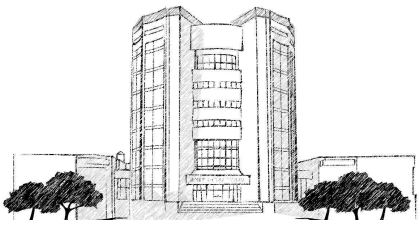
2015년 KISTI 침해사고 대응 분석 보고서
(2/4분기)



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 ····· 27
[별첨 3.] 침해시도 유형별 내용 ····· 28
[별첨 4.] 사이버위기 상황 발생 시 대상별 협조 사항 ····· 29

그림 목차

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

표목차

[표 1. 4월 침해시도 현황] ····· 5
[표 2. 4월 침해 위협 유형별 분석] ····· 6
[표 3. 5월 침해시도 현황] ····· 9
[표 4. 5월 침해 위협 유형별 분석] ····· 10
[표 5. 6월 침해시도 현황] ····· 13
[표 6. 6월 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 이 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 및 과학기술사이버안전센터	- 중앙집중형 24시간 상시 상황 관제 - 침해사고 발생 시 정보화혁신실 통보 - 침해사고 처리결과 확인
정보화혁신실	- 침해사고(유관기관 통보사항 및 내부탐지) 접수 - 침해사고자 사고내용 통보 및 사고처리 강제 - 침해사고 처리지원 및 사후 조치 확인 - 국가사이버안전센터 및 과학기술사이버안전센터 처리결과 통보
내부 전부서	- 침해사고 처리 - 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

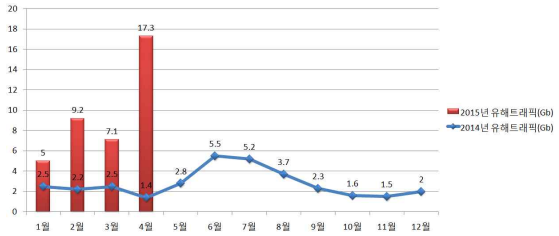
○ 후속조치 : 사고대응 과정에서 발생된 문제들에 대한 검토 회의를 통해 미비점 개선

Ⅲ 현황 분석

1. 4월 종합 분석

○ 4월 침해사고 분석

- 2015년 4월 유해 트래픽은 [그림 3]과 같이 17.3Gb로 전월 대비 10.2Gb증가하여 약 1.5배 증가하였다.

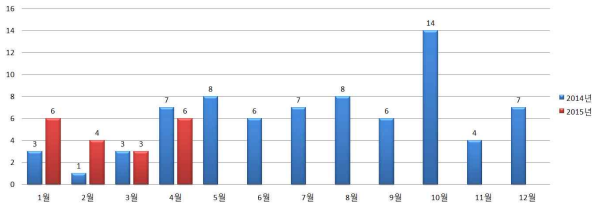


[그림 3] 4월 유해트래픽 추이

- 2015년 4월 침해시도 건수는 [표 1]과 같이 총 6건으로 전월 대비 3건 증가 하였다.

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

[표 1] 4월 침해 시도 현황



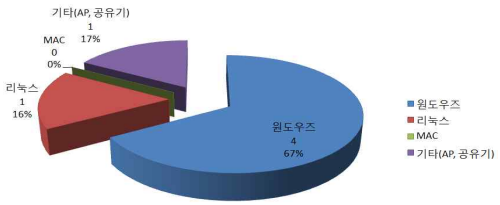
[그림 4] 4월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 2]와 같이 웜·바이러스에 의한 침해시도가 5건으로 가장 많았으며, 그 뒤로 자료훼손 및 유출이 1건 발생하였으며, 자료훼손 및 유출에 대한 침해 시도는 올해 들어 처음이다.

구분	웜.바이러스	자료훼손 및 유출	홈페이지 위.변조	경유지 악용	서비스 거부	단순침입시도	합계
건수	5	1	0	0	0	0	6

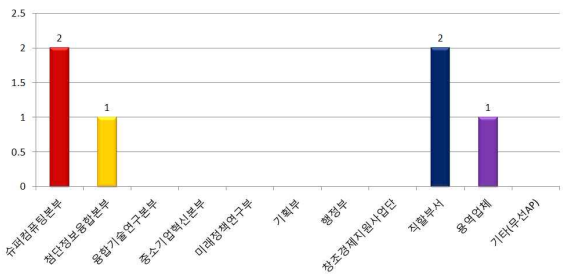
[표 2] 4월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 5]과 같이 윈도우즈를 통한 사고가 4건으로 가장 많은 비중을 차지했으며, 그 뒤로 리눅스 시스템, NAT장비를 이용한 사고가 각각 1건으로 나타났다.



[그림 5] 4월 시스템별(OS) 사고 건수

- 부서별로는 [그림 6]와 같이 슈퍼컴퓨팅본부, 직할부서가 각각 2건씩 하였으며, 그 뒤로 첨단정보융합본부와 용역업체에서 각각 1건씩 발생하였다.



[그림 6] 4월 부서별 사고 건수

○ 4월 보안 이슈 및 향후 계획

- 4월에 발생한 침해시도 중 자료훼손 및 유출에 대한 침해시도가 상주용역사에서 발생하였다.

- 상주용역사 직원이 기관 네트워크에 접속할 경우에는 소속직원과 동일한 보안 정책이 적용된 보안 에이전트가 설치되도록 보안 강화가 요구되며, 해당 관리 부서의 정기적인 보안 점검이 필요하다. 또한 용역사 직원이 외부에서 반입하여 사용중인 노트북에 대한 통제 및 기술적 조치사항을 강화해야 할 것이다.

- 이달의 보안 이슈로는 이메일 계정 탈취 통한 SSL 인증서 발급이 있다. SSL 인증을 위한 메일을 공격자가 열람하거나 인가되지 않은 사용자가 메일을 받을 경우 SSL 인증서를 가로채거나 위·변조할 수 있어 사용자들의 주의가 요구되고 있다. SSL 인증서 발급기관은 인증서 발급을 위해 '이메일 인증'을 지원한다. SSL 인증서 발급기관은 이메일 인증을 사용할 수 있는 관리자용 이메일 계정을 특정 계정으로 제한해 인증을 제공하고 있다.

- 발급기관에서는 발급 대상 기관을 확인하기 위해 이메일 계정과 도메인 주소를 확인하는데, 인증서 발급기관마다 허용하고 있는 이메일 계정은 admin, administrator, webmaster, hostmaster, postmaster,root, ssladmin, info, is, it, mis, ssladministrator, sslwebmaster 등의 계정이다.

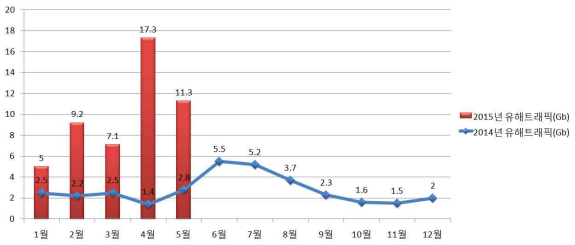
- 하지만 인증서 발급기관에서 허용한 관리자용 이메일 주소를 공격자에게 탈취당하거나 또는 악의를 가진 사용자에게 실수로 발급할 경우 SSL 인증서 발급을 통해 사용자 모르게 HTTPS 통신 데이터의 내용을 변조하거나 도청할 수 있다.

- 이를 해결하기 위해 이메일 계정을 생성하는 관리자는 SSL 인증서 발급기관이 허용한 특정 이메일 계정의 생성을 제한해야 한다. 이미 일반 사용자에게 해당 계정이 생성되어 있을 경우 계정에 대한 비활성화를 권고하고 있다.

2. 5월 종합 분석

○ 5월 침해사고 분석

- 2015년 5월의 유해 트래픽은 [그림 7]과 같이 11.3Gb로 전월대비 6Gb 감소하였으나, 전년도 평균(2.7Gb) 비해 8.6Gb 높은 수치를 보였다.

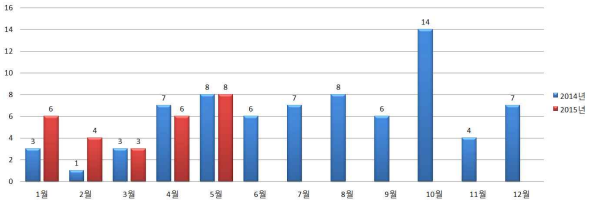


[그림 7] 5월 유해트래픽 추이

- 2015년 5월 침해시도 건수는 [표 3]와 같이 총 8건으로 전월 대비 2건 소폭 상승 하였다.

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

[표 3] 5월 침해 시도 현황



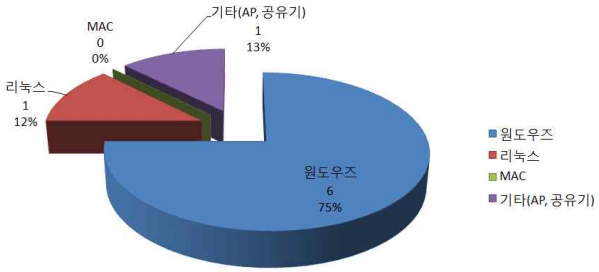
[그림 8] 5월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 4]와 같이 웜·바이러스에 의한 침해시도가 7건으로 가장 많았으며, 그 뒤로 홈페이지 위·변조가 1건으로 나타났다. 홈페이지 위·변조에 대한 침해 시도는 올해 들어 처음 발생하였으며, 시스템 관리자의 주의가 요구된다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	7	0	1	0	0	0	8

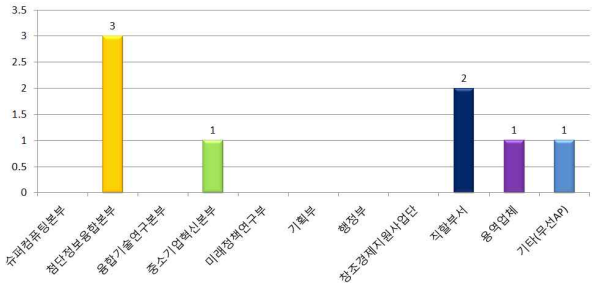
[표 4] 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 9]와 같이 윈도우즈를 통한 사고가 6건으로 가장 많은 비중을 차지했으며, 그 뒤로 리눅스 시스템, 무선AP를 이용한 사고가 각각 1건으로 나타났다.



[그림 9] 5월 시스템별(OS) 사고 건수

- 부서별로는 [그림 10]와 같이 침단정보융합본부가 3건으로 가장 많이 발생하였으며, 그 뒤로 직할부서가 2건, 중소기업혁신본부, 용역업체, 무선AP에서 각각 1건씩 발생하였다.



[그림 10] 5월 부서별 사고 건수

○ 5월 보안 이슈 및 향후 계획

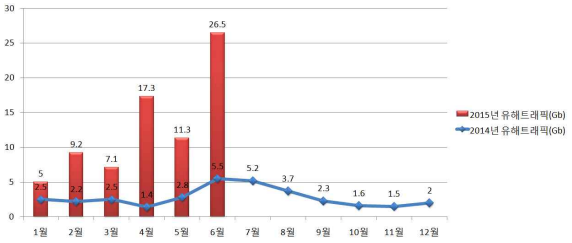
- 이달에는 리다이렉션 취약점을 이용한 사고가 발생하였다. 리다이렉션 취약점은 사용자가 제어할 수 있는 입력을 받아 들여 리다이렉션 작업에 사용 될 때 사용자가 브라우저에 다른 URL을 방문하라고 명령를 내리면서 발생한다. 리다이렉션버그는 주로 조작된 웹사이드를 방문하고 민감한 세부정보에 접근하게 유도하는 피싱공격에 사용된다. 이 취약점으로 공격자는 목표하는 인증된 공격자의 웹사이트로 링크가 걸린 URL을 구성해서 방문하는 모든 사용자를 공격자의 웹사이트로 리다이렉트 시키는 것이 가능하기 때문에 공격자는 잠시 신뢰성 있는 사이트처럼 보이는 조작된 웹사이트를 구성해 잠재적인 희생자를 공격할 수 있다.

- 리다이렉션 취약점은 여러 가지 2차 피해를 야기할 수 있기 때문에 HTML 태그 필터링, 사용자가 기존 사이트를 벗어나려고 하는 경우 경고 메시지 출력, 요청하는 페이지의 인자와 쿠키에 허용되지 않은 타 사이트 URL이 있는지 점검, 시큐어 코딩 등 관리자의 주의가 요구된다.

3. 6월 종합 분석

○ 6월 침해사고 분석

- 2015년 6월 유해 트래픽은 [그림 11]와 같이 26.5Gb로 전월 대비 15.2Gb 증가하여, 전년도 평균(2.7Gb/월)보다 약 10배 높은 수치를 보였다.

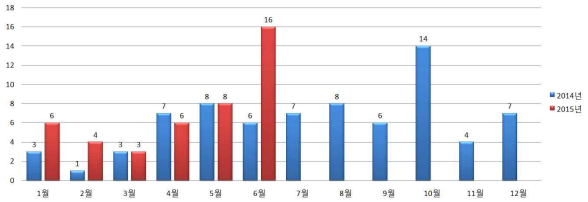


[그림 11] 6월 유해트래픽 추이

- 2015년 6월 침해시도 건수는 [표 5]와 같이 총 16건으로 전월 대비 8건 상승하였다.

구분	2012년							2013년					
	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
침해 시도 현황	8	6	7	8	6	14	4	7	6	3	6	8	16

[표 5] 6월 침해 시도 현황



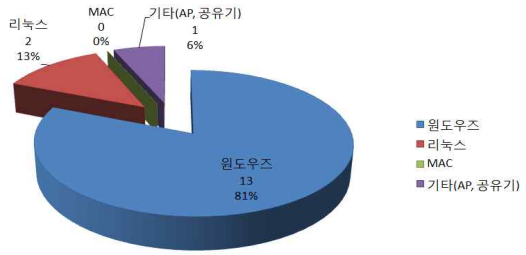
[그림 12] 6월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 6]와 같이 웜·바이러스에 의한 침해시도가 13건으로 가장 많았으며, 그 뒤로 홈페이지 위·변조가 2건 자료훼손 및 유출이 1건 발생하였다. 홈페이지 위·변조, 자료훼손 및 유출에 대한 사고는 시스템관리자의 주의가 요구된다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	13	1	2	0	0	0	16

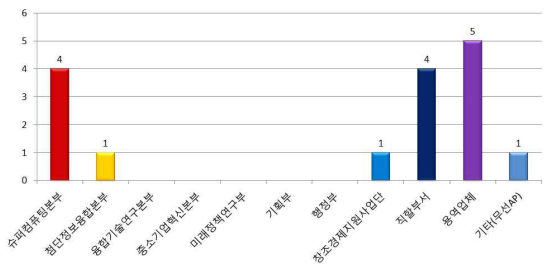
[표 6] 6월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 13]과 같이 윈도우즈 시스템을 통한 사고가 13건으로 가장 많은 비중을 차지했으며, 리눅스를 통한 사고가 2건으로 무선AP를 통한 사고가 1건으로 뒤를 이었다.



[그림 13] 6월 시스템별(OS) 사고 건수

- 부서별로는 [그림 14]과 같이 용역업체가 5건으로 가장 많았고, 그 뒤로 슈퍼컴퓨팅본부, 직할부서가 각각 4건 발생하였으며, 침단정보융합본부와 창조경제지원사업단이 각각 1건씩 발생하였다.



[그림 14] 6월 부서별 사고 건수

○ 6월 보안 이슈 및 향후 계획

- 이달에는 홈페이지 위·변조 시도가 발생하였다.

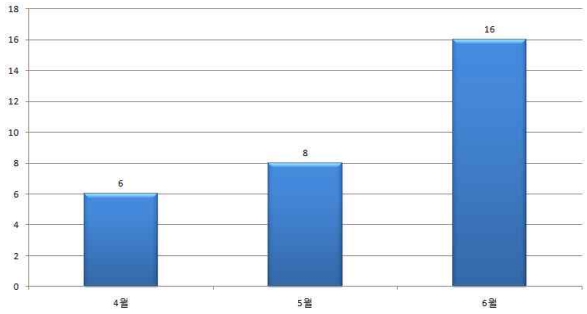
- 해당시스템 분석결과 게시판 업로드 취약점을 악용하여 웹셸을 업로드 한 것으로 파악된다.

- 웹서버를 운영하는 시스템 담당자는 웹 방화벽에서 443으로 전송하는 데이터에 대한 차단 정책(암호화 전송)을 세워야 하며, 첨부파일 업로드 시 스크립트파일 업로드 및 실행 금지 정책을 설정해야한다. 보안정책 강화와 시스템 및 웹 어플리케이션에 대한 보안점검 및 보안 패치 등이 요구된다.

- 웹셸 공격으로 인한 홈페이지 해킹과 이를 통한 주요 정보 및 개인정보가 유출되는 피해사례가 발생하지 않도록 웹방화벽 구축 및 웹셸 탐지 솔루션을 통한 방어가 필요하다.

Ⅳ 종합분석 및 개선방안

○ 2015년 4월부터 6월까지의 침해시도 건수는 [그림 15]와 같이 총 30건으로 6월이 16건으로 가장 많이 발생하였으며, 그 뒤로 5월이 8건 4월이 6건으로 6월에 유해 트래픽 대폭 증가하며 침해사고 건수도 증가한 것으로 보인다.



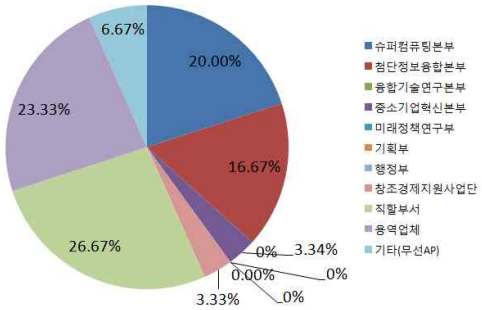
[그림 15] 2분기 월별 침해시도 건수

○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 사고가 25건으로 가장 많은 비율을 차지하였으며, 그 뒤로 홈페이지 위 ·변조사고가 3건 발생되었다.

	1월	2월	3월
웜 · 바이러스	5	7	13
자료훼손 및 유출	1	0	1
홈페이지 위 · 변조	0	1	2
경유지 악용	0	0	0
서비스 거부	0	0	0
단순침입시도	0	0	0
합계	6	8	16

[표 7] 침해 위협 유형별 분석

○ 부서별로는 [그림 16]과 같이 직할부서가 8건(26.67%)으로 가장 많은 비중을 차지하였으며, 그 뒤로 용역업체가 7건(23.33%), 슈퍼컴퓨팅본부가 6건(20%), 첨단정보융합본부에서 5건(16.67%)의 사고가 발생하였다.



[그림 16] 2분기 부서별 사고 건수 비율

- **웜·바이러스에 의한 사고**

- 2분기에 발생한 사고 중 모두 웜·바이러스에 의한 사고가 가장 많은 부분을 차지하였다.

- 웜·바이러스에 의한 사고는 꾸준히 발생하고 있으며, 소속 직원들의 부주의로 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 보안솔루션(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 운영부서를 통해 중앙에서 일괄적으로 기관 IP 자원을 관리하는 정책으로 변화할 필요가 있다. 따라서 정보화혁신실에서는 올해 3분기에 IP현황조사 및 사용자 PC 이름 변경 추진을 통해 부서별 IP할당에 따른 관리 미흡으로 증가된 미사용 IP 관리와 보안사고시 사고 PC의 IP확인 지연으로 인한 보안 위험을 최소화할 계획을 세우고 있다.

- 서버 보안

- 관제현황 보고서에 따르면 2분기 공격 대상 포트와 스캐닝 대상포트 중 가장 많은 비율을 차지한 포트가 각각 TCP/22 (ssh),TCP/1433 (MYSQL)으로 원격접속에 대한 침해시도 및 MS-SQL에 대한 공격시도가 많이 탐지되었다. 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 하며 MS-SQL에 대한 최신 서비스팩 설치, 윈도우 인증사용등 DB보안에도 주의를 기울여야 한다.

- 또한 2분기에는 웹서버 및 개발용 서버를 대상으로 한 자료훼손 및 유출, 홈페이지 위·변조 시도도 총 4건 발생하였다. 시스템 운영자는 침해사고를 발생시킬 수 있는 취약한 파일이나 공개용 웹 게시판 등의 보호 대책을 마련하여야 할 것이다. 또한 자체적으로 시스템을 운영할 경우에는 별도의 네트워크 구축 및 자체 보안대책을 수립하여야 한다.

V 결론

○ 2014년 2분기 총 21건의 침해시도에 비해 2015년 2분기의 총 침해시도건수는 30건으로 9건의 증가를 보였다. 2분기에는 유해 트래픽이 평균 18.37Gb로 전년도 평균(2.1Gb/월)에 비해 10Gb 이상 급증하였다. 이와 관련해서 새로운 바이러스와 악성코드들에 의해 발생할 수 있는 침해와 공격시도들을 대비하여 더욱 세심한 주의가 요구된다.

○ 2분기에는 1분기에 이어 복합 취약점을 이용한 악성코드 유포가 지속 되고 있다. MS IE, MS XML, Adobe Flash Player, Java 애플릿 취약점 등을 복합적으로 악용하여 악성코드를 유포시키는 사례가 1분기에 이어 지속적으로 나타나고 있으며, 이용자가 많은 홈페이지를 이용하여 악성코드를 유포하는 사례도 증가 하고 있어 사용자의 주의를 요구한다.

○ 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 개선 활동 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

○ 4월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
1	2015-04-29 12:20	용역업체	· 웜·바이러스 감염(추정)으로 경유지에 파일업로드 시도 탐지	2015-04-29
2	2015-04-22 13:27	국가나노 기술정책센터 강상규	· 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-04-22
3	2015-04-21 09:02	대용량 데이터허브실 안상언	· 웜·바이러스 및 악성프로그램 감염(추정)으로 인한 경유지로 감염신호 전송 탐지	2015-04-21
4	2015-04-14 01:13	국가나노 기술정책센터 강상규	· 웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-04-14
5	2015-04-13 14:30	미래 기술분석실 이상필	· 웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-04-13
6	2015-04-02 05:00	슈퍼컴퓨팅 서비스통합실	· 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 목적지 IP를 대상으로 대량의 TCP Syn 패킷 전송 행위 탐지	2015-04-02

○ 5월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
7	2015-05-22 12:25	용역업체	· 웹 취약점을 이용한 /etc/passwd 파일 다운로드 탐지	2015-05-22
8	2015-05-21 14:27	정보융합연구실 이석형	· 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-05-21
9	2015-05-11 15:22	국가나노 기술정책센터 김준현	· 웹취약점을 악용하여 홈페이지 변조 탐지	2015-05-11
10	2015-05-11 09:34	국가나노 기술정책센터 정연진	· 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-05-11
11	2015-05-09 22:18	서울 AP	· 웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 경유지 접속시도 탐지	2015-05-09
12	2015-05-08 11:57	미래기술분석실 류정훈	· 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-05-08
13	2015-05-07 10:39	기업혁신전략실 문영수	· 웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-05-07
14	2015-05-06 14:59	정보융합연구실 임지은	· 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보(MAC주소) 전송 시도 탐지	2015-05-06

○ 6월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
15	2015-06-30 09:28	슈퍼컴퓨팅 응용실 차광호	· 웜・바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-06-30
16	2015-06-25 14:24	정보서비스실 이태석	· 웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 중국 악성 도메인 접속 시도 탐지	2015-06-25
17	2015-06-24 15:04	서울 AP	· 웜・바이러스 감염(추정)으로 경유지에 파일업로드 시도 탐지	2015-06-24
18	2015-06-23 09:58	용역업체	· 웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-06-23
19	2015-06-21 17:27	용역업체	· 웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 중국 악성 도메인 접속 시도 탐지	2015-06-21
20	2015-06-20 19:01	용역업체	· 웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-06-20
21	2015-06-20 08:16	용역업체	· 웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보(MAC 주소) 전송 시도 탐지	2015-06-20
22	2015-06-16 23:13	정보화혁신실 이은지	· 웹 취약점을 악용한 파일 업로드 탐지	2015-06-16

사고 번호	발생시간	사고부서	사고내용	처리시간
23	2015-06-16 22:06	정보화혁신실 이은지	· 웹 취약점을 악용한 파일 업로드 탐지	2015-06-16
24	2015-06-14 17:42	정보융합연구실 김순영	· 웜 바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-06-14
25	2015-06-12 18:10	용역업체	· 웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보(MAC주소) 전송 시도 탐지	2015-06-12
26	2015-06-11 14:55	부원장 문영호	· 웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 중국 악성 도메인 접속 시도 탐지	2015-06-11
27	2015-06-11 11:59	창조경제제휴실 정대현	· 웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 중국 악성 도메인 접속 시도 탐지	2015-06-11
28	2015-06-10 12:06	슈퍼컴퓨팅 기술개발실 허태상	· 웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-06-10
29	2015-06-04 15:20	정보융합연구실 김순영	· 웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-06-04
30	2015-06-02 16:20	슈퍼컴퓨팅본부 이필우	· 웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-06-02

[별첨 2] 부서별 사고 건수

부서명	4월	5월	6월
슈퍼컴퓨팅본부	2	0	4
첨단정보융합본부	1	3	1
융합기술연구본부	0	0	0
중소기업혁신본부	0	1	0
미래정책연구부	0	0	0
기획부	0	0	0
행정부	0	0	0
창조경제지원사업단	0	0	1
직할부서	2	2	4
용역업체	1	1	5
기타(무선AP)	0	1	1
합계	6	8	16

[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

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