Solving the Visibility Gap

Cisco Stealthwatch 가시성 평가로 네트워크 보안 강화

네트워크의 규모가 커지고 복잡해짐에 따라 조직은 날로 지능화되는 위협 행위자들로부터 스스로를 지키기 위해 애쓰고 있습니다. 수개월 동안 탐지 또는 보고되지 않는 공격도 자주 발생합니다. 보안 위험을 탐지하고 완화하려면 네트워크에서 발생하는 상황을 파악할 수 있어야 합니다.

이러한 목표 달성을 돕기 위해 Cisco에서는 Cisco Stealthwatch™ Visibility Assessment를 제공하고 있습니다. 이를 통해 내부 네트워크 가시성 및 전반적인 보안 상태를 평가할 수 있습니다.

Cisco에서는 수백 개의 조직을 평가하여 알려지지 않은 호스트 및 전에 탐지되지 않은 악의적인 네트워크 활동을 즉시 발견했습니다. 이러한 결과는 사용자 환경 내의 공격자 행동과 위치에 대한 인사이트를 제공하여 하나의 보안 이벤트가 전면적인 데이터 보안 침해로 진행되지 않도록 예방하는 데 도움이 될 수 있습니다.

주요 내용

Stealthwatch Visibility Assessment에서는 악의적인 활동 또는 보안 위험과 관련된 10가지 주요 기준을 평가합니다. 이 백서에서는 다음 내용을 다룹니다.

- 가시성이 필요한 10가지 주요 영역
- Cisco Stealthwatch를 통해 이러한 영역을 모니터링하는 방법
- NetFlow가 엔드 투 엔드 네트워크 가시성을 제공하는 방법

내부 모니터링 대상 네트워크

내부 가시성은 네트워크 상태를 이해하는 데 매우 중요합니다. Cisco Stealthwatch 기술은 내부 자산을 지속적으로 모니터링 및 보호하고, 서버와 인터넷 간에 전송되는 데이터를 관찰하며, 트래픽 플로우를 처리합니다. 보안 및 네트워크 담당자는 이 메트릭과 기타 메트릭을 통해 호스트, 시스템 및 리소스를 수량화하여 전체 네트워크 환경을 빠짐없이 관리할 수 있습니다. 또한 중요한 자산을 식별하고, 정책을 검증하고, 컴플라이언스를 감사 및 입증하며, 데이터를 기반으로 더 나은 의사결정을 내릴 수 있습니다.

Stealthwatch Visibility Assessment에서는 네트워크에서 활발하게 통신하는 호스트의 수를 확인합니다.

SMB(Server Message Block) 위험

일부 위협은 SMB(Server Message Block) 프로토콜을 사용하여 호스트를 제어합니다. 많은 조직에서 이 프로토콜을 사용하기 때문에 공격자들이 이 프로토콜을 사용하여 악의적인 활동의 징후를 감출 수 있습니다. Conficker와 같은 파괴적인 표적 악성코드는 SMB의 취약점을 공격하여 프록시 툴을 구축하고, 백도어를 설치하며, 데이터를 파괴하고, 서버를 오프라인으로 전환합니다.

Cisco에서 평가한 조직의 절반에서 의심스러운 SMB 트래픽이 발견되었습니다.

SMB는 일반적인 프로토콜이지만 가시성과 적절한 분석을 통해 올바른 SMB 행동과 잘못된 SMB 행동을 분리할 수 있습니다. 예를 들어, 특히 네트워크 내의 호스트와 인터넷의 호스트 간 SMB 세션이 비정상적으로 많다면, 이는 악성코드 전파를 나타내는 징후일 수 있습니다.

FBI에서 연락이 오는 경우

한 글로벌 유전 서비스 회사는 FBI로부터 중국 사이버 범죄자가 이 회사의 네트워크에 손상을 가했다는 사실을 전해 듣게 되었습니다.

이 회사는 Cisco Stealthwatch System을 설치했고 1주일 이내에 보안 침해의 소스를 식별했습니다. 그 결과, 로컬 사용자가 중국에서 로그인하여 한 번에 수 기가바이트의 중요한 파일을 유출한 것으로 나타났습니다. 이 사용자의 액세스 크리덴셜은 사실 도난당한 것으로, 공격자에게 민감한 데이터에 대한 권한 있는 액세스를 제공한 것입니다.

적절한 네트워크 가시성을 이용했다면, 이 행동을 식별하여 회사의 데이터가 손실되기 전에 치료할 수 있었을 것입니다.

고위험 국가에 대한 트래픽

대부분의 조직은 특정 지리적 위치에서만 비즈니스를 수행합니다. 해당 지역의 외부에서 들어오는 트래픽을 식별하는 것은 위협을 탐지하는 효과적인 방법입니다. 예를 들어, 미국 중부의 거주자에게만 서비스를 제공하는 전력 회사의 경우에는 동유럽이나 아시아에서 발생하는 상당한 양의 트래픽을 경험해서는 안됩니다.

매우 많은 양의 위협 활동이 발생하는 지역에서 오는 트래픽을 탐지하는 것이 특히 중요합니다. Cisco가 평가한 조직 가운데 50%가 이미 고위험 국가의 공격자들에 의해 피해를 입었습니다.

의심스러운 국가에서 발생한 트래픽을 모니터링하는 조직은 시스템이 손상되기 전에 공격을 식별하여 차단할 수 있습니다.

DNS 위험

DNS 서버는 호스트 이름을 적절한 IP 주소로 변환하므로 네트워크 운영, 특히 인터넷에 액세스하는 데 필수적입니다. 허가되지 않은 DNS 서버 사용이 탐지되면 이는 악의적인 활동이나 정책 위반의 징후일 수 있습니다. Cisco가 평가한 조직 중 70%가 넘는 조직의 네트워크에서 권한이 없는 DNS 서버가 사용된 사례가 있었습니다.

많은 조직에서 자체 DNS 서버를 기반으로 하여 금지된 웹 사이트에 액세스하지 못하도록 하는 등의 정책을 시행합니다. 일부 전문 지식을 보유한 사용자는 이러한 정책을 우회하기 위해 권한이 없는 DNS 서버를 사용합니다. 이로 인해 사용자가 안전하지 않은 웹 사이트를 방문하거나 웹 컨텐츠에 대한 회사 정책을 위반하는 경우 조직이 위험에 처할 수 있습니다.

더욱 심각한 점은, Cisco 2016 연례 보안 보고서에 따르면 악성코드의 91.3%가 공격에 DNS를 사용한다는 것입니다. 악성코드는 대개 감염된 컴퓨터를 재구성하여 악성 DNS 서버를 사용하도록 합니다. 이러한 악성 서버는 익스플로잇을 일으키거나 액세스 크리덴셜을 피싱하는 웹 사이트로 사용자를 리디렉션하여, 조직은 시스템이 손상되거나 데이터가 유출되는 위험에 놓이게 됩니다.

프록시 위반

대부분의 조직에서는 프록시 서버를 사용하여 알려진 악성 사이트, 부적절한 콘텐츠 및 데이터 유출을 차단하는 동시에 사용자의 인터넷 활동 로그를 유지 관리합니다. 사용자는 정책을 우회하기 위해 이러한 프록시 서버를 우회하려고 시도할 수 있으며, 잘못 구성된 디바이스는 우발적인 컴플라이언스 위반을 초래할 수 있습니다. 이 두 가지 시나리오 모두 조직을 데이터 손실 및 공격 위험에 빠뜨립니다. Cisco Stealthwatch는 엔드 투 엔드 네트워크 가시성 및 모니터링을 통해 프록시 정책을 지속적으로 감사하고 위반이 탐지될 때 알림을 제공합니다.

원격 액세스 보안 침해

원격 네트워크 액세스는 빠른 속도로 웬만한 회사의 표준 비즈니스 방식이 되고 있습니다.

언제 어디서나 회사 리소스에 액세스할 수 있는 기능은 이동이 잦은 직원에게 중요하지만, 이러한 서비스는 공격자들 사이에서도 인기를 얻고 있습니다. 보안이 침해된 경우, 원격 액세스 서비스는 공격자들에게 정당한 사용자와 동일한 권한을 제공합니다.

Cisco가 평가한 조직의 약 38%가 원격 액세스로 인해 몇 가지 유형의 보안 침해를 경험했습니다. 의심스러운 활동을 식별하려면 원격 액세스 트래픽에 대한 가시성을 반드시 확보해야 합니다.

비인가 서버 활동

비인가 서버는 엔터프라이즈 네트워크에 설치되지만 관리자에게 제어 권한이 없는 서버입니다. 공격자들은 비인가 서버를 사용하여 네트워크에 대한 지속적인 액세스 권한을 획득할 수 있습니다. 최근 한 사례로, Cisco에서는 조직의 내부 네트워크에서 사용 중인 알 수 없고 권한이 없는 서버를 30개 이상 발견했습니다. 이러한 서버의 상당수는 패치 및 보안 표준이 최신 상태가 아니었기 때문에 공격에 취약한 상태였으며 조직이 위험에 노출되어 있었습니다.

때로는, 업무를 위해 빠른 테스트 환경을 원하는 엔지니어와 같이 악의 없는 직원이 비인가 서버를 설치하는 경우가 있습니다. 보안 팀에는 이러한 서버에 대해 거의 알리지 않으므로 보안이 올바르게 설정되었다고 확신할 수 없습니다. 만약 테스트가 완료된 후 직원이 서버를 비활성화하는 것을 잊어버리는 경우라면 문제는 더욱 심각해집니다.

또한 공격자들은 손상시킨 네트워크 내부에 서버를 설치합니다. 그런 다음, 이 서버를 네트워크 전반에서 측면으로 이동할 때 작전의 기반으로 사용하거나, 훔친 데이터를 유출하기 전에 해당 데이터의 스테이징 포인트로 사용합니다.

맞춤형 악성코드

Cisco Stealthwatch 평가가 진행되는 동안, 한 대규모 기술 기업에서는 최종 사용자 워크스테이션의 거의 절반이 해당 네트워크 전용으로 작성된 맞춤형 악성코드에 감염되었음을 발견했습니다.

악성코드에 의해 알 수 없는 기간 동안 조용히 데이터가 유출되고 있었습니다. 이러한 상황의 경우 별다른 징후가 없지만, 행동 분석을 통해 네트워크 전반에서 악성코드 검사, 연결 및 전파를 탐지할 수 있었습니다.

행동 분석

오늘날의 네트워크는 규모가 크고 복잡하여, 위협 행위자들이 다양한 방법으로 네트워크에 침입할 수 있습니다. 더욱 우려되는 점은 대부분의 공격자들이 취약하거나 초기 설정되었거나 도난당한 액세스 자격 증명을 사용하므로 정당한 사용자처럼 보인다는 것입니다. 침입자와 침입자가 모방하는 사용자를 분리시키는 한 가지 중요한 방법은 네트워크 활동에서 비정상적이거나 공격과 일치하는 행동을 모니터링하는 것입니다.

예를 들어, 네트워크를 검사하는 호스트는 정찰을 수행하는 것일 수도 있고, 악성코드를 전파하는 것일 수도 있습니다. 마찬가지로, 마케팅 부서에서 근무하며 주로 하루에 몇 메가바이트의 네트워크 리소스에 액세스하는 사용자가 갑자기 몇 기가바이트의 엔지니어링 자료를 다운로드하는 경우, 네트워크 외부로 데이터를 유출할 준비를 하고 있는 것일 수도 있습니다.

Cisco에서 평가한 모든 조직의 네트워크에는 이상 징후를 보이는 의심스러운 행동이 있었습니다.

위험에 처한 보호 자산

모든 조직에는 네트워크의 나머지 부분보다 면밀한 조사와 방어가 필요한 매우 민감한 데이터가 있습니다. 이러한 데이터는 종종 위협 행위자의 궁극적인 목표물이 되기 때문에 이를 보호하는 것이 사이버 보안 전략에서 가장 중요한 부분이 될 수 있습니다. Cisco Stealthwatch 기술을 사용하면 이런 귀중한 리소스를 면밀히 모니터링하면서 악의적인 활동, 정책 위반 및 잘못된 행동의 징후를 찾아낼 수 있습니다. Cisco Stealthwatch는 내부 호스트 또는 외부 인터넷에서 데이터에 액세스할 때 이를 탐지하고, 데이터 센터 같은 민감한 시스템 내부 또는 시스템 간의 트래픽에 대한 가시성을 확장할 수 있습니다.

텔넷 위험

텔넷은 오래되고 안전하지 않은 프로토콜이며, 이를 사용하면 자격 증명 손상 및 데이터 손실이 발생할 수 있습니다. 텔넷은 머신 간의 통신을 용이하게 하지만 대부분의 버전에 효과적인 암호화 기능이 없으므로 패킷 스니퍼의 주요 표적이 됩니다. 데이터가 일반 텍스트로 전송되면 공격자가 이를 가로채서 비밀번호 및 기타 민감한 정보를 확보할 수 있습니다.

대부분의 조직에서는 이 프로토콜을 사용하지 않는다고 생각하지만, Cisco의 평가 결과, 67%에 달하는 조직의 네트워크에 텔넷 트래픽이 있는 것을 확인하였습니다.

민감한 데이터, 금융 프로그램 및 고객 정보를 저장하는 메인프레임 및 기타 시스템에서는 종종 텔넷을 실행하고 이로 인해 공격에 노출됩니다. 1994년 이후부터 소프트웨어 공학 연구소(Software Engineering Institute)의 CERT 부서에서는 텔넷과 같은 일반 텍스트 인증이 아닌 다른 인증을 사용하도록 권장했습니다.

조직이 텔넷에 의해 위험에 노출되지 않도록 하려면, 보안 운영자가 엔터프라이즈 네트워크 전반에 걸쳐 어디서나 텔넷 활동을 탐지하고 대응할 수 있어야 합니다.

네트워크의 어두운 영역 밝히기

네트워크와 데이터를 효과적으로 보호하려면 이러한 각 영역에 대한 가시성을 확보하는 것이 중요합니다. 다행히 대부분의 네트워크에는 기본으로 장착된 모니터링 기능이 있으므로 단순히 이러한 기능을 활용할 수 있는 방법이 필요합니다.

NetFlow와 같은 네트워크 트래픽 메타데이터는 라우터, 스위치 및 방화벽을 포함한 대부분의 네트워크 인프라 디바이스에 내재되어 있습니다. Cisco Stealthwatch는 이 데이터를 수집 및 분석하고 IP 주소, 포트, 사용자, 디바이스 및 애플리케이션을 포함한 모든 네트워크 트래픽의 감사 추적을 생성합니다. Cisco Stealthwatch는 엄두를 못 낼 정도로 큰 용량의 스토리지 공간 없이도 수개월 또는 수년 동안의 플로우 데이터를 저장할 수 있습니다.

Cisco Stealthwatch를 사용하면 보안 전문가가 다음을 수행하는 데 필요한 심층적인 네트워크 인사이트를 확보할 수 있습니다.

- 실시간으로 의심스러운 공격 행동 탐지
- 침입 경로를 파악하기 위해 이전의 공격 시도 조사
- 특정 사용자, 디바이스, 위치 및 시간 범위로 돌아가서 공격 추적
- 조직의 보안 상태 개선

Stealthwatch Visibility Assessment는 네트워크에 환하게 불을 밝혀 내부 가시성 및 전반적인 보안 상태를 평가합니다. 가시성 평가는 14일 동안 네트워크 텔레메트리를 수집하는 Stealthwatch Management Console 및 Flow Collector로 구성됩니다. 그 이후 상세한 정보가 포함된 가시성 평가 보고서 및 현재의 보안 위험 요소에 대한 분석이 제공됩니다.

자세히 알아보려면 www.cisco.com/go/stealthwatch-free-assessment를 방문하십시오.

C11-738293-00 12/16