유해트래픽의 원인과 대응책

2003년 06월 18일

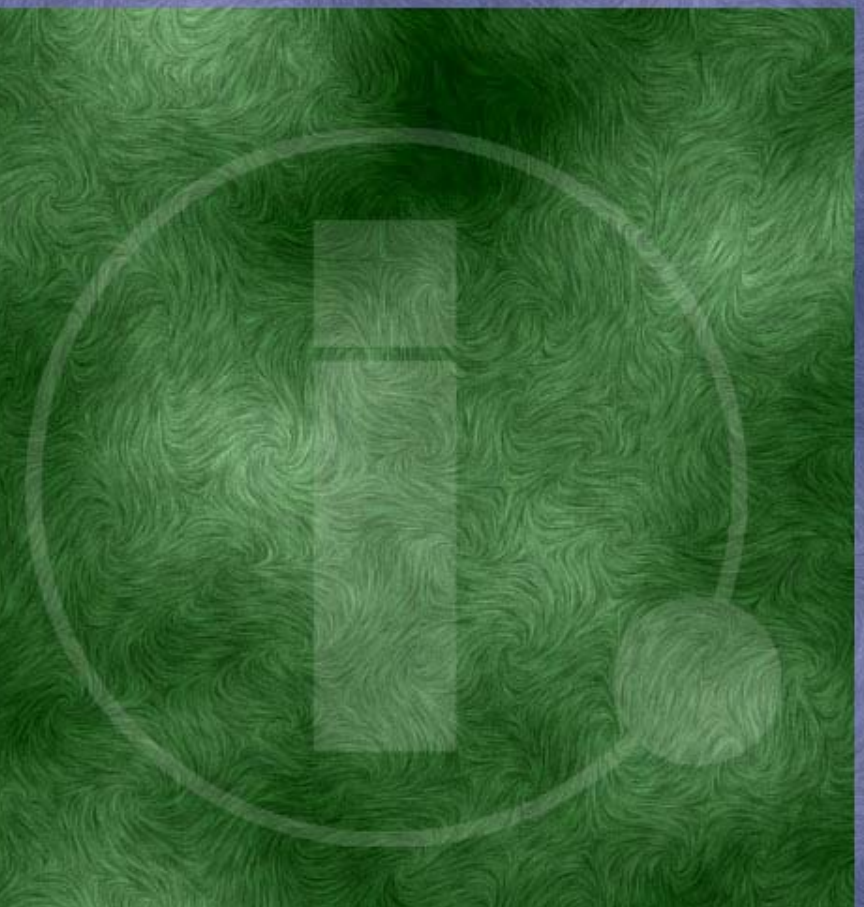
시큐아이닷컴
엔지니어링센타 팀장
윤덕상 (yoondark@secui.com)
CISA/CISSP

목 차

- 유해 트래픽의 출현 배경
- 1.25 인터넷 대란 Review
- 적을 알고 나를 알자!
- 유해 트래픽 대응방안

Next Topic

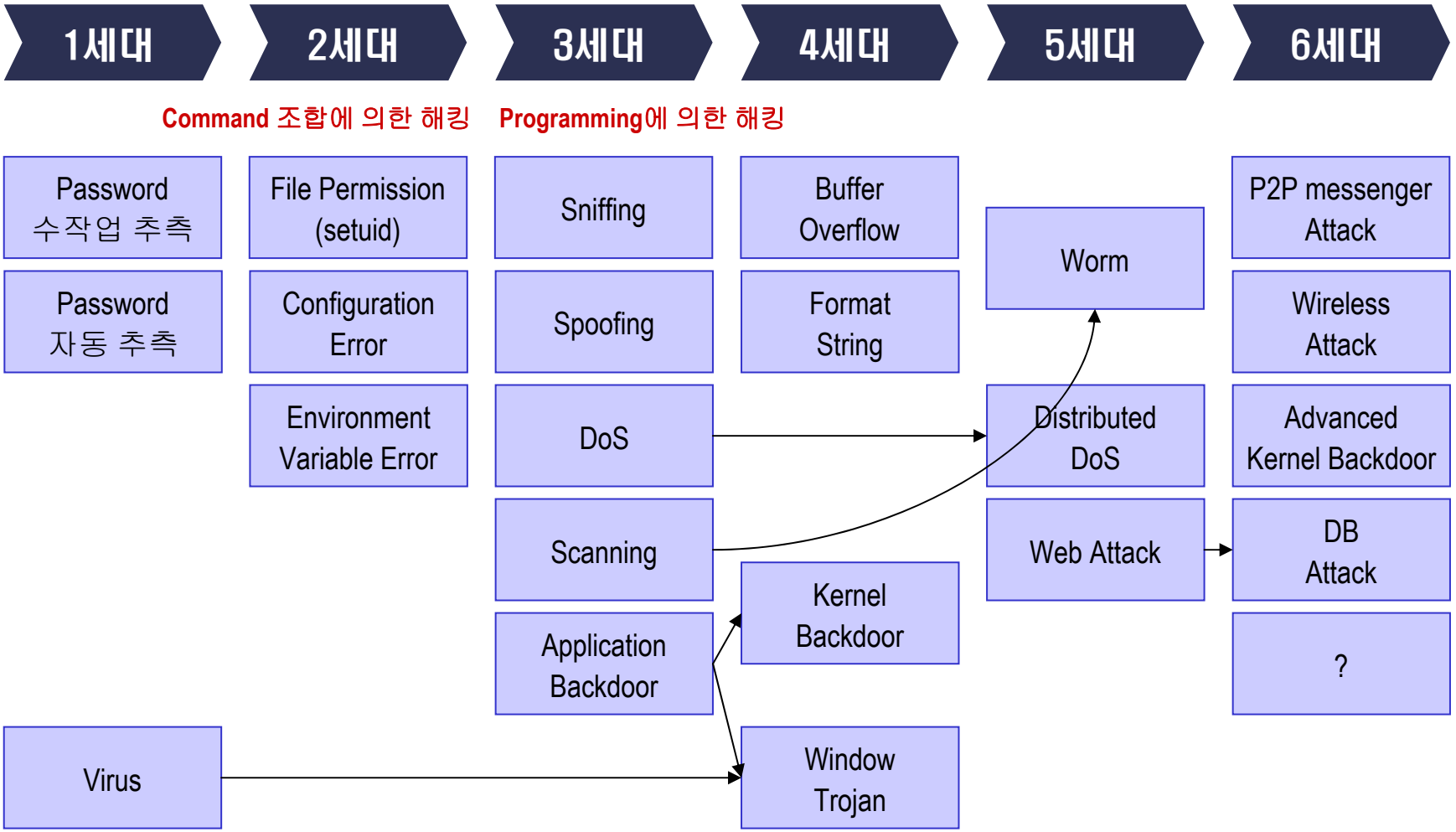
유해 트래픽의 출현 배경



- 유해 트래픽 출현 과정
- 공격기법의 다양화
- 가용성에 대한 위협
- 유해 트래픽으로의 발전

유해 트래픽 출현 과정

- 현재는 5세대에서 6세대로 변화하는 과정 중에 있으며, 1) 해킹기법의 다양화(수동→자동), 2) 서비스 가용성에 대한 위협 증대 3) 유해트래픽 폭증을 주요 특징으로 한 진화가 진행 중



공격기법의 다양화

- 과거 시스템과 네트워크에 대한 지식이 풍부한 사람만이 가능했던 해킹이 자동화 툴(Back Orifice, Daemon Tool 등)의 등장으로 일반인으로 까지 확산되고 있고,
- 과거의 해킹기법이 사라지고 새로운 해킹기법이 등장하는 개념이 아닌, 과거의 해킹기법이 존재하는 가운데 이를 한 단계 발전시킨 형태의 해킹기법의 출현으로,
- 미래에는 시스템 및 네트워크 단의 해킹기법이 수천 종에 이를 것으로 예상

Informational Warfare
Hacking, Password Cracking
Malicious Software, Virus
Trojan horses, Worm, Hoax, Logic bomb
Social Engineering, Disaster
Network Analysis, Eavesdropping
Traffic Analysis, Brute-force Attack
Masquerading, Packet Replay,
Message Modification
Unauthorized Access
Denial of Service
Dial-in penetration attack(war dialing)
Email bomb, Spam mail, Email Spoofing

가용성에 대한 위협 증가

- 과거의 해킹이 허가되지 않는 네트워크・시스템으로 침입하여 데이터의 절취, 변조가 목적이었지만,
- 현재에 와서는 네트워크・시스템의 기능을 마비시켜 서비스 자체에 위협을 가하는 형태로 발전
  (예 : 1.25인터넷 대란)
- 국가시스템(국방・공공・금융・통신) 전반이 정보인프라에 의존하는 현재의 추세라면 이에 대한 피해규모는 최소 수천~수조원 규모에 이를 것으로 예상

[통신 네트워크]

[공공 네트워크]

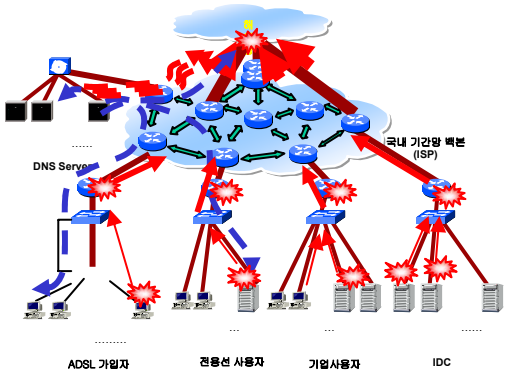
[금융 네트워크]

[국방 네트워크]

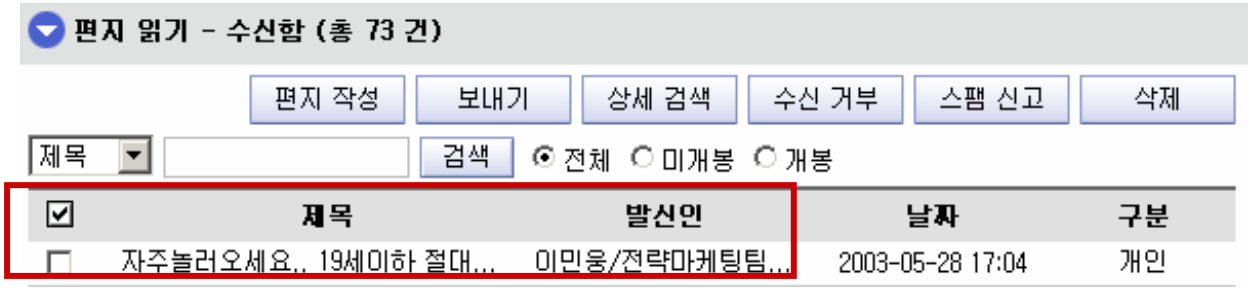
유해 트래픽으로의 발전

- 날로 고도화되고 있는 네트워크 성능에 대비하여, 이를 역이용한 수 만종에 이르는 컴퓨터 바이러스의 확산, 각종 스팸메일 및 불법자료 전송, 불법 사이트 접속 등에 의한 피해규모는 이미 수 조원대의 경제적 피해를 입히고 있음.

✓ 1.25인터넷 대란의 원인이 되었던 Slammer Worm

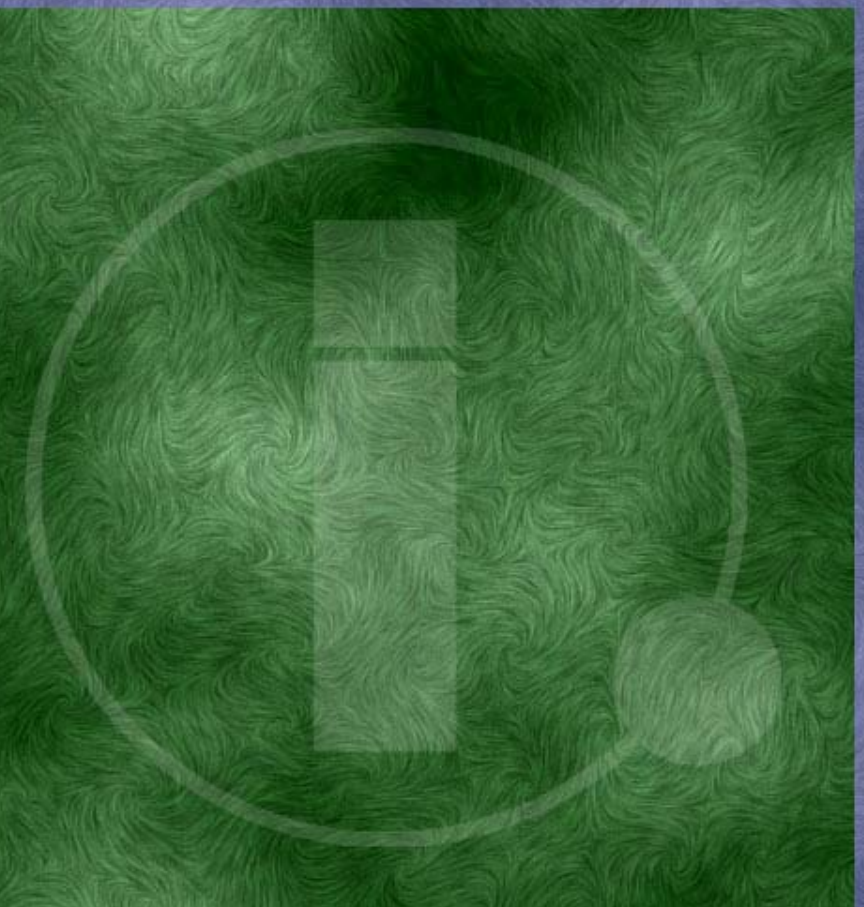


✓ 발신자를 수신자로 위장한 성인사이트 스팸메일 예



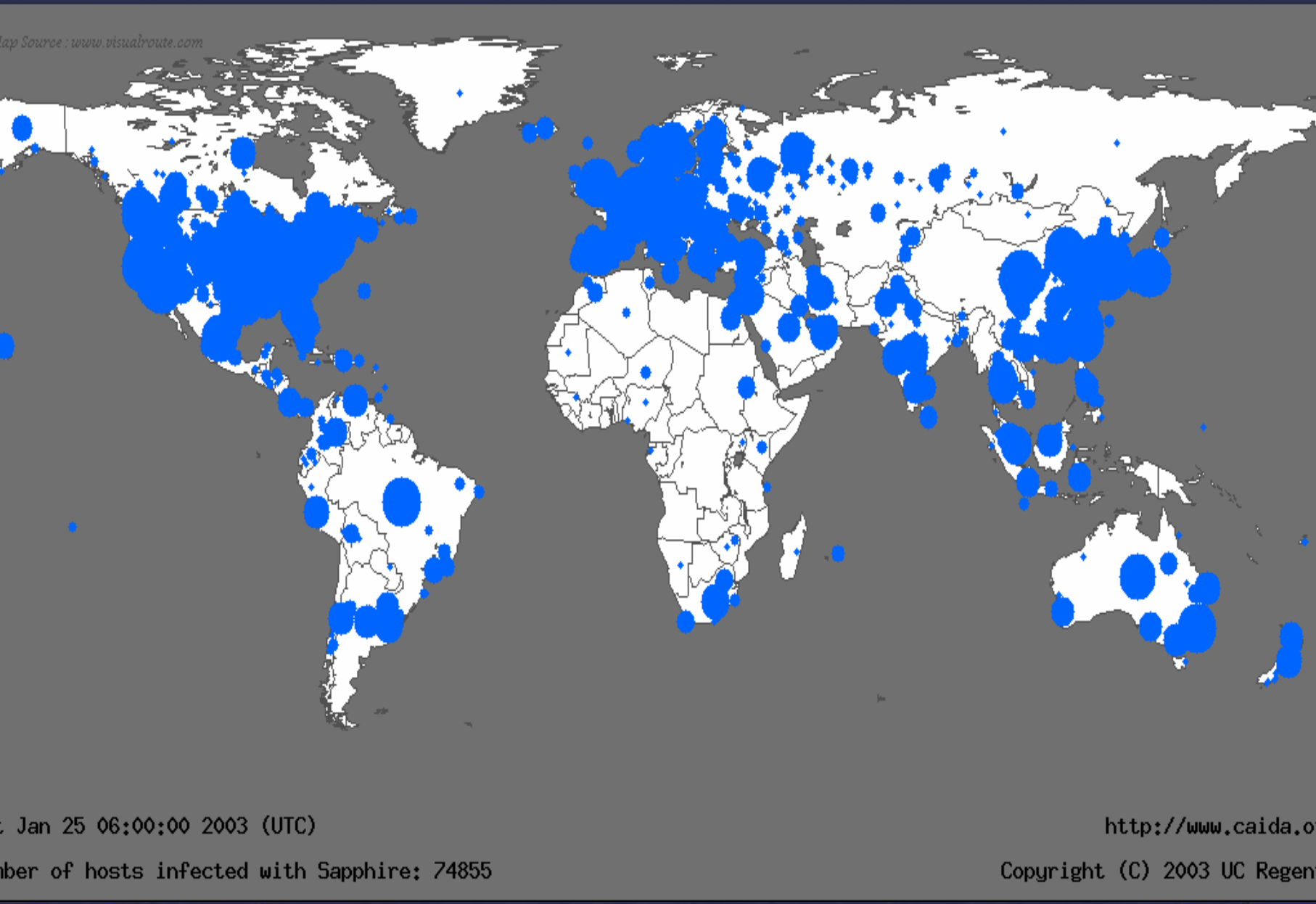
Next Topic

1.25 인터넷 대란 Review

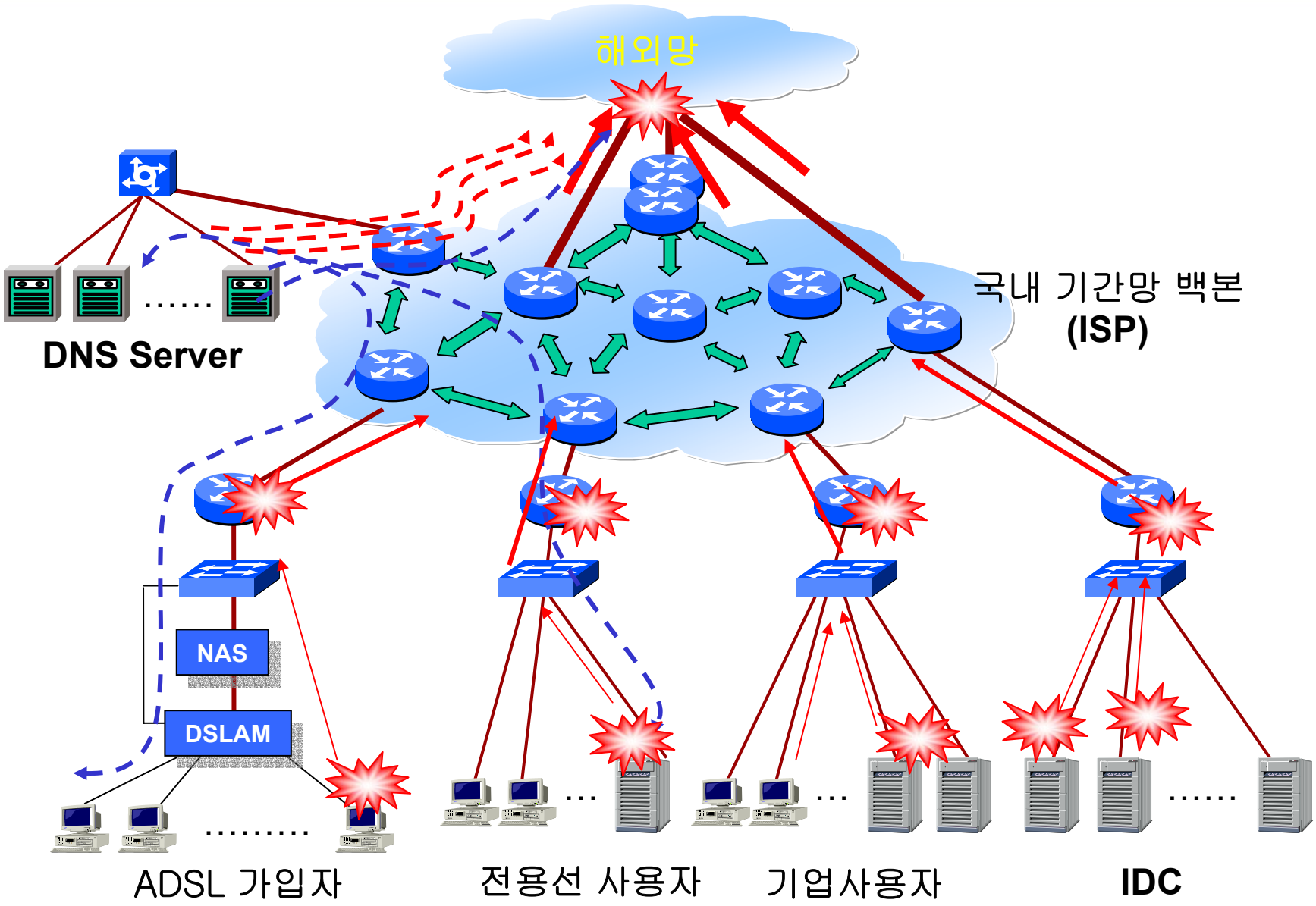


- SQL Slammer Worm 피해지역
- 1.25 대란의 진행과정
- 1.25 대란시 국내피해 확대 원인
- SQL Slammer Worm의 확산속도
- 1.25 대란의 교훈

SQL Slammer Worm 피해 지역



1.25 대란의 진행과정

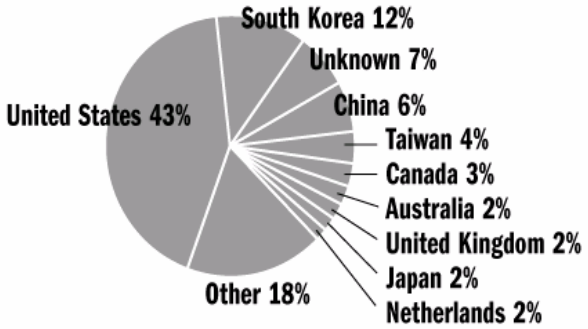

해외망
국내 기간망 백본
(ISP)
DNS Server
NAS
DSLAM
ADSL 가입자
전용선 사용자
기업사용자
IDC

1.25 대란시 국내 피해확대 원인

- 전세계 IP 블록 중 국내에 할당된 IP주소는 0.6%(2천6백만),다른 용도로 사용되는 멀티캐스트 IP용 6.2%를 제외하면, 확률적으로 슬래머 웜의 공격 패킷 중 93.2%가 국외로 발송되어 해외 관문지점의 병목 현상이 발생

구분	할당된 IP				다른용도 (사설, 시험)	미 할당 IP
	한국	미국	일본	중국		
IP(천개)	26,208	1,240,314	95,166	29,396	605.552	1,857,257
비율(%)	0.6	28.9	2.2	0.7	14.1	43.2

- **CAIDA Release (FEB 4)**
  By passively monitoring traffic, Globally, the Slammer Worm attacked 75,000 systems. Some 8,800 Korean System were affected, accounting for 11.82% of the systems attacked globally.

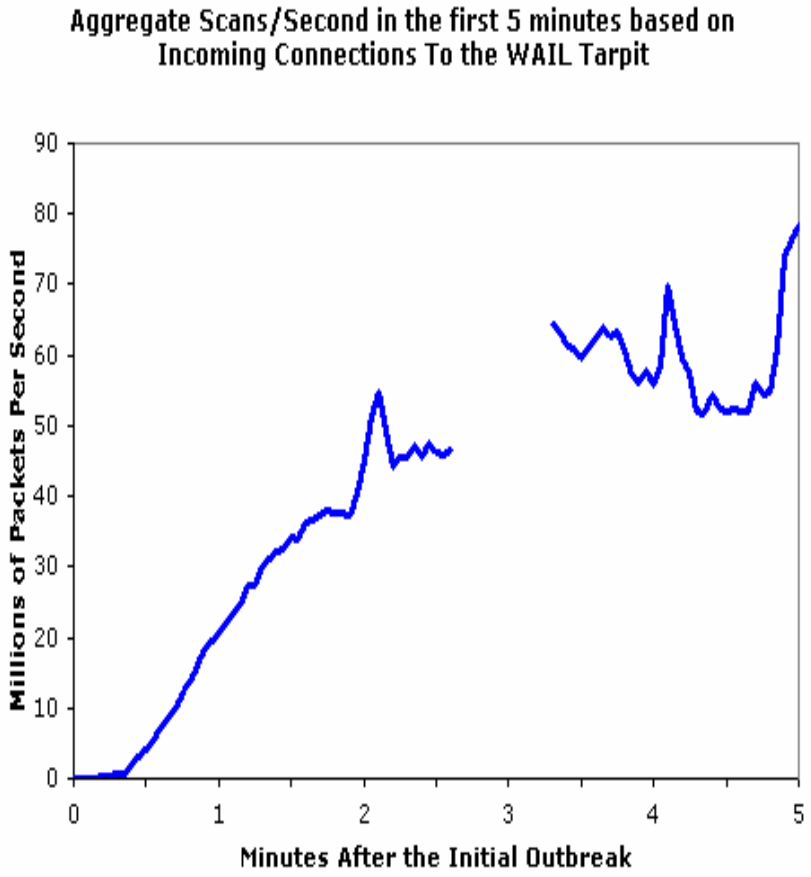


Distribution of machines infected by the Sapphire/Slammer worm.
(Credit: CAIDA/SDSC/UCSD, Gail Bamber)

http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

SQL Slammer Worm의 확산 속도

- 10분만에 전세계 75,000대 이상의 컴퓨터 감염
- 3분만에 전세계 IP 지역 Scanning 가능
  - > 55,000,000 IPs/s
- 매 8.5초마다 공격지역 2배씩 확장
  - Local 영역 감염시간 < 1 분내 가능



1.25 대란의 교훈 – 인식의 변화 필요

- 모두가 피해자이면서 가해자?

나는 피해자다!!!!!!!

천만에.....

1.25 대란의 교훈 – 전역방어 전략 필요

- 지역보호가 아닌 전역방어 전략 필요
  - 더 이상 나홀로 잘하는 보안은 의미가 없다.

감염 차단 및 정보 보호 목적은

달성하였으나 테러영향을 피해

갈 수 없었다 !!!!!!!

1.25 대란의 교훈 – 새로운 개념의 보안장비 필요성 증가

- 보안장비의 역할 및 활용 방법 재정립 필요
  - 방화벽 : 시키는 일만하다 못 견디면 죽는다?
    - 사전 감시, Traffic Shaping, Session Shaping 기능요구
  - IDS : 혼자서는 아무 일도 못하는 보석가게의 CCTV 이다 ?
    - Unknown 공격 판단 및 차단기능요구
  - ESM : 전원 뽑힌 영사기(?), 넌 뭐했니?
    - 사전감시 기능 및 조기경보 체계 확보 요구
    - 공격 Traffic과 분리된 안전한 감시망 요구
  - Anti-Virus : 혼자서 다 하는 척 한다 ?
    - 치료 기능 이외에 Patch 진단, 배포 등 예방기능 요구
    - 최종 대안이므로 근본적인 차단대책 우선필요

1.25 대란의 교훈 – 조기경보 및 대응체계 구축 필요

비상대응 및 사전감시 체계 구축 필요

- 방화벽, **IDS**는 보호해야할 대상 및 목적이 명확한 곳에서 필요한 보안장비이다.
- 백본망에서는 무엇을 차단하고 무엇을 허용해야 할지 판단이 불가능하며 차단할 권리도 없기에 공격의 발생을 근본적으로 차단할 수 없다.
- 하지만 백본망 서비스의 기본 취지인 가용성을 최대한 보장해야 하며
- 다수의 사용자에게 피해가 예상되는 위협에 즉시 대응할 수 있는 체계를 갖추어야 한다.
- 이를위해 백본망에는 사이버 공격에 대한 방어의 개념과 발생지역을 즉시 고립시키고 피해의 확산을 지연시키기 위한 트래픽 댐**(Blocking Sensor)**의 개념을 도입해야 한다.

비상대응체계	피해 지역을 즉시 고립시키고 피해서비스를 차단할 수 있는 중앙통제식 네트워크 차단 시스템 구축 (Blocking)	단기구축
사전감시 및 조기 경보체계	공격징후를 실시간 파악하고 위험경보를 즉시 전파할 수 있는 사전 감시 시스템 구축 (Sensor)	장기구축

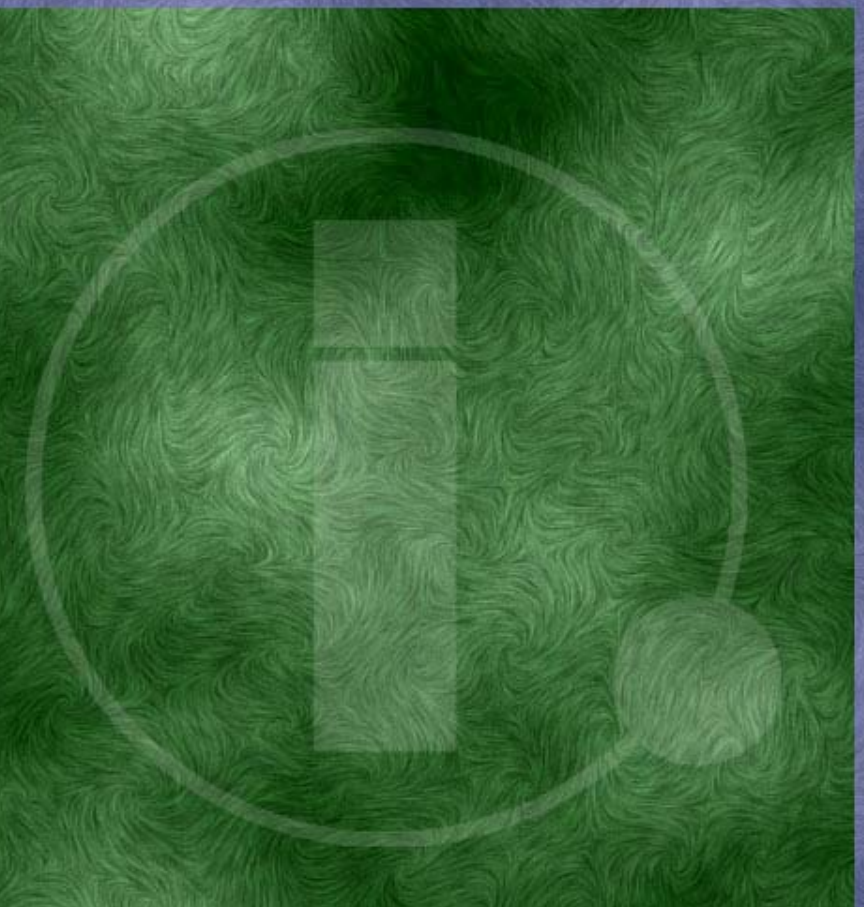
1.25 대란의 교훈 – 네트워크 운영의 구조적 문제 해결 필요

네트워크 및 DNS의 구조적 문제점 개선

- Local 망 → ISP망 → 국가기간 망 → 국제 망으로의 도미노식 피해 확산 방지대책 필요
  - Default Routing 경로에 대한 Traffic 분산 및 다중경로 대책수립
- DNS 서버 운영대책 수립필요
  - 전국적인 사용자를 보유한 DNS서버의 경우 지역분산 정책 수립
  - 주요 Domain의 삭제 및 변경 시 DNS운용자간 상황교환 필요
- Log 관리 체계 정비 필요

Next Topic

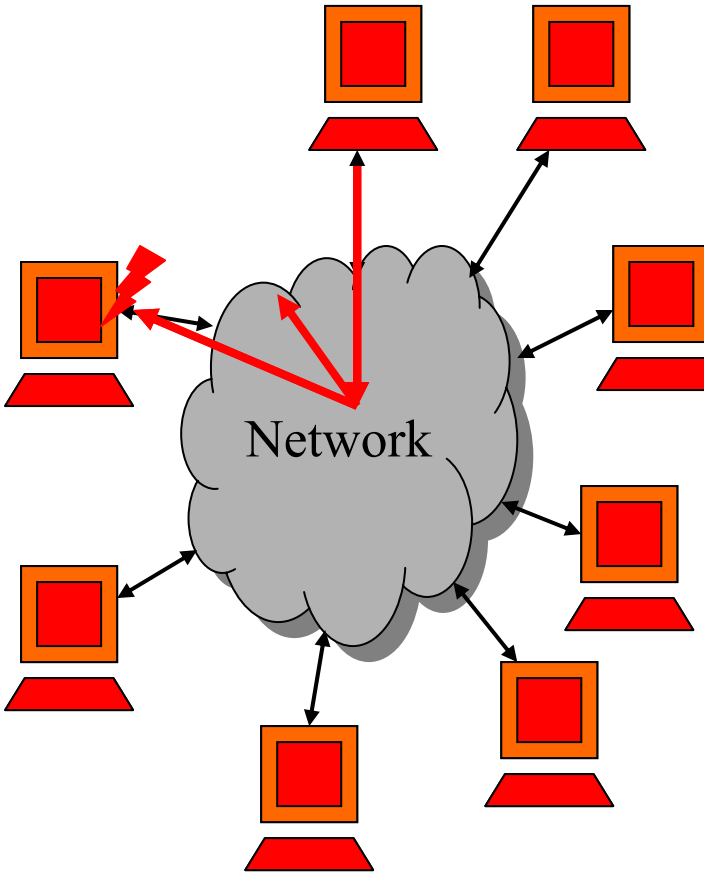
적을 알고 나를 알자!



- Computer Worm이란 무엇인가?
- 왜 Worm이 위험한가?
- 지금까지 출현했던 주요 Worm들
- 공격자들이 Worm을 좋아하는 이유
- Worm이 노리는 주요 공격 대상
- Worm이 선택할 수 있는 확산방법
- 확산방법 분석

Computer Worm이란 무엇인가?

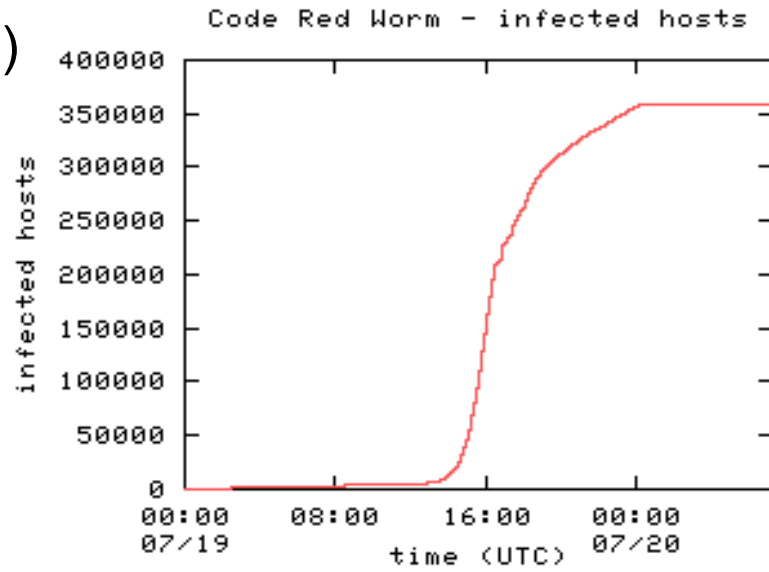
- 자기 복제형 네트워크 프로그램
  - 원격컴퓨터 감염을 목적으로 취약점 공격
  - 감염된 서버들이 또 다른 서버를 공격
- 3가지 공격단계
  - 새로운 공격 목표 탐색
  - 목표 발견시 공격코드 전파
  - 피해 시스템내 공격코드 실행
- 최초 공격이후 사람 개입 불필요
  - Autonomous worms



왜 Worm이 위험한가?

- 사람이 대응할 수 있는 시간보다 빠르다
  - Code Red : 13시간만에 전세계 감염
  - SQL Slammer Worm : 10분만에 전세계 감염
  - 기술발전에 따라 얼마든지 더 빠른 Worm 출현 가능

- Worms에는 매우 위험한 Payload 내장
  - DDOS (Distributed Denial of Service) Attacks
  - Internet scale espionage
  - Data corruption
  - BIOS reflashing



Graph from David Moore's analysis (caida.org

지금까지 출현했던 주요 Worm들

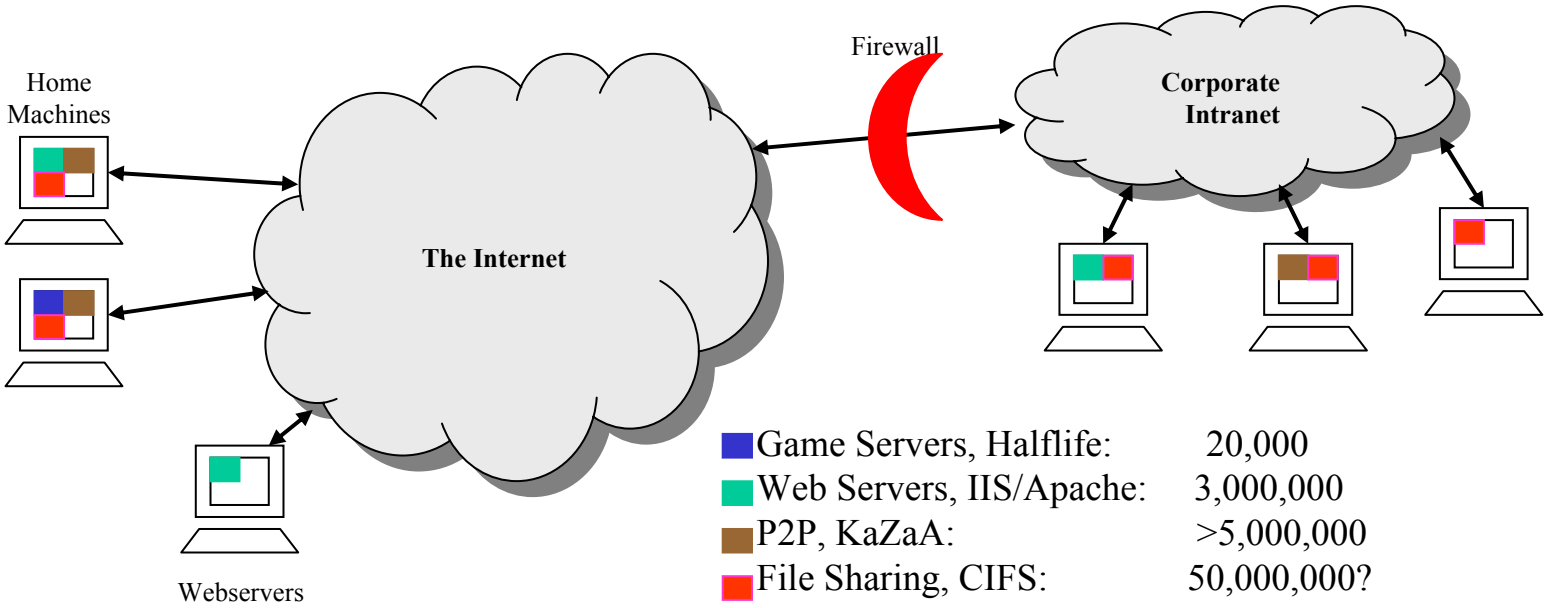
Worm	년도	유형	피해	기타
Morris	1988	Topological	6000	최초의 지능형 Worm 여러가지 취약점 공격이용 전파
Code Red	2001	Scanning	~300,000	최초로 빠른 전파속도를 갖음
CRClean	2001	Passive	none	Anti-Code-Red worm.
Nimda	2001	Scanning Others	~200,000	Local subnet scanning. 여러가지 기능을 효과적으로 조합
Scalper	2002	Scanning	<10,000	취약점 발견뒤 10일만에 출현
Slapper	2002	Scanning	13,000	Scalper Code의 변형
Sapphire (Slammer)	2003	Scanning	>75,000	10분만에 전세계 전파 가장 빠른 전파속도를 자랑

공격자들이 Worm을 좋아하는 이유

- Worm은 가장 효과적인 공격수단
  - 한번에 모든 취약한 시스템들을 공격할 수 있다.
  - 기존 공격에 비해 추적이 어렵다.
- Worm은 제작이 간편
  - 전파 코드가 정형화 되어 있으며 재사용 가능
    - 공격 + 전파
  - Payload내에는 전파기능과 무관한 코드 내장 가능
- 취약점 발견 후 10일만에 출현 기록(Scalper)
  - 최근의 기술로는 1일 이내에 Worm 제작가능
  - Smart attacker라면 당일날 Worm 제작도 가능할것
    - 아직까지 알려지지 않은 취약점을 이용할 수도 있음.

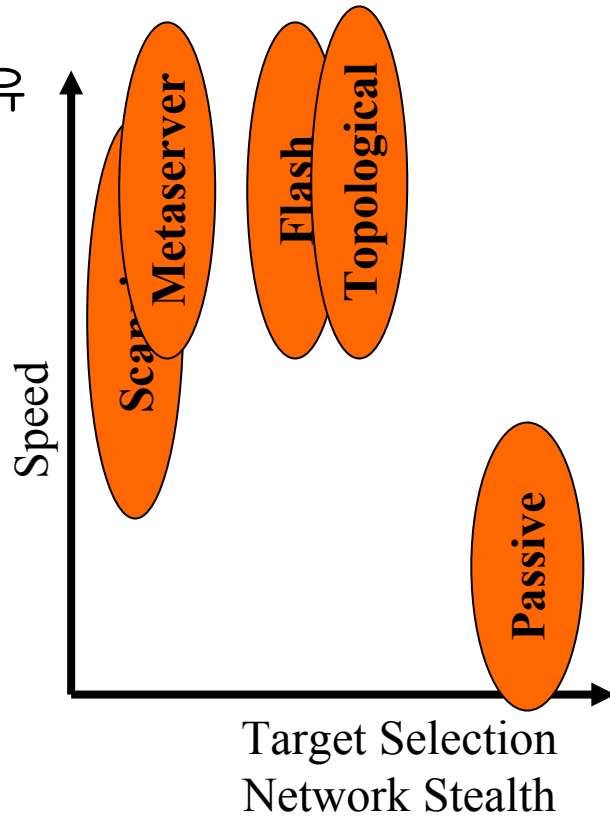
Worm이 노리는 주요 공격 대상

- 주요대상 : 사용자가 많은 유명한 네트워크 프로그램이나 운영체제
- Slammer Worm를 기준으로 취약시스템이 20,000대 이상이면 전세계 장악가능
- 주요 공격대상 후보
  - Windows 운영체제나 기본 프로그램의 취약점(CIFS등) 50,000,000 이상
  - P2P 프로그램(eDonkey, WinMX, KaZaA, 소리바다등) 5,000,000 이상
  - Web Server & Service Program 3,000,000 이상
  - 기타 Game Server 및 응용프로그램 20,000 이상



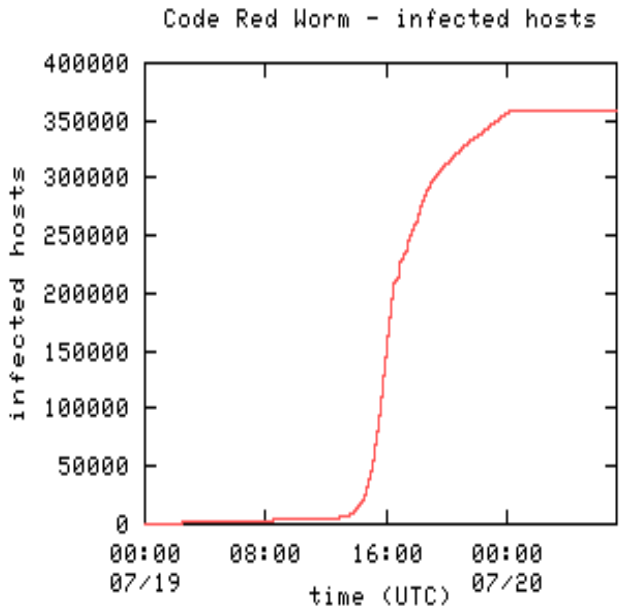
Worm이 선택할 수 있는 확산방법

- Scanning : Random한 목표 선택
  - 가장 일반적, 하지만 속도가 늦음
- Metaserver : 외부 서버로부터 공격 List 수집
  - 빠름, Application에 의존적
- Hitlist & Flash : 사전 제작된 공격 List 보유
  - 빠름, 사전 목표수집기간 필요
- Topological : 감영서버로 부터 공격목표 수집
  - 빠름, Application 의존적
- Passive : 접촉감염(스스로 전파 능력 없음)
  - 속도가 느림, 하지만 탐지가 어려움
  - 외부의 Event의 도움으로 전파
- 여러 종류가 복합된 Worm 출현 가능



확산 방법 분석 – Scanning Worms

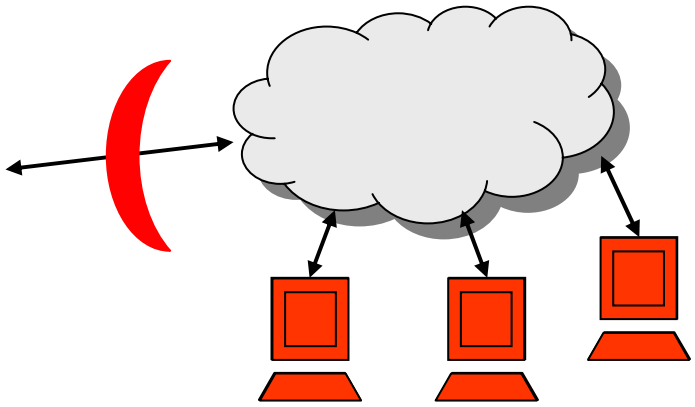
- 무한 반복형 공격
  - Random Address를 취함
  - 해당 서버가 취약하면 감염
- 구현이 매우 간단함
  - 대부분의 코드가 정형화 되어 있음
- 속도(K) 결정항목
  - Rate of scanning
  - Number of vulnerable machines
  - Size of address space
- 초기 감염 이후 기하급수적 확산
  - 이미 공격된 서버에 대한 중복공격 등으로 효율 감소



$$K = \frac{\text{Scan Rate} * \text{Vuln Machines}}{\text{Address Space Size}}$$

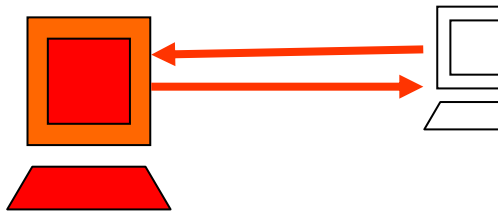
확산 방법 분석 – Scanning Worms 변형

- Local subnet scanning
  - Local지역의 취약서버를 우선 공격
  - Code Red II, Nimda
  - Firewall등의 차단 고려
- More Populated Addresses 우선 공격
  - scalper & slapper
  - Scan over-head를 줄임
- IP Class 단위 Scanning(/24s)
  - Scalper & Slapper
  - Routing-related Cost를 줄임
- Bandwidth-limited scanner
  - SQL Slammer
  - Scanning 속도를 빠르게 함

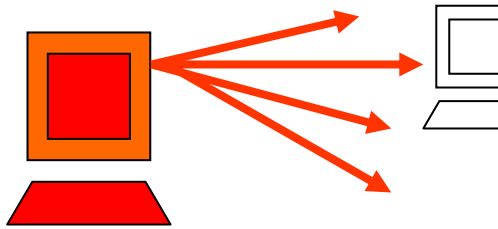


확산 방법 분석 – Bandwidth Limited Scanning

- Code Red의 Scan방식은 Latency-limited 방식
  - Thread 단위: SYN Packet을 Random 주소로 보내고 Response나 Timeout을 기다림
  - Code Red Scanning 속도 : ~6 scans/second,
    - 피해 지역이 2배가 되는데 40분이 소요



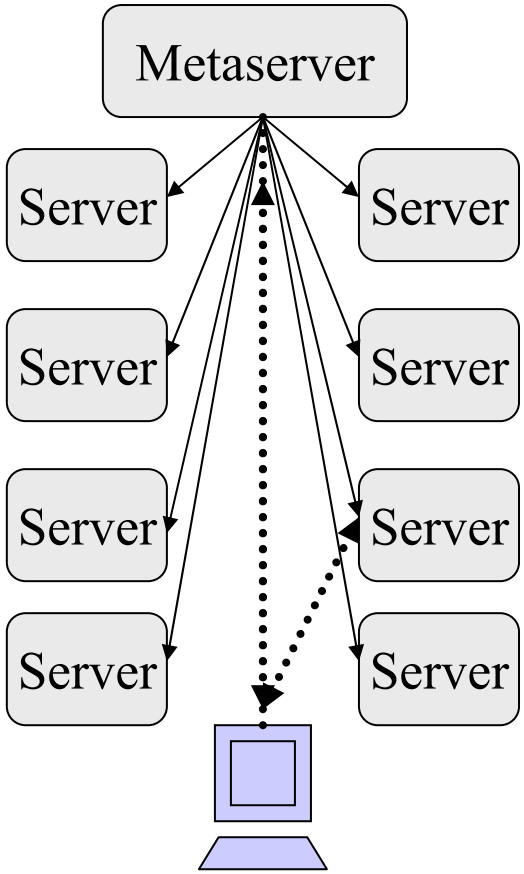
- Slammer의 경우 Bandwidth-limited 방식
  - UDP 패킷사용 (Connetion Overhead 없음)
  - 1 Mb bandwidth → 280 scans/second
  - 100 Mb bandwidth → 28,000 scans/second

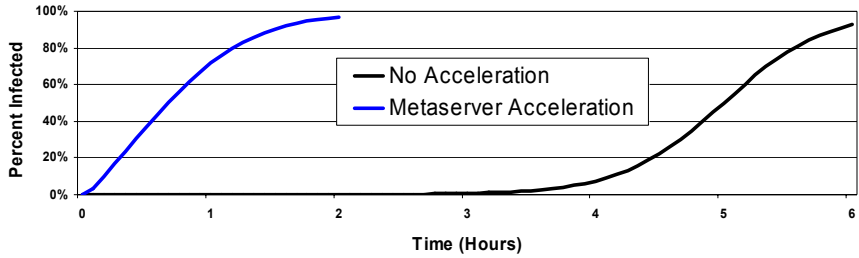


- 작은 Size로 제작된 TCP Worm의 경우도 Slammer와 같은 속도로 전파될 수 있음.
  - SYN 패킷을 Line Speed로 보내고
  - ACK 패킷을 다른 Thread가 처리하도록 할 경우

확산 방법 분석 – Metaserver Worms

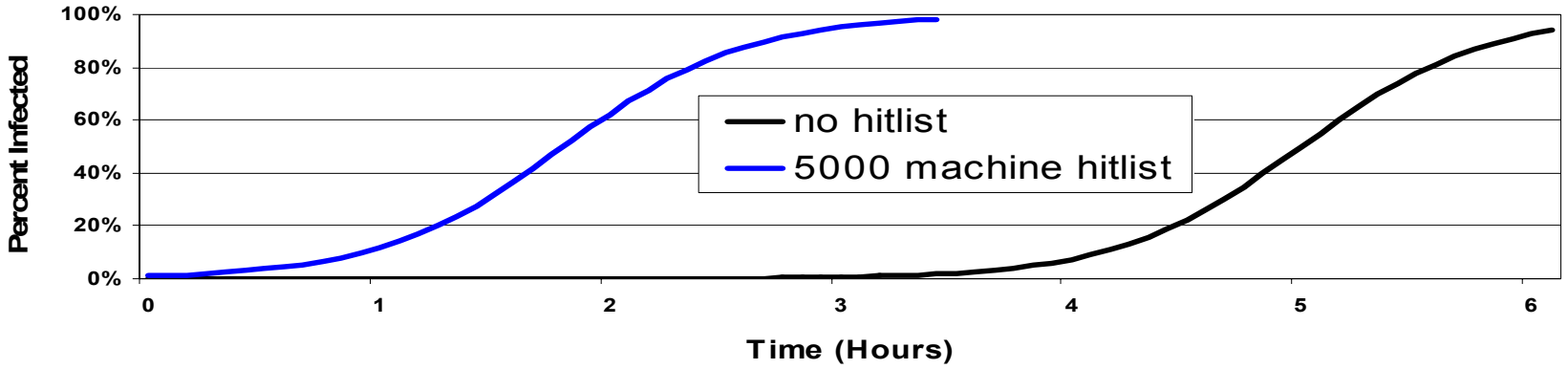
- 제 3지역의 서버로부터 공격목록 수집
  - Games 서버 이용: 게임 상대자 정보수집
  - 검색엔진 이용: Web서버들의 정보 수집
  - Windows Active Directory: Network Neighborhood 정보 수집
- 이 방법이 효과적인 이유
  - Active된 서버에 대한 정보수집 가능
  - 각각의 감염시스템이 정보수집에 동원
    - Divide-and-Conquer 전략 활용
- 아직까지 발견되지는 않음





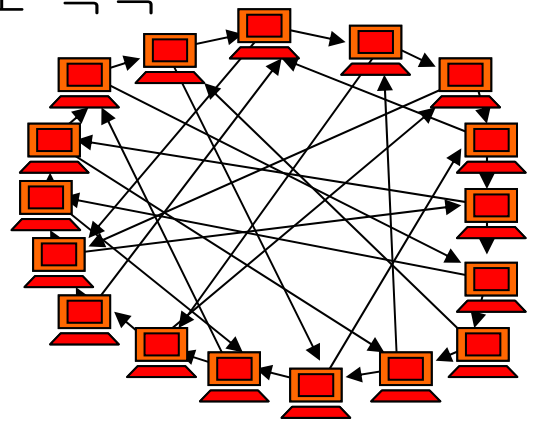
확산 방법 분석 – Hitlisting & Flash Worms

- 취약한 서버들의 공격리스트를 가지고 공격시작
  - divide-and-conquer 공격전략 : O(lg(n)) time
  - Scanning Worm보다 훨씬 빠른 공격 가능
  - 대상 서버를 모두 공격하는데 1분 미만 소요(Flash Worm)
  - Hitlist는 완벽하게 정확할 필요는 없음
- 원시적인 생각임에도 아직까지 발견안됨
  - 취약 서버 정보를 수집해야하는 문제점이 있음



확산 방법 분석 – Topological Information

- 새로운 공격 목표를 감염 서버 내에서 찾음
  - 감염 서버 내 DISK나 Cache로부터 URL정보 획득
  - Mail 주소록 이용
  - UNIX의 Hosts, .ssh 파일 등 이용



- 대부분의 Mail Worm에서 나타남
  - 최근에 출현하는 Mail Worm들은 좀더 지능적인 방법들을 동원함

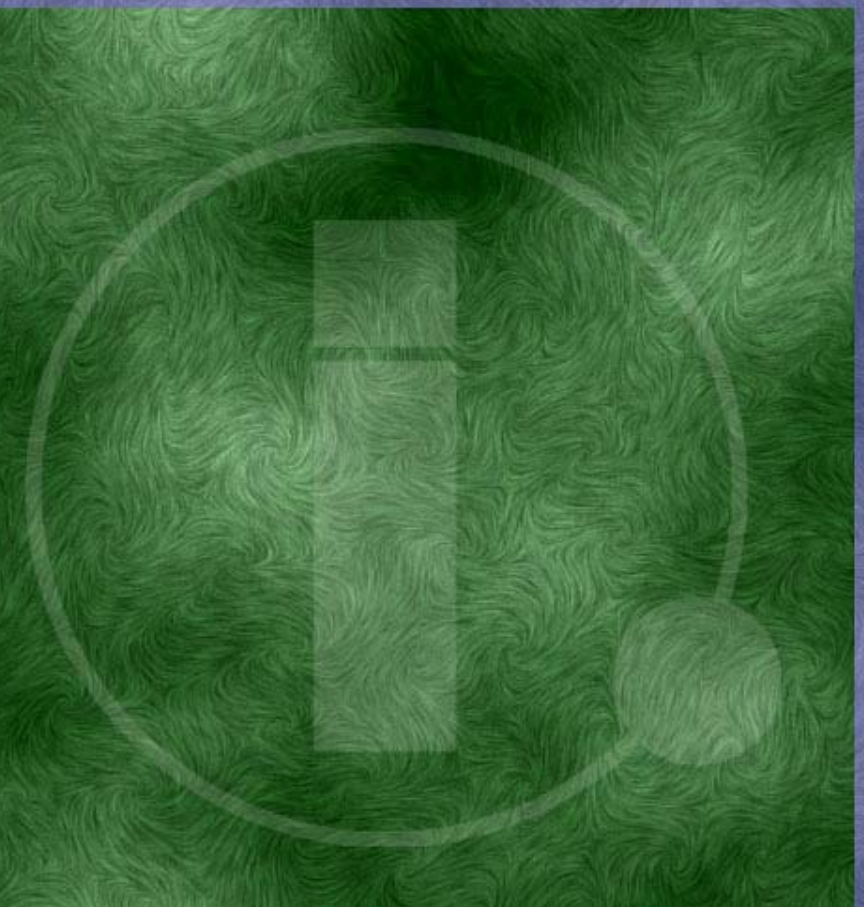
- 인류 최초의 Worm인 Morris worm에서 사용
  - 그 당시 Scanning 공격을 하기에는 사용하는 Address Space가 너무 적었음

확산 방법 분석 – Passive Worms

- 스스로 공격하지 않고 Event를 기다림
  - CRclean: Anti-CodeRed II Worm
    - Wait for Code Red, respond with counterattack
  - Nimda: Trojan web-page를 통해 접근 사용자 감염
- 감염 속도는 예측 불가능
  - Event를 발생시키는 Traffic에 의존적
- Stealth 능력이 뛰어남
  - Scannig 동작이 없어서 감염동작을 통해 탐지해야함
  - Normal Service를 이용할 경우 탐지 거의 불가능

Next Topic

유해 트래픽 대응방안



- 경계 해야 할 유해 트래픽의 유형
- 효과적인 유해 트래픽 억제 방법
- 자동화된 탐지, 분석, 대응시스템 필요
- 유해 트래픽 출현 시 나타나는 이상 징후들
- 유해 트래픽 출현 시 행동요령
- 어떻게 대응해야 하나?
- 대응 솔루션
- Q&A

경계해야 할 유해 트래픽의 유형

분류	공격유형	특징	피해 범위	대응방안
Worm형 공격	1. 다수의 사용자가 사용하는 운영체제나 네트워크 응용프로그램의 취약점을 이용 2. 스스로 감염 및 전파를 수행하는 공격	1. 공격 발원지나 공격 목적지를 구분할 수 없음. 2. 특정 프로그램의 취약점을 이용하므로 통신 Port가 고정되어 있음. 3. 하지만 범용포트(Ex:80/tcp)를 이용하는 경우도 많음 4. 소멸까지 장시간 소요	1. 피해지역 : 인터넷에 연결되어있는 모든곳 2. 파괴력 : 매우 높음	1. 1차 감염 예방 2. Port 차단 3. Contents Filtering
DDOS공격	1. 여러 지역에 있는 취약한 시스템을 사전에 해킹 2. 공격프로그램을 심어 놓고 원격조정으로 한번에 특정 서비스나 네트워크를 무력화	1. 여러 지역에 분포되어 있는 시스템으로부터 공격 2. 공격발원지를 알 수 없으나 특정 서버나 네트워크를 대상으로 하므로 목적지가 고정되어 있음.	1. 피해지역 : 공격 목적지 및 경유지 2. 파괴력 : 높음	1. 차단기능만으로 대응불가 2. Traffic Shaping 3. Session Shaping
시스템 해킹	1. 특정 사용자가 운영하는 시스템에 악의적인 목적으로 2. 허용되지 않는 접속이나 프로그램 수행	1. 공격 발원지나 목적지의 정보를 쉽게 알수 있으나 위조 혹은 중간 경유지 이용 2. Traffic 이상등의 징후가 없으므로 감지가 어려움	1. 피해지역 : 공격을 받은 특정 시스템 2. 파괴력 : 매우 높음 (막대한 손해)	1. 차단 및 탐지용 보안장비 설치
바이러스	1. 자체적인 전파능력이 없음 2. 특정 파일에 기생하여 이동하는 악성 프로그램	1. 바이러스는 네트워크를 스스로 이용하지 않으므로 네트워크에서 탐지 불가 2. 최근들어 Worm과 결합된 Worm Virus 출현	1. 피해지역 : 감염파일을 사용하는 모든 PC나 시스템 2. 프로그래머의 악의성에 따라 피해범위가 가변적임	1. Virus Wall 2. 시스템 및 개인 PC에 Virus 백신 프로그램 설치

효과적인 유해 트래픽 억제 방법

- Bug없는 프로그램 제작(?)
  - Bug는 항상 존재가능(Stack Overflows 등)
  - Patch가 개발되지만 적절히 적용되지 않음
- Firewall, IDS, Anti-Virus 설치(?)
  - 조그마한 헛점을 이용해서 손쉽게 돌파가능
  - 알려지지 않은 취약점을 이용하는 공격이 많음
- 자동 탐지 및 차단이 최선(Automatic Responses)
  - Slammer Worm은 사람이 대응하기에는 너무 빠르다.
  - 공격특성에 따른 유연한 대응가능 장비 필요
- 기타 필요사항
  - 유용한 분석도구
  - 긴급 대응 및 복구 체계
  - 프로토콜별 대응 시나리오

자동화된 탐지, 분석, 대응 시스템 필요

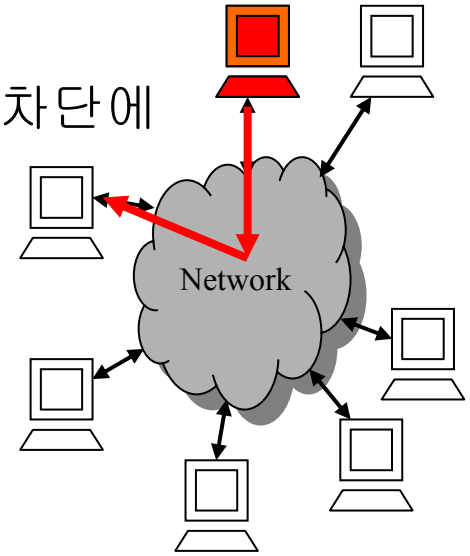
- Automated Detection: 유해트래픽의 활동 탐지
  - 유해 트래픽의 발생여부 및 유해여부 탐지
  - 유해 트래픽의 전파경로 탐지
  - 지역적 접근이 아니라 ISP, 국가기간망과 연동한 접근 필요
- Automated Analysis: 유해트래픽의 특징 및 대응책 분석
  - 어떤 방법으로 전파되는가?
  - 어떠한 서비스의 취약점을 Target으로 하는가?
  - 어떠한 시스템들이 취약한가?(Signature 탐지)
  - 어떤 장비가 피해를 입었는가? 는 무의미
- Automated Response: 확산 차단 및 복구

유해 트래픽 출현시 나타나는 이상 징후들

- Scanning 이용방식
  - Connection 요구에 대한 Reject, 무반응 패킷 증가
  - 대부분의 경우 다양한 IP 대역이 빠르게 나타남
- Metaserver 이용방식
  - Connection 요청이 매우 많아짐
  - 서버에서 사용하지 않는 Query가 발생
  - Outgoing Connection이 폭발적으로 증가함
- Hitlists 이용방식
  - Outgoing Connection이 폭발적으로 증가함
- Topological 형태
  - Outgoing Connection이 폭발적으로 증가함

유해트래픽 출현 시 행동요령

- 확산방법을 신속히 분석
  - 유해 트래픽의 확산방법을 가장먼저 이해
  - Worm이 선택할 수 있는 확산방법은 제한적임
- Worm을 탐지하지 말고 확산방법을 탐지
  - 사전에 알려지지 않은 유해 트래픽에 대한 대책 수립
- 신속한 유해트래픽 확산경로 차단
  - 현재 감염된 서버 복구 보다는 추가적인 확산 차단에 주력
  - 탐지 및 분석결과를 최대한 활용



어떻게 대응해야 하나?

- Network Level의 Detector/Responder 구축
  - 고성능, 다기능 탐지 및 방어장비 필요
    - Flexible, Fast and Reasonably Low cost
    - 유해 트래픽의 특성을 감안한 새로운 방어기능 탑재
    - 고성능(Gigabit이상) 및 다기능 수행 필요
  - 지역 감시체계가 아닌 전역감시체계로 전환

- Multi Layered 분산 감시 체계 구축
  - 유해 트래픽의 행동특성을 이해하고 출현감지 및 자동 대응이 가능한 장비 및 체계 구축

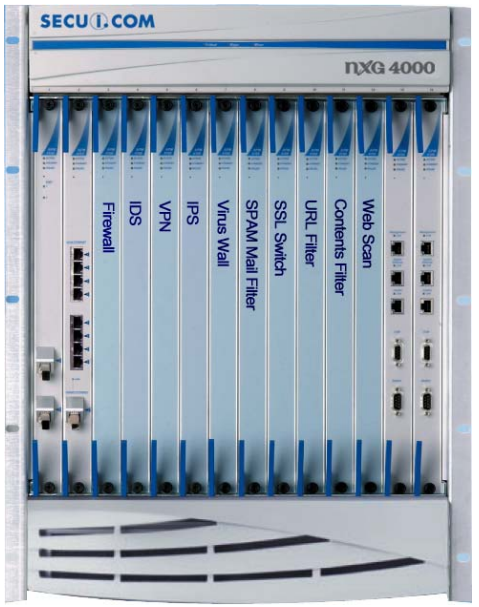
대응 솔루션

Such unique solutions are provided only through SECUi.COM called NXG(Next Generation Gateway)

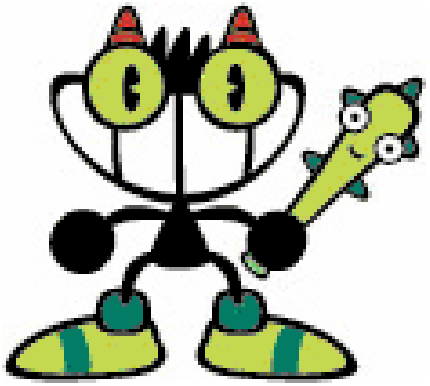
I would like to invite you the next session "The World of NXG"

Next Generation Gateway

nXG



Q&A



감사합니다.