Recorded Future®

브랜드(Brand) 인텔리전스로 조직 보호

브랜드 공격을 신속하게 탐지하고 차단

조직이 자사 브랜드를 겨냥한 사이버 공격을 인지하지 못하는 경우가 너무 많습니다. 위협 행위자가 타이포스쿼팅(typosquatting) 웹사이트, 데이터 유출, C&C(command-and-control) 공격 등 다양한 방식으로 조직의 네트워크를 건드리지 않으면서 브랜드를 공격할 수 있기 때문입니다. 이로 인해 고객 불신에서 막대한 재정적 손실에 이르기까지 치명적인 결과가 초래될 수 있습니다. 여태까지 보안 담당자가 조직 네트워크 외부에 대해 알 수 있는 정보는 제한적이었으며, 사이버 범죄자들이 이러한 공격을 실행하는 것으로 알려진 다크웹에 대한 가시성은 전무한 상황이었습니다. 다음과 같은 과제를 해결해야 합니다.

고객과 직원을 겨냥한 피싱 공격

위협 행위자는 타이포스쿼팅 웹사이트를 만들어 고객과 직원을 유인하고 피싱 공격을 통해 민감한 정보를 노출시킵니다. 이러한 사이트를 효과적으로 추적할 수 있는 방법이 없다면 보안 팀은 악성 콘텐츠를 찾아 제거하는 데 막대한 시간과 자원을 소비하고 효과도 미미할 수 밖에 없습니다. 가짜(유사) 도메인을 일일이 찾아서 제거하기가 너무 어렵기 때문에 많은 가짜 사이트들이 웹에서 장기간 피해를 가중시키게 됩니다.

불완전한 가시성으로 인한 위협 탐지 실패

비공개 다크웹 소스를 확인하지 못한다면 조직은 자사 브랜드나 인프라에 막대한 위험을 초래하는 중요한 정보를 놓치게 됩니다. 가장 일반적인 사이버 공격들이 모두 폐쇄적인 다크웹과 소셜 미디어에서 시작됩니다. 이러한 소스에 대한 명확한 가시성 없이는 보안 팀이 다가오는 공격을 식별 할 수 없으며, 이미 진행 중인 공격에 대응하는 데 급급하게 됩니다.

데이터 유출 및 도용

도난당한 기업 데이터는 텍스트 공유 사이트와 다크웹 채널에 공개됩니다. 사이버 범죄자들은 흔히 조직 내부로 침투하기 위해 이러한 소스에서 유출된 계정 정보를 구매합니다. 그 곳에서 은행 정보, PII, 기프트 카드, 이메일 등을 구매할 수도 있습니다. 또한 직원들이 실수로 GitHub와 같은 사이트에 민감한 회사 정보를 업로드하는 경우도 빈번하게 발생합니다. 자체적으로 민감한 정보를 모니터할 수 없다면 조직은 결국 이로 인한 재정적, 법적, 평판 피해에 노출됩니다.

레코디드 퓨처:
탁월한 브랜드(Brand) 인텔리전스

레코디드 퓨처는 공개/비공개 웹, 딥웹, 다크웹 전반에서 자동으로 데이터를 수집하고 분석하여 관련 데이터를 실시간으로 확인합니다. 보안 팀은 광범위한 브랜드(Brand) 인텔리전스를 기반으로 위조 도메인, 피싱, 데이터 유출 등과 같은 브랜드 공격을 사전에 탐지하고 차단할 수 있습니다.

레코디드 퓨처의 특허 받은 알고리즘 프로세스와 자연어 처리(natural language processing) 기술은 최신 위협, 고객 브랜드, 고객 인프라 간의 관계를 파악하여 바로 활용 가능한 브랜드 인텔리전스를 제공합니다. 단순한 키워드 모니터링 이상의 브랜드 인텔리전스는 브랜드 공격을 선제적으로 탐지하고 비즈니스에 피해가 미치기 전에 차단할 수 있도록 해줍니다. 레코디드 퓨처를 사용하면 다음과 같은 다섯 가지 사용 사례로 브랜드를 쉽게 보호할 수 있습니다.

도메인 오남용 탐지

레코디드 퓨처는 자동으로 신규 등록 도메인을 수집하고 분석하여 타이포스쿼팅(typosquatting) 웹사이트와 피싱 미끼를 찾아냅니다. 보안 팀은 강력한 패턴 검색과 DNS 네임 순열 탐지 기능을 사용하여 자사 브랜드에 대한 위협 경고를 수신할 수 있습니다. 각 도메인마다 위험 점수가 매겨지며 라이브 DNS 조회를 통해 관련 IP 주소, 메일 서버, 네임 서버에 대한 심층 조사가 가능합니다. 보안 팀은 레코디드 퓨처에서 제공되는 위험 점수와 풍부한 컨텍스트를 통해 해당 IP와 도메인을 심층적으로 조사할 수 있습니다. 또한 레코디드 퓨처 플랫폼에서 바로 오남용 도메인에 대한 보고와 차단 요청이 가능합니다.

레코디드 퓨처 활용

Intelligence Goals Library에서 타이포스쿼팅(typosquatting) 탐지를 위한 경고를 설정하십시오. 알림은 이메일을 통해 수신하거나 SIEM으로 푸시할 수 있습니다. Intelligence Cards™로 전환하여 악성 도메인에 대한 추가 정보를 얻을 수 있습니다. 레코디드 퓨처 플랫폼에서 바로 차단 요청을 전송할 수 있습니다. 해당 웹 사이트가 SLA 기간 내에 신속하게 제거되어 위험 및 평판 손상을 완화합니다.

데이터 유출 모니터링

텍스트 공유 사이트(paste site)와 다크웹에 유출된 회사 데이터와 계정을 일일이 수작업으로 검색하는 것은 거의 불가능하며 위험한 방법입니다. 레코디드 퓨처는 민감한 데이터를 판매하는 범죄 포럼을 비롯한 이러한 사이트들의 정보를 즉각적으로 수집하여 처리합니다. 일부 도메인에 대해서는 Insikt Group의 전문 분석이 수행합니다. 레코디드 퓨처 Insikt Group은 광범위한 업계 지식을 보유한 세계적인 수준의 분석가, 언어학자, 보안 연구원들로 구성됩니다. 레코디드 퓨처의 광범위한 소싱과 자연어 처리(NLP)에 Insikt Group의 전문적인 조사와 내부 액세스가 결합되어 데이터 유출 발생 시 즉시 경고를 생성합니다. 레코디드 퓨처는 이러한 게시물을 캐싱하여 분석가가 적절하게 검토하고 에스컬레이션할 수 있도록 합니다.

레코디드 퓨처 활용

온라인에서 민감한 기업 데이터가 언급되면 표시하도록 Intelligence Goals Library에서 알림을 설정할 수 있습니다. 알림이 트리거되면 이메일 또는 레코디드 퓨처 모바일 앱으로 알림이 전송됩니다. 세부 정보를 검토하여 직원이 GitHub와 같은 공유 사이트에 기업 소유의 소스 코드를 게시했는지 확인합니다. 카피를 검토하여 사건을 확인하고 레코디드 퓨처 플랫폼에서 바로 게시 중단 요청을 전송합니다.

업계 위협 모니터링

사이버 범죄자가 귀사의 동종 업계 기업들을 공격하고 있다면, 귀사 역시 타겟이 될 수 있습니다. 레코디드 퓨처는 종합적인 업계 위협 뷰에서 특정 산업에 대한 알려진 위협과 최신 위협을 보여줍니다. 고객은 이를 통해 자사 브랜드와 인프라를 위협하는 위험을 선제적으로 방어할 수 있습니다. 업계 위협 뷰는 해당 업계 기업의 맞춤 왓치리스트(watchlist)에 따라 제공되므로 불필요한 정보를 제외한 꼭 필요한 브랜드 인텔리전스를 얻을 수 있습니다.

레코디드 퓨처 활용

커스텀 왓치리스트(watchlist)로 업계 위협 뷰를 구성하십시오. 해당 업계를 타겟으로 하는 위협에 대한 경고를 설정하십시오. 특정 멀웨어가 동종 업계의 다른 회사를 공격할 경우 이메일 또는 레코디드 퓨처 모바일 앱을 통해 알림을 수신할 수 있습니다. 멀웨어 Intelligence Card™를 검토하고 멀웨어가 어떤 기술 취약성을 통해 배포되고 있는지 알려주는 Insikt Note를 확인하십시오. 이 인텔리전스를 IT 팀과 공유하여 해당 취약성에 대한 패치가 우선적으로 이루어지도록 하십시오.

브랜드 공격 방어

조직은 한정된 소스에서 비효율적인 수작업 방식으로 자사 브랜드에 대한 내용을 모니터하는 데 막대한 자원을 소비합니다. 그러나 위협 행위자들의 진정한 온상은 비공개 범죄 포럼, 소셜 미디어 채널, 외국어 사이트입니다. 레코디드 퓨처는 사이버 공격과 관련하여 브랜드가 언급될 경우 즉시 탐지하고 경고합니다. 이를 통해 해당 공격에 대한 대응 조치를 취할 수 있습니다.

레코디드 퓨처 활용

온라인에서 브랜드가 언급되면 표시하도록 Intelligence Goals Library에서 알림을 설정하십시오. 알림이 트리거되면 이메일 또는 레코디드 퓨처 모바일 앱으로 알림이 전송됩니다. 캐싱된 카피를 검토하여 귀사 고객을 겨냥한 피싱 공격에 대해 알아보십시오. 레코디드 퓨처 플랫폼에서 바로 차단 요청이 가능합니다.

인프라 위험 모니터링

보안 팀은 레코디드 퓨처의 기술을 구성하여 인프라에 대한 위협을 지속적으로 모니터링함으로써 은밀하게 자행될 수 있는 공격을 사전에 방지할 수 있습니다.

자사 도메인 및 IP 주소에 대한 알림을 구성하여 디지털 자산에 대한 악의적인 언급이 있을 때 즉시 경고를 수신할 수 있습니다. 보안 팀은 실시간 브랜드 인텔리전스를 통해 네트워크를 신속하게 보호하고 공격을 방지할 수 있습니다.

레코디드 퓨처 활용

인프라 위험이 증가하면 알 수 있도록 Intelligence Goals Library에 알림을 설정하십시오. 회사 IP 주소의 위험 점수가 높아지면 이메일 또는 레코디드 퓨처 모바일 앱으로 알림이 전송됩니다. 위험 규칙 증거를 검토하여 IP 주소가 C&C(command-and-control)서버에 연결되었는지 확인합니다. 감염된 컴퓨터를 비활성화하여 피해를 방지하십시오. 동일한 IP 주소로 호스팅되는 관련 도메인을 파악하여 레코디드 퓨처 플랫폼에서 바로 차단을 요청할 수 있습니다.

레코디드 퓨처의 브랜드 인텔리전스 모듈은 이전에는 식별이 어렵거나 불가능했던 위협에 대한 탁월한 가시성을 제공합니다. 레코디드 퓨처는 타의 추종을 불허하는 방대하고 다양한 공개, 비공개, 기술 소스를 모니터하여 사이버 공격으로부터 브랜드를 보호하는 데 필요한 정보와 컨텍스트를 보안 팀에 제공합니다. 게시 중단(Takedown) 서비스를 통해 인터넷 상의 악성 콘텐츠를 쉽고 빠르게 제거할 수 있습니다.

주요 기능

- 타의 추종을 불허하는 방대하고 다양한 공개, 비공개, 기술 소스와 딥웹, 다크웹 전반을 모니터하는 탁월한 소스 커버리지
- 인터넷 전반에 대한 신속하고 광범위한 수집 및 분석
- 빠르고 확실한 대응을 위한 동적 위험 점수 및 증거 제공
- 악성 도메인을 신속하게 제거하는 차단(Takedown) 서비스
- 구성 가능하고 즉시 사용 가능한 브랜드 알림 및 데이터 시각화 기능
- 맞춤형 업계 위협 뷰

주요 이점

IDC는 레코디드 퓨처가 조직에 다음과 같은 이점을 제공한다고 보고했습니다.

- 위협 식별 10배 가속화
- 영향을 받기 전에 22% 더 많은 위협 파악

Recorded Future®

www.recordedfuture.com

@RecordedFuture

레코디드 퓨처 소개

레코디드 퓨처(Recorded Future)는 컨텍스트 기반의 실행 가능한 인텔리전스로 실시간 의사결정을 지원하여 보안 및 IT 팀의 효율성을 강화하는 보안 인텔리전스를 제공합니다. 레코디드 퓨처는 일반 웹 사이트는 물론 다크웹과 딥웹까지 광범위한 소스의 데이터를 분석하여 위협 정보, 디지털 브랜드 위험, 취약점, 써드파티 위험, 지정학적 위험 등에 대한 단일 뷰를 제공합니다.