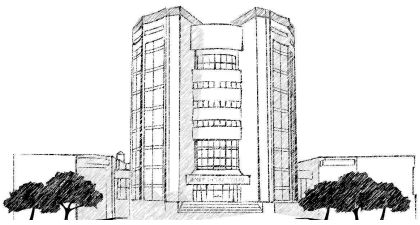
2016년 KISTI 침해사고 대응 분석 (2/4분기)



2016. 11.

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

목 차

그림 목차

표목차

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 정보보호실 통보 - 침해사고 처리결과 확인
정보보호실	- 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 정보보호실 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, 정보보호실 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

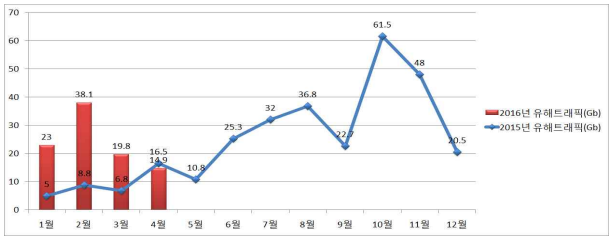
○ 후속조치 : 사고대응 과정에서 발생된 문제들에 대한 검토 회의를 통해 미비점 개선

III 현황 분석

1. 4월 종합 분석

○ 4월 침해사고 분석

- 2016년 4월 유해 트래픽은 [그림 3]과 같이 14.9Gb로 전월 대비 4.9Gb 감소하여 2016년 최저 트래픽양을 보였다.

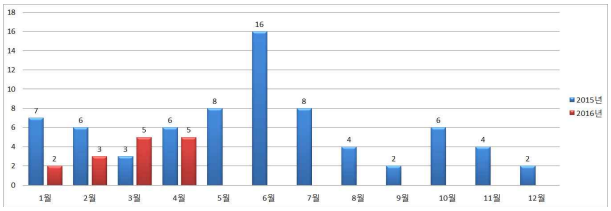


[그림 3] 4월 유해트래픽 추이

- 2016년 4월 침해시도 건수는 [표 1]과 같이 총 5건으로 전월과 동일하게 발생하였다.

구분	2015년									2016년			
	4월	5월	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월
침해 시도 현황	6	8	16	8	4	2	6	4	2	2	3	5	5

[표 1] 4월 침해 시도 현황



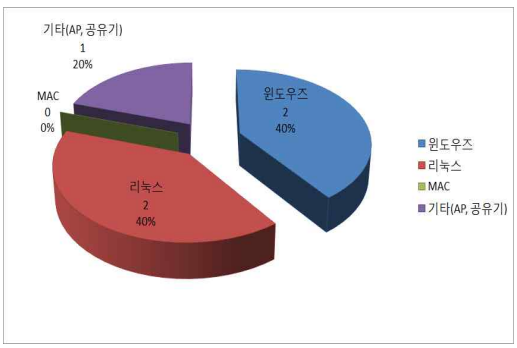
[그림 4] 4월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 2]와 같이 웜·바이러스에 의한 침해시도가 3건으로 가장 많았으며, 그 뒤로 홈페이지 위·변조가 2건 발생하였으며, 홈페이지 위·변조 침해 시도는 올해 들어 처음이다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	3	0	2	0	0	0	5

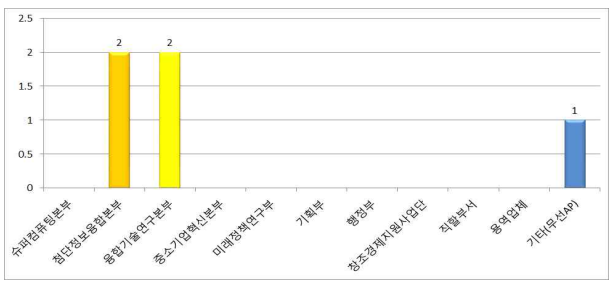
[표 2] 4월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 5]과 같이 윈도우즈 시스템과 리눅스 시스템을 통한 사고가 각각 2건으로 가장 많은 비중을 차지했으며, 그 뒤로 무선AP를 통한 사고가 1건으로 나타났다.



[그림 5] 4월 시스템별(OS) 사고 건수

- 부서별로는 [그림 6]와 같이 침단정보융합본부, 융합기술연구본부에서 각각 2건씩 발생하였으며, 그 뒤로 무선AP에서 1건 발생하였다.



[그림 6] 4월 부서별 사고 건수

○ 4월 보안 이슈 및 향후 계획

- 4월의 보안 이슈로는 Adobe Flash Player의 제로데이 취약점이 발견되었다. 해당 취약한 프로그램으로 사용자가 특수하게 조작된 플래시 파일이 포함된 웹페이지, 스팸 메일 등을 열람할 경우 악성코드에 감염될 수 있으며, 해당 악성코드는 취약점(CVE-2016-1019)을 이용해 시스템 충돌을 발생시키거나 제어할 수 있는 것으로 알려졌다.

- 영향받는 시스템은 어도비 플래시 플레이어 21.0.0.197 및 이전 버전(Windows, Macintosh, Linux, Chrome OS)이므로 취약점에 의한 피해를 줄이기 위해 신뢰되지 않은 웹 사이트 방문 자제, 출처가 불분명한 이메일 및 링크를 열람 금지, 사용하고 있는 백신프로그램의 최신 업데이트 유지 및 실시간 감시기능 활성화가 요구된다.

- 한국인터넷진흥원(KISA)을 사칭한 스피어피싱 이메일이 발견되었다. 해당 스피어피싱 메일은 '[한국인터넷진흥원] 정보보안 용어모음'이란 제목으로 인터넷 발신자 계정은 jeongseon0571이며, 포털사 다음 메일을 도용하고 있다. 또한, 메일에는 악성코드가 심어진 Security Words.hwp 파일을 다운로드 할 수 있도록 링크가 걸려 유포되고 있다.

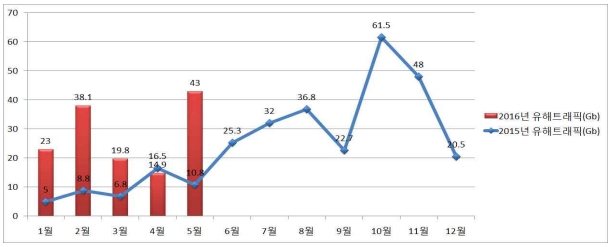
- 메일 내용은 '한국인터넷진흥원 정보관리 담당자 000입니다. 우리 진흥원에서는 보다 편리한 시스템사용을 위한 자원봉사를 하고 있습니다. 시스템 운영에 많은 도움이 되길 바랍니다. 첨부파일의 문서 암호는 sec16'이라며 첨부파일을 열도록 안내하며 악성코드 감염을 유도하고 있다.

- KISA 내부 직원과 KISA를 사칭한 스피어피싱 이메일이 유포되고 있는 만큼, 피해확산 방지를 위해 해당 이메일 수신시 열람금지를 권고하고 있다.

2. 5월 종합 분석

○ 5월 침해사고 분석

- 2016년 5월의 유해 트래픽은 [그림 7]과 같이 43Gb로 전월대비 28.1Gb 증가하였다.

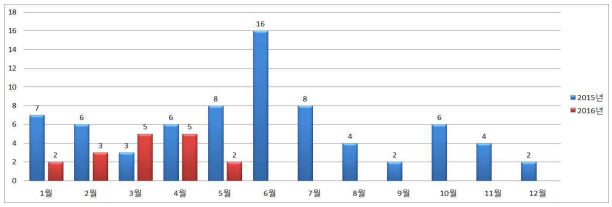


[그림 7] 5월 유해트래픽 추이

- 2016년 5월 침해시도 건수는 [표 3]와 같이 총 2건으로 전월 대비 3건 감소하였다.

구분	2015년								2016년				
	5월	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월
침해 시도 현황	8	16	8	4	2	6	4	2	2	3	5	5	2

[표 3] 5월 침해 시도 현황



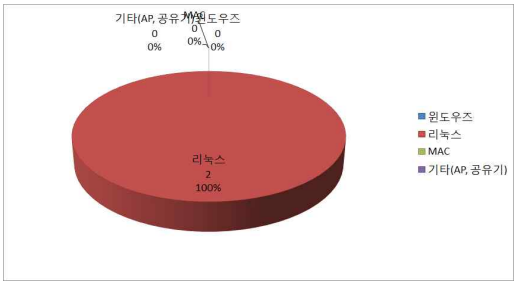
[그림 8] 5월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 4]와 같이 웜·바이러스에 의한 침해시도 1건, 홈페이지 위·변조 1건으로 나타났다. 홈페이지 위·변조에 대한 침해 시도가 저번달에 이어 계속 발생하는 만큼, 시스템 관리자의 주의가 요구된다.

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

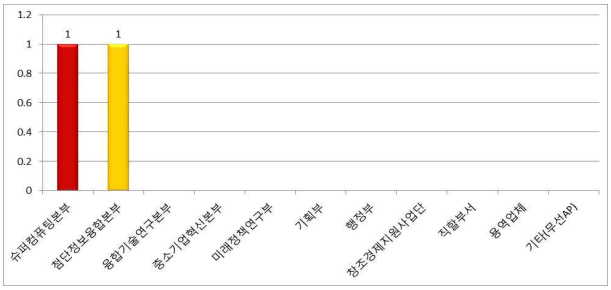
[표 4] 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 9]와 같이 발생한 사고 총 2건 모두 리눅스 시스템을 통한 사고로 나타났다.



[그림 9] 5월 시스템별(OS) 사고 건수

- 부서별로는 [그림 10]과 같이 슈퍼컴퓨팅본부, 첨단정보융합본부가 각각 1건씩 발생하였다.



[그림 10] 5월 부서별 사고 건수

○ 5월 보안 이슈 및 향후 계획

- 이달에는 저번달에 이어 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.

3. 6월 종합 분석

○ 6월 침해사고 분석

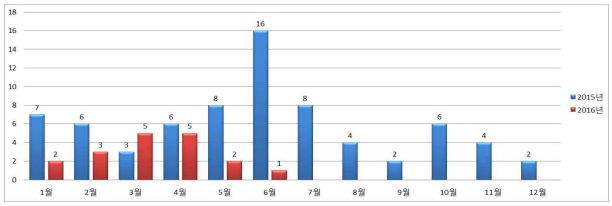
- 2016년 6월 유해 트래픽은 [그림 11]와 같이 44.4Gb로 전월 대비 1.4Gb 증가하여, 올 해 최고 수치를 보였다.

[그림 11] 6월 유해트래픽 추이

- 2016년 6월 침해시도 건수는 [표 5]와 같이 총 11건으로 전월 대비 1건 감소하였다.

구분	2015년							2016년					
	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
침해 시도 현황	16	8	4	2	6	4	2	2	3	5	5	2	1

[표 5] 6월 침해 시도 현황



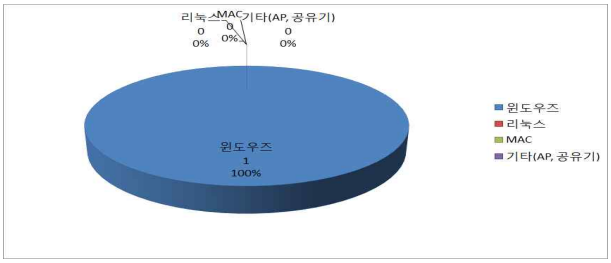
[그림 12] 6월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 6]과 같이 자료훼손 및 유출에 의한 침해시도가 1건 발생하였다.

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

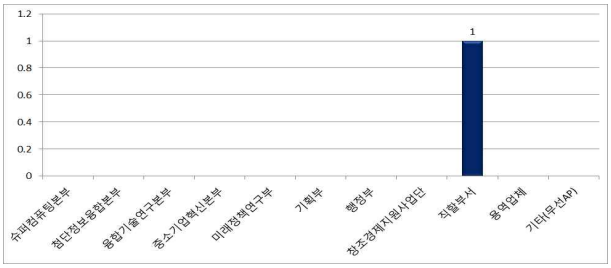
[표 6] 6월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 13]과 같이 윈도우즈 시스템을 통한 사고가 1건 발생하였다.



[그림 13] 6월 시스템별(OS) 사고 건수

- 부서별로는 [그림 14]와 같이 직할부서에서 1건 발생하였다.



[그림 14] 6월 부서별 사고 건수

○ 6월 보안 이슈 및 향후 계획

- 이달에는 자료훼손 및 유출 시도가 발생하였다.

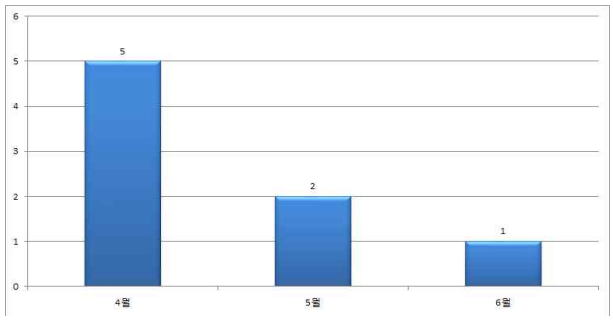
- 해당시스템 분석결과 게시판 업로드 취약점을 악용하여 웹셸을 업로드 한 것으로 파악된다.

- 웹서버를 운영하는 시스템 담당자는 웹 방화벽에서 443으로 전송하는 데이터에 대한 차단 정책(암호화 전송)을 세워야 하며, 첨부파일 업로드 시 업로드 파일에 대한 확장자 체크 등 첨부파일에 대한 검사가 이루어지도록 소스코드에 대한 취약점 보완이 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

○ 2016년 4월부터 6월까지의 침해시도 건수는 [그림 15]와 같이 총 8건으로 4월이 5건으로 가장 많이 발생하였으며, 그 뒤로 5월이 2건, 6월이 1건으로 발생하였다.



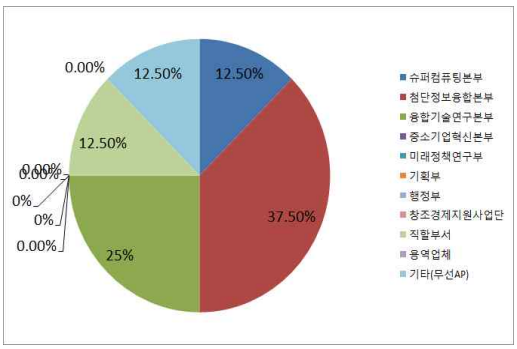
[그림 15] 2분기 월별 침해시도 건수

○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 사고가 4건으로 가장 많은 비율을 차지하였으며, 그 뒤로 홈페이지 위 ·변조사고가 3건, 자료훼손 및 유출 1건 순으로 발생되었다.

	4월	5월	6월
웜 · 바이러스	3	1	0
자료훼손 및 유출	0	0	1
홈페이지 위 · 변조	2	1	0
경유지 악용	0	0	0
서비스 거부	0	0	0
단순침입시도	0	0	0
합계	5	2	1

[표 7] 침해 위협 유형별 분석

○ 부서별로는 [그림 16]과 같이 첨단정보융합본부가 3건(37.5%)으로 가장 많은 비중을 차지하였으며, 그 뒤로 융합기술연구본부가 2건(25%), 슈퍼컴퓨팅본부, 직할부서, 기타(무선AP)가 각각 1건(12.5%)의 사고가 발생하였다.



[그림 16] 2분기 부서별 사고 건수 비율

- **웜·바이러스에 의한 사고**

- 2분기에 발생한 사고 중 웜·바이러스에 의한 사고가 4건으로 절반을 차지하였다. 웜·바이러스에 의한 사고는 매분기 가장 많은 사고로 기록되고 있으며 대다수 사용자들의 부주의에 의해 발생하고 있다. 출처가 의심스러운 메일 열람 금지, 의심스런 웹사이트 방문 자제 등 사용자에 대한 꾸준한 교육이 지속되어야 할 것이다.

- **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**

- 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 정보보호실에서는 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), UDP/5567 (Multicast Object Access Protocol)으로 원격접속에 대한 침해시도가 많이 탐지 되었다. 따라서 시스템 운영자는 비인가된 접속에 대한 로그관리와 ssh와 같은 서비스의 포트설정 변경, 원격에서 루트계정 로그인 금지, 패스워드 정책강화와 주기적인 패스워드 변경 등 서버보안을 위한 보안정책 강화에 주의하여야 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

○ 2015년 2분기 총 30건의 침해시도에 비해 2016년 2분기의 총 침해시도건수는 8건으로 22건의 감소세를 보였다. 2분기에는 유해 트래픽이 평균 34.1Gb로 전년도 평균(25.2Gb/월)에 비해 10Gb 가량 급증하였다. 이와 관련해서 새로운 바이러스와 악성코드들에 의해 발생할 수 있는 침해와 공격시도들을 대비하여 더욱 세심한 주의가 요구된다.

○ 2분기에는 금융정보 탈취 및 원격제어용 악성코드 유포가 언론, 취업포탈, 유학정보센터, 웨딩, 쇼핑몰 등 다양한 분야 웹사이트에 유포가 되어 사용자의 주의가 요구된다. 특히 북한의 핵실험과 장거리미사일 발사 등으로 인한 남북간의 긴장감 속에 사이버 위협도 고조되고 있어 홈페이지 관리에 세심한 주의가 요구된다.

○ 또한 랜섬웨어의 유포방식이 이메일 첨부파일/메신저 전파 등 고전 기법에 각종 응용프로그램, OS, 웹취약점 및 토렌트 등 다양한 유포 방식으로 증가하여 감염효과를 극대화시키기 위한 다양한 시도가 발견되었다. 랜섬웨어는 수많은 신변종이 지속적으로 발생하고 있기 때문에 피해를 줄이기 위해서는 수상한 이메일 첨부파일 및 URL 실행 금지, 중요한 데이터는 외부 저장장치로 백업, 백신 최신 업데이트 유지, 운영체제(OS) / SW 프로그램의 최신 보안패치 적용, 신뢰할 수 없는 웹사이트 방문 자제 등 사용자의 기본 보안수칙을 생활화 하는 자세가 필요하다.

○ 이미지 뷰어 프로그램인 '꿀뷰'를 통한 악성코드 감염도 나타났다. 반디소프트 홈페이지가 외부로부터 공격을 받아 이 기간 동안 홈페이지를 통해서 다운로드 받은 사용자 200여명이 악성코드에 감염되어 ARP 스푸핑 공격에 의해 시스템의 정보가 외부로 유출되는 공격을 받은 것이다. 이처럼 알려진 소프트웨어라 하더라도 무분별하게 사용시 악성코드에 감염될 수가 있으므로 업무용 소프트웨어 이외의 프로그램 사용시 각별한 주의가 요구된다.

○ 향후 허용된 소프트웨어를 제외한 모든 소프트웨어에 정밀한 조사를 통해 업무외 소프트웨어에 대한 삭제를 권고하고 소프트웨어 사용에 대한 관리와 모니터링을 통한 통제가 필요할 것으로 보인다.

[별첨 1] 월별 침해위협 발생 현황

○ 4월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
1	2016-04-06	재난예측 기술연구실 이현조	웜· 바이러스 및 악성 프로그램 감염(추정)으로 인한 경유지로부터 파일 다운로드 시도 탐지	2016-04-07
2	2016-04-08	의사결정 지원기술실 선충녕	웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2016-04-08
3	2016-04-09	정보융합연구실 황윤영	웹쉘 업로드 시도 탐지	2016-04-15
4	2016-04-13	R&D사업정보개발실 김종원	홈페이지 특정 URL에서 관리자 권한으로 접속되는 취약점 노출	2016-04-13
5	2016-04-19	무선 AP	웜·바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2016-04-19

○ 5월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
6	2016-05-14	정보융합연구실 황윤영	한국과학기술정보연구원 KOSEN 홈페이지(www.kosen21.org) 변조(추정) 탐지	2016-05-15
7	2016-05-22	첨단연구망 서비스실 이원혁	웜·바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2016-05-30

○ 6월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
8	2016-06-07	아이디어 플랫폼운영실 김대섭	웜·바이러스 및 악성 프로그램 감염(추정)으로 경유지에 파일업로드 시도 탐지	2016-06-09

[별첨 2] 부서별 사고 건수

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

[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