SK 쉴더스

EQST

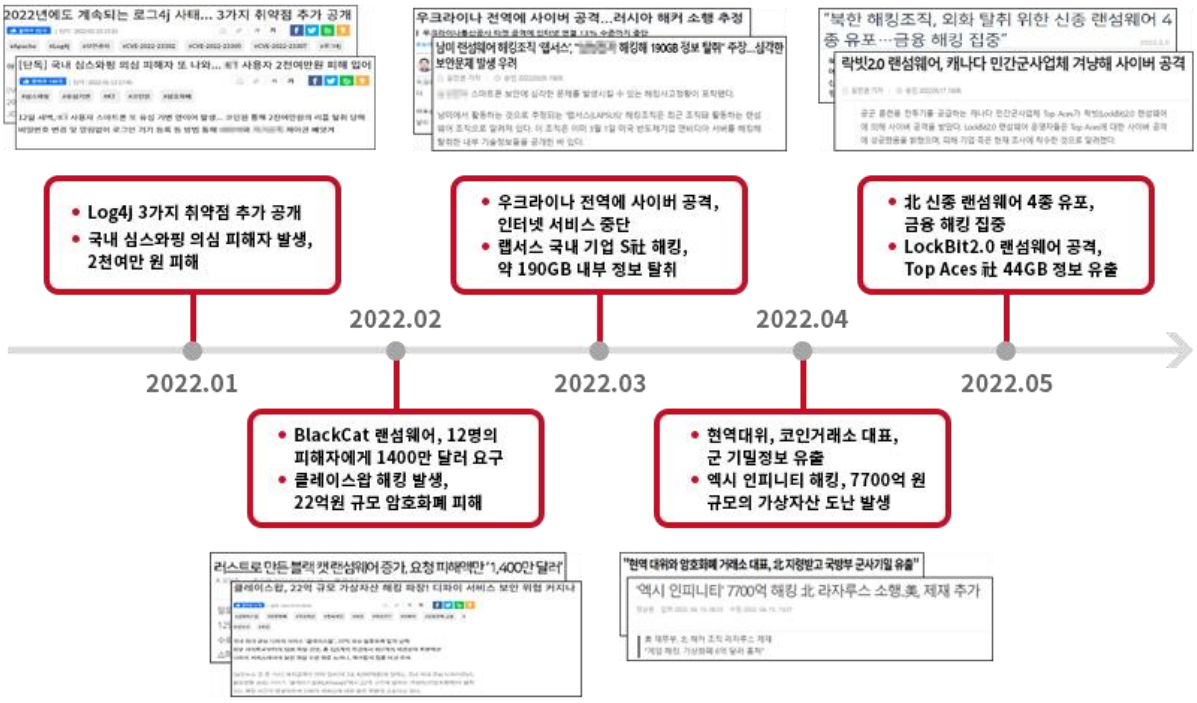
2022 상반기 보안 트렌드

Contents

EQST insight

2022년 상반기 보안 트렌드 리뷰

2022년 상반기 주요 보안 이슈 및 사건



[22년 상반기 보안 이슈 및 사건]

올해 상반기에는 작년에 이어 서비스형 랜섬웨어[1]인 RaaS(Ransomware-as-a-Service)가 지속적으로 발생했고, 가상자산을 타깃으로 한 해킹 사례가 주를 이루었다.

1 월에는 Log4j 와 관련된 취약점이 추가로 공개되었다. 작년 12 월 자바 로깅 라이브러리인 Log4j 에서 강한 파급력을 가진 취약점이 발견된 이후, 관련 취약점이 꾸준히 제보되고 있다. 4 월에는 전 세계적으로 이용되는 Spring Framework 에서 Spring4Shell 이라는 별칭을 가진 고위험도 제로데이가 연달아 발견되면서 국내외에서 큰 이슈가 되었다.

[1] 서비스형 랜섬웨어: 개발자가 랜섬웨어를 제작하여 판매하고, 공격자는 이를 구매하여 유포하는 형태로 공격에 성공할 경우 수익을 나눠가지는 구조

또한, 유출된 개인정보를 이용하여 통신사를 속이고 피해자의 USIM 을 발급하여 가상자산을 빼돌린 심스와핑(SIM Swapping) 사건이 국내 최초로 발생했다. 다수 사람들이 공격을 받았으며 주로 가상자산을 탈취당하는 피해를 입은 것으로 밝혀졌다.

2 월에는 국내 최대 DeFi(Decentralized Finance) 서비스인 KLAYswap [2] 에서 해킹이 발생했다. 공격자는 BGP Hijacking [3] 기법을 통해 네트워크 흐름을 조작하여 정상 SDK 파일로 위장한 악성코드를 다운로드하게 하였다. 악성코드가 설치된 피해자가 거래를 이용할 시 공격자의 가상자산 지갑으로 자산이 전송되는 형태로 공격이 이루어졌으며, 이로 인해 발생한 피해액은 22 억 원 규모에 달했다.

또한, BlackCat 랜섬웨어 그룹은 12 명의 피해자에게 총 1,400 만 달러를 요구하였고 비용을 지불하지 않을 시 DDoS 공격을 수행할 것이라고 협박했다. BlackCat 랜섬웨어 그룹은 기존에는 사용되지 않던 러스트(Rust) 언어를 사용하여 랜섬웨어를 제작하고 이를 공격에 사용하고 있다. 러스트로 제작된 랜섬웨어는 리눅스와 윈도우 시스템에서 모두 실행될 수 있어 범용성이 뛰어나고 많이 알려지지 않은 언어이기에 보안 시스템 우회에 용이하며, 리버스 엔지니어링을 이용한 분석에 어려움을 주고 있다.

3 월에는 러시아가 우크라이나를 침공하면서, 위성 통신망 해킹 및 사회기반시설에 대한 공격을 시도하였고 이로 인해 인터넷이 연결되지 않거나, 전기가 공급되지 않는 등의 피해를 입었다는 보도가 이어졌다. 이제는 사이버 보안이 국가 안보에 필수적인 요소이며 사이버 공격에 대한 대비의 중요성을 강조하는 직접적인 사례가 되었다.

또한, 남미의 해킹 그룹 랩서스가 국내외 대기업을 노린 공격이 포착되었다. 국내 S 社에서 190GB 의 소스코드가 유출되었으며, L 社에서 임직원 이메일 계정 정보가 탈취되었다. 국외의 그래픽 제조업체 N 社를 대상으로 회로도, 펌웨어 등 중요정보가 포함된 1TB 의 데이터가 탈취되기도 했다. 랩서스는 다크웹을 통해 임직원의 계정을 구매하거나 악성 메일을 통해 계정 정보를 획득한 뒤 내부 시스템에 침투하여 내부 정보를 탈취한 것으로 확인되었다.

4 월에는 현역 장교가 4,800 만 원가량의 가상자산을 받고 북한 해커에게 군 기밀정보 유출을 시도한 정황이 발견되었다. 기존의 해커가 악성코드를 이용하여 해킹을 시도한 것과 달리 군 현역 장교를 직접 포섭하였고, 디스코드, 텔레그램과 같은 암호화 채널을 이용하여 더욱 은밀하게 포섭을 시도할 수 있었던 것으로 보인다.

또한, 북한 소속 해킹 부대인 '라자루스'가 블록체인 기반 온라인 게임 엑시 인피니티를 해킹하여 7,700 억 원 규모의 가상화폐를 탈취했다. 엑시 인피니티는 자체 제작한 로닌 네트워크를 사용하여 이더리움 기반으로 거래를 진행하는데, 로닌 네트워크에 존재하는 취약점을 이용하여 가상화폐를 탈취했다. 미 국무부는 탈취한 7,700 억 원 중 1,100 억 원가량이 라자루스가 소유한 가상자산 지갑으로 이동했음을 확인했다고 전했다.

5 월에도 라자루스의 공격이 지속되었다. 사이버 보안 업체 Trellix 가 북한 당국이 외화 탈취를 위해 신종 랜섬웨어 4 종을 유포한 정황을 포착했다고 발표했다. 발견된 랜섬웨어에서는 북한 소속 해킹 부대 '라자루스'가 개발한 VHD 랜섬웨어와 유사한 소스 코드가 발견되었다. 또한, 랜섬웨어에 감염 후

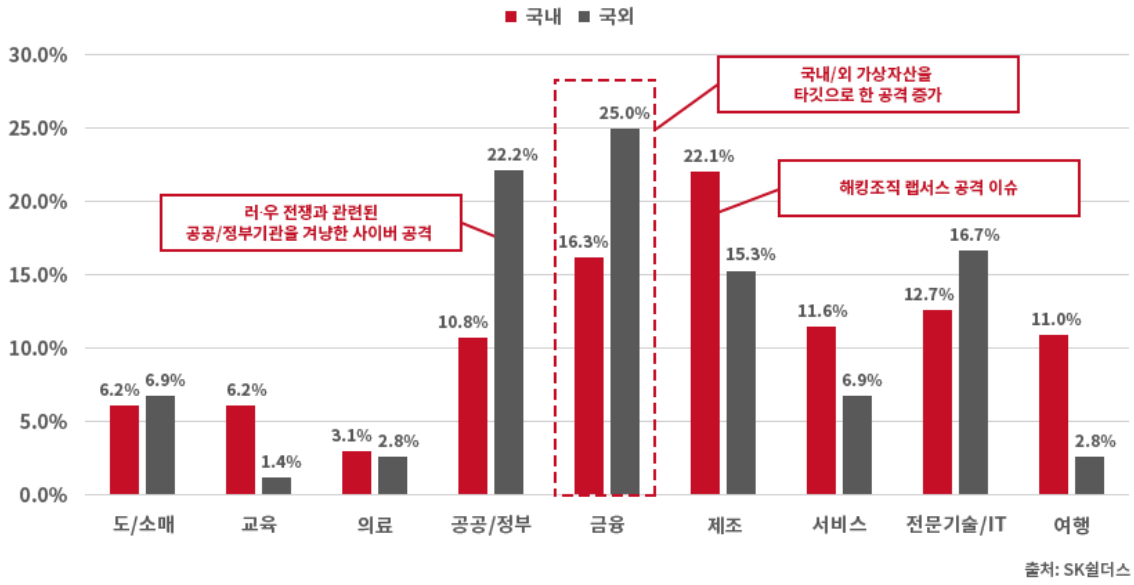
[2] KLAYswap: 국내 K 社의 블록체인 플랫폼 클레이튼(Klaytn)을 기반으로 한 DeFi 서비스

[3] BGP hijacking: BGP 라우터에 침투하여 지속적인 브로드 캐스트를 통해 라우팅 테이블 정보를 조작

금전을 요구하는 협박 메시지의 이메일 주소가 이전에 사용되었던 이메일 주소와 동일하거나 유사한 점을 근거로 북한 당국과의 연관성이 드러났다고 지적했다.

또한, 캐나다 민간 군사 업체(Top Aces 社)가 LockBit2.0 랜섬웨어 그룹에게 공격당해 44GB 의 데이터를 유출 당했고 몸값을 지불하지 않을 시 데이터를 공개할 것이라고 협박을 당했다.

업종별 침해사고 발생 통계



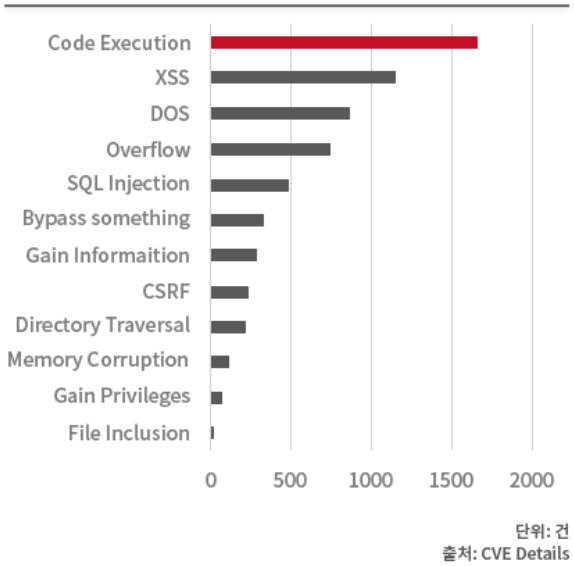
[22년 상반기 업종별 침해사고 통계]

21 년도부터 가상자산을 노리는 공격 시도가 꾸준히 증가하고 있다. 특히 22 년도부터 탈중앙화 금융(DeFi) 시스템의 사용자가 늘어났고, 가상자산을 이용한 거래가 더욱 활발해지면서 공격자의 주 표적이 되고 있다. 이에 따라 금융 업종 침해사고가 큰 비중을 차지하는 것을 볼 수 있다.

국내에서는 제조 업종의 침해사고가 가장 많이 발생했으며, 특히 해킹 그룹 랩서스가 국내 최대 제조사인 S 社, L 社의 핵심 중요 정보를 탈취하는데 성공하여 큰 이슈가 되었다.

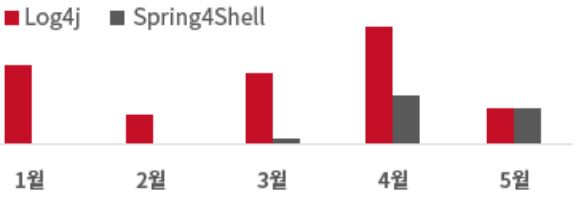
국외에서는 러·우 전쟁으로 인해 기반 시설을 노린 사이버 공격이 대대적으로 이루어져 공공/정부 침해사고가 높은 비중을 차지했다.

취약점 동향



[22년 상반기 CVE 취약점 분류]

22 년 상반기 CVE 에 등록된 취약점 분류를 살펴보면 Code Execution 이 가장 많은 비중을 차지한다. Code Execution 은 로컬 또는 원격에서 공격자가 입력한 명령어를 실행할 수 있는 취약점이다. 그 뒤로는 매년 꾸준히 발생하는 XSS, DoS, Overflow, SQL Injection 순으로 취약점이 등록되었다.



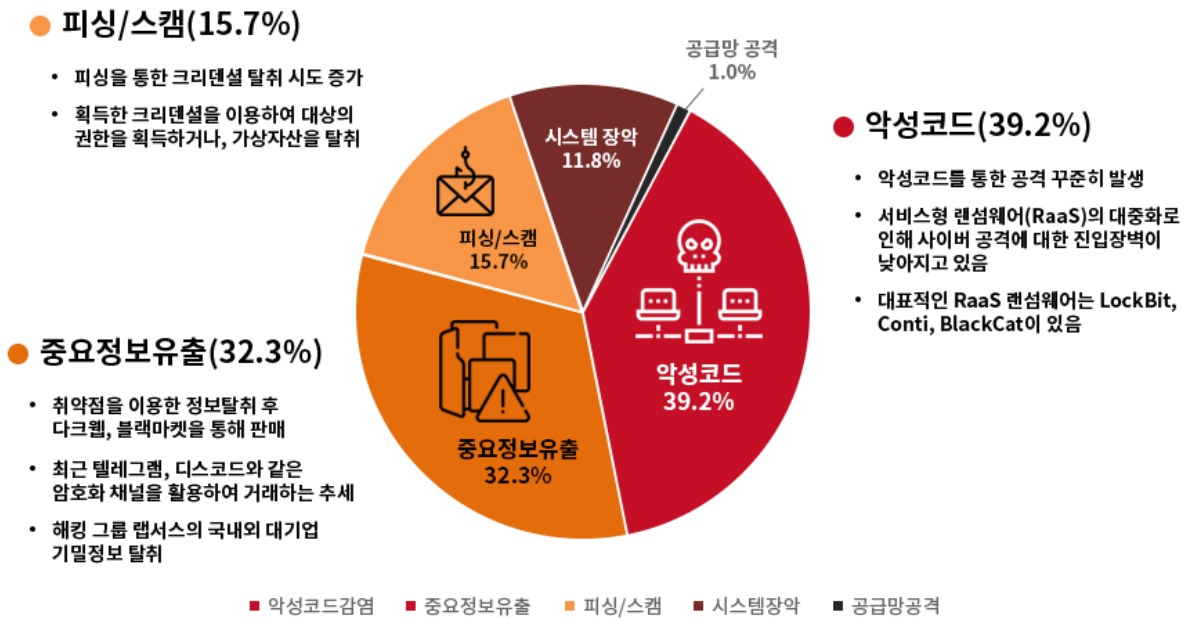
	Log4j *2021년 12월 9일 공개	Spring4Shell *2022년 3월 30일 공개
1월	40,571	-
2월	14,612	-
3월	36,197	60
4월	59,650	24,740
5월	18,179	18,221

단위: 건 (탐지 이벤트)
출처: SK쉴더스

[Log4j/Spring4Shell 이벤트 발생 통계]

등록된 Code Execution 취약점 중 가장 이슈가 되었던 취약점은 Log4j 와 Spring4Shell 이다. 자사 사이버보안관제센터 'Secudium Center'의 이벤트 탐지 분석 결과에 따르면 Log4j 공격은 2 월에 감소하는 경향을 보였으나, 추가 취약점이 발표되면서 다시 증가하는 추세를 보였다. Spring4Shell 의 경우 3 월 말에 발견되어 4 월 동안 활발하게 공격이 시도되었다. 5 월에는 공격이 감소하고 있는 추세이나 영향력이 큰 취약점인 만큼 지속적인 관심이 필요하다.

침해사고 유형별 발생 통계



[22년 상반기 침해사고 유형별 발생 통계]

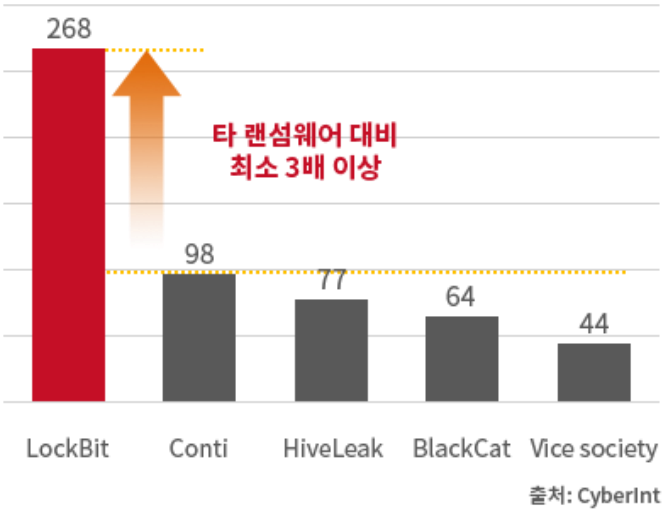
22 년 상반기 침해사고 유형별 발생 통계를 살펴보면 악성코드 감염이 39.2%로 가장 높은 비중을 차지했으며, 중요 정보 유출이 32.3%, 피싱/스캠이 15.7%을 차지했다. 그 외 시스템 장악이 11.8%, 공급망 공격이 1.0%로 뒤를 이었다.

가장 많은 비중을 차지한 악성코드 감염은 최근 성행하는 서비스형 랜섬웨어(RaaS)의 대중화와도 연관이 있다. RaaS 는 개발자가 판매한 랜섬웨어를 공격자가 구매하여 유포하고, 공격이 성공하면 수익을 재분배하는 형태이다. 랜섬웨어를 구매하여 이용하기 때문에 공격자가 악성코드 개발 역량이 부족해도 손쉽게 랜섬웨어 공격을 시도할 수 있게 도와준다. 이에 따라 사이버 공격에 대한 진입장벽이 낮아지고 있는 추세이며, 랜섬웨어 피해 규모도 크게 증가하고 있다.

악성코드 감염 다음으로 중요 정보 유출이 높은 비중을 차지했다. 주로 대상 서버의 보안 취약점을 이용하여 중요 정보를 탈취한 뒤 다크웹, 블랙마켓을 통해 판매하여 이익을 취하거나 중요 정보를 인질 삼아 금전을 요구하는 형태를 보이고 있다. 공격자들은 최근에 다크웹뿐만 아니라 텔레그램, 디스코드와 같은 암호화 채널을 활용하는 추세이며 해킹 그룹 랩서스가 글로벌 IT 기업을 해킹한 뒤 유출된 중요 정보를 빌미로 돈을 요구할 때 텔레그램을 사용한 것을 예시로 들 수 있다.

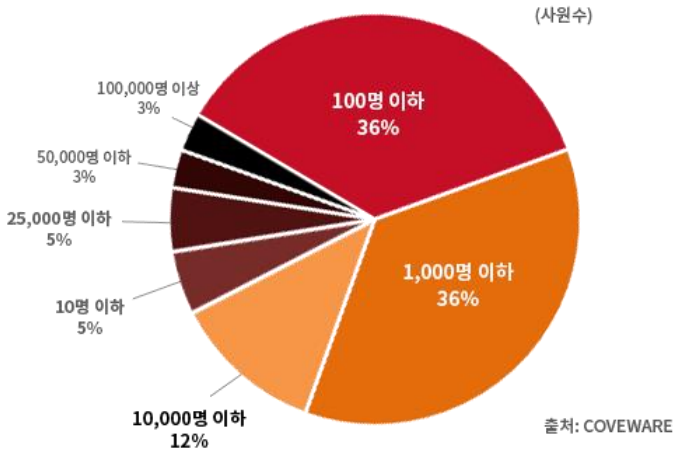
전체 비중의 15.7%를 차지한 피싱/스캠은 가상자산 탈취를 목적으로 크리덴셜 정보 수집에 주로 이용되었다. 공격자는 피싱을 통해 대상의 크리덴셜을 획득하고 이를 이용해 암호화폐 거래소에 접근, 피해자의 가상자산을 탈취한다. 가상자산 거래량이 늘어난 만큼 암호화폐 거래소 이용자를 타깃으로 한 피싱 공격이 증가하고 있어 각별한 주의를 요한다.

랜섬웨어 동향



[22년 상반기 상위 랜섬웨어 그룹]

22 년 상반기 가장 활발하게 활동한 랜섬웨어 그룹은 LockBit 으로 타 랜섬웨어 그룹보다 3 배 이상 많이 관측되었다. LockBit 의 특징은 파일을 ".lockbit" 확장자 파일로 암호화하며, 부분 암호화 기술을 사용하여 다른 랜섬웨어에 비해 암호화 프로세스 속도를 높여 가장 빠른 데이터 암호화 및 랜섬웨어 탐지 기술 우회가 가능하다. LockBit 은 2019 년 9 월부터 활동을 시작했으며 랜섬웨어 페이로드 업그레이드와 공격적인 구인, 포섭 활동을 통해 레빌과 다크사이드에 이어 가장 주목받는 랜섬웨어 위치에 올랐다. "Recorded Future"가 수집한 자료에 따르면, 올해 현재까지 최소 650 개의 조직을 공격한 것으로 파악되었다.



[22년 상반기 랜섬웨어 피해 기업 규모]

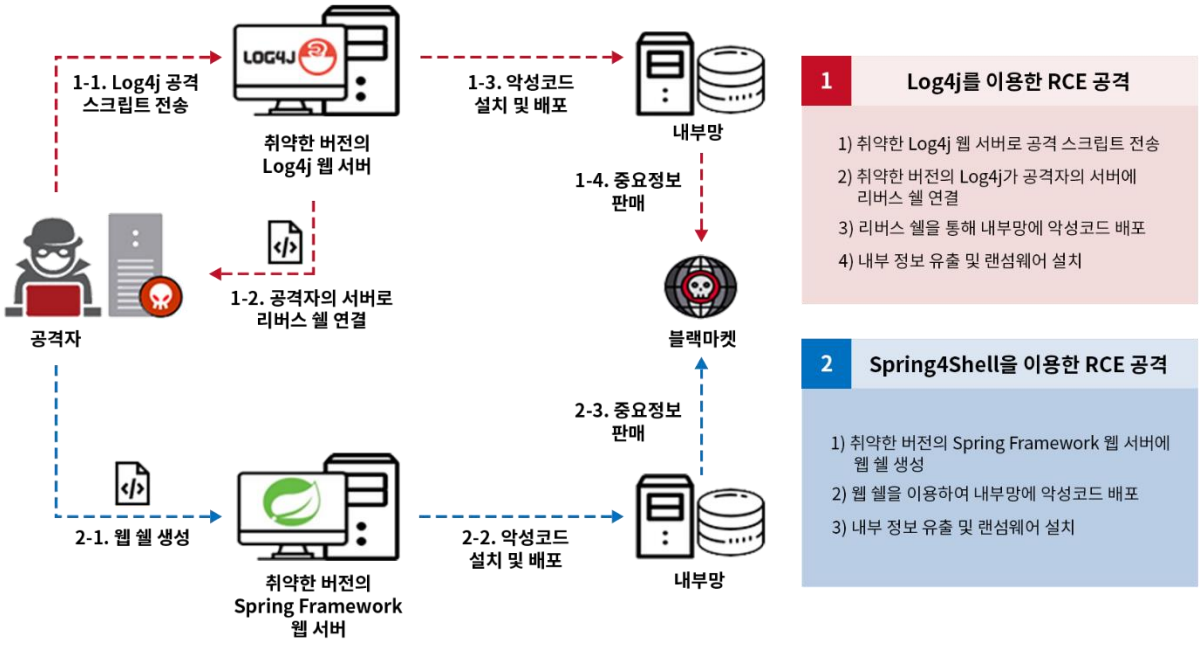
COVWARE 에서 조사한 랜섬웨어 피해 기업 규모 통계를 살펴보면, 사원수 1 천 명 이하 규모의 기업이 72%로 대부분을 차지했다. 21 년 국내 기업에 대한 랜섬웨어 피해의 93%는 중소기업이었던 것으로 보아, 상대적으로 보안이 취약한 작은 규모의 기업들이 피해를 입은 것으로 파악된다. 랜섬웨어에 대한 피해를 줄이기 위해서는 보안 솔루션을 도입하고, 주기적인 백업을 해야 한다.

SK 쉴더스에서는 랜섬웨어 원스톱 대응을 위해 올 3 월에 KARA(Korea Anti Ransomware Alliance)를 발족하여 7 개 회원사(맨디언트, S2W, 트렌드마이크로, 지니언스, 베리타스, 캐롯손해보험, 법무법인 화우)와 함께 협의체를 구성하였다. 또한, 24 시간 사고를 접수할 랜섬웨어 대응센터를 개소하고, 사고 접수부터 원인 파악, 피해 복구, 협상, 배상, 재발방지 대책 등의 모든 절차를 컨설팅 하고 있다.

※. SK 쉴더스 랜섬웨어 대응센터 : kara@sk.com, 1600-7028

제로데이 공격 시나리오

2022년 상반기의 주요 제로데이 취약점은 Log4j와 Spring4Shell이며 관련된 시나리오는 아래와 같다.



[Log4j와 Spring4Shell을 이용한 원격 명령 실행 시나리오]

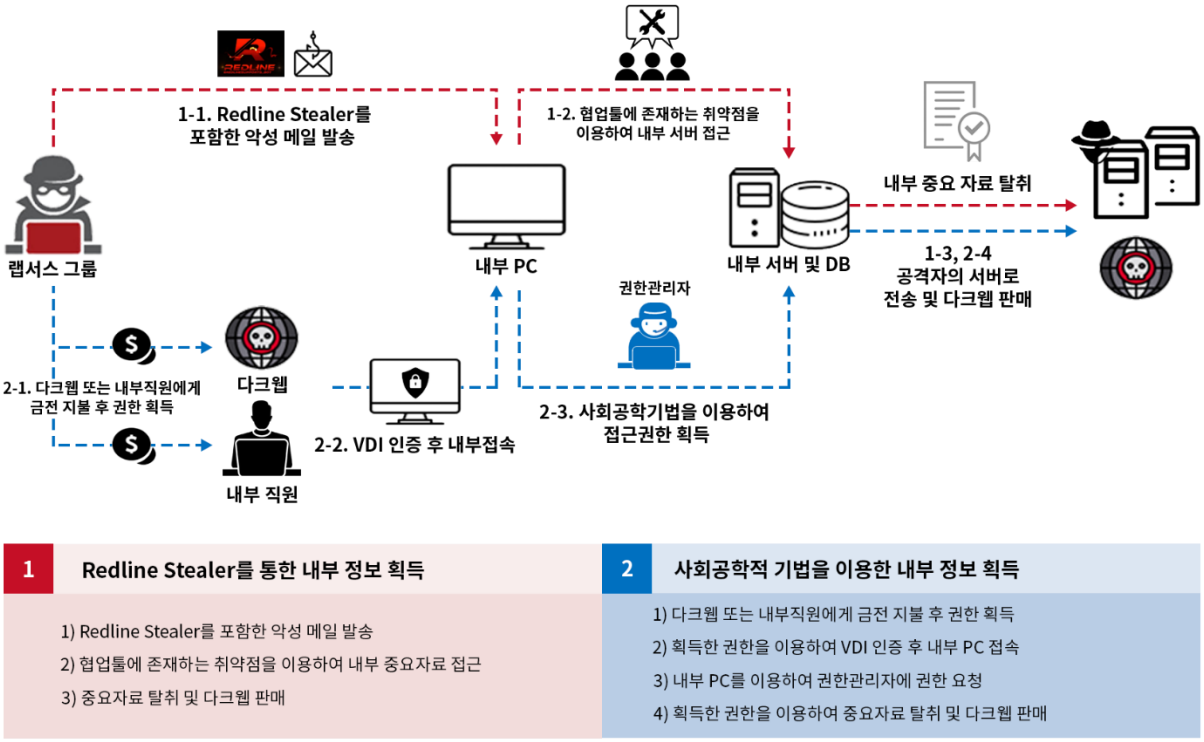
해당 공격 시나리오는 취약한 버전의 Log4j 혹은 Spring Framework 를 사용할 시 공개된 취약점을 이용해 원격 코드 실행이 가능하여 내부 정보가 유출되거나 랜섬웨어에 감염되는 시나리오다.

해커는 Log4j 를 이용한 공격을 위해 미리 악성코드 유포 서버를 준비한 후 취약한 버전의 Log4j 를 사용하는 웹서버를 탐색한다. 해커는 취약점이 발견된 웹서버에 공격 구문을 전송하여 악성코드 유포 서버에서 악성코드를 다운로드해 실행시킨다. 내부 네트워크의 제어권을 장악한 해커는 내부 중요 정보를 탈취, 블랙마켓에 판매한다.

또한 해커는 취약한 버전의 Spring Framework 를 사용하는 웹서버를 탐색 후, 발견한 웹서버에 공격 구문을 전송하여 웹 쉘을 생성시킨다. 해커는 생성한 웹 쉘을 실행시켜 내부 네트워크의 제어권을 가져온다.

랩서스 공격 시나리오

해킹 그룹 랩서스가 글로벌 IT 대기업을 대상으로 공격을 진행하여 내부 기밀자료를 탈취했다. 랩서스 그룹은 Redline Stealer[4]를 활용하여 침투하거나 다크웹 또는 내부 직원에게 구매한 접근 권한을 이용하여 기업의 내부 중요 자료를 탈취해 다크웹에 판매하는 등 피해를 입혔다.



[랩서스 공격 시나리오]

해당 공격 시나리오는 기업의 내부 서버에 침투하여 중요 정보를 탈취하고 다크웹에 판매하는 시나리오다. 1번 시나리오는 해커가 Redline Stealer를 활용하여 접근 정보를 탈취한 후 내부 PC에 접근한다. 그 후 기업에서 사용 중인 협업 툴에 존재하는 취약점을 이용하여 내부 서버로 2차 침투하여 중요 정보를 탈취한다.

[4] Redline Stealer: PC 정보, 브라우저 정보, 소프트웨어 정보, 중요 파일 등을 탈취하기 위해 만들어진 악성코드

공격에 사용되는 Redline Stealer 가 탈취하는 대표적인 정보는 다음과 같다.

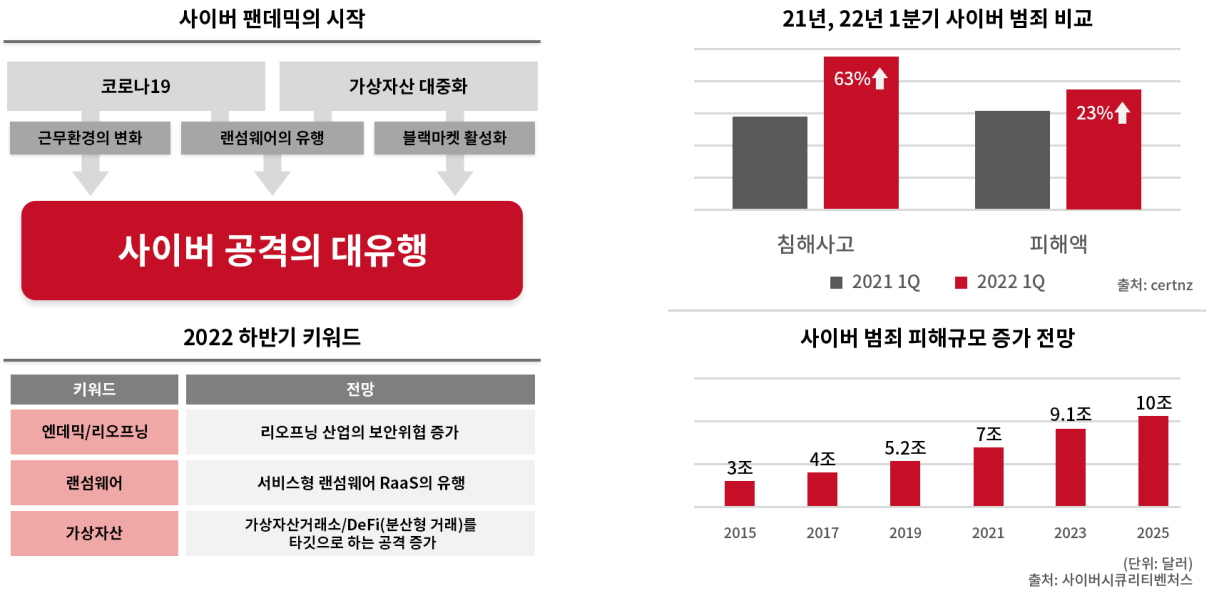
구분	내용
PC 정보	IP 주소, OS 버전, 백신 프로그램, 실행 중인 프로세스, 설치된 프로그램, 설치된 브라우저 등
브라우저 정보	Edge, Chrome, ChromePlus, Opera, Mozilla 등 설치된 브라우저와 브라우저에 저장된 데이터
소프트웨어 정보	RDP, FTP, VPN, Telegram, Discord, Steam 등
중요 파일	key, wallet, seed, txt, doc 등

2 번 시나리오에서 해커는 다크웹에서 내부 PC 에 대한 계정 정보를 구입하거나 내부 직원을 포섭하여 계정 정보를 획득한 후 내부 PC 에 접근한다. 그 후 정상적인 이용자로 가장하여 중요 정보 접근 권한을 획득한 후 내부 중요 정보를 탈취한다.

공격자는 탈취한 정보를 다크웹에 판매하거나 유출을 미끼로 협박을 통해 금전을 획득한다.

사이버 팬데믹 전망과 보안 위협

사이버 팬데믹 개요



[사이버 팬데믹 개요]

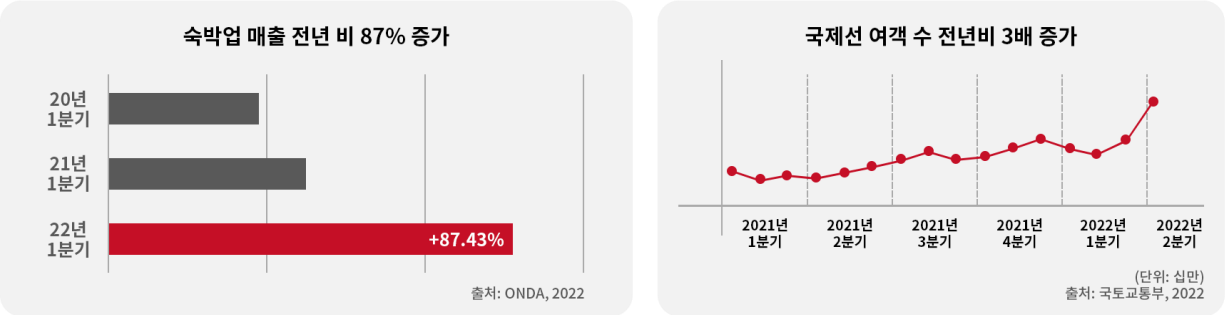
코로나19 이후 디지털 전환의 가속화, 가상자산 대중화의 영향으로 사이버 팬데믹이 시작되었다.

21년 1분기와 22년 1분기에 발생한 사이버 범죄를 비교해 보면 침해사고는 전년대비 63%, 피해액은 전년대비 23% 증가하였다. 사이버 범죄의 피해 규모 역시 2015년 이후 매년 증가하고 있으며, 2025년에는 10조 달러에 이를 것으로 예상된다.

이에 EQST그룹은 22년 하반기 주목해야 할 키워드를 리오프닝, 가상자산, 랜섬웨어로 정리했으며 이와 관련된 보안 현황을 분석하여 앞으로 발생 가능한 다양한 위협들을 정리했다.

사이버 팬데믹 현황 – 리오프닝

첫 번째 키워드는 **리오프닝**이다. 리오프닝은 코로나19로 인해 위축되었던 경제활동이 재개되는 현상을 뜻하며, 숙박, 항공, 여행, 운송 등의 산업이 활성화되고 있다. 대표적인 리오프닝 산업인 숙박업은 매출이 전년 대비 87% 증가하였으며, 항공업에서는 국제선 여객 수가 전년 대비 3배 이상 증가하였다.

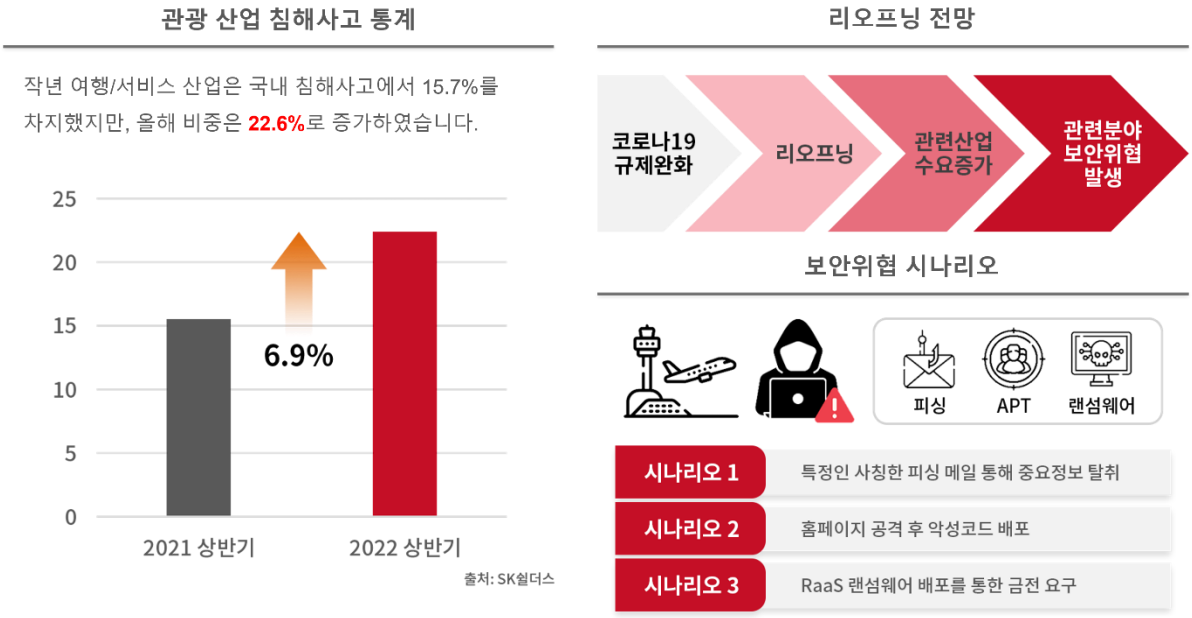


[리오프닝 관련 산업 수요 증가]

리오프닝 전망 및 보안 위협

리오프닝 관련 산업들의 수요가 늘어나고, 매출액이 늘어나면서 관련 산업들을 타깃으로 한 보안 위협이 꾸준히 증가할 것으로 보인다. 21년 국내 침해사고 중 여행/서비스 산업이 차지하는 비중은 15.7%였지만, 22년 상반기에는 22.6%로 전년 대비 6.9%가 증가하였다.

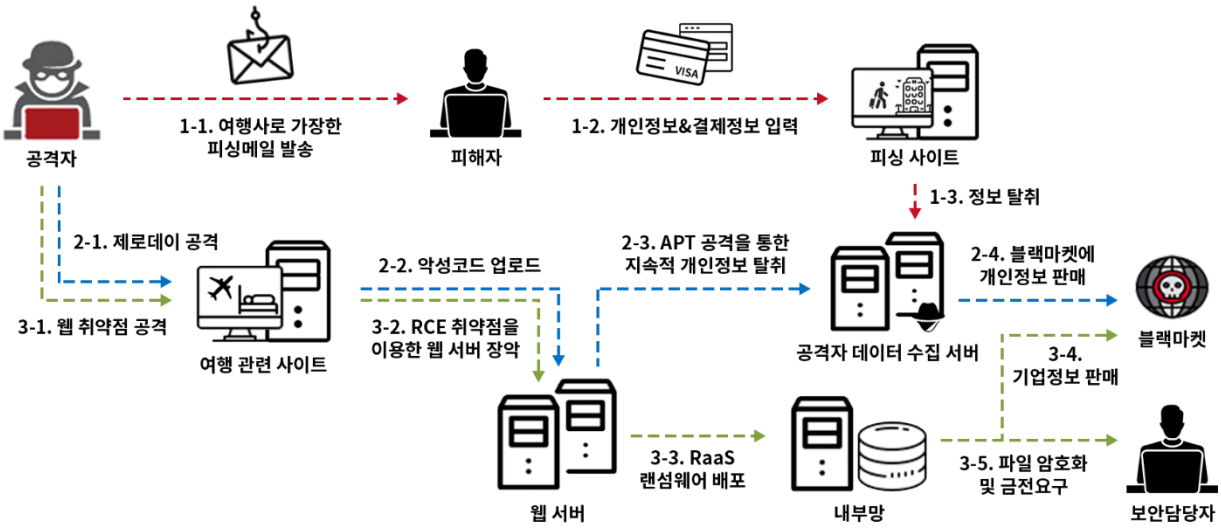
코로나19 기간 동안 해당 산업 군들은 매출 감소로 인해 산업 전반에 걸쳐 인원이 감축되었고, 보안을 관리하는 인원 역시 축소되었다. 이러한 허점을 노린 공격자들의 손쉬운 공격 대상이 될 수 있으므로 각별한 주의가 필요하다.



[리오프닝 전망]

리오프닝 공격 시나리오

공격 방법에 따라 피싱, APT, 서비스형 랜섬웨어를 이용한 공격 시나리오로 분류했다.



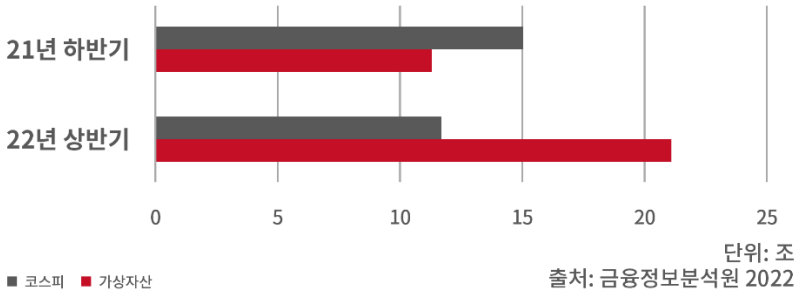
1 피싱을 통한 중요정보 획득	2 APT 공격을 통한 개인정보 탈취	3 서비스형 랜섬웨어(RaaS) 공격
1) 여행사 이벤트로 위장한 피싱메일 발송 2) 피싱 사이트에 중요정보 입력 3) 입력된 중요정보 탈취	1) 제로데이 공격을 통한 APT 악성코드 업로드 2) 악성코드를 통한 지속적인 중요정보 탈취 3) 획득한 정보 블랙마켓 판매	1) 웹 취약점을 이용하여 원격명령실행 2) 내부망에 서비스형 랜섬웨어 유포 3) 중요정보 탈취 및 핵심 파일 암호화 4) 보안 담당자에게 금전 요구

[리오프닝 공격 시나리오]

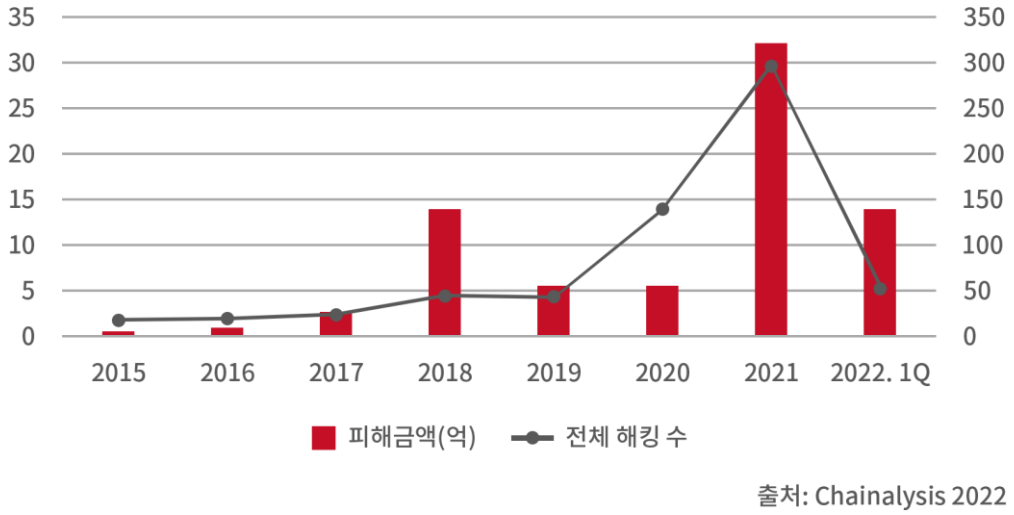
사이버 팬데믹 현황 – 가상자산

두 번째 키워드는 **가상자산**이다. 21 년 하반기에는 코스피 일일 거래량보다 가상자산 일일 거래량이 적었으나, 22 년 상반기 가상자산 일일 거래량이 코스피 일일 거래량을 추월하였다. 유가증권 시장과 가상자산 시장간 거래대금의 차이가 벌어지고 결국 가상자산이 유가증권 시장의 거래대금을 넘어선 것은 가상자산에 대한 관심도와 거래량이 증가한 것이 원인이라고 볼 수 있다.

또한 가상자산에 대한 피해액이 매년 증가 추세를 보이고 있으며, 20 년 대비 21 년에 급증했다. 21 년 1 월부터 가상자산 거래소 이용자 및 가상자산 거래량이 급증하면서 가상자산이 공격자들의 주요 타깃 중 하나가 되었고 가상자산을 노린 해킹 공격이 증가한 것이다. 가상자산이 대중화되고 다수의 이용자들 사이에서 거래가 이루어지는 만큼 가상자산을 노린 공격은 앞으로도 계속 지속될 것으로 전망된다.



[가상자산 거래 증가]



[가상자산 피해액 증가]

아래의 사고 사례 타임라인을 보면 가상자산을 노린 침해사고가 지속적으로 발생하고 있으며, 피해 금액 또한 천문학적인 금액임을 알 수 있다.

[가상자산 피해액 증가]

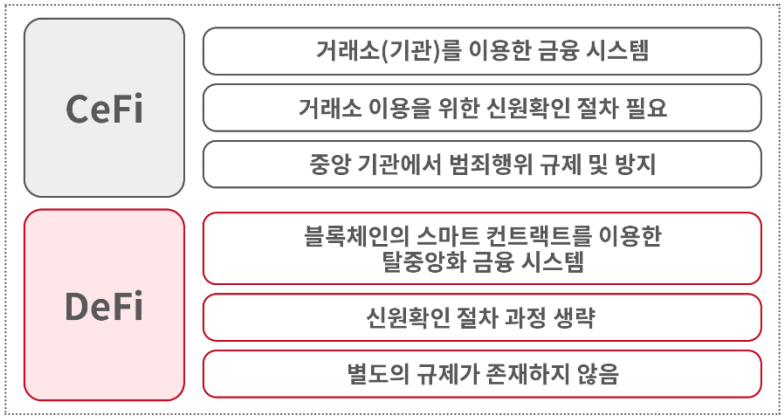
가상자산 해킹 사고는 국/내외를 가리지 않고 지속적으로 발생하고 있다.

국외 사고 사례 중 22 년 3 월에 발생한 '로닌 네트워크' 해킹 사고를 살펴보면 '액시 인피니티'라는 모바일 게임이 사용하는 로닌 네트워크가 해킹을 당했고, 약 6 억 1500 만 달러 규모의 이더리움이 탈취당했다. 로닌 네트워크는 총 9 개의 검증자 노드로 구성되어 입출금 발생 시 이들 중 5 개 이상의 노드의 승인을 받게 되어 있는데 해커가 5 개 노드의 개인키를 해킹하였고, 검증 로직 우회에 성공하여 이더리움을 탈취했다.

국내 사고 사례로는 22 년 2 월에 발생한 K 社의 DeFi 서비스 해킹이 있다. 해킹에 사용된 공격 방법은 BGP Hijacking 으로, BGP(Border Gateway Protocol) 프로토콜은 AS(Autonomous System)에서 IP 대역을 관리하고 정기적으로 라우팅 테이블을 업데이트하는 프로토콜이다. 공격자는 BGP Hijacking 공격으로 악성파일 배포 서버로 접속하도록 라우팅 테이블을 변조했고, 이용자들은 악성 SDK 를 다운로드했다. 악성 SDK 파일은 서비스 이용자의 거래 요청을 변조하여 공격자의 지갑으로 가상자산을 전송했으며, 공격자는 총 22 억 원 규모의 가상자산 탈취에 성공하였다.

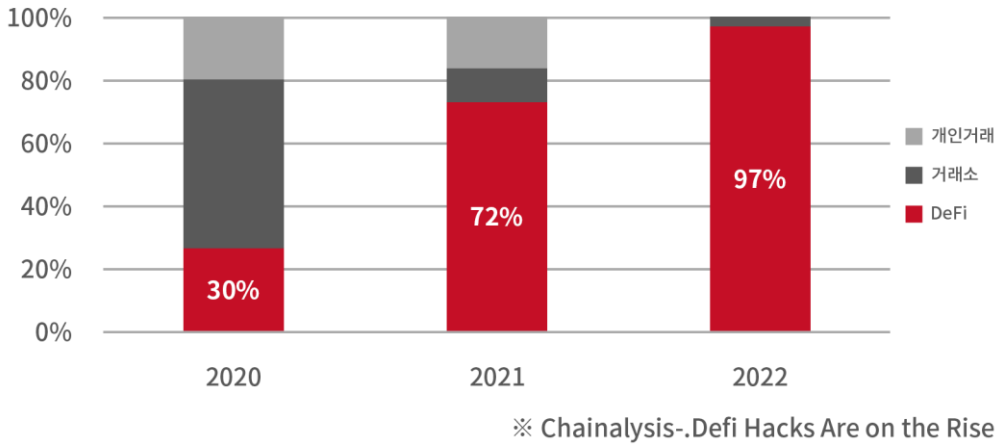
가상자산 전망 및 보안 위협

탈중앙화 금융인 DeFi(Decentralized Finance)가 등장하면서, 가상자산을 타깃으로 한 공격은 더욱 증가할 것으로 예상된다. DeFi 는 거래소(기관)를 통해 거래가 이루어지던 기존의 CeFi(Centralized Finance)와 달리 블록체인 상에서 모든 과정이 자동화되어 거래소 없이 가상화폐 간의 거래가 이루어지는 것이 특징이다. CeFi 와의 차이점은 아래와 같다.



[CeFi와 DeFi]

Chainalysis 는 22 년 상반기 동안 도난당한 가상자산이 16 억 8000 만 달러(약 2 조 1554 억 원)에 달하며, 이 중 97%는 DeFi 플랫폼을 통해 발생했다고 발표했다. 거래소에 의존하던 기존의 방식에서 탈중앙화 방식의 DeFi 시장 규모가 증가하면서 DeFi 플랫폼을 노린 공격이 증가한 것이다. 이처럼 단순히 피싱, 스미싱 등을 이용한 거래소 계정 탈취뿐만 아니라 관련 플랫폼 취약점을 이용한 공격 위협 또한 증가할 것으로 보인다.



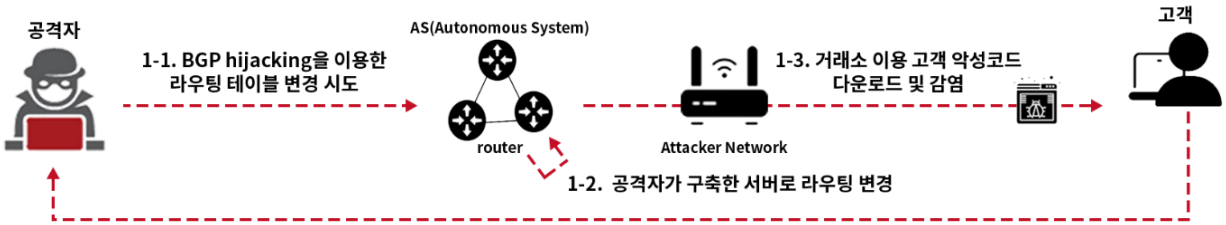
[가상자산 거래 유형별 비율]

가상자산 공격 시나리오

가상자산을 타깃으로 한 공격 시나리오는 다음과 같다.

1) BGP hijacking

* BGP hijacking: 라우터[5]들의 집합인 AS(Autonomous System)에서 라우팅 테이블[6]을 교환할 때 사용하는 BGP 프로토콜을 해킹하여 라우팅 테이블을 조작하는 공격이다. 이로 인해, 사용자가 정상적인 주소로 접속을 시도하더라도 공격자가 조작한 라우팅 테이블에 따라 공격자가 유도한 서버로 접속이 되어 악성코드를 다운받게 된다.



• BGP: Autonomous System 내에서 라우팅을 담당하는 프로토콜
• Autonomous System: 하나의 관리 도메인에 속해 있는 라우터들의 집합
• BGP hijacking: BGP 라우터에 침투하여 지속적인 브로드 캐스트를 통해 라우팅 테이블 정보를 조작

1 BGP hijacking

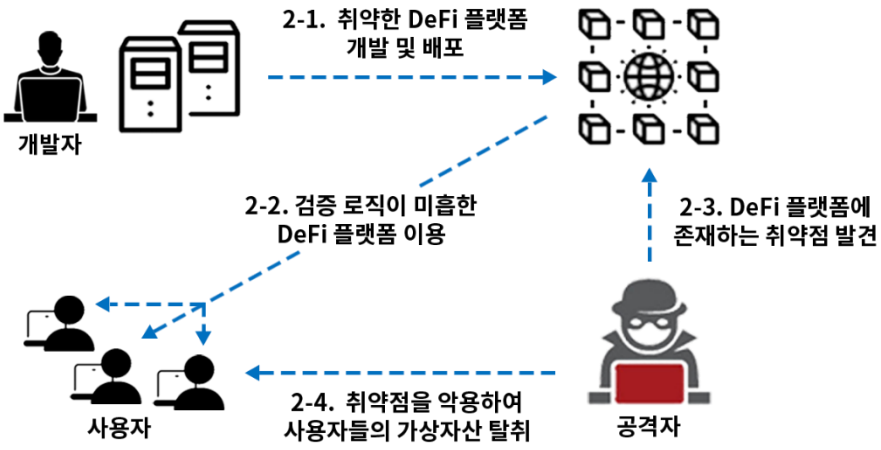
1) BGP hijacking을 이용한 라우팅 테이블 변경 시도
2) 공격자의 지속적인 브로드 캐스트로 인해 AS 내 라우팅 테이블 변경
3) 거래소 이용 시 공격자 구축 서버로 연결되어 악성코드 다운로드 및 감염
4) 악의적인 트랜잭션 전송 및 가상자산 탈취

[가상자산 공격 시나리오]

[5] 라우터: 네트워크 상에서 데이터가 전송되는 최적의 경로를 설정하고 전달하는 네트워크 장치

[6] 라우팅 테이블: 네트워크 상에서 데이터의 경로가 명시되어 있는 테이블로 라우터는 이를 참조하여 데이터를 전달함

2) 설계 오류 악용

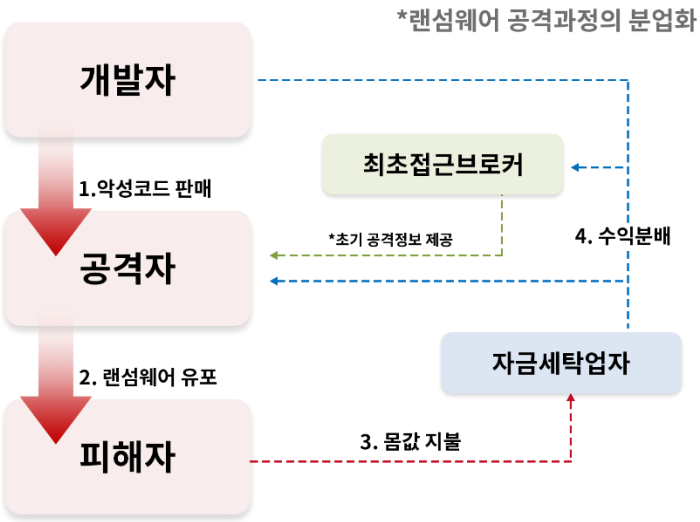


2	설계 오류 악용
	1) 버그가 존재하는 취약한 DeFi 플랫폼 개발 및 이용 2) 공격자의 플랫폼 분석 및 버그 발견 3) 해당 버그를 악용한 사용자들의 가상자산 탈취

[가상자산 공격 시나리오]

사이버 팬데믹 현황 – RaaS

세 번째 키워드인 RaaS(Ransomware-as-a-Service)는 서비스형 랜섬웨어를 뜻하며, 랜섬웨어 개발자가 랜섬웨어를 제작하여 판매하고 공격자는 이를 구매하여 랜섬웨어를 유포하는 형태로 공격에 성공할 경우 수익을 나눠 가지는 구조이다. 이로 인해 개발 역량이 없는 사람도 랜섬웨어를 쉽게 이용할 수 있게 되었고 사이버 공격에 대한 진입 장벽이 낮아졌다.

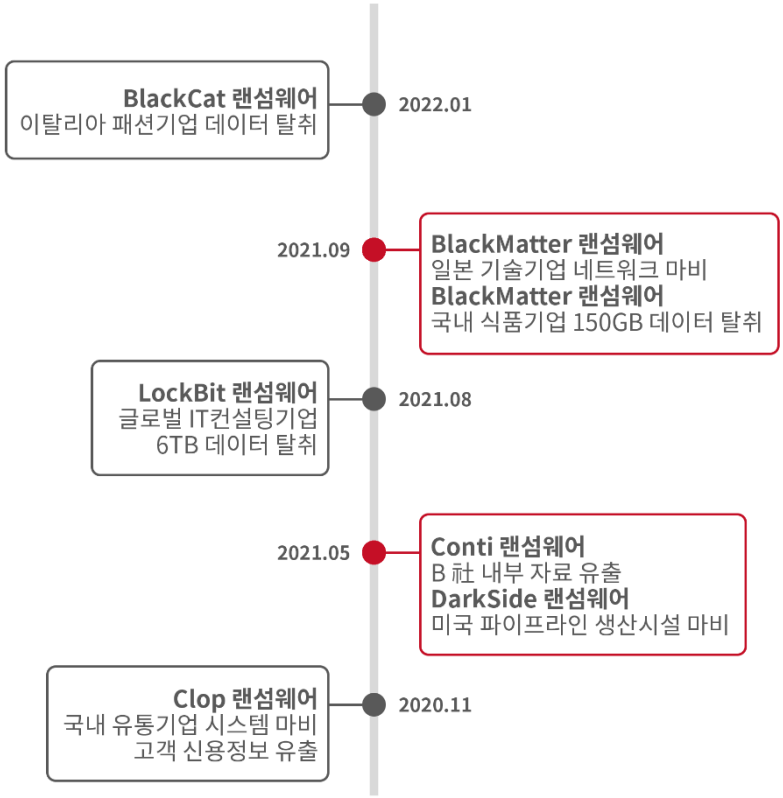


[서비스형 랜섬웨어]

대형 랜섬웨어 그룹인 Conti 역시 공격 과정이 분업화된 서비스형 랜섬웨어의 형태를 띠고 있다.

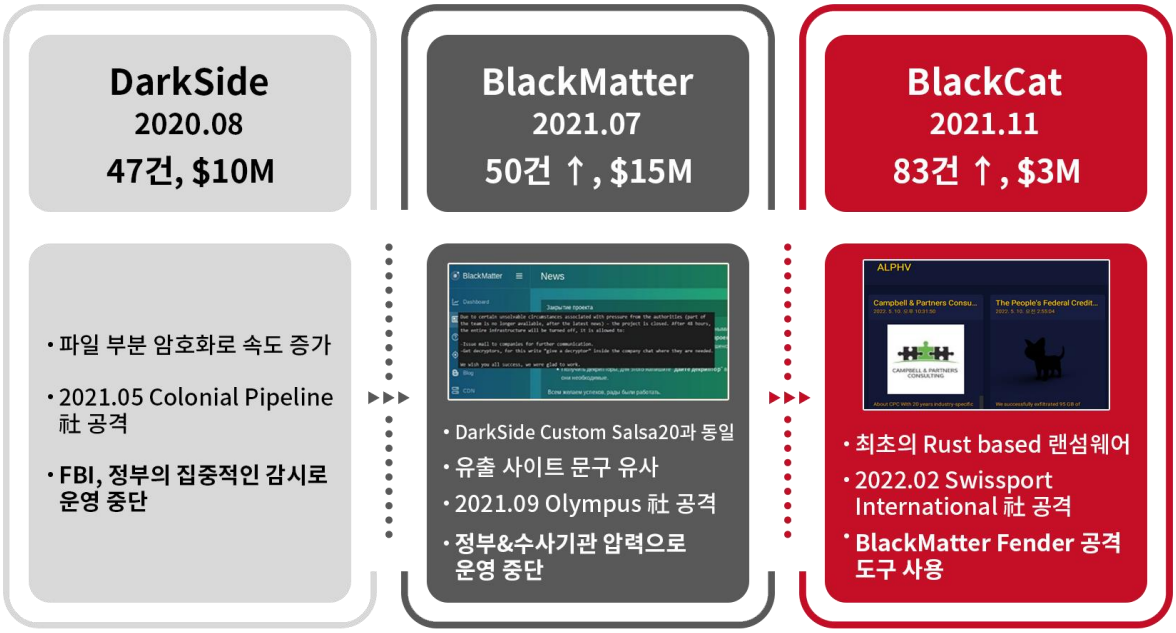
Conti 는 총괄리더를 필두로 조직을 이끌어가는 인사, 교육, 교섭 및 홍보팀을 두고 있으며, 기업을 대상으로 공격을 진행하는 실행부(침투 및 랜섬웨어 감염), 개발부(랜섬웨어 개발), 조사부(공격 대상 탐색), 해석부(타 랜섬웨어 그룹의 랜섬웨어 분석)와 이를 총괄리더와 연결해 주는 중간관리자를 두고 있는 것으로 밝혀졌다.

서비스형 랜섬웨어 주요 사고 사례 타임라인은 아래와 같으며, 꾸준히 RaaS 로 인한 피해가 발생하고 있음을 볼 수 있다.



[서비스형 랜섬웨어 사고 사례 타임라인]

20 년 말부터 서비스형 랜섬웨어가 폭발적으로 증가하기 시작했고 그로 인해 기업들의 피해가 점차 커졌다. 각국의 정부는 랜섬웨어 그룹에 대한 수사와 감시를 통해 랜섬웨어 그룹의 운영을 방해했으나, 랜섬웨어 그룹 또한 Re-Branding 을 통해 수사를 회피하기 시작했다. Re-Branding 에 대한 자세한 설명은 다음 장에서 살펴보도록 한다.



[랜섬웨어 그룹의 Re-Branding]

랜섬웨어 그룹은 Re-Branding 을 통해 정부와 수사기관의 집중 감시를 피하는 움직임을 보이고 있다. 대표적인 랜섬웨어 그룹인 BlackCat 의 Re-Branding 내역을 살펴보면 다음과 같다.

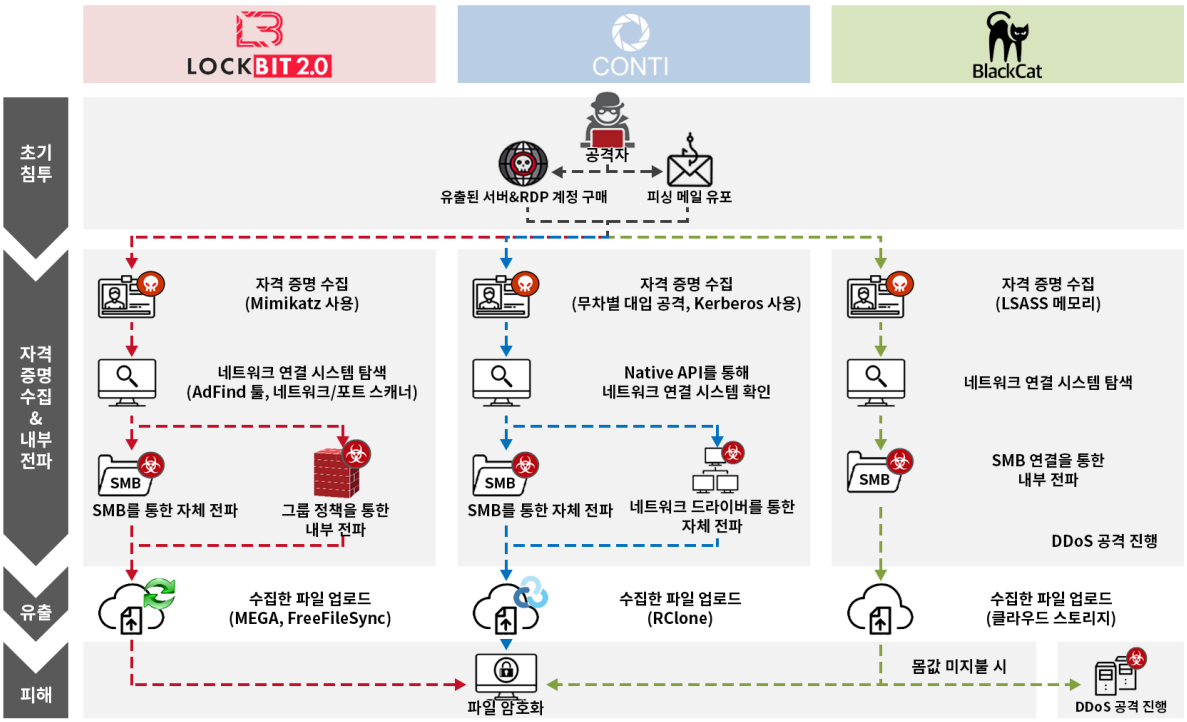
20 년 8 월부터 활동을 시작한 DarkSide 랜섬웨어 그룹은 미국 최대 송유관 운영 회사인 Colonial Pipeline 社를 공격했고, 57 억 상당의 비트코인(BTC)를 몸값으로 받아냈다. 이러한 과정에서 미국 동부 일대의 석유 공급에 차질을 빚게 되었고 휘발유 소비자가격이 7 년 만에 최고치를 돌파하는 등 사회 전반에 영향을 주었다. 결국 DarkSide 는 수사기관과 정부기관의 집중적인 감시를 받게 되어 운영 중단을 선언했다.

21 년 7 월 DarkSide 의 Re-Branding 으로 보이는 BlackMatter 랜섬웨어가 등장했다. 두 랜섬웨어는 파일 암호화에 사용되는 기술, 바탕화면을 변경하기 위해 사용하는 데이터의 저장 위치, 유출 사이트의 문구에서 유사성을 가지고 있었다. BlackMatter 는 일본 의료기기 제조회사인 Olympus 社를 공격하는 등의 활동을 벌이다 수사기관과 정부기관의 압력으로 인해 또다시 운영을 중단했다.

21 년 11 월부터 현재까지 유포되고 있는 BlackCat 랜섬웨어는 악성코드에 사용된 프로그램 언어에서 차이점을 가지고 있으나, 데이터 유출 도구와 랜섬웨어 기능 및 구성 파일의 유사성을 띠고 있어 BlackMatter 의 Re-Branding 으로 보인다. 이처럼 랜섬웨어 그룹은 Re-Branding 을 통해 악성코드를 고도화하고 수사기관의 감시를 피해 활동을 이어가고 있다.

랜섬웨어 공격 시나리오

22 년 상반기 주요 서비스형 랜섬웨어인 LockBit, Conti, BlackCat 랜섬웨어의 공격 시나리오는 다음과 같다.



[랜섬웨어 공격 시나리오]

1) LockBit 2.0

Active Directory [7] 그룹 정책을 악용하여 조직 내의 Windows 도메인 전체의 호스트를 자동으로 암호화한다. 장치 암호화를 완료하면 피해자의 주의를 끌기 위해 연결된 모든 네트워크 프린터에 랜섬웨어 경고 메시지를 반복해서 인쇄하는 등의 기능을 가지고 있다.

[7] Active Directory: 회사 직원들의 계정 정보, 회사에서 사용하는 정책 등에 대한 정보를 저장하고 있는 일종의 데이터베이스

1 LockBit 2.0

1) 유출된 서버 & RDP 계정 구매 또는 피싱 메일 유포를 통한 초기 침투
2) Mimikatz를 사용하여 자격 증명 수집
3) 네트워크에 연결된 시스템 탐색
4) SMB 연결을 통한 자체 전파 또는 그룹 정책을 사용하여 내부 전파
5) 클라우드 스토리지에 수집한 파일 업로드 후 유출
6) 파일 암호화 진행

2) Conti

최대 32 개의 다중 스레드로 작업하기 때문에 파일을 더 빠르게 암호화할 수 있다.

2 Conti

1) 유출된 서버 & RDP 계정 구매 또는 피싱 메일 유포를 통한 초기 침투
2) 무차별 대입 공격과 Kerberos를 사용하여 자격 증명 수집
3) 네트워크에 연결된 시스템 탐색
4) 네트워크 드라이브나 SMB 연결을 통한 내부 전파
5) 수집한 파일 업로드 후 유출
6) 파일 암호화 진행

2) BlackCat

최초로 Rust 언어로 개발된 랜섬웨어로 몸값 미지불 시 DDoS 공격을 통해 협박을 진행한다.

3 BlackCat

1) 유출된 서버 & RDP 계정 구매 또는 피싱 메일 유포를 통한 초기 침투
2) LSASS 메모리에서 자격 증명 수집
3) 시스템 정보 및 네트워크 연결 시스템 확인
4) SMB 연결을 통한 내부 전파
5) 클라우드 스토리지에 수집한 파일 업로드 후 유출
6) 파일 암호화 진행
7) 몸값 미지불시 DDoS 공격을 통한 협박

사이버 팬데믹 보안 대응 전략

지금까지 사이버 공격의 대유행인 사이버 팬데믹 상황에서 공격이 증가할 것으로 예상되는 보안 위협과 공격 시나리오를 알아봤다. 사이버 팬데믹에 대응하기 위해 기업 및 구성원은 보안 위협을 인지하고 이에 대한 보안 수칙을 준수해야 한다. SK 쉴더스는 아래와 같은 맞춤형 보안 전략을 제공한다.

[사이버 팬데믹 보안 대응 전략]

기업 및 구성원은 S/W 최신 업데이트 및 보안 설정을 통해 자체 취약점을 제거해야 한다. 또한 피싱이 의심되는 이메일, SMS 를 주의해야 하며 업무상 불필요한 웹사이트 접속을 지양해야 한다.

SK 쉴더스는 사이버보안, 물리보안 전 분야에서 체계적인 서비스를 제공한다.

사이버보안은 취약점 진단 및 맞춤형 모의해킹 서비스, 보안성 검증 컨설팅, 보안 인프라 구축/운영 및 보안관제 수행, 악성메일/APT 대응 훈련 지원, 악성코드 탐지/차단 솔루션 제공, 블록체인 기반 서비스 보안성 검증 등을 제공한다.

물리보안은 지능형 통합 보안 솔루션 제공, AI 지능형 영상 분석 등의 서비스를 제공한다.

랜섬웨어 대응을 위한 24x365 랜섬웨어 대응센터를 운영 중이며 사고 조사/대응 및 복구 서비스, 랜섬웨어 정보보안 패키지 서비스와 구독형 정보보안 솔루션인 사이버가드를 제공한다. 또한, SK 쉴더스를 비롯한 유관 기관과 국내외 협의체가 참여하여 랜섬웨어에 대한 정보 공유 및 공동 대응 활동을 하는 KARA(Koras Anti Ransomware Alliance)를 운영 중이다.

맺음말

사이버 팬데믹 시대에서 개인과 기업은 다양한 보안 위협에 노출되고 있다. SK 쉴더스에서는 IoT, 클라우드 등의 신기술을 비롯하여 가상자산 플랫폼, 랜섬웨어에 대한 연구를 지속적으로 진행하고 있으며, 이를 토대로 “고객 맞춤형” 서비스를 제공할 것이다. 우리 모두는 사이버 팬데믹 시대를 대응하기 위하여 각자의 위치에서 보안 수칙을 준수하고, 보안 위협에 적극적으로 대처해야 한다.

EQST

2022 상반기 보안 트렌드

2022.06

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹