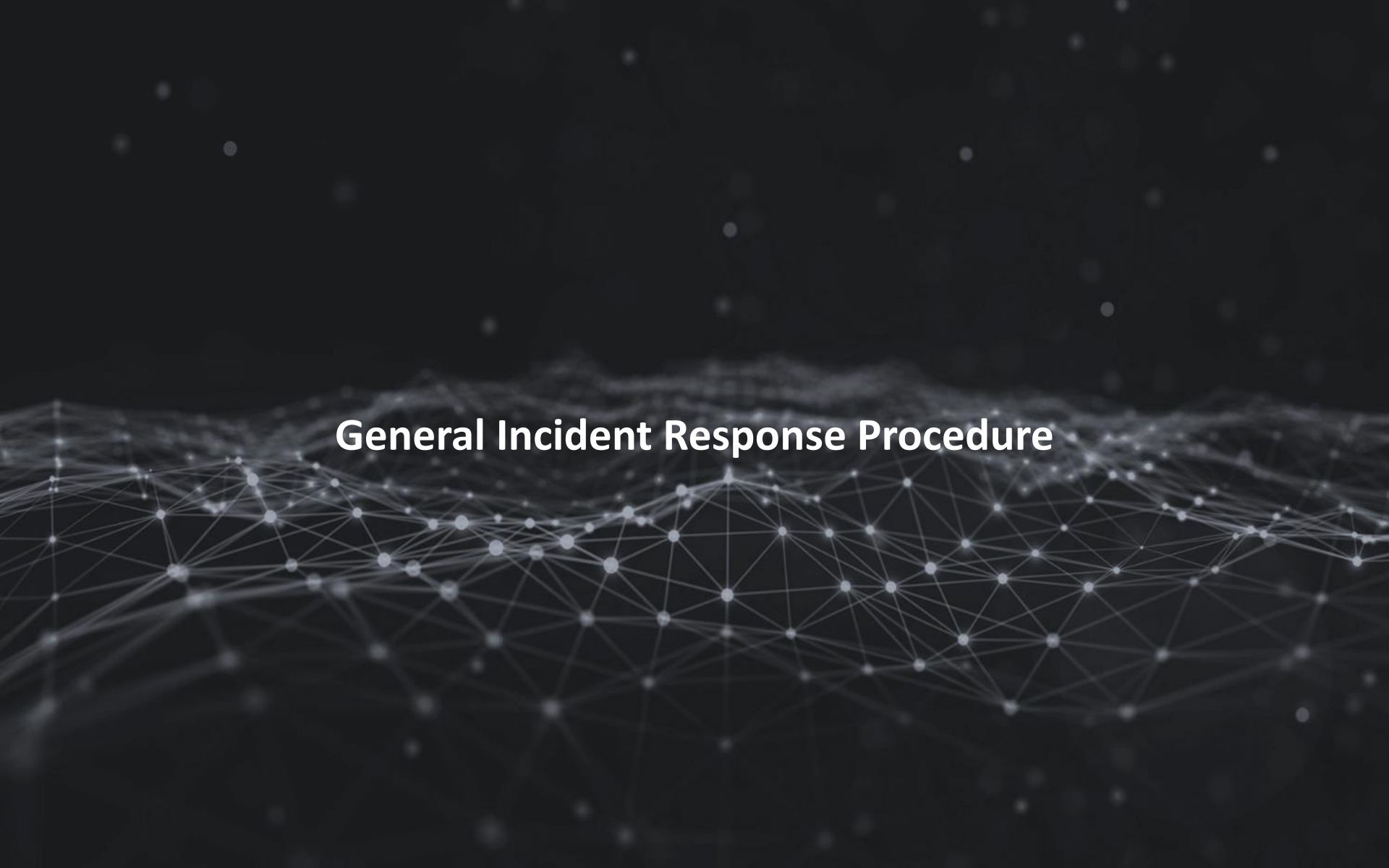
2023

S2W
Safe and Secure World

클라우드 기반 시스템 해킹 사례 분석:
침해사고 대응 방안과 조사 영역 확대

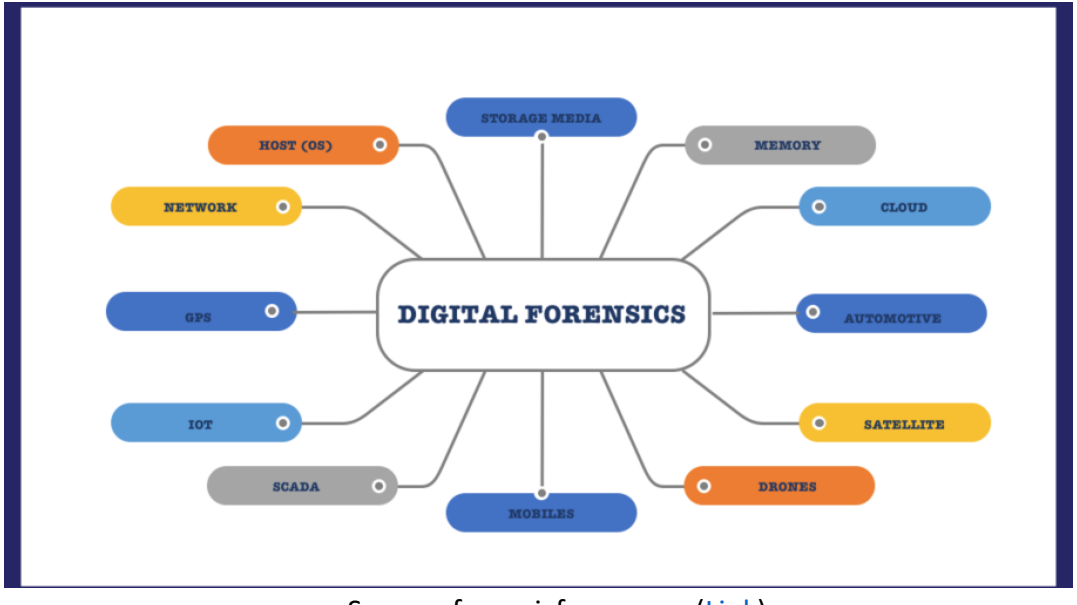
Jungyeon Lim, Threat Detection Team
Team Leader
(jungyunl@s2w.inc)
@S2W TALON


General Incident Response Procedure

General Incident Response Procedure

Incident Response

- **기존 침해사고 조사 범위는 사고를 당한 대상의 내부 인프라에 분석 초점이 맞춰져 있음**
- **내부 Artifacts들을 통해 외부로 시간을 올라가면서 TimeLine 분석**
  - OS Artifacts
  - Network / System Logs
  - Malware Analysis
  - TimeLine Analysis



Source: forensicfocus.com (Link)

General Incident Response Procedure

Incident Response

- **기존 분석 범위 한계점**
  - 공격자가 내부망 침투 후 데이터를 탈취, 삭제, 랜섬웨어 암호화 등 수행한 이력은 식별 가능
  - **But. 공격자가 언제(When), 어디서(Where), 어떻게(How) 침투했는지 정확히 식별하기 어려움**
    - 제일 처음 공격자가 침투한 서버? PC?는 **어디인가**
    - **언제부터** 접근했었는가
    - **어떤 단계**를 거쳐 내부망까지 성공적으로 접근했는가
  - 분석 대상 서버 / PC / Logs 들이 너무 많다
  - 사건 발생 후 시간이 경과했을 경우 휘발된 or 공격자가 삭제한 포렌식 Artifacts
  - 분석 과정에서 식별한 여러 취약 포인트들 중 어떤 곳을 통해 공격자가 들어왔는가?
  - 공격자가 어디서 침투했는지 도저히 모르겠는 경우

General Incident Response Procedure

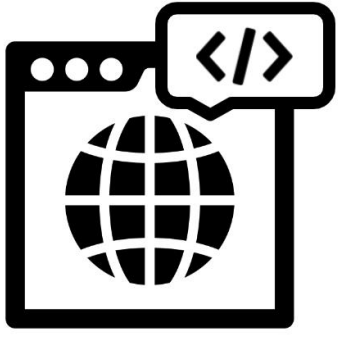
Incident Response

- **피해기업 내부의 정보만으로 공격자의 초기 침투 방법과 전체 과정을 분석하기는 어려움**
- 클라우드 기반 시스템 해킹 사례 등 분석을 통해 침해사고 조사 영역 확대 필요성 확인
  - 유의미한 정보는 오히려 외부에서 내부로 접근하는 관점으로 찾을 수 있는 케이스가 많다
- **공격자의 관점에서 생각해보기**
  - 공격자는 타겟으로 삼은 특정 기업의 취약한 서버, 데이터베이스 등을 어떻게 찾는가?
  - 공격자는 탈취한 데이터를 어떻게 할 것인가? 판매 or 유출?
- **Incident Response with ASM, DDW OSINT, Cloud Analysis**

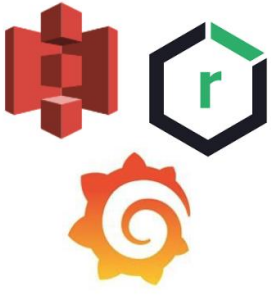
General Incident Response Procedure

What is ASM (Attack Surface Monitoring)

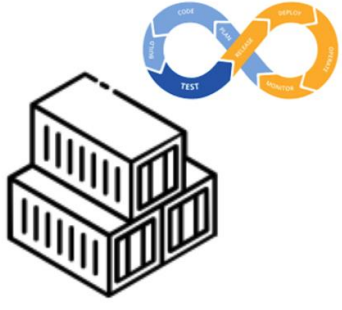
- 기업 내부 자산이 외부에 노출된 현황을 모니터링하고 위협 탐지
- 내부 서버, 클라우드 인프라, 민감 서비스 등의 외부 노출로 인한 피해 방지



개발자 페이지 및 개발망 서브도메인



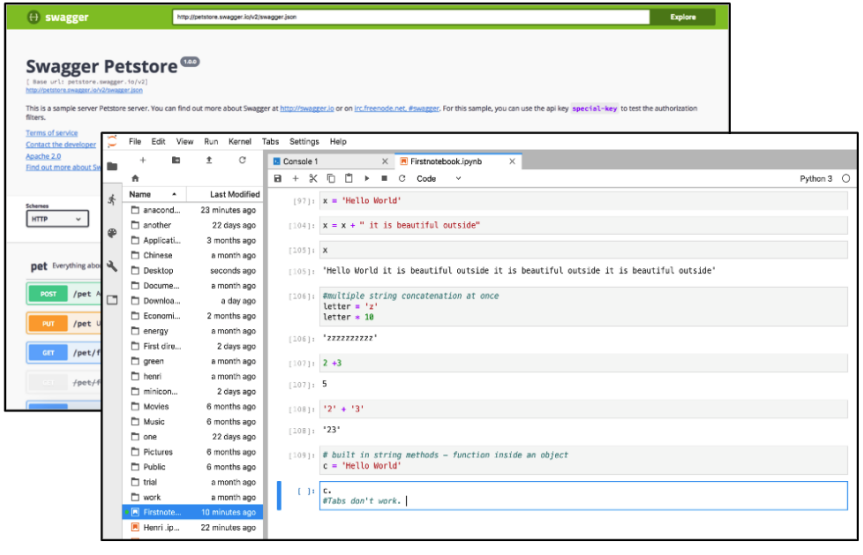
각종 퍼블릭 액세스 서비스들



CI/CD 및 컨테이너 플랫폼

General Incident Response Procedure

What is ASM (Attack Surface Monitoring)



개발자 편의 및 테스트 페이지

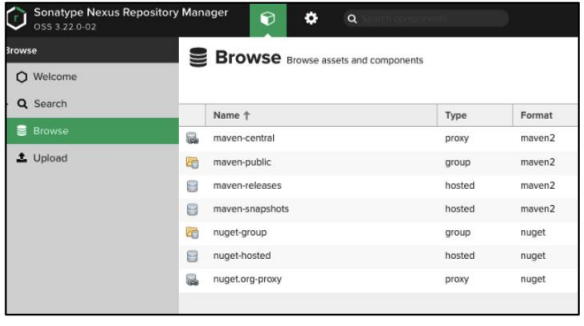
dev-*.domainA.com
test-*.domainB.com

개발망 및 테스트 도메인

General Incident Response Procedure

What is ASM (Attack Surface Monitoring)

퍼블릭 액세스 스토리지

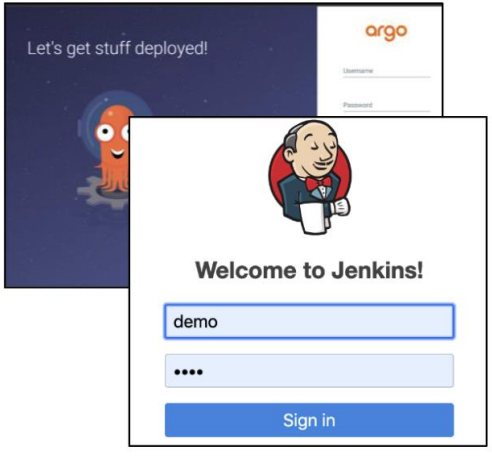


각종 리포지토리, 아티팩토리

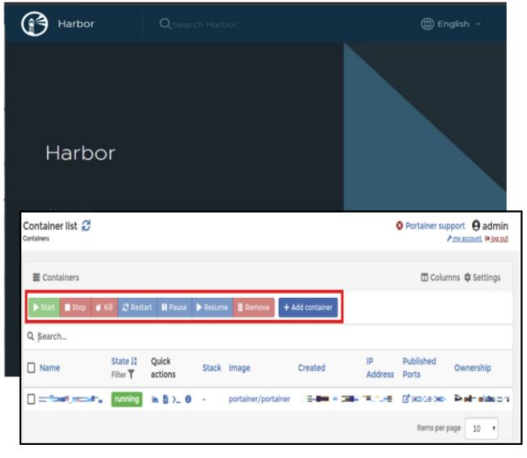
메트릭, 모니터링 페이지

General Incident Response Procedure

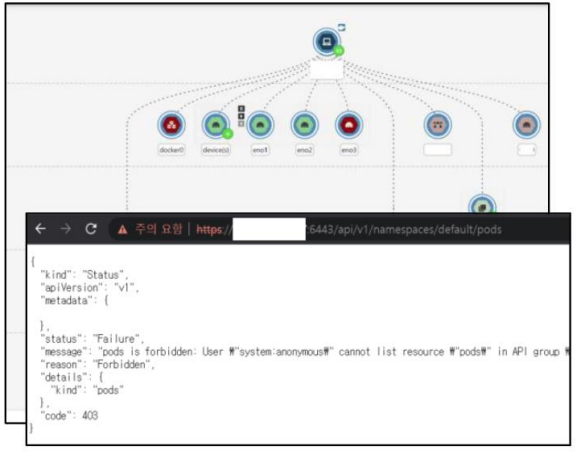
What is ASM (Attack Surface Monitoring)



외부노출 CI/CD 서비스들



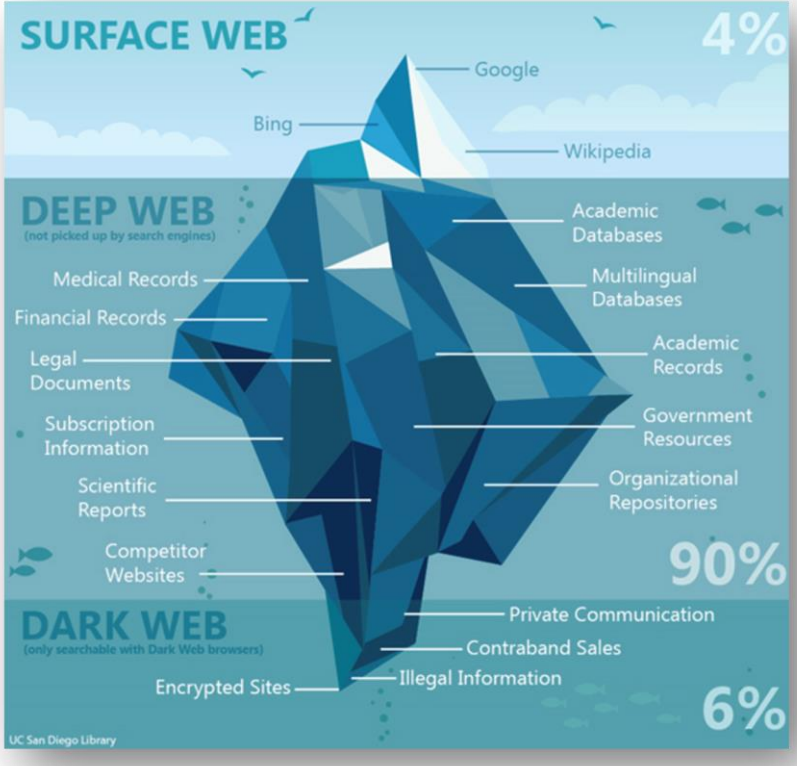
컨테이너 레지스트리, 매니저



쿠버네티스 연관 서비스

General Incident Response Procedure

What is DDW (Deep & Dark Web)



Cocaine

4 scariest videos on youtube #darkweb #deepweb

139 views • 1 day ago

Antihell

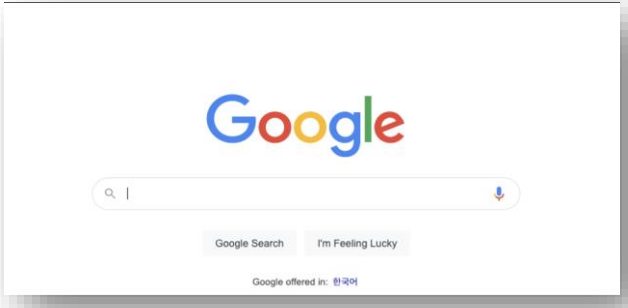
_Scariest videos on YouTube_* #deepweb #darkweb #creepy #scary.

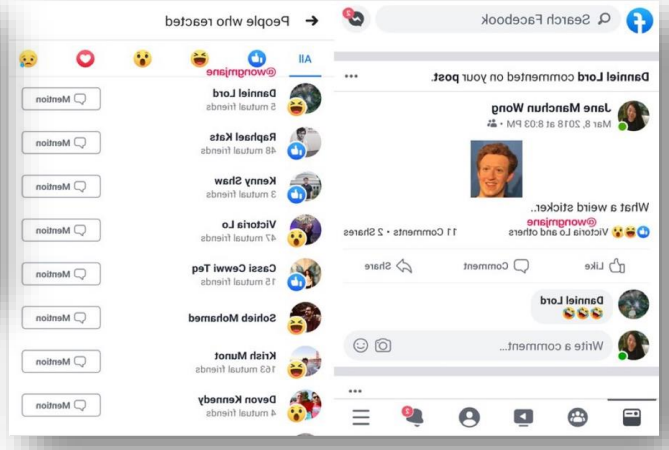
New

General Incident Response Procedure

What is DDW (Deep & Dark Web)

- 표면웹 (Surface Web): 일반 네트워크에서 접근 가능한 웹 사이트 혹은 웹 페이지

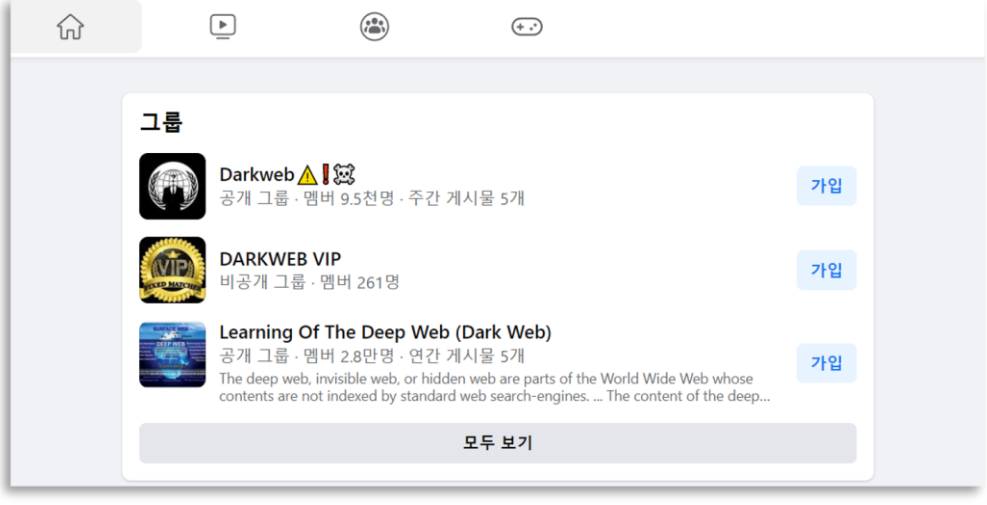


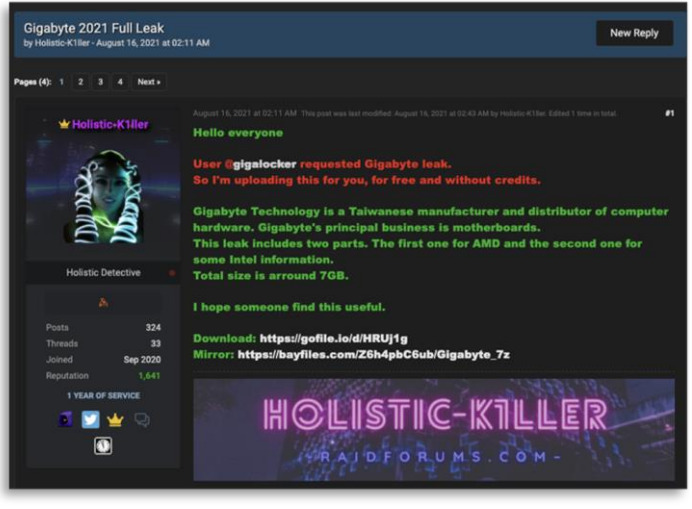


General Incident Response Procedure

What is DDW (Deep & Dark Web)

- 딥웹 (Deep Web): 일반 네트워크에서 접근 가능하지만 일반인이 검색 엔진을 통해 접근하지 못하는 웹 사이트 혹은 웹 페이지

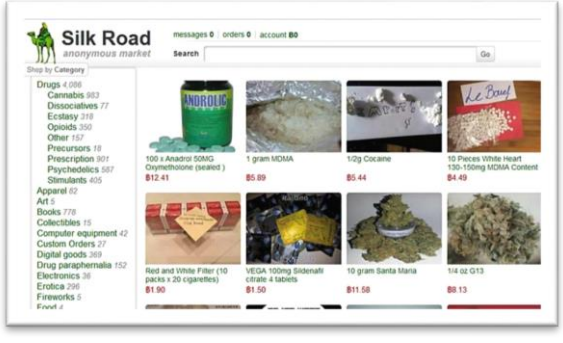




General Incident Response Procedure

What is DDW (Deep & Dark Web)

- 다크웹 (Darkweb): 검색 엔진에 의해 인덱싱되지 않고 Tor와 같은 특수 소프트웨어를 통해서만 액세스할 수 있는 웹 사이트나 웹 페이지를 의미함
- **공격자(Hacker)들은 DDW에서 활동을 많이 함**
  - 공격을 위한 정보 습득
  - 공격을 위한 Initial Access 구매 / 판매
  - 탈취한 데이터 판매 / 구매
  - 랜섬웨어 유출 데이터 공개 / 판매



Case 1: CloudDon,
Cloud Data Breach of Korea e-commerce company

CloudDon, Cloud Data Breach of Korea e-commerce company

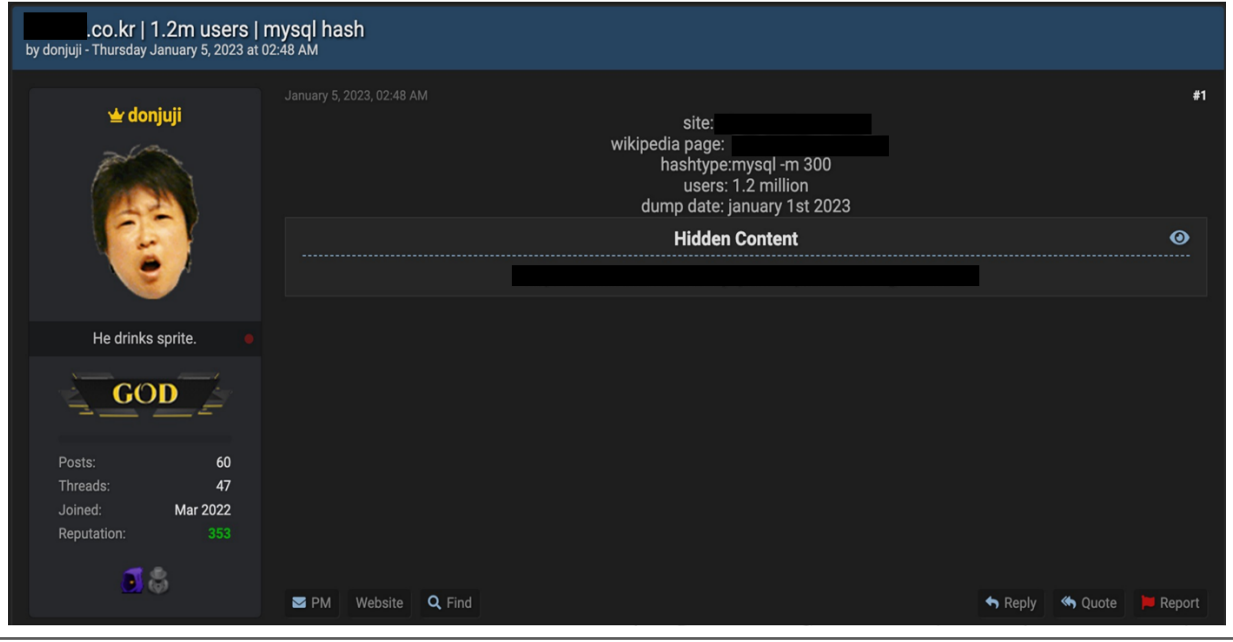
Overview

- 다크웹에서 'Donjuji' ID를 사용하는 공격자의 클라우드 인프라 공격인 점에서 Operation name을 "CloudDon"으로 명명
- 2023년 1월 경 Breached 포럼의 donjuji 유저가 온라인 쇼핑몰 A사의 회원 정보 판매 게시글을 업로드 하였고, 정확한 유출 경위 파악을 위해 피해기업의 침해사고 분석을 진행함
- 판매 게시글이 업로드 되기 전까지는 해킹 사실을 인지하지 못함

CloudDon, Cloud Data Breach of Korea e-commerce company

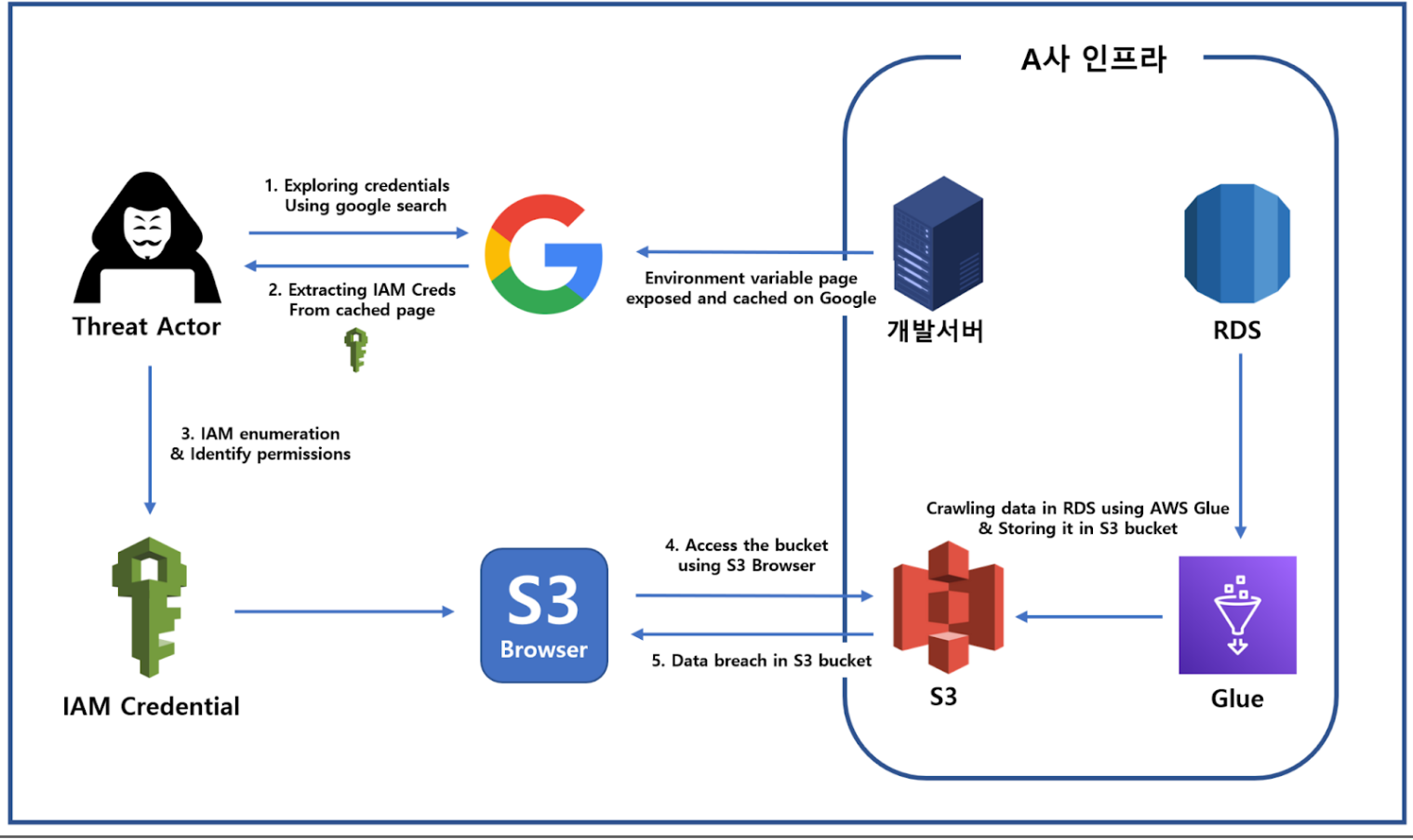
Operation name: CloudDon

- (2023-01-05) Breached 포럼에서 donjuji 유저가 "xxxx.co[.]kr|1.2m users|mysql hash" 제목의 게시글을 업로드
- 국내 쇼핑몰 A 기업의 회원 정보를 판매
- 유출 항목은 이메일 주소와 암호화된 비밀번호 - 총 1,183,323건의 회원들의 계정 정보 유출



CloudDon, Cloud Data Breach of Korea e-commerce company

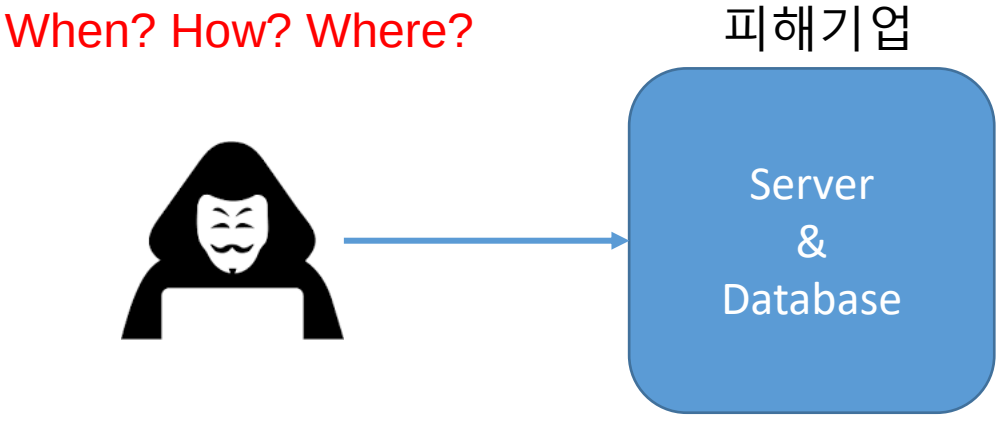
Incident Response Flow



CloudDon, Cloud Data Breach of Korea e-commerce company

Reconnaissance

- 공격자는 어떻게 피해기업 내부 서버, 데이터베이스에 접근했는가?
- 피해기업은 물리서버 없이 AWS Cloud 서비스를 통해 서버들을 운영 중
- Cloudtrail 로그 상 별다른 공격 정황이 확인되지 않음
  - 비인가 로그인 성공 이력 ?
  - 로그인 실패 이력?
  - Brute Force?
  - Injection?



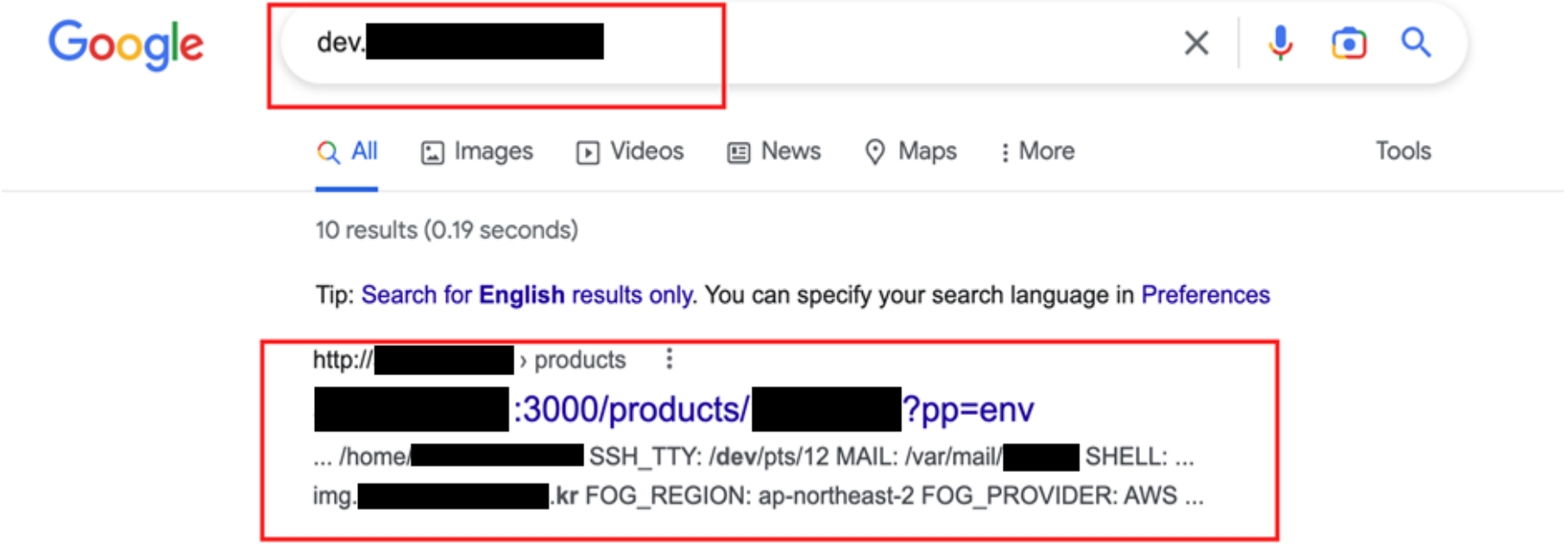
CloudDon, Cloud Data Breach of Korea e-commerce company

Reconnaissance

- 공격자는 어떻게 피해기업 내부 서버, 데이터베이스에 접근했는가?
- 접근 방식을 바꿔보자 -> 공격자의 ASM, DDW OSINT 관점으로 조사 시작

ASM (Attack Surface Monitoring)

- ASM 분석 과정에서 **피해기업의 개발서버 페이지가 외부에 노출되어 구글에서 검색을 통해 식별 가능한 것이 확인됨**



CloudDon, Cloud Data Breach of Korea e-commerce company

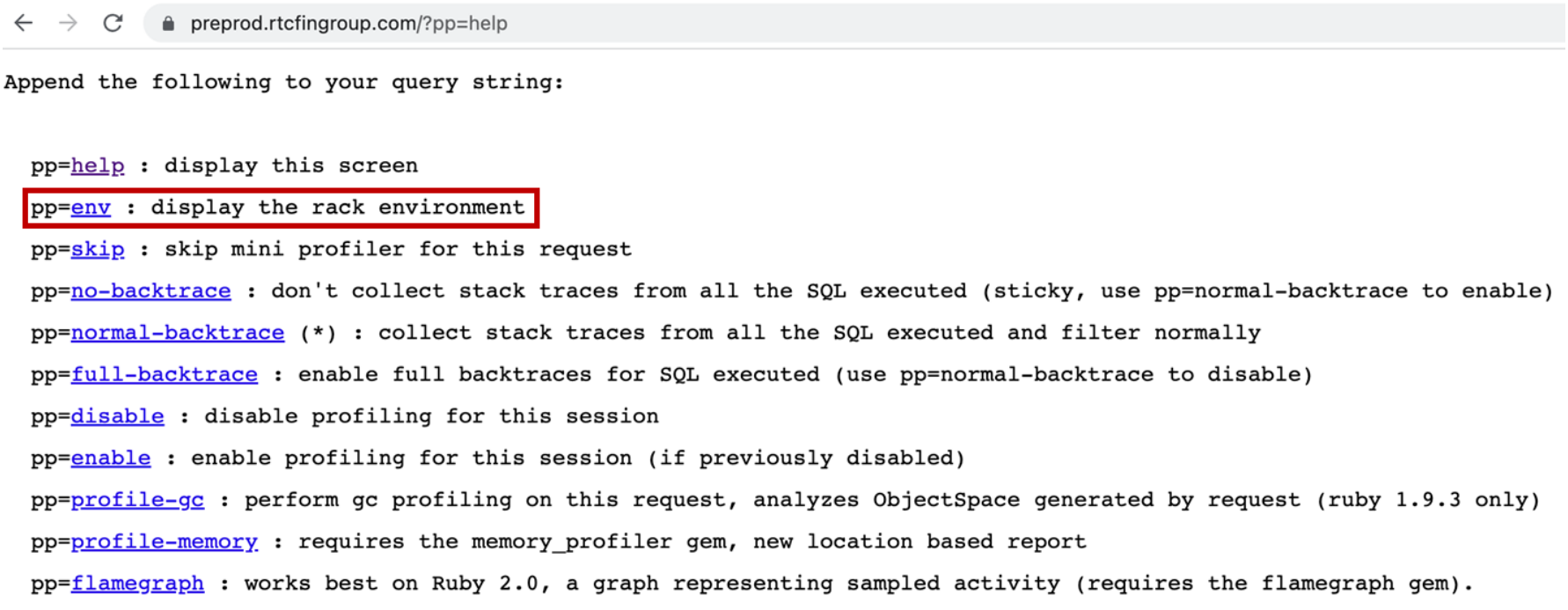
ASM (Attack Surface Monitoring)

- 노출된 페이지는 **개발서버의 환경변수 페이지**
- **하드코딩된 AWS IAM User 크리덴셜**, NAVER, KAKAO 등에 접근 가능한 다수의 인증정보가 존재
- **공격자는 해당 AWS IAM User 크리덴셜을 통해 피해기업의 AWS 서비스에 접근 성공**

```
GEM_PATH: /home/[redacted]/.rbenv/versions/2.6.5/lib/ruby/gems/2.6.0:/home/[redacted]/.gem/ruby/2.6.0
GEM_HOME: /home/[redacted]/.rbenv/versions/2.6.5/lib/ruby/gems/2.6.0
MANPATH: /home/[redacted]/.rbenv/versions/2.6.5/lib/ruby/gems/2.6.0/gems/unicorn-6.0.0/man
RAILS_ENV: development
AWS_ACCESS_KEY_ID: AKIA[redacted]
AWS_SECRET_ACCESS_KEY: [redacted]
FOG_DIRECTORY: img.[redacted].kr
FOG_REGION: ap-northeast-2
FOG_PROVIDER: AWS
OMNIAUTH_FB_APP_ID: [redacted]
OMNIAUTH_FB_APP_SECRET: [redacted]
OMNIAUTH_NAVER_APP_ID: [redacted]
OMNIAUTH_NAVER_APP_SECRET: [redacted]
OMNIAUTH_KAKAO_CLIENT_ID: [redacted]
```

ASM (Attack Surface Monitoring)

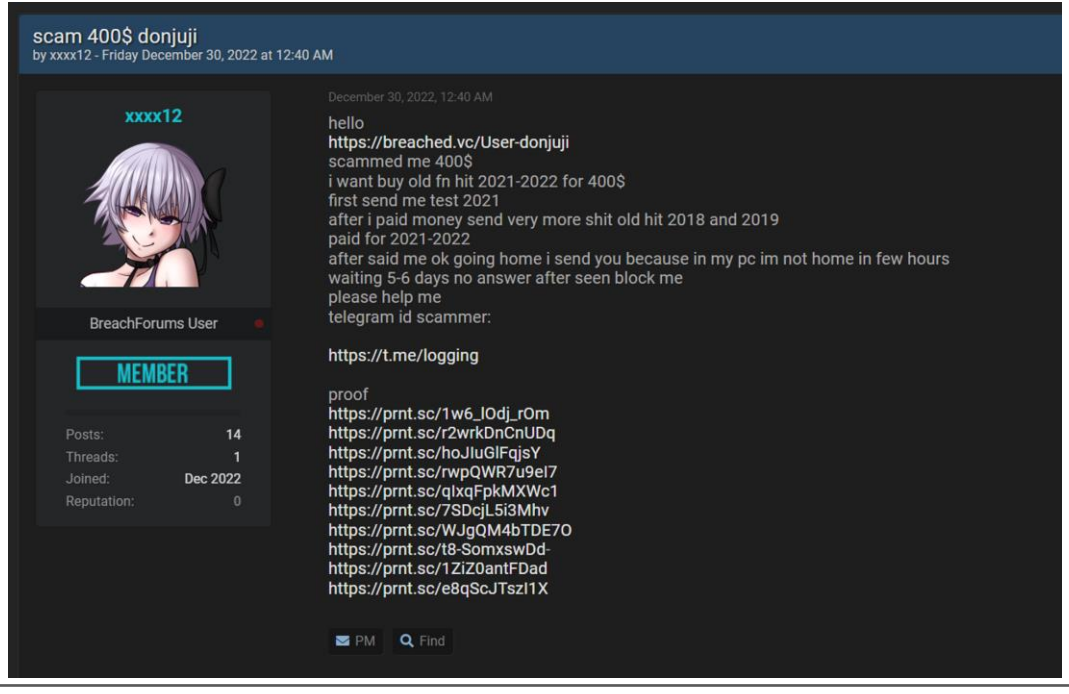
- 인프라 내 개발서버 **외부 노출 및 Ruby기반 Middleware의 라이브러리인 Mini-profiler의 잘못된 구성으로 인한 pp 파라미터 활성화가 주요 원인**이며 이 중 **pp=env 값인 환경변수 페이지가 노출**



CloudDon, Cloud Data Breach of Korea e-commerce company

DDW OSINT (Deep & Dark Web OSINT)

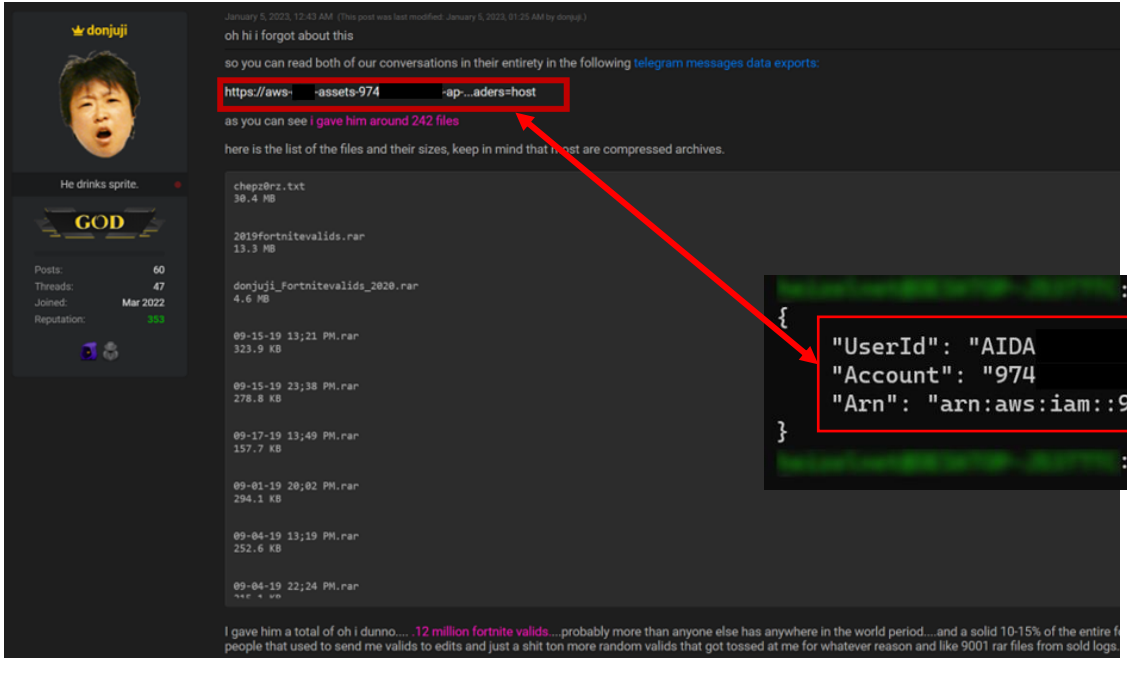
- 피해기업의 데이터를 판매했던 "donjuiji" 유저가 외부에 노출된 AWS IAM 크리덴셜을 통해 피해기업 내부망에 접근한 것이 맞을까? 직접 탈취한 것이 맞을까?
- 분석 중, "donjuji" 유저를 향한 400 $ 먹튀 스캠 신고 이력이 확인됨



CloudDon, Cloud Data Breach of Korea e-commerce company

DDW OSINT (Deep & Dark Web OSINT)

- "donjuji"는 피해기업의 데이터 판매글을 작성하기 2시간 전, 자신에 대한 scam 신고에 대응하기 위해 **스캠 신고자와 대화를 나누었던 텔레그램 스크린샷 등 증빙 파일을 피해기업의 AWS S3에 업로드** 함
- **노출된 IAM User 크리덴셜의 account-id와 donjuji가 업로드한 S3 URL 내 account-id가 일치**



CloudDon, Cloud Data Breach of Korea e-commerce company

DDW OSINT (Deep & Dark Web OSINT)

- Cloudtrail 로그를 통해 2022년 12월 경부터 탈취한 크리덴셜을 이용하여 여러 서비스에 접근 시도하는 **IAM Enumeration** 작업 진행

2022-12-[redacted]	s3.amazonaws.com	GetBucketAcl	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2
2022-12-[redacted]	cognito-idp.amazonaws.com	Error_GET	ap-northeast-2

DDW OSINT (Deep & Dark Web OSINT)

- 식별된 정보를 바탕으로 2023년 1월경 S3 Browser를 사용하여 S3 Transfer Acceleration 옵션 활성화, 버킷 목록 탐색 및 데이터 탈취를 진행
- 이후 탈취한 데이터를 Breached 포럼에서 판매

2023-01-[redacted]	s3.amazonaws.com	GetBucketObjectLockConfiguration	ap-northeast-2	[S3 Browser/10.5.9 (https://s3 ObjectLockCor
2023-01-[redacted]	s3.amazonaws.com	GetAccelerateConfiguration	ap-northeast-2	[S3 Browser/10.5.9 (https://s3browser.com)]
2023-01-[redacted]	s3.amazonaws.com	GetAccelerateConfiguration	ap-northeast-2	[S3 Browser/10.5.9 (https://s3browser.com)]
2023-01-[redacted]	s3.amazonaws.com	GetAccelerateConfiguration	ap-northeast-2	[S3 Browser/10.5.9 (https://s3browser.com)]
2023-01-[redacted]	s3.amazonaws.com	GetAccelerateConfiguration	ap-northeast-2	[S3 Browser/10.5.9 (https://s3browser.com)]

Conclusion

- "donjuji" 유저는 노출된 IAM 크리덴셜(S3FullAccess, RDSFullAccess)과 버킷 정보를 사용하여 S3 Explorer 프로그램을 통해 접근 가능한 데이터를 탐색 후 민감정보를 탈취
- 주요 보안 검토 필요 및 위험요소 항목
  - IAM 크리덴셜 권한 과부여(S3FullAccess, RDSFullAcess) 및 IP range 미적용
  - IAM 크리덴셜 MFA 이용한 세션 토큰 미적용
  - S3 버킷 KMS(Key Management System) 이용한 암호화 미적용
  - S3 버킷 Object Lock 미적용

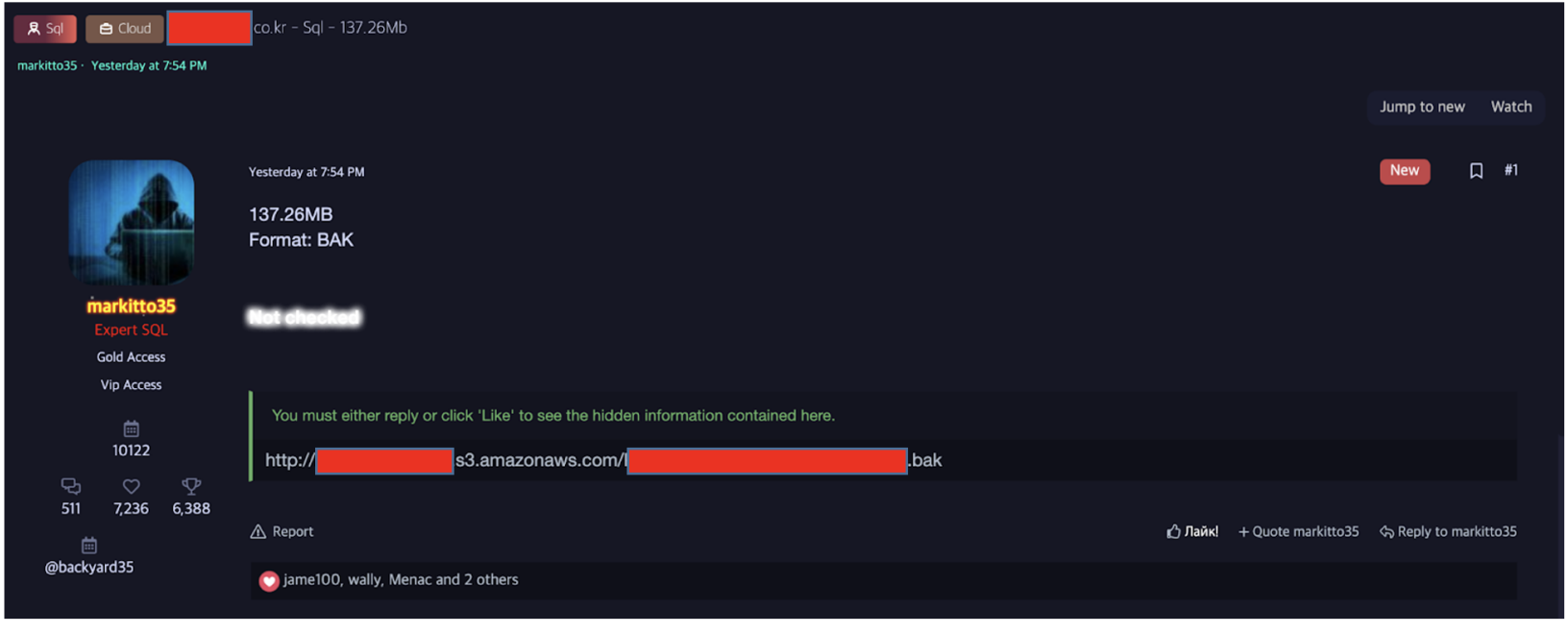
Num	IP	Country	Description
1	**71.202.232.31**	California(USA)	S3 Browser 를 사용한 외부 접근
2	**157.97.121.215**	New Jersey(USA)	S3 Browser 를 사용한 외부 접근
3	**159.203.143.99**	New Jersey(USA)	Cognito 서비스 접근 시도
4	**167.172.20.150**	New Jersey(USA)	Cognito 서비스 접근 시도
5	**182.3.41.124**	Jakarta(Indonesia)	security-group 백도어 설치 시도

Case 2: SQL Backup Data Breach of Korea insurance company

SQL Backup Data Breach of Korea insurance company

Overview

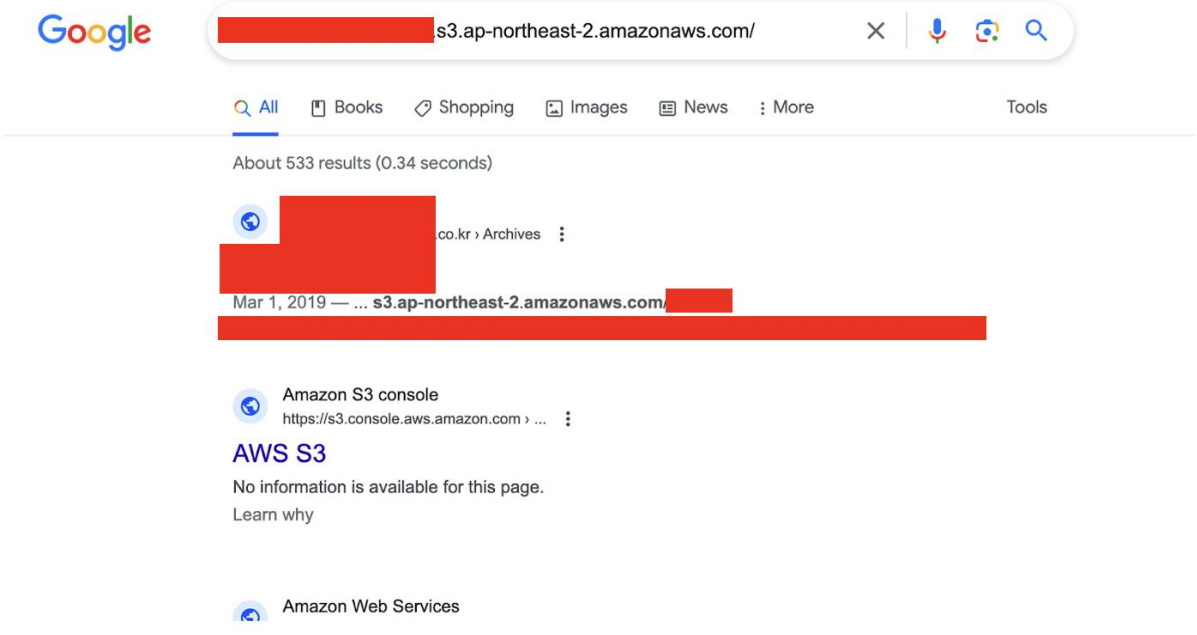
- 2023년 11월 한국 보험회사의 SQL Backup 데이터가 DDW에 유출됨
- Backup 파일만 유출된 것이 아닌 다운로드 가능한 정확한 AWS S3 URL 형태로 공개됨



SQL Backup Data Breach of Korea insurance company

ASM (Attack Surface Monitoring)

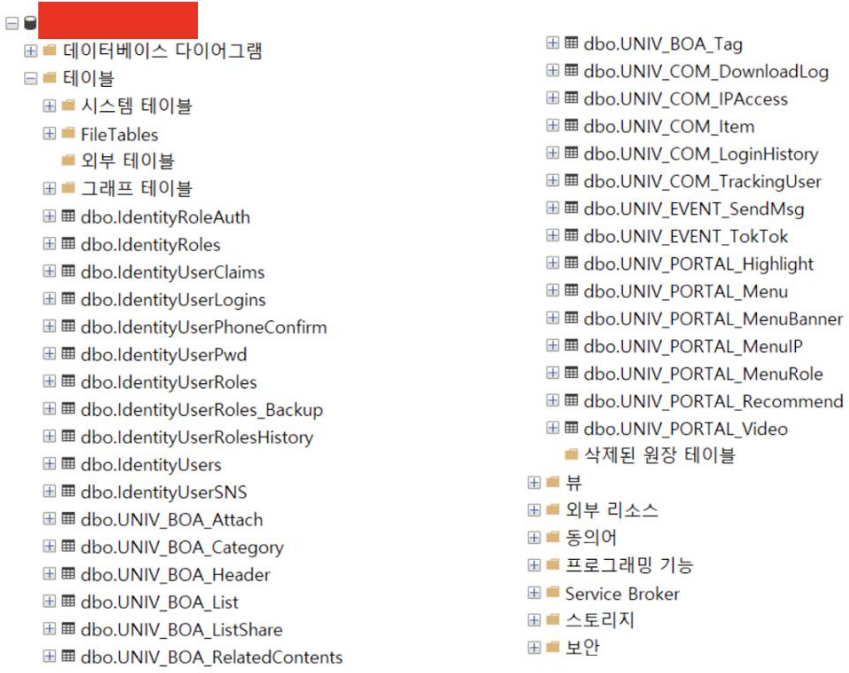
- 공개된 Backup 파일 다운로드 AWS S3 URL은 외부에 노출되어 구글 검색만으로도 확인 가능
- 노출된 http://****.Archives/1 도메인에서 해당 AWS S3 URL을 사용 중, html 코드로 확인 가능



SQL Backup Data Breach of Korea insurance company

ASM (Attack Surface Monitoring)

- Backup 파일을 복원하면 34개의 테이블과 데이터들을 확인 가능
- 관리자 계정의 Email, PW를 포함하여 42건의 계정 정보, 및 IP를 포함한 로그인 기록 등 민감 데이터가 평문으로 노출됨



SQL Backup Data Breach of Korea insurance company

Conclusion

- DDW 모니터링 및 ASM 분석이 없었다면 유출 사실을 파악하지 못하고 분석도 이루어지지 못했을 것
- 유출된 Backup 파일은 피해기업의 로깅 데이터가 저장되어 있는 원본 데이터베이스의 백업 파일
- 중요도가 높은 자산을 하나의 S3 버킷에 혼용하여 사용하면 버킷 설정이 잘못 구성될 경우 모든 데이터가 의도치 않게 도출될 수 있음
- 개인정보가 포함된 데이터베이스 백업 및 스냅샷을 암호화하여 관리해야 함

ETC : Data Breach of Korea finance company

Data Breach of Korea finance company

Overview

- 2023년 하반기 한국의 Finance 회사의 사용자(회원) 정보 데이터베이스가 유출됨
- ASM 분석을 통해 현재 사용하고 있지 않으나 정리되지 않았던 내부용 개발 도메인이 외부에 노출된 것을 식별
  - ID, PW 입력에 SQL Injection 공격을 수행
  - MS SQL 데이터베이스에서 사용자(회원) 정보가 담긴 테이블 조회
- 피해기업의 데이터가 판매 / 유출되는지 DDW 모니터링 중

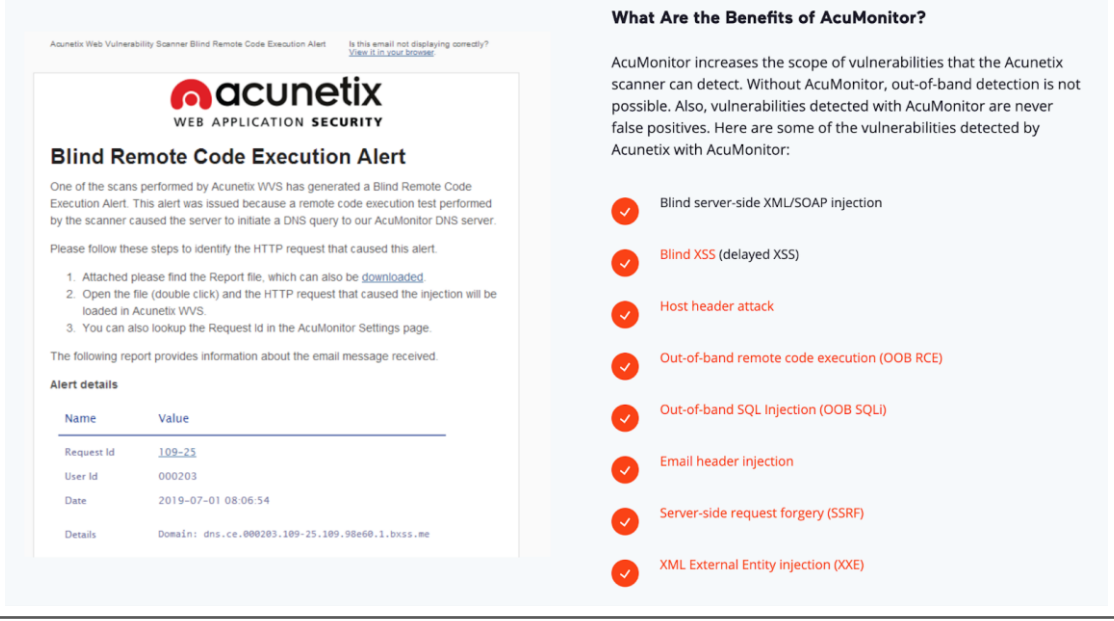
dev-*.domainA.com
test-*.domainB.com

개발망 및 테스트 도메인

Data Breach of Korea finance company

ASM (Attack Surface Monitoring)

- 2023년 하반기, 공격자는 Acunetix 웹스캔 도구를 사용하여 SSRF, XML Injection, XSS, SQL Inection 등 다양한 공격 기법을 시도함
- 그 과정에서 외부에 오픈된 개발(dev.*) 도메인 식별
- Secure coding이 적용되지 않은 프로시저 식별



Acunetix Web Vulnerability Scanner Blind Remote Code Execution Alert

Is this email not displaying correctly? View it in your browser.

acunetix
WEB APPLICATION SECURITY

Blind Remote Code Execution Alert

One of the scans performed by Acunetix WVS has generated a Blind Remote Code Execution Alert. This alert was issued because a remote code execution test performed by the scanner caused the server to initiate a DNS query to our AcuMonitor DNS server.

Please follow these steps to identify the HTTP request that caused this alert.

1. Attached please find the Report file, which can also be downloaded.
2. Open the file (double click) and the HTTP request that caused the injection will be loaded in Acunetix WVS.
3. You can also lookup the Request Id in the AcuMonitor Settings page.

The following report provides information about the email message received.

Alert details

Name	Value
Request Id	109-25
User Id	000203
Date	2019-07-01 08:06:54
Details	Domain: dns.ce.000203.109-25.109.98e60.1.bxss.me

What Are the Benefits of AcuMonitor?

AcuMonitor increases the scope of vulnerabilities that the Acunetix scanner can detect. Without AcuMonitor, out-of-band detection is not possible. Also, vulnerabilities detected with AcuMonitor are never false positives. Here are some of the vulnerabilities detected by Acunetix with AcuMonitor:

- Blind server-side XML/SOAP injection
- Blind XSS (delayed XSS)
- Host header attack
- Out-of-band remote code execution (OOB RCE)
- Out-of-band SQL Injection (OOB SQLi)
- Email header injection
- Server-side request forgery (SSRF)
- XML External Entity injection (XXE)

Data Breach of Korea finance company

ASM (Attack Surface Monitoring)

- 피해기업은 개발(dev.*) 도메인이 외부에 오픈된 것을 전혀 인지하지 못했던 상태
- Secure coding이 적용되지 않은 프로시저 또한 식별하지 못한 상태
- 분석 당시 공격 과정 및 행위는 식별 했으나 네트워크 로그 분석만으로는 정확히 언제(When), 어떻게(How), 어디서(Where) 침투했는지 식별에 어려움이 존재했었음
- **내부망에 존재하고 외부에서 접근이 불가하다고** 했던 dev, devadmin 등 도메인이 **사실은 모두 외부에 노출되어 누구나 접근이 가능**했었음

dev-*.domainA.com
test-*.domainB.com

개발망 및 테스트 도메인


Conclusion

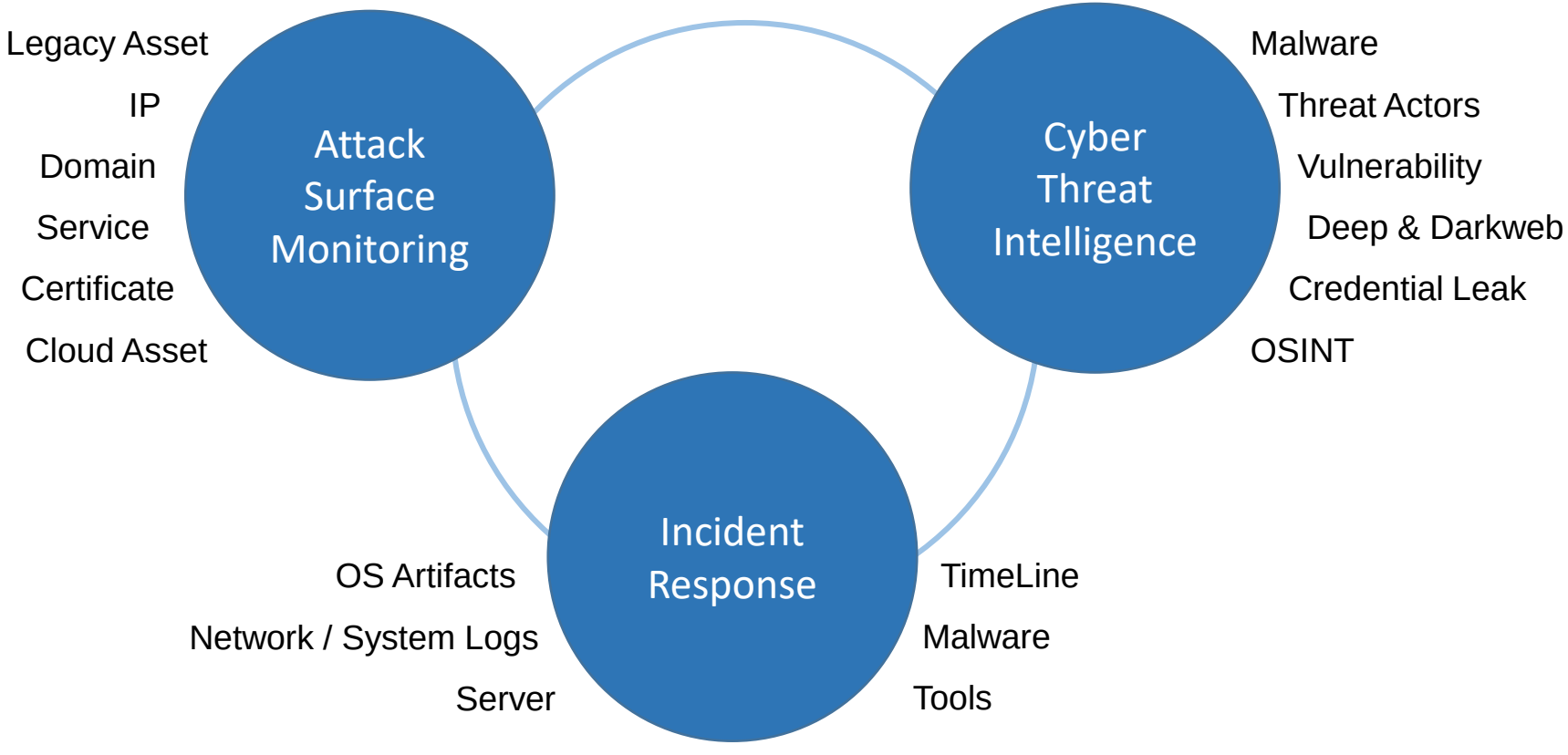
Conclusion

Incident Response with ASM, DDW OSINT, Cloud Analysis

- ASM, DDW OSINT, Cloud 분석이 없었다면 피해사실을 애초에 인지하지 못했거나, 침투 경로를 전혀 분석하지 못했을 것
- DDW 포럼들을 모니터링하지 않았다면 피해기업의 데이터 유출
- ASM 분석을 하지 않았다면 공격자가 어떻게 침투했는지 밝혀내지 못했을 것
- **양방향 접근 관점으로 분석이 필요함**
  - **외부에서 내부로 접근하는 분석**
    - 외부에서 내부로 접근 가능한 다양한 접근 포인트들 분석을 통해 초기 침투 지점 파악
    - DDW에 유출되는 데이터를 통해 피해 사실 파악 및 추적
  - **내부에서 외부로 접근하는 분석**
    - 내부에 공격자가 남긴 흔적들을 따라 거슬러 올라가며 초기 침투까지 파악

Conclusion

Incident Response with ASM, DDW OSINT, Cloud Analysis




Thank you

S2W
Safe and Secure World

About S2W

S2W is a big data intelligence company specialized in hidden channels and cryptocurrencies.

S2W captures massive amount of data from various channels and conducts analysis with the unique AI based multi-domain analytics engine.

S2W Offers a threat intelligence solution **S2-XARVIS**, cryptocurrency anti-money laundering solution **S2-EYEZ**, digital fraud detection system **S2-TRUZ**.

Contact

For any queries, please contact

info@s2w.inc

www.s2w.inc