제15회 정보보호심포지엄
Symposium on Information Security 2010

에스토니아, 7.7 그리고 미래 대응

보안 컬럼니스트
전상훈 (p4ssion@gmail.com)

주 최 한국인터넷진흥원 Korea Internet & Security Agency
후 원 방송통신위원회 KOREA COMMUNICATIONS COMMISSION
언제 어디서나 인터넷 관련 상담은 e콜센터 118

목 차

- 에스토니아 cyber war
- 7.7 DDoS
- 공격의 진화 및 대응
- 결론

에스토니아 Cyber war

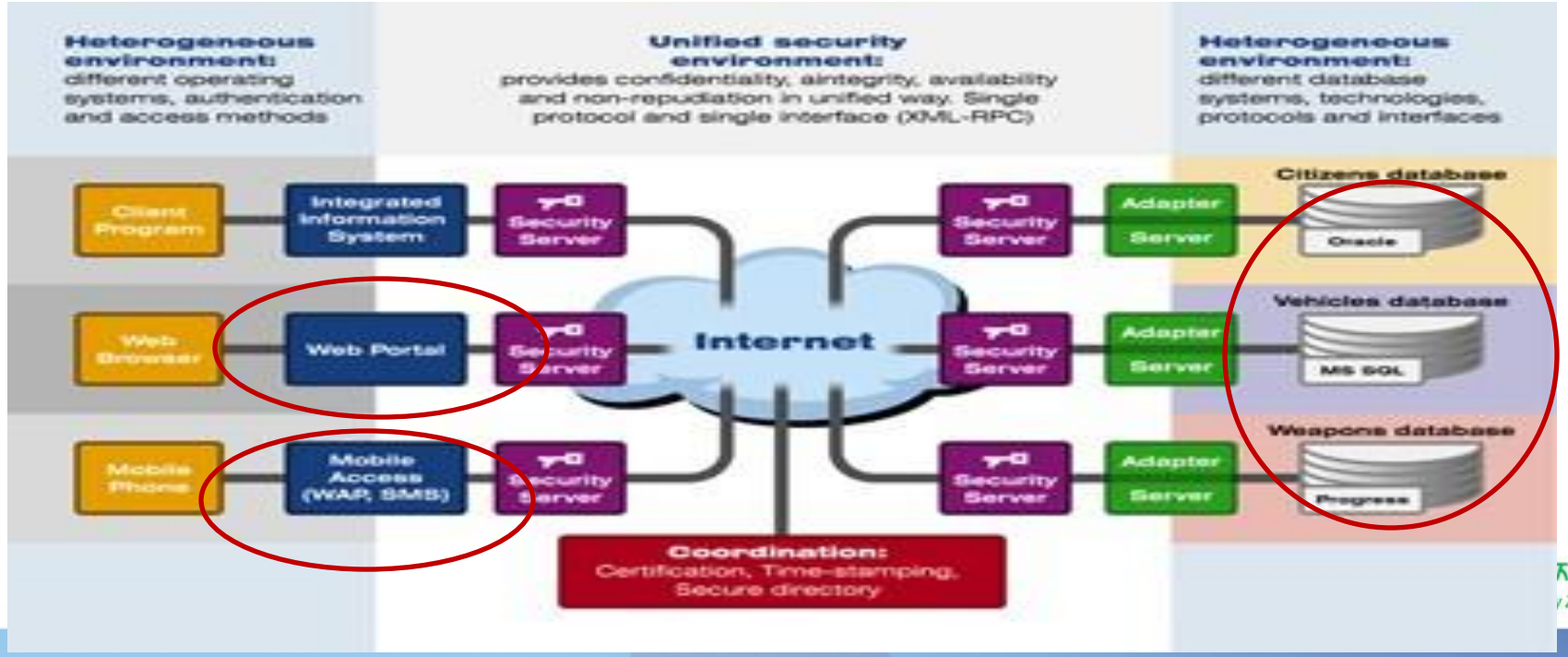
- 위치 : 북 유럽 , 발트해 연안, 러시아와 인접
- 러시아로부터 1991년 구소련연방 붕괴시 독립.
- 동유럽의 정보통신 강국으로 성장, 실험적인 모델 도입, e-stonia로 불려짐
- 2004년 EU와 NATO에 가입.

- 분쟁 내용: 수도 탈린에 위치한 소련군 참전용사의 비를 외곽으로 이전 하면서 분쟁이 시작됨. 정치적 동기에 의해 국가간의 갈등이 증폭.

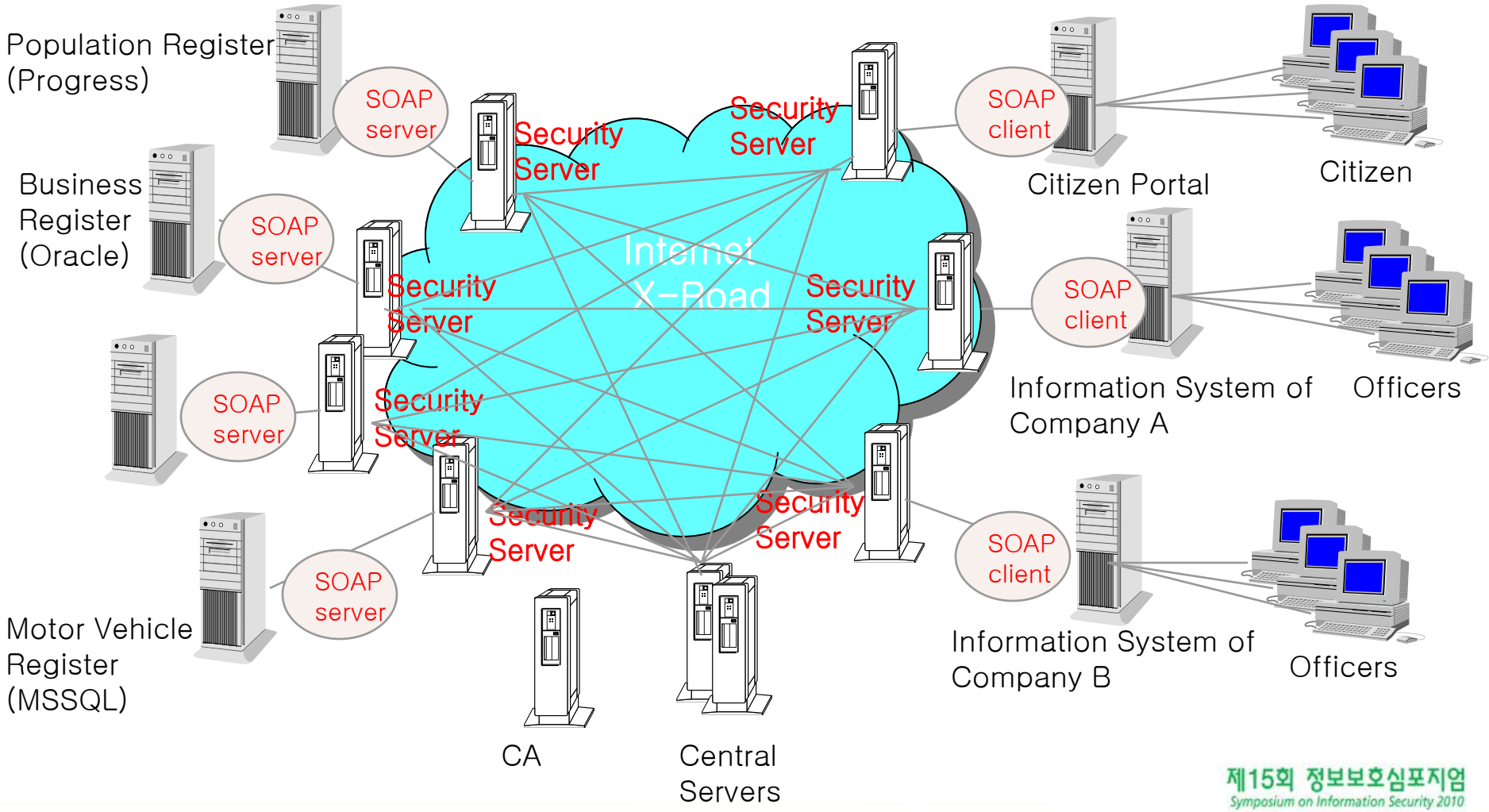
- 공격 대상: 에스토니아의 Infra structure 및 관공서, 은행,포털 등
- 공격 추정 그룹: 러시아 내의 극우 성향의 그룹으로 추정
  (국가 차원의 실험적 공격?)
- 공격 일시: 2007년 4.27일 이후 3주간 지속 되며 특징적으로 3차례로 분류

에스토니아 Cyber war

- 에스토니아의 IT Infra-structure의 특징
  - 중앙 집중 , 온라인 액세스 확대, 정부 기관의 온라인 업무 처리
  - X-Load 시스템 도입을 통한 355개 이상의 정부기관의 상호 연결 가능
  - ID-Card를 이용한 상거래 및 은행까지 연계된 결재 모델 구축 (전자 투표에도 활용)
  - 암호화된 연결 및 PKI 기반의 인증 구조를 가지고 있으며 데이터의 교환 및 전송은 HTTP
  - 모바일, Web, C/S base 활용하며 이기종 DB와의 연결에 통일성을 기해 접근성을 높임



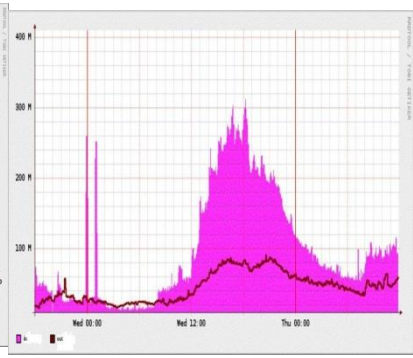
에스토니아 Cyber war -xload



에스토니아 Cyber war

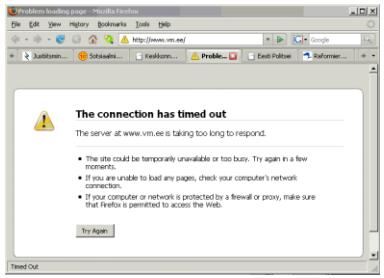
➢ Cyber Attack 유형

- Bandwidth Attack
  - 115 ICMP Flood , 4 Tcp / Syn Flood
  - 12 flood Attack. 70~95 Mps 10시간 이상 지속
  - General ICMP DDos using by Rental Botnets
  - 부분적으로 1.2G 가량의 트래픽 유입



- General Application Attack (SQL Injection, Apache, PHP ..etc)

- Web site defacement
  & Service Down



- Email –spam (주요 정부기관 인사 및 당직자 대상 – 정상 업무 처리 불가)

- Phishing

에스토니아 Cyber war

➢ Cyber Attack 진행

- 1 차
  - 2007년 4.27일 에스토니아 정부 IDC와 상업용 사이트에 대한 DDos Attack
  - 러시아 인터넷사이트들 통해 batch 파일 공유 및 공격도구 공유를 통한 자동공격 코드 대량 유포 – 집중적인 트래픽 유입

- 2차
  - 러시아 내의 LiveJournal 사이트에 에스토니아 의회 의원들의 이메일 주소가 게시
  - 수백만통 이상의 미메일이 당국자들에게 전달 되고 시스템 부하 발생됨

- 3차
  - 5.3~ 5.9 Web site에 대해 다양한 도구를 이용한 공격이 집중적으로 이루어짐
    - sql injection
    - Known vulnerability – apache , php

  - 푸틴 러시아 총리의 에스토니아 동상 이전과 관련된 비난으로 Script kiddes들에 의한 공격 격화

에스토니아 Cyber war

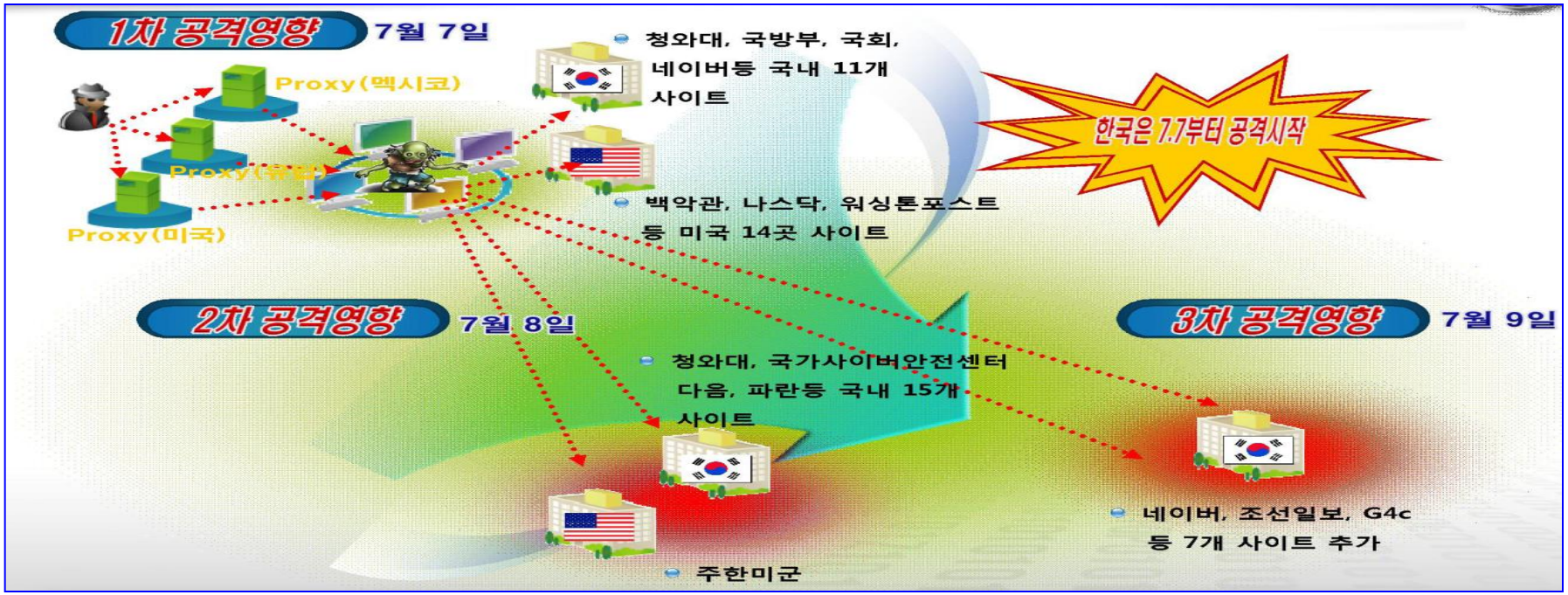
➢ Cyber Attack 피해 및 대응

- 피해
  - 네트워크 장비들에 직접적인 영향
  - Routing Table 변경
  - DNS 부하 증가로 전체 속도 현저히 떨어짐
  - 이메일 서버의 과부하로 문제 발생
  - 온라인 서비스 활용 불가, 전체 연동망인 Xload의 연동 불가로 행정 및 금융 업무 마비
  - 정부망, 의회, ISP, Bank, 언론사, 통신사 업무 중단됨 – Critical Infra Attack 및 영향 사례

- 대응
  - 외부로 부터 유입되어 오는 트래픽의 차단, 국내만 사용 하도록 적용 *.ru 도메인 차단
  - NATO 및 US CERT와 협력하여 외부 Botnet Server에 대한 탐지 및 차단 시행
  - 우회전략을 이용하여 공격자들에게는 사이트가 다운된 것으로 보이도록 하여 추가 공격 방지
  - 낮은 수준의 DDos를 위해 DDos 전용 장비의 도입
  - Estonia의 대역폭을 초과하는 공격에 대해 Black list 작성 및 차단
  - NATO의 사이버전 사령부 estonia에 설치

7.7 DDos

- 일시 : 2009.07.07 ~07.09
- 형태 : 10만여대 이상의 좀비 PC를 이용한 ICMP Echo, UDP 80, TCP 80 Syn, Http Get flood, Http Get & CC Attack 등 총 5종의 Traffic을 교대로 발생 시킴



<src: kisa>

7.7 DDos

➢7.7 DDos 공격의 특징

- 은닉화
- Logic Bomb 형태
- 다양한 업데이트 경로
- 기능별 구조화
- 효율적인 트래픽 분배와 영향력 있는 타켓의 선정
- 국내의 일반 PC의 좀비화

7.7 DDos

➢7.7 DDos 공격의 특징

- 은닉화
  - ▪공격 코드 자체를 분석이 어렵도록 구조를 분산하거나 핵심 부분에 대한 부분 Anti debugging 적용
  - ▪ 감염 이후 즉시 공격을 시작 하는 것이 아닌 지령을 통한 예약 공격 기능
  - ▪ 공격 명령 및 업데이트 기능은 flash.gif 형태로 알아채기 어렵게 함
  - ▪ 업데이트 서버 및 공격 지령 서버를 분산하여 세계 각지에 운영함

- Logic Bomb 형태
  - ▪ 예정된 공격 대상과 공격 형태 정의가 된 유형
  - ▪ 최종 공격 완료 이후에는 디스크 파괴로 증거 인멸

- 다양한 업데이트 경로
  - ▪ 해외에 6곳 이상의 Mirror site 운영 (공격지 및 형태 다운로드)
  - ▪ 총 14곳 이상의 접속 지점 운영
  - ▪ 메일을 이용한 업데이트 및 전파는 실패로 추정 (대량 스팸메일 발생으로 종료)

7.7 DDos

➢7.7 DDos 공격의 특징

- 기능별 구조화
  - ▪기능을 분산 시켜 둠으로써 이상 파일 탐지를 회피, 기능간의 조율 및 적용 최적화

- 효율적인 트래픽 분배와 영향력 있는 타켓의 선정
  - ▪세심하게 과다한 트래픽이 발생 되지 않도록 공격 형태 설정
  - ▪공격 기법의 다변화 (5종류 이상)
  - ▪ 예정된 공격 리스트를 트래픽 및 공격 대상도 분배하여 배정
  - ▪ 언론사 및 금융, 정부 기관, 포털 등 파급력 있는 곳을 선정 하여 과시성으로 대범한 공격 운영

- 국내의 일반 PC의 좀비화
  - ▪ 차단이 어려운 국내망의 일반 pc를 활용하여 공격
  - ▪ ip 변조가 수반되도록 하여 노출을 최소화
  - ▪ 기간마다 (1일간격) 다른 대상을 공격 함으로써 좀비 pc 노출 최소화

7.7 DDos

➢7.7 DDos에 관한 etc

- 좀비 pc 의 악성코드 유통 경로
  - 10만여대 이상의 좀비 PC 확보는 2009년 상반기 부터 진행 된 것으로 보임
  - 웹 하드 서비스에 가입 하지 않은 PC에서도 발견 (웹 하드 이외의 별도 유포 방식 이용 ?)
  - 웹 서비스의 취약성 (SQL Injection, xss)을 이용한 악성코드 유포는 일반적 현상임
  - 차단이나 감시망을 우회하도록 일정 규모 이상의 트래픽 발생을 하지 않음

- 기존 BotNet 차단 매커니즘의 한계
  - 기존 Botnet을 이용한 DDos 공격은 C&C 서버를 차단하는 것에 중점을 둠
  - 7.7 DDos는 C&C 서버가 사실상 존재 하지 않음 (공격 리스트를 업데이트 하는 유형만 존재)
  - 기존에 업데이트된 3일간의 공격은 차단 방법이 없었음. (만약 이후의 일자까지 있었다면?)

- 악성 행위의 정의는? 악성코드의 정의는?
  - 공격이 시작 되기전 기설치된 악성코드들은 그 자체로는 악성코드 진단 대상이 되지 않음
  - 백신에 의한 처리는 샘플 입수 후 사후 대응의 성격

7.7 DDos

➢7.7 DDos에 관한 etc

- 변화되는 공격 방식에 대한 연구 부족
  - 새로운 가능성과 위험 부분에 대한 연구 부족
  - Control 유형에서 업데이트 유형으로 변화 예측 부족 – 초기에는 기존 Botnet 차단 방식으로 접근 – C&C 서버 차단 방식
  - 다양한 공격이 결합된 방식에 대한 연구 부족
  - DDos 보안 장비로는 막기가 어려운 유형 (제품이 아닌 시스템과 체계로 해결 해야함)

- 과연 이게 끝일까?

  - CI (Critical Infra structure)에 대한 다양한 공격이 병행 된다면? 우리의 피해는? 연구는?
  - DDos 이후 동일 사건을 막을 수 있는 사전 대응 체계는 충분 했나? 진행 되고 있나?
  - 통합된 지휘체계는 안정적으로 운영 되고 있고 정보 교류는 제대로 되고 있나?
  - 악성 가능성이 있는 코드의 분별 (Risk) 에 대해 심도 있는 연구?
  - 취약한 웹 서비스들은 언제까지 방치 할 것인가? 기존 방식이 효과가 있었나?

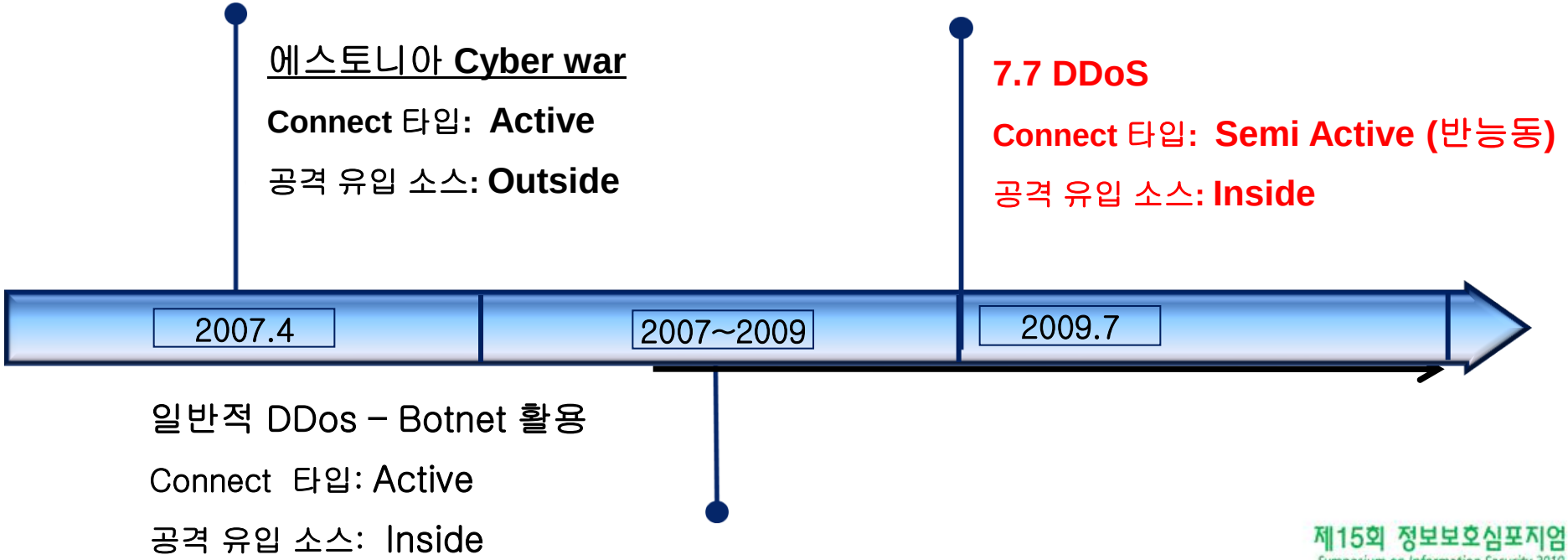
  (악성코드 유포 URL은 한주에 만개를 넘나든다. - ahnlab)

7.7 DDos

공격의 진화 및 대응

➢에스토니아, 7.7 DDos 공격 유형의 변화

- ➢ DDos 공격 유형은 크게 연결 방식과 유입 형태에 따라 구분.
  - ➢Connect 타입: Control 유형을 의미하며 Client를 통제 하는 방식에 따라 결정됨
  - ➢ 공격 유입소스: 보호 해야 될 Infra를 기준으로 선별 가능 (해외 또는 국내, 사내 또는 사외)



공격의 진화 및 대응

➢에스토니아, 7.7 DDos 공격 유형의 변화

- ➢ 각 이슈별 기본적인 대응 방안 : 개별 시스템 및 조직 단위의 기술적인 대응은 논외
- ➢ 연결 유형 , 공격 시작지점, Malware에 따라 특징을 잡을 수 있다.
  - 7.7 Semi active – C&C 서버 형태의 직접 제어가 아니라 Agent 차원의 직접 다운로드 방식으로 설계 – C&C 차단에 따른 Agent 소멸 효과 없음. 오로지 백신만이 대응 가능함

Estonia cyber war	General DDos	7.7 DDos, Future
Active	Active	Semi Active
Outside	Inside + malware	Inside+non malware
•Botnet C&C 차단 •외부 트래픽 차단 • 외부 도메인차단 • Black List 관리 • 정형화된 공격 패턴 관리	• Botnet C&C 차단 • Vaccine을 통한 Malware 제거 • 정형화된 공격패턴 대응	• Botnet C&C 차단 ???? (예정된 공격은 다 수행됨) • Vaccine을 통한 사후 대응 (다양한 변종 및 기능 분산으로 실 대응에 시간 소요) • 업데이트 서버 확인 후 차단 • 공격 형태가 예정된 형식으로의 자유 변화

공격의 진화 및 대응

➢공격 유형의 변화에 대한 대응

➢ 명령 전달 방식

- Download 방식 및 다양한 우회 전달 방식에 대한 대응 필요 (정보 공유 필수)

➢복합화된 공격에 대한 처리

- 다양한 DDos 공격 매커니즘에 대한 대응 방안 수립, 가변화 되는 공격 대응 필요
- 패턴 매칭의 대응은 한계치에 도달

➢ 사전 탐지 기능의 강화

- 공격 시작 되기전까지는 탐지 될 수 없는 악성코드 유형에 대한 준비
- 분석 샘플에 대한 종합적인 분석과 방향 제시 필요 (민.관 협동)
- 전역적 대응을 위한 유기체계 강화 (무료백신, 온라인 포털 서비스 등)

➢ 7.7 DDos는 실효적 공격의 충격 보다는 방식의 전환을 통해 허를 찔린 경우
만약 좀 더 치밀했고 계획적으로 구현 하였다면 큰 위기 상황 직면.
Agent 규모 확대, 명령 전송 방식의 노출 빈도 대폭 감소 , 여러 변종 활용, Anti debugging 기술, CI (Critical Infra)에 대한 공격이 병행 되었다면 심각도는 대폭 상승 하였을 것임

결 론

➢Lesson Learn

- ➢ 행위 기반 탐지 로직에 대한 연구 및 활성화
  - ➢ Network, System , File 단위

- ➢ 악성코드 공유 분석기능의 확대
  - ➢ 공유 분석 기능 이외에 예측과 전망을 고민 할 수 있는 기능 필수
  - ➢ 근본 문제 원인 제거를 위한 선도적인 예방 활동 강화 (Secure coding)

- ➢ 체계적 지휘통제 시스템 필요
  - ➢ 정확한 사건 개요 파악 이후 산별적인 대응이 아닌 체계적인 대응을 통해 피해를 최소화 해야 함. 컨트롤 타워의 활성화 및 전문가 집단화 필요

- ➢근본적인 악성 코드 유포 문제를 줄이기 위한 산업적, 국가적 노력 필요
  - ➢ 현재 웹서비스를 통한 악성코드 유포 문제는 무시 되고 있는 상황임.
  - ➢ 근본 문제 해결 (소스코드의 수정) 없이는 향후 악성코드의 범람과 그에 따른 추가적인 피해 (DDOS , 개인정보 유출)는 피할 수 없음.

결 론

➢Lesson Learn

- ➢ 보안 장비의 투입으로 현 상태의 근본적인 문제 해결은 불가능함.
  - ➢ 체계적인 대응 시스템에 대한 연구
  - ➢ 근원적인 문제 해결 체제 구축 (저렴하고 접근성 높으며 개발자 단위까지 영향을 미치도록)

- ➢ 일회적인 대응으로 그쳐서는 안됨
  - ➢현재의 산업의 발전 방향에 비추어 볼 때 향후 치명적인 요소가 될 것임
  - ➢ 7.7 이후 1년이 되어 가는 시점에 진행 된 것은 무엇?

- ➢ CI (Critical Infra Structure)에 대한 실질적인 보호 방안 강구
  - ➢ 만약 CI 내로 연결된 부분에서 문제가 발생 한다면????

- ➢ Risk = Threat (피해를 일으키는 사람, 사건, 이슈) * 취약성 * 파급력 (보관 정보의 가치 및 중요성) - 기반시설은 파급력이 높아지고 일반 시스템은 조금 더 낮아지는 정도

<u>전체 시스템에서 단 한 곳만 뚫려도 Risk는 기하급수로 증가한다.</u>

지금 우리는 어디쯤?

바다란 세상 가장 낮은 곳의 또 다른 이름
p4ssion@gmail.com

감사합니다.