사례 연구

최신 악성 프로그램 차단 기술이 적용된 클라우드로 이전한 Heritage Bank

요약

고객명: Heritage Bank
규모: 직원 수 800명, 고객 수 30만 명
업종: 금융 서비스
위치: 호주 전국에 영업망 및 퀸즐랜드주에 61개의 지점

"Threat Grid와 통합된 AMP for Endpoints를 구축한 데 이어 AMP for Networks를 설치하면서 비로소 안심할 수 있게 됐습니다. 전세계에서 사용 중인 컴퓨터 중 한 대만 악성 프로그램에 감염돼도 사태가 심각해지는데 Threat Grid는 이를 감지하는 즉시 나머지 컴퓨터도 철저히 보호합니다."

라클란 피터스(Lachlan Peters)
Heritage Bank 보안팀장

호주 은행 중 가장 많은 고객을 확보하고 있는 Heritage Bank는 1875년 이래로 "사람 우선" 주의를 실천해 왔습니다. 이 은행은 지난 100년간 회원 대상으로 주택 건설 자금 융자를 위한 공동 출자금 확보에 주력해온 두 주택 금융 조합이 1981년에 합병하면서 탄생했습니다. 이익 배분을 위한 주주가 없는 관계로 Heritage는 인기 상품, 이율 및 서비스의 제공으로부터 발생한 이익을 재투자하고 있습니다.

"사람 우선" 주의는 모토 그 이상의 의미를 갖습니다. 보안팀장 라클란 피터스의 보안에 대한 시각에서도 엿볼 수 있듯 "사람 우선" 주의는 Heritage Bank와 그 문화에 깊숙이 깃들여 있습니다.

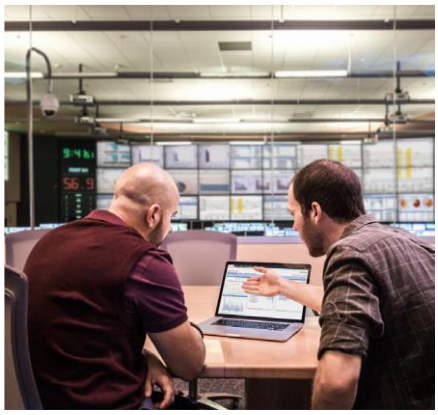
피터스는 다음과 같이 설명합니다. "회원들에게 일상 생활에 대한 걱정 없이 자신의 목표를 추구할 자유를 선사하는 것이 Heritage Bank의 목표이기 때문에 우리가 제공해야 할 금융 상품과 서비스에 맞춰 보안도 꾸준히 현대화하고 있습니다. Heritage Bank는 전통적인 보안 솔루션을 사용해왔으나 클라우드 기반 솔루션, 이메일 및 협업의 필요성이 증가하면서 기존의 솔루션으로는 전반적인 보안 공백을 메울 수 없게 됐습니다."

Heritage는 전통적으로 물리적 보안을 중시해왔는데, 이 같은 보안 전략은 악의를 품은 공격을 강력하게 막아내지만 일단 안으로 들어오면 감당할 수 없다고 피터스는 설명합니다.

그러나 암호화된 트래픽과 정교한 공격 수법이 등장하면서 피터스가 이끄는 보안 팀은 포괄적인 보호 능력을 확보하기 위해 가시성을 높여야 했습니다.

피터스는 다음과 같이 말합니다. "클라우드 솔루션, SaaS 및 웹 기반 앱이 보편화되자 전송 중인 트래픽을 다른 사람들이 이해하지 못하도록 암호화 사용 비중을 늘렸지만 보안 솔루션도 트래픽을 이해하지 못한다는 게 문제였습니다. 또 다른 문제는 직원들이 빈번히 피싱 및 스피어 피싱 공격에 노출되고 제로 데이 공격도 끊이지 않는다는 점입니다. 시그니처 기반의 보안만으로는 이러한 유형의 위협을 감지하고 차단하기에 역부족입니다."

Heritage Bank가 Cisco AMP for Endpoints와 Threat Grid로 거둔 효과:



미심쩍은 이메일을 수작업으로 검사하는 데 소요되는 시간 월평균 2일 절약

클라우드와 SaaS에 더욱 안전하게 트래픽 전송

APT를 차단할 방안을 모색하던 Heritage는 FireEye와 시스코를 비롯한 여러 보안 솔루션 제공업체의 솔루션 평가 과정에 참여했습니다.

피터스는 다음과 같이 설명합니다. "Threat Grid가 내장 된 Cisco AMP for Endpoints는 위협을 원천 봉쇄할 뿐만 아니라 모니터링, 탐구학습법(heuristics) 및 샌드박싱을 통해 완벽한 보호 기능을 발휘함으로써 엔드포인트를 지속적으로 보호한다는 점을 알게 됐습니다. 시스코의 솔루션이 상대적으로 보다 체계적이었습니다. 시스코는 보안 전문 기업답게 AMP for Networks 같은 다른 솔루션과의 통합을 중시하고 Talos의 위협 인텔리전스도 지원 받습니다. 이처럼 다양한 솔루션을 연계하면 시너지 효과가 발생합니다. 다른 솔루션은 진화하는 위협 상황에 대한 이와 같은 수준의 가시성을 제공하지 못합니다."

보안과 생산성의 동시 향상

Cisco® AMP for Endpoints와 Cisco Threat Grid의 구축을 통하여 생산성 증대 효과와 보안 강화 효과가 동시에 발생했다고 피터스는 강조합니다.

이어서 피터스는 다음과 같이 설명합니다. "AMP for Endpoints를 도입하자 비즈니스 프로세스에 악영향(특히, 이메일 처리 속도 저하)을 미치는 기존의 게이트웨이 솔루션에 대한 의존도가 줄어들면서 안정성이 향상됐습니다. AMP for Endpoints는 악성 파일을 거의 빠짐없이 감지하는 반면, 오탐지 발생률이 극도로 낮습니다. 이런 사실을 알기에 수작업으로 이메일을 검사할 필요가 없어서 한 달에 이틀은 절약되는데, 이는 세 명으로 구성된 보안 팀에게는 대단한 도움입니다."

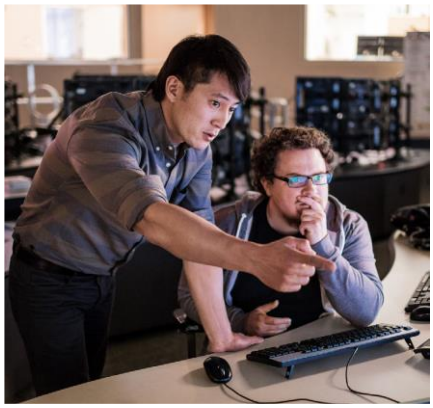
또한 Heritage는 다른 보안 계층을 우회하고 조심성 없는 사용자를 속일 수 있었던 최신 공격 수법도 보다 효과적으로 차단할 수 있게 됐습니다.

피터스는 다음과 같이 말을 잇습니다. "지난 해 전통적인 시그니처 기반 솔루션이 제대로 인지하지 못하는 매크로 중심의 워드 문서가 쇄도했습니다. 그래서 사이버 범죄자가 암호를 조금만 손보면 시그니처가 일치하지 않더라도 무사히 보안 검사를 통과할 수 있었습니다. 그런데 AMP for Endpoints는 이러한 유형의 공격을 포착하고 기존의 게이트웨이 솔루션이나 엔드포인트 솔루션 같은 다른 보안 계층으로는 해소할 수 없는 보안 공백을 메우고 있습니다."

사용자 교육은 항상 만만치 않은 과제인데 피싱 및 스피어 피싱 공격은 사용자가 악성 링크나 첨부 파일을 클릭하면서 본격적으로 전개됩니다. 그러나 AMP for Endpoints는 견고한 최종 방어선을 구축하고 최종 사용자가 피싱 사기에 노출되기도 전에 이를 감지하여 차단한다고 피터스는 강조합니다.

이러한 유형의 공격은 랜섬웨어 같이 좀 더 심각하고 큰 비용 손실을 초래하는 공격으로 이어지기도 합니다. 그러나 Heritage Bank에서는 랜섬웨어와 사회 공학적 수법에 의존한 기타 공격이 더 이상 문제가 되지 않습니다.

피터스는 다음과 같이 강조합니다. "모든 기업이 랜섬웨어 때문에 골머리를 앓고 있습니다. Threat Grid와 통합된 AMP for Endpoints를 구축한 데 이어 AMP for Networks를 구축하면서 비로소 안심할 수 있게 됐습니다. 전세계에서 사용 중인 컴퓨터 중 한 대만 악성 프로그램에 감염돼도 사태가 심각해지는데 Threat Grid는 이를 감지하는 즉시 나머지 컴퓨터도 철저히 보호합니다."



더욱 빠르고 쉽게 보안 공백 해소, 위협 심각도 지정 및 치료

Heritage는 새로 도입한 보안 솔루션을 기반으로 하여 비즈니스도 더욱 효율적으로 운영할 수 있게 됐습니다.

피터스는 다음과 같이 설명합니다. "네트워크에서 트래픽이 암호화되고 나면 프록시 서버와 IPS가 할 수 있는 일은 다소 제한적입니다. 직원들이 일반적으로 보안을 유지하기 어려운 클라우드 기반 솔루션과 기타 솔루션을 사용하더라도 AMP for Endpoints와 Threat Grid가 있기에 보안 팀이 안심하고 비즈니스를 지원할 수 있습니다. AMP for Endpoints를 사용하면 다른 솔루션이 검사하거나 감지하지 못하는 것들이 유입되지 않을까 걱정되어 밤잠을 설치지 않아도 됩니다."

성공과 직결되는 통합

피터스와 그의 팀은 미심쩍은 파일을 더욱 확실히 파악하는 데 Threat Grid의 패턴 분석 및 샌드박싱 기능을 활용하고 있습니다.

피터스는 이어 다음과 같이 말합니다. "Threat Grid 보고서를 통해 얻은 결과를 토대로 침해지표(Indicators of Compromise: IoC)를 작성하고 방화벽 로그를 확인할 수 있습니다. 파일이 악성인지 파악하고 악성 파일로 판명된 경우 해당 파일을 철저히 차단하므로 더 이상 불안해할 필요가 없습니다. 호시탐탐 방어 시스템을 우회할 기회를 엿보는 범죄자보다 한발 앞서가려면 AMP for Endpoints 및 AMP for Networks와 통합된 Threat Grid가 필수적입니다. 개인적으로, 아직 이 솔루션을 도입하지 않은 기업에 적극 추천합니다."

현재 Heritage Bank는 AMP for Endpoints를 보완하기 위해 위협이 엔드포인트에 도달하기 전에 네트워크 내부에서 감지하여 차단하는 AMP for Networks도 사용하는 중입니다.

이와 관련하여 피터스는 다음과 같이 설명합니다. "이제 막 AMP for Networks를 설치하기 시작했는데 조만간 두 솔루션 간의 연동에 의한 진정한 시너지 효과가 발생할 것으로 기대합니다. 사용자가 파일에 액세스하기도 전에 AMP for Networks로 미심쩍은 파일을 감지하고, Threat Grid에 미심쩍은 파일을 업로드하여 분석함으로써 악성 여부를 판명할 수 있습니다. AMP for Endpoints의 부담을 일부나마 덜 수 있게 된 것입니다."

또한 AMP for Networks는 보다 우수한 가시성을 제공하므로 보다 정확하게 위협의 영향을 평가하고, 대응해야 할 위협의 우선 순위를 정하며, 보다 효과적으로 위협에 대응할 수 있습니다. 이에 대한 피터스의 설명은 다음과 같습니다. "AMP for Networks를 설치했더니 벌써 가시성이 유례없는 수준으로 향상됐습니다. 과거에는 네트워크 내부에 구체적으로 어떤 위협이 존재하는지 알고 있더라도 직감에 의존할 수밖에 없었습니다. 그러나 이제 파일의 궤적을 바탕으로 실제로 어떤 일이 일어나고 있는지 확인하고 모든 인스턴스에 우선 순위를 매길 수 있습니다. 예를 들어, 장비가 악성 프로그램을 실행하여 격리 조치됐거나 악성 파일이 침투하려고 시도한 경우 보안 팀이 그 즉시 인지할 수 있습니다. 무슨 일이 벌어질 조짐만 보여도 보안 팀이 어디부터 살펴봐야 하는지 알 수 있는 것입니다."

통합 중심의 최신 악성 프로그램 차단 체제 덕분에 피터스와 그의 팀은 감지 시간을 단축할 수 있습니다. 결과적으로 공격으로 인한 손실을 최소화하고 더욱 빠르고 손쉽게 치료할 수 있습니다.

피터스는 다음과 같이 말을 잇습니다. "꽤 오래 전에 엔드포인트에 보안 체제를 전면적으로 재구축했는데, 재구축 작업을 담당했던 IT 부서와 재구축 작업이 진행되는 동안 컴퓨터를 사용하지 못하게 된 직원에게 그리 큰 불편은 없었습니다."

제품 및 서비스:

- Cisco Advanced Malware Protection(AMP) for Endpoints
- Cisco Threat Grid
- Cisco AMP for Networks
- Cisco Firepower® Management Center

AMP for Endpoints, AMP for Networks, Threat Grid의 전반적인 운영 상황은 Cisco Firepower Management Center를 통해 확인할 수 있습니다. 악성 프로그램의 활동 현황과 예상 동태를 보다 완벽하게 파악하고 있게 됐다고 피터스는 설명합니다.

아울러 그는 다음과 같이 말합니다. "AMP for Endpoints에서 명령줄 정보를 선택하는 간단한 방법으로 악성 프로그램이 특정 솔루션의 일부 보안 기능을 비활성화하려고 시도했는지 확인할 수 있습니다. 또한 파일 목록을 훑어보다가 전염률이 낮은 인스턴스를 발견한 경우 버튼만 클릭하면 자동으로 모든 파일이 치료됩니다."

클라우드를 염두에 둔 향후 계획

피터스는 연결이 이뤄지기도 전에 악성 연결을 차단하는 시스코 클라우드 기반의 통합 보안 솔루션을 추가로 도입하는 방안을 고려 중입니다. 1차 방어선에서 악성 도메인, URL, IPS 및 파일을 차단하는 인터넷 보안 게이트웨이인 Cisco Umbrella가 대표적인 경우에 해당됩니다.

이와 관련하여 그는 다음과 같이 말합니다. "DNS 터널링이 앞으로 더 많은 문제를 야기할 것으로 예상되는데, AMP 외에도 이와 같은 유형의 보안 솔루션은 악성 프로그램이 네트워크에 침투하는 것을 막는 데 도움이 됩니다. 악성 프로그램이 침투할 틈을 주지 않으니 암호화나 다른 피해를 입을 염려도 없습니다."

또한 피터스는 네트워크 내외부에 존재하는 SaaS(Software-as-a-Service) 애플리케이션을 찾아서 통제할 수 있는 클라우드 액세스 보안 브로커(CASB)인 Cisco CloudLock을 구현하는 방안도 고려하고 있습니다.

피터스는 다음과 같이 설명합니다. "기업에서 사용되는 SaaS 솔루션이 늘어나면서 IT 부서의 통제력은 약화되고 있기 때문에 CASB가 필수적일 것으로 전망됩니다. Cisco AMP와 Threat Grid을 통해 얻은 안정감을 한결같이 유지하려면 직원들이 아무 생각 없이 특정한 보안 옵션을 비활성화하지 않는지 모니터링하는 일도 게을리하지 말아야 합니다."

피터스가 이끄는 보안 팀은 직원과 고객의 요구사항을 미리 간파하는 동시에 정교한 공격을 차단하기 위하여 노력을 기울이고 있습니다.

피터스는 다음과 같이 말합니다. "Heritage 보안 팀은 항상 한걸음 앞서가면서 고객에게 기대 이상의 보호 환경을 지원하는 데 만전을 기하고 있습니다. 이러한 점에서 시스코와 우리는 유사한 철학을 갖고 있습니다. 시스코 통합 보안 아키텍처의 규모와 장점은 투자가치를 상쇄하고도 남을만한 시너지 효과를 창출합니다. 특히 플랫폼 간 공유 정보를 활용할 경우 그 효과가 배가됩니다.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco는 전 세계에 200여개의 사무소를 두고 있습니다. 주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트(www.cisco.com/go/offices)를 참조하십시오.