

S2W 회사소개

| Who Are We?



비전: 사이버 공간이 보다 안전한 세상이 되는 기술을 제공하는 것

사이버 공간 내 생활이 더욱 넓어지며,
범죄자들은 주 수익 출처로서
“사이버 공간”을 주목하고 있습니다.

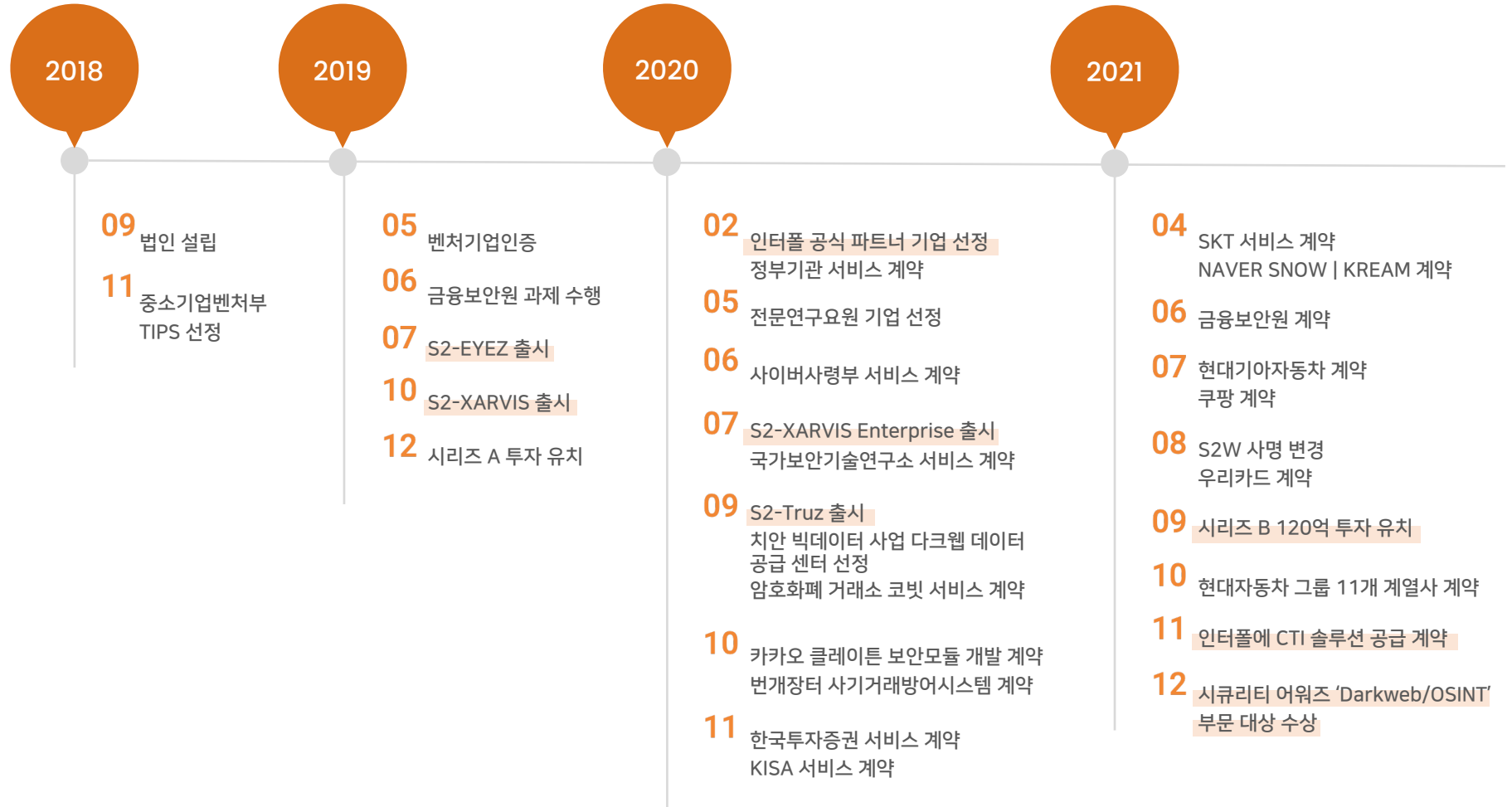
- 사이버 위협은 크게 아래 3가지로 구분됩니다
- 랜섬웨어 등 해킹을 통한 자산 공격/침해
 - 마약, 도박, 성착취물 등 불법/반사회적 활동
 - 플랫폼 내 사기, Bot 이용 조작 등의 어뷰징

효율적인 사이버 위협 대응을 위해서는,
사이버 위협보다 더 빠르고 효과적으로
대응하는 기술력이 요구됩니다.

- 사이버 위협 대응을 위한 인텔리전스 요소 기술
- 사이버 우범지대 가시성 확보 기술
 - 위협 요소의 탐지 및 위험도 평가 역량
 - 빅데이터의 관계기반 분석 및 추론엔진 기술

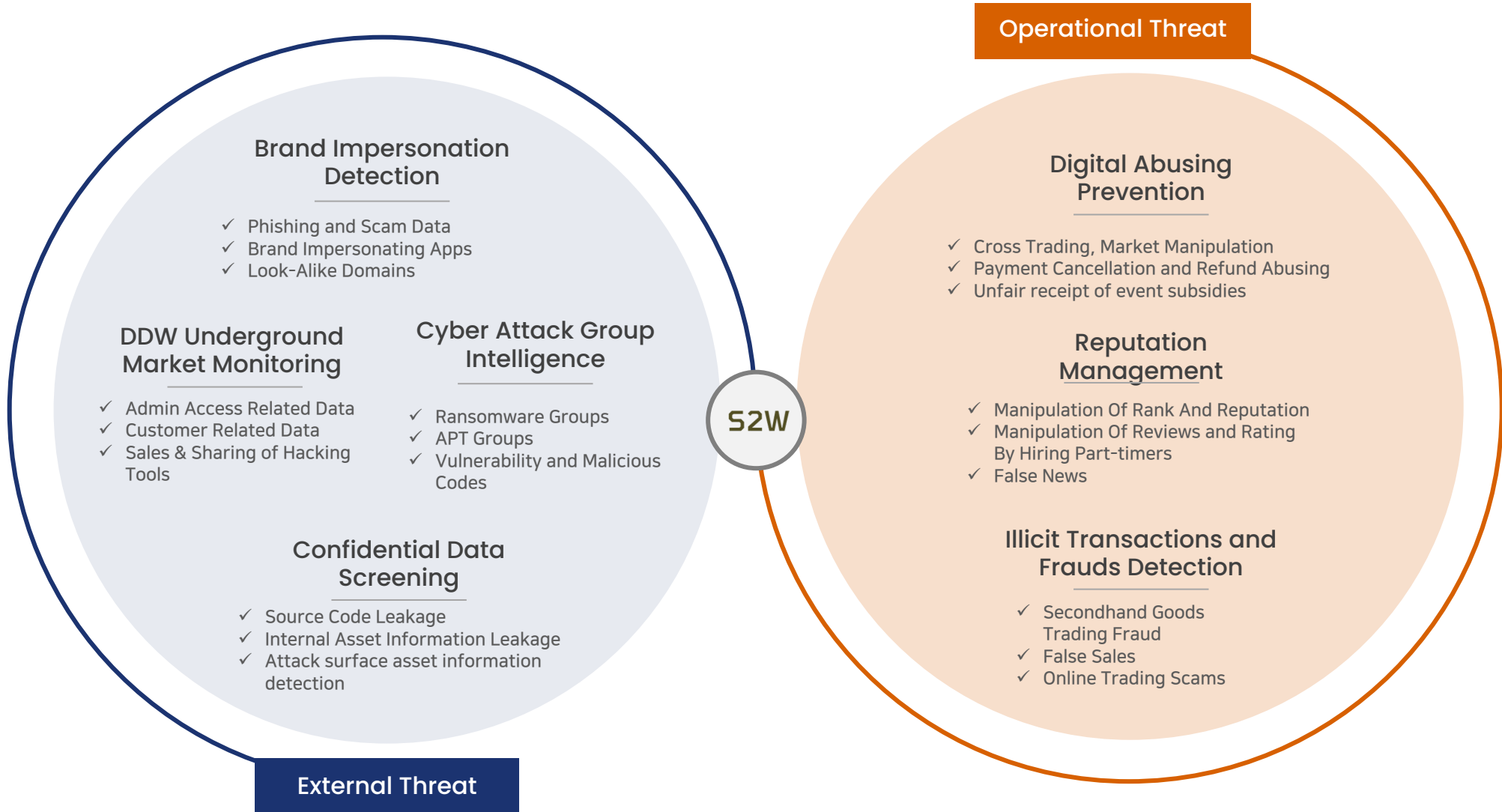
Company History

4년차 딥테크 스타트업으로, 현재 인터폴 및 국내 유명 기업에 위협 인텔리전스 솔루션을 공급 중



| S2W Service Coverage

S2W는 다크웹/해킹 공격 등 외부 위협과, 플랫폼 특징을 악용한 악성행위를 주로 탐지



| Why S2W?

Collect: S2W는 자동화된 데이터 수집 기술력으로 풍부한 위협 데이터를 보유

Collect

1.5M

Darkweb domains

90M+

Darkweb pages

5M+

Document files

20B+

Credentials

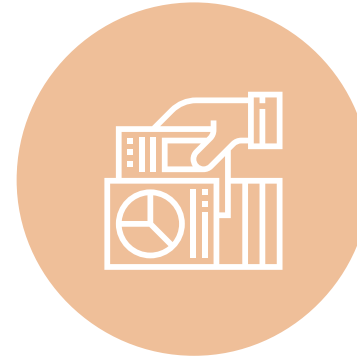
100M+

Images



Data Collection

Collects various types of data from a wide range of sources for analysis



Data Refinement

Extract key elements from collected data

60+

Data Category

20+

Identifier

Identify

Unknown threats

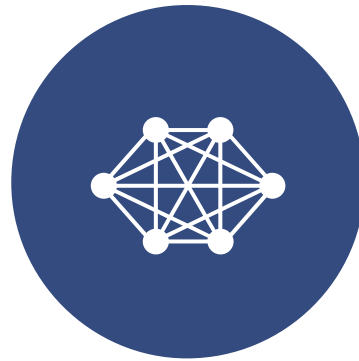
| Why S2W?

Connect: S2W 지식 그래프를 기반으로 actionable intelligence를 제공

Connect

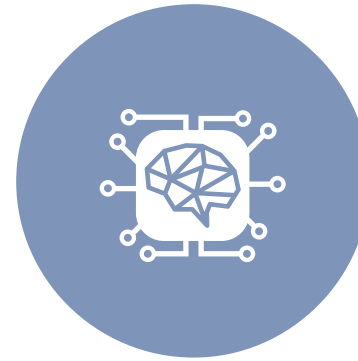
110M+

Graph nodes



**Knowledge
Graph**

Identify hidden threats by
analysing connections
between collected data



**Actionable
Intelligence**

Extract information needed
to provided appropriate
intelligence

Threat

w/ in-depth analysis

Digital Abusing

w/ Deep-learning

Cryptocurrency

w/ On-chain monitoring

| S2W Solution Overview



Threat Intelligence

개인정보, 재무정보, 기업 기밀 유출, 정보 유출
및 외부 위협으로부터 고객을 보호해주는
솔루션입니다.

- ✓ Brand Protection
- ✓ Threat Intelligence
- ✓ Data Breach Monitoring
- ✓ Comprehensive Threat Search
- ✓ Multichannel Threat Analysis



Digital Fraud / Anomaly Intelligence

고객의 시스템에서 이루어지는 의심스러운
거래와 부정 행위를 탐지하는 솔루션입니다.

- ✓ Digital Behavior Analysis
- ✓ Digital Fraud Detection
- ✓ Anomaly Scoring
- ✓ Intellectual Property Protection
- ✓ Illegal Transaction Monitoring



Cryptocurrency Intelligence

의심스러운 암호화폐 거래를 탐지 및 방지해주는
AML 솔루션 입니다.

- ✓ Illicit Transaction Detection
- ✓ Cryptocurrency Clustering
- ✓ Prevent Suspicious Transaction
- ✓ Threat Detection from DDW/Internet
- ✓ Crypto Audit Services

| S2W People – R&D

S2W 위협 인텔리전스 빅데이터 플랫폼 개발을 위한 R&D 전문성

R&D 주요 인력 (총원 31명)

CTO

윤창훈 연구소장

- KAIST 정보보호 박사
- 익명화 네트워크 데이터 수집/분석
- 다크웹: 2019 WWW 발표 (웹 분야 최우수 학술대회)

자연어 처리

정진우 수석 연구원

- KAIST 전산학과 박사
- (전) 삼성전자 종합기술원
- 사이버 위협 정보 추출
- 텍스트마이닝 기술 전문가

악성코드 분석

김민수 수석 연구원

- KAIST 정보보호 박사
- (전) 국가보안기술연구소
- 악성코드 분석 자동화
- 바이너리 및 해킹 기법 연구

데이터 베이스 개발

항인욱 이사

- 서울대학교 컴퓨터공학과 석사
- (전) 삼성전자
- 대규모 시스템 개발/구현
- 고성능 데이터 베이스 개발/구현

수집

양준석 수석연구원

- KAIST 정보보호 석사
- (전) LG전자 연구소
- 사이버 범죄 데이터 수집 플랫폼 구축

빅데이터 처리

김연근 수석 연구원

- KAIST 정보보호 석사
- 익명화 서비스 기반 범죄 데이터
- 교차 분석 등 사이버 범죄 플랫폼 및 인터페이스 설계

암호 화폐 추적

이승현 수석 연구원

- KAIST 전산학과 박사
- 가상화폐 분석
- 다크웹 관련 2019 NDSS 발표 (세계 4대 보안학회)

딥러닝

이문헌 이사

- KAIST 전산학과 석사
- (전) ETRI, 삼성전자, 티맥스
- 인공지능 스타트업 CTO
- AI 기반 이미지 및 텍스트 인식 시스템 개발



| S2W People – TALON (CTI Analyst Group)

Actionable Intelligence 제공을 위한 전문 분석가 그룹

TALON 주요 인력 (총원 18명)

TALON Head

곽경주 이사

- (전) 금융결제원 / **금융보안원** 침해위협분석
- 사이버 범죄/국가급 배후 공격그룹 분석
- MITER ATT&CK (마이터어택), 공격그룹 Andariel 등재

Core Tech

Vulnerability
Research & Discovery
Core Technology
Research



- 고려대 사이버국방학과, 카이스트 석사
- **DEFCON 및 각종 CTF 우승** 경력 다수
- 다수의 Oday 취약점 발견 및 리포팅
- 백신, VirtualBox 등 관련 취약점 연구
- Oday, n-day 취약점 연구 및 POC 작성

Threat Analysis

Malware analysis	Malicious Infra analysis & Tracking
Threat-actor Profiling	Detection Research
Vulnerability Analysis	Analysis Methodology Research



- (전) **금융보안원** 침해위협분석팀
- DEFCON 및 각종 CTF 대회 상위입상 다수
- 북한 배후 위협 그룹 분석
- OSINT 정보 수집 및 분석



- **정보보호올림피아드 금상**
- 국제 해킹대회 (**DEFCON 등**) 다수 입상
- 취약점 연구 및 악성코드 분석



- (전) **KISA 코드분석팀**
- 국가 배후 및 랜섬웨어, 스틸러 등 사이버 범죄 관련 공격 조직 분석



- (전) **AHNLAB 분석가**
- 북한, 중국 관련 공격 조직 및 악성코드 분석

Threat Hunting

OSINT	All-source analysis
HUMINT	Intelligence tool Dev.
SOCMINT	Discover new intel sources



- (전) **ENSIGN/HORANGI** 분석가
- DDW 위협 정보 분석 및 사용자 프로파일링
- Takedown 프로세스 지원 및 대응



- (전) **경찰청 디지털포렌식센터** 분석가
- DDW 위협 정보 분석
- 암호화폐 추적



- DDW 위협 정보 분석 및 사용자 프로파일링
- 중국 DDW 인텔리전스 수집 및 분석
- 서울청 공조, 다크웹 마약 사범 검거

| S2W Publication & Patent

사이버 위협 인텔리전스의 코어 기술 분야의 원천기술력을 축적 중

	제 목	기술 스택		
		수집	처리	분석
논문	• Cybercriminal Minds: An investigateive study of cryptocurrency abuses in the Dark Web (NDSS 2019)	다크웹 수집		가상화폐 분석
	• Doppelgangers on the Dark Web: A large-scale Assessment on phishing Hidden Web Services (WWW 2019)	다크웹 분석 피싱정보 수집		해킹기법 분석
	• OPERATION NEWTON: HI KIMSUKY? DID AN APPLE(SEED) REALLY FALL ON NEWTON'S HEAD? (Virus Bulletin 2021)			악성코드 분석
특허 (등록)	• 암호화폐 거래 분석 방법 및 시스템		블록체인 데이터 처리	가상화폐 자동분석
	• 지식 그래프를 이용하여 사이버 시큐리티를 제공하는 방법, 장치 및 컴퓨터 프로그램		그래프 데이터베이스	멀티도메인 추론엔진
	• 암호화폐 거래 분석 방법 및 장치			가상화폐 거래분석
	• 암호화폐 거래를 분석하기 위한 데이터 획득 방법 및 장치	가상화폐 수집		
	• 멀티 도메인에서 데이터를 수집하는 방법, 장치 및 컴퓨터 프로그램	다양한 위협 수집	대용량 데이터 처리기술	
특허 (출원)	• 악성코드 분석 시스템 및 시스템의 동작 방법			악성코드 자동분석
	• 웹 페이지에서 자동으로 사용자 식별 객체 획득하는 방법	딥웹/서피스웹 수집		인터넷 위협정보 분석
	• 멀티 프로세스를 통해 파일을 저장하기 위한 방법 및 이를 위한 장치		빅데이터 처리기법	
	• 유사도 기반의 악성코드 진단 방법 및 장치		AI 기반 코드 처리	악성코드 분석 알고리즘
	• 가상화폐 트래킹 방법 및 그 장치			가상화폐 추적
	• 전자 상거래에서의 이상거래 추적 방법 및 시스템		어뷰징 데이터 처리기법	관계기반 분석

| Our Clients & Partners

Public Sector						And more	
Financial	한국투자 증권			BNK 부산은행			
Telecom & Hightech							
Mobility							
Commerce & Platform			BALAAAN				
Manufacturing & Others							And more
Partners					AI Spera		

| S2W with Interpol

국경 없는 사이버 위협 해결을 위해 첨단 기술력과 분석 인텔리전스 제공

Cyclone 작전

Clop 랜섬웨어 검거 작전

- ✓ 원점 추적 위한 Clop 관련 인프라 정보 분석
- ✓ Clop 랜섬웨어 비트코인 자금흐름 분석
- ✓ 다크웹 내 Clop 랜섬웨어 오퍼레이터들의 활동 분석 및 프로파일링




Quicksand 작전

Gandcrab & Revil Sodinokibi 검거 작전

- ✓ 악성코드 관련 분석 정보
- ✓ 공격 그룹 관련 정보 제공

온라인 아프리카 범죄 조직 분석




- ✓ 다크웹 내 아프리카 관련 범죄 분석 제공
(마약, 인신매매, 밀수 등)

 EN  

INTERPOL deployed Operation Cyclone with the assistance of information provided by its private partners Trend Micro, CDI, Kaspersky Lab, Palo Alto Networks, Fortinet and Group-IB through INTERPOL's Gateway project.

Gateway boosts law enforcement and private industry partnerships to generate threat data from multiple sources and enable police authorities to prevent attacks.

Further illustrating the power of private sector cooperation in cybercrime investigations, two Korea-based cyber threat companies – **S2W** LAB and KFSI – also provided INTERPOL with valuable dark web data analysis throughout the operation.

 EN  

Bitdefender supported operations by releasing tailor-made decryption tools to unlock ransomware and enable victims to recover files. These innovative tools enabled more than 1,400 companies to decrypt their networks, saving them almost EUR 475 million in potential losses.

KPN, McAfee, **S2W** helped investigations by providing cyber and malware technical expertise to INTERPOL and its member countries.

Operation Quicksand continues to supply evidence that is feeding into further cybercrime investigations and enabling the international police community to disrupt numerous channels used by cybercriminals to launder cryptocurrency and commit ransomware crime.

Online African organized crime from surface to dark web

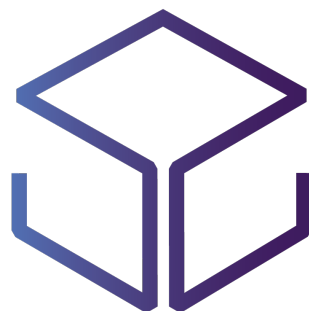
✓ S2W가 제공한 분석 내용으로 발간한 인터폴 내부 보고서

ANALYTICAL REPORT

Crime-specific keywords in dark web domains, other than 'porn'

Keyword	Count
Drug	26.1
Credit	14.8
Murder	10.1
Smuggling	2.9
Hitman	5.3
Trafficking	4.9

Figure 18. Dark web screenshot of a vendor site



S2W

Safe and Secure World

For any inquiries, please contact
info@s2w.inc