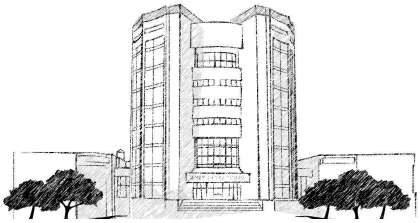
2016년 KISTI 침해사고 대응 분석 (1/4분기)



2016. 11.

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 ····· 22
[별첨 2.] 부서별 사고 건수 ····· 24
[별첨 3.] 침해시도 유형별 내용 ····· 25
[별첨 4.] 사이버위기 상황 발생 시 대상별 협조 사항 ····· 26

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 7. 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 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 대응 절차를 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

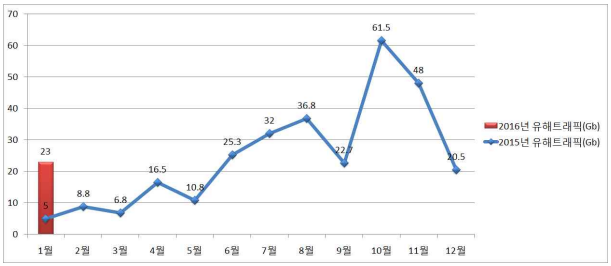
○ 후속조치 : 사고대응 과정에서 발생된 문제들에 대한 검토 회의를 통해 미비점 개선

Ⅲ 현황 분석

1. 1월 종합 분석

○ 1월 침해사고 분석

- 2016년 1월 유해 트래픽은 [그림 3]과 같이 23Gb로 전월 대비 18Gb증가 하였고 전년도 같은 기간에 비해 4배 이상 증가하였다.

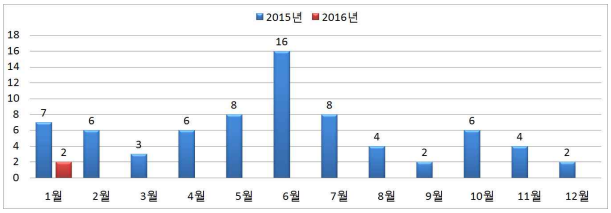


[그림 3] 1월 유해트래픽 추이

- 2016년 1월 침해시도 건수는 [표 1]과 같이 총 2건으로 전월과 동일하며, 전년도 같은 기간에 비해 5건 감소하였다.

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

[표 1] 1월 침해 시도 현황



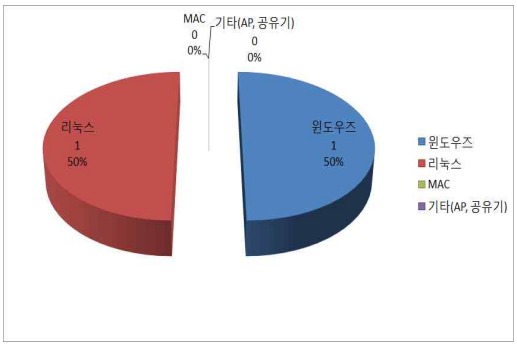
[그림 4] 1월 침해시도 건수 추이

- 침해 위협 유형별로 살펴보면 [표 2]와 같이 웜·바이러스에 의한 사고 1건, 자료훼손 및 유출 사고가 1건 발생되었다.

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

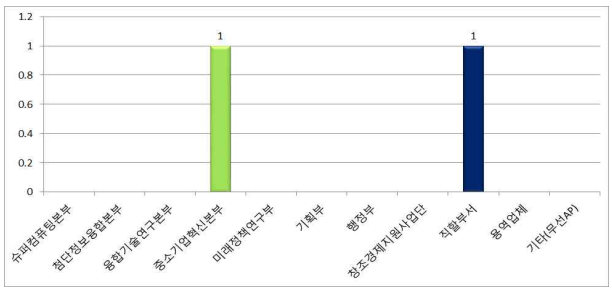
[표 2] 1월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 5]와 같이 윈도우즈 시스템과 리눅스 시스템을 통한 사고가 각각 1건으로 동일하게 발생하였다.



[그림 5] 1월 시스템별(OS) 사고 건수

- 부서별로는 [그림 6]와 같이 중소기업혁신본부, 직할부서에서 각각 1건씩 발생하였다.



[그림 6] 1월 부서별 사고 건수

○ 1월 보안 이슈 및 향후 계획

- 1월 보안 이슈는 전국 공공기관을 대상으로 악성코드가 심어진 청와대 사칭 메일이 대량 발송됐다. 메일 발송 시 첨부파일에는 HWP 취약점 파일이 포함됐으며, 한컴 취약점을 이용하여 공격하는 것으로 나타났다. 일반적으로 한글과컴퓨터사의 '한글' 취약점은 한글 파일의 글자크기, 외국어, 그림, 효과 처리 부분 등으로, 첨부된 한글파일 실행 시 그림이나 특정 효과를 나타내기 위한 명령을 공격자가 예상하지 못한 데이터를 조작해 오동작을 일으켜 공격자가 만든 코드가 실행된다.

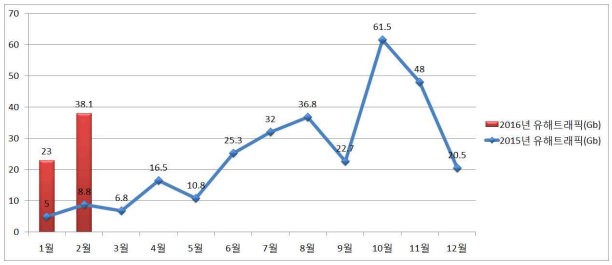
- 이번 사건의 경우 이례적으로 중국 정부기관 웹사이트를 해킹해 C&C(Command and Control) 서버로 활용하고 있고, 사이버공격 범위가 넓게 확인되고 있어 공공기관의 보안관제와 보안점검 등에 만전을 기울여야 할 것으로 보인다.

- 기관은 소속직원들에게 '한글'의 자동업데이트 기능을 통한 업데이트 및 한글과 컴퓨터사의 홈페이지를 통한 보안패치 프로그램 설치, 출처를 알 수 없는 이메일 클릭금지, OS 및 바이러스 백신 업데이트의 보안 업데이트 필수 등의 보안교육이 요구된다.

2. 2월 종합 분석

○ 2월 침해사고 분석

- 2016년 2월의 유해 트래픽은 [그림 7]과 같이 38.1Gb로 전월대비 15.1Gb 증가하였으며, 전년도 동월보다 4배 이상 증가하였다.

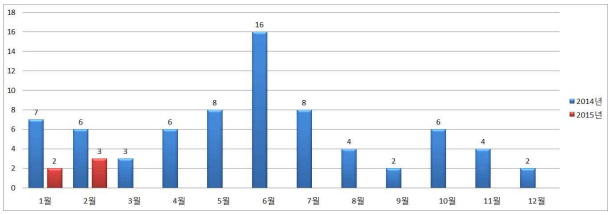


[그림 7] 2월 유해트래픽 추이

- 2016년 2월 침해시도 건수는 [표 3]과 같이 총 3건으로 전월 대비 1건 증가하였다.

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

[표 3] 2월 침해 시도 현황



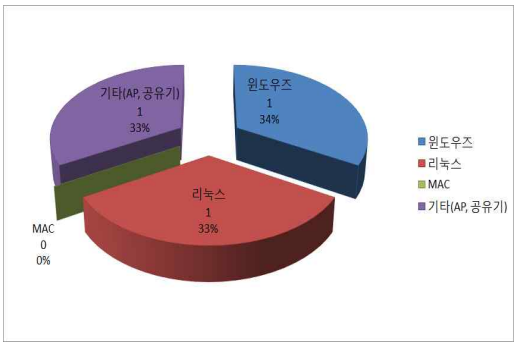
[그림 8] 2월 침해 시도 건수 추이

- 침해 위협 유형별로 살펴보면 [표 4]와 같이 웜·바이러스에 의한 침해가 2건, 그 뒤를 이어 자료훼손 및 유출이 1건 발생하였다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	2	1	0	0	0	0	3

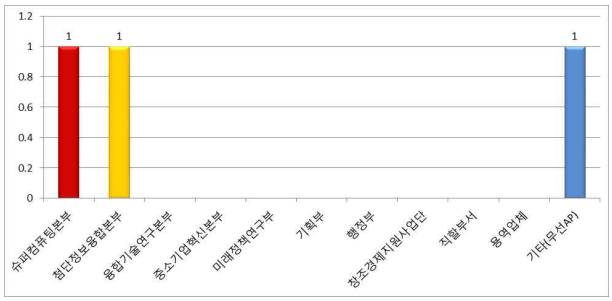
[표 4] 2월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 9]과 같이 윈도우즈 시스템, 리눅스 시스템, 기타(AP, 공유기)를 통한 사고가 각각 1건씩 발생하였다.



[그림 9] 2월 시스템별(OS) 사고 건수

- 부서별로는 [그림 10]과 같이 슈퍼컴퓨팅본부, 첨단융합본부, 기타(무선AP)가 각각 1건씩 발생하였다.



[그림 10] 2월 부서별 사고 건수

○ 2월 보안 이슈 및 향후 계획

- 2월에는 리눅스 GNU C 라이브러리(glibc)에서 원격코드 실행 가능한 취약점이 발견되었다. 해당 취약점은 glibc의 getaddrinfo 함수에서 발생하는 버퍼오버플로우 취약점(CVE-2015-7547)이다. GNU C 라이브러리(glibc)란 리눅스 계열 운영체제에서 C언어로 작성된 실행파일들이 동작하기 위해 공통적으로 사용하는 기능을 쉽게 이용할 수 있도록 묶어 놓은 소프트웨어 집합을 말하며, 낮은 버전 사용자는 시스템 임의코드 실행 등에 취약할 수 있으므로 최신버전으로 업데이트를 요구한다.

- 이와 관련하여 서버 관리자의 경우 CentOS, Debian, Redhat, Ubuntu, Suse 등 OS의 버전을 GNU glibc 2.9 이후 버전을 사용하는 시스템으로 업데이트 해야한다.

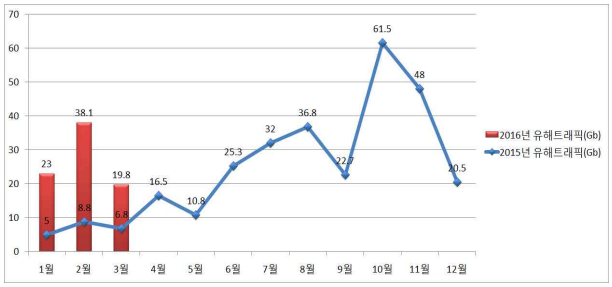
- 오라클, Java SE6·7·8에서 원격코드 실행 가능한 취약점이 발견되었다. 이 취약점을 통해 공격자는 특수하게 조작된 웹 사이트 방문 및 다운로드 파일을 유도해 악성코드 유포가 가능하다.

- 따라서 취약점에 의한 피해를 줄이기 위해 사용자는 신뢰할 수 없는 웹사이트 방문 및 첨부파일을 열어보지 않도록 주의해야 하며, 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나 Java 자동업데이트 설정이 요구된다.

3. 3월 종합 분석

○ 3월 침해사고 분석

- 2016년 3월 유해 트래픽은 [그림 11]와 같이 19.8Gb로 전월 대비 18.3Gb 감소하였고, 2016년 상반기 최저 트래픽 양을 보였다.

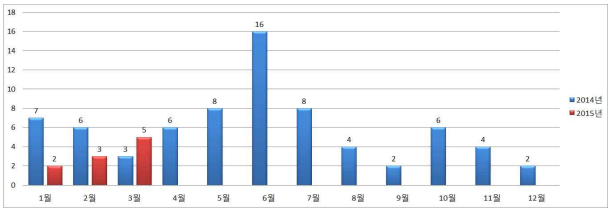


[그림 11] 3월 유해트래픽 추이

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

구분	2014년										2015년		
	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월
침해시도 현황	3	6	8	16	8	4	2	6	4	2	2	3	5

[표 5] 3월 침해 시도 현황



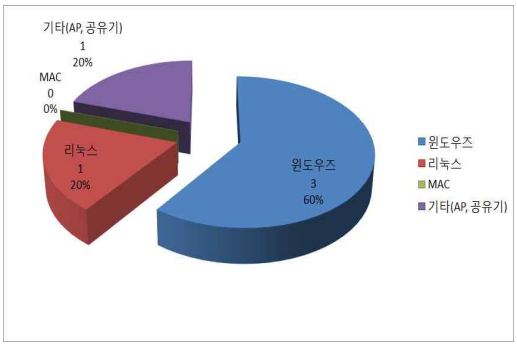
[그림 12] 3월 침해시도 건수 추이

- 침해 위협 유형별로 살펴보면 [표 6]과 같이 웜·바이러스에 의한 사고가 4건, 경유지 악용이 1건으로 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	4	0	0	1	0	0	5

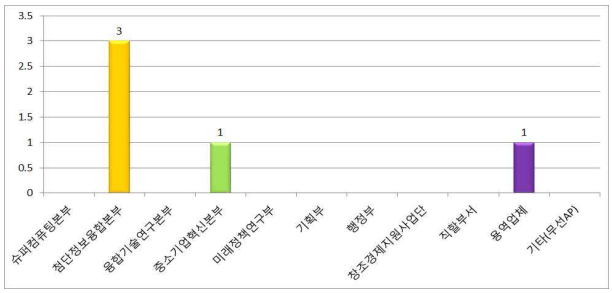
[표 6] 3월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 13]과 같이 윈도우즈 시스템을 통한 사고가 3건으로 가장 많은 비중을 차지했으며, 그 뒤로 리눅스 시스템, 기타(AP, 공유기)를 통한 사고가 각각 1건씩 발생하였다.



[그림 13] 3월 시스템별(OS) 사고 건수

- 부서별로는 [그림 14]와 같이 침단정보융합본부가 3건으로 제일 많았으며, 중소기업혁신본부, 용역업체에서 각각 1건씩 발생하였다.



[그림 14] 3월 부서별 사고 건수

○ 3월 보안 이슈 및 향후 계획

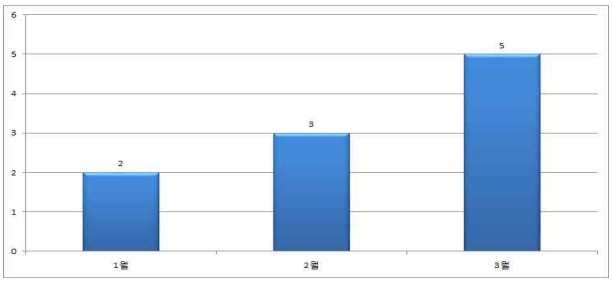
- 3월의 보안 이슈로는 OpenSSL 취약점을 예방하기 위한 긴급 보안 업데이트가 발표됐다.

- OpenSSL 측에서 발견한 취약점은 SSLv2를 이용한 TLS에 대한 프로토콜 간 공격(CVE-2016-0800), 힙 오버플로우에 기반을 둔 공격으로 원하는 위치의 메모리를 사용하는 DFB(Double-Free Bug)(CVE-2016-0705), SRP 데이터베이스에서의 메모리 누수(CVE-2016-0798), 널 포인터에 임의의 값을 대입하여 발생하는 널 포인터 역참조 에러 및 동적 할당한 크기보다 더 큰 영역에 접근함으로써 발생하는 힙 커럽션 에러(CVE-2016-0797), 고정 메모리 이슈(CVE-2016-0799), 알고리즘의 약점을 찾거나 무차별 공격을 하는 대신 암호체계의 물리적인 구현과정의 정보를 기반으로 하는 부채널 공격(CVE-2016-0702), 그대로 해결할 수 없는 문제를 작은 문제로 분할하여 문제를 해결하는 방법인 분할 정복 알고리즘(CVE-2016-0703), RSA 암호화 메시지 내용을 점차적으로 노출하기 위한 Bleichenbacher 공격(CVE-2016-0704)으로 총 8건이다.

- 따라서 해당 취약점에 영향받지 않기위해 OpenSSL 1.0.1, 1.0.2 사용자는 각각 OpenSSL 1.0.1s, 1.0.2g로 업데이트 해야한다.

Ⅳ 종합분석 및 개선방안

○ 2016년 1월부터 3월까지의 침해시도 건수는 [그림 15]와 같이 총 10건으로 3월이 5건으로 가장 많이 발생하였으며, 그 뒤로 2월이 3건, 1월이 2건 발생하였다.



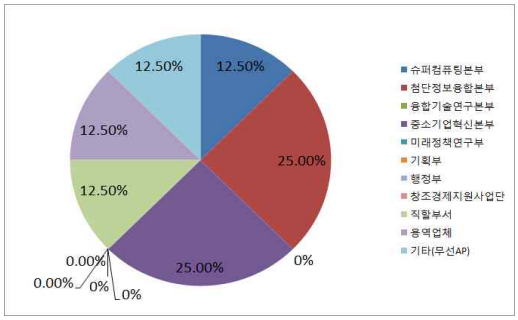
[그림 15] 1분기 월별 침해시도 건수

○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 사고가 7건, 그 뒤를 이어 자료훼손 및 유출이 2건, 경유지 악용이 1건 발생하였다.

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

[표 7] 침해 위협 유형별 분석

○ 부서별로는 [그림 16]과 같이 첨단정보융합본부와 중소기업혁신본부가 2건(25%)으로 가장 많은 비중을 차지하였으며, 그 뒤로 슈퍼컴퓨팅본부, 직할부서, 용역업체, 기타(무선AP)에서 각각 1건(12.5%)의 사고가 발생하였다.



[그림 16] 1분기 부서별 사고 건수 비율

● **웜·바이러스에 의한 사고**

- 분석 결과 4분기에 발생한 사고중 웜·바이러스에 의한 사고가 6건으로 가장 많이 발생했으며 자료훼손 및 유출 2건, 경유지 악용 1건 순으로 발생하였다.

- 웜·바이러스에 의한 사고는 사용자들의 안전하지 못한 웹사이트 접속으로 인해 발생하는 경우가 대부분이다. 따라서, 위 문제를 해결하기 위한 대책으로 방화벽을 통한 알려진 안전하지 못한 웹사이트 접속 차단 및 게임, 증권 사이트와 같이 업무이외의 사이트의 차단을 실시함과 동시에 사용자에 대한 지속적인 교육을 통해 보안의식을 높일 수 있는 방안이 요구된다.

● **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 무선 AP를 통한 사고의 경우 발생 사고자를 파악하지 못하여 사고 조사가 이루어지지 못한 사례도 발생하였다.

- 현재 무선 AP의 경우 아이디를 통한 IP를 할당하여 관리하도록 하고 있으나, 네트워크 운영부서를 통해 중앙에서 MAC 등록을 통한 IP 관리 및 주기적인 모니터링을 통하여 무선 AP를 통한 사고에 대해서도 적절한 조치가 이루어질수 있도록 정책적인 변화가 필요하다.

● **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 1월 공격대상 포트중

TCP/22 (ssh)는 91.5%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

○ 2015년 4분기 총 12건의 침해시도에 비해 2016년 3월까지의 총 침해시도건수는 10건으로 2건이 감소하였다. 하지만 1월 이후 침해시도 건수는 꾸준히 증가하고 있어 침해시도에 대한 주의가 요구된다.

○ 1분기에는 국내 전력기관에 이메일을 통해 랜섬웨어를 포함한 매크로 악성코드가 유입되는 것이 발견되었으며 워드 문서내에 깨진 문자를 넣어놓고 깨진 문자를 보려면 매크로를 실행하도록 하여 랜섬웨어에 걸리도록 유도하기에 메일 수신시 매크로 실행 메시지가 뜨면 악성코드일 가능성이 높기 때문에 매크로 실행을 자제해야 하며, 메일 수신에 각별한 주의가 요구된다.

○ 또한 리눅스 GNU C 라이브러리(glibc)에서 원격코드 실행 가능한 취약점이 발견되어 이용자들의 주의가 요구된다. 이 취약점은 getaddrinfo 함수에서 발생하는 버퍼오버플로우를 이용한 취약점으로 낮은 버전의 사용자는 시스템 임의코드 실행 등에 취약할 수 있으므로 최신버전으로 업데이트가 필요하다.

○ 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

○ 1월 침해 위협 발생 현황

사고번호	발생시간	사고부서	사고내용	처리시간
1	2016-01-14	정보시스템운영실 전승엽	OpenSSL의 취약점을 이용하여 시스템 정보유출 탐지	2016-01-14
2	2016-01-20	부산울산경남지원 박민지	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2016-01-21

○ 2월 침해 위협 발생 현황

사고번호	발생시간	사고부서	사고내용	처리시간
3	2016-02-13	대전 AP	웜・바이러스 피해(추정)	2016-02-13
4	2016-02-13	대용량데이터허브실 김진	OpenSSL의 취약점을 이용하여 시스템 정보유출 탐지	2016-02-13
5	2016-02-16	정보융합연구실 황윤영	웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 감염신호 전송	2016-02-16

○ 3월 침해 위협 발생 현황

사고번호	발생시간	사고부서	사고내용	처리시간
6	2016-03-13	정보기반실 임석종	경유지악용 추정으로 IRC를 통해 악성프로그램 다운로드 탐지	2016-03-13
7	2016-03-14	정보서비스실 최현규	해킹메일 열람(추정)으로 인한 경유지 접속시도 탐지	2016-03-14
8	2016-03-16	대구경북지원 서슬기	해킹메일 유입	2016-03-16
9	2016-03-22	기술은행보안센터연구실 김선호	해킹경유지 탐지 통보	2016-03-23

[별첨 2] 부서별 사고 건수

부서명	1월	2월	3월
슈퍼컴퓨팅본부	0	1	0
첨단정보융합본부	0	1	1
융합기술연구본부	0	0	0
중소기업혁신본부	1	0	1
미래정책연구부	0	0	0
기획부	0	0	0
행정부	0	0	0
창조경제지원사업단	0	0	0
직할부서	1	0	0
용역업체	0	0	1
기타(무선AP)	0	1	0
합계	2	3	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 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 이에 대한 대비 필요 3. 네트워크 이상트래픽 과다 탐지 또는 부분 장애 등 사이버위협 징후 탐지활동 강화 필요