2021년 하이테크 범죄 동향과 최신 대응방안

- 주적(主敵)-중심 위협 탐지 그리고 위협 헌팅

이정상 상무 (스텔스 솔루션)/서현석 대표 (Group-IB Korea)

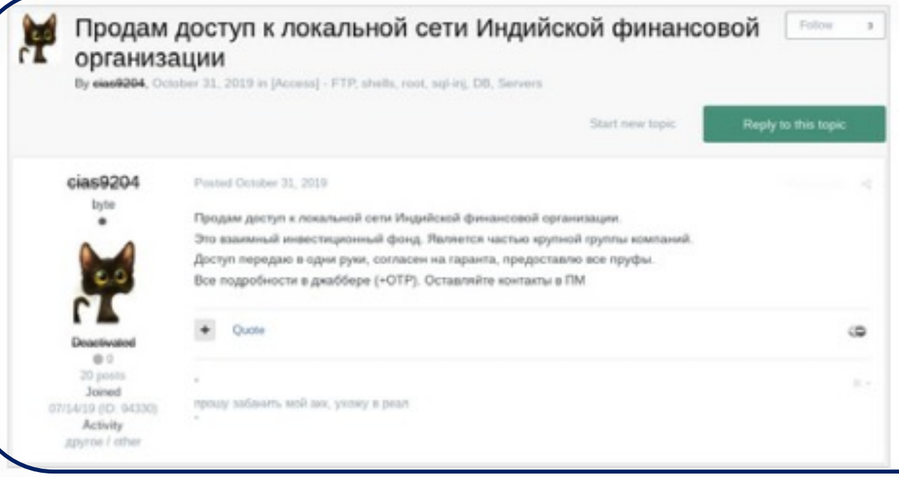
목 차

- 주요 탐지 결과 및 보안 트렌드 예측
  1. 랜섬웨어 공격
  2. 군 & 방위산업 공격
  3. 통신 산업에 대한 위협
  4. 금융기관에 대한 위협
  5. 소매산업에 대한 위협
  6. 웹피싱과 사회공학 공격

- 최신 위협 대응: 포괄적 보안 프레임워크
  1. 글로벌 위협 헌팅: Threat Intelligence & Attribution (TIA)
  2. 로컬 위협 헌팅: Threat Hunting Framework (THF)
  3. 사기행위 헌팅: Fraud Hunting Platform (FHP)
  4. 브랜드 보호: Digital Risk Protection (DRP)

랜섬웨어 공격

- **전략과 기술의 변화**: 랜섬웨어의 원활한 배포를 위해 기업의 네트워크를 해킹그룹간의 협업으로 접근
  - 랜섬웨어의 목표: 개인 사용자 → 기업, 공공기관, 금융회사
  - 랜섬웨어 개발자는 기업 네트워크 접근 경험 및 지식 부족
  - APT 해킹그룹은 기업 네트워크 침투능력 보유
- 랜섬웨어 **"제휴 프로그램"**의 출현
  - Public: 다크웹내에서 공개된 포럼에서 자유롭게 협업 논의
  - Private: 랜섬웨어 개발자와 APT그룹간의 직접적인 협업 논의
  - **피해자가 몸값을 지불한 후, 랜섬웨어 개발자들은 협업한 APT그룹에 지분 분배**
- 다크웹상에서의 랜섬웨어 제휴 프로그램 요청 샘플:


Продам доступ к локальной сети Индийской финансовой организации

By cias9204, October 31, 2019 in [Access] - FTP, shells, root, sql-inj, DB, Servers

Follow

Start new topic

Reply to this topic

cias9204

byte

Deactivated

0

20 posts

Joined

07/14/19 (ID: 94330)

Activity

другое / other

Posted October 31, 2019

Продам доступ к локальной сети Индийской финансовой организации.

Это взаимный инвестиционный фонд. Является частью крупной группы компаний.

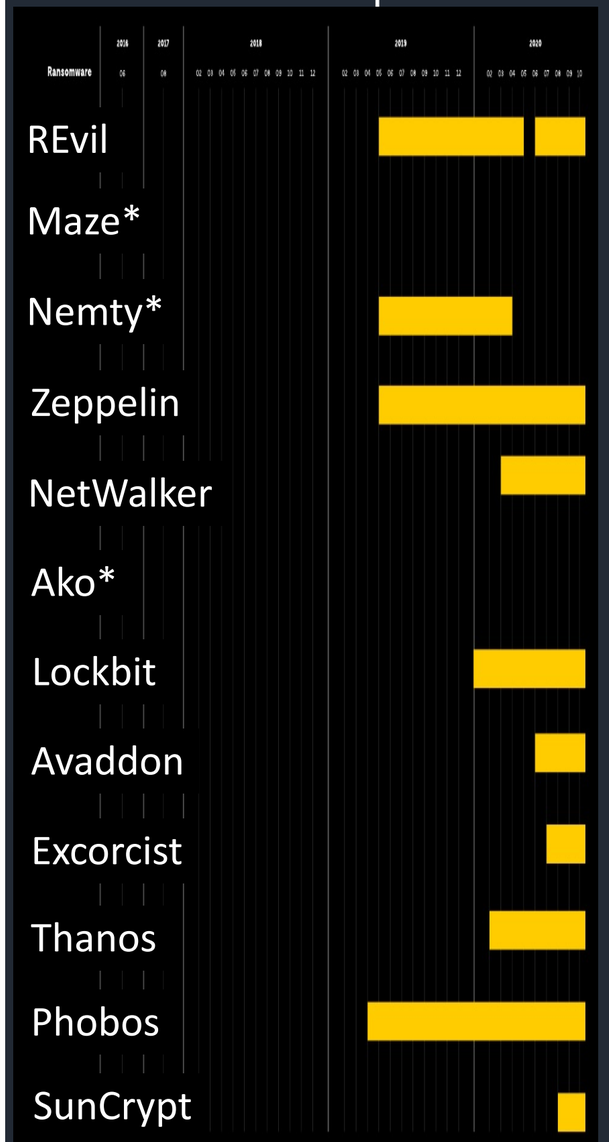
Доступ передаю в одни руки, согласен на гаранта, предоставлю все пруфы.

Все подробности в джаббере (+OTP). Оставляйте контакты в ПМ

Quote

прошу забанить мой акк, укажу в реал

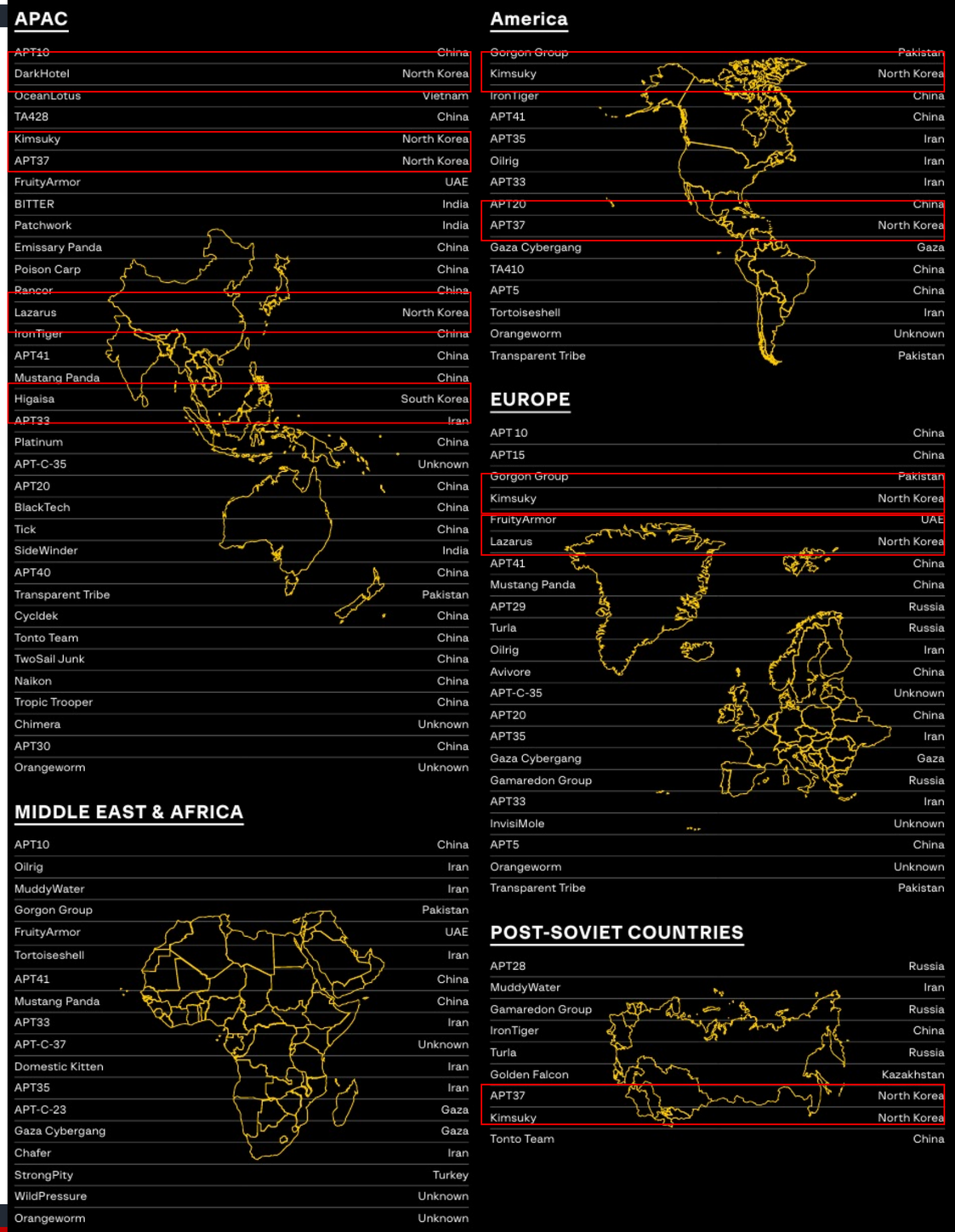
- 제목: **인도 금융 회사 내부 네트워크 접근**
- 2019년 10월 21일 작성
- 모기업이 대형 그룹사인 뮤추얼 투자 펀드회사의 내부네트워크 접근 내용 판매
- 한사람한테만 판매 할 것이며 에스크로서비스 제공
- 확실한 증거 제공 가능
- 모든 정보는 OTP 내용을 포함해서 Jabber로 제공
- 포럼에서 제외되고 싶으므로 협업 성사 후 본인 계정 삭제 요청



* Private affiliate program

군 & 방위산업 공격

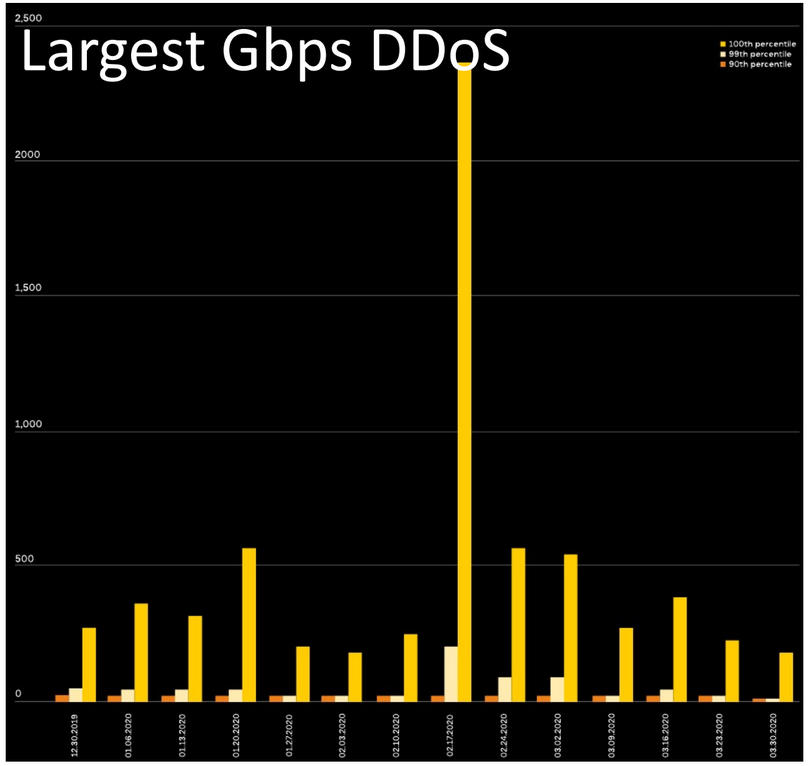
- 최근 위협 동향
  - 스파이 활동 중심에서 **인프라 시설을 파괴하려는** 적극적인 시도로 대체
  - 최근 주요 공격 대상은 인도의 핵시설(19년 9월), 이란의 핵시설(20년7월)과 이스라엘의 급수 시스템(20년 4월)
- 일부 국가 지도자들은 공개적으로 다른 나라에 대한 성공적인 공격을 발표 (예: 이스라엘 모사드)
- 20-21 기간 동안 **7개의 새로운 APT 그룹**이 검색
  - Tortoiseshell, Poison Carp, **Higaisa**, AVIVORE, Nuo Chong Lions, Chimera, WildPressure
  - 최근 몇 년간 눈에 띄지 않게 남아있던 6개의 알려진 그룹이 공격을 재개: Golden Falcon, Naikon, APT20, APT5, APT30, Cycldek
  - **북한 해킹 그룹**: **DarkHotel, APT37, Lazarus, Kimsuky**
- 해커들은 **에어갭**(air-gapped)망을 공격하기 위해 도구 개발 시작: 지난 1년 동안 총 4개의 USB를 활용한 도구 확인
- 아시아 태평양 국가들이 주요 목표물이 되고 있습니다.
  - **중국, 북한, 이란, 파키스탄**의 사이버 범죄자들의 관심

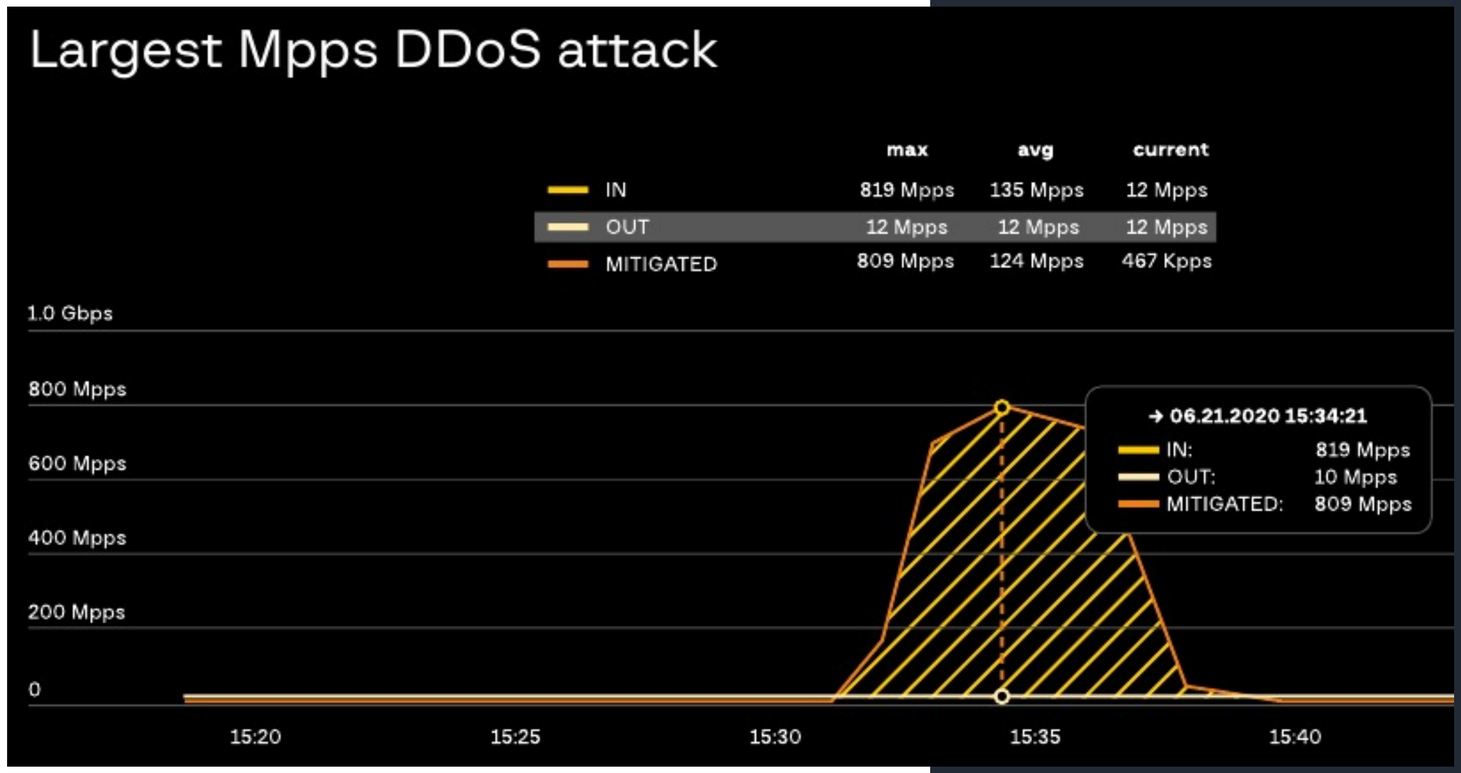


통신 산업에 대한 위협

주로 국가 후원하는 APT그룹은 통신 산업에 대해 정교한 공격 진행

- APT41, OilRig, Molerats, Mikroceen 등등
- DDoS, SMS Hacking, BGP Hijacking





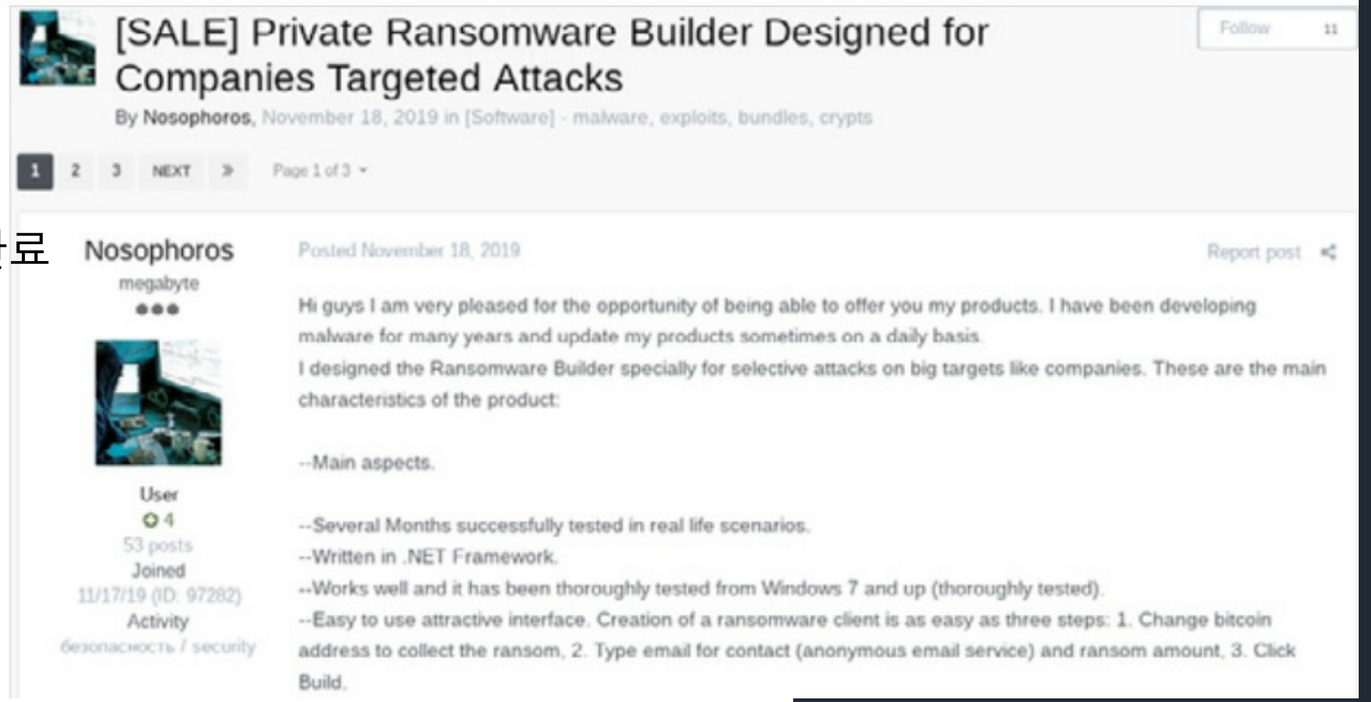
- CLDAP 이용한 2.3 Tbps 공격 (20년 2월, 아마존 방어)
- IoT 단말기 이용 증가
- Mirai 봇넷, SYN 플러드, ICMP 플러드, HTTP 플러드

- 유럽의 한 은행을 8억9백만 PPS 공격 (20년 6월, 아카마이)
- 96.2% 의 새로운 IP 주소들 → 새로운 봇넷의 출현
- 2분만에 418Gbps → 809Gbps 도달 후 10분 동안 지속

금융기관에 대한 위협

- 최근 위협 동향
  - 5개의 해킹그룹 (Cobalt, Money Taker, Silence, Silent Cards, Lazarus) 은 지속적으로 SWIFT, ATM 스위치, 카드 프로세싱 시스템, ATM 탈취 행위를 진행
- 하지만 최근에는 이들 조차도 랜섬웨어에 초점을 맞추고 있습니다.
- 랜섬웨어 제작기 (Ransomware Builder) 판매 사례

- 아이디: Nosophoros
- 2019년 11월 18일 작성
- 설명:
  - 실환경에서 수개월에 걸쳐서 성공적인 테스트 완료
  - .NET Framework로 제작됨
  - 윈도우7부터 이후 버전까지 원활한 작동
  - 직관적이면서 쉬운 사용법, 3 스텝으로 랜섬웨어 클라이언트 제작 할 수있다고 강조
    1. 랜섬을 회수하기 위해 비트코인 주소 수정
    2. 이메일주소 변경과 랜섬 금액
    3. 클릭 “제작 (Build)”


[SALE] Private Ransomware Builder Designed for Companies Targeted Attacks

By Nosophoros, November 18, 2019 in [Software] - malware, exploits, bundles, crypts

Follow 11

1 2 3 NEXT » Page 1 of 3

Nosophoros
megabyte
User
4
53 posts
Joined
11/17/19 (ID: 97282)
Activity
безопасность / security

Posted November 18, 2019

Report post

Hi guys I am very pleased for the opportunity of being able to offer you my products. I have been developing malware for many years and update my products sometimes on a daily basis.
I designed the Ransomware Builder specially for selective attacks on big targets like companies. These are the main characteristics of the product:

--Main aspects.

--Several Months successfully tested in real life scenarios.
--Written in .NET Framework.
--Works well and it has been thoroughly tested from Windows 7 and up (thoroughly tested).
--Easy to use attractive interface. Creation of a ransomware client is as easy as three steps: 1. Change bitcoin address to collect the ransom, 2. Type email for contact (anonymous email service) and ransom amount, 3. Click Build.

소매산업에 대한 위협

- 최신 위협 동향
  1. JS snifer의 수가 2.5배 증가
  2. 약 1년동안 POS 트로이 목마로 탈취한 6,370만 개의 은행 카드 덤프가 판매
  3. 카드 덤프의 92%가 미국과 관련
- 소매업계에 심각한 피해를 줄 수 **있는 4 가지 주요 위협 요소**

  텍스트 카드 정보 (번호, 유효기간, 수유자 이름, 주소, CVV) vs. 카드덤프(카드 마그네틱 정보)
  1. **JS sniffer**: 은행 카드정보 (**텍스트 카드정보**) 탈취 자바스크립트 도구
     - 46만개의 카드 정보 유출, 64만여개의 은행카드 정보가 3백6십만불에 거래 정황
  2. **POS 터미널 공격**: **카드덤프** 정보 탈취 도구, 14개의 트로이 목마 도구 발견, 작년 한해에만 156% 카드덤프 증가
  3. 봇을 이용한 **계정 입력 공격** (Credential Stuffing): Brut force 공격 종류
     - 하나의 계정이 유출되면 동일 소유자의 다른 계정도 해킹 당할 위험 증가 (동일한 계정/비번 사용)
     - 리워드 포인트/선불카드 포인트/멤버쉽 등급 상승 포인트 탈취/**개인정보 탈취**

Country	Number of dumps H2 2019 — H1 2020	Percent
UNITED STATES	58,921,367	92.37%
INDIA	1,723,722	2.70%
SOUTH KOREA	644,672	1.01%
UNITED KINGDOM	584,519	0.92%
CANADA	565,535	0.89%
BRAZIL	447,412	0.70%
MEXICO	276,935	0.43%
FRANCE	234,076	0.37%
UNITED ARAB EMIRATES	208,089	0.33%
AUSTRALIA	182,263	0.29%

웹피싱과 사회공학 공격

- **최근 위협 동향**
  1. 2019년 중반부터 2020년 중반까지 인지되어 제거된 피싱사이트는 그 전기간 대비 118% 증가
     - **코로나19 팬더믹**
     - **전략 수정**: 기술의 발전으로 인한 피싱사이트 재사용 증가
- **피싱 탐지 회피 기술**
  1. One-time 링크
  2. 서브넷 차단
  3. 유저에이전트 차단
  4. 지역 차단
  5. **정식 홈페이지로 리다이렉트시켜 의심 회피**

- **피싱 제휴 프로그램**:
  1. 피싱
  2. 위조 은행 리워드
  3. 가짜 로또 프로그램
  4. 가짜 유료 설문
  5. 돈세탁 계정 생성

- **Phishing-as-a-Service**
  1. 피해대상 모집 담당 봇
  2. 성공적인 피싱 자금인출 홍보담당 봇
  3. 멤버들간의 안전한 통신을 위한 패쇄 채널 공급
  4. 피싱링크 생성 담당 봇
  5. 이 모든 패키지를 SaaS 형태로 제공

	H2 2019 — H1 2020
Government resources	0.1%
Financial institutions	15.0%
Payment services	6.6%
Postal services	15.6%
Internet service providers	0.7%
Online services	39.6%
Cloud storage systems	14.5%
Social media	4.5%
Dating sites	1.2%
Cryptocurrency	0.0%
Healthcare organizations	0.0%
Bookmaker offices	2.2%

2021년 하이테크 사이버 범죄 보고서

https://www.group-ib.com/resources/threat-research/2020-report.html

Group-IB 보안 프레임워크 소개

사이버 위협 인텔리전스
위협 헌팅 프레임워크
사기 헌팅 플랫폼
디지털 위험 관리

Group-IB 보안 프레임워크

위협 인텔리전스 (TIA)

급변하는 최신 위협에 대한 상세한 속성 제공과 투자보호와 신속한 사고 대응을 위해서 기존 시스템과의 연동성 제공

주적(主敵) 관점의 위협 헌팅 솔루션

사기 행위 헌팅 솔루션

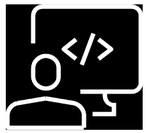
브랜드 보호 플랫폼

위협 헌팅 프레임워크 (THF)

Huntbox | Sensor | Polygon | Huntpoint | Sensor Industrial | Decryptor

사기행위 헌팅 플랫폼 (FHP)

Processing Hub | Web Snippet | Mobile SDK | Preventive Proxy



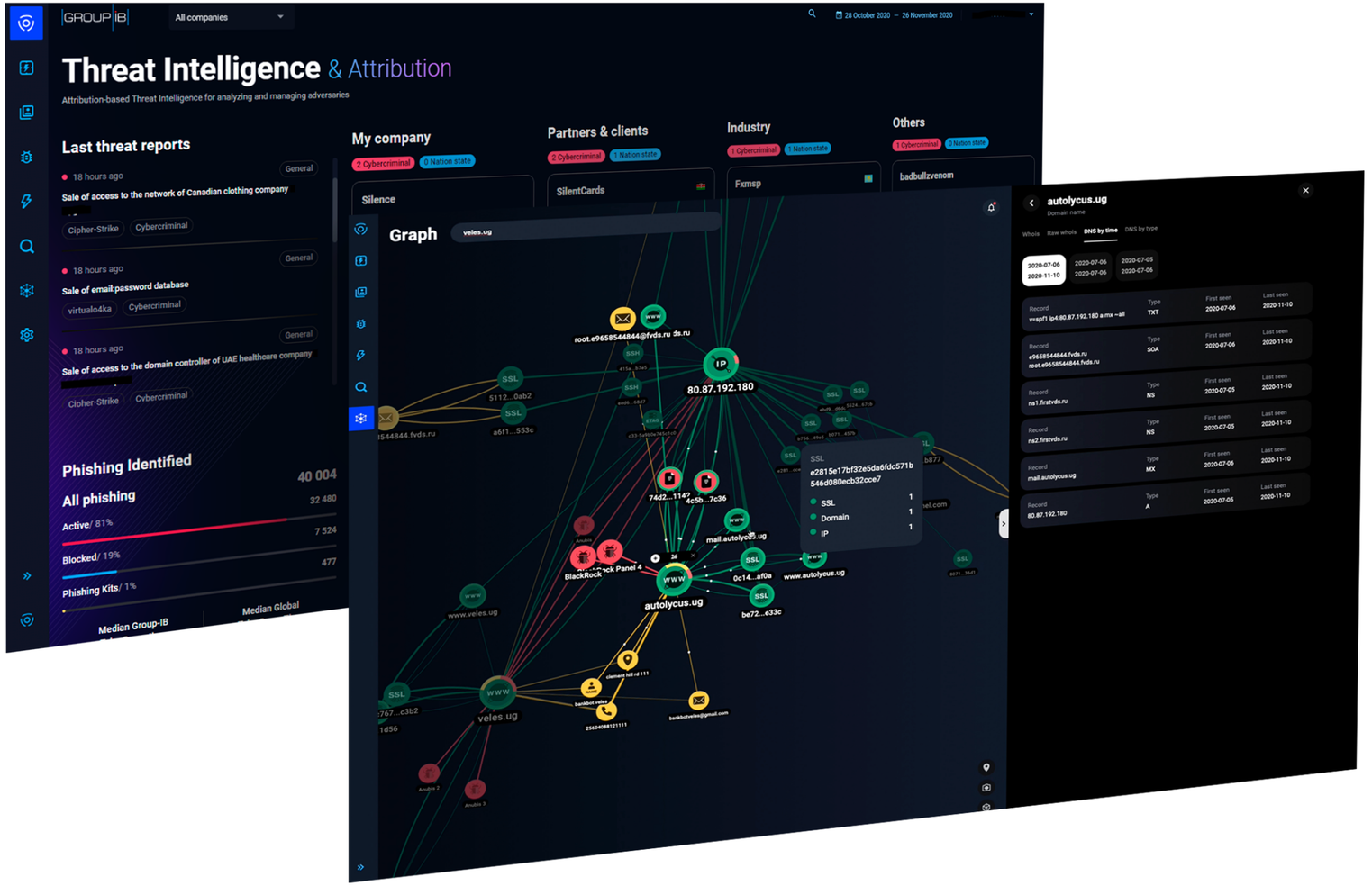
디지털 위험 보호 (DRP)

불법 복제 방지 | 사기 방지 | 위조 방지

Group-IB Threat Intelligence & Attribution 소개

위협 인텔리전스 데이터를 기반으로 한 글로벌 레벨의 공격자 속성 정의

- **공격자 관리**: 공격 지표 관리를 넘어 공격자 관리
- **주적-관점 보호**: 무관하거나 일반적인 위협이 아닌 공격자로부터의 보호
- **심층 분석**: 원시 데이터 분석을 넘어 공격자에 대한 심층 조사
- **최신 트랜드 반영**: 고객에게 가장 관련성이 높은 데이터 제공 → 최신 트랜드 이해를 돕기 위한 상황 데이터 제공



GIB 인텔리전스만의 고유 기술 및 데이터 소스

다양한 데이터 자원

위협 데이터

모바일, PC 봇넷 C&C 포렌식, 카드 정보, ISP에 설치된 네트워크 센서

멀웨어 인텔리전스

네트워크 센서, 샌드박스, 하니팟, 씽크홀, 스팸 트랩

Group-IB 고유의 **악성 프로그램 분석 플랫폼**은 악성 파일의 심층 분석에 사용됩니다.

휴먼 인텔리전스 (Humint)

사건 대응, 사이버 범죄 조사 및 폐쇄된 커뮤니티에 대한 액세스: 딥/다크웹

빅데이터 기반 공격자 추적 및 분석 도구

데이터 검색 및 추출을 위한 자동 시스템

- 사전 예방적 피싱 탐지 및 피싱 키트 추출 기술
- 자동화된 멀웨어 구성 파일 추출
- 11개 언어로 된 다크웹 포럼의 정보 수집 및 분석

공격자를 중심으로 데이터 분석

- 공격자 도구의 변경 내용 추적
- 공격자 프로파일 모음집 제공
- 대량의 데이터를 신속하게 상관관계화 하는 머신 러닝 기술

공격자 인프라 식별

개별 범죄 행동의 고유한 특성을 계산하여 향후 공격에 사용 될 인프라를 정확히 예상

다양한 보안조직을 위한 다양한 제공 서비스

기계 판독 – 3rd party 연동

- 고유한 침해 지표 (IoCs)
- 맞춤형 데이터
- 간편한 연동

인간 중심

- 전문가 증언
- 숙련된 분석가 (리버스 엔지니어링 전문가, 사이버 범죄 전문가)

분석 도구

- 네트워크 그래프
- 기본 제공되는 멀웨어 제거 기능
- 다크웹 데이터 접근

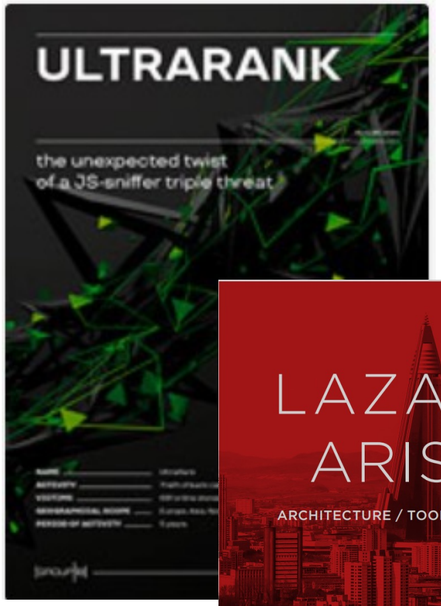
RFI 및 맞춤형 분석

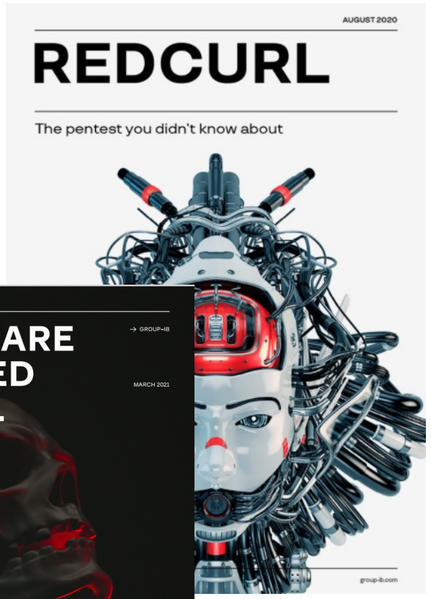
- SLA 기반 신속 응답
- 다국어 지원
- 유니크한 자원

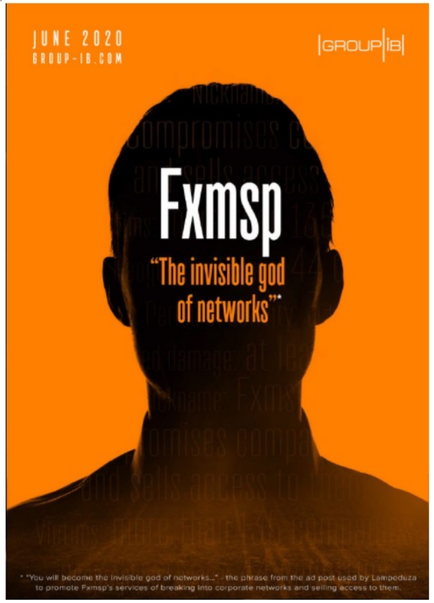
피싱 모니터링 및 피싱 사이트 제거 기능

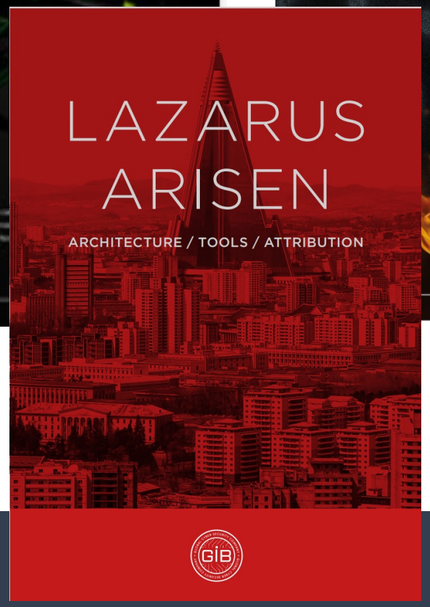
- 피싱 도메인 모니터링, 피싱 키트 추출, SSL, 광고
- 자동 분석 및 즉각적인 자동 실행
- 복잡한 보안사고 사례의 조사 및 제거 기능

Group-IB만의 최신 해킹그룹 보고서 작성 및 제공









언론 보도:

theguardian Bloomberg Forbes REUTERS

Esquire CNN The Register® InformationWeek DARKReading SC MAGAZINE

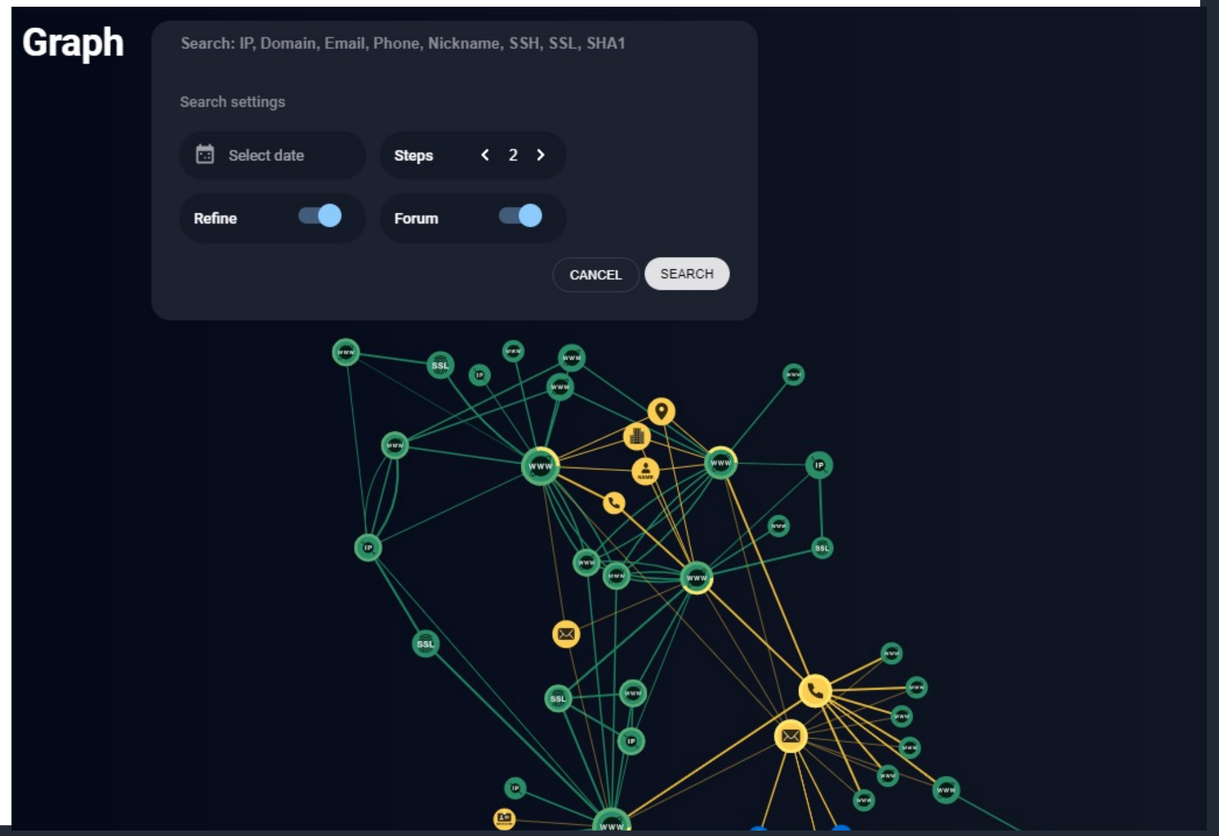
그래프 분석

그래프 분석기능은 Group-IB 만의 외부 위협 헌팅기능을 제공하는 시각화 도구 포함

그래프 기능은 인터넷을 스캔하여 대량의 데이터를 수집하고 GIB 고유의 링크 구축 알고리즘을 활용하여 숨어있는 의심스러운 연결을 시각화

Use Case

- 위협 헌팅
- 심층 침해 지표
- 알람 상관 관계 구축
- 피싱 및 사기 방지
- 백엔드 및 백도어 검색



- 후이즈 도메인 등록정보
- DNS 도메인 레코드
- SSL 인증서 등록 데이터
- 배너의 IP주소 및 숨겨진 등록 데이터
- 프록시 서비스 뒤에 숨겨진 백엔드
- 과거 등록 데이터 기록, 호스팅 관련 전송 기록, 서비스 변경 이력 정보
- 다크웹 활동

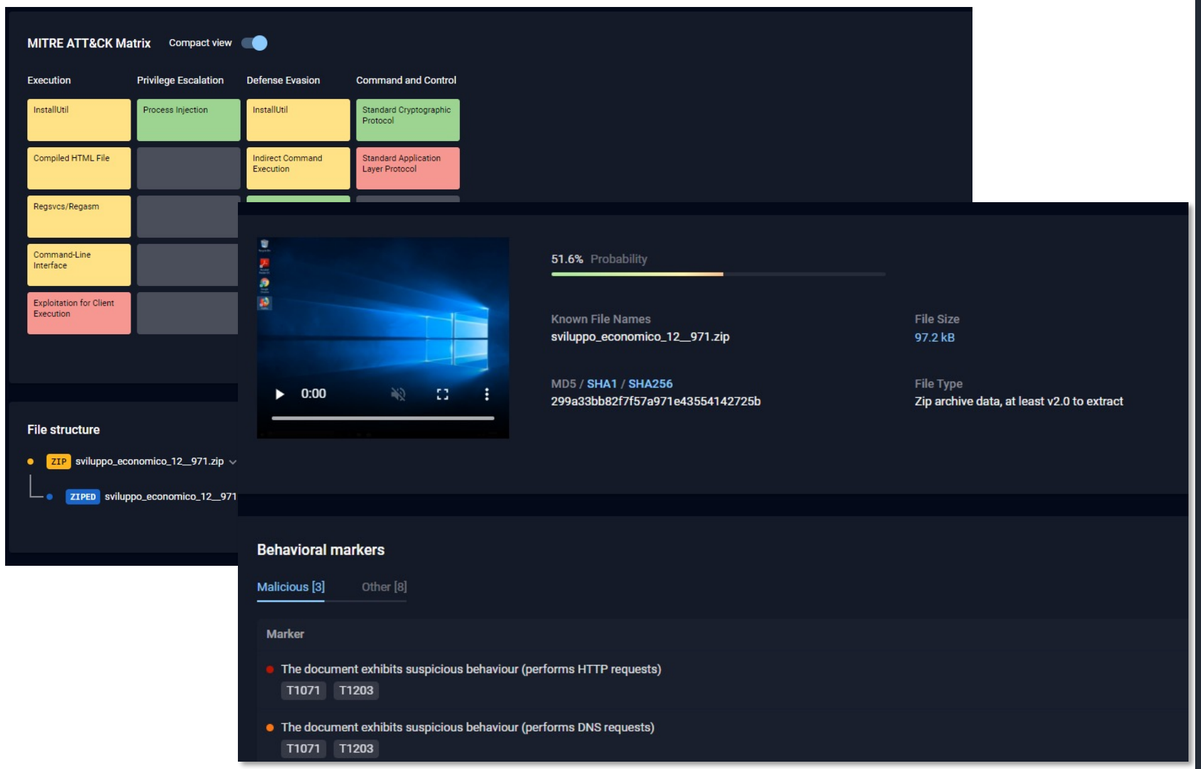
내장된 악성 프로그램 제거 플랫폼

Threat Intelligence & Attribution 인터페이스에서 THF Polygon으로 파일 또는 링크 직접 전송

THF Polygon은 데이터 유출 위험이 없이 심층 행위 분석을 수행하고 상세한 보고서를 제공

사용 방안

수동 모드에서 파일은 제한 없이 다운로드 될 수 있으며, 상용 버전의 THF Polygon에서는 흐름 기반의 분석기능을 제공



- 보안성 평가
- 행위 표식
- 네트워크 활동 분석
- 프로세스 트리
- 파일 구조
- MITRE ATT&CK ®
- 활동 동영상 녹화

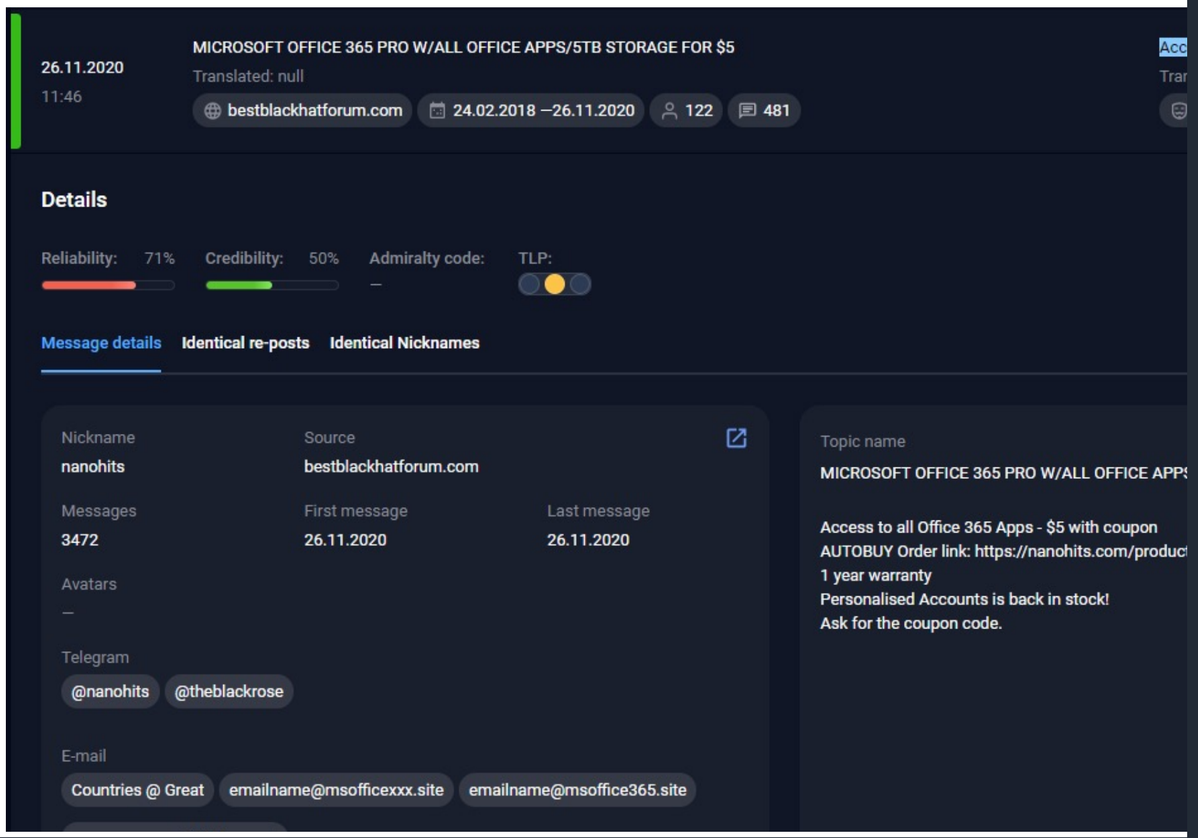
최대 규모의 다크 웹 데이터 아카이브

스크래퍼, 크롤러, 스크립트 또는 " 빅 데이터 " 방식이 비효율적인 폐쇄적 해킹 커뮤니티에 효과적이며 대상 커뮤니티에 침투하여 유효한 정보 수집

- 언더그라운드 포럼에 대한 접근
- 10년 넘게 개발/유지보수된 Sockpuppet계정
- 글로벌 주요 언어별 분석가 보유

고객사 자체 조사를 위한 포괄적 정보 액세스 제공

GIB는 고객에게 내부자 위협 모니터링이나 다크웹에서의 고객사에 대한 언급과 같은 다양하면서 사전대응에 유용한 정보를 제공합니다.

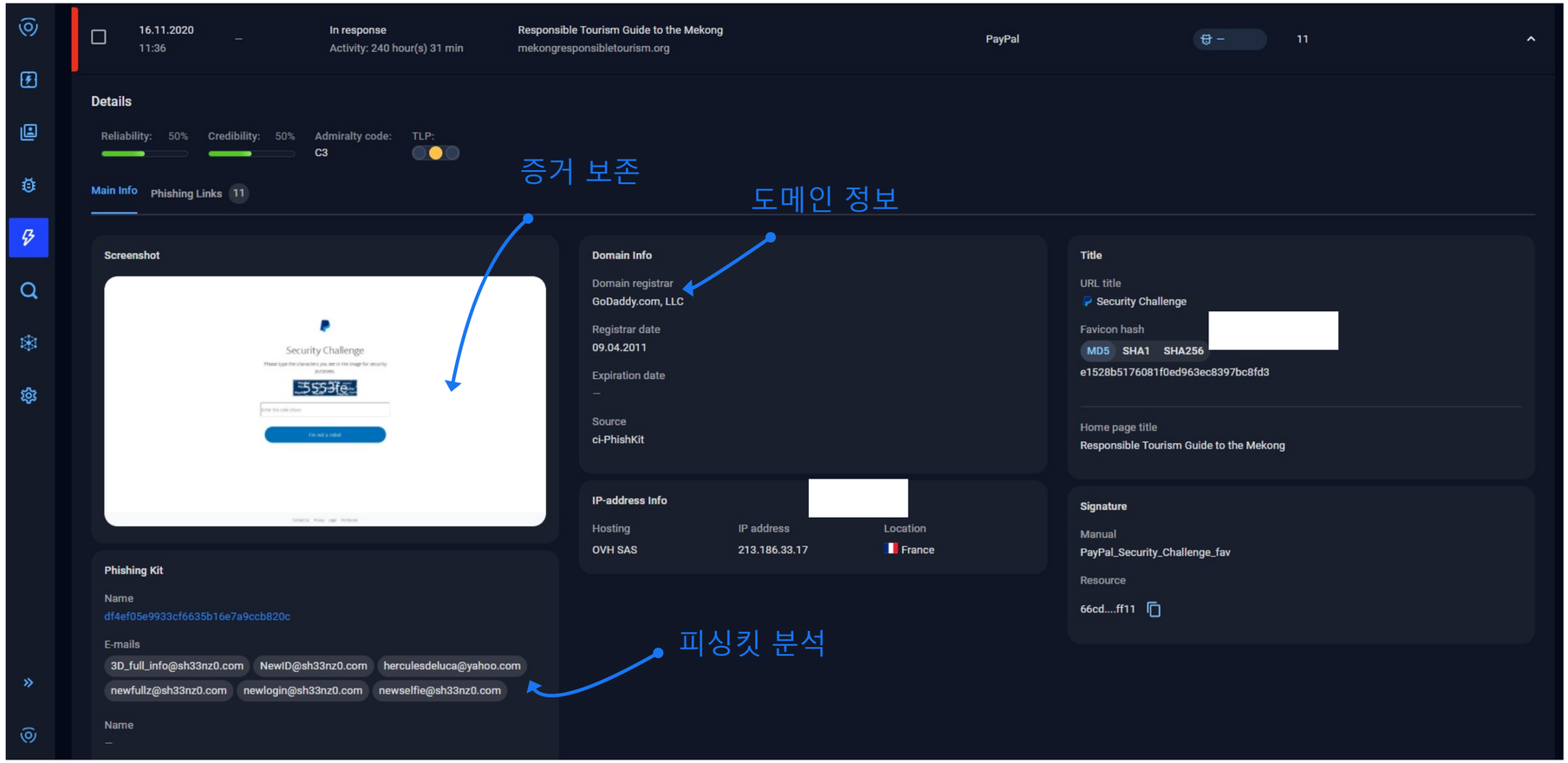


- 새로운 악성 프로그램 및 업데이트 정보
- 새로운 공격 벡터
- 내부자 행위 검색
- 해킹그룹의 전술과 목표 변화 감지
- 탈취 데이터 판매 현황
- 해커 프로파일

피싱 탐지 및 제거

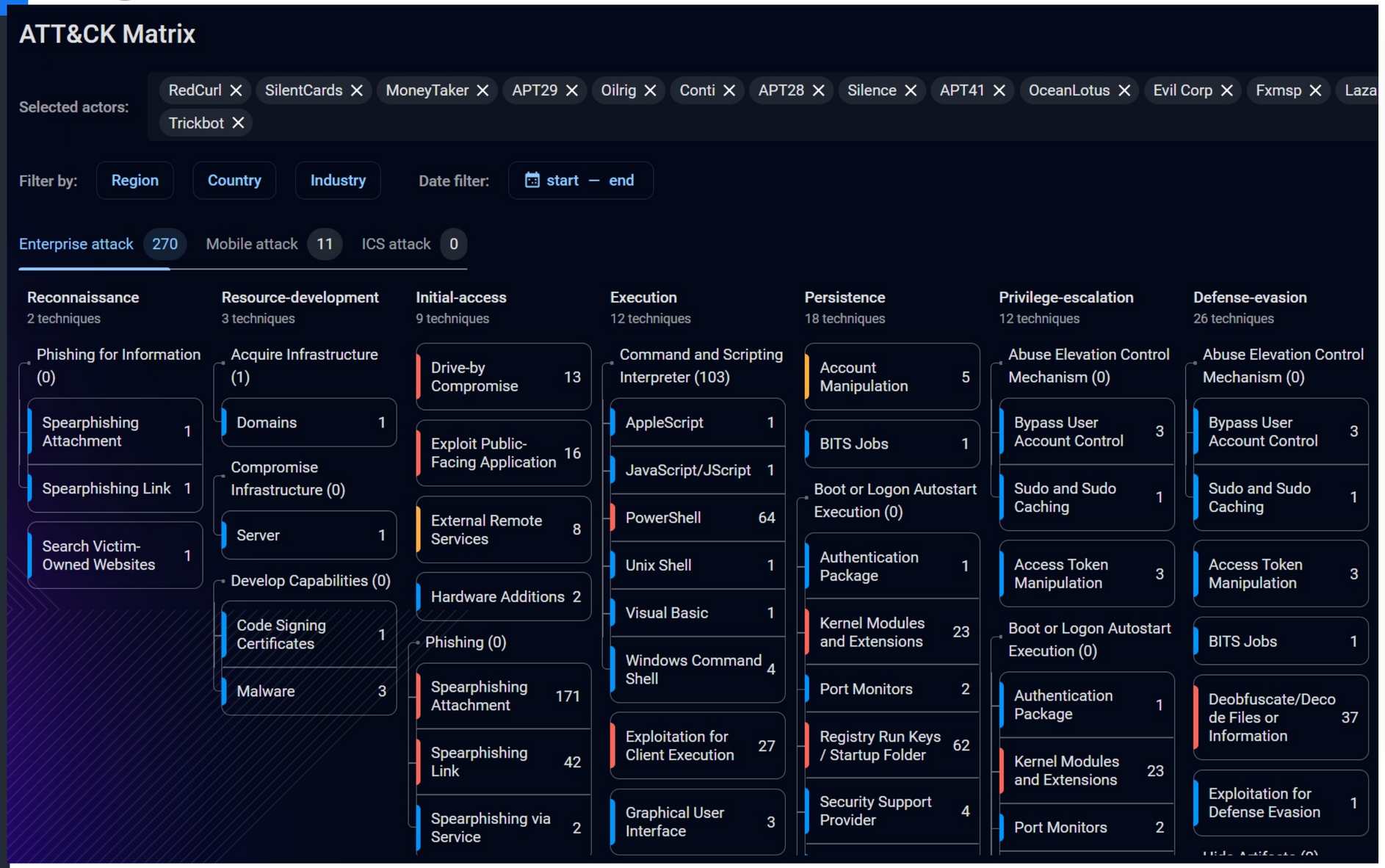
Group-IB의 위협 인텔리전스는 도메인 생성 단계부터 사기성 웹 사이트를 탐지합니다.

- 악성 도메인
- 만료된 가짜 SSL 인증서 식별
- 가짜 또는 악의적인 모바일 애플리케이션



- 조기발견
- 24/7/365 사고 대응
- 99% 제거율
- 신속한 피싱사이트 제거속도
- 디지털 증거 보존
- 18년 이상의 사고조사 경험 및 노하우

MITRE ATT&CK Matrix 제공



가장 신뢰받는 위협 행위자의 TTP 정보 데이터베이스

- 피싱 도메인 모니터링, 피싱 키트 추출, SSL, 광고
- 자동 분석 및 즉각적인 자동 실행
- 복잡한 보안사고 사례의 조사 및 제거 기능

기존 보안 스택과의 연동 기능

보안 스택을 보다 스마트하게 구축 → 보안팀, 보안시스템, 보안전략 개선

풍부한 맥락을 가진 GIB만의 고유 데이터

- 탈취된 계정, 은행 카드, 모바일 단말기
- 피싱 공격
- 표적 멀웨어
- 자료 유출

광범위하고 다양한 기술적 지표를 제공

- 상표권 남용
- 취약점
- 평판 훼손
- DDOS 공격
- 범죄 자금 운반책

- 프록시 서버
- 사설/봇넷 SOCKS
- 핵티비즘 공격
- 의심스러운 IP주소
- 토르 (ToR) 노드

API 혹은 STIX/TAXII를 이용한 연동

- SIEM
- Firewall
- TIPS
- IDS/IPS

주요 위협 인텔리전스 플랫폼 (TIP)과의 연동 MISP Threat Sharing, THREATCONNECT, ANOMALI, EclecticIQ, THREATQUOTIENT

Threat Intelligence 데모

Group-IB 보안 프레임워크

위협 인텔리전스 (TIA)

급변하는 최신 위협에 대한 상세한 속성 제공과 투자보호와 신속한 사고 대응을 위해서 기존 시스템과의 연동성 제공

주적(主敵) 관점의 위협 헌팅 솔루션

사기 행위 헌팅 솔루션

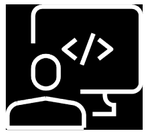
브랜드 보호 플랫폼

위협 헌팅 프레임워크 (THF)

Huntbox | Sensor | Polygon | Huntpoint | Sensor Industrial | Decryptor

사기행위 헌팅 플랫폼 (FHP)

Processing Hub | Web Snippet | Mobile SDK | Preventive Proxy



디지털 위험 보호 (DRP)

불법 복제 방지 | 사기 방지 | 위조 방지

위협 헌팅 프레임워크 개요: 로컬 레벨

센서 (IT)
네트워크 트래픽 분석, 이상 징후 및 감염 탐지

탐지

산업용 센서 (OT)
산업제어 시스템 분석
ICS/SCADA/OT

탐지

디크립터 (Decryptor)
보호된 인프라의 TSL/SSL 트래픽 복호화 전용 솔루션

복호화

폴리곤 (Polygon)
분리된 환경에서의 파일 및 이메일 분석

예방

헌트포인트 (Huntpoint)
호스트에 대한 탐지, 대응 및 포렌식

대응

지표 (Indicators)

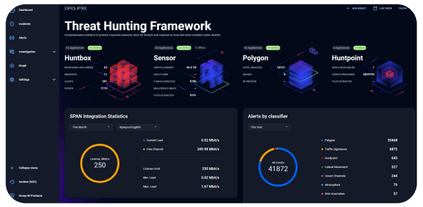
지표 (Indicators)

보고서 (Reports)

이벤트 (Events)

헌트박스 (Huntbox)

- 이벤트 상관관계
- 소급분석
- 자동 위협 헌팅
- 대응 간소화



THF 탐지:

- 뱅킹 및 모바일 트로이 목마
- 제로데이 위협
- 데스크톱, 서버 및 모바일 플랫폼을 향한 공격, 트로이 목마, 백도어 및 악의적인 스크립트
- 숨겨진 통신 채널 (Covert channel)
- 파일리스(Fileless) 위협
- Living off the land (LotL) 공격: 대상 컴퓨터에 이미 설치된 도구를 사용하거나 간단한 스크립트와 셸 코드를 메모리에서 직접 실행하는 공격

위협의 문맥

숨겨진 연결 (connection)

공격자 프로파일링

침해지표 향상

글로벌 외부 위협 헌팅 및 주적 인프라 노출

위협 인텔리전스 및 속성 (TI&A)

적에 대한 인지

- 전략, 기술, 과정 (TTPs)
- 고유 행위 패턴
- 복잡한 표적 공격의 해부도

숨겨진 인프라 노출

- 특정 행위 패턴을 기반으로 한 알고리즘 검색
- 데이터 수집의 독점 기술
- 소급 분석을 위한 과거 데이터 저장소

42억개
매일 검사하는 IPv4 주소 개수

2억천백만개
SSH 핑거프린트 (fingerprint) 혹은 해시값

6억5천만개
도메인과 16년 동안의 과거 데이터

16억개
SSL 인증서

포괄적 내부 네트워크 인프라 보호


GLOBAL CYBER SECURITY COMPANY • GLOBAL CYBER SECURITY COMPANY •
GIB

THF 데모

Group-IB 보안 프레임워크

위협 인텔리전스 (TIA)

급변하는 최신 위협에 대한 상세한 속성 제공과 투자보호와 신속한 사고 대응을 위해서 기존 시스템과의 연동성 제공

주적(主敵) 관점의 위협 헌팅 솔루션

사기 행위 헌팅 솔루션

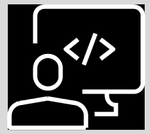
브랜드 보호 플랫폼

위협 헌팅 프레임워크 (THF)

Huntbox | Sensor | Polygon | Huntpoint | Sensor Industrial | Decryptor

사기행위 헌팅 플랫폼 (FHP)

Processing Hub | Web Snippet | Mobile SDK | Preventive Proxy



디지털 위험 보호 (DRP)

불법 복제 방지 | 사기 방지 | 위조 방지

Group-IB 사기행위 헌팅 플랫폼

클라이언트 측 사기 행위 방지 및 디지털 신원 보호

온라인 뱅킹, 포털 및 모바일 앱상에서의 실시간 세션, 플랫폼 및 장치 보호

1. 탐지: 인터넷 뱅킹 사기, 금융사기, 사회공학 공격, 지불 공격, 자금세탁, 피싱, 채널 간 공격 등을 탐지합니다.

2. 차단: 악의적인 봇 활동을 차단합니다.

3. 감소: 잘못된 오탐의 수를 줄이고 사용자에 대한 추가 인증 단계 (SMS) 를 감소시킵니다.

4. 절감: 리스크 보호 프로세스에 따른 비즈니스 비용 절감합니다.

80% 까지 잘못된 오탐과 사용자 알림 감소

100,000,000+ 이상의 전 세계 주요 기업의 최종 사용자를 보호 합니다.

Gartner의 온라인 사기 행위 탐지 관련, 선두 공급업체로 인정받았습니다.

FHP 목표

FHP 기대 효과

사용자 보호 및 비용 절감

탐지 및 예방

사회 공학 공격

- 이메일 사기 (Scam)
- 스미싱 (SMS-phishing)
- 사회 관계망 사기
- 피싱

사용자 계정 사기

- 사기 계정 등록
- 계정 탈취
- 로열티(예: 마일리지) 프로그램 사기

지불 사기

- P2P 지불 사기
- 카드부재 지불 사기
- 스푸핑

멀웨어

- 악성 웹 삽입
- 뱅킹 트로이 목마
- 비승인 원격 접속

교차 채널 & 교차 고객 공격

- 온라인/포털을 통한 공격
- 모바인 단말기를 통한 공격

불법 자금 세탁

- 불법 현금화 네트워크
- 탈세 계획

봇 & 봇넷

- 사용자 행위를 모방하는 봇
- 그 외 다양한 악성 봇

최적화

비효율적인 인증 체계 향상

- 클라이언트 인증을 위한 추가 확인 단계
- 문자 알림, 토큰, 스크래치 카드사용에 따른 기하급수적인 비용 증가

부정적인 고객 경험 감소

- 고객과의 불필요한 통화
- 거래 제한
- 실수로 인한 계정 잠김

첨단 사기행위 방지기술

교차 채널 분석

행위 분석

디바이스 핑거프린팅

적응형 인증

- 18년 이상의 사이버 범죄 퇴치 경력
- 특허받은 기계 학습 및 인공지능 기술
- Group-IB 고유의 위협 인텔리전스 데이터

봇 탐지 및 차단

글로벌 사용자 프로파일링

에이전트 없는 멀웨어 탐지

정책 엔진

연동 플랫폼:

RSA

sas

GBG

ingenuous

Radar

ArcSight

Bottomline


GLOBAL CYBER SECURITY COMPANY
GIB
GLOBAL CYBER SECURITY COMPANY

FHP 데모

Group-IB 보안 프레임워크

위협 인텔리전스 (TIA)

급변하는 최신 위협에 대한 상세한 속성 제공과 투자보호와 신속한 사고 대응을 위해서 기존 시스템과의 연동성 제공

주적(主敵) 관점의 위협 헌팅 솔루션

사기 행위 헌팅 솔루션

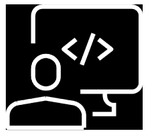
브랜드 보호 플랫폼

위협 헌팅 프레임워크 (THF)

Huntbox | Sensor | Polygon | Huntpoint | Sensor Industrial | Decryptor

사기행위 헌팅 플랫폼 (FHP)

Processing Hub | Web Snippet | Mobile SDK | Preventive Proxy



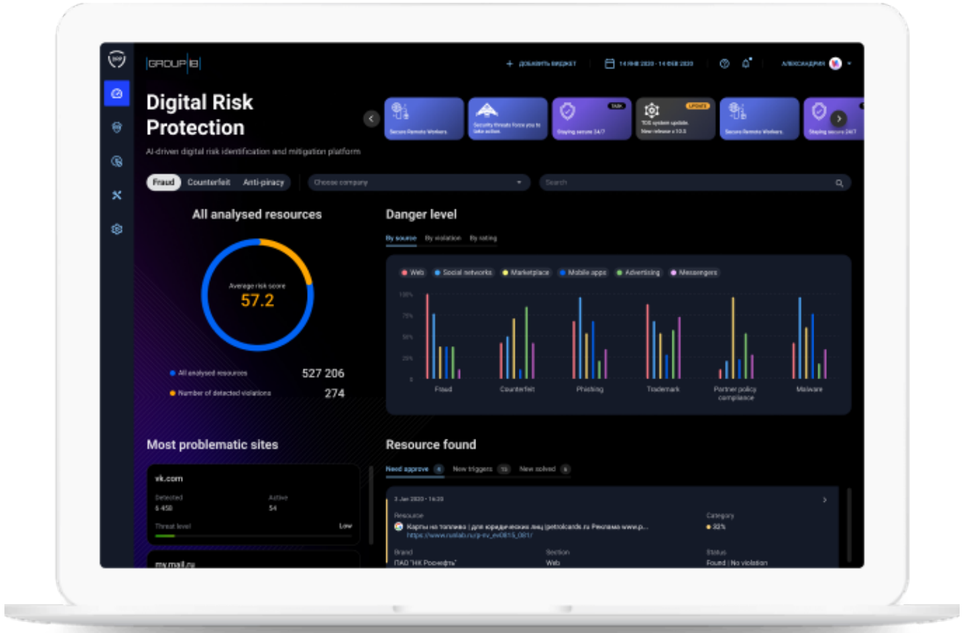
디지털 위험 보호 (DRP)

불법 복제 방지 | 사기 방지 | 위조 방지

Group-IB 디지털 위험 보호 솔루션

Group-IB 디지털 위험 보호 솔루션은 인터넷 상에서 벌어지는 불법적인 사용으로부터 고객의 지적 재산권과 브랜드 가치를 보호하기 위해 고안되었습니다.

GIB가 독자적으로 개발한 소프트웨어



DRP플랫폼은 머신러닝, 사이버 보안 기술, 그리고 브랜드 보호 전문가들의 법률적 경험을 결합되어 포괄적 디지털 위험 보호 기능을 제공합니다.

50
명 이상의 국제적 브랜드 보호 전문가들로 구성

9
년 이상의 브랜드 보호 경험 보유

350
개 이상의 성공적인 브랜드 보호 경험

적발된 위반 사항 분석 및 집행 우선순위 결정

분석 지원 자원

- 딥 웹 (Deep web)
- 검색 엔진
- 모바일 앱 스토어
- 상황 별 광고
- 온라인 광고 및 마켓플레이스
- 소셜 미디어와 사회 지도자
- 텔레그램 채널
- 피싱 데이터베이스

브랜드 이름 언급

위반 결정

집행 우선 순위 결정

대응 – Take-down (제거)

85% 이상의 위반 행위 차단 및 소송 지원

디지털 리스크 보호 솔루션

스캠 방지

- 불법 광고
- 위조 모바일 앱
- 피싱 및 사기성 웹페이지
- 소셜 미디어 상에서의 위조 계정/그룹
- 가짜 파트너십

위조 방지

- 인터넷 상에서의 불법 제품 판매
- 병행 수입 시장
- 파트너십 위반

불법 복제 방지

- 동영상 컨텐츠
- 소프트웨어, 컴퓨터 게임
- 도서, 신문, 기사
- 음원

다양한 산업군에서 금전적 손실 및 평판적 손실 방지:

- 명품 브랜드
- 전자 제품
- 주류
- 자동차
- 화장품, 향수
- 보험
- 제조사
- FMCG
- 유아용 제품
- 스포츠 용품
- 미디어 산업
- 건설

1주일간 스캐머에 의한 손실

소매 회사

사기 홍보 방법: 상황별 광고

1주당 검색 수	**10 000**
클릭 대비 뷰 광고 효과	**14%**
방문객 대비 구매 전환율	**9%**
평균구매단가	**$30**

$ 3,780 1주당 매출 손실

금융사

사기 홍보 방법: 은행 고객을 대상으로 한 소셜미디어 피싱

잠재적 피해자 수	**50,000**명
피해자	하루당 **150**명
사기 피해 고객	**1%**
은행 카드에서 도난당한 평균 금액	**$ 1,000**

$ 10,500 고객피해 보상금액

제조사

사기 홍보 방법: 대상 별 이메일 뉴스레터

1일 수신자 수	**1,000** 명
이메일 뉴스레터의 효과	**20%**
방문객 대비 구매 전환율	**1%**
평균 구매 금액	**$ 800**

$ 11,200 매출 손실

Brand Protection 데모

Q&A

감사합니다!

Stealth Solution / Group-IB Korea
ericli@stealths.co.kr / hs.seo@group-ib.com