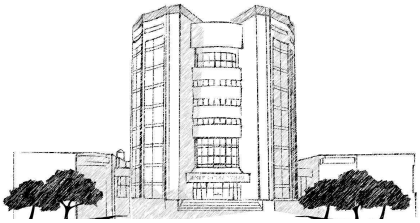
# 2015년 KISTI 침해사고 대응 분석 보고서
## (1/4분기)



2015. 11.

KISTI 한국과학기술정보연구원
Korea Institute of Science and Technology Information
www.kisti.re.kr

## 목 차


I. 개요 ····· 1
1. 목적 및 필요성 ····· 1
2. 분석 내용 및 범위 ····· 1
3. 분석 활용 계획 ····· 1

II. KISTI 침해사고 대응 ····· 2
1. KISTI 침해사고 대응체계 ····· 2
2. 대응절차 ····· 3

III. 현황 분석 ····· 5

IV. 종합분석 및 개선방안 ····· 17

V. 결론 ····· 21

[별첨 1.] 월별 침해위협 발생 현황 ····· 23
[별첨 2.] 부서별 사고 건수 ····· 25
[별첨 3.] 침해시도 유형별 내용 ····· 26
[별첨 4.] 사이버위기 상황 발생 시 대상별 협조 사항 ····· 27


## 그림목차


[그림 1. KISTI 침해사고 대응 체계] ····· 2
[그림 2. KISTI 침해사고 대응 절차] ····· 3
[그림 3. 1월 유해트래픽 추이] ····· 5
[그림 4. 1월 침해사고 건수 추이] ····· 6
[그림 5. 1월 시스템별(OS) 사고 건수] ····· 7
[그림 6. 1월 부서별 사고 건수] ····· 7
[그림 7. 2월 유해트래픽 추이] ····· 9
[그림 8. 2월 침해 시도 건수 추이] ····· 10
[그림 9. 2월 시스템별(OS) 사고 건수] ····· 11
[그림 10. 2월 부서별 사고 건수] ····· 11
[그림 11. 3월 유해트래픽 추이] ····· 13
[그림 12. 3월 침해시도 건수 추이] ····· 14
[그림 13. 3월 시스템별(OS) 사고 건수] ····· 15
[그림 14. 3월 부서별 사고 건수] ····· 15
[그림 15. 월별 침해 시도 건수] ····· 17
[그림 16. 부서별 사고 건수 비율] ····· 18


## 표목차


[표 1. 1월 침해시도 현황] ····· 5
[표 2. 1월 침해 위협 유형별 분석] ····· 6
[표 3. 2월 침해시도 현황] ····· 9
[표 4. 2월 침해 위협 유형별 분석] ····· 10
[표 5. 3월 침해시도 현황] ····· 13
[표 6. 3월 침해 위협 유형별 분석] ····· 14
[표 19. 침해 위협 유형별 분석] ····· 17

# Ⅰ 개요

## 1. 목적 및 필요성

○ 지능화 다양화 되고 있는 사이버 위협 및 APT와 같은 표적 공격으로부터 주요 정보시스템 및 데이터를 안전하게 보호하기 위한 보안 활동 및 대응 방안이 필요함

○ 사이버보안센터에 침해사고 신고 및 처리결과를 분석하여 가시화하고 현장 실사를 통한 보안점검 및 취약점 분석 등을 통하여 향후 사고의 재발방지에 대한 개선 노력이 필요함

## 2. 분석 내용 및 범위

○ 침해사고 발생 현황 및 침해 위협 유형별 분석

- 월별 침해사고 발생 현황 및 처리결과에 대한 통계 분석
- 침해 위협 유형을 6가지로 분류하고 해당 사고에 대한 조사·분석 및 대응을 통한 위협 사항 도출

○ 부서별 월별 사고 건수 및 처리결과에 대한 분석

- 부서별 월별 사고 건수 및 처리결과에 대한 통계 분석
- 사고 미처리에 대한 원인 분석

## 3. 분석 활용 계획

○ 침해사고 대응 전략 수립

- 사고 재발 방지 대책 및 사고 대응 프로세스 고도화
- 사고 처리 지원에 대한 환경 및 수준 분석을 통한 시사점 도출



# Ⅱ KISTI 침해사고 대응

## 1. KISTI 침해사고 대응체계

○ KISTI의 침해사고 대응체계는 국가정보원 국가사이버안전센터(NCSC) 및 미래창조과학부 과학기술사이버안전센터(S&Tsec), 원내 전 부서와의 긴밀한 협조체계를 기반으로 대응


[그림 1] KISTI 침해사고 대응 체계

| 구분 | 역할 |
|---|---|
| 국가사이버안전센터<br>및<br>과학기술사이버안전센터 | - 중앙집중형 24시간 상시 상황 관제<br>- 침해사고 발생 시 정보화혁신실 통보<br>- 침해사고 처리결과 확인 |
| 정보화혁신실 | - 침해사고(유관기관 통보사항 및 내부탐지) 접수<br>- 침해사고자 사고내용 통보 및 사고처리 강제<br>- 침해사고 처리지원 및 사후 조치 확인<br>- 국가사이버안전센터 및 과학기술사이버안전센터 처리결과 통보 |
| 내부 전부서 | - 침해사고 처리<br>- 침해사고 처리결과 정보화혁신실 제출 |



## 2. 대응절차

○ KISTI의 침해사고 대응절차는 예방, 탐지, 분석, 대응, 복구 등의 체제를 유지하고 있으며, 세부적으로는 준비단계, 사고탐지단계, 초기대응단계, 사고처리단계, 복구단계, 보고서작성단계, 보고단계 등으로 이루어짐


[그림 2] KISTI 침해사고 대응절차

○ 준비단계 : 침해사고를 예방하기 위하여 시스템을 점검하고 보안장비를 설치하는 것은 물론 사고대응팀을 구성하여 구성원의 역할과 대응절차를 사전에 수립

○ 탐지단계 : 국가정보원 사이버안전센터, 미래창조과학부 과학기술사이버안전센터, 정보화혁신실 등으로부터 이상 징후를 탐지

○ 초기대응 : 침입인지 단순한 장애인지를 결정하는 단계로 사고의 완전한 분석이 아닌 사고의 확산을 방지하고 차단하는 조치를 취하며, 추후 정밀조사를 위한 증거자료 수집



○ 조치단계 : 사고자에게 사고 사실을 통보하고 6하 원칙에 기인하여 언제 누구에 의해 어떤 자료가 유출, 훼손되었는지 조사하고 복구할 수 있는 방법에 대한 자료 수집

○ 복구단계 : 악성 프로그램을 제거하고 삭제된 프로그램을 복구하는 등의 과정을 통해 침해 시스템과 네트워크를 정상적인 상태로 되돌리는 단계

○ 보고단계 : 사고 내용에 대한 내용을 보고할 수 있도록 문서화

○ 후속조치 : 사고대응 과정에서 발생된 문제들에 대한 검토 회의를 통해 미비점 개선

# Ⅲ 현황 분석

## 1. 1월 종합 분석

○ 1월 침해사고 분석

- 2015년 1월 유해 트래픽은 [그림 3]과 같이 5Gb로 전월 대비 3Gb증가 하였고 전년도 같은 기간에 비해 2배 증가하였다.

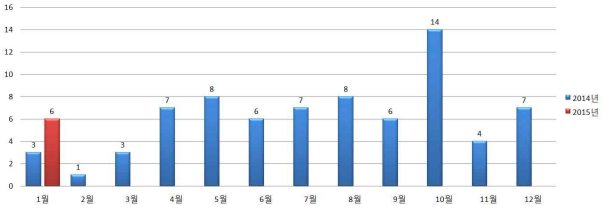

[그림 3] 1월 유해트래픽 추이

- 2015년 1월 침해시도 건수는 [표 1]과 같이 총 6건으로 전월 대비 1건 감소하였고, 전년도 같은 기간에 비해 3건 증가하였다.

| 구분 | 2014년 | | | | | | | | | | | | 2015년 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 1월 |
| 침해 시도 현황 | 3 | 1 | 3 | 7 | 8 | 6 | 7 | 8 | 6 | 14 | 4 | 7 | 6 |

[표 1] 1월 침해 시도 현황






[그림 4] 1월 침해시도 건수 추이

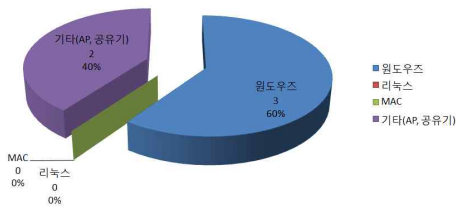
- 침해 위협 유형별로 살펴보면 [표 2]와 같이 6건 모두 웜·바이러스에 의한 사고로서 이중 5건이 (TCP 80)를 통하여 발생한 것으로 분석된다. 이는 소속직원들이 안전하지 않은 웹사이트에 방문하거나 악성광고 클릭 등으로 악성 프로그램이 사용자 PC 등에 심어진 것으로 추정된다.

| 구분 | 웜·바이러스 | 자료훼손 및 유출 | 홈페이지 위·변조 | 경유지 악용 | 서비스 거부 | 단순 침입시도 | 합계 |
|---|---|---|---|---|---|---|---|
| 건수 | 6 | 0 | 0 | 0 | 0 | 0 | 6 |

[표 2] 1월 침해 위협 유형별 분석

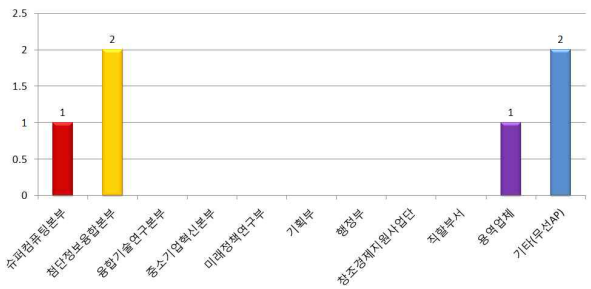
- 시스템별(OS)로는 [그림 5]와 같이 윈도우즈 시스템을 통한 사고가 3건으로 가장 많았으며, 그 뒤로 AP나 공유기를 통한 사고가 2건 발생하였다.






[그림 5] 1월 시스템별(OS) 사고 건수

- 부서별로는 [그림 6]와 같이 첨단정보융합본부, 무선AP를 통한 사고가 2건으로 가장 많이 발생하였으며, 그 뒤로 슈퍼컴퓨팅본부, 용역업체가 각각 1건씩 발생하였다.




[그림 6] 1월 부서별 사고 건수



○ 1월 보안 이슈 및 향후 계획

- 1월의 사고는 웜·바이러스에 의한 사고로서 사용자의 관리 소홀로 보여 진다. 추후 소속 직원들에 대한 보안 교육 등의 대책 마련이 필요하며, 무선AP에 대한 관리적 대책이 필요하다.

- 1월에는 12월 23일 한국수력원자력 정보유출사고 발생이후 국가공공기관 사이버위협 '주의' 경보를 발령한 이후 1월 6일 사이버위기 경보단계를 '관심'으로 하향 조정했고, 일주일 후인 1월 13일 18시부로 사이버위기 경보단계를 '관심'에서 '정상'으로 환원했다. 이에 각 단계에 따른 직원 및 시스템 운영 담당자에 대한 협조가 원활이 이루어졌다.

- 한국수력원자력 정보유출사고는 악성코드가 담긴 한글 파일이 첨부된 이메일을 배포하여 임직원 1만 799명의 개인정보와 내부 문서가 유출된 사고로 유출된  개인정보파일은 암호화조차 되어있지 않아 2차 피해로 확산될 가능성이 매우 큰 사고였다.

- 기관은 소속직원들에게 출처를 알 수 없는 이메일 클릭금지, 바이러스 백신 업데이트 및 OS의 보안 업데이트 필수 등의 보안교육을 실시하고 각 시스템 관리자는 DB암호화 등의 보안조치를 통해 한국수력원자력 정보유출 사고와 같은 보안사고가 일어나지 않도록 주의를 요구 한다.

## 2. 2월 종합 분석

○ 2월 침해사고 분석

- 2015년 2월의 유해 트래픽은 [그림 7]과 같이 9.2Gb로 전월대비 4.2Gb 증가하였으며, 전년도 최고치에 비해 3.7Gb 증가하였다.

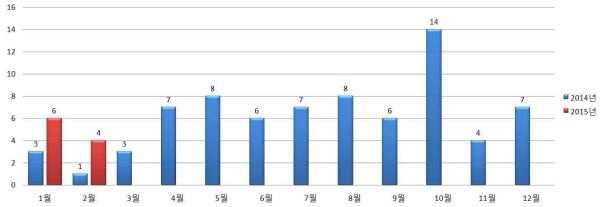

[그림 7] 2월 유해트래픽 추이

- 2015년 2월 침해시도 건수는 [표 3]과 같이 총 4건으로 전월 대비 2건 감소하였고, 지난해 12월 이후 최근 3개월간 감소추세가 이어지고 있다.

| 구분 | 2014년 | | | | | | | | | | | 2015년 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 1월 | 2월 |
| 침해 시도 현황 | 1 | 3 | 7 | 8 | 6 | 7 | 8 | 6 | 14 | 4 | 7 | 6 | 4 |

[표 3] 2월 침해 시도 현황






[그림 8] 2월 침해 시도 건수 추이

- 침해 위협 유형별로 살펴보면 [표 4]와 같이 4건 모두 웜·바이러스에 의한 사고로서 웹서비스 (TCP 80) 이용 중 발생한 것으로 추정된다.

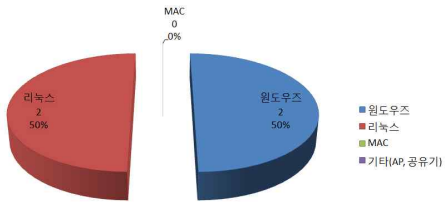
| 구분 | 웜·바이러스 | 자료훼손 및 유출 | 홈페이지 위·변조 | 경유지 악용 | 서비스 거부 | 단순 침입시도 | 합계 |
|---|---|---|---|---|---|---|---|
| 건수 | 4 | 0 | 0 | 0 | 0 | 0 | 4 |

[표 4] 2월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 9]과 같이 윈도우즈 시스템과 리눅스 시스템을 통한 사고가 각각 2건 발생하였다.

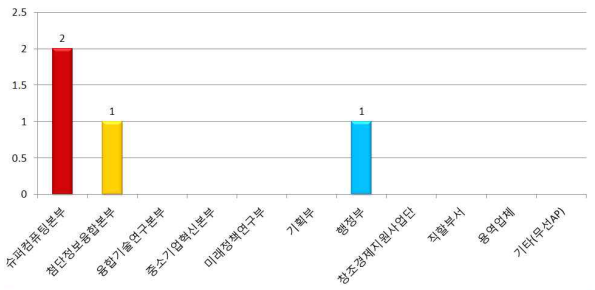
- 리눅스 시스템 사고 중 1건은 테스트용 시스템에서 발생한 것으로 해당 시스템을 포맷 조치하였다.






[그림 9] 2월 시스템별(OS) 사고 건수

- 부서별로는 [그림 10]과 같이 슈퍼컴퓨팅본부가 2건으로 가장 많이 발생하였으며, 그 뒤로 첨단정보융합본부, 행정부가 각각 1건씩 발생하였다.




[그림 10] 2월 부서별 사고 건수



○ 2월 보안 이슈 및 향후 계획

- 슈퍼컴퓨팅본부에서 발생한 사고는 테스트서버가 웜·바이러스 및 악성 프로그램에 감염(추정)되는 사고로써 테스트서버에 대한 보안 점검 미흡으로 파악된다.

- 테스트서버는 외부 인터넷을 차단하고 VM사용 시 최신이미지를 이용하여 취약점을 최소화 하여야 한다. 또한, 해당 테스트 서버 담당자는 비인가자의 접속차단과 비정상행위 프로세스 모니터링 등 시스템에 대한 보안 강화가 요구 된다.

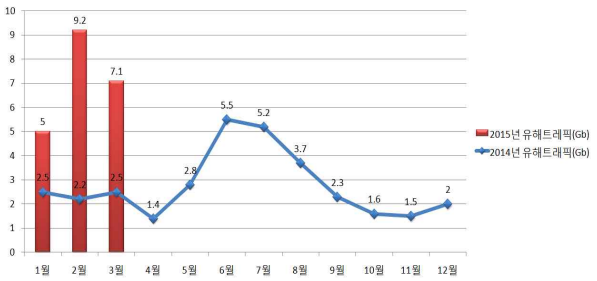
- 2월에는 Open SSL의 새로운 취약점이 발견되었다. 해당 취약점은 SSL을 통해 강제로 암호화 방식을 취약한 RSA로 다운 그레이드 시킬 수 있는 취약점(CVE-2015-0204)이다. RSA의 암호화 비트를 512비트로 다운그레이드 하는 해당 취약점은 탈취된 데이터를 손쉽게 복호화 가능하게 만들어 주의를 요구한다.

- 이와 관련하여 서버 관리자의 경우 Open SSL의 업그레이드 작업을 실시하고 작업이 완료되기 전까지 사용자에게 기본브라우저 외에 크롬, 파이어폭스 등 타 브라우저 사용을 안내 해야한다.

## 3. 3월 종합 분석

○ 3월 침해사고 분석

- 2015년 3월 유해 트래픽은 [그림 11]와 같이 7.1Gb로 전월 대비 2.1Gb 감소하였으나, 여전히 전년도 평균(2.7Gb/월)보다 높은 수치를 보였다.



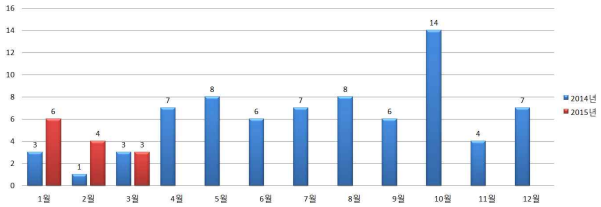

[그림 11] 3월 유해트래픽 추이

- 2015년 3월 침해시도 건수는 [표 5]와 같이 총 3건으로 전월 대비 1건 감소하였으며, 4개월간 감소 추세가 지속되고 있다.

| 구분 | 2014년 | | | | | | | | | | 2015년 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 1월 | 2월 | 3월 |
| 침해시도 현황 | 3 | 7 | 8 | 6 | 7 | 8 | 6 | 14 | 4 | 7 | 6 | 4 | 3 |

[표 5] 3월 침해 시도 현황






[그림 12] 3월 침해시도 건수 추이

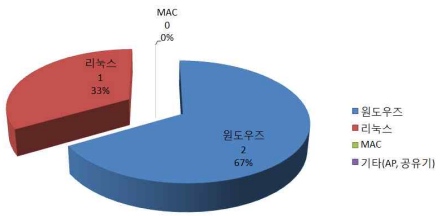
- 침해 위협 유형별로 살펴보면 [표 6]과 같이 3건 모두 웜·바이러스에 의한 사고로서 소속직원들이 안전하지 않은 웹사이트에 방문하거나 악성광고 클릭 등으로 악성 프로그램이 사용자 PC 등에 심어진 것으로 추정된다..

| 구분 | 웜·바이러스 | 자료훼손 및 유출 | 홈페이지 위·변조 | 경유지 악용 | 서비스 거부 | 단순 침입시도 | 합계 |
|---|---|---|---|---|---|---|---|
| 건수 | 3 | 0 | 0 | 0 | 0 | 0 | 3 |

[표 6] 3월 침해 위협 유형별 분석

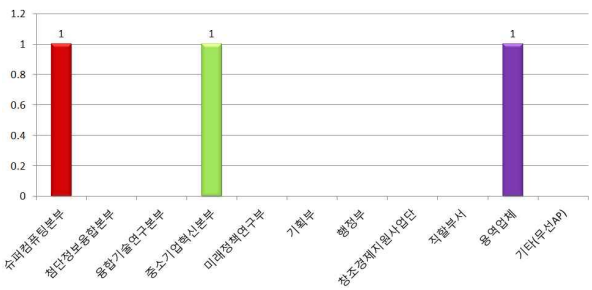
- 시스템별(OS)로는 [그림 13]과 같이 윈도우즈 시스템을 통한 사고가 2건으로 가장 많은 비중을 차지했으며, 그 뒤로 리눅스 시스템을 통한 사고가 1건 발생하였다.






[그림 13] 3월 시스템별(OS) 사고 건수

- 부서별로는 [그림 14]와 같이 슈퍼컴퓨팅본부, 중소기업혁신본부, 용역업체가 각각 1건씩 발생하였다.




[그림 14] 3월 부서별 사고 건수



○ 3월 보안 이슈 및 향후 계획

- 3월의 보안 이슈로는 용역 업체에 대한 관리 소홀로 인한 것이며, 추후 소속 직원들에 대한 주기적인 보안 교육 및 관리적 차원의 대책 마련이 필요하다.

- 또한, 기관 인프라(기계실, 전기실) 관리 및 모니터링으로 활용되는 PC는 외부 인터넷 사용을 금하고 내부 업무 목적용으로 활용되도록 주의가 요구된다.

- 이달에는 2013년 3.20 사이버테러를 일으킨 것으로 추정되는 북한의 해커 조직이 국내의 북한관련 사이트들을 해킹해서 방문자들에게 악성코드를 유포하고 있는 것이 포착됐다. 유포된 악성코드는 기존 3.20사이버테러 당시 유포된 악성코드와 전체적인 동작 구조에서는 크게 유사하나 세부 코드가 많이 변형되어 제작된 것으로 분석됐다. 해당 악성코드에 감염되면 PC에서 한글, PDF, 워드, 엑셀 등 문서 파일명을 수집해 C&C 서버로 전송하며, 추가로 악성코드를 다운받아 실행하게 된다.

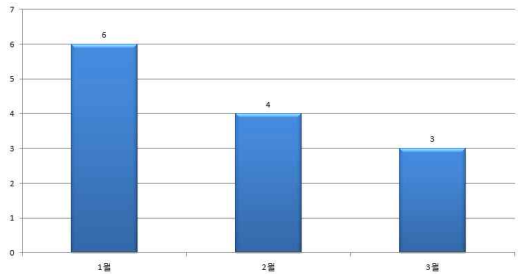
- 이들 조직이 악성코드를 유포하기 위해 사용하는 취약점은 현재 확인된 것이 총 2종으로 플래시 취약점(CVE-2014-0569)와 OLE 취약점(CVE-2014-6332)이다. 해당 취약점에 대한 패치는 나와 있으나, 패치를 하지 않은 사용자가 이들이 노리는 웹사이트에 접속하면 즉시 악성코드에 감염된다.

- 그러나 OLE 취약점(CVE-2014-6332)은 윈도우XP에서는 더 이상 보안 패치가 제공되지 않기 때문에 윈도우XP에서 인터넷 익스플로러를 사용할 경우 누구든지 해당 웹사이트에 접속하면 악성코드에 감염될 수 있다.

- 따라서, 더 이상 보안패치가 지원되지 않는 윈도우XP는 최대한 사용을 자제하고, 플래시와 윈도우 운영체제에 대한 보안 업데이트는 반드시 최신 상태를 유지해야 할 것으로 보인다.

## Ⅳ 종합분석 및 개선방안

○ 2015년 1월부터 3월까지의 침해시도 건수는 [그림 15]와 같이 총 13건으로 1월이 6건으로 가장 많이 발생하였으며, 그 뒤로 2월이 4건 3월이 3건으로 점차 감소하는 수치를 보였다.




[그림 15] 1분기 월별 침해시도 건수

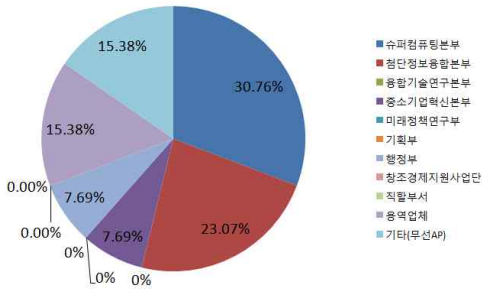
○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 사고가 13건으로 모든 사고가 웜·바이러스에 의해 발생되었다.

| | 1월 | 2월 | 3월 |
|---|---|---|---|
| 웜 · 바이러스 | 6 | 4 | 3 |
| 자료훼손 및 유출 | 0 | 0 | 0 |
| 홈페이지 위 · 변조 | 0 | 0 | 0 |
| 경유지 악용 | 0 | 0 | 0 |
| 서비스 거부 | 0 | 0 | 0 |
| 단순침입시도 | 0 | 0 | 0 |
| 합계 | 6 | 4 | 3 |

[표 7] 침해 위협 유형별 분석



○ 부서별로는 [그림 16]과 같이 슈퍼컴퓨팅본부가 4건(30.76%)으로 가장 많은 비중을 차지하였으며, 그 뒤로 첨단정보융합본부가 3건(23.07%), 기타(무선AP)와 용역업체가 각각 2건(15.38%), 중소기업혁신본부와 행정부에서 각각 1건(7.69%)의 사고가 발생하였다.




[그림 16] 1분기 부서별 사고 건수 비율

**• 웜·바이러스에 의한 사고**

- 분석 결과 중 주목할 만한 사항은 1분기에 발생한 사고가 모두 웜·바이러스에 의한 사고인 부분이다.

- 웜·바이러스에 의한 사고는 꾸준히 발생하고 있으며, 소속 직원들의 부주의 로 인해 발생하는 경우가 많다. 따라서, 위 문제를 해결하기 위한 대책으로 업무용 PC의 윈도우등 OS의 보안업데이트와 백신 소프트웨어 업데이트등 신규 취약점에 대한 대비가 필요하며 웹사이트 방문시 의심스러운 프로그램 설치 금지 및 출처가 의심스러운 메일 열람 금지등 사용자 교육이 요구 된다.



**• 보안사고 대응**

- 현재 국정원 및 과학기술사이버안전센터를 통한 침해사고 접수 시 개인이 1차적으로 SysCheck 점검 및 백신 검사를 실시하고 있다. (단, 지원 요청 시 유지보수 업체에 의해 점검)

- 하지만 사고 발생 직후 즉각적인 대응이 어려워 정확한 사고 조사가 이루어지지 못하는 경우가 많으며, 서울 분원 및 각 지원에서 발생하는 사고에 대해서는 정보보안 담당 직원을 통한 점검 없이 백신 점검 및 포맷 등의 조치만 지원하고 있다. 향후 사고 대응 및 악성코드 분석을 위한 보안 솔루션(포렌식 도구, 이벤트 수집 및 분석 도구 등) 도입 및 사고 조사에 필요한 전문 인력 확보가 요구된다.

**• IP 주소 관리 강화**

- 한편 사고 IP 주소에 대한 정확한 시스템을 파악하지 못하여 사고 조사가 이루어지지 못한 사례도 발생하였다.

- 현재는 부서 단위로 C클래스를 할당하여 부서에서 자율적으로 IP를 관리하도록 하고 있으나, 신규 직원 및 퇴직 직원 발생, 혹은 소속 직원의 부서 변경 시 정확한 IP 관리가 이루어지지 않기에 향후 네트워크 운영 부서를 통해 중앙에서 일괄적으로 기관 IP 자원을 관리하는 정책으로 변화할 필요가 있다. 따라서 정보화혁신실에서는 올해 3분기에 IP현황조사 및 사용자 PC이름 변경 추진을 통해 부서별 IP할당에 따른 관리 미흡으로 증가된 미사용 IP 관리와 보안사고시 사고 PC의 IP확인 지연으로 인한 보안 위험을 최소화할 계획을 세우고 있다.



- 마지막으로 사이버보안센터를 활용하여 침해사고의 프로세스를 체계화 하고 자료 증적을 통한 사후 점검 등 소속직원들의 자발적인 재발방지를 위한 노력이 요구된다.

**• 서버 보안**

- 관제현황 보고서에 따르면 1분기 공격 대상 포트와 스캐닝 대상포트 중 가장 많은 비율을 차지한 포트가 각각 TCP/22 (ssh),TCP/23 (telnet)으로 원격접속에 대한 침해시도가 많이 탐지 되었다. 특히 2월 공격대상 포트중 TCP/22 (ssh)는 79.8%로 ssh를 기본 22번 포트로 사용할 경우 공격 대상이 될 가능성이 매우 높았다. 따라서 시스템 운영자는 비인가된 접속에 대한 로그관리와 ssh와 같은 서비스의 포트설정 변경, 원격에서 루트계정 로그인 금지, 패스워드 정책강화와 주기적인 패스워드 변경 등 서버보안을 위한 보안정책을 강화하여야 한다..

# V 결론

○ 2014년 1분기 총 7건의 침해시도에 비해 2015년 3월까지의 총 침해시도건수는 13건으로 50% 이상의 증가율을 보였다. 하지만 1월 이후 침해시도 건수는 꾸준히 감소하고 있어 3월에는 3건으로 전년도 평균(6건/월)보다 낮은 수치를 보였다.

○ 1분기에는 작년 12월 한국수력원자력 정보유출 사고 이후 유해 트래픽이 평균 7.1Gb로 전년도 평균(2.1Gb/월)에 비해 3배 이상 급증하였다. 이와 관련해서 새로운 바이러스와 악성코드들에 의해 발생할 수 있는 침해와 공격 시도들을 대비하여 더욱 세심한 주의가 요구된다.

○ 1분기에는 모든 사고가 웜·바이러스에 의해 발생하였다. 최근 동향을 살펴보면 MS IE, MS XML, Adobe Flash Player, Java 애플릿 취약점 등을 복합적으로 악용하여 악성코드를 유포시키는 사례가 지속적으로 나타나고 있으며, 복잡한 자동화 공격도구를 결합하여 지속적으로 악성코드가 유포되는 등 악성코드의 유포방식이 다양해지고 있다.

○ 따라서, 개발자 및 서버 관리자는 이러한 새로운 방식의 악성코드 유포방식에 대비하여 근본적으로 홈페이지 개발 시점부터 보안의식 및 시큐어코딩으로 홈페이지를 구축하고, 주기적인 취약점 점검 및 패치를 적용하여 웹서버가 해킹되지 않도록 사전에 방지해야 한다. 또한, 이용자는 MS 윈도우의 보안 업데이트를 항상 최신 상태로 유지할 것을 권장하고 백신프로그램을 이용하여 주기적으로 점검하여야 하며, Adobe Flash Player 및 Java 관련 취약점에 의한 악성코드에 감염되지 않도록 주의하여야 한다.



○ 향후 침해사고 발생 시 해당 직원에 대한 책임 추적성을 강화하고 사이버 보안진단의 날 행사를 활성화하는 등 전사적으로 보안문화가 형성될 수 있도록 해야 할 것이다.

○ 향후 급증하는 사이버 침해와 정보 유출 사고에 대한 대응능력 배양 및 중요 정보자원의 위협 요인에 대한 사전 예방활동 강화를 위하여 지속적인 정보보안 모니터링 체제 강화를 통한 통합 위협 분석 및 위협 요인에 대한 개선활동 수행이 요구된다. 또한 업무환경 변화 및 유관기관의 정책 변화에 대응하기 위한 내부규정 정비, 자체 보안감사 수행 및 예방활동 강화 등 정보보호 수준 신뢰도 제고를 위한 정보보안 전략 수립 등 종합적인 전주기적 보안관리 활동을 수행해야 할 것이다.



**[별첨 1] 월별 침해위협 발생 현황**

○ 1월 침해 위협 발생 현황

| 사고 번호 | 발생시간 | 사고부서 | 사고내용 | 처리시간 |
|---|---|---|---|---|
| 1 | 2015-01-28 10:38 | 국내정보실 공현철 | · 정보유출형 악성코드 감염(추정)에 의한 경유지로 접속 시도 탐지 | 2015-01-28 |
| 2 | 2015-01-26 10:25 | 미래기술분석실 허요섭 | · 웜·바이러스 감염(추정)으로 인하여 경유지로 시스템 정보(MAC 주소, OS 버전 등) 전송 시도 탐지 | 2015-01-26 |
| 3 | 2015-01-23 20:04 | 대전 AP | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보(MAC 주소, OS 버전 등) 전송 시도 탐지 | 2015-01-23 |
| 4 | 2015-01-14 19:08 | 대전 AP | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보(MAC 주소, OS 버전 등) 전송 시도 탐지 | 2015-01-14 |
| 5 | 2015-01-03 22:15 | 용역업체 | · 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지 | 2015-01-03 |
| 6 | 2015-01-02 20:26 | 대용량데이터허브실 김진 | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 목적지 IP를 대상으로 대량의 UDP 패킷 전송 행위 탐지 | 2015-01-02 |



○ 2월 침해 위협 발생 현황

| 사고 번호 | 발생시간 | 사고부서 | 사고내용 | 처리시간 |
|---|---|---|---|---|
| 7 | 2015-02-26 14:46 | 정보융합실 조혜민 | · 정보유출형 악성코드 감염(추정)에 의한 경유지로 접속 시도 탐지 | 2015-02-26 |
| 8 | 2015-02-26 13:12 | 재무관리실 심원보 | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 Darknet 접속 탐지 | 2015-02-26 |
| 9 | 2015-02-21 12:35 | 슈퍼컴퓨팅응용실 신승찬 | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 목적지 IP를 대상으로 대량의 TCP Syn 패킷 전송 행위 탐지 | 2015-02-21 |
| 10 | 2015-02-03 07:43 | 첨단연구망서비스실 박정욱 | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 목적지 IP를 대상으로 대량의 UDP 패킷 전송 행위 탐지 | 2015-02-03 |

○ 3월 침해 위협 발생 현황

| 사고 번호 | 발생시간 | 사고부서 | 사고내용 | 처리시간 |
|---|---|---|---|---|
| 11 | 2015-03-26 12:49 | 계산과학공학연구실 조기현 | · 웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 목적지 IP를 대상으로 스캐닝 행위 탐지 | 2015-03-26 |
| 12 | 2015-03-19 09:36 | 용역업체 | · 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지 | 2015-03-19 |
| 13 | 2015-03-08 18:34 | 기업혁신전략실 전성진 | · 악성 RAT(원격제어 프로그램) 감염(추정)으로 인한 지령서버 접속 시도 탐지 | 2015-03-08 |

**[별첨 2] 부서별 사고 건수**

| 부서명 | 1월 | 2월 | 3월 |
|---|---|---|---|
| 슈퍼컴퓨팅본부 | 1 | 2 | 1 |
| 첨단정보융합본부 | 2 | 1 | 0 |
| 융합기술연구본부 | 0 | 0 | 0 |
| 중소기업혁신본부 | 0 | 0 | 1 |
| 미래정책연구부 | 0 | 0 | 0 |
| 기획부 | 0 | 0 | 0 |
| 행정부 | 0 | 1 | 0 |
| 창조경제지원사업단 | 0 | 0 | 0 |
| 직할부서 | 0 | 0 | 0 |
| 용역업체 | 1 | 0 | 1 |
| 기타(무선AP) | 2 | 0 | 0 |
| 합계 | 6 | 4 | 3 |



**[별첨 3] 침해시도 유형별 내용**

| 침해시도 | 내용 |
|---|---|
| 웜・바이러스 | · 웜·바이러스 감염 시도 및 전파 시도 |
| 자료훼손 및 유출 | · FTP, 서버 및 PC 등의 권한이나 공유 설정의 취약으로 자료가 변조, 삭제되거나 유출, 열람 시도 |
| 홈페이지 위・변조 | · 취약점 등을 이용하여 홈페이지의 메인 페이지 변조 시도나 사용하지 않는 페이지 삽입 시도 및 피싱을 목적으로 한 홈페이지의 변조 |
| 경유지 악용 | · 해킹 피해 이후 다른 사이트를 공격하는 경유지로 활용하려는 시도 |
| 서비스 거부 | · 정보시스템의 데이터나 자원을 적절한 대기 시간 내에 사용하는 것을 방해하거나 과도한 부하를 일으켜 사용을 방해하려는 시도 |
| 단순침입시도 | · 스캐닝 기법 등으로 시스템이나 네트워크의 취약점 점검 및 계정 추측 등의 침입 시도 |



**[별첨 4] 사이버위기 상황 발생 시 대상별 협조 사항**

| 구분 | 협조사항 |
|---|---|
| 직원 | 1. OS, 백신, 업무용 프로그램 최신 업데이트 수행<br>2. 백신 소프트웨어 실시간 감시기능 사용<br>3. 출처, 첨부파일이 의심스러운 이메일은 열람하지 말고 삭제<br>4. 개인컴퓨터의 부팅, 로그인, 화면보호기의 패스워드를 설정하고 반드시 사용<br>5. 공유폴더 사용의 최소화하고 사용 시 반드시 최소 권한만을 부여하여 사용<br>6. 웹사이트 방문 시 설치하는 프로그램은 인증서 및 디지털서명을 참고하여 신뢰성을 확인 후 설치<br>7. 메신저를 이용한 파일 다운로드 시 최신 백신소프트웨어로 점검 후 사용<br>8. 중요한 자료는 패스워드를 설정하여 저장 |
| 시스템 운영 담당자 | 1. 웜 바이러스, 해킹 등에 의한 피해발생 가능성이 증가함에 따라 각종 시스템의 모니터링 강화<br>2. 해외 사이버 공격 피해가 확산되어 국내 유입이 우려되므로 이에 대한 대비 필요<br>3. 네트워크 이상트래픽 과다 탐지 또는 부분 장애 등 사이버위협 징후 탐지활동 강화 필요 |