

K-CTI 2023

최신 다크웹 동향으로 본 CTI 솔루션이 나아가야 할 길

S2W 박민수 이사 (mspms@s2winc)

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.

Contents

- 최신 다크웹 동향 및 시사점
- 보안담당자를 위한 CTI 솔루션의 필수 요건

최신 다크웹 동향 및 시사점

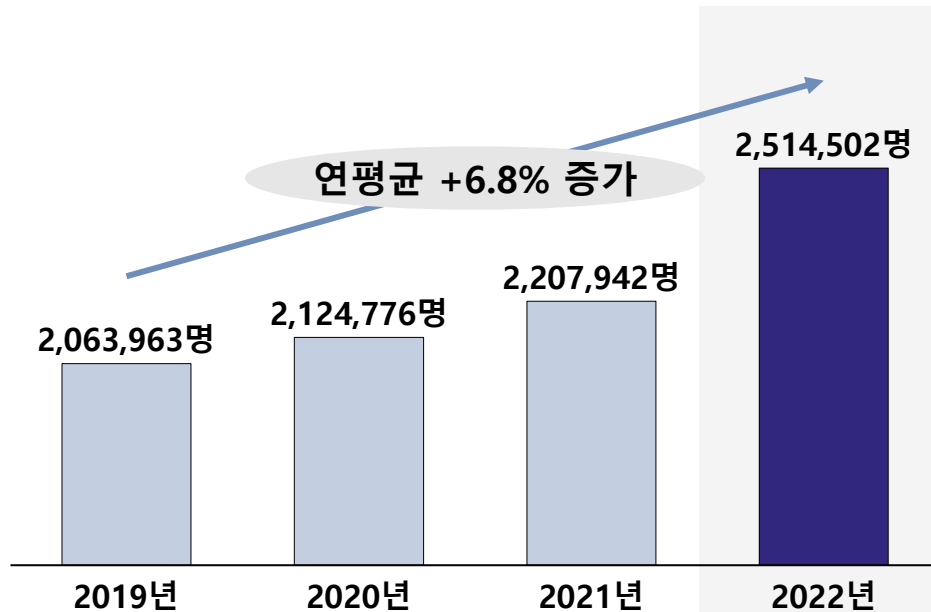
딥&다크웹: 최신 해킹 기술과 공격에 필요한 자료를 손쉽게 저렴하게 구할 수 있는 공간

The collage illustrates the ecosystem of the Deep & Dark Web for cyberattacks, featuring several key platforms:

- RAMP (Russian Anonymous Marketplace Platform):** A Russian-language marketplace with sections for 'Все публикации' (All publications), 'Партнёры' (Partners), 'Софт' (Software), 'Доступы / БД / Логи' (Access / Databases / Logs), 'СПАМ / Трафик' (Spam / Traffic), 'Серверы' (Servers), 'Кардинг' (Carding), 'Работа' (Work), and 'Разное' (Miscellaneous). A prominent advertisement for '[Ransomware] LockBit 2.0 - криптолокер, партнёрская программа.' (crypto locker, partner program) is shown, posted by 'LockBit Продавец' on August 19, 2021.
- Genesis Marketplace:** A platform with a sidebar menu including 'Dashboard', 'Genesis Wiki', 'News', 'Bots', 'Generate FP', 'Orders', 'Purchases', 'Payments', 'Tickets', and 'Software'. The 'Available Bots' section shows a table with columns for 'COUNTRY', 'LAST 24H', 'LAST WEEK', 'LAST MONTH', and 'AVAILABLE'. A specific bot, 'Reconshell', is highlighted with 5,436 subscribers.
- Hacking Forum:** A forum with sections for 'Articles \文章', 'Data base & leakage \数据库和泄漏', 'Books', and 'Anonymity and Security'. It lists various threads and messages, including 'HTB EarlyAccess, Techn...' and 'Brazilian Databases'.
- Ransomware Homepage:** A page featuring a 'LEAKED DATA' banner and a section for 'PUBLISHED FILES' with a 'Secret data link' and 'open links'.
- Telegram Channel:** A channel named 'Reconshell' with a focus on 'VPS web hacking tools'. It includes a list of hashtags like #WebHacking, #VPS, #Bugbounty, #Hacking, #KaliLinux, #Exploit, #Vulnerability, #Infosec, #Appsec, #Malware, #Pentest, #VAPT, #Cyber, #Security, #Scanner, #Hacker, #OSINT, and #IncidentResponse. The channel also mentions 'Penetration Testing Tools, ML and Linux Tutorials' and 'VPS web hacking tools - Penetration Testing Tools, ML and Linux Tutorials'.

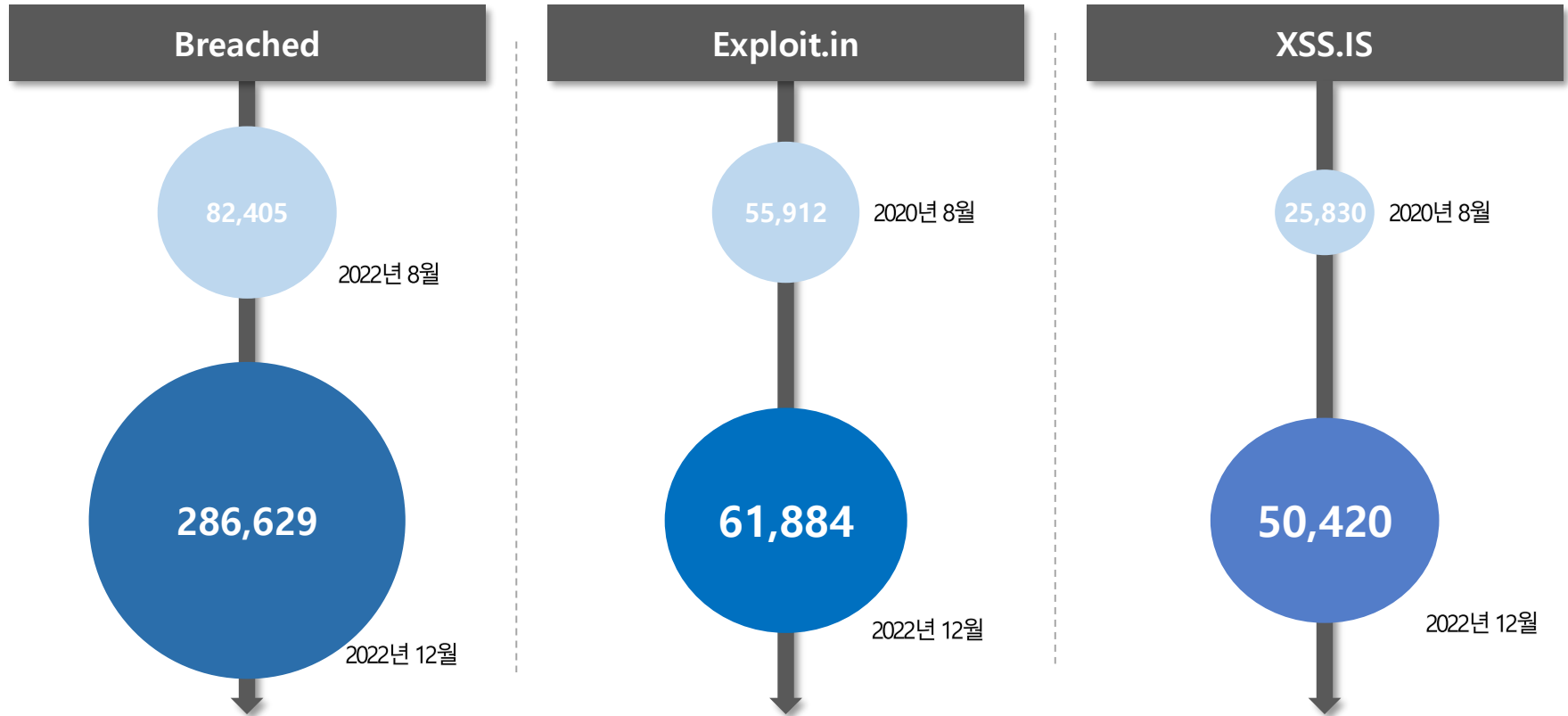
다크웹 유저: 다크웹 접속자 수는 꾸준한 상승 추세

2019 – 2022 전세계 일평균 다크웹 접속자

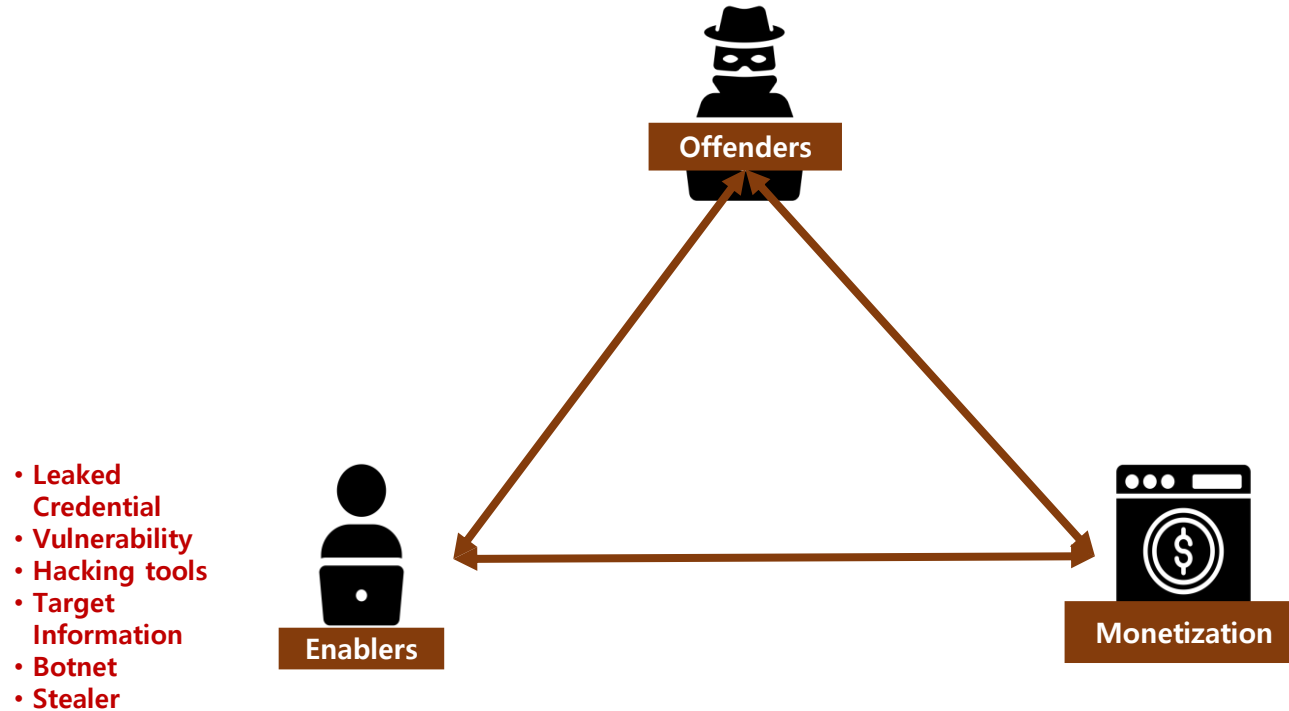


일평균 접속자
250만명 돌파

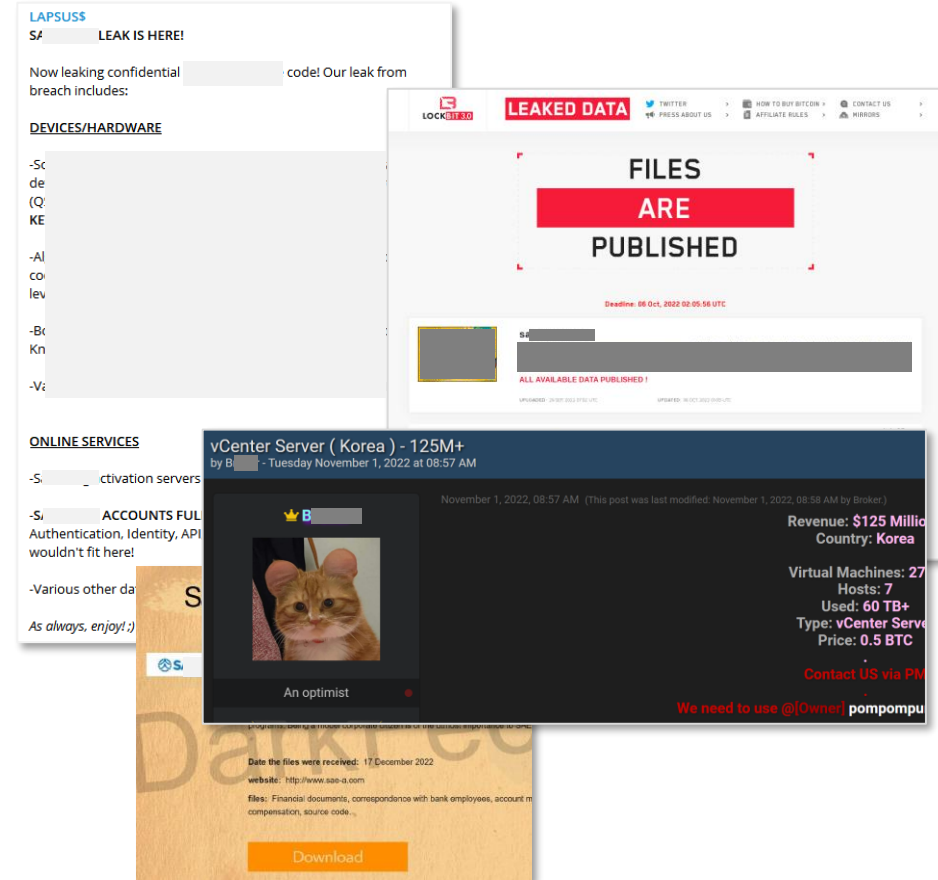
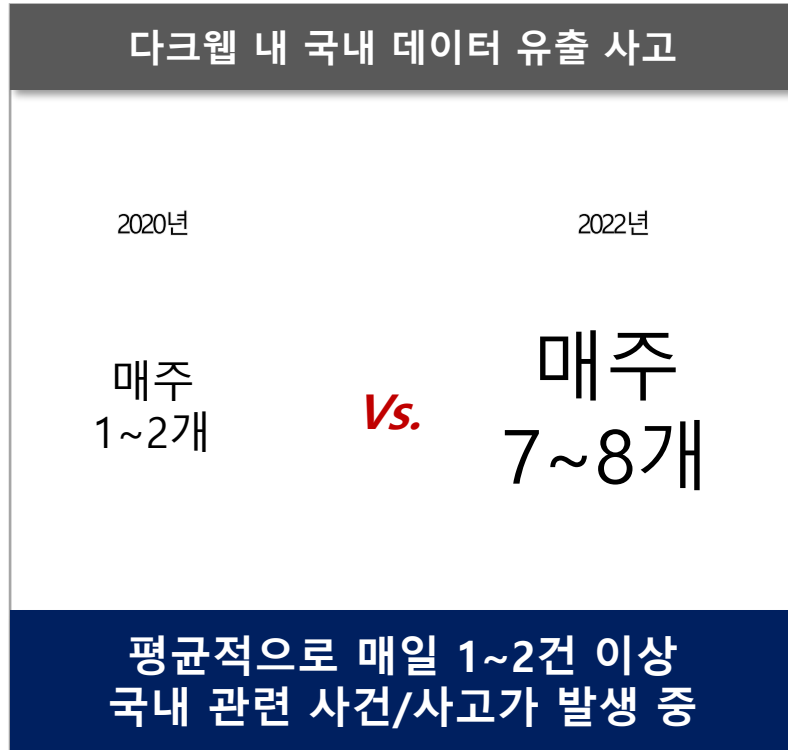
주요 해킹 포럼 회원수도 꾸준히 증가세



딥&다크웹을 중심으로 사이버범죄 생태계가 지속 진화 중



딥&다크웹 내 국내 관련 사건/사고는 과거와 비교해 현격히 증가



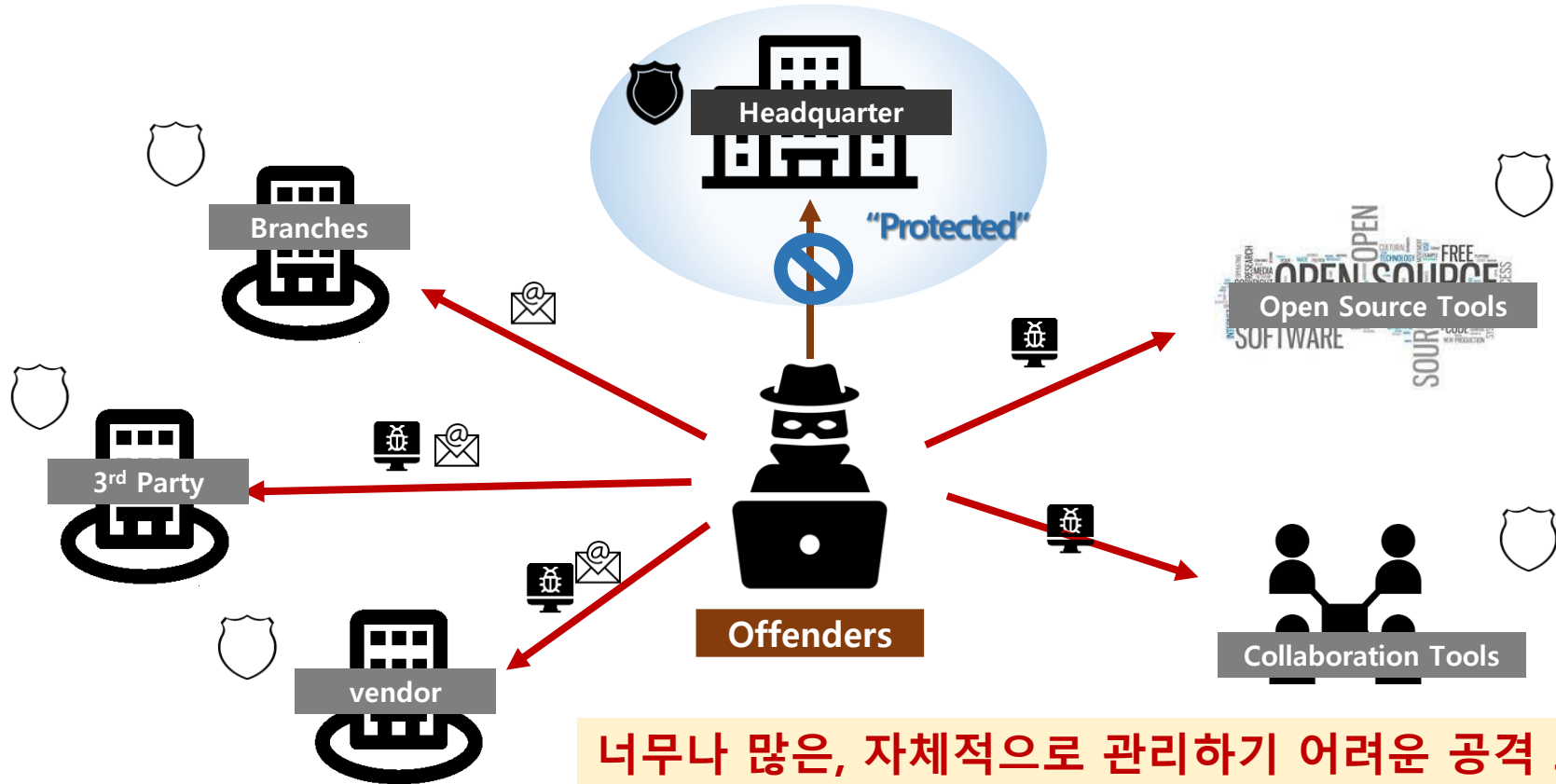
유출된 파일에는 기업 기밀 자료, 민감 개인 정보, 소스코드, 도면 등 그 범위는 매우 다양함

DATA LEAKAGE

The collage displays several types of leaked data:

- Top Left:** A form titled "보험금 지급 청구서" (Insurance Claim Form) and a "제적증명서" (Certificate of Discharge).
- Top Center:** A document titled "1종 보통" (1st Ordinary License) for a "자동차운전면허증 (Delicate License)" (Motor Vehicle Driving License).
- Top Right:** A document titled "자동차보험 가입증명서" (Motor Vehicle Insurance Confirmation Certificate) and a "자동차보험 증권" (Motor Vehicle Insurance Certificate).
- Bottom Left:** A document titled "회의록" (Meeting Minutes) for "A사 내부 회의록" (Internal Meeting Minutes of Company A).
- Bottom Center:** A document titled "D사 이메일 및 제품 도면" (Email and Product Drawing of Company D).
- Bottom Right:** A document titled "B사 외부 평가단 설의 회의 참석자 명단" (List of Attendees for the External Evaluation Team Meeting of Company B).
- Bottom Far Left:** A document titled "C사 내부 대외비 문서" (Internal Confidential Document of Company C).
- Bottom Far Right:** A large spreadsheet with multiple columns and rows, likely containing sensitive data.

공격은 기업 본사 뿐 아니라, 보안이 상대적으로 취약한 협력사, 자회사 및 Open Source ,
다양한 공급망 등 다양한 사각지대에서 발생



S2W가 돌아본 2022년 주요 트렌드 (1) 범 다크웹 공간 확대

텔레그램이 다크웹과 유사한 정보 유출의 채널로 활발하게 활용

파일 업로드 및 공유, 채널 생성 등이 용이한 텔레그램으로 해커들이 활동 영역을 넓히는 중



S2W가 돌아본 2022년 주요 트렌드 (2) 유저 프로파일링의 중요성

해티비즘 해커 활동 증가

사회적 이슈에 적극적인 의견을 제시하며 반대되는 국가/조직에 대해 사이버 공격을 가하는 '해티비즘' 성향을 천명하는 공격 그룹 다수 포착.

특정 국가, 산업 데이터 전문 해커 등장

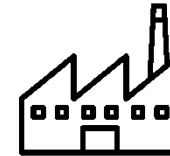
특정 국가나 산업을 집중 타겟하는 공격 그룹 존재.
이에 관련 국가/산업은 해당 공격 그룹을 면밀히 모니터링 할 필요 있음

한국 집중 타겟, 신종 위협 그룹 주목 중

Gwisin Ransomware: 금융권 및 제약회사 타겟
DemoCRov (Masscan Ransomware) : 작년 국내 콜택시 운영업체 전산 센터와 백업 서버 마비
Teng Snake: 금융권 웹사이트 취약점 및 기업 AD 서버 권한 취급



Set target and Attack



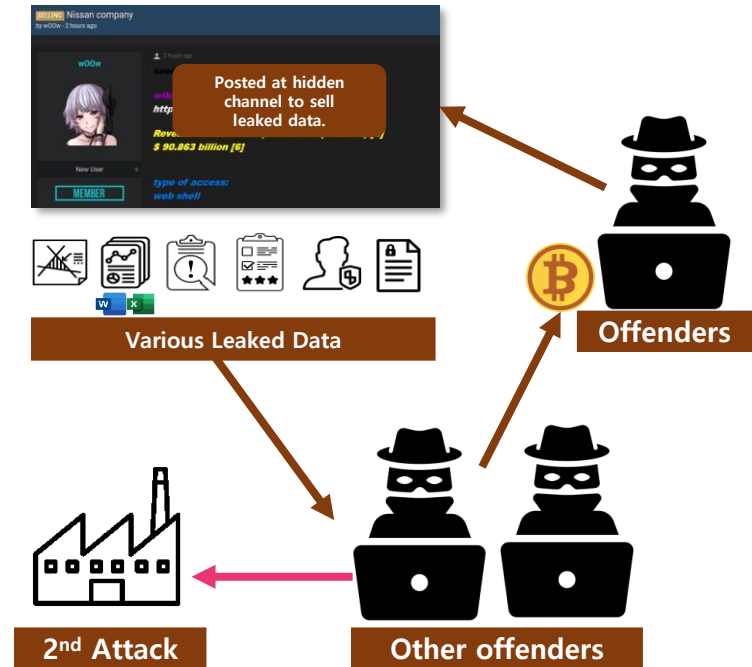
S2W가 돌아본 2022년 주요 트렌드 (3) 주기적 공격 표면 관리 및 예기치 못한 데이터 유출 영역 대응 필요성 증대

한번만 감염되도 2차, 3차 데이터 재확산

과거 유출된 데이터가 타 해킹 포럼이나 텔레그램을 통해 재공유되는 정황 다수 포착. 일부 피해 기업은 네트워크 접근 권한 수차례 유출

랜섬웨어의 진화, 협력/관계사 모두 방어 필요

'22년에 가장 활발했던 랜섬웨어 그룹 'LockBit' 은, 11월에 국내 기업의 데이터를 유출. 데이터에는 협력사 데이터도 포함, 2차 피해 야기



S2W가 돌아본 2022년 주요 트렌드 (4) 공격자가 선호하는 취약점 지속 모니터링 필요

지속 주목해야 할 Confluence 취약점

- '22년 5월 Confluence 서버에 임의 명령을 실행할 수 있는 취약점 발견 후, 패치 공개되었으나 CyberCrime 그룹에서 사용한 정황 포착

2022.06.21

Confluence Vulnerability(CVE-2022-26134) Issue Tracking

TALON REPORT > VULNERABILITY

PDF Report

- Confluence 서버 취약점인 CVE-2022-26134는 취약한 On-premise 서버를 대상으로 임의의 명령을 실행할 수 있는 취약점
 - 영향받는 제품: Confluence Server, Confluence Data Center
- 취약한 Confluence 서버에 대해 임의 명령을 실행할 수 있는 CVE-2022-26134가 발견되었으며, 취약점에 대한 주요 타임라인은 다음과 같음
 - 2022.05.31, Volety에서 ITW에서 발견한 취약점을 제보
 - 2022.06.03, 해당 취약점에 대한 패치가 공개
 - 2022.06.03, Rapid7에서 취약점 분석 내용 및 Payload 공개
 - 2022.06.11, MS에서 CVE-2022-26134 취약점을 사용하는 Threat Actor 및 악성코드 공개 (DEV-0401, DEV-0234, Cerber2021, ETC)
 - 2022.06.11, BleepingComputer에서 Prodaft에서 공개한 AvosLocker 그룹이 CVE-2022-26134 취약점을 사용하는 정황에 대해 공개
- 해당 취약점을 사용하는 공격 그룹이 명확히 밝혀지지 않았지만, 취약점 패치 및 공격 Payload가 공개된 이후 CyberCrime 그룹에서 사용한 정황들이 발견되고 있어 주의가 필요함
 - 관련 그룹: AvosLocker, Cerber2021(Cerberimposter), DEV-0401, DEV-0234, ETC

Endless Log4Shell

- KINSING 악성코드, MIRAI 봇넷 등에 악용되는 CVE-2021-44228



보안담당자를 위한 CTI 솔루션의 필수 요건

구슬이 서말이라도 꿰어야 보배다 : 우수한 전략보다, 실행가능한 환경이 중요



정보보호 업무 효과적 수행 저해 요인 1위...“보안전담 조직과 인재 부족”



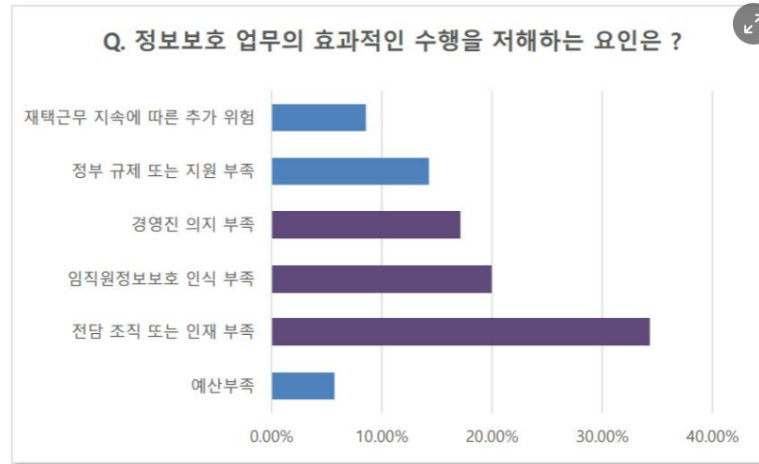
HOME > 이슈 > 긴급속보

정보보호 업무 효과적 수행 저해 요인 1위...“보안전담 조직과 인재 부족”

김민권 기자 | 승인 2021.02.08 14:38



CONCERT, 2021년 기업 정보보호 이슈 전망 보고서 발표

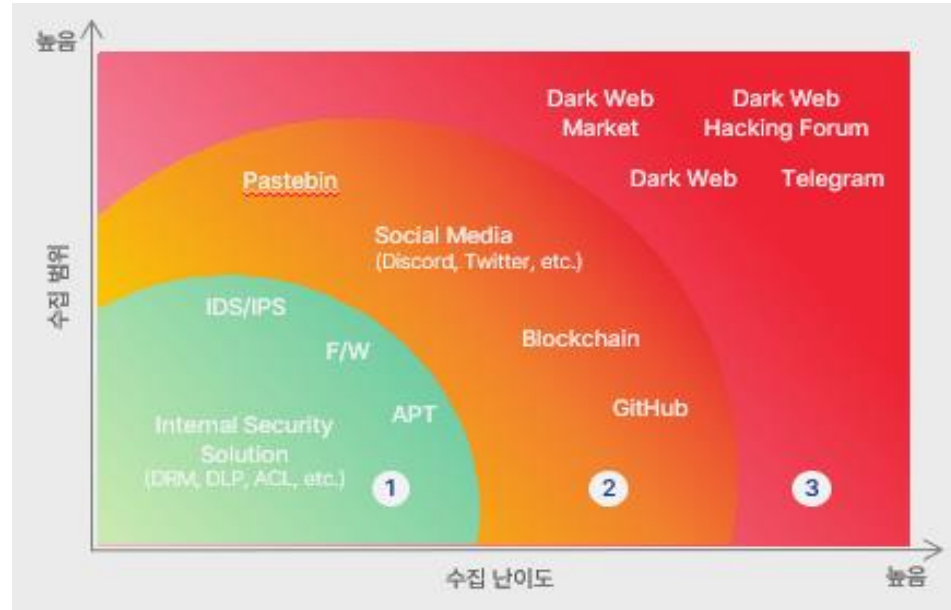




보안담당자를 위한 **최적의 CTI 솔루션 Checklist**

- 1** 다양한 채널을 커버하고 있는가?
- 2** 다양한 위협에 능동적인 대응이 가능한가?
- 3** 필요할 때 분석가 지원이 잘 되는가?

1 다양한 채널을 커버하고 있는가?



1 Internal Threat Intelligence

2 External Threat Intelligence: Surface Web

3 External Threat Intelligence: Deep/Dark Web

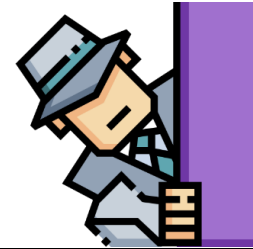
2 다양한 위협에 능동적인 대응이 가능한가?



Malware



Vulnerability



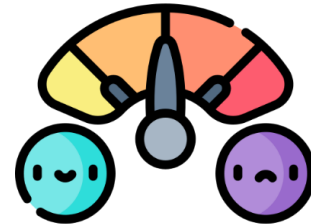
Incidents



Data Breach



Threat Actor



Abusing

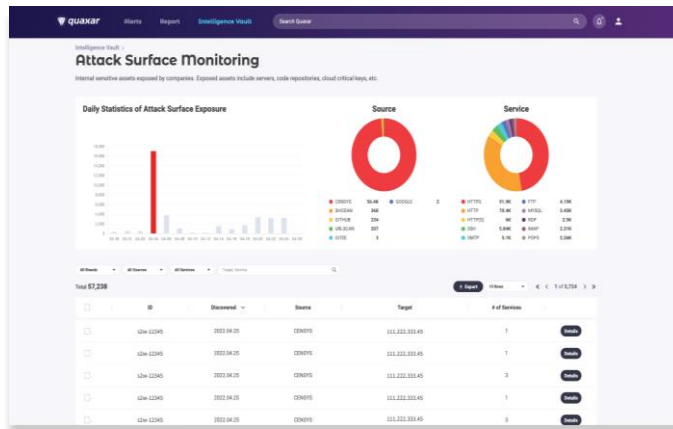
2 다양한 위협에 능동적인 대응이 가능한가?

사이버 위협 인텔리전스 **컨텐츠**

Malware	랜섬웨어, 스틸러, 봇넷, 백도어, 원격제어형 ...
Vulnerability	각종 취약점 정보 (Spring4shell, Log4shell, Dirty-Pipe, ProxysHELL) ...
Incidents	LAPSUS\$, Gwisin, BGP 하이재킹, 월패드 이슈 ...
Data Breach	딥웹 포럼, 다크웹 기반 유출 사이트, 소셜 미디어, 텔레그램, 표면웹 상에 노출된 민감 정보 ...
Threat Actor	국가 배후 공격 그룹, 사이버 범죄 조직, 딥/다크웹 포럼 사용자 ...
Abusing	유사 도메인, 정상 서비스/명령어를 악용한 공격(Living-Off-the-Land Attacks) ...

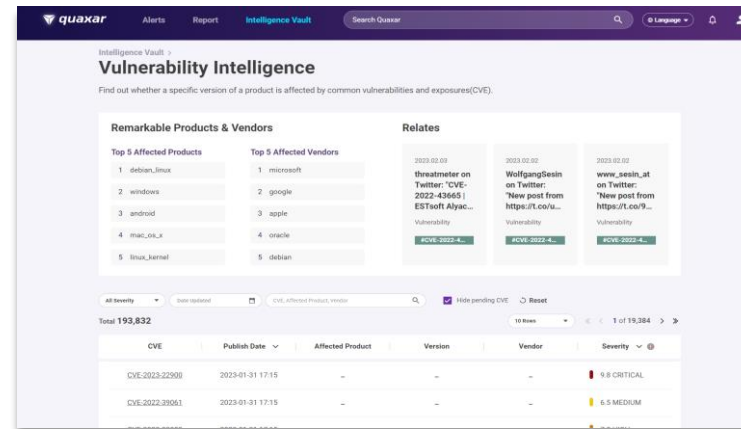
2 With Quaxar, 다양한 위협에 능동적인 대응이 가능!

주요 기능



공격 표면 자동 탐지 (ASM)

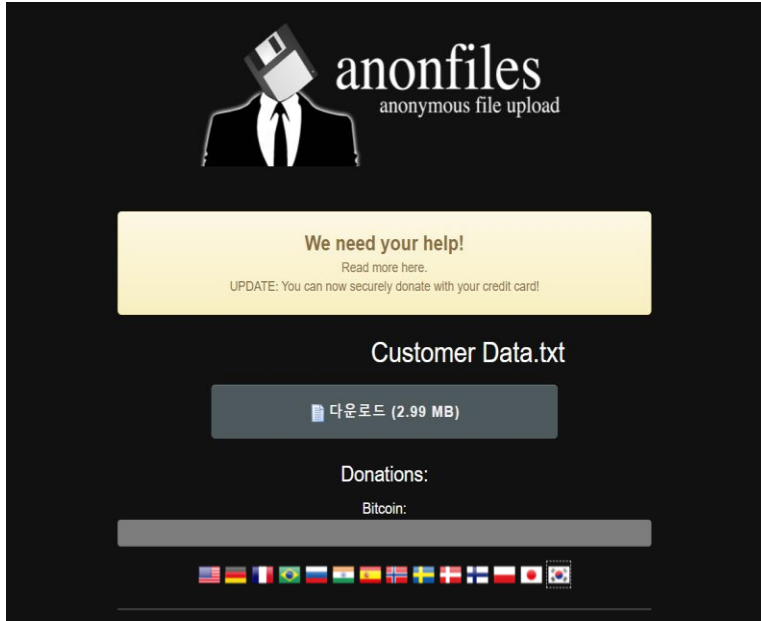
기업의 공격 표면을 주기적으로 모니터링 합니다.
내부 통제를 벗어난 기업 내부 인프라, 자산 등의
정보 노출을 관리합니다.



취약점 정보

취약점 정보 검색에 따른 정보를 체계적으로 제공 합니다.
제품의 특정 버전이 공개적으로 알려진 소프트웨어의
보안취약점 (CVE)의 영향을 받는지 확인할 수 있습니다.

2 Inside Quaxar – ATOM (계정유출모니터링 서비스)



Ransomware에 감염되어 유출된 고객 정보



임직원의 검색기록, 히스토리 및 저장된 패스워드

2 Inside Quaxar – ATOM (계정유출모니터링 서비스)

클라우드 벤더 계정 정보 유출

Challenge

클라우드 서비스 벤더 기업 A의 임직원 계정이 유출되어 기업A의 고객사와 고객사 관련 자산 정보 유출된 사례. 기업A는 임직원 계정 유출 상황을 인지하지 못하고 있는 상태.

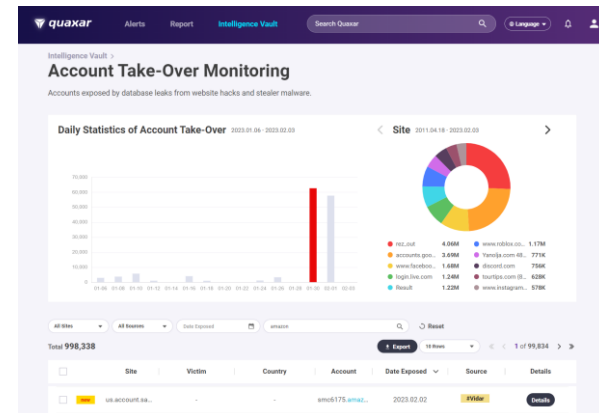
Action

ATOM은 S2W 고객사의 임직원 계정 정보가 외부로 유출된 정황 탐지. 사고 조사 결과 고객사가 이용중인 클라우드 서비스 벤더 기업A의 임직원 계정 정보가 유출되면서 발생한 사고임을 파악. 해당 계정 유출 사고는 당사의 고객사 뿐만 아니라 기업A의 다른 고객사들의 클라우드 인프라 정보가 유출된 심각한 상황.

S2W는 ATOM을 통해 스틸러 로그를 탐지, 해당 유출 계정이 어떤 스틸러에 감염되었는지 분석.

Benefit

ATOM을 통해 기업 클라우드 인프라 정보 유출 사고 파악 가능. ATOM의 스틸러 로그 모니터링은 임직원 감염 현황을 확인하고 기업에서 사용하는 Third Party 서비스나 협력사 직원의 감염으로 인한 유출 정보도 모니터링.



2 Inside Quaxar – ASM (공격표면관리 서비스)

Exposed Attack Surface



개발자 페이지 및
개발망 서브도메인



각종 퍼블릭 액세스 서비스들

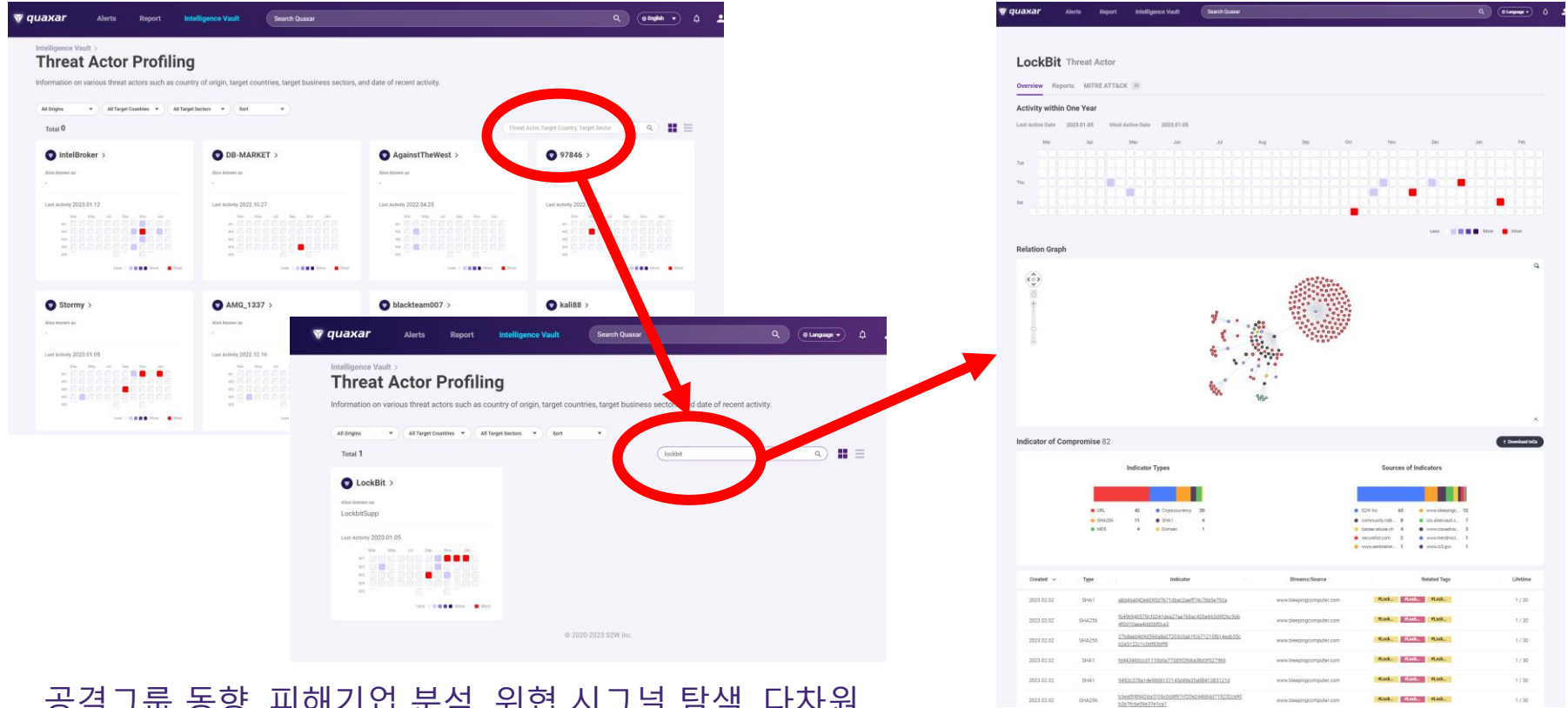


CI/CD 및 컨테이너 플랫폼

2 Inside Quaxar – Threat Actor Profiling (위협그룹 프로파일링)



2 Inside Quaxar – Threat Actor Profiling (위협그룹 프로파일링)



공격그룹 동향, 피해기업 분석, 위협 시그널 탐색, 다차원
관계분석 등을 통한 외부 위협 사전 예측

3 필요 시 분석가 지원이 잘 되는가?

사이버 위협 인텔리전스 콘텐츠

Malware	랜섬웨어, 스틸러, 봇넷, 백도어, 원격제어형 ...
Vulnerability	각종 취약점 정보 (Spring4shell, Log4shell, Dirty-Pipe, Proxysql) ...
Incidents	LAPSUS\$, Gwisin, BGP 하이재킹, 월패드 이슈 ...
Data Breach	딥웹 포럼, 다크웹 기반 유출 사이트, 소셜 미디어, 텔레그램, 표면웹 상에 노출된 민감 정보 ...
Threat Actor	국가 배후 공격 그룹, 사이버 범죄 조직, 딥/다크웹 포럼 사용자 ...
Abusing	유사 도메인, 정상 서비스/명령어를 악용한 공격(Living-Off-the-Land Attacks) ...

3 필요 시 분석가 지원이 잘 되는가?

사이버 위협 인텔리전스 콘텐츠 : S2W Original & Exclusive

Malware	랜섬웨어, 스틸러, 봇넷, 백도어, 원격제어형 ...
Vulnerability	각종 취약점 정보 (Spring4shell, Log4shell, Dirty-Pipe, Proxyshell) ...
Incidents	LAPSUS\$, Gwisin, BGP 하이재킹, 월패드 이슈 ...
Data Breach	딥웹 포럼, 다크웹 기반 유출 사이트, 소셜 미디어, 텔레그램, 표면웹 상에 노출된 민감 정보 ...
Threat Actor	국가 배후 공격 그룹, 사이버 범죄 조직, 딥/다크웹 포럼 사용자 ...
Abusing	유사 도메인, 정상 서비스/명령어를 악용한 공격(Living-Off-the-Land Attacks) ...
S2W	TALON REPORT (악성코드, 취약점, 위협그룹, 민감정보 유출 및 내부 자산 노출 정보 ...), Professional Service (침해사고 조사, 악의적인 콘텐츠에 대한 차단 [Take-Down] ...), S2Gether (커뮤니티), Active Intelligence (주요 악성코드 및 위협그룹 추적/조사, 연관성 분석 및 그래프 제공, 광범위한 채널 커버 ...) Exclusive Intelligence (유효성이 높은 고객사 맞춤형 위협 정보 – 평균 80% 이상)


3 필요 시 분석가 지원이 잘 되는가?

사이버 위협 인텔리전스 콘텐츠 : **S2W Original & Exclusive**

S2Gether

RFI

3 필요 시 분석가 지원이 잘 되는가? 세계적 수준의 분석가 그룹이 꼼꼼히 지원



INTERPOL

Cyclone 작전 | Clop 랜섬웨어 검거 작전

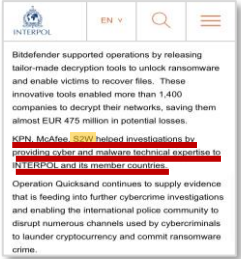

- 원점 추적 위한 Clop 관련 인프라 정보 분석
- Clop 랜섬웨어 비트코인 자금흐름 분석
- 다크웹 내 Clop 랜섬웨어 오퍼레이터들의 활동 분석 및 프로파일링

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)



국기정보원

국정원, 민간 공동대응 '국가사이버안보협력센터' 문

A. 장민규 기자 · 2022.11.30 18:10 · 2022.12.01 07:32 · 0 댓글

사이버위협에 맞서 국정원, 유관기관 및 IT보안업체 소통 창구 마련



Digital Today

30일 국가사이버안보협력센터 개소식에서 참석자들이 대사로 환영사를 하고 있다. 박종욱 국정원 3차장 (왼쪽 네번째부터), 이종호 과학기술정보통신부 장관, 임규민 국정원장, 조해진 국회 정보위원회, 유상범 국회 정보위 간사 등이 기념촬영하고 있다. [사진: 국정원]

[디지털투데이 강진규 기자] 국가정보원과 민간이 함께 사이버위협 정보 기술을 공유하고 공동 대응하기 위한 협력센터가 문을 열었다.

국가정보원은 30일 경기도 안국 제2테크노밸리에서 강진규 국가정보원장, 조해진 국회 정보위원장, 유상범 정보위 간사, 이종호 과기정통부 장관, 이종범 정보보호산업협회장, IT업계 대표 등 정보보안업계 관계자들이 참석한 가운데 '국가사이버안보협력센터' 개소식을 개최했다.

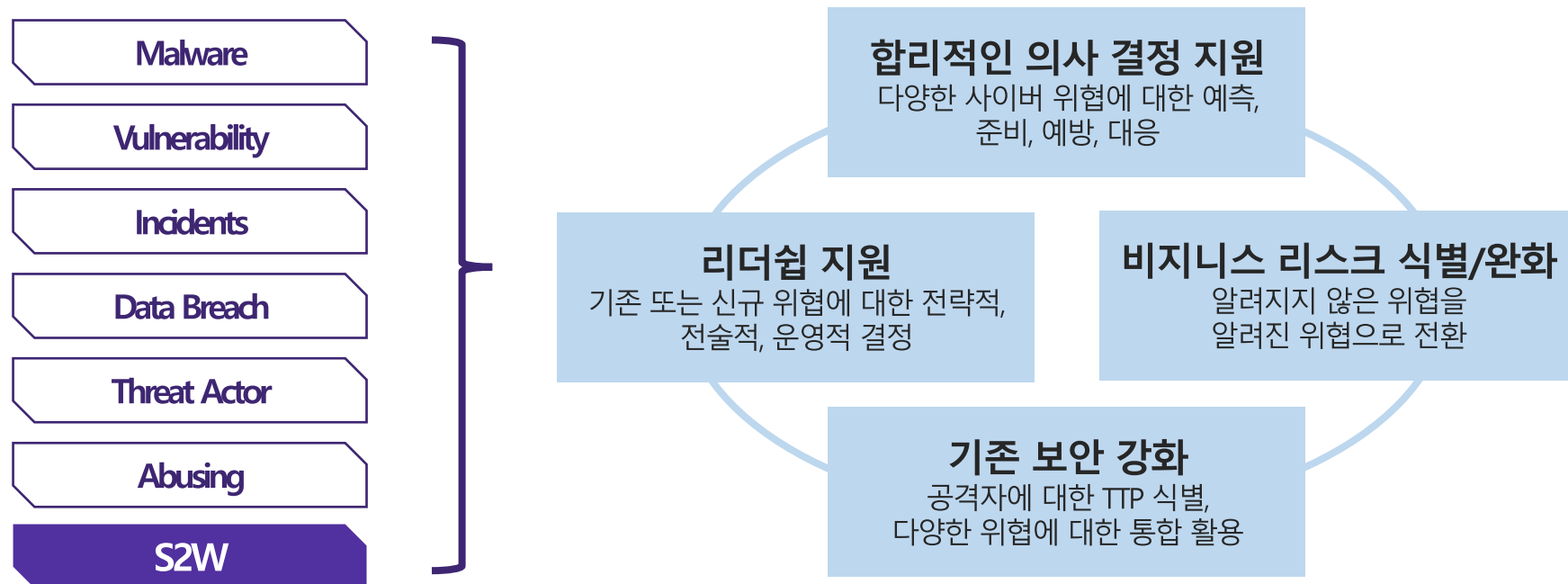
사이버안보협력센터는 국정원 국가사이버안보센터가 기술력, 고도화되고 있는 사이버공격에 맞서 민관이 힘을 합쳐 공동 대응하기 위해 개소했다.

센터에는 국정원 과학기술정보통신부 국방부 등 유관기관과 안랩, 이스트시큐리티, S2W, 체이널리시스 등 IT보안업체 전문 인력들이 함께 근무한다.

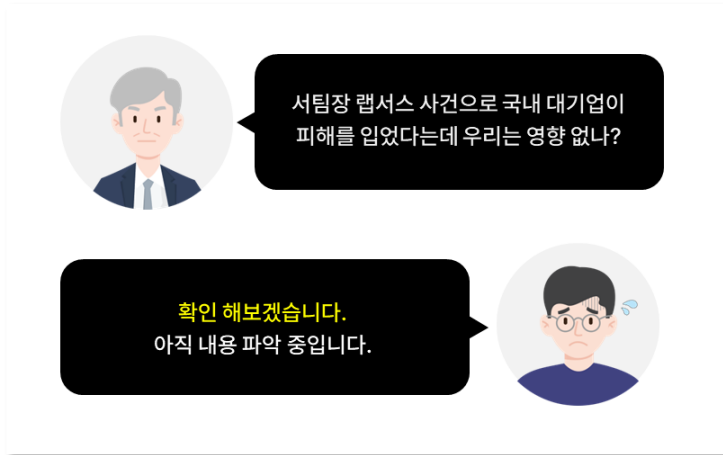
국정원, 과학기술정보통신부, 국방부 등 유관기관
과 안랩, 이스트시큐리티, S2W, 체이널리시스 등
IT 보안업체 전문 인력들이 함께 근무한다.

3 필요 시 분석가 지원이 잘 되는가?

사이버 위협 인텔리전스 콘텐츠 : S2W Original & Exclusive

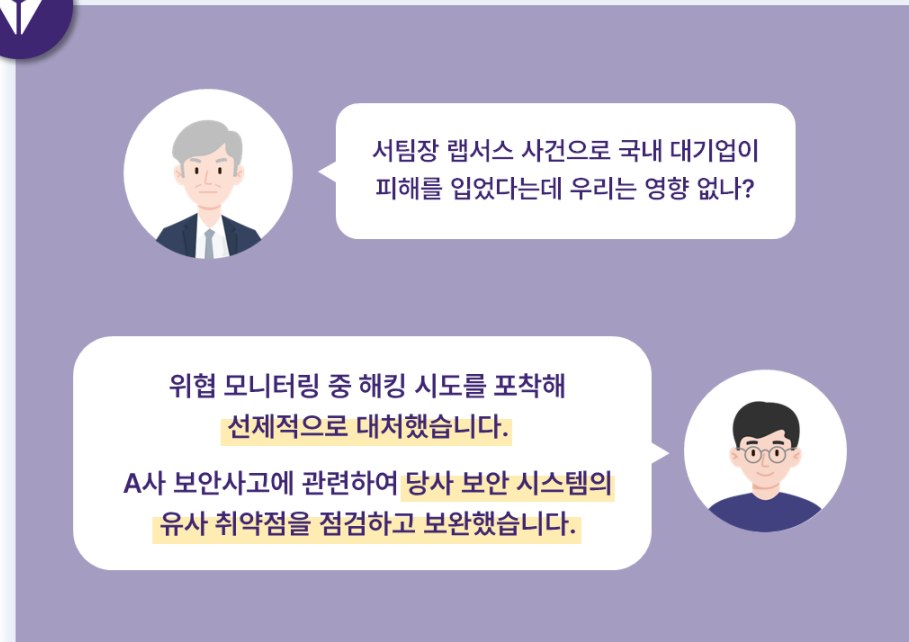


“확인 해보겠습니다”



서팀장 랩서스 사건으로 국내 대기업이 피해를 입었다는데 우리는 영향 없나?

확인 해보겠습니다.
아직 내용 파악 중입니다.



서팀장 랩서스 사건으로 국내 대기업이 피해를 입었다는데 우리는 영향 없나?

위협 모니터링 중 해킹 시도를 포착해
선제적으로 대처했습니다.
A사 보안사고에 관련하여 당사 보안 시스템의
유사 취약점을 점검하고 보완했습니다.

Beyond Security, Quaxar

Beyond Security

기업의 핵심 자산 보호를 넘어
지속적인 성장을 위한 비즈니스
의사 결정에 도움을 줍니다.

Tailored Intelligence

기업의 최적화된 운영 환경을
위해 세밀하게 고안된
맞춤형 인텔리전스를 제공합니다.

Reframing Threat ResPonse Process

위협 대응 프로세스에 Quaxar를
접목해 보다 신속하고 효과적인
위협 대응이 가능합니다.



Discover more about S2W and our solutions

Please contact us through the email below.

info@s2w.inc

www.s2w.inc | +82 07 5066 5277

12, Pangoyeok-ro 192beon-gil #03, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.