악성코드와 해킹

컴퓨터공학과 장대희

경희대학교
KYUNG HEE UNIVERSITY

PWNJAB
@KYUNGHEE UNIVERSITY

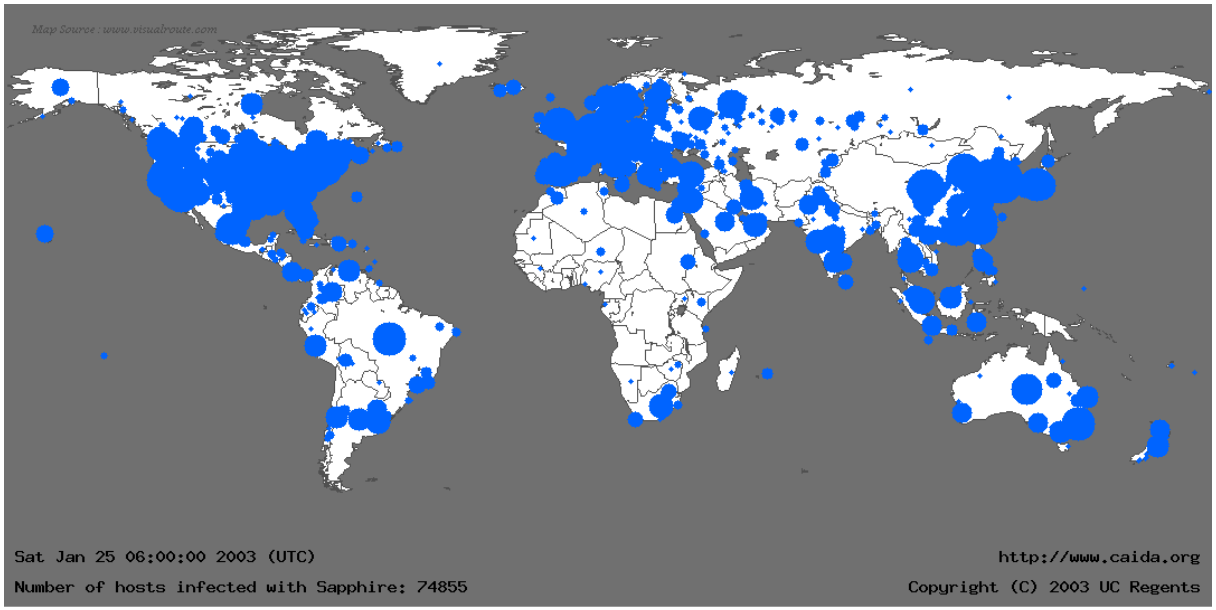
악성코드란 무엇인가?

- **Software with "malicious intention"**
  - Ransomware
  - Bitcoin Miner
  - Adware
  - etc

악성코드의 파급력

❖SQL Slammer

- The SQL Slammer Virus, also known as the Sapphire Virus, is malware in the form of a worm that caused a Denial of Service on many internet hosts in 2003, and caused thousands of network outages and even dramatically slow down Internet traffic
- 전세계 인터넷 마비



악성코드의 파급력

❖인터넷나야나 사건

- 2017년 6월, 대한민국의 웹 호스팅 업체인 인터넷나야나의 웹 서버 및 백업 서버 153대가 랜섬웨어의 일종인 에레버스(Erebus)의 리눅스용 변종에 일제히 감염된 사건.

  대한민국에서 호스팅 업체가 랜섬웨어에 감염된 것은 인터넷나야나가 최초이다.

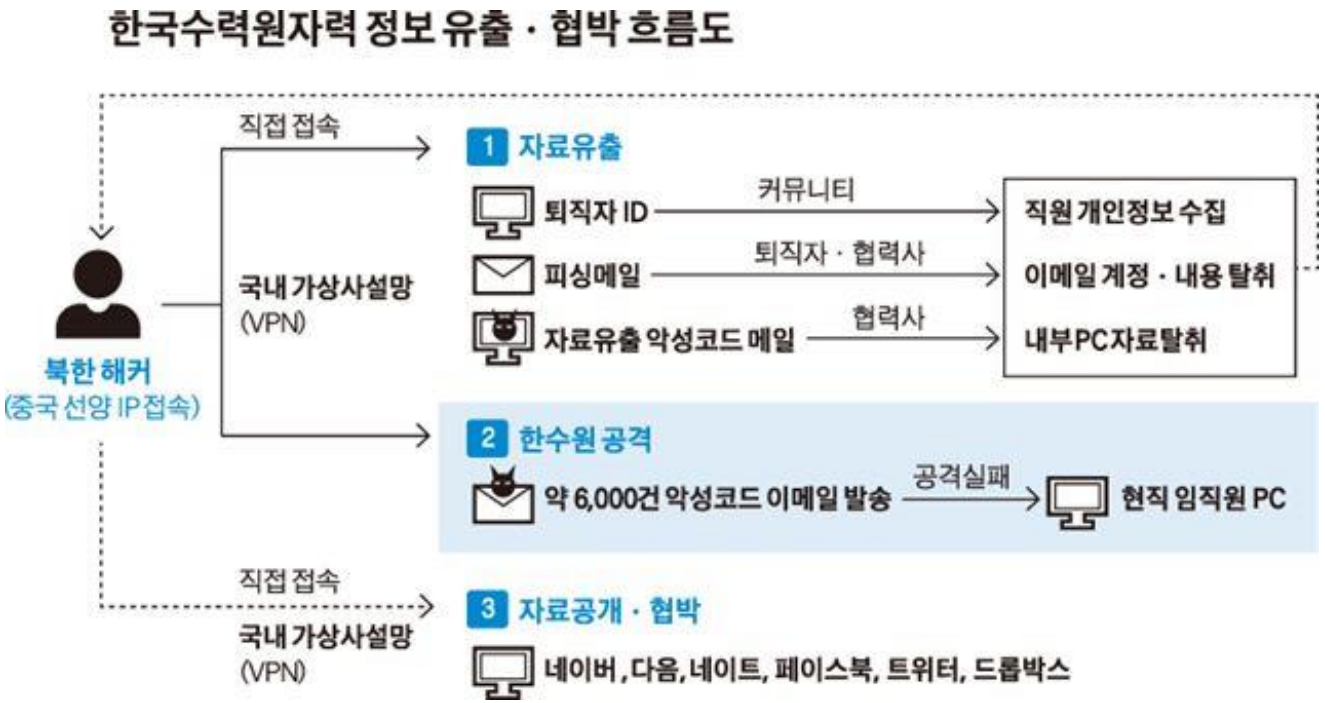
[한국어 해석][8]
우리 총책이 말하길, 너네 기계도 많이 산다며
비트코인 550개면 합당한 가격 아니야?
(복호화하기에)충분한 돈이 없으면 대출이라도 받아.

너네 회사 직원 40명 넘어.
평균 연봉도 다 3만 달러[9]는 되네.
3만 달러 * 40명 = 120만 달러
서버값 = 비트코인 550개 = 162만 달러[10]

돈 못 내겠으면 파산하든가.
근데 너희 애들, 와이프, 고객들, 직원들 얼굴 볼 수 있겠니?
넌 평판과 명성을 모두 다 잃고
수많은 소송에 시달리게 될 거다.

악성코드의 파급력

❖한수원 해킹



악성코드의 파급력

❖Stuxnet

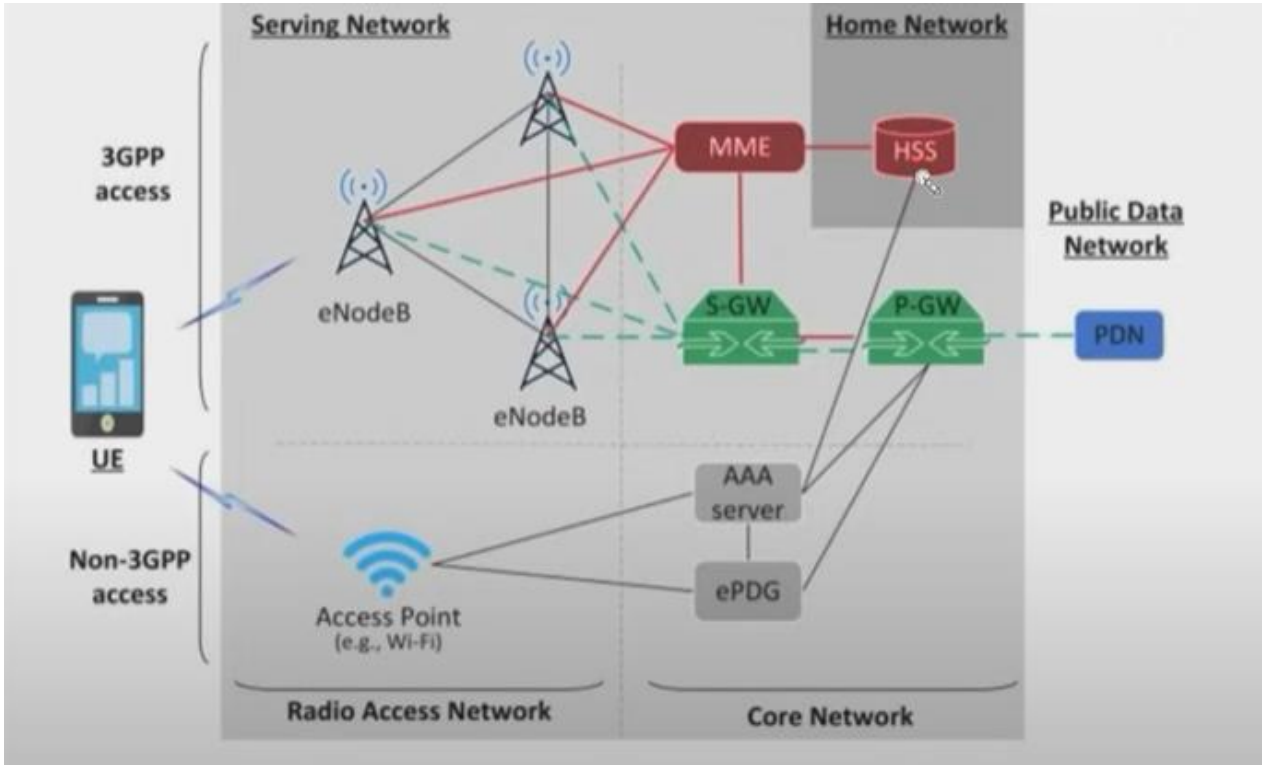
- **Stuxnet** is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.
- 최초의 원자력발전소 SCADA 망 해킹사건
  - ✓ 원자력 발전소 장치 제어
- 윈도우 제로데이 취약점 이용, 루트킷 설치
- According to a report by Reuters, the NSA ge North Korea's nuclear program using a version of

Country	Share of infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Other countries	9.2%

악성코드의 파급력

❖BPFDoor (SKT 해킹)

- Linux Malware using BPF for stealthy network comminucation
- BPF: Kernel Packet Filter

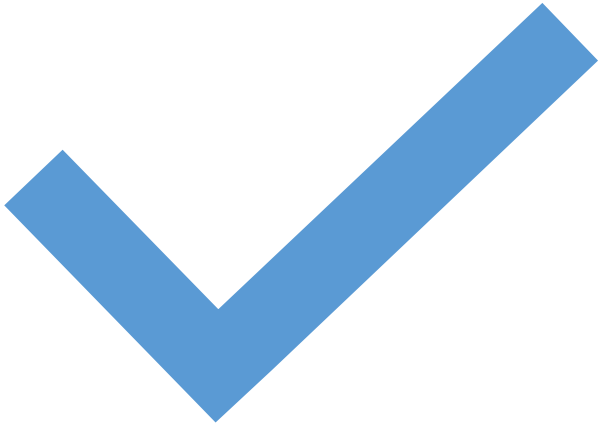


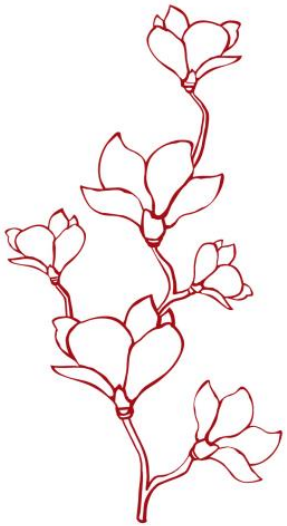
BPFDoor / bpfdoor.c

Code | Blame | 900 lines (766 loc) · 28.3 KB | Code 55% faster wi

```
112  struct config {
459          //
460
461          struct sock_fprog filter;
462          struct sock_filter bpf_code[] = {
463                  { 0x28, 0, 0, 0x0000000c },
464                  { 0x15, 0, 27, 0x00000800 },
465                  { 0x30, 0, 0, 0x00000017 },
466                  { 0x15, 0, 5, 0x00000011 },
467                  { 0x28, 0, 0, 0x00000014 },
468                  { 0x45, 23, 0, 0x00001fff },
469                  { 0xb1, 0, 0, 0x0000000e },
470                  { 0x48, 0, 0, 0x00000016 },
471                  { 0x15, 19, 20, 0x00007255 },
472                  { 0x15, 0, 7, 0x00000001 },
473                  { 0x28, 0, 0, 0x00000014 },
474                  { 0x45, 17, 0, 0x00001fff },
475                  { 0xb1, 0, 0, 0x0000000e },
476                  { 0x48, 0, 0, 0x00000016 },
477                  { 0x15, 0, 14, 0x00007255 },
478                  { 0x50, 0, 0, 0x0000000e },
479                  { 0x15, 11, 12, 0x00000008 },
480                  { 0x15, 0, 11, 0x00000006 },
481                  { 0x28, 0, 0, 0x00000014 },
482                  { 0x45, 9, 0, 0x00001fff },
483                  { 0xb1, 0, 0, 0x0000000e },
484                  { 0x50, 0, 0, 0x0000001a },
485                  { 0x54, 0, 0, 0x000000f0 },
486                  { 0x74, 0, 0, 0x00000002 },
487                  { 0xc, 0, 0, 0x00000000 },
488                  { 0x7, 0, 0, 0x00000000 },
489                  { 0x48, 0, 0, 0x0000000e },
490                  { 0x15, 0, 1, 0x00005293 },
491                  { 0x6, 0, 0, 0x0000ffff },
492                  { 0x6, 0, 0, 0x00000000 },
493          };
494
495          filter.len = sizeof(bpf_code)/sizeof(bpf_code[0]);
496          filter.filter = bpf_code;
```

악성코드의 정의 및 종류





악성코드란?

❖악의적인 행위를 위해 작성된 코드
- “악의적이다” -> 정의가능?
- 광고앱은 악성인가?
- 게임은 악성코드인가?
- 원격제어 앱은 악성코드인가?

❖악성코드의 종류?
- 백도어
- 랜섬웨어
- 가짜 앱
- 애드웨어
- 키로거
- 봇넷
- …

❖악성코드의 유포방법은?

백도어?

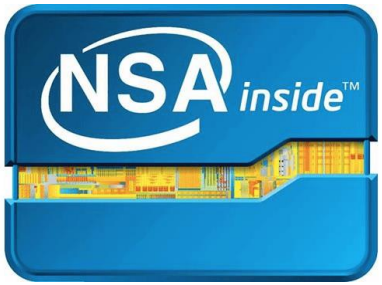
❖백도어란?

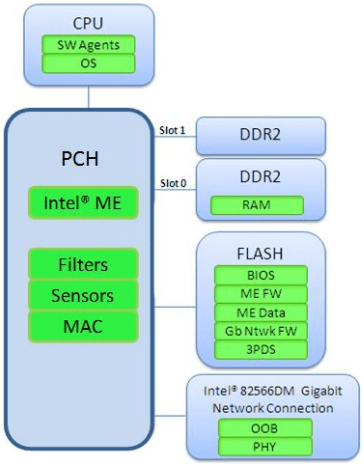
- A **backdoor** is a **malware** type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update **malware**.

백도어 사례

❖NSA 의 Intel ME 백도어

- Security Researchers at Positive Technologies have found a way to disable the Intel Management Engine (ME), a very widely hated component included in Intel CPUs implemented from Intel Core 1st to 7th generation CPUs (2006-2017).
- What is Intel ME? It's a tiny processor inside of Intel CPUs that has its own operating system, with its own processes, threads, memory manager, hardware bus driver, file system, and many other components.

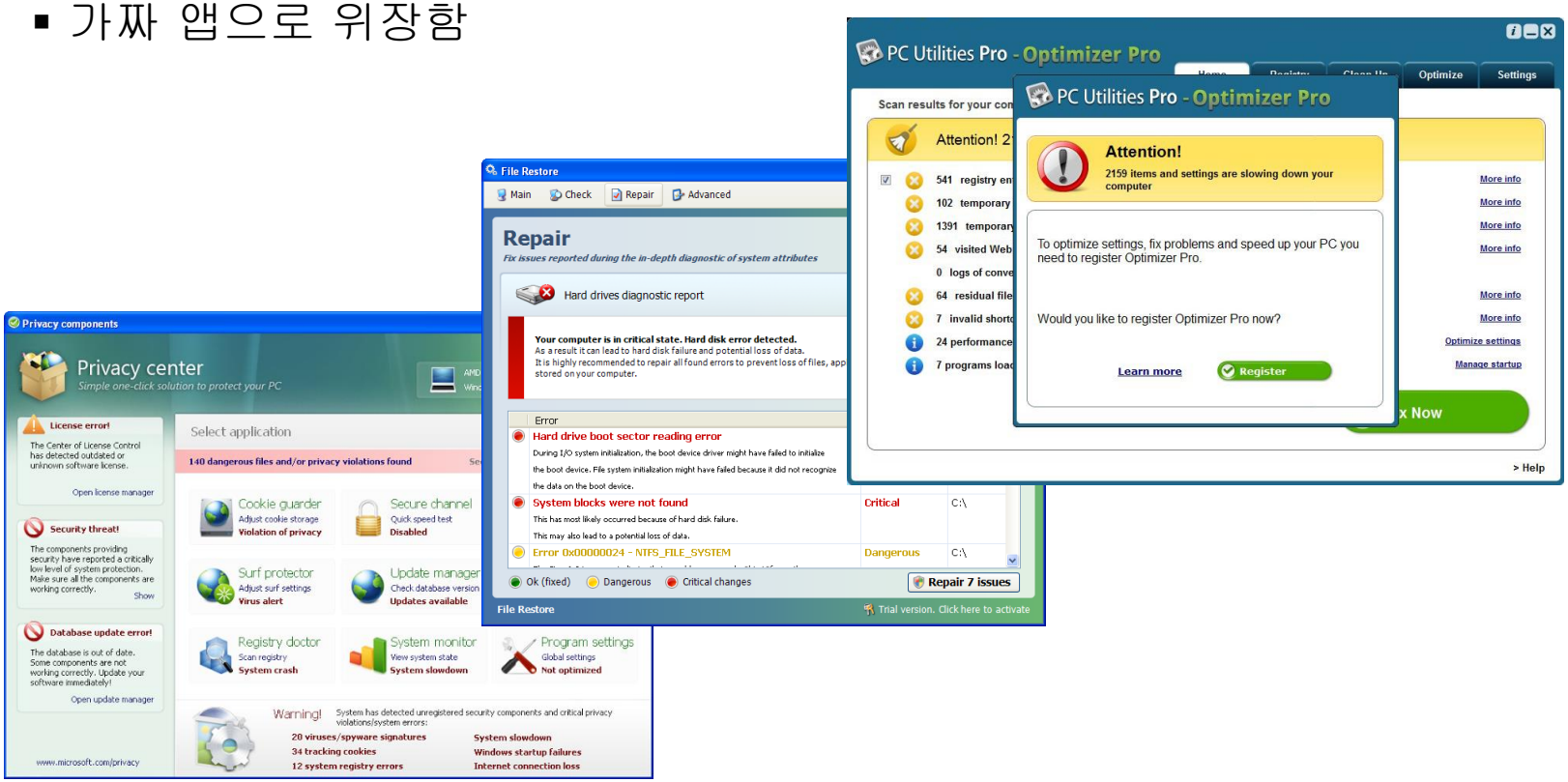




위장 앱

❖가짜 앱 기반의 악성코드

- 가짜 앱으로 위장함



랜섬웨어

❖랜섬웨어란?

- **Ransomware** is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. This class of malware is a criminal moneymaking scheme that can be installed through deceptive links in an email message, instant message or website.

Crypto-Ransomware (Cryptolocker) (2013)

❖Crypto Locker 악성코드

- 암호화 사용
- 랜섬웨어들 중 초기 악성코드

컴퓨터 바이러스 통로 (비기술적 해킹)

❖autoexec.bat

- Short for "automatically executed batch file", autoexec.bat is a startup file used with MS-DOS and early versions of Microsoft Windows operating systems (Windows 3.x and Windows 95). It contains commands that are to be executed by the operating system when the computer first boots. For example, if autoexec.bat contained the line "*c:₩windows₩win*", Windows 3.x would be executed when the computer first boots.

❖autorun.inf

- [autorun] open=command...
- Windows 7 부터 차단.
- CD 만 허용

❖매크로바이러스

- 문서파일 속에 실행스크립트 삽입
  - ✓ '실행하시겠습니까?' 버튼을 클릭해야 실행.

컴퓨터 바이러스 통로 (비기술적 해킹)

❖이메일

- Email by itself is harmless, but hackers use attachments and downloads to embed viruses on your computer. The virus then accesses data or tracks your logins to gather information for its creator. Alternatively, it can simply hack in to your email and start sending spam mail using your account.

❖트로이의 목마

- 다른 프로그램으로 위장

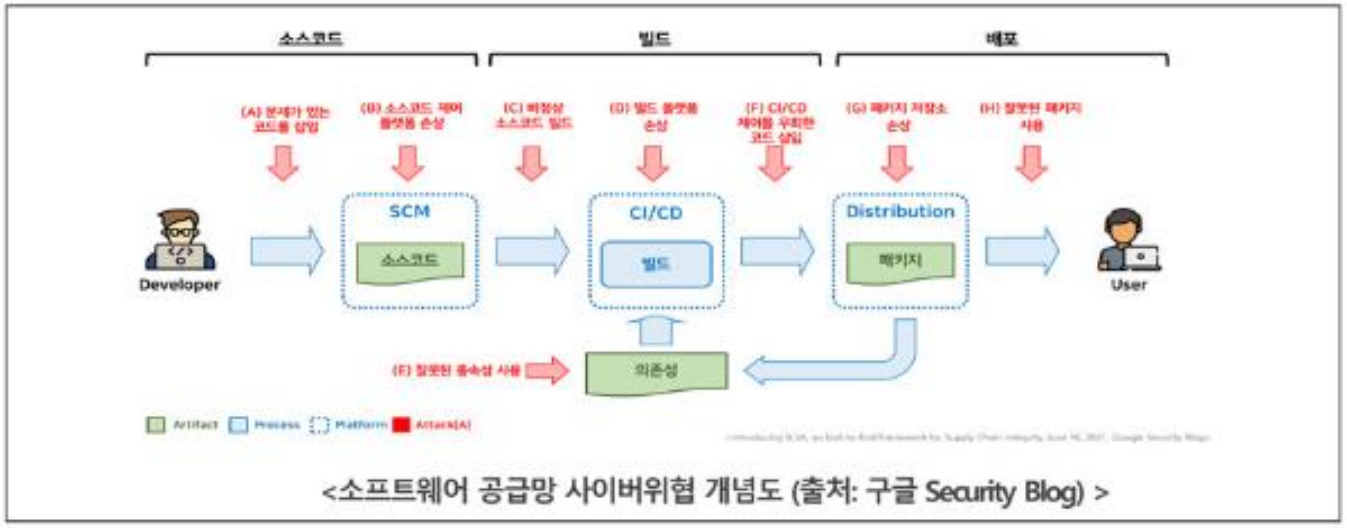
컴퓨터 바이러스 통로 (비기술적 해킹)

❖공급망 해킹 (?)

- A supply chain attack in hacking refers to compromising a target not by attacking them directly, but by infiltrating software or hardware they trust and use, often during development, build, or distribution phases. It's like poisoning the ingredients before the dish is cooked.

❖SBOM (Software Bill of Materials)

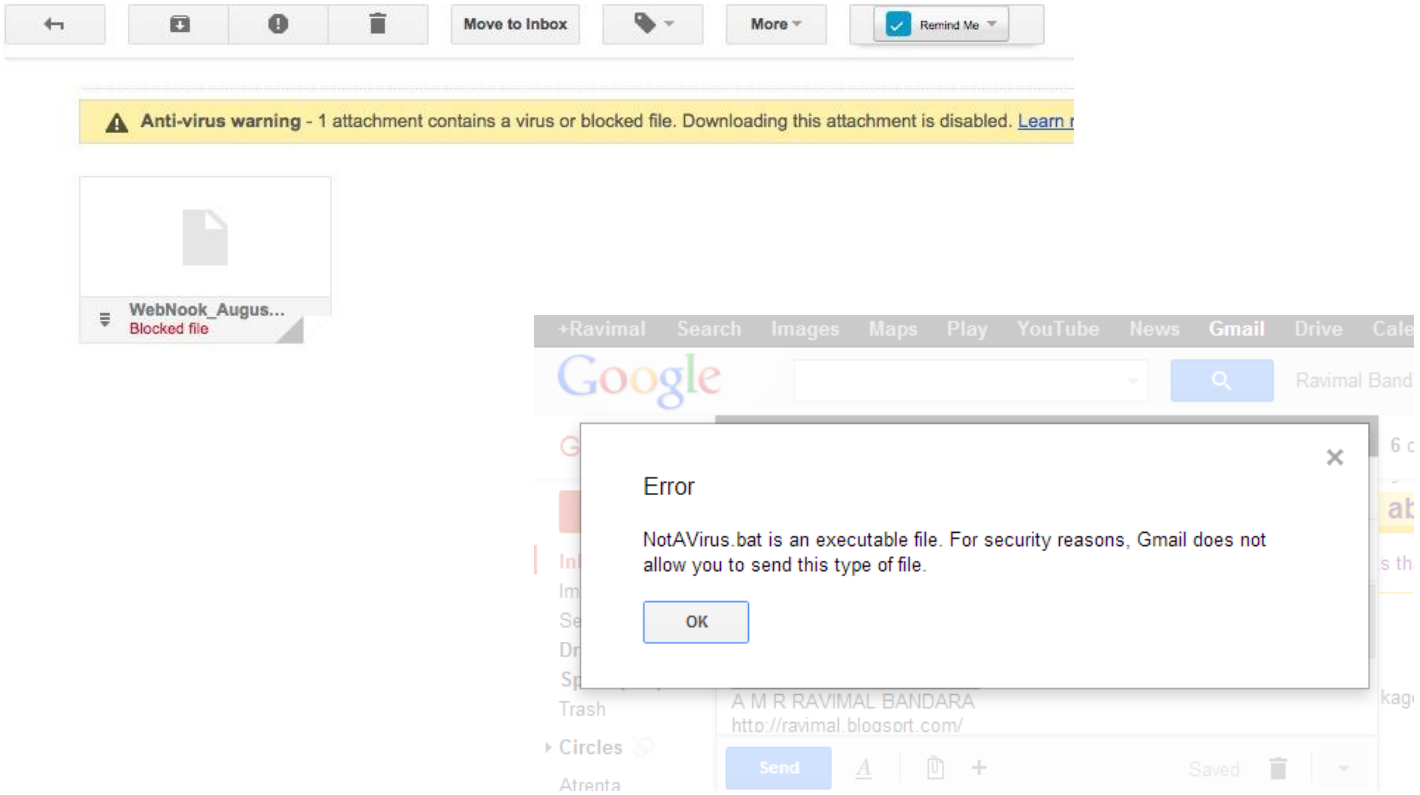
- Track all components used in builds



<소프트웨어 공급망 사이버위협 개념도 (출처: 구글 Security Blog) >

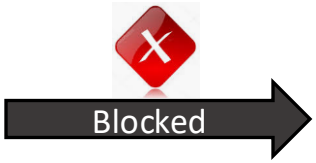
바이러스 차단 예시

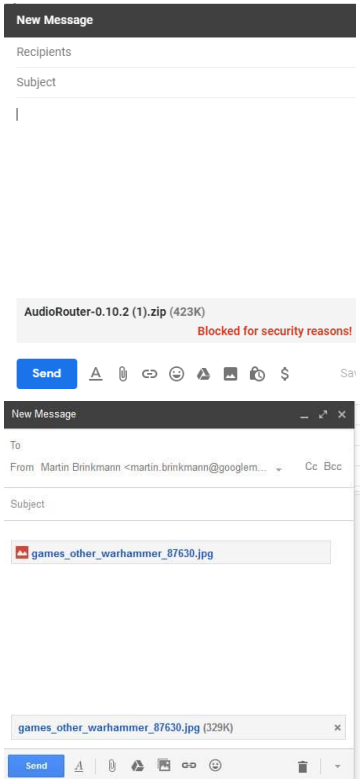
❖G메일 바이러스 필터



How to spread Malware?

Executable Files (Binary, Script, etc)

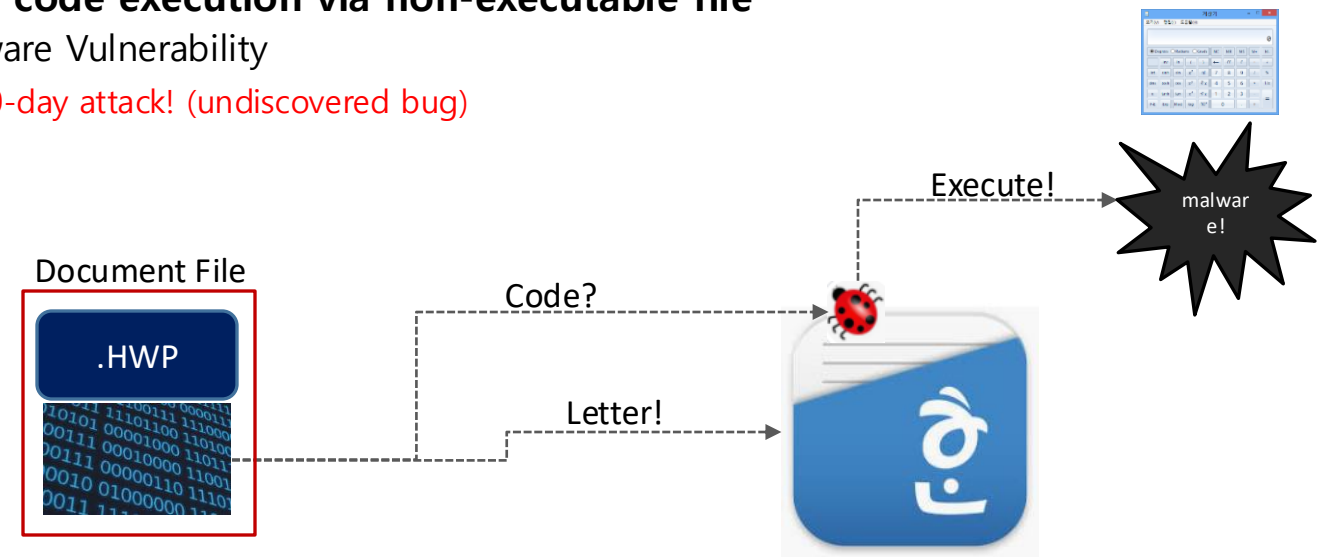




Non-Executable Files (Documents, Image…)

How to spread Malware

- **Solution: code execution via non-executable file**
  - Software Vulnerability
    - ✓ 0-day attack! (undiscovered bug)



컴퓨터 바이러스 통로 (기술적 해킹)

❖취약점 이용

- 웹브라우저
- 운영체제 (커널)
- 문서편집기
- 한글
- 동영상편집기

계산기?

- **Proof of Concept**
  - Arbitrary Code Execution
- **Real Attack Case**
  - Substituted to Malware

0-day? 1-day?

❖Why call it 0-day?

- Known to public : day 1
- Before day 1?
  - ✓ Day 0 ☺

Report to public

Now we are public.. day-1 ☺

악성코드의 지속성

❖악성코드 감염 그후..?
- 어떻게 시스템에 머무를 것인가?

❖레지스트리
- AppInit_DLLs

❖프로그램 변조
- WFP

❖루트킷
- OS 자체를 변조

결론

❖악성코드의 정의/분류는 주관성이 있음
- 명확한 정의/분류 는 어려움

❖악성코드는 금융범죄와 밀접한 관계
- 개인정보 수집 → 광고업체에 판매
- 랜섬웨어 → 돈 요구
- 애드웨어 → 광고수익
- 마이닝봇 → 비트코인 채굴

❖악성코드는 기술적/비기술적 방식 모두를 이용하여 전파가능
- 취약점 악용 or 사람을 속임

❖악성코드 사고들은 정부차원의 보안정책에 큰 영향을 주게됨
- 보안관련 교육, 해킹대회 등


Q
A