quaxar

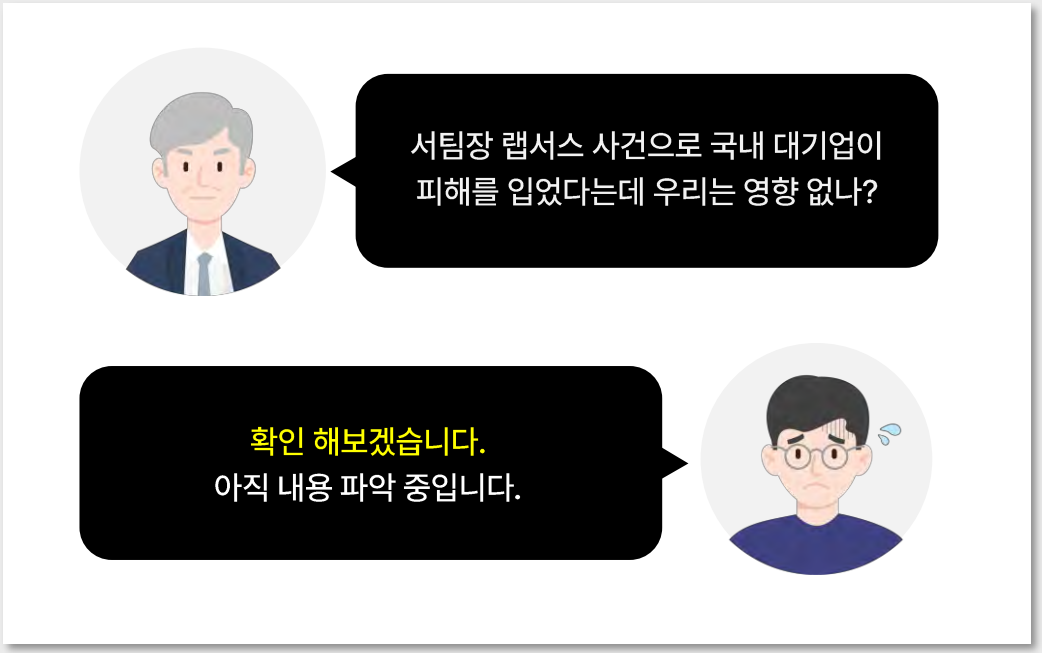
Leveling up your Cyber Threat Intelligence

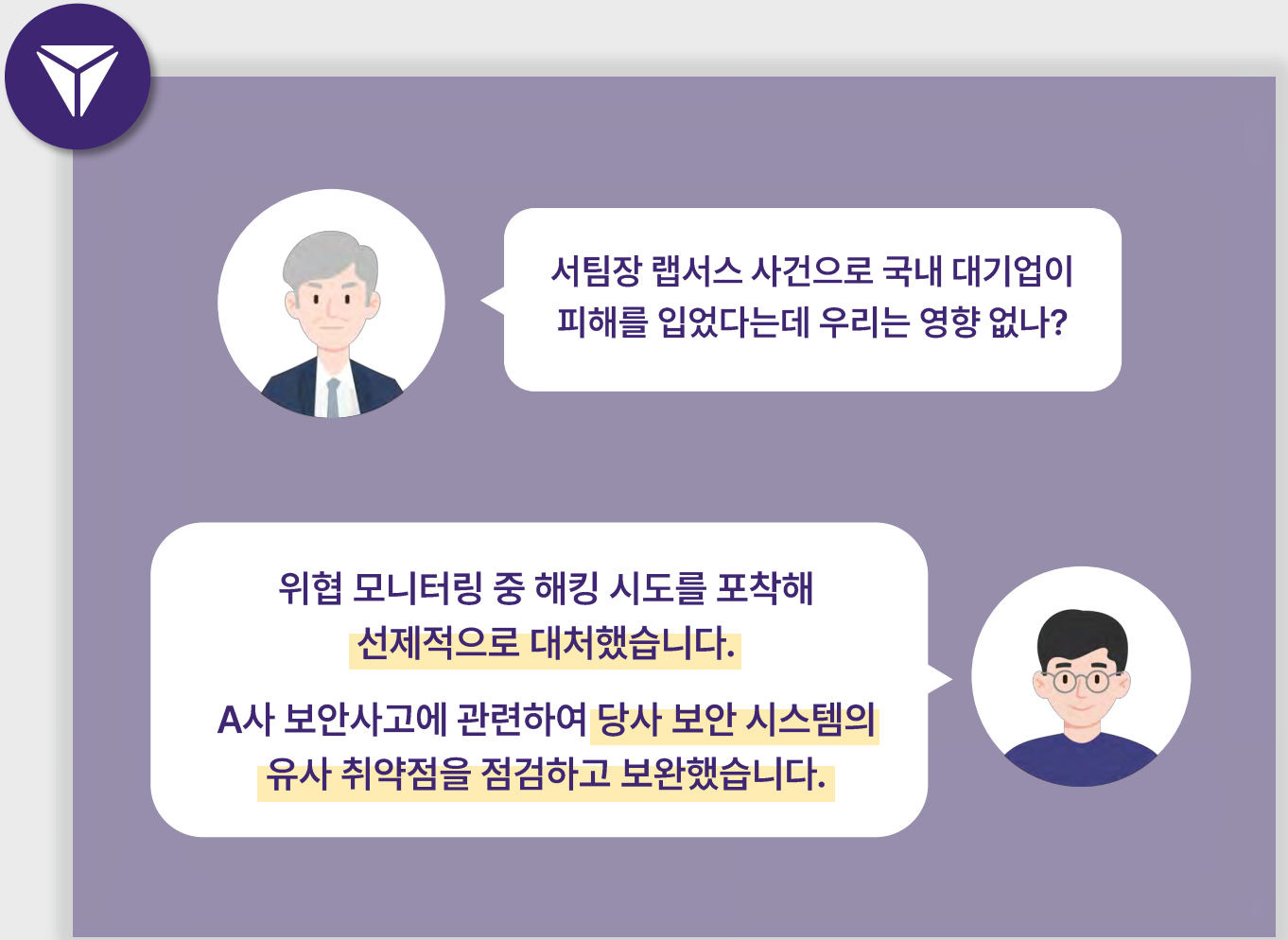
# CTI 솔루션 활용 사례

서현민 팀장 / Global Business

“확인 해보겠습니다”

# "확인 해보겠습니다"



# “확인 해보겠습니다”

랩서스 활동 지표가
업데이트 되었습니다.
대응 완료하였습니다.

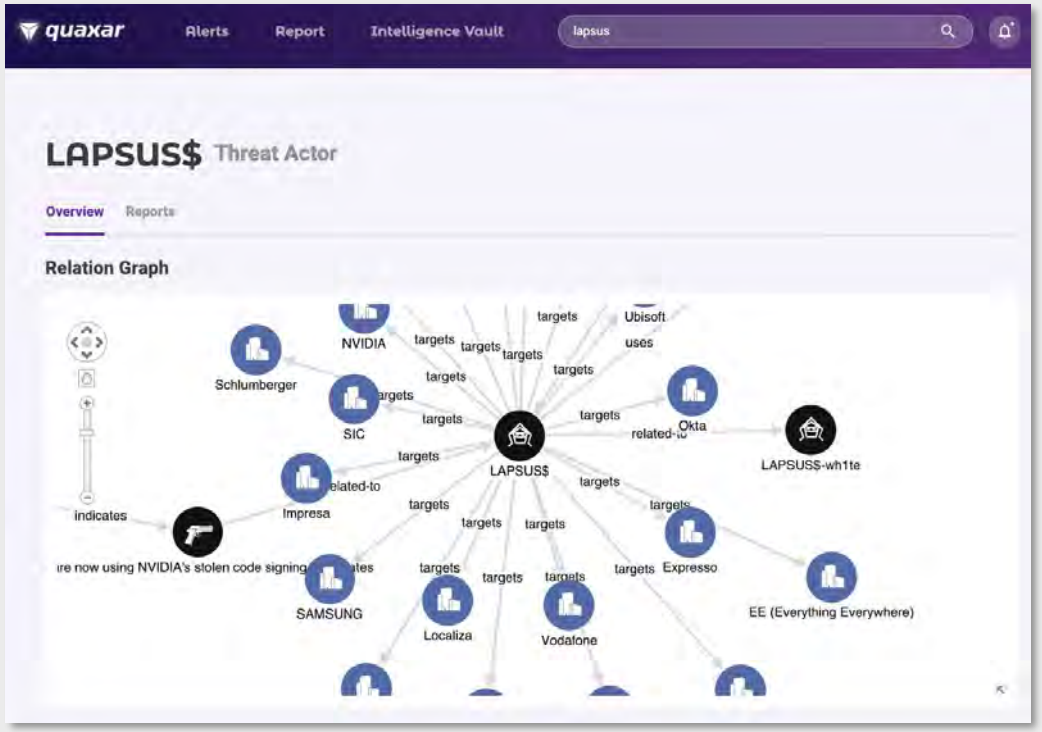
다크웹 딥웹 내 활동 인지

랩서스로 그룹명 변경

사고 발생

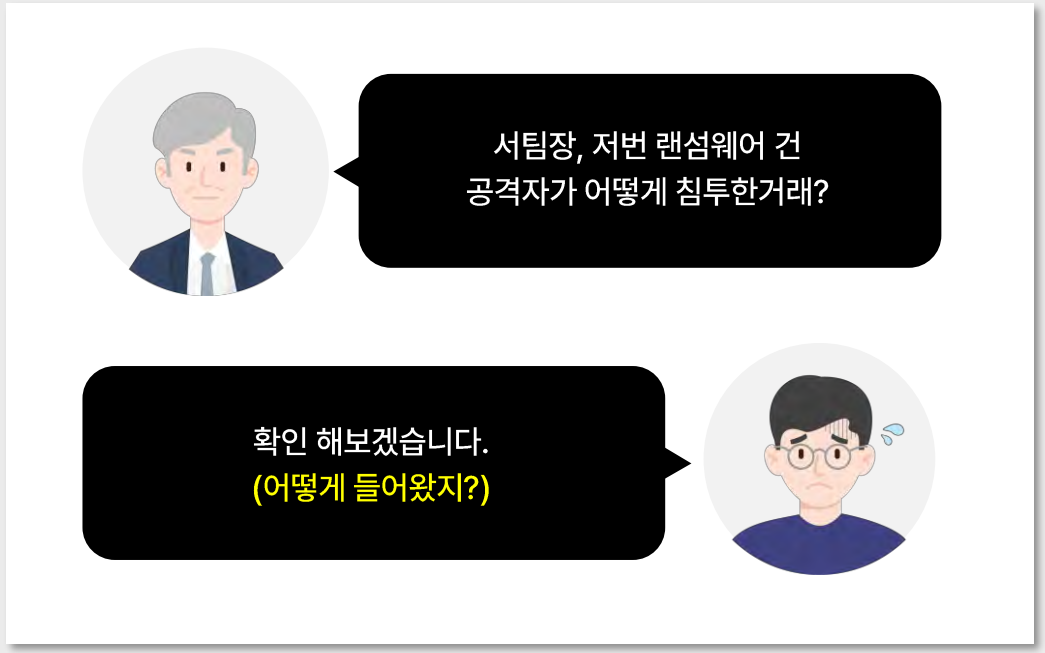
랩서스 활동 지표 확인

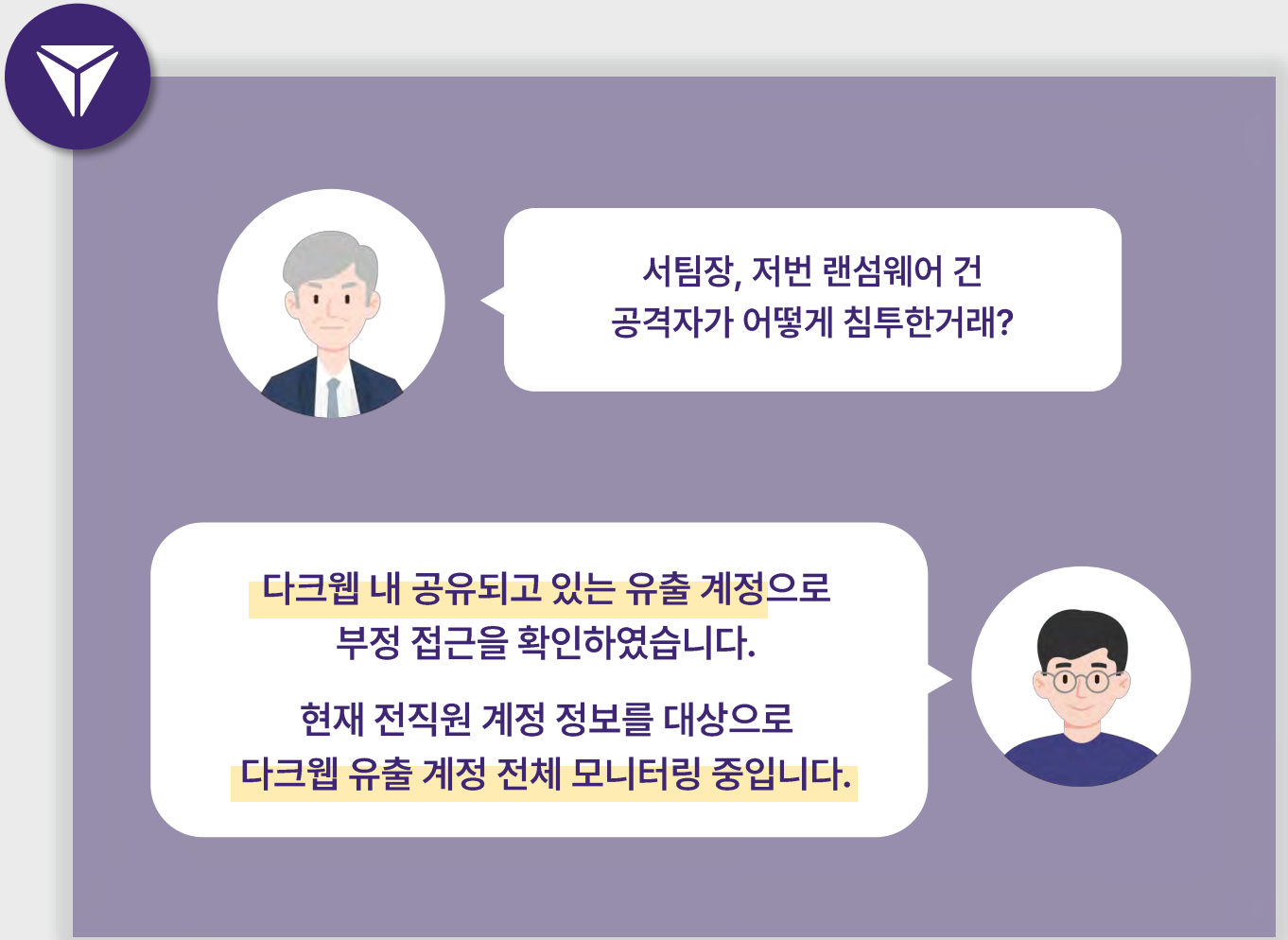
API를 통한 내부 장비 적용



“어떻게 들어왔지?”

# "어떻게 들어왔지?"



# "어떻게 들어왔지?"

유출 계정에 대해 조치 완료했습니다.
재발방지를 위해 다크웹 계정 유출 모니터링을 상시 가동중입니다.

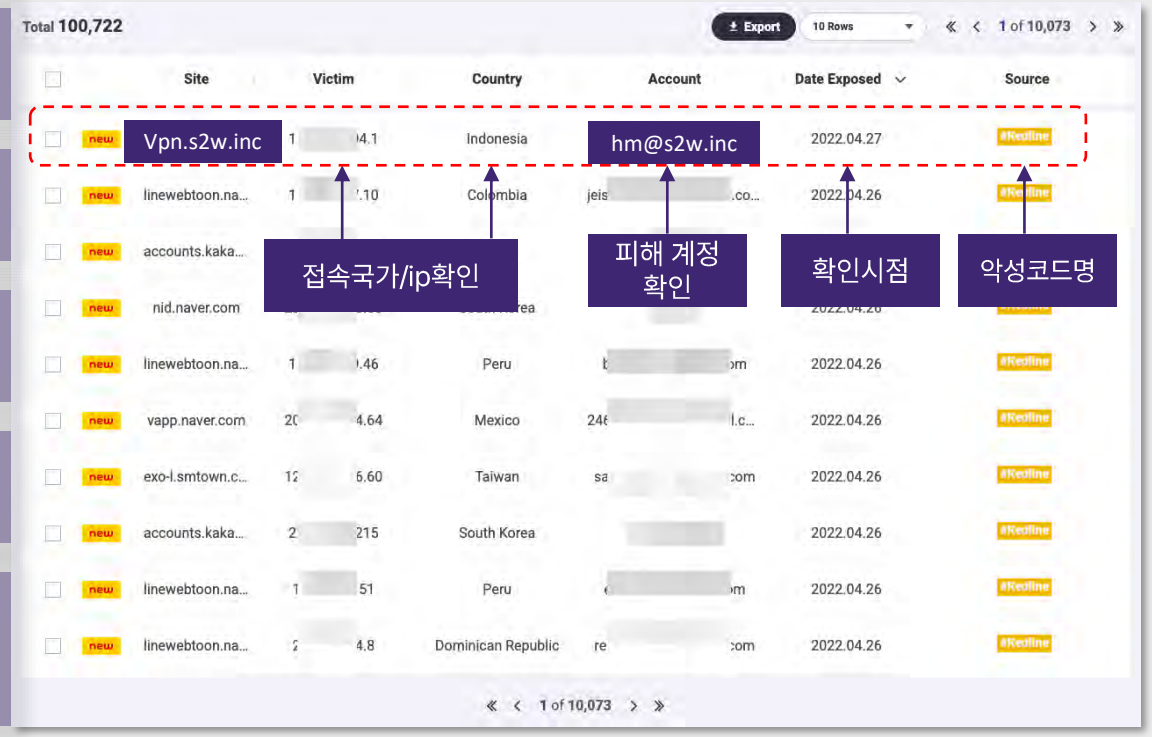
고객사 계정 정보 등록
(도메인 정보)

다크웹 및 딥웹 유출 계정 정보
실시간 탐지

정보 매칭 시 시스템 알림메일 전송

매칭된 직원 시스템 계정 즉시 변경
및 영향도 파악

부정접근 이력 확인 후
추가 대응



“나랑 관련된 거임?”

# "나랑 관련된 거임?"

서팀장, Log4J 우리는 어떻게 대응하고 있어?

확인 해보겠습니다.
(솔직히 Log4J 처음 들었을 때 이렇게까지 심각한 이슈인지 몰랐다.)

Log4J 취약점 영향도가 자사 서비스 90%이상입니다. 내부 비상대책회의가 필요한 시점입니다.

Log4J 취약점을 이용한 봇 공격들이 있는지 확인 중입니다. 추가 공격 대응하겠습니다.

전사에 긴급 상황 공지하고
각 부서에 긴급 패치 진행 예정이니 서비스 영향도 파악 지원 요청도 같이 부탁해

# "나랑 관련된 거임?"

**Log4J 이슈에 관하여**
**당일 대응 완료 하였습니다.**

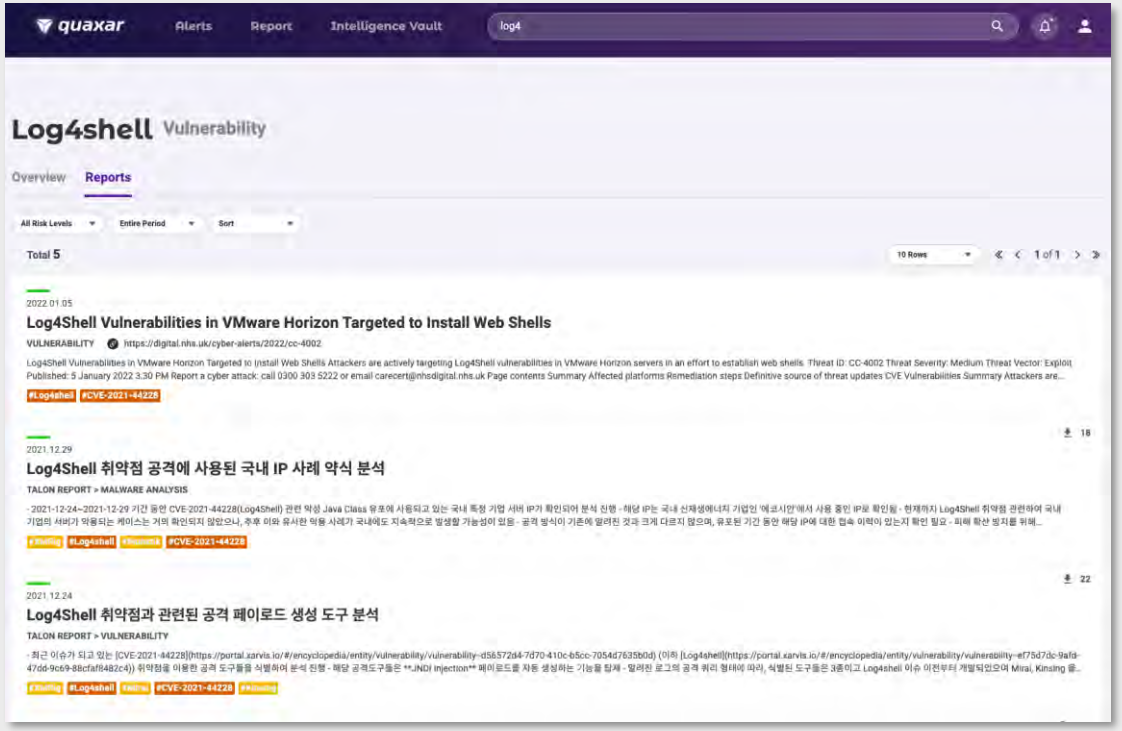
Hot Issues&Trends에서
Log4J/Log4shell 인지

Log4shell 관련 분석리포트 확인

자사 서비스 긴급 패치 공지

취약점 공격에 사용된 국내 IP 파악

봇넷을 이용한 추가 공격
정황 파악 및 대응준비






S2W

“우리 꺼야?”

# "우리 꺼야?"

이렇게 통제가 촘촘한데, 우리 자산이 외부에 유출될 수 없어.

[ALERT] 내부 자산으로 파악되는 자산이 탐지되었습니다.

이거 우리 자산 맞는 것 같은데?
누가 올렸고 언제 올라왔지?

이건 우리를 사칭하는 업체인 것 같네, 게시 중단 요청을 해야겠어.

# "우리 꺼야?"

일일이 매번 직접 검색하고
눈으로 확인 하는 건 쉽지않아.
시스템이 24시간 모니터링하고
이상이 있을 때만 대응 해야지.

고객사 핵심 키워드 및 public IP 대역 등록

고객사 추정 자산 탐지

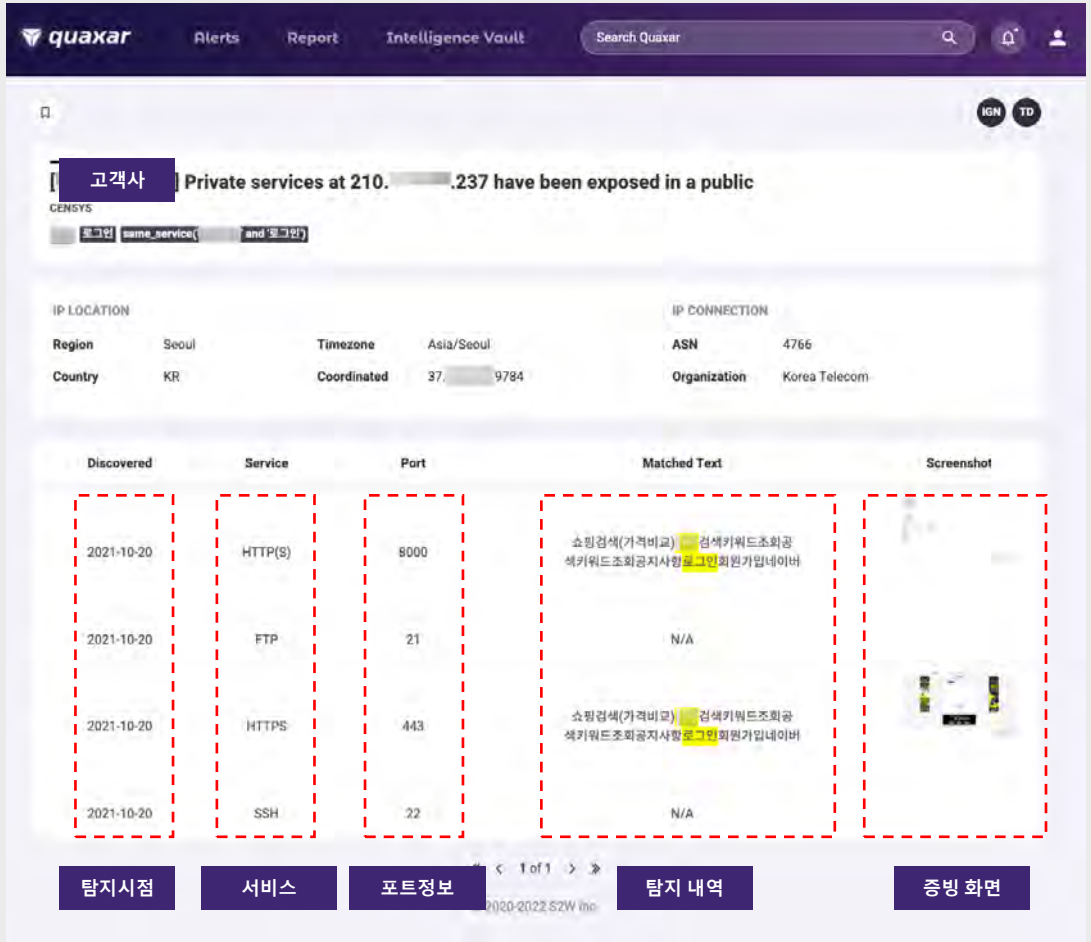
담당자 확인

YES

NO

Take Down

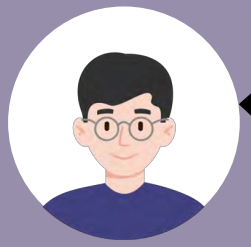
Ignore



“제가 어떻게 다 혼자해요”

# “제가 어떻게 다 혼자해요”

우린 남들처럼 해킹 대회 우승한 그런 분석인력은 없어. 근데 그들과 같은 대응 수준을 하지 않으면 이슈 트래킹하기가 어려워.



랩서스가 활용했다는 Redline 악성코드 상세 분석 요청 드립니다.
해당 악성코드가 돌아가는 로직을 확인하여 대응 방법을 구체화하고 싶습니다.

[RFI] 요청 접수 완료하였습니다.

해당 악성코드에 대한 상세 분석은 영업일 기준 1~2일 내로 올라갈 예정입니다.

# “제가 어떻게 다 혼자해요”

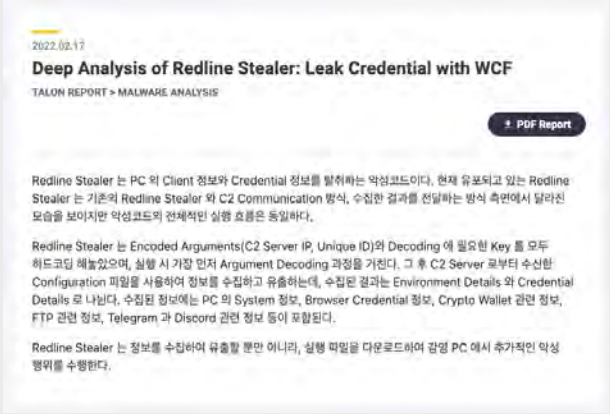
우리 보안팀 규모는 크지 않지만,
수십 명의 분석가가 함께하는
기분이야.

특정 공격그룹 활용
공격 기법 인지

악성코드 상세 분석 요청 의뢰

상세 분석 보고서 등록

내부 보안장비에 시그니쳐 및 관련
IoC 등록


2022.02.17

Deep Analysis of Redline Stealer: Leak Credential with WCF

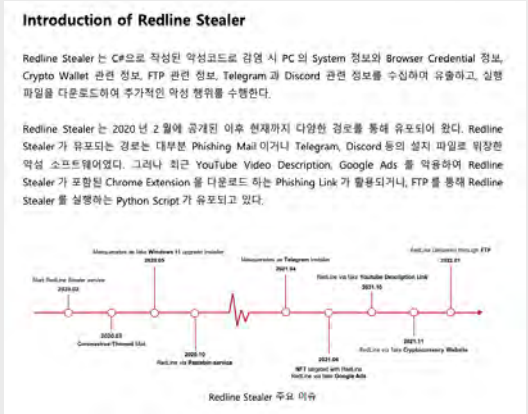
TALON REPORT > MALWARE ANALYSIS

PDF Report

Redline Stealer 는 PC 의 Client 정보와 Credential 정보를 탈취하는 악성코드이다. 현재 유포되고 있는 Redline Stealer 는 기존의 Redline Stealer 와 C2 Communication 방식, 수집한 결과를 전달하는 방식 측면에서 달라진 모습을 보이지만 악성코드의 전체적인 실행 흐름은 동일하다.

Redline Stealer 는 Encoded Arguments(C2 Server IP, Unique ID)와 Decoding 에 필요한 Key 를 모두 하드코딩 해놓았으며, 실행 시 가장 먼저 Argument Decoding 과정을 거친다. 그 후 C2 Server 로부터 수신한 Configuration 파일을 사용하여 정보를 수집하고 유출하는데, 수집된 결과는 Environment Details 와 Credential Details 로 나뉜다. 수집된 정보에는 PC 의 System 정보, Browser Credential 정보, Crypto Wallet 관련 정보, FTP 관련 정보, Telegram 과 Discord 관련 정보 등이 포함된다.

Redline Stealer 는 정보를 수집하여 유출할 뿐만 아니라, 실행 파일을 다운로드하여 감염 PC 에서 추가적인 악성 행위를 수행한다.

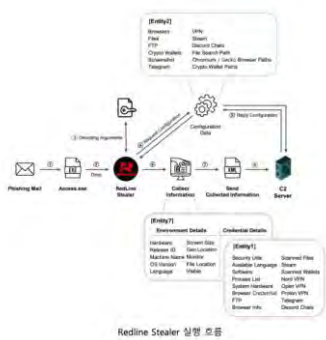

Introduction of Redline Stealer

Redline Stealer 는 C#으로 작성된 악성코드로 감염 시 PC 의 System 정보와 Browser Credential 정보, Crypto Wallet 관련 정보, FTP 관련 정보, Telegram 과 Discord 관련 정보를 수집하여 유출하고, 실행 파일을 다운로드하여 추가적인 악성 행위를 수행한다.

Redline Stealer 는 2020 년 2 월에 공개된 이후 현재까지 다양한 경로를 통해 유포되어 왔다. Redline Stealer 가 유포되는 경로는 대부분 Phishing Mail 이거나 Telegram, Discord 등의 설치 파일로 위장한 악성 소프트웨어였다. 그러나 최근 YouTube Video Description, Google Ads 를 악용하여 Redline Stealer 가 포함된 Chrome Extension 을 다운로드 하는 Phishing Link 가 활용되거나, FTP 를 통해 Redline Stealer 를 실행하는 Python Script 가 유포되고 있다.



Redline Stealer 주요 이슈


Redline Stealer 실행 흐름

| Type | Indicator | Related Tags |
|---|---|---|
| MD5 | 10adb0969eb2b385d6bb8ad8e91bb0c4 | |
| SHA256 | c6d48514031cc6e83445b95f9ed4e975f2cdcebc2e9cc1914605058ff7af7764 | |
| SHA256 | 38a5b96fd07f03041f6eff913b85fc621fa314e1de87326accb06ee218c37756 | |
| IPv4 | 62.182.159.86 | |
| SHA256 | cd3f0808ae7fc8aa5554192ed5b0894779bf88a9c56a7c317ddc6a4d7c249e0e | |
| SHA256 | 9ac01cc861cfe9e340c66a5cd527ab8a7e3de345b851ebcf07a7ca08eeee2f88 | |



S2W

# Beyond Security, Quaxar

## Beyond Security

기업의 핵심 자산 보호를 넘어 지속적인 성장을 위한 비지니스 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.



S2W


## S2W와 솔루션에 대해 더 알고 싶으신가요?

S2W의 문은 언제나 열려있습니다, 아래의 메일 주소로 문의주세요.

info@s2w.inc

www.s2w.inc
경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277