2023
사이버
보안 위협 전망

Cyber Security Forecast **2023**

AhnLab ESTsecurity IGLOO NSHC S2W

kaspersky MANDIANT Microsoft splunk> TREND MICRO

과학기술정보통신부

KISA 한국인터넷진흥원

Contents

과학기술정보통신부

KISA 한국인터넷진흥원

2023 사이버 보안 위협 전망

Cyber Security Forecast 2023

1

국가·산업 보안을 위협하는
글로벌 해킹 조직의 공격 증가

2

재난, 장애 등 민감한 **사회적 이슈를**
악용한 사이버 공격 지속

3

지능형 지속 공격과 **다중협박**으로
무장한 **랜섬웨어의 진화**

4

디지털 시대
클라우드 전환에 따른 **위협 증가**

5

갈수록 복잡해지는 **기업의**
SW 공급망과 **위협 증가**

AhnLab ESTsecurity IGLOO NSHC S2W

kaspersky MANDIANT Microsoft splunk> TREND MICRO

2022년 사이버 보안 위협 분석 및 2023년 사이버 보안 위협 전망

Cyber Security Forecast **2023**

▪ 2022년 사이버 보안 위협 분석

1. 국가·사회 혼란을 야기하는 사이버 공격

- 全 세계 랩서스, 킬넷 등 글로벌 해킹조직의 공격으로 인한 피해 발생
- 카카오톡 장애, 이태원 사고 등 사회적 이슈 악용 공격 발생
- 정부·방송사 유튜브 공식 채널 계정해킹, 기관 사칭 해킹메일 유포

2. 재택근무 확산, 클라우드 전환 등 IT환경 변화를 악용한 공격

- 비대면 원격근무 환경 등 기업의 보안 취약점을 노린 지능형 지속 공격 발생
- 클라우드 가상자산 채굴 악성코드 감염, 개인정보, 데이터 유출 사고 발생

3. 디지털 사회를 마비시키는 랜섬웨어, 디도스 공격

- 콜택시, 배달대행업체 등 대국민 서비스에 대한 랜섬웨어, 디도스 공격
- 랜섬웨어 주요 공격 대상 중소기업(89%) 제조업(40%) (’22.11월 기준)
- 디도스 공격 매분기 증가추이, 영상저장장치(DVR), 셋톱박스 등 IoT기기 주요원인

2023년 사이버 보안 위협 전망

1. 국가·산업보안을 위협하는 글로벌 해킹 조직의 공격 증가

- 국가 지원형 공격 대응을 위한 준비 태세 강화 필요
- 비국가적, 비조직화된 해킹 그룹에 의한 공격 증가
- 수익 극대화에 적합한 대상 선택형 공격 및 가상자산 타깃형 공격 증가

2. 재난, 장애 등 민감한 사회적 이슈를 악용한 사이버 공격 지속

- 사회적 이슈를 악용한 피싱, 스미싱, 해킹메일 유포 및 지능형 지속공격(APT) 등 지속예상
- 정교한 가짜뉴스 등 신뢰도 및 사회에 영향을 미치는 공격 주의
- 이메일 및 소셜 미디어(SNS) 등 개인화된 채널을 활용한 공격 증가

3. 지능형 지속 공격 및 다중협박으로 무장한 랜섬웨어 진화

- 단순범죄에서 지능형 지속 공격(APT) 형태로 진화
- 내부망에 백업용 저장장치 검색·훼손 주의
- 암호화 파일 복구, 유출 데이터 공개, 디도스 공격, 고객 직접 협박 등 다중 협박 형태로 진화

4. 디지털 시대 클라우드 전환에 따른 위협 증가

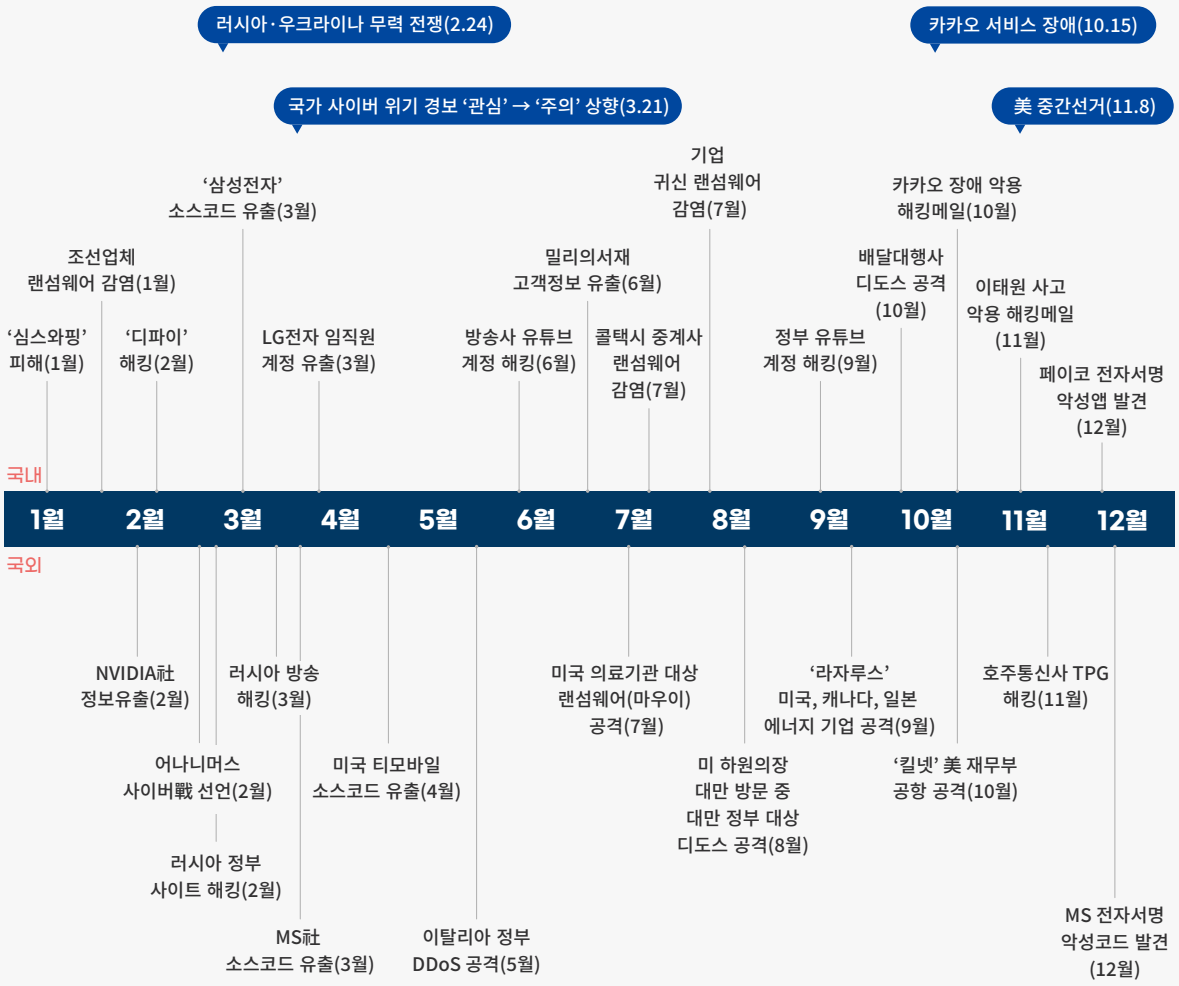
- 클라우드로 전환시 보안 설계 및 전략 미흡으로 인한 위협 증가
- 계정관리의 과잉권한 부여 및 잘못된 설정 등으로 데이터 유출 사고 증가
- '하이브리드 클라우드', '멀티 클라우드' 등 운영 형태에 맞는 보안대책 수립 필요

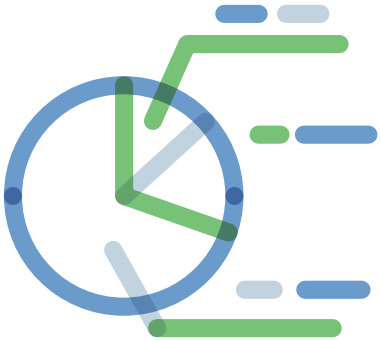
5. 갈수록 복잡해지는 기업의 SW 공급망과 위협 증가

- 소프트웨어 개발 공유 사이트를 통한 공급망 공격 증가
- 오픈소스 등 써드파티 코드에 의한 취약점 노출 및 악성코드 감염 우려
- 업데이트 서버 및 소스코드 변조, 인증서 탈취를 통한 공급망 공격 증가

2022년
사이버 보안 위협 분석

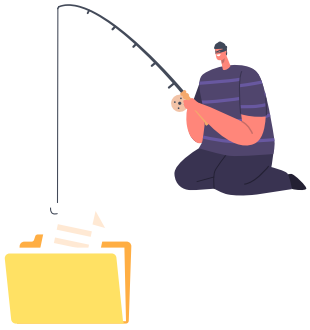
Cyber Security Forecast 2023





- **[국제정세]** 랩서스, 킬넷 글로벌 해킹 조직의 활동 증가
- **[국내위협]** 공급망, 정보유출, 랜섬웨어, 디도스, 사회적 이슈 악용 지속 등

1. 국가 間 무력 전쟁에 사이버 戰으로 확대 - 하이브리드戰 양상
2. 랩서스 글로벌 해킹 조직 - NVIDIA, 삼성전자 등 공격
3. 로그4j 등 유명 오픈소스에 의한 공급망 위협
4. 全 산업 분야에 걸쳐 랜섬웨어 공격 발생
5. 비대면 시대, 기업 재택근무환경을 통한 내부망 침투
6. 온라인 서비스 이용증가로 인한 클라우드 서비스 수요 확대 및 클라우드 공격
7. 정부, 방송사 유튜브 계정 해킹
8. 콜택시, 배달대행업체 등 다중이용서비스 대상 랜섬웨어 및 디도스 공격 발생
9. 사회적 이슈를 악용한 해킹메일, 스미싱 유포
10. SW 생태계 신뢰성을 악용한 공격 – 정상 인증서로 서명된 악성코드 발견



1

2022년 사이버 보안 위협 분석

1 국가·사회 혼란을 야기하는 사이버 공격

2 재택근무 확산, 클라우드 전환 등 IT환경 변화를 악용한 공격

3 디지털 사회를 마비시키는 랜섬웨어, 디도스 공격

1 국가·사회 혼란을 야기하는 사이버 공격

Cyber Security Fore cast 2023

- 全 세계 랩서스, 킬넷 등 글로벌 해킹그룹의 공격으로 인한 피해 발생
- 카카오톡 장애, 이태원 참사 등 사회적 이슈 악용 공격 발생
- 정부·방송사 유튜브 공식 채널 계정해킹, 기관 사칭 해킹메일 유포

■ ’22년 전 세계적으로 **랩서스**(LAPSUS$), 친러시아 성향의 해킹조직인 **킬넷**(Killnet) 등 **글로벌 해킹그룹**에 의한 지속적인 사이버 공격으로 인해 글로벌 기업과 정부 등에 피해가 발생했다.

주요사고 사례

· NVIDIA, 삼성전자, LG전자, Microsoft, 옥타, T-mobile 등 랩서스 해킹 사건(2~4월)

· 킬넷 이탈리아 기업(5월), 일본 정부(9월), 미국 공항, 재무부(10, 11월) 등 공격

■ 국내에서도 판교 데이터센터 화재로 인한 카카오 장애 이후 카카오톡 업데이트 파일로 위장한 악성코드가 발견되었으며, 이태원 사고와 관련된 공문서로 위장한 공격도 확인되는 등 **국민적 관심이 집중된 사건, 사고를 사이버 공격에 즉각적으로 악용**하는 양상을 보였다.

언론보도

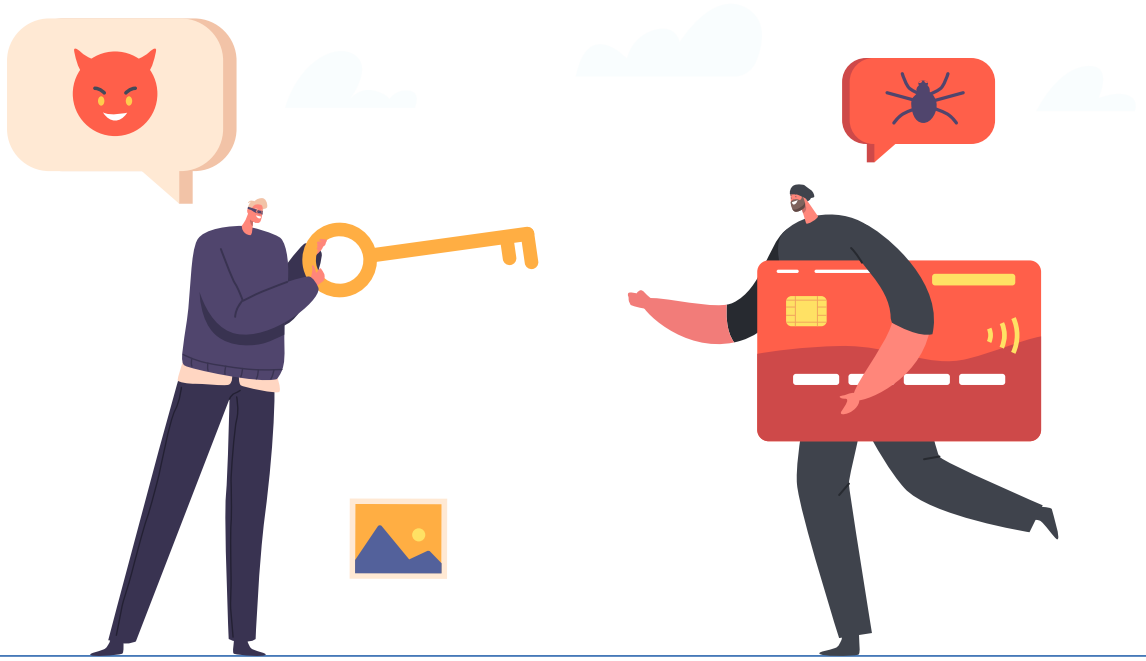
· 카카오 서비스 장애 이슈 악용 사이버 공격 주의(10월)

· 北 해커, “이태원 중대본 보고서” 위장해 공격(12월)

- **정부나 방송사 공식 유튜브 채널 계정을 탈취**하여 가상자산 관련 영상을 게재하거나 정부 기관을 사칭한 해킹메일을 유포하는 등 해킹 목적에 따라 대형사고로 이어질 수 있는 공격들이 발생하고 있어, 파급력이 큰 **공식채널에 대한 계정관리와 기관 사칭 해킹메일에 대한 각별한 주의**가 필요하다.

언론보도

- 방송사·정부 공식 유튜브 채널 잇단 해킹 … 누구의 소행일까(9월)
- 문체부·관광공사 유튜브 해킹 경찰수사의뢰(9월)
- 외교 학술회의 토론 사칭한 북한 해킹공격 발견(12월)



2 재택근무 확산, 클라우드 전환 등 IT환경 변화를 악용한 공격

Cyber Security Fore cast 2023

- 비대면 원격근무 환경 등 기업의 보안 취약점을 노린 지능형 지속 공격 발생
- 클라우드 가상자산 채굴 악성코드 감염, 개인정보, 데이터 유출 사고 발생

■ 코로나19 이후, 비대면 원격근무 환경이 확산되면서 **재택근무 등 보안에 취약**할 수 있는 지점을 노려, **기업 내부 침투를 통해 중요 정보가 유출** 되는 사고가 발생한 바 있다.

언론보도

- 삼성 해킹한 '랩서스' ... 탈취한 데이터로 협박(3월)
- 삼성전자까지 털렸다... 재택근무용 PC도 해킹 표적(7월)
- 삼성·LG 뚫은 해커조직 '랩서스', 제로트러스트 가동됐더라면(10월)

■ 해외에서도 원격근무가 보편화되면서 기업의 클라우드 활용이 늘어나고 주요 시스템이 클라우드로 전환되는 가운데, 클라우드 기반의 악성코드가 발견되고 클라우드 설정 오류로 인한 공항 데이터 유출, 10억 명의 개인 정보가 유출되는 등 **클라우드 관련 보안사고가 점차 확대**되고 있다.

해외사고 사례

- 아마존 클라우드에서 가상자산 채굴 악성코드 발견(4월)
- 아마존 클라우드 설정 오류, 3TB의 공항 데이터 유출(7월)
- 알리바바 클라우드 해킹으로 약 10억 명의 개인정보 유출(7월)
- 잘못된 데이터베이스 설정으로 인한 마이크로소프트 데이터 유출(10월)

3 디지털 사회를 마비시키는 랜섬웨어, 디도스 공격

- 콜택시, 배달대행업체 등 대국민 서비스에 대한 랜섬웨어, 디도스 공격
- 랜섬웨어 주요 공격 대상 중소기업(88.5%) 제조업(40.3%) (’22.11월 기준)
- 디도스 공격 매분기 증가추이, 영상저장장치, 셋톱박스 등 IoT기기 주요원인

■ 디지털 사회 가속화로 IT기술을 이용한 생활 밀접 서비스가 증가되면서 랜섬웨어, 디도스 공격으로 인한 대국민 서비스 중단은 **사회 · 경제적 불편을 넘어 일상생활의 마비**로 이어지기도 했다.

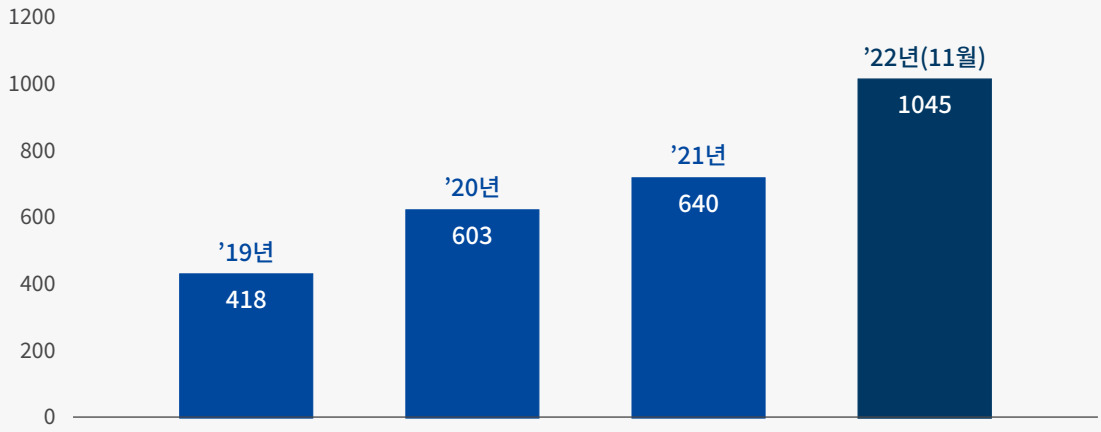
주요사고 사례

- 콜택시 중계 서비스 제공사 랜섬웨어 감염 사고(7월) - 전국 콜택시 마비
- 배달대행업체 디도스 공격(10월) - 자영업자•배달기사 피해, 배달 마비

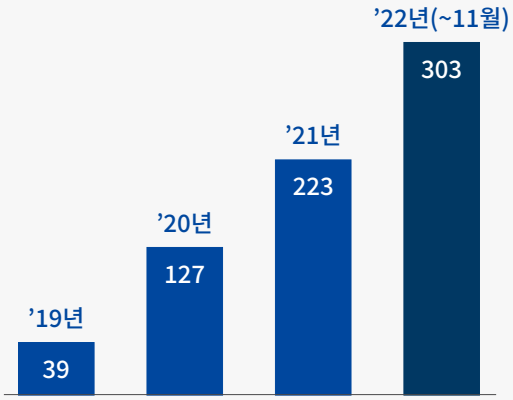
■ ’22년 한국인터넷진흥원에 접수된 침해사고 신고를 분석해보면 전년대비 약 **1.6배 증가**하여 사이버위협은 지속적으로 증가하고 있는 것으로 나타났으며, 신고의 **약 29%가 랜섬웨어 사고**로 피해발생 분포로 보면 **중소기업이 88.5%**(규모별), **제조업이 40.3%**(업종별)로 제일 비중이 큰 것으로 나타났다.

특히, 랜섬웨어 피해 중소기업을 보면 백업률은 정부의 데이터금고 지원 사업 등의 효과로 35.6%(’21년)에서 41.8%(’22년)로 증가한 것으로 나타났지만, 여전히 **백업이 없는 중소기업에 대한 지원 확대와 기업의 보안투자를 통해 데이터 복구 신뢰성을 확보할 필요**가 있을 것으로 보인다.

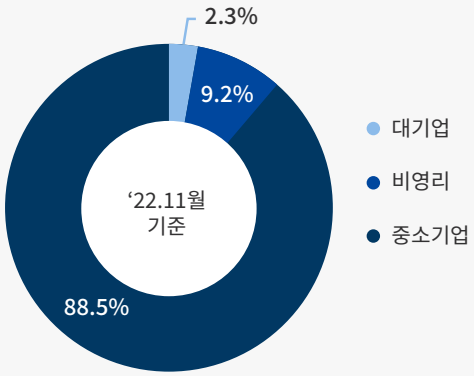
연도별 전체 침해사고 건수



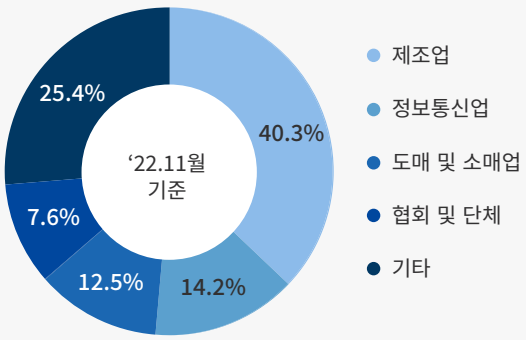
연도별 랜섬웨어 신고 건수(개)



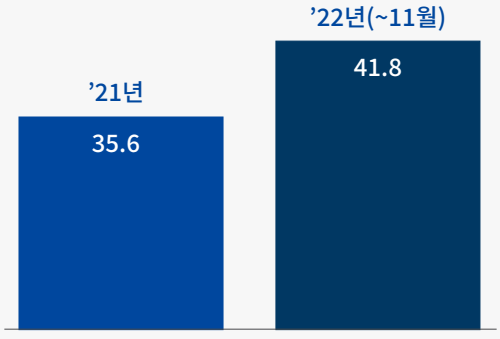
규모별 랜섬웨어 신고 비율(%)



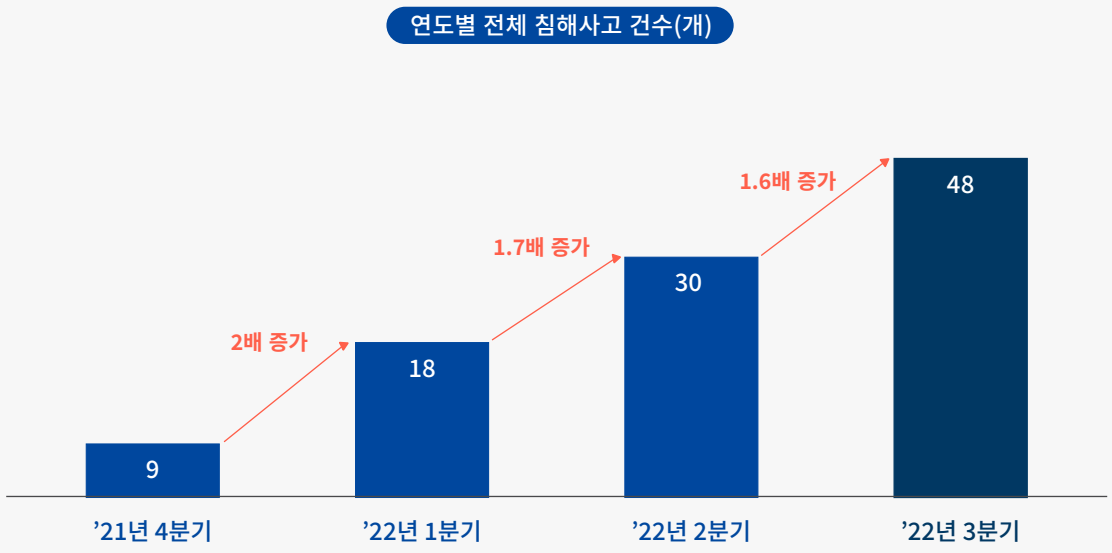
업종별 랜섬웨어 신고 비율(%)



랜섬웨어 피해 중소기업 백업 보유 비율(%)



- **디도스 공격도 지속적으로 증가**하고 있으며, 공격에 악용된 기기 대부분이 사물인터넷(IoT) 악성코드에 감염된 영상저장장치, 셋톱박스 등으로 확인 되었다. 감염된 다수의 IoT기기로 이루어진 봇넷을 통해 대량의 디도스 공격을 발생시키는 것으로 보인다.



2

2023년 사이버 보안 위협 전망

1 국가·산업 보안을 위협하는 글로벌 해킹 조직의 공격 증가

2 재난, 장애 등 민감한 사회적 이슈를 악용한 사이버 공격 지속

3 지능형 지속 공격과 다중협박으로 무장한 랜섬웨어의 진화

4 디지털 시대 클라우드 전환에 따른 위협 증가

5 갈수록 복잡해지는 기업의 SW 공급망과 위협 증가

1 국가·산업 보안을 위협하는 글로벌 해킹 조직의 공격 증가

- 국가 지원형 공격 대응을 위한 준비 태세 강화 필요
- 비국가적, 비조직화된 해킹 그룹에 의한 공격 증가
- 수익 극대화에 적합한 대상 선택형 공격 및 가상자산 타깃형 공격 증가

- 우크라이나 사태가 장기화됨에 따라 **'23년에도 글로벌 해킹 조직의 활동은 증가**할 것이며, **주요 기반시설이나 글로벌 기업을 대상으로 대규모 사이버 공격 시도**가 지속될 것으로 전망된다.

- 한편, 공격자 연령이 점차 낮아지고 소셜미디어(SNS)를 통해 공격행위를 공개하는 등 **사이버 범죄 조직의 대담한 활동이 앞으로 더욱 빈번**하게 일어날 것으로 예측되면서 랩서스와 같이 **비국가적, 비조직적 공격자에 의한 침해사고 우려도 여전**하다.

- 공격자들은 수익 극대화를 위해 공격 대상의 규모, 대외 신뢰도, 피해 파급력, 데이터 민감도 등을 조사하여, **피해기관·기업이 그 사실을 대외에 공개 하기 어렵거나, 신속한 복구가 필요한 곳을 목표로 선정**하여 공격할 가능성이 높다.

- 또한, 직접적인 수익 창출을 위해 가상거래소, 전자지갑, 디파이(DeFi, Decentralized Finance, 탈중앙화 금융) 등을 겨냥한 **가상자산 타깃형 공격도 더욱 활발**해질 것으로 예상된다.

2 재난, 장애 등 민감한 사회적 이슈를 악용한 사이버 공격 지속

- 사회적 이슈를 악용한 피싱, 스미싱, 해킹메일 유포 및 지능형 지속 공격(APT) 등 지속 예상
- 정교한 가짜뉴스 등 신뢰도 및 사회에 영향을 미치는 공격 주의
- 이메일 및 소셜 미디어(SNS) 등 개인화된 채널을 활용한 공격 증가

- 사회적 이슈를 악용한 피싱, 스미싱, 해킹메일 유포 뿐 아니라 **지능형 지속 공격**(APT, Advanced Persistent Threat)이 나타날 것으로 예상되며, 첨단기술을 활용한 **가짜 뉴스 등을 이용해 국가 신뢰도를 저해하고 사회 전반에 영향**을 미치는 활동이 증가할 것으로 전망된다.

- 또한, **사회공학적 기법을 통해 악성코드가 지속적으로 유포**될 것이며, 이메일 뿐만 아니라 SNS 등 개인화된 채널을 활용한 공격도 증가될 것으로 보인다.

3 지능형 지속 공격 및 다중협박으로 무장한 랜섬웨어의 진화

- 단순범죄에서 지능형 지속 공격(APT) 형태로 진화
- 내부망에 백업용 저장장치 검색·훼손 주의
- 암호화파일복구, 유출데이터공개, 디도스공격, 고객 직접 협박 등 다중 협박 형태로 진화

- **랜섬웨어 공격도 지능형 지속 공격**(APT) 형태로 계속 진화하고 있다.

- 공격경로는 해킹메일, 웹서버 취약점, 인증관리서버, 원격접근 등을 악용 하고 있으며, 오픈소스를 활용하거나 상용도구를 활용해 인증정보 탈취와 권한 상승(Privilege Escalation) 등 공격 양상의 변화가 두드러지고 있다.

- 또한, 백업용 저장장치도 찾아내 훼손하여 데이터 복구를 어렵게 하고 피해 시스템의 이벤트 로그나 메모리 증적을 없애 추적을 회피하고 있다.

- 공격자는 금전적 수익을 극대화하기 위해 **암호화 파일 복구, 유출 데이터 공개, 디도스 공격과 함께 기업 고객도 직접 협박**하는 등 다중협박(Multi Extortion) 형태로 진화하고 있다.

- 특히, 공격자는 피해 기업들이 데이터 복구보다 랜섬웨어 피해가 외부로 공개되어 **브랜드 이미지 손상을 더욱 우려**한다는 점을 노려, 금전을 요구 하면서 협박 수단으로 피해 기업의 시스템에서 갈취한 **민감 정보를 일부 공개**하는 사례가 지속될 것으로 보인다.

4 디지털 시대 클라우드 전환에 따른 위협 증가

- 클라우드로 전환시 보안 설계 및 전략 미흡으로 인한 위협 증가
- 계정관리의 과잉권한 부여 및 잘못된 설정 등으로 데이터 유출 사고 증가
- '하이브리드 클라우드', '멀티 클라우드' 등 운영 형태에 맞는 보안대책 수립 필요

- 코로나19 장기화로 사회 전반이 더욱 빠르게 디지털로 전환하고 있다. 물리적 위치에 제한이 없고 업무 확장이 용이한 클라우드의 장점 때문에* 기업들은 온프레미스 환경에서 **클라우드 환경으로 전환**하는 추세이다.

  * 기업이 자체 시설에서 보유하고 직접 유지 관리하는 내부 데이터 센터

- 이러한 클라우드 전환 과정에서 새로운 보안 취약점이 드러나고, 향후 클라우드 전환 증가와 함께 고려가 필요한 클라우드 보안 아키텍처와 보안전략 미흡으로 위협도 증가할 것으로 예상된다. 특히, 계정 관리 실수와 과잉 권한으로 위협이 증가하고 데이터 유출로 이어질 가능성이 있다.

- 접근 통제를 위한 인증과 접근 프로세스 도입 등 **'보안을 고려한 클라 우드 관리 전략'을 체계적으로 수립**하고, '하이브리드 클라우드', '멀티 클라우드' 등 각 기업의 업무 특성을 반영한 클라우드 운영 형태에 맞춰 빈틈없는 클라우드 보안대책을 수립하여야 한다.

5 갈수록 복잡해지는 기업의 SW 공급망과 위협 증가

- 소프트웨어 개발 공유 사이트를 통한 공급망 공격 증가
- 오픈소스 등 써드파티 코드에 의한 취약점 노출 및 악성코드 감염 우려
- 업데이트 서버 및 소스코드 변조, 인증서 탈취를 통한 공급망 공격 증가

- **기업 공급망**은 다양한 SW 제품, 개발업체, 수요자 등 구성요소가 많고, IT자산, 개발환경, 인력, 계약관리 등 관계가 복잡하여 **공격 탐지와 조치가 어렵고 파급도가 매우 큰 특징**을 가지고 있다.

- 최근 SW 개발자들이 깃허브(GitHub) 등 소스코드 개발 공유사이트를 많이 이용하는 점을 노려 그 안에 악성코드를 삽입하거나 소스코드를 탈취 하는 공격이 증가할 것으로 예상된다. 오픈소스의 사용도 증가하면서 로그4j 등 유명 오픈소스의 심각한 취약점을 악용하거나, 라이브러리에 악성 코드를 삽입하는 등 광범위한 보안문제를 발생시킬 것으로 보인다.

- 또한, SW 개발업체에 직접 침투하여 업데이트 서버 변조를 통한 악성코드 유포, 소스코드에 악성기능 추가와 기업의 정상 인증서 탈취 후 위조 서명된 악성 코드 등을 유포하는 공급망 공격 시도도 나타날 것으로 전망된다.

2023년 사이버 보안 위협 대응전략

디지털 전환 시대 보안 대응전략

제로트러스트

Zero Trust

지능화, 고도화된 사이버 위협 대응체계 구축

- 경계형 보안 → 제로트러스트 전환

* 다중인증 및 자원 접근통제 강화
* 신원 기반의 자원 접근통제, 동적 정책
* 세분화 보안정책 및 내외부 통합관제 관리
* 신뢰성 지속적 검증 및 제어

공급망보안

Supply Chain Security

복잡한 공급망, 전방위 위협 대응체계 구축

- 공급망 보안체계 구축

* 오픈소스 등 서드파티 코드 관리체계 구축
* SW 공급업체 등 협력사 보안 관리
* 자체 개발 SW 관련 보안관리체계 구축
* SW 안정성 확보, SBOM 도입

사이버복원력

Cyber Resilience

예측불가능한 공격에 대한 복구 체계

- 효과적인 대응, 회복력 강화

* 사업 연속성, 조직운영 복원력 등 전반 회복 대응체계 구축
* 신속한 복구 프로세스 수립 및 훈련

- 경계형 보안에서 제로트러스트 보안으로 전환 필요
- 오픈소스 등 소프트웨어 안전성을 확보할 수 있는 공급망 보안체계 도입 필요

- 비대면 원격근무의 확산과 클라우드 전환으로 기업 업무망이 복잡해지고, 네트워크 경계가 모호해지면서 **내부 직원의 계정과 권한을 탈취한 해커를 정상 이용자로 신뢰하면서 내부망의 자료가 유출되는 등 사고 사례가 증가**하고 있다.

- 이러한 문제를 해결하기 위해 모든 대상에 대한 잠재적인 위협을 미리 식별하고, 새로운 접근에 대해서는 거듭 확인하여 적절한 권한을 부여 하는 **‘제로트러스트’**가 주목받고 있다.

- 또한, SW 개발부터 운영, 유지보수 등 **SW 공급 全단계**가 복잡해지고 구성요소도 많아지면서, SW 공급망의 **보안 위협을 줄이고 위험성을 관리**해야 할 필요성이 늘고 있다.

- 이에 미국 바이든 정부도 국가 사이버보안 개선에 대한 행정명령(EO14028, '21.5)을 발표하면서 **제로트러스트 아키텍처를 美연방정부에서 구현**하도록 요구하고, 연방기관에 SW내장 제품을 납품할 경우 **SBOM*** 제출을 의무화 하는 등 **공급망 보안 강화**에 집중하고 있다.

  * SBOM(Software Bill of Materials), SW의 구성요소를 식별하기 위한 명세서

- 과학기술정보통신부와 KISA도 올해 초부터 연구반을 구성하여 보안모델과 가이드 마련 필요성을 제시한 바 있으며, 이를 구체화하고 능동적으로 대응하기 위해 지난 10월 **'제로트러스트·공급망 보안 포럼'을 발족**하였다.

▸ **사이버공격에 효과적으로 대응하기 위한 사이버 레질리언스 대응체계 전환 필요**

- 여러 고도화된 방어체계에도 불구하고 예측 불가능한 침해사고가 발생 하기 마련이며, 조직은 방어에만 치중하기 보다는 그 피해가 확대되지 않도록 조기에 대응하고 회복하는 대응체계를 갖추는 것이 중요하다.

- 사이버 침해를 당하더라도 업무 중단이 되지 않도록 백업체계를 마련 하고 신속한 복구 프로세스를 사전에 훈련하는 등 **사이버 레질리언스 (Cyber Resilience) 대응체계를 도입**할 필요가 있다.