랜섬웨어 위협의 미래 대응 전략

다변화 하는 랜섬웨어, 확실한 방어 방안은?

매일 수 천개 이상의 새로운 랜섬웨어가 전세계에 유포됩니다. 이러한 랜섬웨어의 폭발적 증가에 대한 기존 방어 방법의 한계와 이를 극복할 수 있는 방법을 알아봅니다.

랜섬웨어 위협의 미래 대응 전략

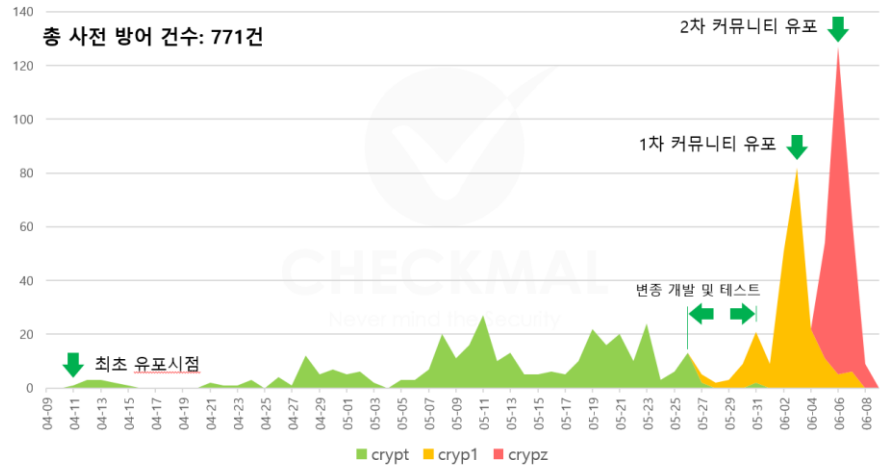
다변화 하는 랜섬웨어, 확실한 방어 방안은?

최선의 방법?

PC 나 자료를 파괴하는 악성 프로그램은 최대한 자신의 정체를 숨기기 위해 정상적인 프로그램으로 숨어 듭니다. 백신과 같은 보안 소프트웨어는 이러한 악성 프로그램을 분석하여 특성을 추출하고 더 이상 실행되지 않게 방어를 합니다.

하지만, 랜섬웨어 공격과 같이 새롭게 유행하는 악성 프로그램은 매일 정상적인 프로그램으로 보이게 또 다른 변종을 만들어 냅니다.

실제로, 2016 년 6 월 국내 대형 커뮤니티에 서비스되는 광고 서버를 통해 CryptXXX 랜섬웨어가 유포되었습니다. 이 랜섬웨어는 웹 페이지를 방문하는 것만으로도 감염이 되는 특징을 가지고 있으며, 또한 이틀 간격으로 변종이 유포되어 많은 사용자 피해가 발생하였습니다.



과연 기존의 백신과 같이 악성 프로그램이 출현해야만 특성을 추출할 수 있는 방어 방법이 최선일까요?

CASE STUDY #1

K 대형병원은 1500 대의 내부 PC 에 유명 AV 제품을 사용하였으나, 월 10 건 이상의 랜섬웨어 공격을 인지하였다.

이후 상황인식 엔진을 탑재한 AppCheck Pro 를 구축하여 랜섬웨어 공격을 성공적으로 방어하고 있으며, 현재 월 70 여건의 공격 방어 리포트가 생성되고 있다.

CHECKMAL

기존 탐지 방법의 한계 : 분석해야만 알 수 있는 정보

가장 널리 사용되는 **시그니처 기반**의 탐지 기법은 악성코드의 특징을 목록화 하여 판단하는 방법으로, 보유하고 있는 목록에 탐지하고자 하는 악성코드의 시그니처가 없을 경우 이를 방어할 수 없습니다. 일반적으로 악성코드 시그니처는 주기적으로 업데이트 되므로 업데이트 되기전까지는 새로운 악성코드에 노출될 확률이 높습니다.

기존의 **행위 기반** 탐지 기법은 특정 행위를 "패턴화" 시켜 행위를 시그너처화 하여 탐지하는 방법으로 새로운 행위가 발생하였을 경우 이를 탐지하기 어렵습니다.

네트워크 기반 탐지 기법 또한 암호화된 네트워크를 통해 공격자가 명령을 내리는 경우 이를 탐지하기가 어려우며, 임의의 파일을 생성하고 이를 랜섬웨어가 암호화 하였을 때 탐지하는 기법인 **디코이(Decoy) 기반** 탐지기법도 생성된 파일을 간단하게 우회가 가능합니다.

우리가 일반적으로 사용하는 프로그램의 취약점을 이용해 악성코드를 실행하는 방법을 탐지하는 **익스플로잇 기반** 탐지 기법의 경우 사용자가 직접 실행하도록 유도하는 피싱(phishing) 방식은 탐지가 불가능하며, 등록된 정상프로그램만 실행할 수 있도록 하는 방식인 **ACL(Access Control List)기반**의 방어기법은 새롭게 등록되는 프로그램과 업데이트 되는 정상 프로그램에 대한 관리가 어렵기 때문에 실질적인 업무 환경에서는 효용성이 떨어지게 됩니다.

특히 랜섬웨어는 보안 제품에 탐지되지 않는 새로운 기법을 빈번히 사용합니다. 과연, 이 랜섬웨어를 방어하는 최선의 전략은 무엇일까요?

CASE STUDY #2

국내 모 대기업은 랜섬웨어 방어 BMT 를 개최한 결과, 참가한 국내외 10 여개의 유수 AV(안티 바이러스) 및 APT 방어 제품 중 AppCheck Pro 가 유일하게 제시된 환경에서 랜섬웨어를 100% 차단하는 성능을 보였다.

이에 체크멀은 해당 기업과 3000 대의 AppCheck Pro 납품 계약을 체결하였다.

CHECKMAL

차세대 랜섬웨어 방어 전략: 상황인식 랜섬웨어 탐지 기술

이렇게 시시각각 새로운 변종이 나타나는 랜섬웨어라도 그 목적은 언제나 같습니다. 결국 마지막엔 사용자가 파일을 사용하지 못하게 암호화를 하는 것입니다.

상황을 인식하는 랜섬웨어 탐지 기법은 사용자의 파일을 사용하지 못하게 암호화 하는 행위를 탐지하는 기술입니다. 기존의 보안 제품처럼 랜섬웨어의 특징을 보는 것이 아닌 실제 사용자의 파일을 변조하는 상황을 종합적으로 판단, 새롭게 나타나는 랜섬웨어의 훼손 행위에 대해서도 시그니처 없이 정확한 탐지가 가능합니다.

- **시그니처**와 **행위 기반 탐지 우회**하는 랜섬웨어의 경우, 상황인식 탐지 기법은 파일이 변경되기 전과 후를 지속적으로 모니터링하여 관리하므로 시그니처 없이 순수한 행위만으로 방어가 가능합니다.
- **네트워크 기반 탐지 우회**에도 최종 엔드포인트(End-point)에서 실제 행위를 탐지하므로 방어가 가능합니다.
- **미끼를 우회**하는 방식이나 사용자가 실수로 **랜섬웨어를 직접 실행**하는 경우에도 랜섬웨어의 최종 목적인 파일을 실시간으로 모니터링함으로써 변조에 대한 탐지가 가능합니다.

만약, 차단이 실패했을 때에도 사용자의 파일을 복원할 수 있는 대안이 제시되어야 합니다.

즉, 랜섬웨어의 최종 목적인 "파일의 훼손"을 철저하게 감시할 수 있다면 시스템의 효율성과 효용성을 모두 향상시킬 수 있습니다

CASE STUDY #3

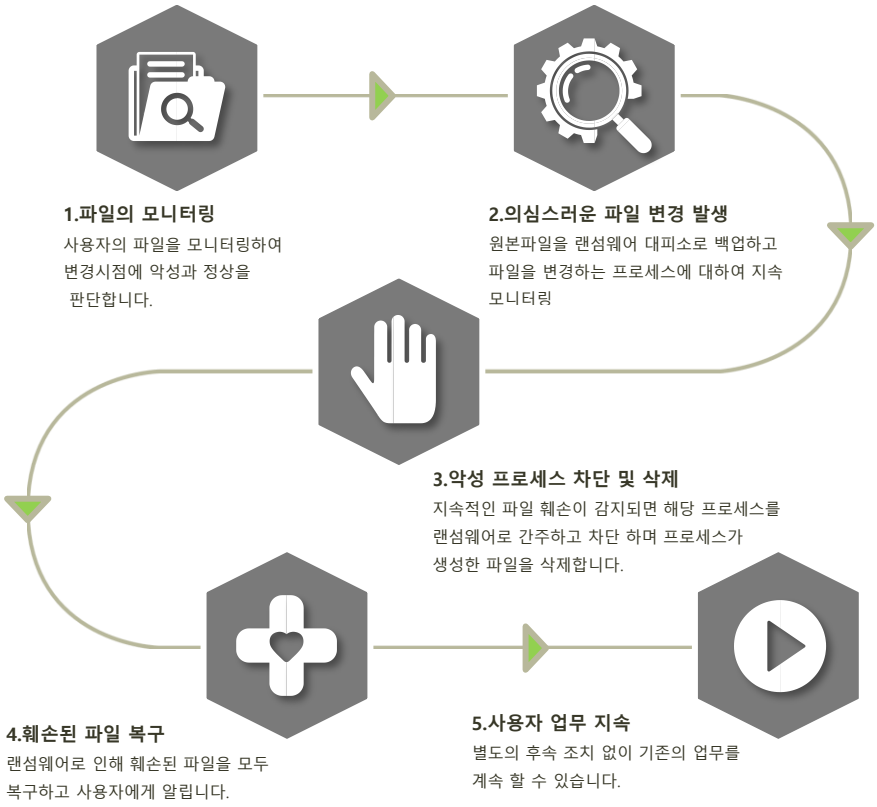
모 공공기관에서는 최근 정보보호 강화 사업에서 국내에서 빈번히 발생하는 랜섬웨어에 대응을 위해 상황인식 기반 안티 랜섬웨어 제품인 AppCheck Pro 를 500 여대 도입했다.

CHECKMAL

기본에 충실한 랜섬웨어 대응 솔루션: AppCheck Pro

체크멀 AppCheck 은 자체 개발한 상황 인식 알고리즘을 통하여 이러한 랜섬웨어의 마지막 행동을 중심으로 모니터링하고 방어하는 랜섬웨어를 방어하는 기본에 충실한 제품입니다.

체크멀에서 자체 개발한 캅(CARB)엔진은 랜섬웨어를 특정할 수 있는 시그니처나 패턴 없이 파일 변조 시점에서의 상황을 판단하는 핵심 기술로, 파일의 변화를 실시간으로 감지해서 알려지지 않은 훼손 행위에 대해서도 정확히 탐지, 원상복구가 가능합니다.



이는 기존의 보안 제품이 주로 사용하는 클라우드 연동 방식의 분석 시스템 체계를 넘어서 자체적으로 파일의 훼손행위를 판단할 수 있어 인터넷이 연결되지 않은 환경에서도 탐지율에 영향을 받지 않는 독보적인 특징을 가지고 있습니다.

15 만 사용자의 선택

커널 환경에서 동작하는 랜섬웨어의 상황인식 기반 엔진은 속도와 안정성, 그리고 호환성을 보장해야 한다.

15 만 사용자를 보유한 AppCheck 는 다양한 사용자 환경에 검증된 랜섬웨어 탐지 전용 솔루션이다.

CHECKMAL