이며
지금도 여전히 해킹을 완전히 막지 못하고 있다.

05 인공지능(머신러닝, 빅데이터)은 만능이다 — X

인공지능은 "학습"을 전제로 하는 기술이다.
즉, "학습" 할 수 없다면 아무것도 아니다.

06 망을 분리했으니 보안제품이 없어도 된다 — △

망 분리 후에도 해킹은 계속되고 있다.

07 클라우드 컴퓨팅을 했으니 보안제품이 없어도 된다 — X

클라우드 컴퓨팅은 보안 때문에 하는 것이 아니다.

신개념 악성행위 차단시스템 소개 - 트로이컷

1. 악성행위 차단 시스템이란 ?

   프로세스가 하는 행위만을 보고 악성인지 진성인지를 판단하는 시스템

2. 왜 악성행위 차단 시스템이어야 하나?

   Processing Capacity Exceeded + Malwareless attacks

3. 트로이컷의 차단 기준

   사용자입력 - 유일한 불변의 기준

사용자에 의한 전송 vs 불법적인 정보 유출

구분	사용자에 의한 전송	불법적인 정보 유출
어플리케이션	사용자가 실행시켰음	사용자가 실행시키지 않았음
사용자 입력	무수히 발생 - 내용 작성 - 보내기 버튼	없음 - 내용 작성 없음 - 보내기 버튼 누르지 않음

4. 장점

알려지지 않은 신·변종 악성코드에 의한 공격까지 실시간 차단 가능

5. 단점

내부자에 의한 유출은 차단 불가 - 로깅 가능

6. 제공하는 기능

법률 및 규정	기능	기능 설명
□ 국정원「국가정보보안기본지침」 ○ 제25조(전자정보 보안조치) ▪ 정보통신망을 통하여 보관·유통되는 전자정보의 보안을 위한 조치 □「정보화업무운영 및 이용에 관한 규정」 ▪ 관계기관의 장은 해킹이나 자료의 유출 등 보안사고 방지에 필요한 조치 강구	불법 정보유출 방지	APT 공격에 의한 불법 정보유출 방지
		P2P, 그리드, 파일공유 등에 의한 불법 정보유출 방지
	계정탈취 방지	패스워드 유출 방지
	블랙리스트 차단	유해 프로그램 실행 방지
□「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 ○ 제45조(정보통신망의 안정성 확보 등) ▪ 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치	랜섬웨어 공격 방지	랜섬웨어 공격 방지
		정보탈취 랜섬웨어 공격 방지
		전자동 스마트 백업
□「악성프로그램 확산 등에 관한 법안」	좀비PC방지	좀비PC공격 방지
		악성트래픽 방지
□「국가,공공기관 내부망과 인터넷간 안전한 자료전송 보안가이드라인,국가정보원 2012,2」 ▪ 전송되는 파일에 대해 전송일시, 파일명, 파일 반/출입 사용자에 대한 정보를 포함한 감사데이터 생성	감사 데이터 생성	정보 전송 감사데이터
		암호화 정보전송 감사데이터
		악성 트래픽 감사데이터
		프로그램 실행 감사데이터
	SYSLOG 제공	SYSLOG 제공
	HASH 제공	프로세스, 파일 HASH 제공

7. 제품비교

구분	트로이컷	타 제품들
방어개념	행위 차단 - 세계 최초 / 유일 - 특허 보유	코드 차단
방어영역	아웃바운드	인바운드
차단방식	- CoA알고리즘에 의한 - 사용자입력기반 - 악성 행위 차단	- 시그니처 기반 - 규칙(룰 혹은 정책) 기반 - 임계치 기반
특장점	컴퓨터의 동작원리에 의해 차단 - 패치나 업데이트 없이 차단	패치나 업데이트를 전제 - 선 등록, 후 차단
패치	- 시그니처 및 룰, 정책 없음 - 수시 패치로 인한 업무부하 및 위험요소 없음	시그니처 및 룰, 정책 등 수시 패치로 인한 업무 과중 및 오패치로 인한 위험요소 상존
사고대응	공격을 실시간 자체적으로 차단하므로 부산스럽게 대응할 필요가 전혀 없음	사고 발생 시 네트워크와 전원을 차단하는 등 시급하게 대응해야 하므로 업무부하가 과중함
장애처리	중앙관제서버에서 원격으로 처리 가능	장애가 발생한 PC에서 직접 처리
예외처리	사용자 입력없이 동작하는 업무 프로그램만 예외 처리하면 되는데, 설치 시 최장 1개월만 탐지모드로 운영한 후에 등록하면 됨.	수시로 예외처리를 등록해야 함

결 언

사이버 보안은

“더도 아니고 덜도 아니고”

정확하게 자신이 아는 만큼만 막을 수 있습니다.

보안관리자가 잘못된 용어에 함몰되는 순간,

그 기관의 보안은 이미 뚫린 것이나 다름없습니다.

세종텔레콤은 합리적인 가격과 최상의 서비스로 귀사의 경쟁력을 높여드립니다

감사합니다

SEJONG TELECOM | 세종텔레콤㈜ | 서울시 강동구 상일로 10길 36