일반적인 사기 탐지

c Secure Bank

왜 Group-IB인가?

Group-IB는 첨단 기술을 사용하여 사이버 범죄 및 사기를 예방하고 조사하는 선도적 인 국제 기업 중 하나이다.

1000+

전 세계적으로 성공적인 조사, 특히 복잡한150 건의 형사 사건

$300 000 000

우리의 노력 덕분에 Group-IB의 고객들이 돌려 받은 금액이다

EUROPOL INTERPOL

공식 파트너 인터폴(EUROPOL) 및 인터폴(INTERPOL)

OSCE

유럽 안보 협력기구 (OSCE)에 의해 추천되어 있다

WORLD ECONOMIC FORUM

세계 경제 포럼의 정회원

Forrester Gartner

Group-IB 의 위협 인텔리젠스(Threat Intelligence)– Forrester и Gartner의 평가에 따라 최고의 세계 시스템에 들어 있다

BUSINESS INSIDER

Business Insider에 따라 가장 영향력있는 7 가지 사이버 보안 회사 중 하나이다

IDC

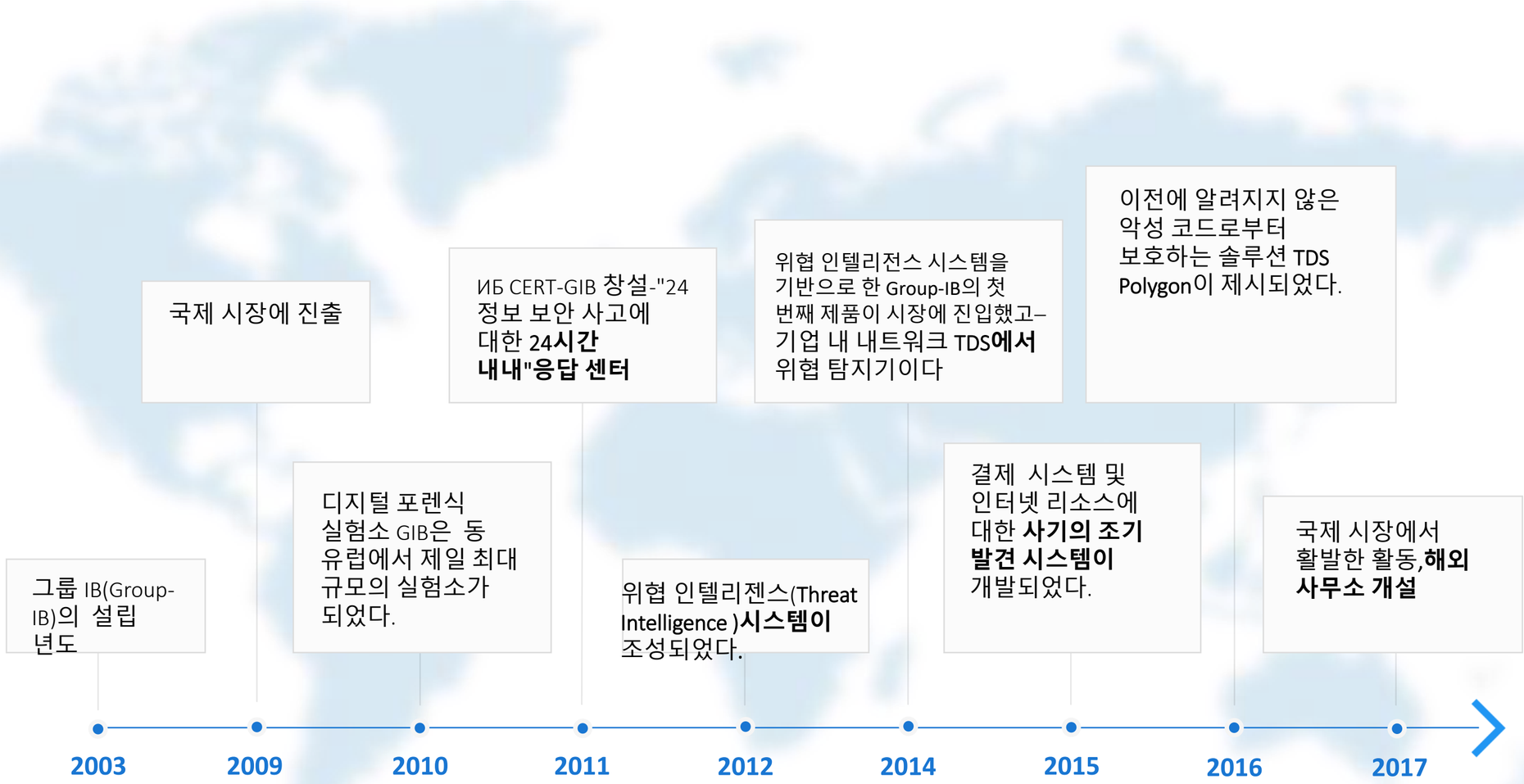
러시아에서 사이버 위협 연구 시장의 리더이다

우리에 대한 정보

theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ

회사의 역사



GROUP-IB

Group-IB의 장기적인 경험은 사이버 위협의 조기 발견 시스템에 구현했다. 이 시스템은 가장 최신의 데이터 및 실제 해커 공격에 대한 심층 분석을 기반으로 한 하이테크 제품 계열이다.

260+
명의 직원

40%
개발자의

27
평균 연령

45 000
часов реагирования

독특한 리소스 기반

15 년 동안 축적된 독특한 리소스 기반

우리는 해커 활동을 모니터링하고 봇 네트워크를 추적하며 사고를 예방하는 데 필요한 데이터를 추출하기 위한 첨단 인프라를 만들었다. **데이터의 90 %는 폐쇄된 소스에서 시스템으로 들어간다**. 그 중 대다수는 독창적입니다폐쇄 된 사이트를 모니터링하고 봇넷의 변경 사항을 모니터링하며 맬웨어 구성 파일을 추출하고 도난당한 식별자에 대한 정보를 수집한다.

1 네트워크 인프라 스트럭처

- 모니터링 및 HoneyNet 트랩의 분산 네트워크
- 봇넷의 분석
- 네트워크 공격 추적자
- 해커 포럼 및 폐쇄 된 네트워크 커뮤니티에 대한 머니터링
- TDS 센서에 대한 데이터

2 휴먼 인렐리젠스(HUMAN INTELLIGENCE)

- Group-IB실험소의 범죄 과학 수사의 결과
- 조사 자료
- 악성 코드 모니터링 및 분석
- 연락처 데이터베이스 및 CERT-GIB 사건에 대한 대응 사례
- 감사 결과
- 그룹 -IB 타겟 분석

3 데이터 교환

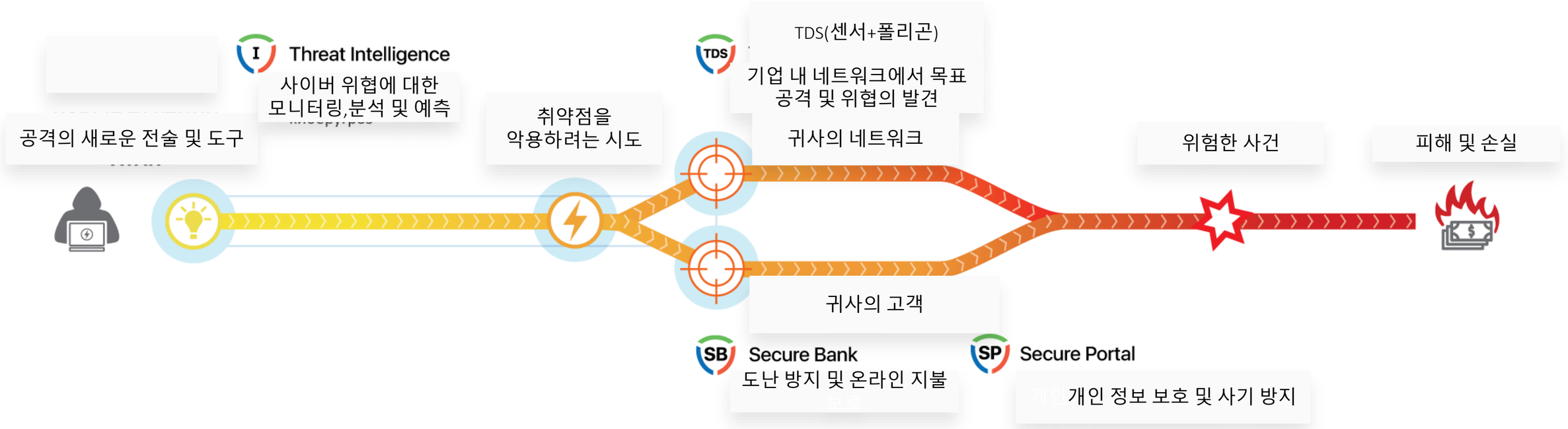
- 컴퓨터침해사고대응팀 CERT
- 기록기 및 호스팅 공급자
- 보안 장비 제조업체
- 사이버 위협에 대응하는 조직 및 협회
- Europol, Interpol 및 법 집행 기관

사이버 위협에 대한 조기 경고 시스템

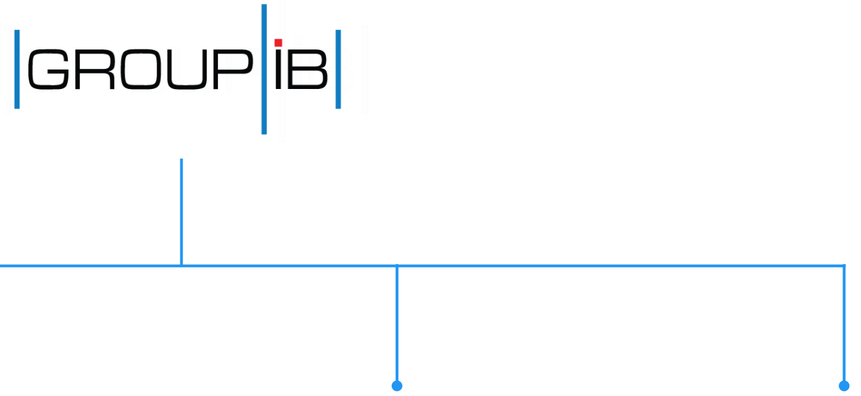
우리는 당신에게 가장 중요한 것을 제공한다.즉 사고에 대비하는 사건을 제공한다.

사이버 위협에 대한 조기 경고 시스템Group-IB은 새로운 위협에 대해 신속하게 파악하고 귀하의 방어선에 위협의 발생을 차단할 수 있게 한다. 이 시스템은 우리 팀의 15 년의 경험,해커 캠페인에 대한 및사이버 범죄 세계의 실제 정보에 대한 심층 분석을 기반으로 한다.

15 년 디지털
포렌직,정보 보안에 대한 컨설팅 및 감사관련 경험



회사의 구조



조기 경고 시스템

- 위협 인텔리전스
- TDS
- 세큐어 뱅크(Secure bank)
- 세큐어 포털(Secure portal)

위협 방지

- 안전 감사
- Compromise Assessment
- 레드 티밍 (Red Teaming)
- 브랜드 보호(Brand Protection)
- 무단 복사 방지(Anty-piracy)

대응 24/7/365

- 정보 보안 사고에 대응하는 센터 CERT-GIB

사고 조사

- 컴퓨터 법의학 및 악성 코드 연구
- 정보 보안 사고에 대한 연구
- 독립적인 재정 조사 및 기업 조사

GROUP IB

다양한 유형의 위협을 처리하는 데있어 시너지 효과를 얻을 수 있게 하여 .Group-IB의 제품 및 서비스 사업 방향은 서로를 보완한다.

Group-IB & AIG CyberEdge

사이버 범죄를 방지하고 보험에 가입한 러시아 최초의 통합 제품

경우에 따라 사이버 범죄자는 멀웨어뿐만 아니라 사회 공학,기만 및 직원 뇌물수수를 사용한다. AIG와의 협력 덕분에 Group-IB의 고객들은 복잡한 공격으로부터 보호를 받는다

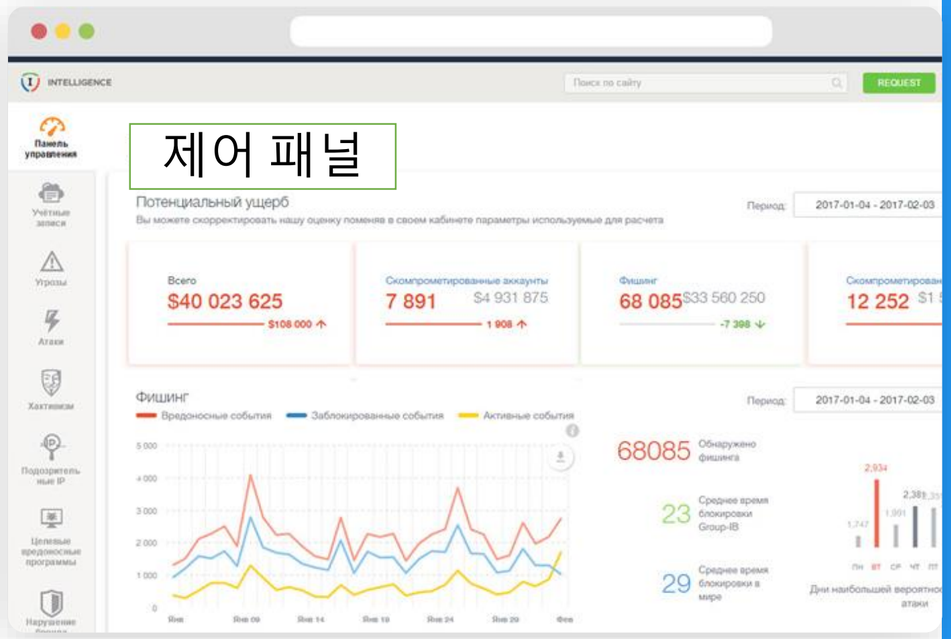
보험에 포함된 것

- 데이터 무결성으로 인한 손해
- 데이터와 관련하여 행정 수사
- 데이터 유출에 대한 대응 비용

위협 인텔리젠스(Threat Intelligence)

회사, 고객 및 파트너에 대한 위협에 대한 모니터링, 분석 및 예측.

- 가중치가있는 위험 평가 및 위협 우선 순위 결정을 위한 전략적 정보
- 공격을 대비하는 운영 데이터 보호 시스템의 설정
- 사고 대응 시간을 최소화는전술 지표



국내 소프트웨어 등록부에 포함됨

Forrester Gartner IDC

Gartner (2015) 및 Forrester (2017) 분석 기관에 따르면 Group-IB는세계 최고의 위협 인텔리젠스의 제공 업체 중 하나이다. 2017 년 IDC는 Group-IB를 사이버 위협 연구 시장의 선두주자로 인정했다.

GROUP-IB

- 공격 및 위협에 대한 즉각적인 통보
- 시각적인 웹 인터페이스
- 귀하가 관심이 있는 분야의 해커 활동 추적, 분석 및 예측
- 위협보고를위한 STIX / TAXII 지원
- 손상된 데이터 및 식별자에 대한 직접 액세스
- 24 시간 지원

위협 인텔리전스(Threat Intelligence)

위협 인텔리전스의 사용 결과

분석가와 사건 대응 팀

위협 인텔리전스(Threat Intelligence)데이터를 기반으로하는 사고에 대한 질적인 우선 순위 지정

사고 대응 프로세스 가속화

위협에 대한 세부적인 맥락에 집중, 회사에 잠재적으로 관심이있는범죄 집단의전술 및 도구에 대한 지식

최고 경영자(CEO) 및 최고 관리층

보안 시스템,사고 대응 팀 및 분석가에 대한 투자에 의한 투자 수익률 극대화

- 경영 의사 결정에 영향을 미치는 위협에 대한 정보 얻기
- 범죄 목적으로 회사 브랜드를 사용하지 못하게하고 명성 위험의 감소

CISO

- 사이버 위협의 진화에 대한 깊은 이해와 실제 공격에 대한 분석을 토대로 정보 보안 전략의 수립
- 현재의 위협으로부터 보호하기 위한 기술 솔루션의 가중치 적용 여부
- 분석가와 사건 대응 팀의 효율성과 역량을 향상시킨다.

MSSP

- 위협 컨텍스트에 대한 깊은 이해를 바탕으로 고객에게 서비스 제공
- 고객과 관련된 위협에 대한 데이터를 기반으로 고객을 대상으로 더 나은 타겟팅을 제공합니다.
- 위협 인텔리젠스 데이터를 기반으로 하여 위협의 증가 및 글로벌 위협에 대처하기 위한 수단

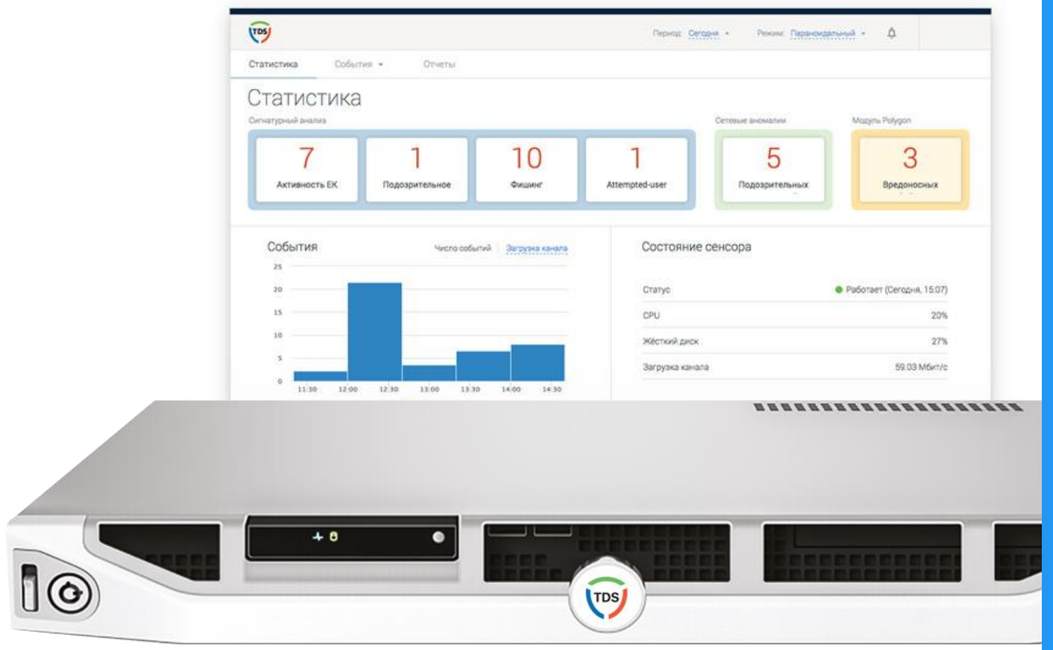
Group-IB의 위협 인텔리젠스는 귀하에게 :

- ✓ 인시던트에 대한 응답 시간 최소화
- ✓ 새로운 도구 및 공격 방법의 출현을 추적하십시오.
- ✓ 폐쇄 된 해커 사이트로부터 개인화 된 데이터 수신
- ✓ 회사의 정보 보안에 투자하기 위해 선택한 전략의 효과 성 평가

TDS Sensor

TDS - 대상 공격 탐지

감염된 사이트를 탐지하고 침입, "누출, 표적 공격"및 산업 스파이를 방지한다.



표적 공격의 특성과 전 세계 다른 지역의 범죄 집단 활동에 대한 깊은 이해 덕분에 다른 사람들이 볼 수없는 위협을 식별한다.또한:

- 원치 않는 위험한 네트워크 상호 작용
- 위험한 전송 물
- 스파이웨어
- 원격 관리 도구
- 취약점을 악용하려는 시도

고정밀 위협 탐지를위한 고유 소스 및 저작권 :

1.동작 분석 알고리즘? 기계 학습

2.컴퓨터 법의학 연구소의 공격에 대한 정보

3.Group IB의 위협 인텔리전스 시스템에 대한 데이터

GROUP-IB

현재 및 이전에 알려지지 않은 모든 멀웨어 제품군에 대한 즉각적인 알림

Wi-Fi 네트워크에서 감염된 모바일 장치의 식별

24 시간 지원 및 컨설팅

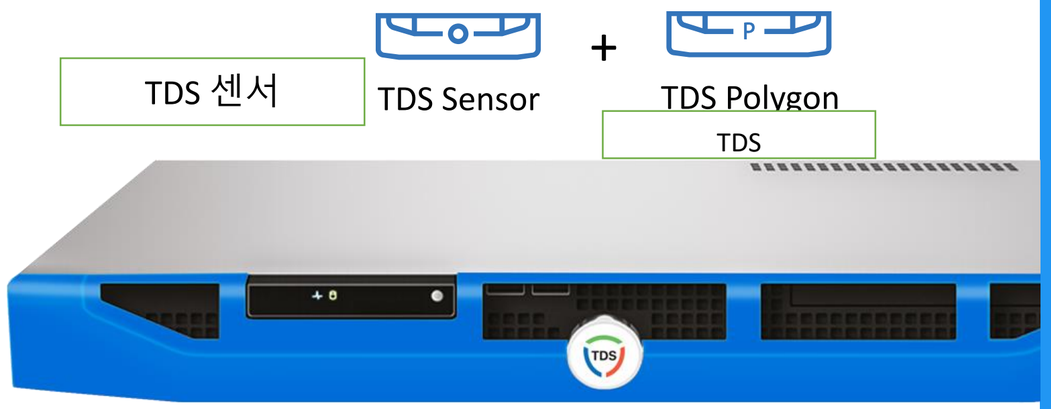
편리한 웹 인터페이스 및 시각적 보고서

Group-IB 전문가들에 의한 로그에 대한 수동 분석 및 매우 중요한 사건 할당

객체의 위험도를 확인하기 위해 정기적으로 업데이트되는 분류 자

기언 내 네트워크 폴리곤(Polygon)의 위협 감지기

폴리곤(Polygon)은 TDS에서 받은 파일들을 귀사의 보안 루프 안의 안전하고 격리된 환경에서 실행하고 동작을 분석하며 개체의 위험 수준에 대해 객관적인 결론을 내린다



가상 머신들의 팜

의심스러운 파일은 사업 특성 및 지역에 따라 설정되는 테스트 환경에서 실행된다.

로우 레벨의 시스템 모니터

존재를 드러내지 않고 가장 로우 레벨의 폴리곤은 안전한 환경에서 실행될 때 객체의 동작을 추적한다

정기적으로 업데이트되는 분류자

객체의의 위험은 머신 마인드(machine mind) 및 사용하고 설정돈 빈도로 새로운 정보를 받는 분류자를 사용하여 결정된다.

.

이메일 첨부 파일

사회 공학의 사용으로 인한 악의적 인 파일

다운로드되는 파일
백그라운드에서 사용자 및 / 들또는 컴퓨터들이 다운로드한 개체

목표 공격
귀사의 인프라에만 지향하는 악성 소프트웨어

및 바이러스 백신 및 시그니처 기반 접근 방식으로 탐지되지 않은기타 이전에 알려지지 않은 악성 개체 -

TDS 의 작동 방식

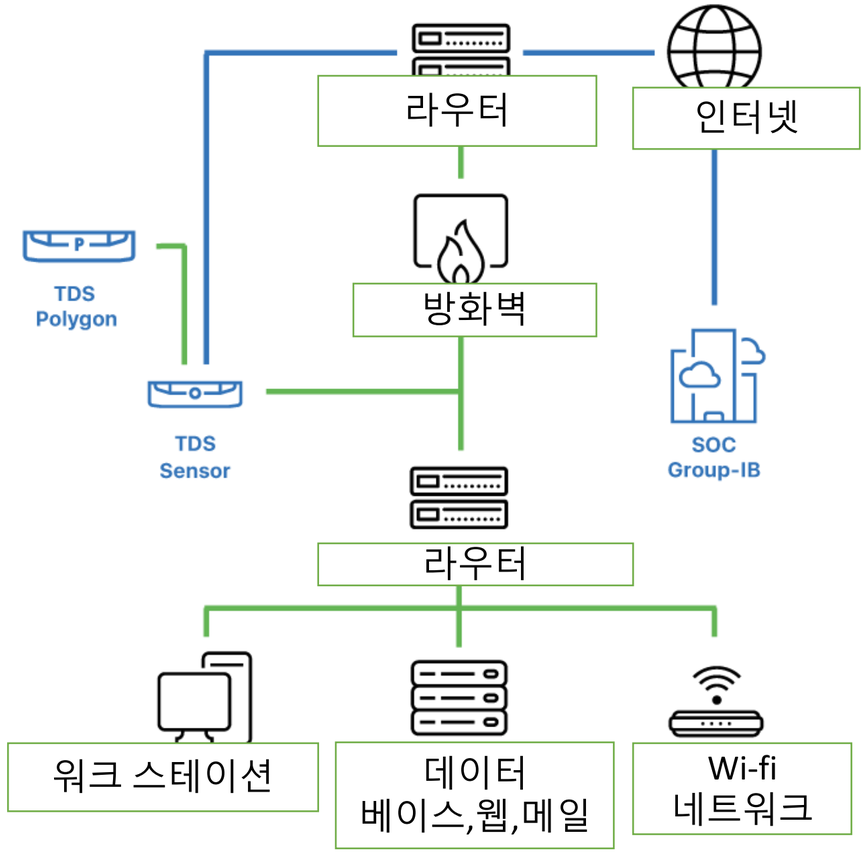
트래픽 분석의 센서

고유한 출처의 데이터를 기반으로 개발된 악의적인 활동의 징조에 대해 명령 센터와의 상호 작용을 구축하여 감염된 사이트를 탐지한다.

기계 학습 알고리즘을 사용하여 악성 코드가 생성한 네트워크의 이상을 탐지한다.

이전에 알려지지 않은 악성 코드를 탐지하는 행태 분석 시스템TDS 폴리곤과 통합된다.

탐지된 사건에 대한 정보를 보안 채널을 통해 SOC GROUP-IB로 전송하거나 정보 보안 이벤트를 기록하는 내부 회사 시스템으로 전송한다.



SOC GROUP-IB

센서에서 받은 인시던트에 대한 정보는 데이터 센터에서 분류되고 상관된다

이벤트는 자격을 갖춘 Group-IB 전문가들에 의해 수동으로 분석된다.

SOC 전문가들이 전화 및 전자 메일을 통해 중요한 위협에 대해 귀사의 전문가들에게 알리고 모든 분석 결과를 편리한 웹 인터페이스에서 사용할 수 있다.

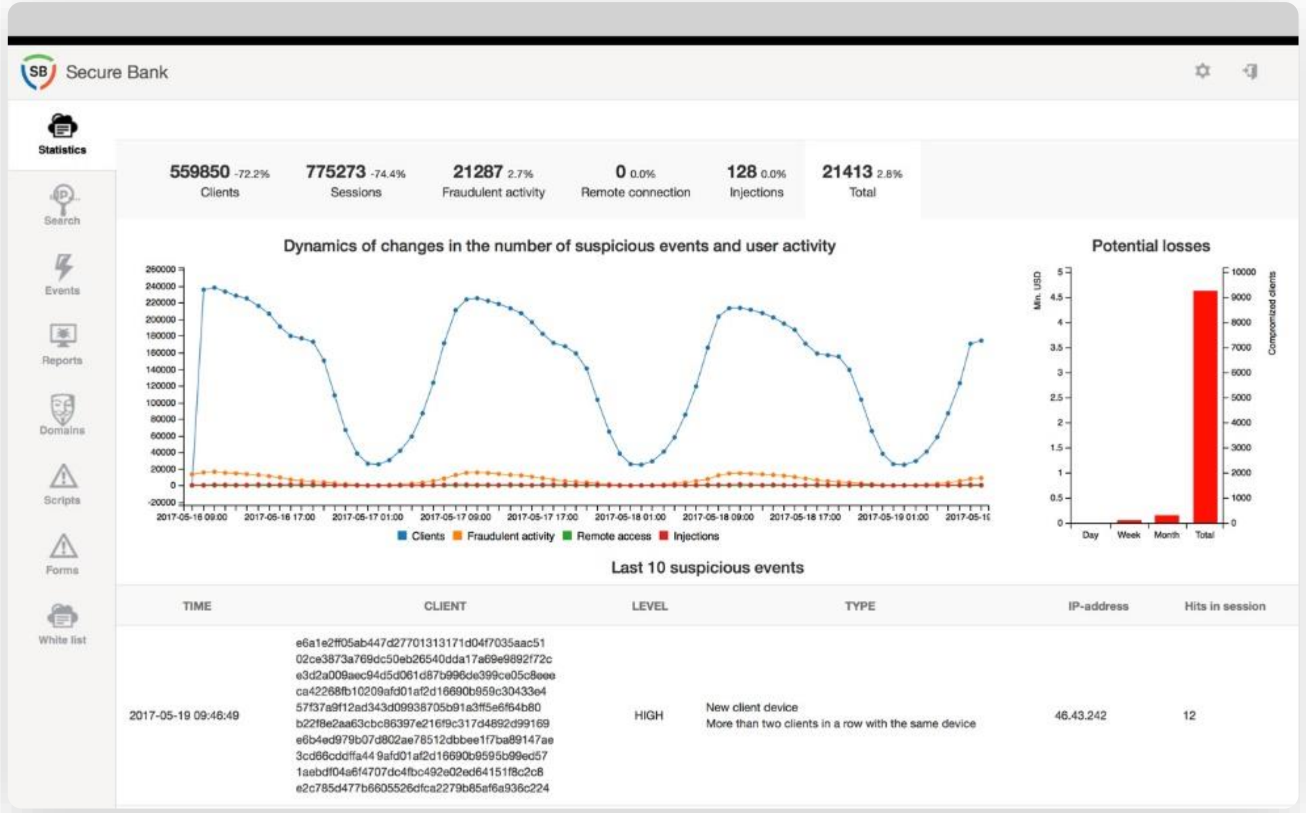
숙련된 Group-IB 전문가들은 중요 사건들을 식별하여 귀사의 IS 서비스가 대응에 집중할 수 있게 지원한다.

세큐어 뱅크(Secure Bank)

GROUP-IB

결제 시스템의 사기를 조기 발견하는 시스템

실시간으로 모든 장치 및 클라이언트 플랫폼에서
은행 사기를 사전에 탐지한다



우리의 솔류션:

- ✓ 사기의 조기 발견을 통한 도난을 방지한다.
- ✓ 오동작 처리 및 고객에게 전화 처리 비용을 절감한다.
- ✓ 온라인 및 모바일 뱅킹 시스템의 보안 및 매력을 높인다.
- ✓ 은행의 신뢰성을 강화시켜 고객에게 감염 및 공격에 대해 경고 할 수있는 기회를 제공한다.

세큐어 뱅크(Secure Bank)은 «스베르뱅크 온라인»을 보호한다

Secure Bank는 국내 소프트웨어의 등록부에 포함된다.

- 사기성 결제 및 사기성 결제 계획에 대한 준비를 나타낸다.
- 새로운 공격 및 사기 계획을 탐지한다
- 규칙 및 시그니처 에 대한 매일 업데이트
- 분석 지원 및 컨설팅
- JavaScript- 온라인 뱅킹 보호를 위한 모듈
- Android и iOS용 (모바일)Mobile SDK
- 클라이언트 장치에 설치하지 않아도 된다.

Secure Bank의 작동 방식

세큐어 뱅크(Secure Bank)는 은행의 웹 페이지,또는 모바일 으행 어플리케이션과 함께 로드되며 고객에게 해당 장치의 감염 또는 손상에 대해 즉시 알려준다.

시스템은 악의적인 웹 주입, 사회 공학, 피싱, 봇넷 네트워크, 계정 압류, 불법 현금 인출 네트워크 및 기타 유형의 은행 사기를 탐지한다.

사기 방지 기술 Secure Bank

- 장치의 디지털 지문
- 사용자의 전체 프로필
- 고급 규칙 작성기
- 동작 분석
- 악성 프로그램의 에이전트 프리 탐지
- 교차 채널 분석
- Group-IB의 데이터 위협 인텔레젠스(Threat Intelligence)

Secure Bank는 악성 코드 탐지 및 행동 분석의 고급 수단을 사용하여 사기가 발생하기 전에 이를 탐지한다.

AF

기존의 일반 사기 방지 시스템은 거래를 분석하고 클라이언트 장치가 멀웨어에 감염되었는지 여부 또는 거래 전에 의심스러운 항목이 있는지 여부를 감지하지 못한다.

1. 사기 행위 시도 (악성 프로그램 시동,사회 공학,원격 엑세스
2. 사기 결제의 행위의 저지름
3. 현금 인출

사기 행위는 몇 초 부터 몇 개월까지 걸릴 수 있다.

은행 인프라와 연결된 호환 통합

조기 경고 시스템: Threat Intelligence TDS Secure Bank Secure Bank

기존의 사기 방지 시스템에서 보이지 않은 위협 탐지

지불 사기

- *신용 사기*
- *CNP 운영 사기?*
- *악성 웹 주사*

Secure Bank는 전자 결제 및 고객 신용 카드 정보를 보호한다.

신분 도용

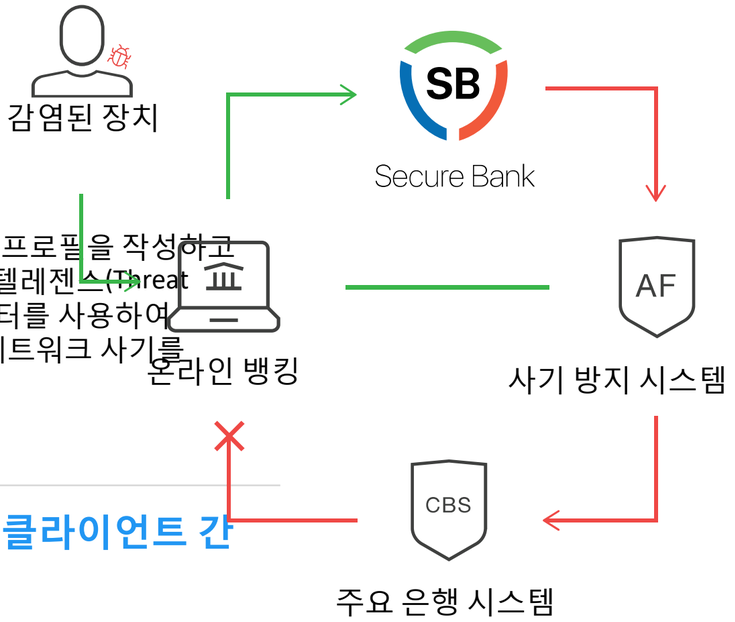
- *계정 캡처*
- *계정 사기*
- *봇 액션*

동작 분석 시스템과 장치의 디지털 “지문”기술을 사용하여 도난 당한 계정 데이터 사용을 추적 할 수 있게 한다.

사회 공학

- *우편 사기*
- *표적 공격*
- *피싱*

단일 클라이언트 프로필을 작성하고 Group-IB 위협 인텔레젠스(Threat Intelligence) 데이터를 사용하여 데이터 누출 및 네트워크 사기를 방지한다.



돈 세탁

- *불법 현금 인출 네트워크*
- *탈세 계획*

계정과 다른 은행 구조 간의 상호 작용의 분석은 의심스러운 거래를 식별하는데 도움이 된다.

악성 프로그램

트로이 목마

- *파밍*
- *봇넷*

Secure Bank의 특허 된 알고리즘은 클라이언트 측에 추가 프로그램을 설치하지 않고 은행 트로이 목마를 발견한다.

교차 채널 및 클라이언트 간 공격

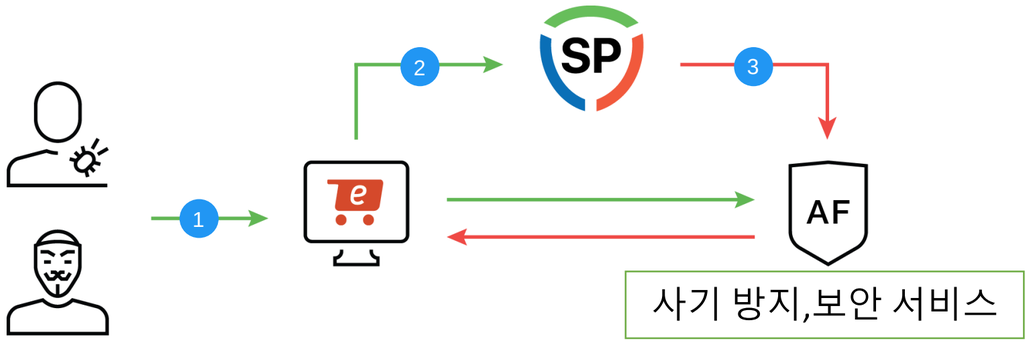
E-commerce

- *모바일 장치*
- *웹 인터페이스*
- Secure Bank는 온라인 인터넷 상점 및 기업 포털을 포함한 모든 모바일 및 웹 플랫폼에서 고객을 보호한다.

세큐어 포털(Secure Portal)

사용자들을 위한 인터넷 포털의 보안을 보장하는
가장 약한 고리인 조기 사기 탐지 시스템

국내 소프트웨어 등록부에 포함됨



1. 포털 페이지의 JavaScript 모듈은 클라이언트 장치의 고유한 지문을 확인하고 사기 행위의 지표를 수집한다.
2. 확인되지 않은 데이터는 보안 채널을 통해 SP로 전송되며, SP에서는 위협 인텔리전스 시스템의 데이터를 사용하여 처리된다.
3. 고객이 실시간으로 사기에 대해 알게되면 API를 사용하여 인시던트에 대한 응답을 자동화 할 수 있다

솔류션에 웹 방지:

- 보너스 점수관련 사기 행위를 위한 제 3 자들의기업 포털에 대한 액세스 차단
- 암호 선택, 치트 투표, 가짜 리뷰 배치 방지 유료 구독 공유
- 경쟁자들의 의 광고를 포털 페이지에 표시하여 구매자 끌어당기기 방지

GROUP-IB

개인 정보 및 은행 카드 정보 도난 의 방지

도난당한 카드 구매를 감지한다.

봇의 사용을 막는다.

포털의 IT 인프라에 대한 투자ㄹ르 필요로 하지 않는다

사기 방지 시스템, SIEM, 방화벽, EPS통합을 위한 API

24 분석 지원 및 컨설칭

정보 보안에 대한 감사

우리는 규모가 크고 목적이 큰 IT 인프라의 약점을 이해하면서 가장 큰 은행과 유망한 창업 기업, 거대 대기업 및 소규모 법률 회사와 협력한다.

- 원격 은행 서비스 및 모바일 뱅킹 애플리케이션
- DoS / DDoS 공격 방지, 부하 테스트 수행
- 통신 사업자들의 신호 네트워크 전환의 정확성
- 기업 / 정부 포털을 포함한 웹 리소스, 전자 상거래 사이트
- 사회 기술적 테스트 (사회 공학)
- 네트워크 인프라의 취약점 검색
- iOS, Android, Windows Phone를 포함한 스프트웨어 지원
- POS, mPOS- 터미널 보안에 대한 연구
- 상업 기밀 및 개인 데이터에 대한 보호 시스템
- 자동화 된 공정 제어 시스템 및SCADA 시스템의 소프트웨어

Group IB의 정보 보안 감사 :

- 우리는 10 년 넘게 취약점을 분석한다.
- 귀사 시스템의 내부 논리에 깊이 집중한다.
- 다른 사람들의 시야에서 사라지는 리스크를 파악한다.
- 각 보고서에는 의사 결정자들을 위한 간략한 요약으로 상세한 설명이 포함되어 있으며 전문가들을 위한 구체적인 권장 사항이 포함되어 있다

Compromise Assessment

침해의 흔적 및해커 공격에 대비할 조짐의 식별

Compromise Assessment은 해커 공격에 대한 준비 흔적, 데이터 손상 조짐을 밝혀 내고 손상 범위를 평가하여 어떤 시스템이 공격 받았는지와 정확히 어떻게 되었는지 확인한다.

Group-IB의 전문들이 실제 피해를 입기 전에 잠재 위협을 밝힌다.

Compromise Assessment일환으로 Group-IB 전문가들은 TDS 소프트웨어 및 하드웨어를 설치하고 수 백 건의 조사를 통해 경험이 있는 전문가들은 인프라 및 감지 된 데이터 침입의 징후를 분석한다.

Compromise Assessment의 결과에 따라:

1. **손상 보고서**
   인프라 손상의 연대기에 대한 설명, 침입자의 행동에 대한 상세한 분석
2. **수행 된 작업에 대한 보고서**
   Compromise Assesment의 각 단계에서의 작업 범위 및 결과에 대한 자세한 설명
3. **권고 사항**
   향후 공격을 방지하기위한 인프라 업그레이드 권고 사항
4. **임원을 위한 보고서**
   인프라 검사의 주요 결과를 설명하는 요약 보고서

- ✓ 컴퓨터 법의학 전문가들은 손상 여부를 발견하기 위해 주요 인프라 요소를 확인한다.
- ✓ 자체 개발의 특수한 포렌직 도구 및 고유한 위협 인텔리전스 데이터를 사용한다.
- ✓ 주요 인프라 노드의 검사 : 도메인 컨트롤러, 프로세싱, 결제 게이트웨이 등
  반복되는 인시던트를 방지하기 위해 인프라 스트럭처의 연대표를

TDS 패키지는 발견되지 않은 "목표 사이버 공격의 초기 징후"를 발견할 수 있게 하고

- ✓ TDS 센서는 네트워크의 이상, 감염 및 비정상적인 장치 동작을 감지한다.
- ✓ TDS 폴리곤은 격리된 환경에서 잠재적으로 위험한 개체의 동작을 분석하고 위험 정도를 결정한다.
- ✓ 확인된 모든 사건들은24/7방식으로전문가에 의해 분석된다.

방지: 보안 감사 약속 평가 레드 티밍 브랜드보호 해적 소탕 망치

몇 달 동안 숨겨진 위협을 보지 못할 수도 있다.

대상 공격 준비

해커들은 몇 달 동안 공격을 위한 인프라를 배포한다.

합병 및 인수

다른 비즈니스와의 통합은 북마크, 백도어, CVE와 같은 새로운 인프라에 숨어있는 위험을 수반한다.

불성실한 경쟁자

영업 비밀에 대한 접근성 확보하면서 경쟁자들은 시장에서 지배력 확보한다.

내부자 또는 해고된 직원들

회사의 인프라가 어떻게 작동하는지를 알면서 조용히 데이터를 "병합"하고 오랫동안 눈에 띄지 않게 되어 있다

레드 티밍(Red Teaming)

보안 서비스를 강화하기 위한 대상 공격을 정기적으로 모방한다. 보안 팀과 관련된 본격적인 훈련은 다음 질문에 답할 것이다 :

- 귀사의 시스템이 사고를 효과적으로 예방, 탐지 및 대응할 준비가되어 있습니까?
- 표적 공격 중에 보안 담당자들이 어떻게 행동합니까?
- 회사의 공격 방어에 대한 능력을 높이기 위해 보안 접근 방식에 대하여 무엇을 구체적으로
- 변경해야합니까?

레드 티밍(Red Teaming)은 공격을 정기적으로 모방 한 결과 표적 공격 준비를 강화하고 새로운 취약성을 발견 및 제거하여 팀을 교육하고 실제 위협에 대응하는 프로세스를 개선하는 데 도움이 된다.

Red Teaming의 결과에 :

- 임원을 위한 보고서
- 보안 시스템 개선을위한 상세한 결과 보고서 및 전문가 권장 사항
- 치명적인 취약점을 발견 한 경우의 비상 경고

Red Teaming은 시간에 제한이 없 다. 이 무제한 접근 방식을 통해 Red Teaming은 다른 도구 및 공격 경로를 시도하여 수개월 동안 공격을 준비 할 수있는 실제 공격자의 행동에 최대한 가깝게 접근 할 수 있게 된다IO

Red Teaming이라는 용어는 군대에서 유래된 말이다. 운동 중에 빨간색 팀이 공격을 하고 블루 팀은 스스로를 방어한다.

레드 티밍의 방법론:

목표의 정렬
도구 선택

→

몇 달 동안 : 표적 공격에 대한 정기적 인 모방. 이에 대해 정보 보안 담당자만 경고 받았다.

→

공격의 새로운 측면을 여는 인프라 변경 사항을 지속적으로 모니터링한다.

브랜드 보호(Brand Protection)

인터넷상의 브랜드에 대한 위협을 발견하고 제거하는 기술 서비스이다.

우리는 실제의 온라인 위협으로부터 회사들의 재정정적인 피해를 방지하고 명성 손상을 방지한다:

- 브랜드 및 온라인 사기의 무단 사용
- 위조 확산 및 제휴 정책 미준수
- 정보 공격 및 부정적인 리뷰

위반 사항을 찾아내는 고급 기술 :

기계 학습 시스템

이전 경험을 토대로 위반 사항을 독립적으로 평가한다.

빅 데이터

빅 데이터의 분석 기술은 소셜 네트워크에서 사이트 간 및 그룹 간 링크를 자동으로 감지한다.

인텔리젠스 드라이븐(Intelligence driven)

사이버 범죄 조사에 사용 된 Group-IB 기술은 위반자와 직접 접촉 할 수 있다.

3 000 000개의 리소스
24/7 자동 추적

매일 **10 000개의**
위반이 제거된다.

85% 의 위반이
재판 전에 제거된다

GROUP-IB

- 위험한 사이트 의 신속 차단
- Runet 밖에서 반응 가능성
- 24 시간 모니터링
- 디지털 증거 수집
- 사기 사이트 간의 링크 식별
- 재발에 대한 예방

해적 소탕(Anti-Piracy)

스마트 디지털 컨텐츠 보호 시장의 선두주자

- vk.ru, veterok.tv,kinostock.tv 를 포함하여 120 000+ 리소스의 모니터링
- 재판에 의해 해적 사이트에 대한 성곡적인 차단 사례
- 대형 해적 사이트에서 온라인 콘텐츠 차단
- 사용자들을 귀사의 공식 리소스로 리디렉션

30 분

우리는 상당히 중요한 변경된 불법 복제된 콘텐츠도 발견한다

24 시간루넷(Runet)에서

가장 큰 해적 사이트 runet에서 콘텐츠 배포를 중지한다.

7 일 귀하의 콘텐츠에 대한 최대 99 %의 링크를 차단하고 다루기 어려운 사이트에 대한 솔루션을 제공할 것이다.

- 올바른 차단 디자인
- 알림 덕분의 높은 수익률
- 직관적인 인터페이스
- 24 시간 모니터링
- 다양한 재판 전의 조치
- "원 버튼"으로 불법 복제물 제거

대응 센터 CERT-GIB

CERT-GIB (컴퓨터 응급 대응 팀) — 24 시간 정보 보안 사고 대응 센터

- 피싱 (Phishing) 리소스의 출현, 악성 코드의 확산, 모조품 거래를 머니터링한다
- 우리는 대응과 조사의 모든 단계에서 완전한 법적 지원을 제공한다.
- .RU, .РФ 및 1000 개 이상의 도메인 영역에서 위험한 사이트를 신속하게 차단한다.
- 우리는 전 세계에서 운영하고 있다 : 파트너 네트워크를 통해 호스팅 제공 업체 및 도메인 이름 등록 업체아 함께 운영하고 있다.

로스쩨흐(Rostec)

러시아 최대의 국영 기업 중 하나인 로스쩨흐(Rostec)은 Group-IB를 자체 CERT RT-Inform을 만들기 위한 파트너로 선택했다.

인터넷 및 인터넷 개발 기금의 국가 도메인 조정 센터의 관할 기관

국제 연합 FIRST и Trusted Introducer의 정회원

파트너 IMPACT – 사이버 위협에 대응하기위한 국제 파트너쉽

카네기 대학 (Carnegie University)의 인증을받은 CERT 상표가 공식적으로 사용된다.

컴퓨터 법의학 연구소 및 조사 부서

컴퓨터 법의학 및 악성 코드 분석을 위한 동유럽에서 가장 큰 실험실.

최첨단 장비 및 고급 바이러스 분석

트랙을 숨기는 기술을 회피할 수 있는 세계적인 최고의 개발.

법 집행 기관과의 상호 작용

수색 작전의 활동에 공식 참여는 포함

모든 정보 매체에서 데이터 검색

데이터가 삭제, 숨김 또는 암호화 된 경우에도 해당 데이터를 찾을 수 있다.

모바일 대응 팀

디지털 증거 수집 및 연구 현장,사건 결과를 제거하기 위한 권장 사항

러시아에서 80% 의 공명하는 첨단 범죄은 우리의 전문가들에 의해 조사된다

각 개인에 대한 개별 접근법

전문가 팀 : "증거개시제도(E-Discovery 및포렌직(Forensic)에서"재무 감사 및 기업 법률까지

해외로 빼 자산을 돌려준 경험이 있다

수사 중 하나의 결과로 33 억 루불이 손해를 입은 회사로 돌아왔다.

사이버 범죄의 경제적 이해

위협 인텔리전스 독점 정보를 사용하여 자금 흐름 체인 복원

변호사, 수사관, 검사에게 건설팅을 해준다

조사의 모든 단계에서 상담이 가능하다.

- 컴퓨터 및 기술적 검정
- 법정에서 디지털 증거를 제시하는 광범위한 경험
- 디지털 증거 수집
- 악성 프로그램 연구
- 아웃소싱 및 독립적인 심사
- 디지털 검증

PRE-IR ASSESSMENT

정보 보안 사고에 대한 효과적인 대응 준비.

IR 사전 평가 (Pre-IR Assessment)는 시스템, 팀 및 프로세스가 사고에 대비하고 대응할 준비가되었는지 확인하는 데 도움이 된다.

일반적인 문제

많은 양의 데이터가 손실되거나 로깅이 잘못되었습니다.

이 사건으로 공황 상태와 통제되지 않는 행동이 야기됩니다.

응답 프로세스가 디버깅되지 않고 역할이 분담되지 않는다.

Pre-IR Assesment의 결과

사고에 효과적으로 대응할 수 있도록 시스템을 설정하기위한 권장 사항

자신감 및 잘 정립된 행동 계획

부서간의 커뮤니케이션

주요 구성 요소의 포괄적인 평가

1 기술

네트워크 및 시스템 인프라의 검증 - 디지털 증거를 완전하고 정확하게 수집 할 수있는 능력, 손상의 지표를 탐지 할 수있는 능력, 인시던트를 즉시 중단하고 대응하는 동안 네트워크를 관리 할 수있는 능력..

결과-스크립트 실행, 다양한 유형의 인시던트에 필요한 데이터 검색 및 수집과 같은 실제 시스템에서의 프로세스 개발이다.

2 사람

IT 서비스 및 정보 보안 직원들의 역량 검증

결과-인시던트 대응에 대한 Group IB의 전문가들이 진행하는 2 일간의 교육이고 자신이 있고 훈련된 팀이다.

3 규정

규정 및 문서의 완전성, 관련성 및 실제 타당성 **확인.**

결과 – 인시던트 발생시 실제로 유용하게 사용될 수있는 규정 및 문서

4 구조

팀의 책임 분담 및 조직 구조의 분포 **확인**

결과 - 인시던트에 대한 대응 과정에서 여러 부서의 조정 및 팀워크가 이루어진다.

GROUP IB

사전 IR 평가(Pre-IR Assessment)의 진행 방식

준비

정보 수집

특정 고객 및 업계를위한 프로그램의 적응

유효성 검사 규칙 승인

타이밍 프로세스

Group-IB 전문가의 고객 회사에 출동

다양한 사건에 대한 일반적인 데이터 쿼리

완전성, 가용성 및 데이터 수집 속도 분석

사고 대응에 대한 교육 실시

결론

효과적인 응답을위한 시스템 설정에 대한 권장 사항

구조 및 프로세스의 최적화

대응 계획

기성품 규정

훈련 된 팀

2003 년부터 사이버 범죄를 예방하고 조사하고 있다.

www.group-ib.ru

info@group-ib.ru

twitter.com/groupib

t.me/group_ib

group-ib.ru/blog

+7 495 984 33 64

facebook.com/group-ib

instagram.com/group_ib