2017년 KISTI 침해사고 대응 분석 (2/4분기)

2017. 10.

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 등급 분류

○ KISTI 침해사고 형태 및 피해 양상

사고 형태	· 정보시스템에 대한 사이버공격을 통한 정보유출/변조/유실 · 업무PC에 대한 사이버공격을 통한 정보유출/변조/유실 · 내부직원의 개인적인 이득을 위한 고의적인 정보유출/변조/유실

침해사고 발생

피해 양상	· 정보의 유출, 변조 또는 유실로 인한 KISTI 업무 마비 · 정보 관리 소홀로 인한 법적 처벌 · KISTI 대외신인도 하락

○ KISTI 침해사고의 등급 분류

구분	판단기준	비고
심각	◦ 대규모 사이버공격에 의한 정보유출 ◦ 그 외 KISTI 대외 신뢰도에 심각한 피해라고 판단된 경우	사고
주의	◦ 소규모 사이버공격에 의한 정보유출 ◦ 그 외 KISTI 대외 신뢰도에 심각한 피해라고 판단된 경우	사고
관심	◦ 정보 유·노출이 아닌 단순 의심, 문의 ◦ KISTI 대외 신뢰도에 피해 없음	의심

2. KISTI 침해사고 대응 체계

○ KISTI의 침해사고 대응체계는 국가정보원 국가사이버안전센터(NCSC) 및 미래창조과학부 과학기술사이버안전센터(S&T sec), 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

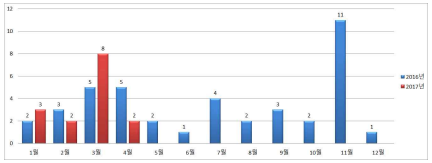
○ 초기대응 : 침입인지 단순한 장애인지를 결정하는 단계로 사고의 완전한 분석이 아닌 사고의 확산을 방지하고 차단하는 조치를 취하며, 추후 정밀조사를 위한 증거자료 수집

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

○ 복구단계 : 악성 프로그램을 제거하고 삭제된 프로그램을 복구하는 등의 작업을 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



[그림 4] 4월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 2]와 같이 웜·바이러스에 의한 침해시도가 2건으로 가장 많았으며, 그 외 다른 유형의 침해 위협은 발생하지 않았다.

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

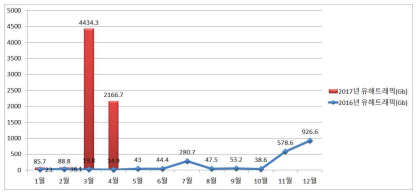
[표 2] 4월 침해 위협 유형별 분석

III 현황 분석

1. 4월 종합 분석

○ 4월 침해사고 분석

- 2017년 4월 유해 트래픽은 [그림 3]과 같이 2,166.7Gb로 전월 대비 2,267.6Gb 감소하였다.



[그림 3] 4월 유해트래픽 추이

- 2017년 4월 침해시도 건수는 [표 1]과 같이 총 2건으로 전월 대비 6건 감소하였다.

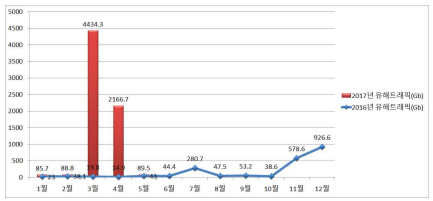
구분	2016년									2017년			
	4월	5월	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월
침해 시도 현황	5	2	1	4	2	3	2	11	1	3	2	8	2

[표 1] 4월 침해 시도 현황

2. 5월 종합 분석

○ 5월 침해사고 분석

- 2017년 5월의 유해 트래픽은 [그림 7]과 같이 89.5Gb로 전월대비 2,077.2Gb 감소하였으며, 3월 및 4월과 달리 다른 달들과 비슷한 수준을 유지하였다.

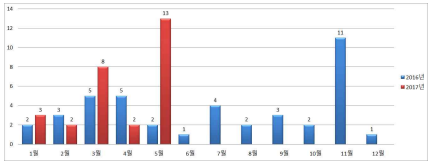


[그림 5] 5월 유해트래픽 추이

- 2017년 5월 침해시도 건수는 [표 3]과 같이 총 13건으로 지난달에 비해 11건 증가하였다.

구분	2016년								2017년				
	5월	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월
침해 시도 현황	2	1	4	2	3	2	11	1	3	2	8	2	13

[표 3] 5월 침해 시도 현황

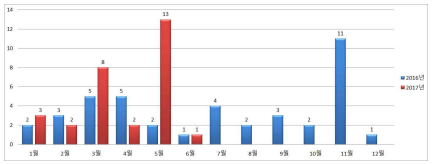


[그림 6] 5월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 4]와 같이 웜·바이러스에 의한 침해시도가 9건, 자료훼손 및 유출에 의한 침해시도가 3건, 경유지 악용에 의한 침해시도가 1건 발생하였다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	9	3	0	1	0	0	13

[표 4] 5월 침해 위협 유형별 분석



[그림 8] 6월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 6]과 같이 웜·바이러스에 의한 침해시도가 1건으로 해당 유형의 침해시도가 지속적으로 발생하는 추이를 보이고 있다.

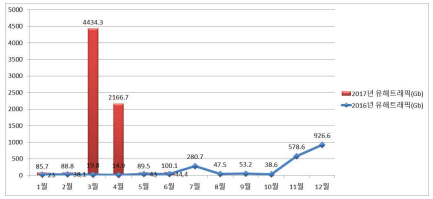
구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	1	0	0	0	0	0	1

[표 6] 6월 침해 위협 유형별 분석

3. 6월 종합 분석

○ 6월 분석

- 2017년 6월 유해 트래픽은 [그림 11]과 같이 100.1Gb로 전월 대비 10.6Gb 증가하였다.



[그림 7] 9월 유해트래픽 추이

- 2017년 6월 침해시도 건수는 [표 15]와 같이 총 1건으로 전월 대비 12건 감소하였다.

구분	2016년							2017년					
	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
침해 시도 현황	1	4	2	3	2	11	1	3	2	8	2	13	1

[표 5] 6월 침해 시도 현황

4. 2분기 원내 침해사고 분석결과

○ 2분기 원내 월별 침해사고 현황

구분	2016년							2017년					
	6월	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월
침해 시도 현황	1	4	2	3	2	11	1	1	0	2	1	1	1

[표 7] 2분기 원내 월별 침해사고 현황

- 2016년 원내 침해사고 위협 현황에 비해 2017년 침해사고의 위협의 빈도는 현저히 줄어들었으며, 이에 대한 원인으로는 노후화된 기존 보안장비의 교체에 따른 안정화로 인한 효과로 파악되고 있다.

○ 2분기 침해 위협 유형별 분석 현황

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

[표 8] 2분기 원내 침해 위협 유형별 분석 현황

○ 2분기 시스템별 침해사고 현황

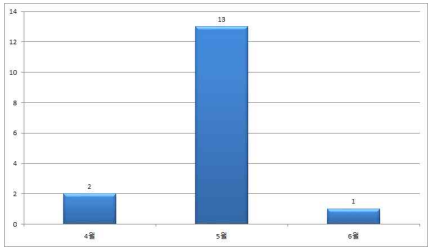
구분	윈도우즈	리눅스	MAC	기타(AP, 공유기)	합계
건수	3	0	0	0	3

[표 9] 2분기 시스템별 침해사고 현황

- 시스템별(OS)로는 윈도우즈 시스템을 통한 사고가 3건 발생하였다.
- 부서별로는 행정부, 전문위원실, 용역업체 에서 각각 1건씩 발생하였다.

Ⅳ 종합분석 및 개선방안

○ 2017년 4월부터 6월까지의 침해시도 건수는 [그림 15]와 같이 총 16건으로 5월이 13건으로 가장 많이 발생하였으며, 그 뒤로 4월이 2건, 6월이 1건으로 발생하였다.



[그림 9] 2분기 월별 침해시도 건수

○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 침해시도가 12건으로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 자료훼손 및 유출에 의한 사고가 3건, 경유지 악용에 의한 사고가 1건 발생되었다.

	4월	5월	6월
웜·바이러스	2	9	1
자료훼손 및 유출	0	3	0
홈페이지 위·변조	0	0	0
경유지 악용	0	1	0
서비스 거부	0	0	0
단순침입시도	0	0	0
합계	2	13	1

[표 10] 침해 위협 유형별 분석

○ 침해사고 대응 향상을 위한 제언

- **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**

  - 부서별 IP할당에 따른 관리 미흡으로 증가된 미사용 IP 관리와 보안사고시 사고 PC의 IP확인 지연으로 인한 보안 위험을 최소화하기 위해 IP현황 조사 및 사용자 PC이름 변경을 추진하고 있으나 사용PC의 포맷 및 신규 입사자에 대한 변경 미흡 등으로 인하여 아직도 IP관리에 대한 허점이

존재하고 있다. 주기적인 홍보 등을 통하여 완벽한 IP 관리가 이루어질 수 있도록 하는 노력이 필요하다.

- **서버 보안**

  - 관제현황 보고서에 따르면 3분기 공격 대상 포트와 스캐닝 대상포트 중 가장 높은 비율을 차지한 포트가 각각 TCP/22 (ssh), TCP/80 (HTTP)으로 원격접속에 대한 침해시도가 많이 탐지 되었다. 따라서 시스템 운영자는 비인가 된 접속에 대한 로그관리와 ssh와 같은 서비스의 포트설정 변경, 원격에서 루트계정 로그인 금지, 패스워드 정책강화와 주기적인 패스워드 변경 등 서버보안을 위한 보안정책 및 웹서버의 디렉토리에 대한 접근권한 관리, 불필요한 에러로그 출력 제거, 불필요한 웹서버 정보출력을 제거하여 웹보안성을 강화하여야 한다.

Ⅴ 결론

○ 2016년 2분기 총 8건의 침해시도에 비해 2017년 2분기의 총 침해시도건수는 16건으로 8건의 증가를 보였다. 2분기에는 유해 트래픽이 평균 785.43Gb로 전년 동기 대비 여전히 높은 수치를 보이고 있으나, 올해 1분기의 1,536.27Gb에 비해서는 대폭 감소하였다. 이와 관련해서 새로운 바이러스와 악성코드들에 의해 발생할 수 있는 침해와 공격시도들을 대비하여 감소 추세를 이어나가는 것이 요구된다.

○ 2분기 정보보안 이슈 및 대응방안

  - 2017년도 2분기 정보보안 주요 이슈로는 국방망 해킹에 따른 '작계 5015' 유출(4월), 워너크라이(WannaCry) 랜섬웨어에 따른 전세계 피해확산(5월), 인터넷 서비스 랜섬웨어 피해(인터넷 나야나)로 인한 공격사례(월)를 들 수 있으며, 정보보안 이슈가 기업 비즈니스에 위협(Risk)을 주는 사례가 지속적으로 발생하고 있는 점이다.

  - 지난 2016년 인터넷 쇼핑몰 APT공격 사례와 유사하게 인터넷 서비스업체에 대한 맞춤형 공격이 발생하였다. 이는 윈도우기반 에레버스(Erebus) 랜섬웨어의 변종으로 리눅스 서버에 작동하는 사례로 다수의 인터넷 서비스가 접속이 중단되는 사태를 야기하였다. 그 결과 인터넷 호스팅업체에서 4억의 현금 및 법인 매각으로 총 13억원을 지불하여 해커와 협상을 하게 되어 사건은 일단락되었으며, 이 사건으로 인하여 다수의 유사 업체에 대한 공격이 감행될 수 있는 가능성을 남겨두었다.

- 해외에서는 표적공격을 통한 메시지 전달형, 파괴적 성향의 악성코드, 제로데이 취약점을 이용한 자력형 공격이 증가하였으며, 주요 사건으로는 2016년 미국 대선과정에서 민주당측에 펼쳐진 해킹 사건을 예로 들 수 있다. 또한 디스크 삭제와 같은 파괴적 성향의 악성코드 공격은 컴퓨터의 마스터 부트 레코드(MBR)을 삭제하는 형태의 악성코드도 등장하였다. 마지막으로 제로데이 취약점이나 악성코드 툴킷 대신 탐지 회피를 목적으로 클라우드 서비스나 툴(Tool)의 형태로 배포되는 자력형 공격이 주로 등장하였다. 해커들의 주된 공격 형태는 기존의 익스플로잇 취약점을 통한 공격보다 랜섬웨어의 확산과 함께 확대되는 이메일을 통한 악성코드 배포가 지속적으로 증가하고 있으며, 피싱(Phishing) 메일 형태나 특정 타깃을 대상으로 하는 스피어피싱 공격이 증가하고 있다.

- 침해사고에 대한 원내 연구자의 대응은 아래와 같이 수행해야 한다.

1. 취약성 공격 차단 프로그램 사용

- 이번 랜섬웨어의 확산 방법과 같이 웹사이트를 통해 사용자의 취약성을 이용한 악성코드 배포 시에는 취약성을 이용한 공격을 사전에 차단하는 프로그램을 이용하여 안전한 상태를 유지할 수 있다.

2. 스팸 메일 첨부파일 실행 금지

- 출처가 불분명한 메일 삭제, 발신인이 확인되지 않으면 클릭 금지, 지인의 메일도 한 번 더 확인해야 한다.

3. 운영체제 및 각종 응용프로그램 보완 업데이트 진행

- MS OS 업데이트를 포함하여 IE, JAVA, Flash Player, Microsoft Silverlight, XMLDOM, Office, 한글 등 대표적인 어플리케이션은 항상 최신 버전을 유지한다.

4. 백신 프로그램 최신 업데이트 유지

- 백신 프로그램을 필수적으로 설치하고 최신 버전을 유지한다.

5. 중요 문서 및 파일 백업 필수

- 중요한 파일에 대해서 해당 시스템 이외의 별도 저장 공간에 백업하고, 해당 시스템에 저장 시에는 압축 암호화해 별도 보관, 혹시 감염되더라도 피해를 최소화해야 한다.

6. 개발서버 보안조치

- 개발에 사용하던 웹서버 및 더 이상 사용하지 않아 관리되지 않는 웹사이트는 서버중지 및 도메인 삭제 등의 조치를 통해 악성코드 유포지 및 해킹의 경유지로 사용되지 않도록 하는 조치가 요구된다. 또한 사용 중인 웹사이트의 경우, 보안업데이트, 보안정책 강화, 소스코드 취약점 보완 등을 통해 보안 취약점을 해결하여야 한다.

[별첨 1] 2분기 원내 침해위협 발생 현황

○ 원내 침해위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
1	2017-04-17	전문위원실	원내 사용자 멀웨어 감염(Rookie)	2017-04-18
2	2017-05-09	총무시설실 (기계실)	원내 사용자 랜섬웨어 감염(Cerber)	2017-05-16
3	2017-06-17	총무시설실 (시설경비)	원내 사용자 웜바이러스 감염	2017-06-19

○ 침해위협 탐지 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
1	2017-04-11	응용기술개발실	원내 시스템 웜바이러스 피해의심	2017-04-12
2	2017-05-06	정보시스템 운영실	웹쉘 업로드 시도 탐지	2017-05-10
3	2017-05-15	첨단연구망 서비스실	멀웨어로 인한 자료훼손 및 유출	2017-05-16
4	2017-05-16	정보시스템 운영실	멀웨어로 인한 자료훼손 및 유출	2017-05-16
5	2017-05-16	응용기술개발실	웜바이러스 피해(서버)	2017-05-17
6	2017-05-26	정보보호실	웜 바이러스 피해(PC)	2017-05-28
7	2017-05-29	노동조합	웜 바이러스 피해(PC)	2017-05-29

[별첨 2] 부서별 사고 건수

부서명	4월	5월	6월
슈퍼컴퓨팅본부	0	0	0
첨단정보융합본부	0	0	0
융합기술연구본부	0	0	0
중소기업혁신본부	1	0	0
미래정책연구부	0	0	0
기획부	0	0	0
행정부	0	0	0
창조경제지원사업단	0	0	0
직할부서	0	0	0
용역업체	0	1	1
기타(무선AP)	0	0	0
합계	1	1	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 이에 대한 대비 필요 3. 네트워크 이상트래픽 과다 탐지 또는 부분 장애 등 사이버위협 징후 탐지활동 강화 필요