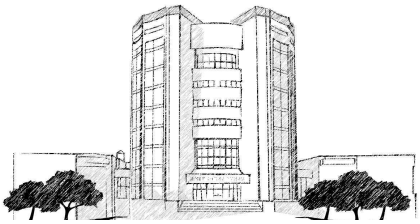
2015년 KISTI 침해사고 대응 분석 보고서
(4/4분기)



2016 11.

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

목 차

그림 목차

표 목차

Ⅰ 개요

1. 목적 및 필요성

○ 지능화 다양화 되고 있는 사이버 위협 및 APT와 같은 표적 공격으로부터 KISTI의 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 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 복구 할 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

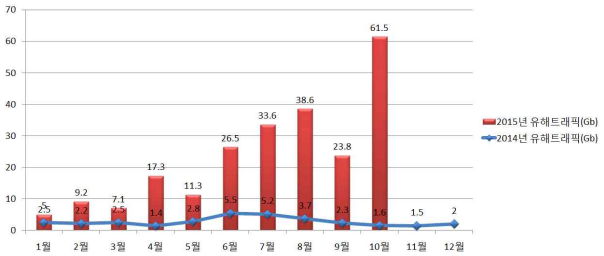
○ 후속조치 : 사고대응 과정에서 발생된 문제들에 대한 검토 회의를 통해 미비점 개선

III 현황 분석

1. 10월 종합 분석

○ 10월 침해사고 분석

- 2015년 10월 유해 트래픽은 [그림 3]과 같이 61.5Gb로 전월 대비 37.7Gb 증가하여, 2015년 내 가장 높은 수치를 보였다.

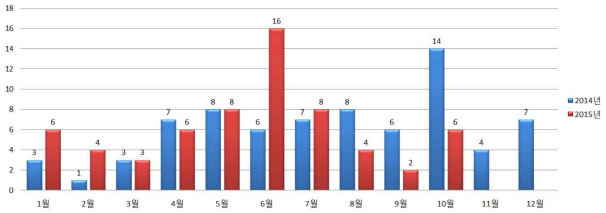


[그림 3] 10월 유해트래픽 추이

- 2015년 10월 침해시도 건수는 [표 1]와 같이 총 6건으로 전월 대비 4건 증가하였다.

구분	2014년			2015년								
	10월	11월	12월	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월
침해 시도 현황	6	14	4	7	6	3	6	8	16	8	4	2	6

[표 1] 10월 침해 시도 현황



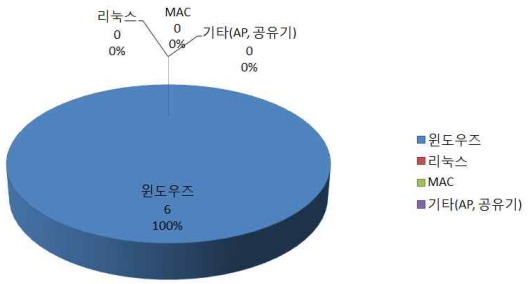
[그림 4] 10월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 2]와 같이 웜·바이러스에 의한 침해시도가 6건으로 대부분 웹 서비스(TCP 80) 이용 중 발생한 것으로 파악된다.

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

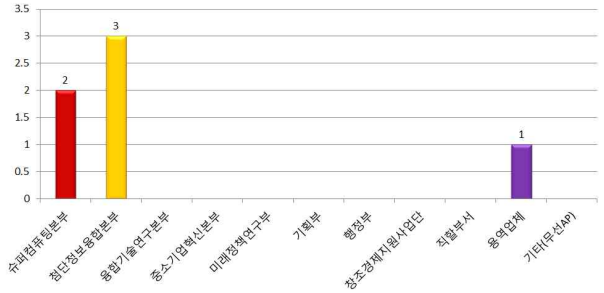
[표 2] 10월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 5]과 같이 윈도우즈 시스템을 통한 사고가 6건으로 모든 사고가 윈도우 시스템을 통해 발생하였다.



[그림 5] 10월 시스템별(OS) 사고 건수

- 부서별로는 [그림 6]과 같이 침단정보융합본부가 3건으로 가장 많았고, 그 뒤로 슈퍼컴퓨팅본부가 2건 발생하였으며, 용역업체가 1건 발생하였다.



[그림 6] 10월 부서별 사고 건수

○ 10월 보안 이슈 및 향후 계획

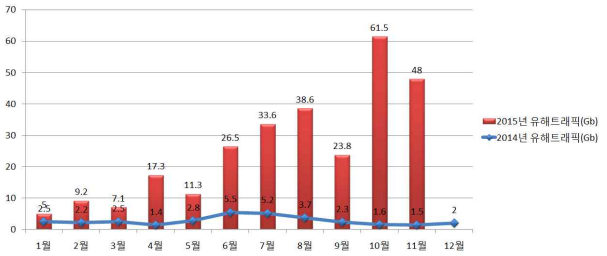
- 표준 HTTP 포트인 TCP/80포트를 이용한 침해시도는 올해 초부터 꾸준히 발생하고 있다. 주로 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보를 전송하는 행위가 많이 발생하였다.

- 이에 대한 예방책으로 웹사이트 방문 시 의심스러운 프로그램(ActiveX)의 설치를 금하며, 출처 및 의심스러운 이메일은 열람하지 않도록 주의가 요구된다. 또한 업무용 PC가 DDoS 공격 및 해킹 공격을 유발하는 좀비 PC가 되지 않도록 윈도우 운영체제의 보안 및 백신을 최신 버전으로 업데이트 하는 등 신규 취약점에 대한 대비가 요구된다.

2. 11월 종합 분석

○ 11월 침해사고 분석

- 2015년 11월의 유해 트래픽은 [그림 7]과 같이 48.Gb로 전월대비 13.5Gb 감소하였다.

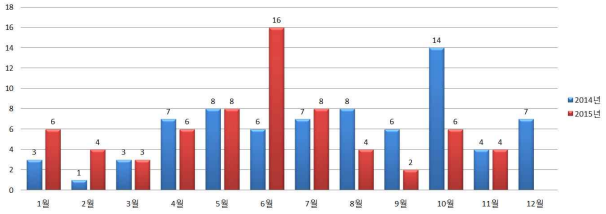


[그림 7] 11월 유해트래픽 추이

- 2015년 11월 침해시도 건수는 [표 3]과 같이 총 4건으로 전월보다 2건 적은 수치를 보였다.

구분	2014년		2015년										
	11월	12월	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월
침해 시도 현황	14	4	7	6	3	6	8	16	8	4	2	6	4

[표 3] 11월 침해 시도 현황



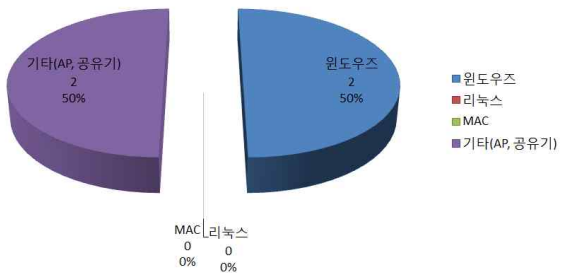
[그림 8] 11월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 4]와 같이 웜·바이러스에 의한 침해시도가 4건으로 모든 사고가 웜·바이러스에 의해 발생 하였다.

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

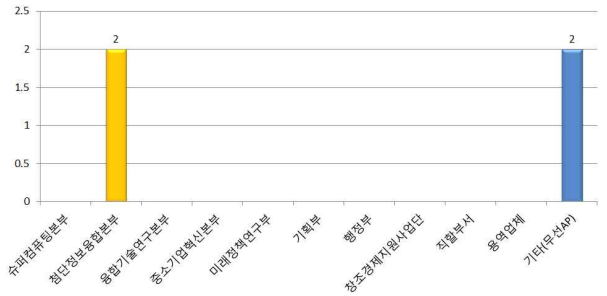
[표 4] 11월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 9]와 같이 윈도우즈 시스템을 통한 사고와 무선AP를 통한 사고가 각각 2건으로 발생하였다.



[그림 9] 11월 시스템별(OS) 사고 건수

- 부서별로는 [그림 10]과 같이 첨단정보융합본부와 기타(무선AP)가 각각 2건씩 발생하였다.



[그림 10] 11월 부서별 사고 건수

○ 11월 보안 이슈 및 향후 계획

- 기존 랜섬웨어와는 조금 다른 방식으로 사용자들을 협박하는 새로운 랜섬웨어 변종인 '키메라(Chimera)'가 등장했다. 키메라 랜섬웨어는 일반적인 파일 암호화 작업에 스퀘어웨어(Scareware) 방식이 결합된 형태를 말하며, 스케어웨어는 사용자를 협박해 불안감을 조성하는 악성코드를 말한다.

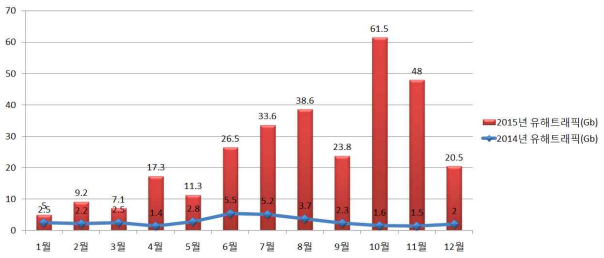
- 키메라 랜섬웨어는 일반적인 랜섬웨어처럼 파일을 암호화해 사용자를 협박하는 것은 똑같지만 협박 방식이 일반 랜섬웨어와 차이가 난다. 일반적인 랜섬웨어는 '너의 소중한 파일을 돌려받고 싶으면 돈을 내라'고 하지만 키메라는 '돈을 내지 않으면 너의 소중한 파일을 인터넷에 공개하겠다'고 협박하는 방식이다.

- 사람의 심리를 이용하는 악성코드로 이를 예방하기 위해서는 주기적인 백업 및 소프트웨어 업데이트가 요구된다. 또한, 의심스러운 링크나 첨부파일을 열지 않도록 주의해야 한다.

3. 12월 종합 분석

○ 12월 분석

- 2015년 12월 유해 트래픽은 [그림 11]와 같이 20.5Gb로 전월 대비 27.5Gb 감소하였다.

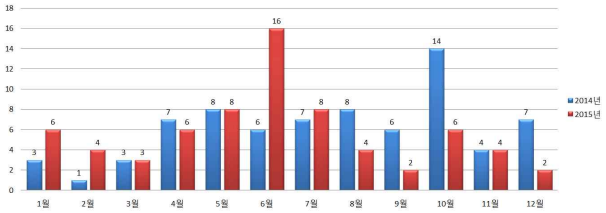


[그림 11] 12월 유해트래픽 추이

- 2015년 12월 침해시도 건수는 [표 5]와 같이 총 2건으로 전월 대비 2건 적은 수치를 보였고 10월 이후 꾸준히 감소하고 있다.

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

[표 5] 12월 침해 시도 현황



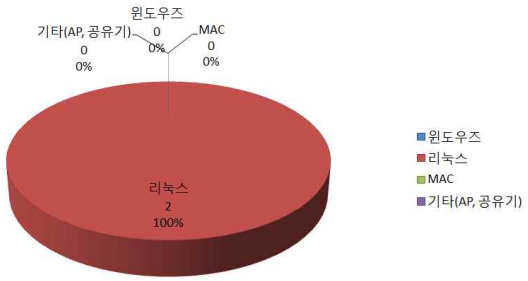
[그림 12] 12월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 6]과 같이 웜·바이러스에 의한 침해시도가 1건, 자료훼손 및 유출에 의한 침해가 1건 발생하였다.

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

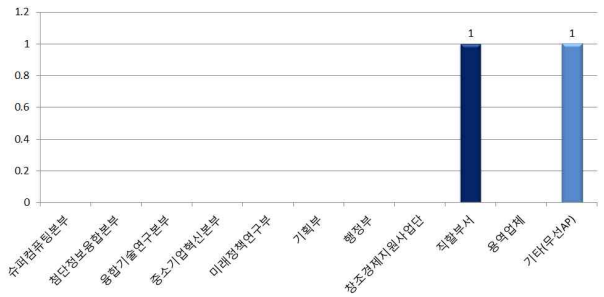
[표 6] 12월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 13]과 같이 리눅스 시스템을 통한 사고가 2건으로 모두 리눅스를 통하여 사고가 발생하였다.



[그림 13] 12월 시스템별(OS) 사고 건수

- 부서별로는 [그림 14]와 같이 직할부서 및 기타(무선AP)가 각각 1건씩 발생하였다.



[그림 14] 12월 부서별 사고 건수

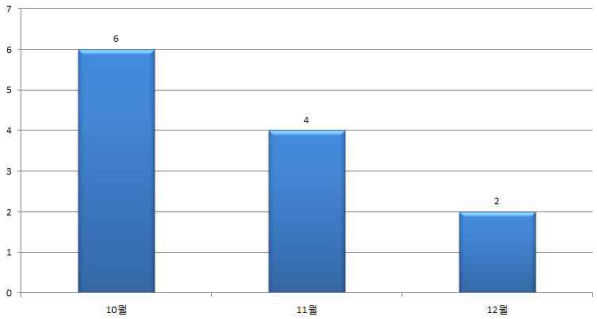
○ 12월 보안 이슈 및 향후 계획

- 한국어 페이지를 제공하는 두 번째 랜섬웨어 라다만트(Radamant)가 발견되었다. 라다만트는 12월 25일 경 한국에서 처음 발견되어 크립토락커(Crypt0Locker) 이후 두 번째로 한국어 페이지를 제공하는 랜섬웨어다. 다른 랜섬웨어들과 마찬가지로 악성코드를 생성하고, 웹 브라우저 및 웹 브라우저 플러그인 취약점을 이용해 악성코드를 유포하는 DBD(Drive-By Download) 방식으로 유포된다. 한국을 공격대상 중 하나로 삼았기 때문에 앞으로 더 자주 등장할 랜섬웨어로 예상되는 만큼 예방에 힘써야 할 것이다.

- DNS 서비스를 위해 주로 사용하는 BIND DNS에 원격에서 서비스 거부를 발생시킬 수 있는 취약점이 발견됐다. 해당 취약점은 잘못된 클래스 속성 데이터를 응답 패킷에서 처리할 때 발생하는 서비스 거부 취약점(CVE-2015-8000)이다. 영향 받는 버전은 BIND 9.0.x버전부터 9.9.8버전까지, BIND 9.10.0버전부터 9.10.3버전까지이지만, 우리 기관은 지난 8월 BIND 버전 업그레이드를 하여 취약점에 영향이 없다.

Ⅳ 종합분석 및 개선방안

○ 2015년 10월부터 12월까지의 침해시도 건수는 [그림 15]와 같이 총 12건으로 10월이 6건으로 가장 많이 발생하였으며, 그 뒤로 11월 4건, 12월 2건으로 꾸준히 감소하고 있다.



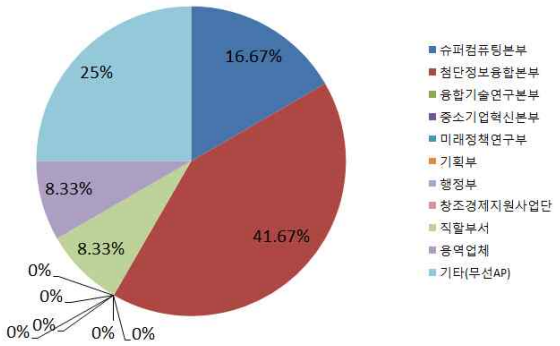
[그림 15] 3분기 월별 침해시도 건수

○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 사고가 11건으로 가장 많은 비율을 차지하였으며, 그 뒤로 자료유출 및 훼손사고가 1건 발생되었다.

	10월	11월	12월
웜 · 바이러스	6	4	1
자료훼손 및 유출	0	0	1
홈페이지 위 · 변조	0	0	0
경유지 악용	0	0	0
서비스 거부	0	0	0
단순침입시도	0	0	0
합계	6	4	2

[표 7] 침해 위협 유형별 분석

○ 부서별로는 [그림 16]과 같이 첨단정보융합본부가 5건(41.67%)으로 가장 많은 비중을 차지하였으며, 그 뒤로 기타(무선AP)가 3건(25%), 슈퍼컴퓨팅본부에서 2건(16.67%), 직할부서와 용역업체에서 각각 1건(8.33%)의 사고가 발생하였다.



[그림 16] 4분기 부서별 사고 건수 비율

• 웜·바이러스에 의한 사고

- 4분기에 발생한 사고 중 91.67%(12건 중 11건)가 웜 · 바이러스에 의한 사고로 가장 많은 부분을 차지하였다. 웜 · 바이러스에 의한 사고가 꾸준히 발생하고 있어 소속 직원들의 주의가 요구된다.

- 따라서, 위 문제를 해결하기 위한 대책으로 업무용 PC의 윈도우 등 OS의 보안업데이트와 백신 소프트웨어 업데이트 등 신규 취약점에 대한 대비가 필요하며 웹사이트 방문 시 의심스러운 프로그램 설치 금지 및 출처가 불분명한 메일, 첨부파일 열람 금지 등 사용자 교육이 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 보안솔루션(포렌식 도구, 이벤트 수집 및 분석 도구 등) 도입 및 사고 조사에 필요한 전문 인력 확보가 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 보안솔루션(포렌식 도구, 이벤트 수집 및 분석 도구 등) 도입 및 사고 조사에 필요한 전문 인력 확보가 요구된다.

• IP 주소 관리 강화

- 4분기에는 부서별 IP주소 현황조사 및 사용자PC이름 현행화를 통해 보안사고 발생시 신속한 사고자 파악이 이루어져 사고조사가 빠르게 이루어 졌다.

- 기존에는 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 정보화혁신실에서는 부서별 IP할당에 따른 관리 미흡으로 증가된 미사용 IP 관리와 보안사고시 사고 PC의 IP확인 지연으로 인한 보안 위험을 최소화 하기 위해 IP현황조사 및 사용자 PC이름 변경을 추진하였다.

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

• **서버 보안**

- 관제현황 보고서에 따르면 4분기 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. 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 3분기 총 14건의 침해시도에 비해 2015년 4분기의 총 침해시도건수는 12건으로 2건의 감소를 보였다. 4분기에는 유해 트래픽이 평균 43.3Gb로 올해 최고치를 보였다. 이와 관련해서 새로운 바이러스와 악성코드들에 의해 발생할 수 있는 침해와 공격시도들을 대비하여 더욱 세심한 주의가 요구된다.

○ 4분기에는 3분기에 이어 Adobe Flash Player 취약점을 이용한 악성코드 유포가 지속 되고 있다. Adobe Flash Player 취약점을 이용한 악성코드를 유포시키는 사례가 올해들어 지속적으로 나타나고 있으므로 보안업데이트에 각별한 주의가 요구된다.

- 향후 직원에 대한 꾸준한 침해사고 교육 및 침해사고 발생 직원에 대한 경고 등을 통하여 경각심을 일깨우며 지속적인 정보보안 모니터링을 통한 전주기적 보안 업무환경을 형성할 수 있도록 해야할 것이다.

[별첨 1] 월별 침해위협 발생 현황

○ 10월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
1	2015-10-06 11:08	정보융합연구실 우제문	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-10-06
2	2015-10-12 17:04	첨단연구망 서비스실 이원혁	웜・ 바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-10-13
3	2015-10-13 10:52	정보서비스실 신수미	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-10-13
4	2015-10-22 09:02	정보서비스실 신수미	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-10-22
5	2015-10-26 10:25	슈퍼컴퓨팅 인프라실 최윤근	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-10-26
6	2015-10-27 23:33	용역업체	정보유출형 악성코드 감염(추정)에 의한 경유지로 접속시도 탐지	2015-10-28

○ 11월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
7	2015-11-02 10:41	NTIS사업실 장도	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-11-02
8	2015-11-12 20:43	원내 무선 AP	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-11-13
9	2015-11-24 09:50	원내 무선 AP	웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보(MAC 주소) 전송시도 탐지	2015-11-24
10	2015-11-26 10:28	NTIS사업실 장도	웜・ 바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-11-26

○ 12월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
11	2015-12-30 22:03	정보시스템운영실 박남규	OpenSSL의 취약점을 이용하여 시스템 정보유출 탐지	2015-12-31
12	2015-12-31 07:45	오탐	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 목적지 IP를 대상으로 스캐닝 행위 탐지	2015-12-31

[별첨 2] 부서별 사고 건수

부서명	10월	11월	12월
슈퍼컴퓨팅본부	2	0	0
첨단정보융합본부	3	2	0
융합기술연구본부	0	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	1	0	0
기타(무선AP)	0	2	1
합계	6	4	2

[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