이달의 위협: 악성 크립토마이닝 (암호화폐 채굴)

특징

오늘날 관측되고 있는 위협 활동 중 대부분은 사이버 범죄자가 금전적 이득을 취하는 데 목적을 두고 있습니다. 그런 특징은 공격자가 공격에 성공한 장치를 피해자가 사용하지 못하도록 비밀번호를 설정한 채 몸값을 요구하는 랜섬웨어에서 특히 두드러집니다. 그러나 피해자가 몸값을 지불하리란 보장은 없습니다. 공격자들은 암호화폐 채굴이 (종종 사용자의 눈을 피해) 돈을 벌기 좋은 방법이라는 사실을 깨닫게 됩니다. 시스템 통제권을 완전히 장악하는 랜섬웨어와 달리, 채굴 소프트웨어는 백그라운드에서 은밀히 실행되면서 수익을 올립니다. 위협이 탐지되지 않는 한 공격자가 느긋하게 앉아서 암호화폐를 통해 수익을 올릴 수 있으므로 거의 완벽합니다.

주의가 필요한 이유

랜섬웨어처럼 치명적이지는 않다는 컴퓨터에서 실행되는 모든 소프트웨어와 마찬가지로 채굴 소프트웨어도 리소스를 필요로 합니다. 누구나 경험했듯이 너무 많은 리소스를 소모하는 소프트웨어는 시스템의 전반적인 성능에 악영향을 미칠 수 있습니다. 뿐만 아니라 추가 리소스를 원활하게 사용하려면 더 많은 전력이 필요합니다. 시스템 한 대에 가해지는 부담은 그리 크지 않지만 기업 전체의 엔드포인트 개수에 비용을 곱하면 전기료가 눈에 띄게 증가할 수 있습니다. 게다가 범죄자가 기업 리소스를 사용하여 암호화폐를 채굴할 경우 규정 준수 문제가 발생할 수 있습니다. 네트워크를 관리 측면에서 가장 걱정스러운 부분은, 악의적인 크립토마이닝 감염이 네트워크 구성이나 전체 보안 정책의 허점을 의미한다는 것입니다. 이러한 허점은 다른 수단을 통해 공격자들에게 쉽게 이용될 수 있습니다. 만약 네트워크에서 크립토마이닝에 감염된 사실이 발견된다면, 그러한 허점을 악용하여 더 많은 악성 행위가 일어나는 것을 막기 쉽지 않을 것입니다.

크립토마이닝 소프트웨어 작동 원리

크립토마이닝이란 디지털 통화 형식의 코인(암호화폐)을 채굴하는 과정을 뜻합니다. 일반적으로 검증료를 지불하거나 새로운 코인이 주기적으로 생성되는 디지털 거래의 확인 절차를 돕게 되면 그 대가로 코인이 지급됩니다. 크립토마이닝은 백그라운드에서 코인을 채굴하는 전용 애플리케이션을 컴퓨터에 설치하여 수행할 수 있습니다. 웹 브라우저에서 크립토마이닝을 수행하는 방법도 있습니다. 사이버 범죄자가 암호화폐 채굴 소프트웨어를 호스팅하는 웹 서버에서 웹 페이지를 요청하면 서버는 해당 웹 페이지가 열려 있는 한 계속 코인을 채굴하는 암호화폐 채굴 패키지를 전송합니다.

악성 크립토마이닝에 주목해야 할 이유

세상에 존재하는 모든 암호화폐 채굴 애플리케이션이 악성은 아닙니다. 개인이 본인 소유의 컴퓨터에 암호화폐 채굴 소프트웨어를 설치한 경우 이는 완벽하게 합법입니다. 바이러스 백신과 기타 엔드포인트 기술이 합법적인 소프트웨어와 인증 받지 않은 소프트웨어를 항상 정확히 구분할 수 있는 것은 아닙니다. 암호화폐 채굴 소프트웨어의 출처를 알아야 하고 설치된 암호화폐 채굴 소프트웨어가 통신을 시도하는 대상을 알아야 하는데, 이를 위해서는 보다 완벽한 보안 솔루션이 필요합니다.

더 읽을거리

- 시스코 보안 제품을 사용하여 암호화폐 채굴 차단
- 암호화폐 채굴로부터 네트워크 보호
- https://blogs.cisco.com/security/demystifying-cryptocurrency-mining-threats
- https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

CXX-XXXXXX-00 09/18

필요한 조치

악성 크립토마이닝을 탐지하고 차단하려면 고급 엔드포인트 보호 솔루션을 광범위한 방어 전략의 필수 요소로 삼아야 합니다. 네트워크 보안 분석 기술을 활용하면 기업의 네트워크에 기생하여 은밀히 작동하는 크립토마이닝 활동의 근원지를 파악할 수 있습니다. 크립토마이닝 애플리케이션이 아예 설치되지 못하게 막으려면 암호화폐 채굴과 관련된 웹 사이트에 대한 네트워크 연결을 차단해야 합니다. 또한 DNS 계층 보안은 마이닝 트랜잭션이 사이버 범죄자에게 전송되는 것을 방지하므로 크립토마이닝을 막는 데 매우 효과적일 수 있습니다. 다단계 보안 전략을 통해 차세대 방화벽, 엔드포인트, 보안 분석, DNS 계층을 아우른 효과적인 방어선을 구축하면 네트워크에 침투하려는 크립토마이닝 악성 코드를 감지하고 저지할 수 있습니다.

Cisco가 사용자를 보호하는 방법

차세대 방화벽/차세대 침입 방지 시스템	악성 트래픽(예: 암호화폐 채굴 사이트 접속)을 감지하고 차단합니다.
Advanced Malware Protection(AMP) for Endpoints	알려진 악성 크립토마이닝 애플리케이션이 설치되는 것을 방지합니다.
Cisco Stealthwatch®	네트워크에서 이뤄지는 모든 암호화폐 채굴 활동을 감지합니다. 악성 코드에 감염되어 격리 조치된 호스트(Cisco ISE를 통해 격리 조치된 호스트 포함)와 암호화된 트래픽도 예외는 아닙니다.
Cisco Umbrella™	알려진 크립토마이닝 도메인에 트래픽이 전송되는 것을 저지합니다.