(사)국방정보통신협회

사이버 공급망 위협에 대한 대응

2021. 6. 29

한양대 융합국방학과 孫 暎 東

1 사이버 공급망 공격

2 사이버 위협 고도화

- 미국 솔라윈즈(SolarWinds) 해킹 사례

미 솔라윈즈(SolarWinds) 해킹

√ 공격 개요

o 솔라윈즈 내부망에 침투해 모니터링 솔루션인 '오리온(Orion)'에 백도어 설치

o 오리온을 사용하는 기관·기업이 버전을 업데이트하는 과정에서 백도어 확산

√ 공격 과정

o 2019년 9월 공격자, 솔라윈즈의 내부망 침투 시도

o 2020년 2월 오리온의 취약점을 찾아내 백도어 설치·유포

3월 주요 공격대상을 선별해 별도의 해킹 툴을 설치하고 정보 탈취

12월 파이어아이(FireEye), 백도어를 확인하고 '국가주도 공격' 발표

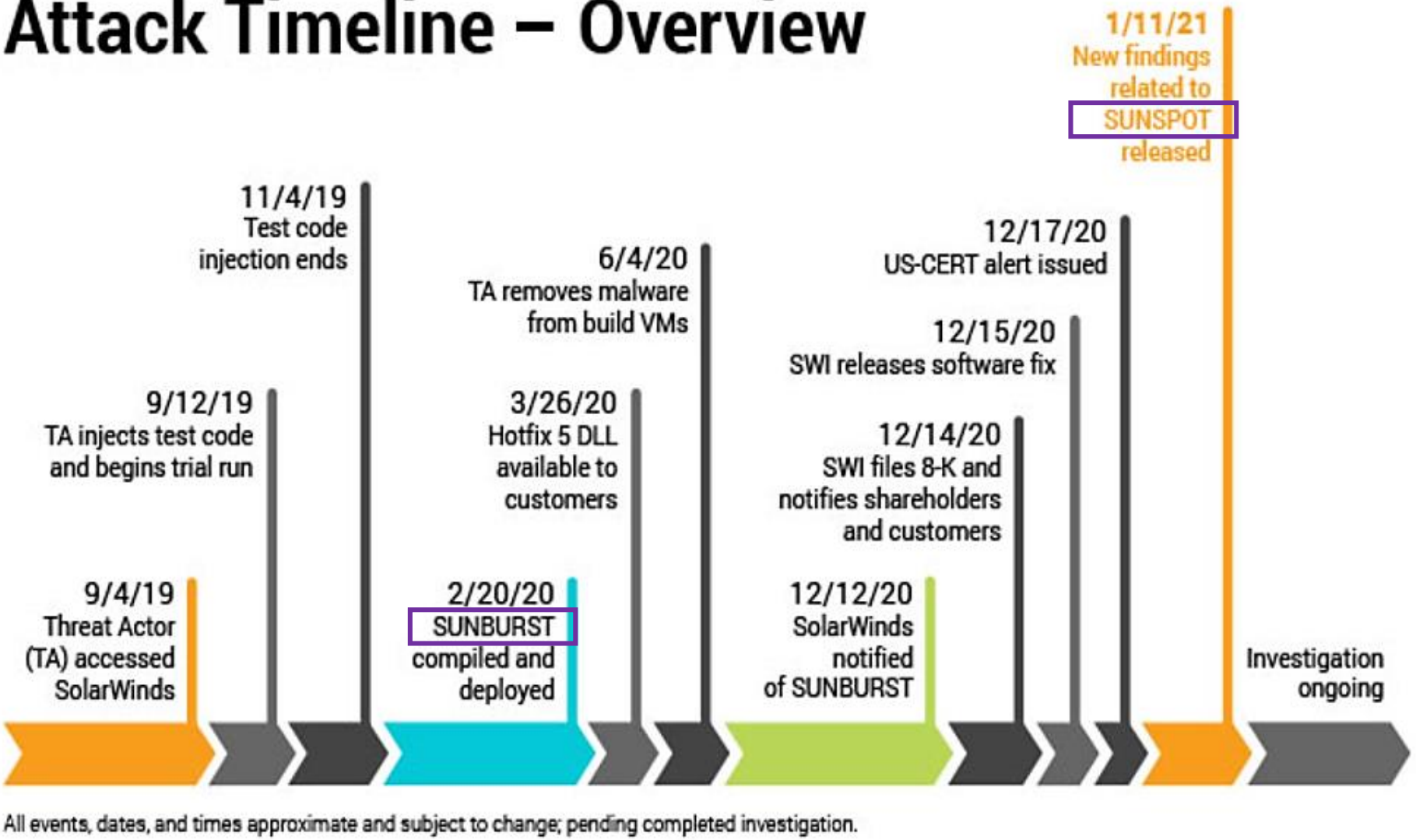
√ 피해 규모

☞ MS(2021. 1)

o 공격 대상 : 오리온을 사용하는 18,000여 기관·기업

- 국가기관 : 국토안보부·국무부·재무부·상무부·에너지부 등 최소 9곳
- 보안기업 : 마이크로소프트·파이어아이
- 민간기업 : 인텔 등 100여 곳, 이후 추가 피해를 확인하였지만 비공개

Attack Timeline – Overview



SolarWinds SUNBURST attack timeline, according to January 11, 2021, SolarWinds blog

미 솔라윈즈(SolarWinds) 해킹

√ 러시아 정보국 특정

o 2021년 1월 미국 정보기관, 러시아 해커로 추정하고 정부기관 포렌식 수행

MS, 러시아 신생 해커조직 '노벨리움(Nobelium)' 지목・추적

o 2021년 4월 미국・영국 정보기관, 러시아 해외정보국(SVR)을 배후로 특정

√ 대대적인 추가 공격

☞ MS(2021. 5)

o 2021년 5월 노벨리움, 미 국제개발처(USAID)의 이메일 마케팅 계정 탈취

24개국 150개 기관의 3,000개 계정을 확보해 피싱 공격 시작

o SW 공급망을 겨냥한 은밀한 악성코드 공격 → 이메일 표적 공격으로 전환

√ 바이든 행정부 대응

o 2021년 2월 19일 바이든 행정부, 솔라윈즈 공격에 대한 러시아 처벌 선언

23일 수사기관・보안기업, 미상원 정보위원회에 참석해 증언

※ MS 사장, "1,000명 이상의 유능한 엔지니어가 작업한 세상에서 가장 정교한 공격"

o 2021월 6월 (미-러 회담) 바이든, 대선개입・해킹의혹을 제기하며 보복 시사

아시아경제(2021. 5. 10)

미 콜로니얼 파이프라인 해킹

√ 사건 개요(2021년)

o 5월 7일 콜로니얼, 랜섬웨어 공격으로 송유관 가동이 중단된 지 몇 시간 만에 공격자에게 비트코인 75개를 지급하고 '복호화 툴' 수취

o 5월 12일 송유관 재가동 ※ 바이든 행정부, 18개 행정구역에 비상상태 선포

√ 비트코인 추적 • 회수

o 5월 10일 연방수사국(FBI), 공격 배후로 러시아 해커조직 '다크사이드' 특정

※ 다크사이드, "우리의 목표는 돈을 버는 것이지 사회문제를 일으키는 것이 아니다."

o 6월 7일 23번을 거친 최종 계좌(전자지갑)에서 비트코인 75개 중 63.7개 압류

√ 다크사이드(DarkSide)

o 2020년 다크웹에 등장하여 RaaS(Ransomware-as-a-Service) 사업 운영

- 전문 해커가 아니더라도 랜섬웨어 공격을 할 수 있게 지원하는 플랫폼

- 데이터 증거 샘플, 해킹 보고서 작성 등 협상 과정에 필요한 기능 제공

※ 2021년 3월 출시한 '다크사이드 2.0'의 경우 수수료 25%, 500만 달러 이상은 10%

1 사이버 공급망 공격

2 사이버 위협 고도화

"인류가 존재하는 한 전쟁은 사라지지 않는다."

☞ 알버트 아인슈타인(Albert Einstein)

디지털 혁명과 국가안보

√ 디지털 혁명에 따른 안보변화

☞ 클라우스 슈밥(Klaus Schab)

(1) 분쟁 복잡성 : 전통적인 전투기술과 새로운 기술이 중첩 → 하이브리드전

(2) 모호한 경계 : 전쟁 • 평화, 전투원 • 비전투원, 폭력 • 비폭력

(3) 새로운 공포 : 국가 행위자 + 소규모 집단이나 개인이 대규모 피해를 야기

√ 안보에 영향을 미치는 신무기

(1) 드론 : 대(對)테러작전이 지구촌을 대상으로 이뤄지는 상황
→ 전투영역(combat zone) 불분명

(2) 지향성 에너지 무기(DEWs_Directed Energy Weapons)

(3) 자율형 로봇 : 공격대상을 스스로 감지 • 추적 • 파괴 • 평가
→ 군사기술혁신, '인구 절벽'과 밀접

(4) 사이버 공격 : 시 • 공간 제약이 없어 일방적으로 유리
→ 익명성, 책임 • 식별(attribution) 문제

사이버 위협(Cyber Threat)

√ 사이버 공격의 정의

☞「정보통신망법」·「사이버안보업무규정」

o 침해사고 : 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 관련 시스템을 공격하는 행위

o **사이버공격** : 해킹·악성코드·서비스거부·전자기파 등 **전자적 수단**에 의하여 정보통신시스템을 침입·교란·마비·파괴하거나 정보를 누출·훼손·왜곡

√ 확대되는 사이버 위협

(1) **외부자 위협** : 위험을 일으키는 적극적인 행위인 사이버공격과 같은 맥락

(2) **내부자 위협** : 접근이 허용된 내부 구성원에 의한 정보시스템 보안상 위협

(3) **공급망 위협** : 제3의 공급자를 통해 타깃의 정상적인 활동을 저해하는 위협

√ 사이버 영역별 대응

(1) 금융·에너지·교통 등 기반시설의 직간접적 영향을 봉쇄하는 **물리적 대응**

(2) 정보시스템(SW·HW·NW·DB)의 악의적 침해를 방어하는 **논리적 대응**

(3) 위장 앱이나 악성메일(스피어피싱)과 같은 시맨틱 공격에 대한 **인지적 대응**

외부자 위협(Outsider Threat)

√ 해킹(Hacking)

o 네트워크 취약점을 이용해 불법적으로 접근하거나 허가 받지 않은 특정 정보시스템에 침투해 기밀성・무결성을 저해하는 행위

o 해커가 원하는 정보에 접근・교란하기 위해 수행하는 일련의 계획적인 행동

√ 디도스(DDoS) 공격

o 특정 서버가 감당할 수 없을 정도의 대규모 트래픽을 한꺼번에 일으켜 **합법적 사용자가 정보자산에 접근하지 못하게 함으로써** 가용성**을 저해하는 행위**

※ 2016년 10월 사물인터넷(IoT) 기기로 미국의 도메인서비스기업 다인(Dyn) 공격

√ 악성코드(Malware) 공격

o 프로그래밍에 사용되는 코드 중 사용자 시스템에서 동작할 때 **유해한 기능을 수행토록 작성된 코드의 통칭** 예) 바이러스・웜・트로이목마・랜섬웨어・크립토재킹

※ 2012년 5월 무려 5년이나 잠복하면서 대(對)이란 스파이활동을 한 '플레임(Flame)'

※ 2019년 5월 미국, 북한 해커로 지목한 원도용 악성코드 '일렉트릭피시(Electricfish)'

내부자 위협(Insider Threat)

√ 의도적 · 비의도적 위협 ↑

- o 내부자가 절도 · 파괴 행위를 통해 조직에 직접적인 손해를 입히는 것뿐만 아니라 부주의한 구성원이나 외주 · 계약업체 역시 별다른 의도 없이 실수로 발생
- o 의도적 · 비의도적 위협은 디지털 기기의 연결성 · 복잡성과 맞물려 지속 증가

√ 인적 보안의 중요성 증대

- o 설문) 악의적인 내부자로 인한 사고발생 비율(47%)보다 사용자의 부주의, 과실, 잘못된 권한 등으로 인한 사고발생 비율(51%) ↑ ☞ CA Technologies(2018)
- o 설문) 소속기관에서 가장 취약한 보안 분야 : 인적보안(53.06%), 기술보안(28.57%), 위기대응(7.14%), 보안정책(6.12%) ☞ 2018 국가정보보호백서

√ 스노든 게이트(2013년 6월)

- o 미 정보기관 전직 요원이 파이브아이즈(Five Eyes) 정보기관이 전 세계 일반인들의 통화와 인터넷 사용기록을 무차별적으로 수집 · 사찰해온 사실을 폭로

※ 백도어 프로그램 '프리즘(PRISM)'과 감시 · 정찰시스템 '엑스키스코어(Xkeyscore)' 공개

공급망 위협(Supply Chain Threat)

√ 제3의 공급망 공격

o 표적을 직접 공격하기보다 장비나 솔루션을 납품하는 제3의 공급자를 겨냥

o 공격자는 강도 높은 보안시스템을 뚫는 것보다 표적이 사용하는 각종 소프트웨어와 전자기기를 개발・생산・유통하는 단계에서의 빈틈을 공략

√ 공급망 위협의 가시화

o 백신 프로그램 업데이트와 PC관리 서버를 통해 악성코드를 감염・기밀 유출

※ 2017년 9월 미국, 연방 정부기관에서 사용하는 카스퍼스키랩 보안솔루션 퇴출

o 라우터・스위치・방화벽 등 네트워크 장비 제조단계에서 악성코드를 심거나 이미 설치된 장비에 몰래 침투시키는 공격도 만연 예) 중국산 스파이칩(2018. 10)

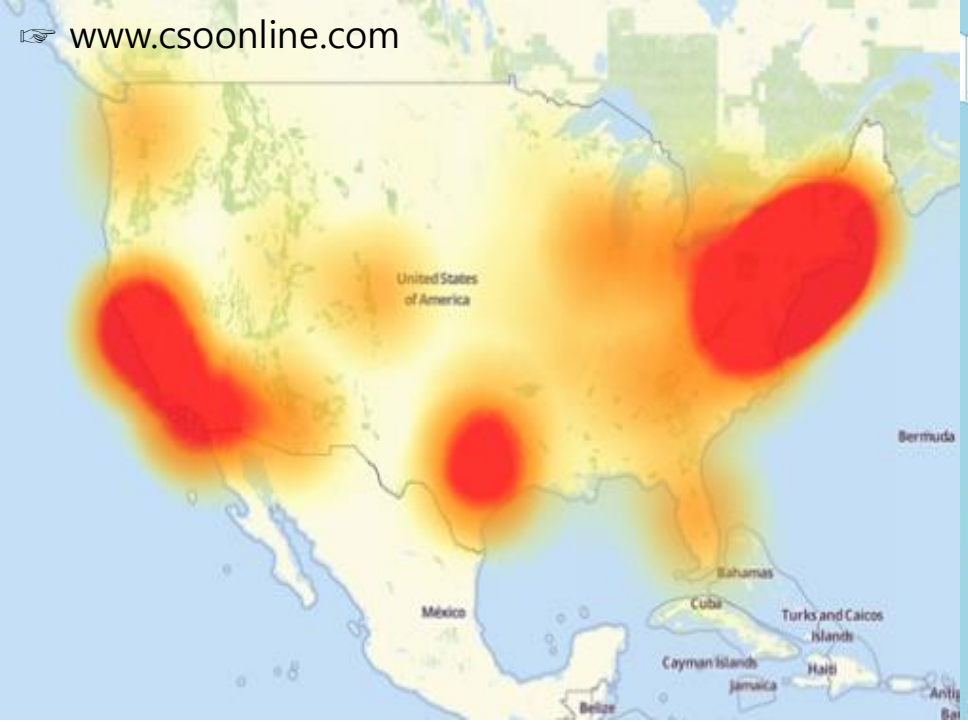
√ 미중 상호불신 제품구매 금지

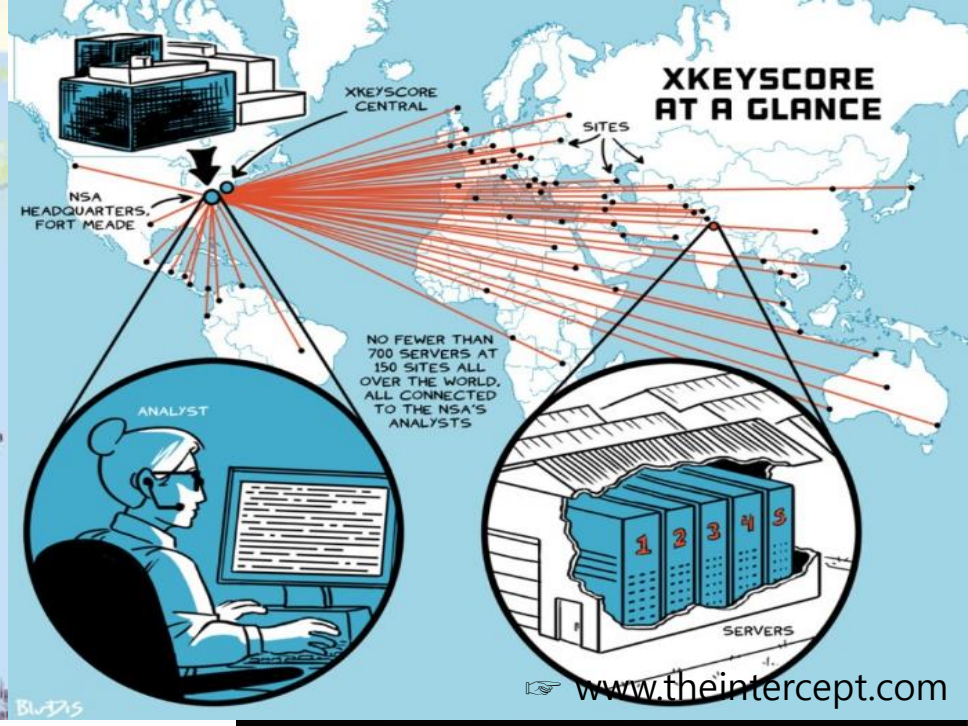
o 미국,「국방수권법 2012」을 제정해 국가기반시설에 외산 장비 도입 금지

o 중국, 2017년 6월 국가 통제를 전제로 한「네트워크안전법(網路安全法)」시행

※ 에티오피아 아프리카연합(AU) 건축 지원(2억 달러) 후 5년간 해킹 ☞ 르몽드(2018. 1)

☞ www.csoonline.com





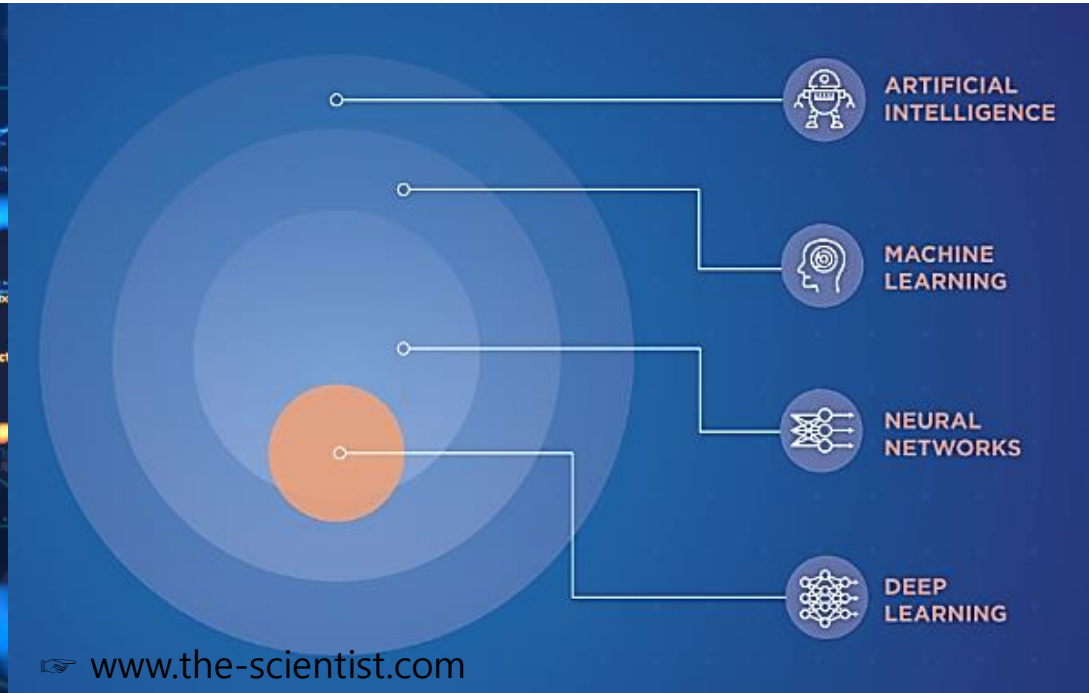
☞ www.theintercept.com

☞ www.supplychain247.com

사이버 보안 패러다임 변화

구분	As-Is	To-Be
공격주체	특정집단・불만세력	국가・비국가・비인간 행위자
공격대상	불특정다수	특정소수(국방・금융・기반시설)
보호대상	단말・네트워크 (정보시스템과 데이터 보호)	디바이스・네트워크・플랫폼 (사람과 환경에 대한 안전)
보안정책	정부 규제 위주	시장역할과 민간역량 활용
정보공유	부문별 제한된 정보획득	민・관・군 공조체계 + 국제협력
경쟁우위	데이터 수집・분석	빅데이터 + 알고리즘
기술개발	(필요성) 기술 중심의 추격형 하드웨어・프로젝트 중심	(즉시성) 사람 중심의 선도형 소프트웨어・프로세스 중심

☞ www.net-stage24.com



☞ www.the-scientist.com