quaxar

Leveling up your Cyber Threat Intelligence

랩서스 그룹 관련 인텔리전스 및 대응방안

Lessons learned from Lapsus$

Kyoung-ju Kwak | Head of Cyber Threat Intelligence, Talon, S2W

S2W

곽경주

Head of Cyber Threat Intelligence, Talon @ S2W

- 금융결제원 (~2015.04)
- 금융보안원 (~2020.07)
- **S2W 사이버 위협 인텔리전스 (CTI) 부문 총괄이사 / Quaxar Product Owner (~현재)**

주요 발표

- The Case study of incidents in Korea Financial Sector, International Symposium on Cyber Crime Response, 2014
- The New Wave of CyberTerror in Korea Financial Sector, PACSEC Japan, 2016
- Fly me to the BLACKMOON, HITCON Taiwan, 2016
- Silent Rifle, How to take control all of your system, Hackon Norway, 2016
- Campaign RIFLE : Andariel, The maiden of Anguish, Kaspersky Cyber Security Weekend (Phuket), 2017
- Underground Invasion Tunnels : State-Sponsored Cyber Miners Recent Status, Kaspersky SAS (Cancum), 2018
- Nation-State Moneymule's Hunting Season : APT Attacks Targetting Financial Institutions, Blackhat Europe & Asia

CONTENTS

랩서스 그룹 관련 인텔리전스 및 대응방안

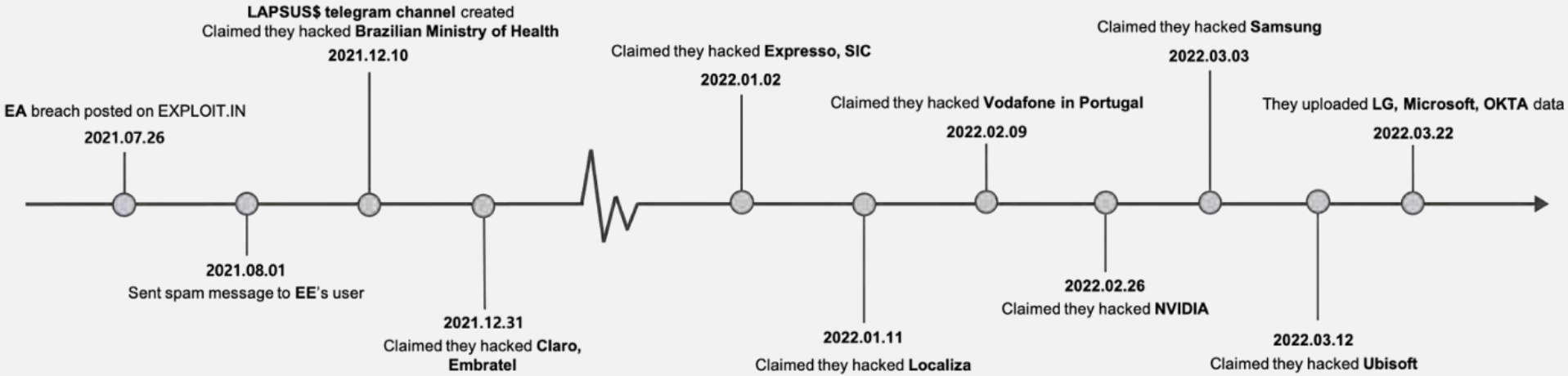
Lessons learned from Lapsus$

SUMMARY

quaxar

- LAPSUS$ 해킹 그룹은 2021년 5월부터 딥웹 포럼에서 활동을 시작한 것으로 추정됨
- 텔레그램에서는 브라질의 보건부에 대한 최초 데이터 유출을 시작으로, 최근 NVIDIA 및 **삼성**에 대한 주요 데이터 뿐만 아니라 LG, Microsoft, **그리고** Okta에 대한 데이터를 업로드하며 전 세계의 주목을 받고 있음
- **최소 5명 이상의 멤버들로 구성**되어 있는 것으로 추정되는 이 그룹의 가장 큰 목적은 **금전적 이득**이며, 간혹 그들만의 **재미를 위해** 기업을 해킹하는 사례도 확인됨

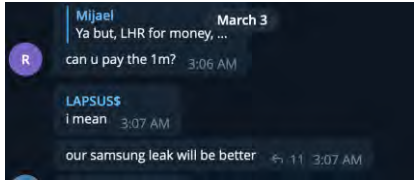
LAPSUS$ Breach Timeline



quaxar

S사 사고 이후, "국내" 랩서스 관련 대응 타임라인 (S2W 기준)

2022.03.03 03:07AM
Lapsus Chat 채널에서 S사 탈취 정보에 대한 언급

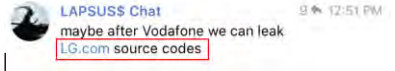


2022.03.05 07:00AM (토요일)
S사 데이터 유포 토런트 파일 랩서스 채널에 게시

2022.03.06 (일요일)
S2W 고객사에
랩서스 침투 수법에 대한
인텔리전스 공유

2022.03.08
랩서스 관련 상세 종합 보고서
고객사 대상 공유

2022.03.09
S2W 고객사 대상으로
랩서스 최신 주요 IOC 제공



2022.03.15
랩서스가 L사
데이터 유출
예고

2022.03.22
텔레그램에

1) L사 유출 데이터 게시
2) Microsoft 유출 데이터 게시

2022.03.23
OKTA 측 침해사고
공식 입장문에 대한
반박글
텔레그램 게시

랩서스 그룹 관련 인텔리전스 및 대응방안

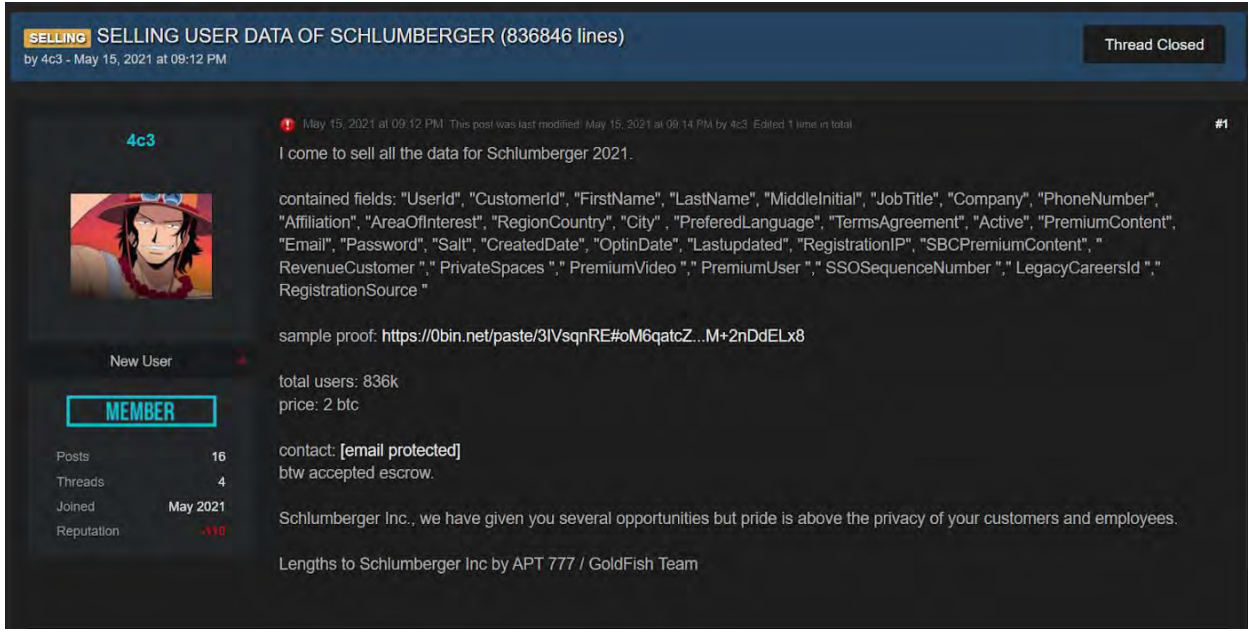
Lessons learned from Lapsus$

HISTORY OF LAPSUS$

History of LAPSUS$ (1/3)

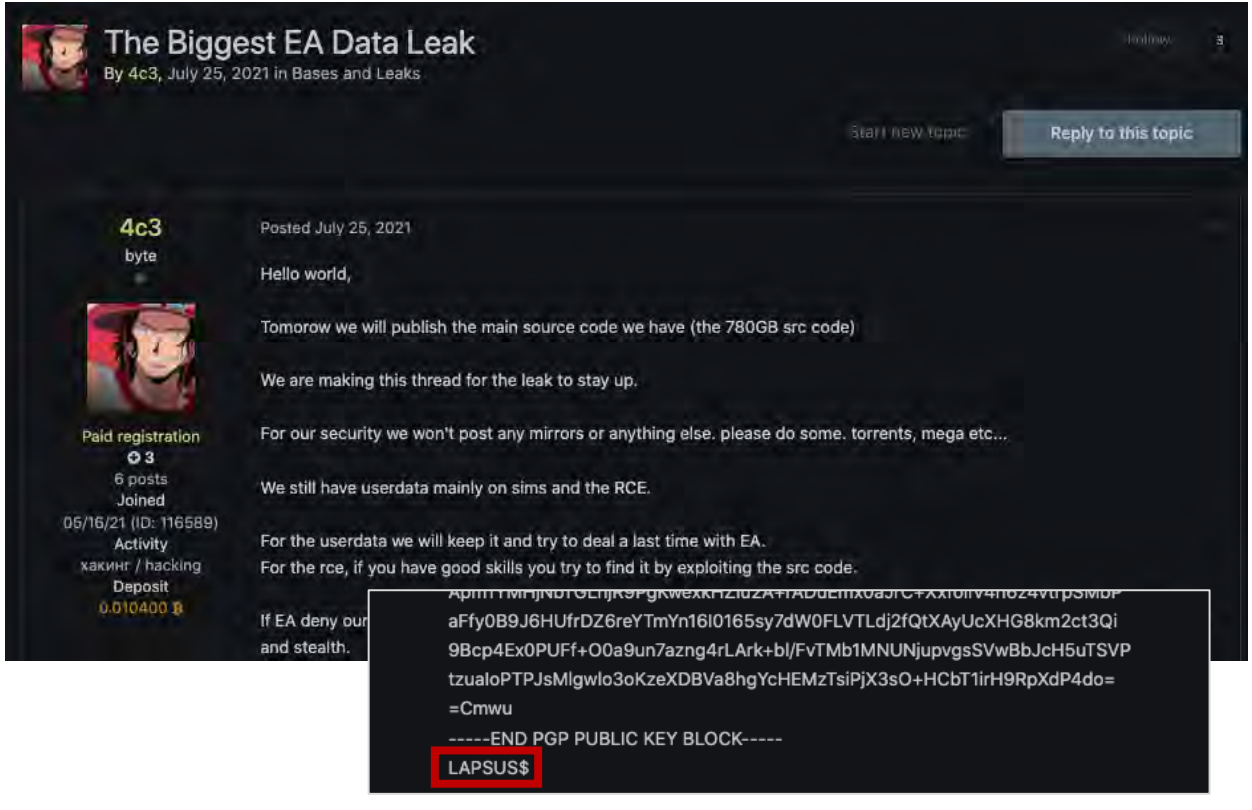
quaxar

- LAPSUS$ 해킹 그룹의 흔적은 **2021년 5월 15일 딥웹 포럼인 RaidForums**에서 최초로 확인되었음
- 당시 **세계 최대 유전 서비스** 업체인 SCHLUMBERGER로부터 데이터를 탈취했다고 주장하며, 고객과 직원 정보가 포함된 836,000건의 데이터를 2BTC에 판매한다는 게시글을 최초로 업로드하였음
- 당시에는 **APT777 / GoldFish Team** 이라는 이름을 사용하였음

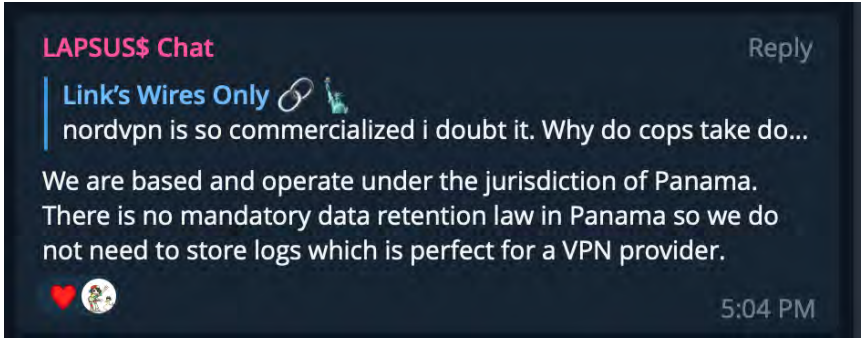


quaxar

- LAPSUS$ 라는 팀명은 2021년 7월 25일, 세계적 게임 회사인 EA의 소스코드 탈취에 대한 글을 포럼에 게시할 때 처음으로 사용하였음



- EA 데이터 탈취 이후를 기점으로 **팀을 본격적으로 셋업**, 대형 기업 대상 공격을 수행하고 있음
- 이후 2021년 10월, **브라질 보건부를 해킹**하고 협박하기 위해 현재의 **텔레그램 채널**을 개설하였음
- 브라질 보건부 공격 당시 자신들이 **제로데이**를 사용했다고 언급하기도 하였고, 이후 윈도우즈 커널 드라이버 관련 제로데이 사용에 대해 언급하는 등 그룹 내 **수준급 실력의 멤버**가 있는 것으로 추정됨
- **최소 5명**으로 구성되어 있으며, 대부분 브라질 국적을 가지고 있는 것으로 추정되며, 세르비아 출신도 있음을 암시하였음
- **Panama 법에 의거하여 공격을 수행**하고 있다고도 언급하였음
  - Panama의 경우, Budapest Convention에 가입되어 있긴 하나, 사이버 범죄에 대한 강력한 제재 조항이 없는 국가이며, 특히 Data retention 이 강제가 아닌 관계로 사용자들의 로그 등을 남기지 않음



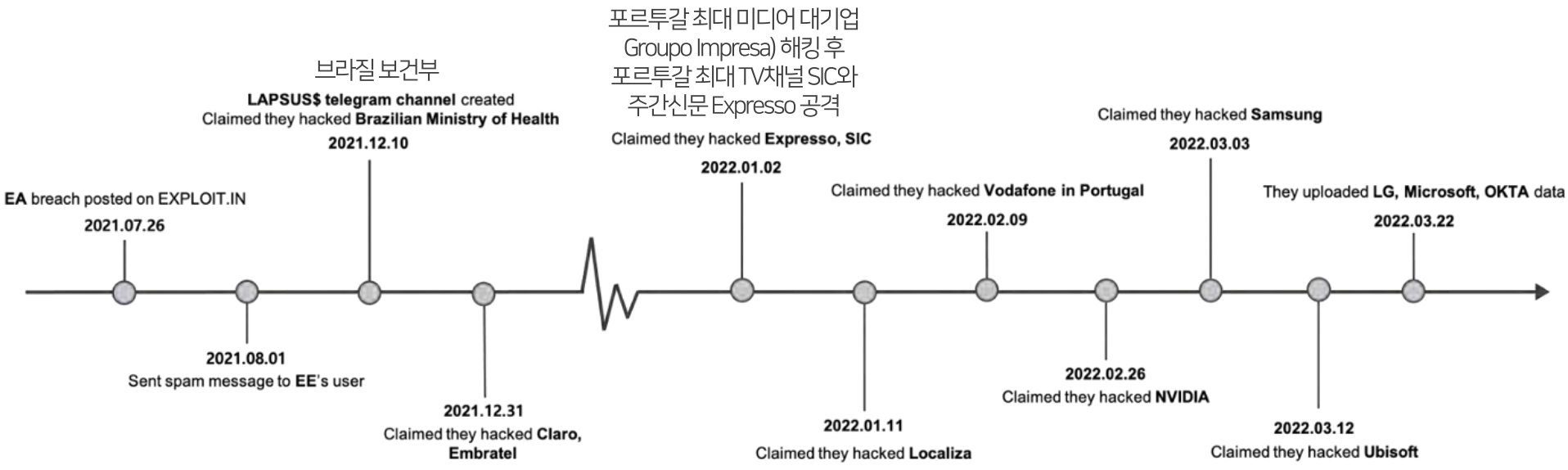
랩서스 그룹 관련 인텔리전스 및 대응방안

Lessons learned from Lapsus$

DATA BREACH TIMELINE

Data Breach Timeline

quaxar



세계에서 7번째로 큰
멕시코 통신회사인
America Mobil의 자회사

Localiza Rent a Car SA는 라틴아메리카 및
세계에서 가장 큰 렌터카 업체 중 하나로,
현지 시간으로 오전 2시 30분에서 4시,
Localiza의 홈페이지에 접속하면
포르노 사이트로 리다이렉션되는 현상이 확인

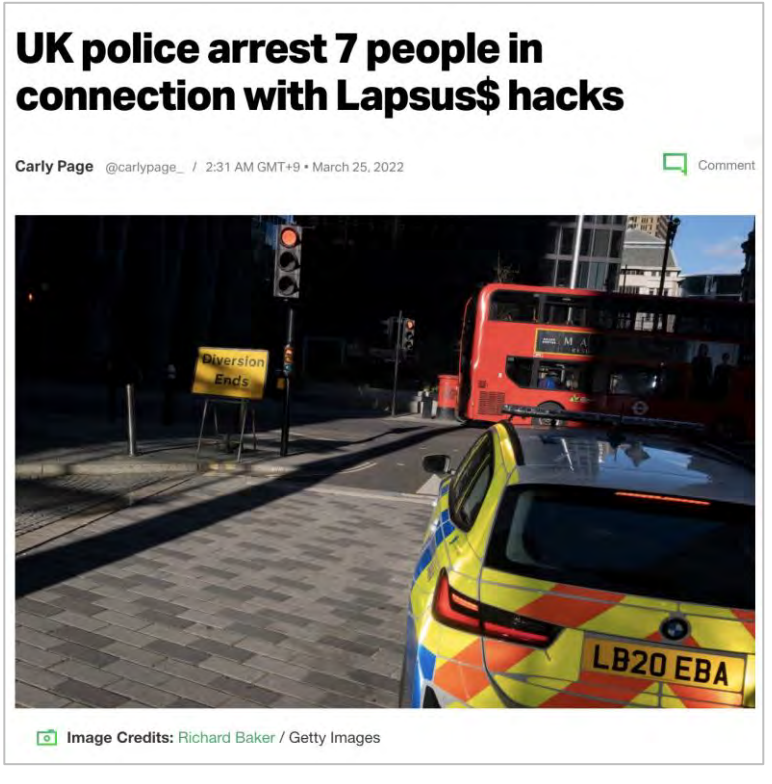
랩서스 그룹 관련 인텔리전스 및 대응방안

Lessons learned from Lapsus$

MEMBERS OF LAPSUS$

- 현재 신원이 밝혀지고 경찰에 검거된 일부 멤버들이 있으며,
  랩서스 코어 멤버들의 큰 그림 (꼬리자르기 또는 속임수)으로 추정되기도 함

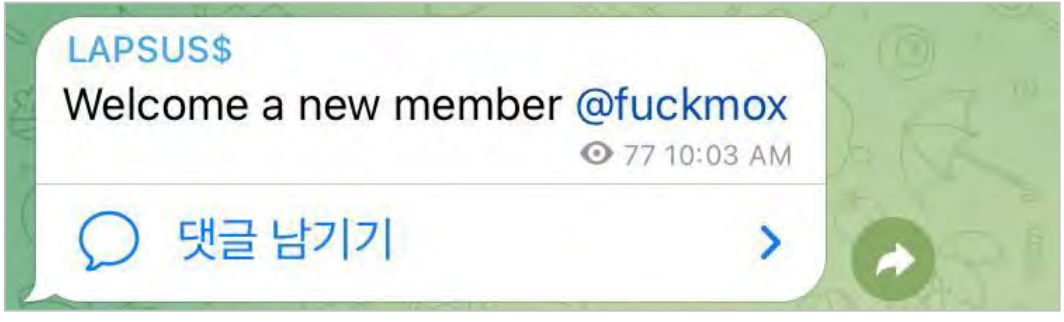
랩서스 텔레그램 프로필 이미지

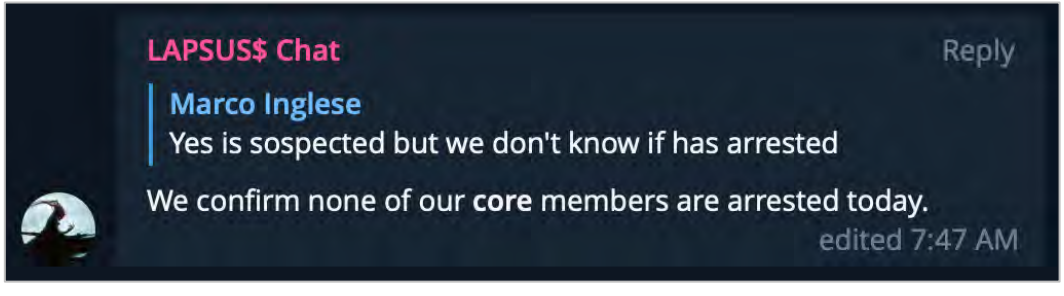


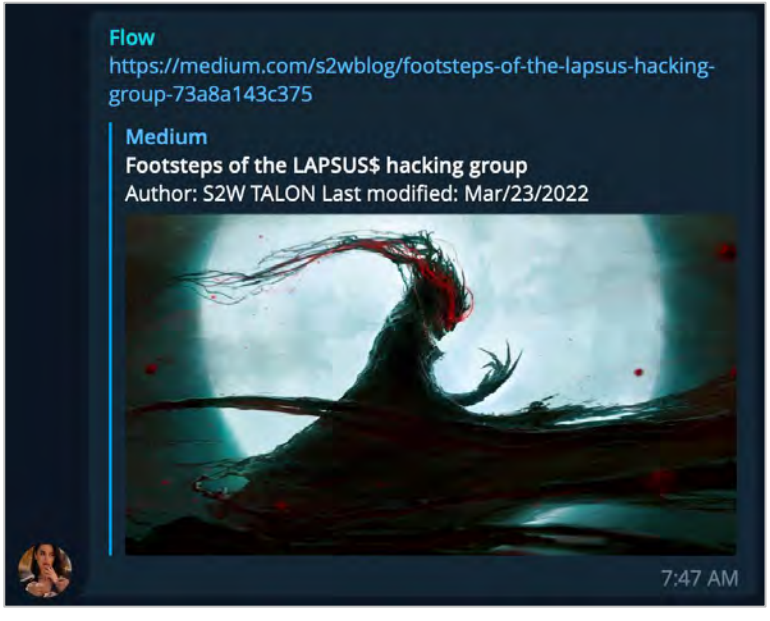
- Arion Kutaj (알바니아계)
- 거주지 : Oxford / Kidlington / Bicester
- 자폐증을 앓고 있다고 하며, private 0day community에서 유명해진 후 Lapsus$에 합류

quaxar

- 랩서스 멤버 체포 기사 보도 직후,







랩서스 그룹 관련 인텔리전스 및 대응방안

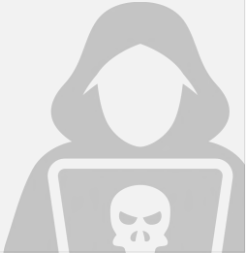
Lessons learned from Lapsus$

STRATEGY OF LAPSUS$

quaxar

초기 침투 전략

- Redline 스틸러 직접 운영하며 계정 탈취
- 딥/다크웹 포럼에서 계정 및 세션 토큰 구매
- 내부자 공모 통한 주요 계정 확보
- 확보 계정을 통해 공격 대상 내부 시스템 접근
- 추가 크리덴셜 확보하여 2차 인증 또는 암호 복구 기능 통해 MFA 우회
  (이후 IP / MAC 인증도 우회하였다고 주장)
- SIM 스와핑 공격 수행을 통해 SMS 기반 MFA 인증 우회

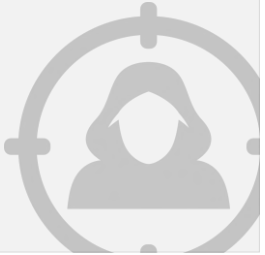


침투 후 내부 정보 획득 및 권한 상승 전략

- AD Explorer를 이용하여 해당 네트워크 내 모든 사용자와 그룹 열거
- SharePoint, Confluence, Jira, GitLab, Github, Teams, Slack과 같은 **내부 협업 도구에 대한 검색 및 접근**

내부 방어 기법 우회 전략

- 침투한 기업으로부터 **정상 코드서명 인증서 탈취 후 악성코드 서명**에 악용
- 피해 기업 내 클라우드 환경에서 공격용 신규 가상 머신 생성
- 클라우드 인스턴스 글로벌 관리자 계정 생성



https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/


Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code

April 22, 2022 14 Comments

KrebsOnSecurity recently reviewed a copy of the private chat messages between members of the LAPSUS$ cybercrime group in the week leading up to the arrest of its most active members last month.

1. 랩서스는 **러시안마켓 (다크웹 내 계정 판매 사이트)** 등에서
   초기침투 계정 확보
2. T-Mobile 의 강력한 고객 관리도구인 Atlas 접근 성공 후 **심스와핑**
3. 랩서스는 Atlas를 이용해 FBI, 국방부 관련 정부요원정보를 확인
4. T-Mobile의 Slack과 Bitbucket 계정 확보
   이후, T-Mobile 내부 **3만개 이상의 레포지토리**에서 소스코드 다운로드
5. 랩서스 그룹은 내부 멤버 Mox를 겁주기 위해 그의 신상과 거주지를 확인하고
   미리 확보해둔 미국 경찰의 Identity를 이용해 **Apple 의 EDR (Emergency Data Request)**
   요청을 악용하여 Mox의 실제 이름도 알아낼수 있다고 협박함
6. **Genesis 마켓**에서는 EA의 초기 침투 계정을 확보함
7. **Krebs가 제시하는 기업들의 대응방안**

What's even more remarkable is that anyone can access dark web bot shops like Russian Market and Genesis, which means larger companies probably **should be paying someone to regularly scrape these criminal bot services, even buying back their own employee credentials to take those vulnerable systems off the market**. Because that's probably the **simplest and cheapest incident response** money can buy.

b. 요약: **딥다크웹 마켓에서 유출 계정들 구매해라 (회수해라)**

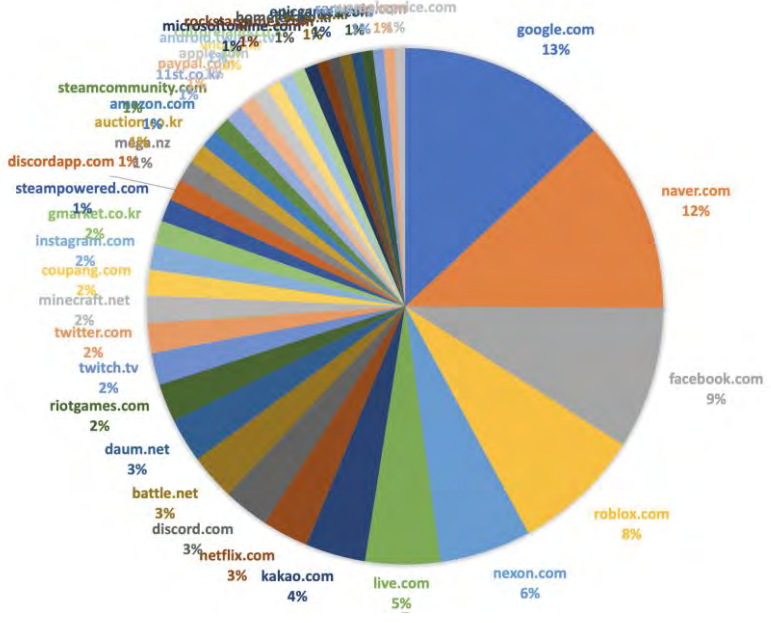
랩서스 그룹 관련 인텔리전스 및 대응방안

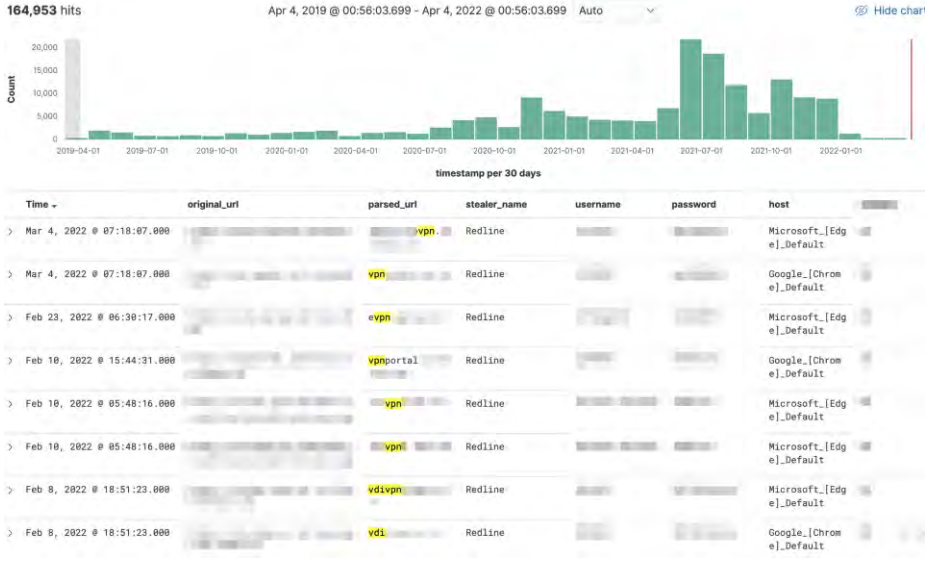
Lessons learned from Lapsus$

ANTICIPATION & MITIGATION

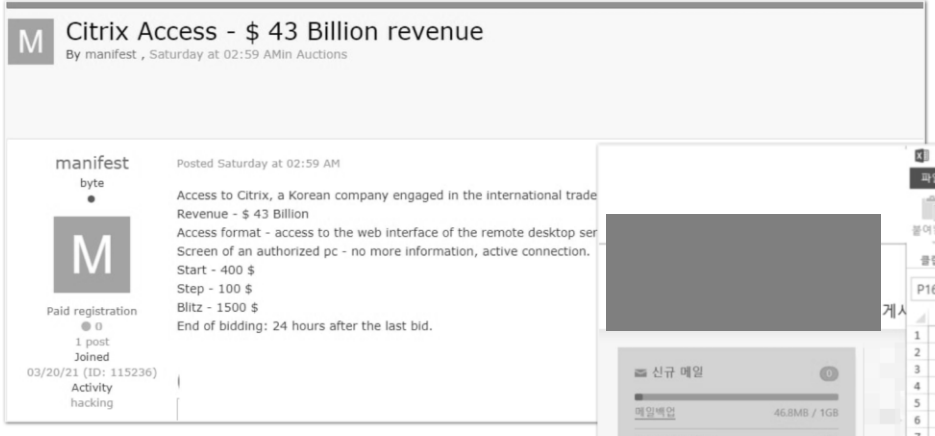
quaxar

- 2020년, Maze 랜섬웨어를 기점으로 수많은 Copycat 랜섬웨어 그룹들이 생겼음
- 랩서스의 초기 침투 전략을 Copycat 하는 많은 공격 그룹이 생겨날 것으로 예상됨
- 랩서스 초기 침투 전략의 핵심: **유출 계정 악용, MFA (Multi Factor Authentication) 우회**
- 다크웹 내 유출 계정 (국내 기준 총 400만여개)





다크웹 유출 계정 악용한 국내 사고 사례



다크웹 내 기업 VPN 계정 판매글

- **피해기업 매출: 48조**
- **한국 회사라고 설명**

판매자가 첨부한 해킹 증명 자료

quaxar

다크웹 유출 계정 악용한 해외 사고 사례

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 5, 2021, 4:58 AM GMT+9

The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked, he

Colonial Pipeline

By Darkside Ransomware

EA

By LAPSUS$

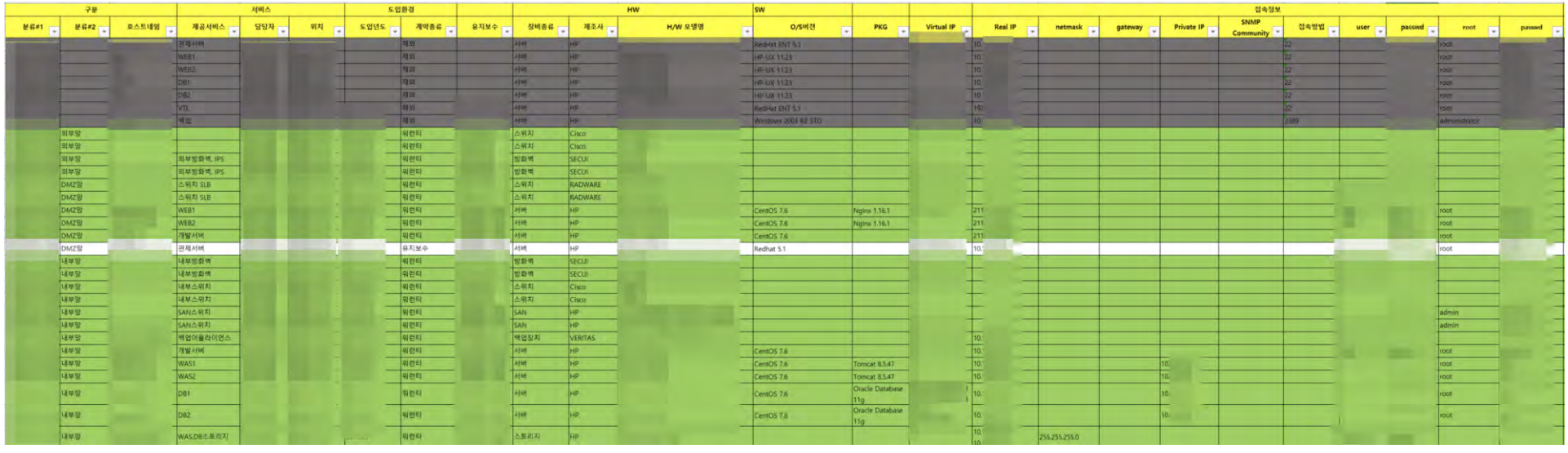
The cost of the EA data breach: $10 and a bit of social engineering

Facepalm: The hackers responsible for the recent data breach involving Electronic Arts have divulged how they did the deed. A representative for the hacking group told Motherboard they got the ball rolling by purchasing stolen cookies online for just $10. Ouch.

quaxar

스틸러 악성코드 관련 국내 사고 사례

- 외주 직원 스틸러 감염으로 인한 고객사 내부 인프라 정보 유출

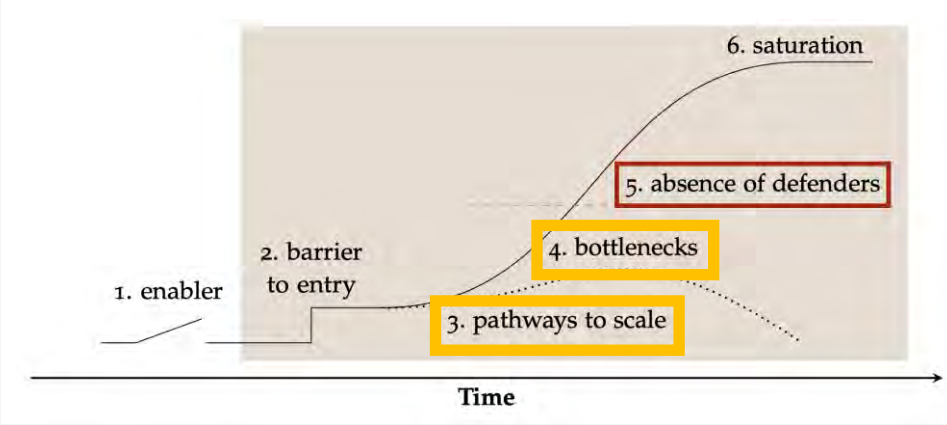


구분			서비스			도입환경			HW			SW			접속정보									
분류#1	분류#2	호스트네임	제공서비스	담당자	위치	도입년도	계약종류	유지보수	장비종류	제조사	H/W 모델명	O/S버전	PKG	Virtual IP	Real IP	netmask	gateway	Private IP	SNMP Community	접속방법	user	passwd	root	paswd
			관제서버				재외		서버	HP		RedHat ENT 5.1			10.					22			root	
			WEB1				재외		서버	HP		HP-UX 11.23			10.					22			root	
			WEB2				재외		서버	HP		HP-UX 11.23			10.					22			root	
			DB1				재외		서버	HP		HP-UX 11.23			10.					22			root	
			DB2				재외		서버	HP		HP-UX 11.23			10					22			root	
			VTL				재외		서버	HP		RedHat ENT 5.3			192					22			root	
			백업				재외		서버	HP		Windows 2003 R2 STD			10.					3389			administrator	
	외부망						위런티		스위치	Cisco														
	외부망						위런티		스위치	Cisco														
	외부망		외부방화벽, IPS				위런티		방화벽	SECUI														
	외부망		외부방화벽, IPS				위런티		방화벽	SECUI														
	DMZ망		스위치 SLB				위런티		스위치	RADWARE														
	DMZ망		스위치 SLB				위런티		스위치	RADWARE														
	DMZ망		WEB1				위런티		서버	HP		CentOS 7.6	Nginx 1.16.1		211								root	
	DMZ망		WEB2				위런티		서버	HP		CentOS 7.6	Nginx 1.16.1		211								root	
	DMZ망		개발서버				위런티		서버	HP		CentOS 7.6			211								root	
	DMZ망		관제서버				유지보수		서버	HP		Redhat 5.1			10.								root	
	내부망		내부방화벽				위런티		방화벽	SECUI														
	내부망		내부방화벽				위런티		방화벽	SECUI														
	내부망		내부스위치				위런티		스위치	Cisco														
	내부망		내부스위치				위런티		스위치	Cisco														
	내부망		SAN스위치				위런티		SAN	HP													admin	
	내부망		SAN스위치				위런티		SAN	HP													admin	
	내부망		백업어플라이언스				위런티		백업장치	VERITAS					10.									
	내부망		개발서버				위런티		서버	HP		CentOS 7.6			10.								root	
	내부망		WAS1				위런티		서버	HP		CentOS 7.6	Tomcat 8.5.47		10.				10				root	
	내부망		WAS2				위런티		서버	HP		CentOS 7.6	Tomcat 8.5.47		10.				10				root	
	내부망		DB1				위런티		서버	HP		CentOS 7.6	Oracle Database 11g		10.				10				root	
	내부망		DB2				위런티		서버	HP		CentOS 7.6	Oracle Database 11g		10.				10				root	
	내부망		WAS,DB스토리지				위런티		스토리지	HP					10.		255.255.255.0							

quaxar

"Silicon Den: Cybercrime is Enterpreneurship", Ross Anderson (Cambridge)

- LAPSUS$의 현재 단계는 3 또는 4로 판단됨
- 올해 FBI, Interpol 등의 **국내외 수사기관 vs LAPSUS** 의 결과가 중요한 분수령이 될 것으로 판단됨



<Trajectory of a new crime type>

SEEKING INFORMATION

LAPSUS$

Cyber Intrusions of United States-Based Technology Companies
March 21, 2022

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of computer networks belonging to United States-based technology companies.

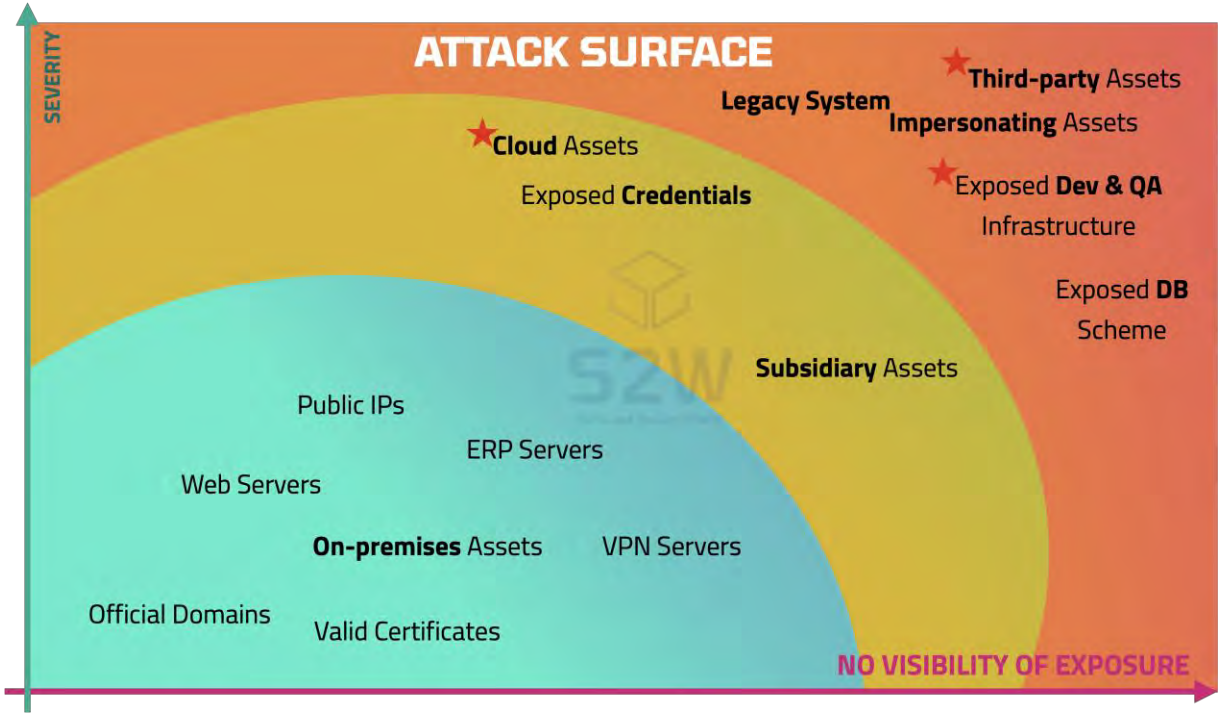
On March 21, 2022, individuals from a group identifying themselves as Lapsus$ posted on a social media platform and alleged to have stolen source code from a number of United States-based technology companies. These unidentified individuals took credit for both the theft and dissemination of proprietary data that they claim to have illegally obtained. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

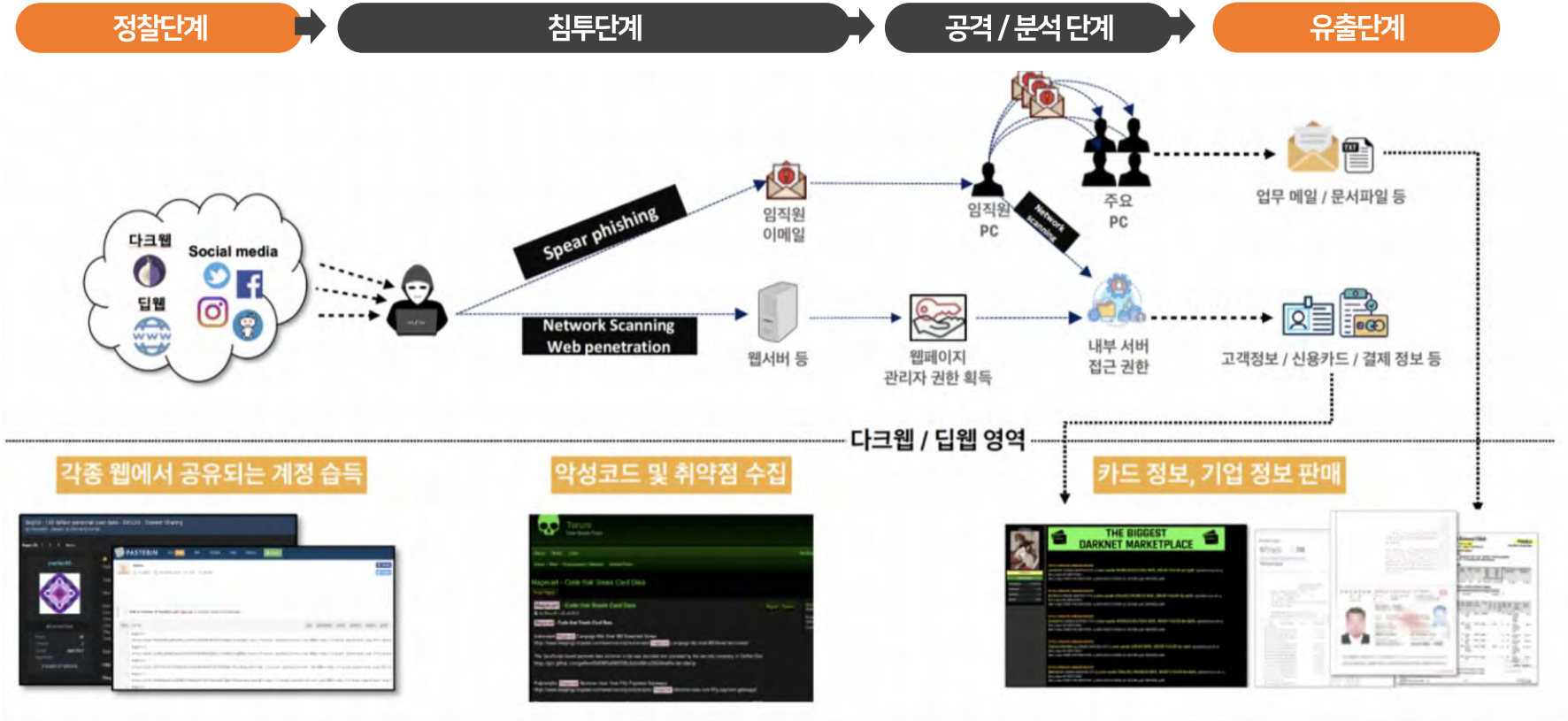
Field Office: San Francisco

quaxar

- 기업 내부에서 식별 하지 못하고 있는 수많은 공격 표면 (서버, 서비스, 외주 업체 관리 데이터, 외주 업체 직원, 퇴사자 등)이 존재함
- 공격자는 방어가 제대로 갖춰져 있지 않은 공격 표면에서 정보 취득 또는 침투 공격 거점으로 활용
- 우리회사에서 식별되지 않고 있는 자산은 무엇이 있는지 지속적인 모니터링 필요 **(Attack Surface Management)**



정찰 / 유출 단계에 대한 가시성 확보

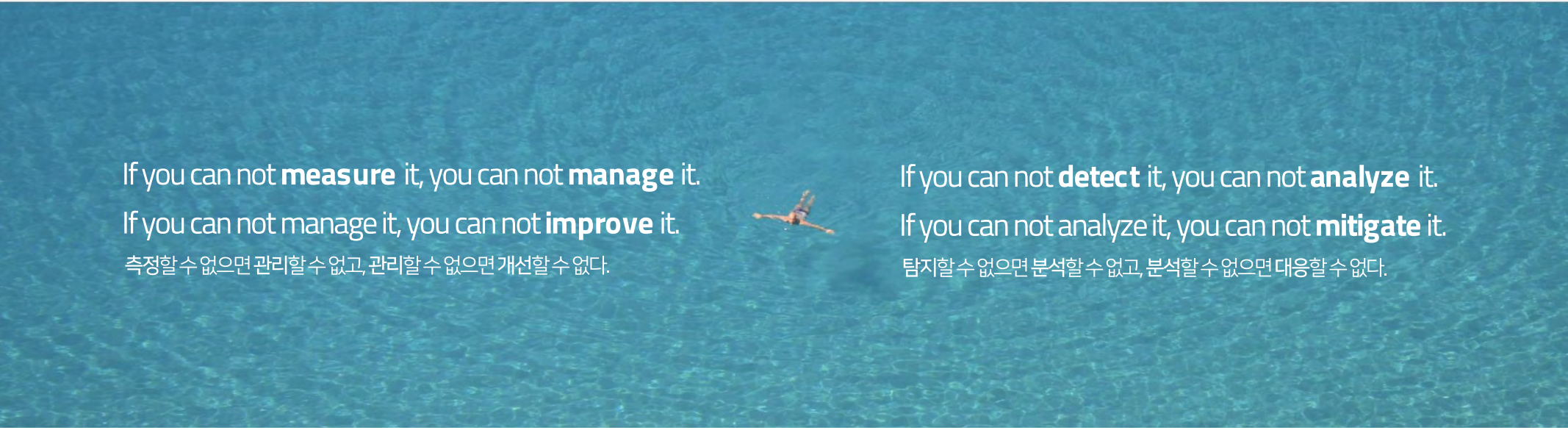


랩서스 그룹 관련 인텔리전스 및 대응방안

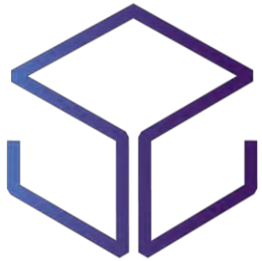
Lessons learned from Lapsus$

CONCLUSION

quaxar



정보와 자산에 대한 가시성 확보는 보안의 부수적 / 수동적 활동이 아니라 **필수적 / 결정적 활동**



S2W

Safe and Secure World

For any inquiries, please contact
info@s2w.inc