



quaxar

Leveling up your Cyber Threat Intelligence



CTI 솔루션 활용 사례

서현민 팀장 / Global Business

“확인 해보겠습니다”

“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.



“확인 해보겠습니다”



랩서스 활동 지표가
업데이트 되었습니다.
대응 완료하였습니다.



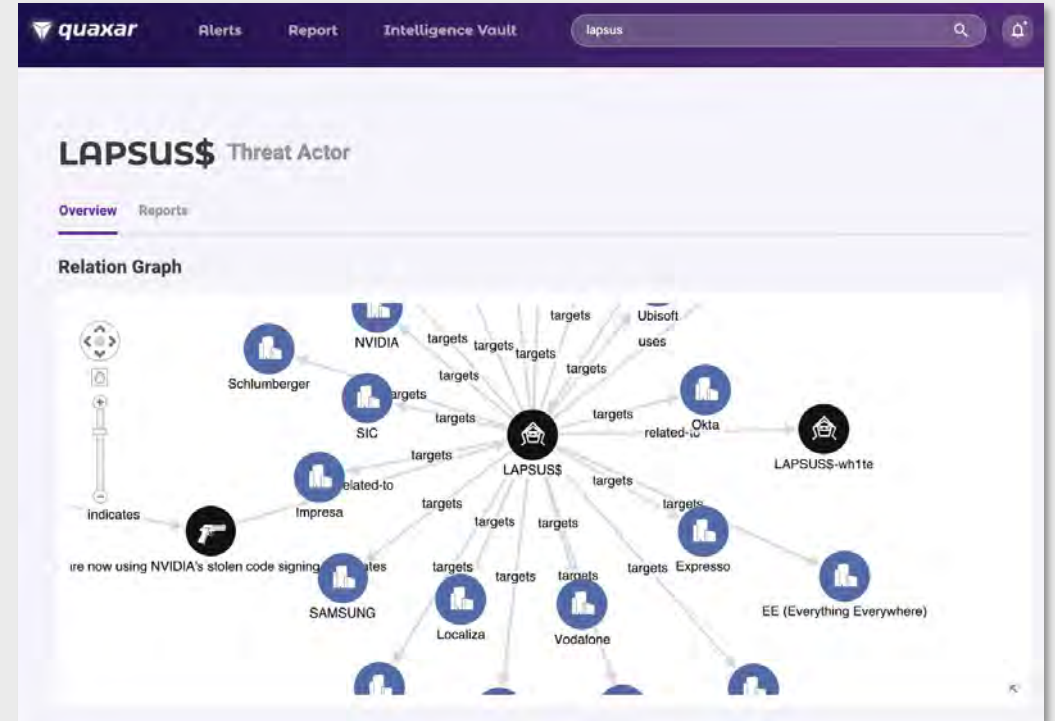
다크웹 딥웹 내 활동 인지

랩서스로 그룹명 변경

사고 발생

랩서스 활동 지표 확인

API를 통한 내부 장비 적용



“어떻게 들어왔지?”

"어떻게 들어왔지?"



서팀장, 저번 랜섬웨어 건
공격자가 어떻게 침투한거래?

확인 해보겠습니다.
(어떻게 들어왔지?)



서팀장, 저번 랜섬웨어 건
공격자가 어떻게 침투한거래?

다크웹 내 공유되고 있는 유출 계정으로
부정 접근을 확인하였습니다.

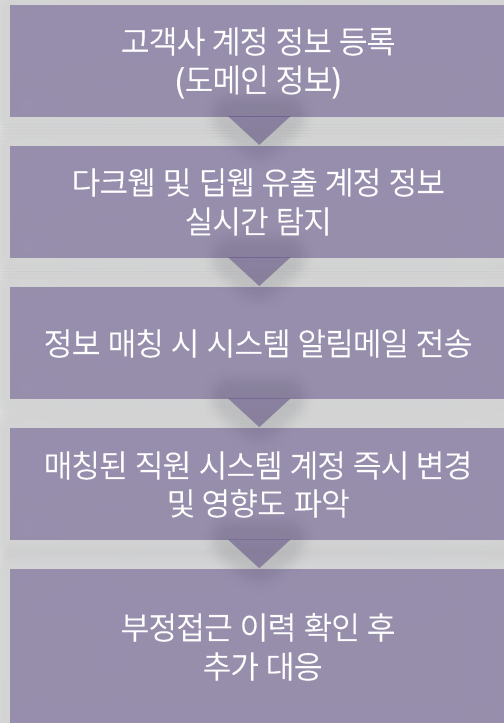
현재 전직원 계정 정보를 대상으로
다크웹 유출 계정 전체 모니터링 중입니다.



"어떻게 들어왔지?"



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



Total 100,722

Site	Victim	Country	Account	Date Exposed	Source
Vpn.s2w.inc	1	Indonesia	hm@s2w.inc	2022.04.27	#Redline
linewebtoon.na...	1	Colombia	jeis...	2022.04.26	#Redline
accounts.kaka...					
nid.naver.com					
linewebtoon.na...	1	Peru		2022.04.26	#Redline
vapp.naver.com	20	Mexico	24f...	2022.04.26	#Redline
exo-l.smtown.c...	12	Taiwan	sa...	2022.04.26	#Redline
accounts.kaka...	2	South Korea		2022.04.26	#Redline
linewebtoon.na...	1	Peru		2022.04.26	#Redline
linewebtoon.na...	2	Dominican Republic	re...	2022.04.26	#Redline

Annotations on the table: '접속국가/ip확인' points to the Country column, '피해 계정 확인' points to the Account column, '확인시점' points to the Date Exposed column, and '악성코드명' points to the Source column. A red dashed box highlights the first row.

“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

quaxar Alerts Report Intelligence Vault log4

Log4shell Vulnerability

Overview Reports

All Risk Levels Entire Period Sort

Total 5

10 Rows << 1 of 1 >>

2022.01.05

Log4Shell Vulnerabilities in VMware Horizon Targeted to Install Web Shells

VULNERABILITY <https://digital.nhs.uk/cyber-alerts/2022/cc-4002>

Log4Shell Vulnerabilities in VMware Horizon Targeted to Install Web Shells. Attackers are actively targeting Log4Shell vulnerabilities in VMware Horizon servers in an effort to establish web shells. Threat ID: CC-4002 Threat Severity: Medium Threat Vector: Exploit Published: 5 January 2022 3:30 PM Report a cyber attack: call 0300 303 5222 or email carecent@nhsdigital.nhs.uk Page contents Summary Affected platforms Remediation steps Definitive source of threat updates CVE Vulnerabilities Summary Attackers are...

#Log4shell #CVE-2021-44228

2021.12.29

Log4Shell 취약점 공격에 사용된 국내 IP 사례 약식 분석

TALON REPORT > MALWARE ANALYSIS

-2021-12-24~2021-12-29 기간 동안 CVE-2021-44228(Log4Shell) 관련 악성 Java Class 유무에 사용되고 있는 국내 특정 기업 서버 IP가 확인되어 분석 진행 - 해당 IP는 국내 신재생에너지 기업인 '에코시안'에서 사용 중인 IP로 확인됨 - 현재까지 Log4Shell 취약점 관련하여 국내 기업의 서버가 악용되는 케이스는 거의 확인되지 않았으나, 후쿠 미와 유사한 악용 사례가 국내에도 지속적으로 발생할 가능성이 있음 - 공격 방식이 기존에 알려진 것과 크게 다르지 않으며, 유포된 기간 동안 해당 IP에 대한 접속 기록이 있는지 확인 필요 - 피해 확산 경지를 위해...

#Shifting #Log4shell #Incidents #CVE-2021-44228

2021.12.24

Log4Shell 취약점과 관련된 공격 페이로드 생성 도구 분석

TALON REPORT > VULNERABILITY

-최근 이슈가 되고 있는 [CVE-2021-44228](<https://portal.xarvis.io/#/encyclopedia/entity/vulnerability/vulnerability-d5657204-7d70-410c-b5cc-7054d7635b0d>) (이하 [Log4shell](<https://portal.xarvis.io/#/encyclopedia/entity/vulnerability/vulnerability-e775d7dc-9af9-47d6-9cc9-88cfa8482c4>)) 취약점을 이용한 공격 도구를 식별하여 분석 진행 - 해당 공격도구들은 **JNDI injectoo** 페이로드를 자동 생성하는 기능을 탑재 - 알려진 로그의 공격 쿼리 형태에 따라, 식별된 도구들은 3종으로 Log4shell 이슈 이전부터 개발되었으며 Mirai, Kimsing 등...

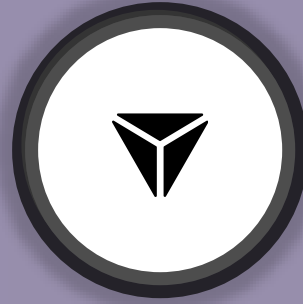
#Shifting #Log4shell #Incidents #CVE-2021-44228 #Incidents

“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?

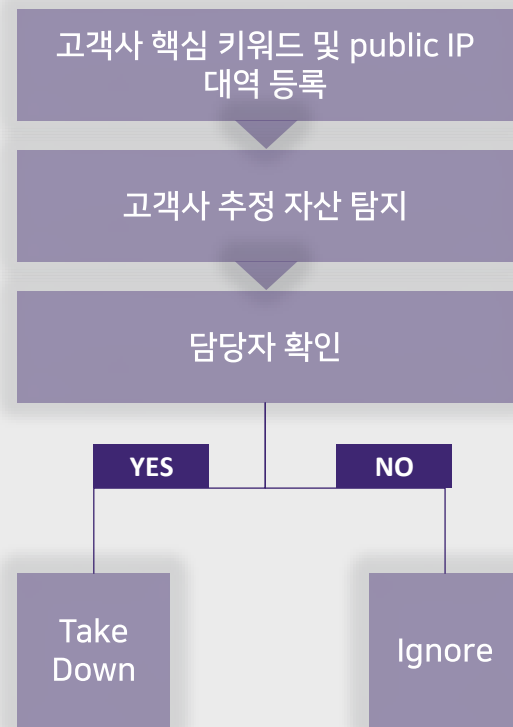
이건 우리를 사칭하는 업체인 것 같네,
게시 중단 요청을 해야겠어.



"우리 꺼야?"



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



quaxar Alerts Report Intelligence Vault Search Quaxar

고객사 Private services at 210. .237 have been exposed in a public

GENSYS

로그인 same_service(and 로그인)

IP LOCATION				IP CONNECTION	
Region	Seoul	Timezone	Asia/Seoul	ASN	4766
Country	KR	Coordinated	37. 9784	Organization	Korea Telecom

Discovered	Service	Port	Matched Text	Screenshot
2021-10-20	HTTP(S)	8000	쇼핑검색(가격비교) 검색키워드조회공 색키워드조회공지사항로그인회원가입네이버	
2021-10-20	FTP	21	N/A	
2021-10-20	HTTPS	443	쇼핑검색(가격비교) 검색키워드조회공 색키워드조회공지사항로그인회원가입네이버	
2021-10-20	SSH	22	N/A	

탐지시점 서비스 포트정보 1 of 1 탐지 내역 증빙 화면

© 2020-2022 S2W Inc.

“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 시그니처 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.

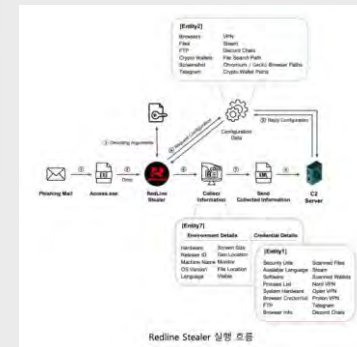
Redline Stealer 는 Encoded Arguments(C2 Server IP, Unique ID)와 Decoding 에 필요한 Key 를 모두 하드코딩 해놓았으며, 실행 시 가장 먼저 Argument Decoding 과정을 거친다. 그 후 C2 Server로부터 수신한 Configuration 파일을 사용하여 정보를 수집하고 유포하는데, 수집된 결과는 Environment Details와 Credential Details 로 나뉜다. 수집된 정보에는 PC 의 System 정보, Browser Credential 정보, Crypto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

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

Introduction of Redline Stealer

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 실시간 채팅 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



Type	Indicator	Related Tags
MD5	10adb0969eb2b385d6bb8ad8e91bb0c4	Phishing Mail
SHA256	c6d48514031cc6e83445b95f9ed4e97f2dcdebc2e9cc19146050581f7a1776a	Phishing Mail
SHA256	38a5b96fdd710304116ef9131b85fc621fa314e1de87326cccb00ee218c37756	Phishing Mail
IPv4	62.182.159.86	Phishing Mail
SHA256	cd310808ae7fc8aa5554192e5b0894779f88a9c5ea7c317d66a4d7c249e0e	Phishing Mail
SHA256	9ac01cc861cfe9e340c66a5cd527ab8a7e3de345b851ebcf07a7ca08e9cc2f98	Phishing Mail

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.



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

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.