Malware 동향 분석과 향후 예측
- 국방기관 및 방산분야를 중심으로 -

최준성* · 국광호**

요 약

본 연구는 이메일을 활용한 멀웨어 공격 중 국내 국방 분야 및 방산 분야에 대한 공격 동향을 분석하고, 새로운 공격 유형을 예측하였다. 국방 분야와 방산업계 대상으로 발생하는 멀웨어 배포는 주로 사회공학적으로 수집된 개인정보를 바탕으로, 특정 기능이 포함된 악성코드가 포함된 문서 파일로 배포한다. 배포된 멀웨어는 피해자 사용 단말기의 정보를 습득하려는 의도로 사용된다. 본 연구는 실제 사례들에 대한 분석을 통해 이메일을 활용한 멀웨어 배포 동향을 분석하여, 향후 시도될 것으로 예상되는 멀웨어 배포 유형을 예측했다.

The Analysis of the Malware Trend and the Prediction on the Defense Service and Industry

Junesung Choi* · Kwangho Kook**

ABSTRACT

In this study, we analysis the distributing malware using email on the korean defense service and defense industry as the social engineering attack. E-mail attack distributes the document files with the malware. Using the malware, attacker get the Information of the targeted people and devices. we proposed expected new types of attacks by analysis and transformation. And, expect the new email attack agendas which will be tried..

Key words : Malware, Social Engineering Attack, Defense Service, Defense Industry

접수일(2012년 8월 16일), 수정일(1차:2012년 9월 13일, 2차:9월19일), 게재확정일(2012년 9월 21일)

★ 이 연구는 서울과학기술대학교 교내 학술연구비 지원으로 수행되었습니다.

* 서울과학기술대학교 IT정책전문대학원 산업정보시스템공학 전공

** 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 (교신저자)

1. 서 론

정보 시스템의 장애 유발, 불법 정보수집, 시스템 자원에 대한 불법접속 등을 위한 멀웨어에 의한 피해는 급속도로 증가하고 있는 추세이다. 아울러 국내 국방 분야와 방위산업계에서도 이와 같은 피해가 자주 발생하고 있다. 본 연구는 국내 국방분야와 방위산업계 종사자들을 대상으로 발생하고 있는 이메일을 통한 멀웨어 배포하는 방법들에 대해 연구한다. 이를 통해, 앞으로 예견되는 새로운 공격 유형을 예측한다. 결과적으로 향후 발생할 수 있는 국내 국방 분야 및 방위산업계에 대한 멀웨어의 확산과 배포로 피해가 발생하는 것을 방지하고자 한다. 본 연구에서는 최근 3년간 국내 국방 분야와 방위산업계에 시도된 대한 이메일 활용 멀웨어 공격 동향 양상을 수집하고 분석했다. 본 연구의 범위는 멀웨어를 배포하기 위한 사회공학적 공격 방법, 국내 국방분야와 방위산업계에서의 멀웨어 배포 상황과 대응 현황, 향후 발생 할 수 있는 새로운 멀웨어 배포 이메일의 예측과 새로운배포 유형에 대한 관리적 대응 방안을 연구하는 것이다. 연구에 활용된 방법은 문헌 조사를 통하여서 다양한 사회공학적 공격 방법을 연구하였고, 실제 발생한 멀웨어 배포 메일의 시료 수집과 조사를 통해 국내 국방분야와 방위산업계에서 발생한 사례들을 분석하였다. 이를 통해 멀웨어 배포의 전형적인 특성을 도출하여, 향후 예상되는 멀웨어 배포메일을 예측했다. 또한 기술적 변화의 예측으로 새로운 공격 유형도 예측했다. 국방분야와 방위산업분야는 국방 운영과 계획, 무기체계의 연구개발등으로 인하여, 국가적으로 중요한 기밀을 많이 포함하고 있는 영역이다. 단적인 예를 들자면 영미권의 전차와 구소련권이 전차의 전차전을 예로 들 수 있다. 구소련의 전차들은 전차운전석과 1열로 승무원이 탑승하는 구조로 인해, 운전석에 피폭이 발생하는 경우 전차 전체의 승무원이 사망하는 구조를 가지고 있었다. 이와 같은 무기체계의 구조적 취약점이나 운용상의 한계나 취약점이 전투 후 노획된 전차의 잔해를 통하여 확인되는 것과, 전투전 도면의 유출 등을 통해 미리 확인되는 경우 전투의 방법과 양상이 크게 달라질 수 있는 사안이다. 현재 각국은 다양한 무기체계들을 운용하며 적국에 공개되지 않은 새로운 구조의 무기체계들을 개발하고 있다. 또한 각 군은 적 무기체계와 무기체계 운용교리를 분석하여, 이에 대한 대응 방법들을 모색하는 것이 보편적인 추세이다. 이로 인해 국내 국방관련기관과 방위산업계에는 이메일을 통한 멀웨어 배포시도가 일어나고 있다. 그러나 대부분의 경우에는 해당 멀웨어 배포가 멀웨어 배포인지 인식하지 못하고 있다. 이로 인해 트로이목마 기능 등을 수행하는 멀웨어들이 중단되지 않고, 계속 배포되는 문제가 있다. 이번 연구는 실제 발생된 사례를 공유하여 유사한 사례가 발생하지 않도록 예방하는 것이 가장 중요한 목적이다. 본 연구의 기대효과는 기존에 발생된 멀웨어에 대한 유형화를 통해 멀웨어 배포를 예방할 수 있다. 또한 향후 예측할 수 있는 새로운 멀웨어 공격 유형을 미리 전파하여 피해를 예방할 수 있다.

2. 관련 연구

국방 및 방산분야는 군사기밀과 군사보안과 관련되어 있다.이로 인해 지속적인 사이버테러 공격 대상이 되고 있다.[1] 국방분야 공공기관인 중앙행정기관인 국방부, 외청인 방위사업청과 각급 부대들의 경우에는 업무망이 상용인터넷망과는 완전히 구분된 별도의 독자 업무망(국방인트라넷)으로 구성되어 있다. 상용인터넷과 독립된 업무망에 대한 직접적인 사이버 테러는 현재 매우 제한된 상태이다. 다만, 최근 지능화된 지속적 위협들의 경우 망분리가 되어 있는 공격 대상들에 대한 취약점을 찾아 공격하는 방법들이 개발되고 있는 추세이다.[1,9] 이 경우 발생할 수 있는 문제로는 인원보안의 문제인 개인이 내부 업무자료를 외부로 임의 반출하여 개인PC에 자료를 보관하는 경우의 발생이다. 이 경우 평소 개인의 PC에 부주으로 설치된 멀웨어들을 통한 문제가 발생할 수 있다. 방산업계의 경우에는 국방부와 방위사업청의 정부출연연구기관으로써 공공기관인 국방과학연구소, 국방연구원, 국방기술품질원의 경우에는 업무망과 상용인터넷이 완전하게 분리 되어 있다. 반면, 방산업체들은 비용관계 등의 문제 때문에 별개의 업무망분리와 SBC(Sever Based Computing)등의 보안성 향상 대책들을 사용

하고 있지 않은 경우가 대부분이다. 일반 상용인터넷 망을 사용하는 경우에는 사회공학적인 공격방법으로 배포되고 있는 멀웨어의 설치가 매우 용이하다. 그리고 내부 보유 정보의 보호가 쉽지 않은 문제가 있다.

2.1 사회공학적 공격

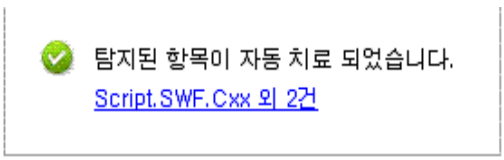
국방 및 방산업계에 대한 멀웨어 이메일 배포와 관련된 정보수집과 공격의 일련의 과정들은 사회공학적 공격 방법으로 분류할 수 있다. 이번 연구에서 의미하는 사회공학이란 사회적이고 심리적인 요인을 이용하여 사람을 조종하여 소기의 목적을 달성하고자 하는 일련의 행동들이나 방법의 활용의 총체를 의미한다. 사회공학적 공격이란 시스템의 취약성이 아닌 인간과 인간관계의 취약성을 공격하여 원하는 정보를 얻거나 목적을 달성하는 사이버테러 혹은 해킹 공격 기법을 통칭을 의미한다.[1,5-10] 전설적인 해커이자 현재는 보안컨설팅 전문가로 활동 중인 케빈 미트닉의 경우에는 자신의 저서들에서 해킹과정에서 사회공학적 공격을 많이 활용했으며 취약점 분석과정에서도 사회공학적 공격을 현재도 많이 활용하고 있음을 밝히고 있다.[7-9] 사회공학적 공격은 그 정의가 내려지기 오래 전부터 해킹이 시작된 이래 지속적으로 활용되었다. 그러나 학문적으로 정리가 시도된 것은 얼마 되지 않았다. 최근의 사회공학적 공격을 체계화하려는 시도에는 크리스토퍼 헤드네기와 죠니 롱 등의 시도들이 있었다. 이들은 각각 자신들의 저서에서 보안의 가장 취약한 부분은 기계적인 보안 요소가 아니라 사람이라고 정의하고 있다. 그리고 사회공학적 공격에 활용되는 기본적인 심리이론, 정보수집방법, 구체적인 질문, 위장, 속임수, 조작, 설득방법, 그리고 다양한 도구와 장비들의 사용법들을 정리하고 있다.[5,6] 최근에는 SNS와 각종 정보기기 활용의 증가하고 있다. 이를 통해 사회공학적 공격을 위한 정보 획득이 용이해 지고 있으며, 다양한 사회공학적 공격들이 활발하게 행해지고 있다. 생활 속에서 가장 흔하게 접하는 사회공학적 공격에는 피해자의 금품을 탈취하기 위해 시도되고 있는 전화와 이메일 등을 활용한 피싱이 있다. 이와 유사한 공격 유형들에는 공격대상범위에 따라 파밍, 웨일링 등이 있다.

군과 관련된 사회공학적 공격의 경우, 주로 이메일의 제목으로 사용되는 것에는 '동기생 자료', '동기 주소록 송부' 등이 있다. 이들 공격에서 사용된 메일 송신자의 아이디로는 'navy77', '양병은', '정수park' 등이 있다.[1-4] 군과 관련된 분야이면서, 사회공학적 공격에 노출되어 있는 방산업계 중 산업체에 대한 사회공학적 공격에 대한 연구는 거의 이루어지고 있지 않은 실정이다. 현재 국내방산업계 사회공학적 공격동향과 대응방향에 대하여 정도의 분석과 연구가 시도된 정도이다. 해당하는 기존 연구결과[1]에 의하면, 국내 방산업계는 수주영업성격을 띄는 관계로 발주기관 사칭 시, 방산업계 종사자의 사회공학적 공격에 노출될 가능성이 높다. 그리고 사회공학적 공격 정보 획득수단으로 각종 학술정보와 SNS 활용이 주요 수단이 되고 있다. 주요 공격수단으로는 이메일을 활용한 멀웨어의 배포가 주를 이룬다. 향후에는 USB저장매체 배포나 고객기관 사칭이 주를 이룰 것으로 예상하고 있다.[1] 이번 연구에서는 현재 공격 방식의 주종을 이루고 있는 사회공학적 이메일로 배포된 멀웨어에 대해 실제 공격 사례를 실증적으로 분석하고, 대응 방안과 향후 공격유형들을 예상한다.

2.2 멀웨어 (Malware)

멀웨어(악성프로그램, 악성코드 : Malware, Malicious Software, Malicious code)는 시스템의 운영에 장애를 유발하거나 정보수집, 시스템 자원에 대해 허용받지 않은 접근을 수행하거나 기타 침해행위를 목적으로 작성된 프로그램을 의미한다. 악성코드라는 명칭을 사용하기도 한다. 기존에는 컴퓨터 바이러스(virus)라는 표현이 주종을 이루었으나, 웜(worm), 트로이목마(Trojan Horse), 루트킷(rootkits), 백도어(back door), 스파이웨어(spyware), 키로거(key-logger, key stroke logger) 등의 다양한 공격 방식들을 포괄하는 의미로 현재는 멀웨어(Malware,)라는 표현을 주로 사용하고 있다.[2-4] 다양한 멀웨어(Malware,)중에서 개인접속정보탈취나 금융정보 탈취에는 '키로거'가 주로 사용된다. 운영체제 내부 프로그램이나 커널의 치환을 통해, 안정적인 백도어와 키로깅을 확보하는 것에는 '루트킷'이 활용된다. 트로이 목마는 그 명칭 만큼이나, 매우 고전적인 방식으로 정상적인 SW나 문서 화일을 위장하고 피해자의 컴퓨터에 기생한다. 많은 멀

웨어는 기본적으로 트로이 목마의 성격도 가지고 있다. 분석 결과 국방 분야 및 방산업계에 대한 공격에서 활용되는 멀웨어는 백도어와 트로이목마, 루트킷, 스파이웨어의 속성을 가지고 있다. 멀웨어는 잦은 변형이 이루어지는 있다. 시료 분석 결과 1달에 1~2번씩 변형 공격이 발생하는 국내 국방 분야 및 방산업계 대상 공격에는 대부분 매번 새로운 유형의 멀웨어가 배포되고 있다. 새로운 악성코드 초기 발견 시에는 백신이 감지를 못하고, 1~2달 지난 악성코드만을 감지하는 문제가 있다. 그래서 대부분의 경우에는 멀웨어 배포 공격을 인지하지 못하는 경우가 발생한다. 현재 많은 경우, 멀웨어 메일이 배포와 피해 발생이 발생하고 나서야 해당 메일을 열어보지 말라는 주의보가 발령되고 있다. 그러므로 국방분야와 방산업계에서는 예방이 가장 중요한 요소가 되고 있다. (그림 1)에는 실제 8월 초에 시도된 공격중 탐지된 악성코드의 치료화면 나타나 있다. 해당 공격의 경우에는 지난 5월 활용된 공격이 재활용되어 있어 감지가 되었다. 그러나 개별 추가 분석 결과 내부에 추가적인 악성코드가 있음에도 백신에서는 감지가 되지 않았다. 그러므로 치료가 된 것으로 표시되는 사항도 안심할 수가 없다. 백신의 종류에 따라서도 탐지되는 정도가 차이가 큰 것도 문제이다. 따라서 의심되는 메일에 대해서는 첨부 화일을 열지 않는 것이 최선의 예방이 된다. 이번연구에서는 이러한 예방 차원에서 기존 공격을 분석하여, 향후 발생될 공격 메일을 예측하여 제시한다.



(그림 1) 최근 이메일 공격(8월) 악성코드

2.3 공격대상의 속성

국내 국방 분야와 방위산업 분야의 속성을 알아본다. 국방기관과 방위산업체에 대한 보안성 확보 요구는 아무리 강조해도 부족함이 없다. 국방기관과 방위산업체는 국방부직속 보안부대인 국군기무사령부의 통제를 받게 되어 있어, 국군기무사령부 주관의 정기 보안감사를 수검하도록 되어 있다. 방산업체의 경우에는 사업수주를 위한 제안서의 평가에서 보안감사 성적을 반영하게 되어 있다. 국방기관의 경우, 여러 분야에서 지속적인 해킹과 포섭 시도가 있어왔던 것으로 알려져 있다. 한편으로 최근 국내방산역량의 증대에 따라, 방산업계에 대한 해킹 시도도 지속적으로 발생하고 있다. 대기업 집단에 소속된 방산업체의 경우에는 보안부서의 별도 운영과 및 전산보안체계의 확보 등으로 문제 발생이 어느 정도 방지되는 경향을 보이고 있는 것으로 알려져 있다. 반면 중소방산업체의 경우 별도의 관리부서 확보가 어렵다. 그리고 일반 인터넷만을 사용하고 있다. 이런 환경의 특성 상 사회공학적 공격이나 해킹 시도에 매우 취약한 상황이다. 현재 국방기관과 방산업체에이메일을 활용한 멀웨어를 배포하는 공격이 주기적으로 발생하고 있다. 공격에 활용된 메일의 특성을 보면, 공격자는 단순하게 좀비PC를 확보하거나 사용자 정보만을 얻고자 하는 일반 해커가 아닌 국방 분야에 대한 특정 목표를 수행하고 있는 것으로 추정된다.

3. 이메일 활용 공격 동향

본 연구는 국내 국방기관과 방산업계에 시도되고 있는 이메일 활용 멀웨어 배포의 사회공학적 공격 시도들 중에 3년간의 실증사례를 분석한다. 향후 1년간 예측되는 유형을 사전 예측하고 그 대응 방안을 여러 가지 측면에서 제시한다. 연구 자료의 수집은 국방기관 및 국내방산업계 종사자의 인터넷 이메일에 수신된 이메일과 멀웨어를 분석하였다. 여기서 공격 메일과 수신처의 수집은 연구자가 직접 공격대상자로서 수신한 메일에 나타난 수신처와 공격 내용을 주로 활용한다. 이를 바탕으로 기관 및 기업에 수신된 내용을 역추적하였다. 이를 통해 연구자가 받지 못한 공격들을 타인들이 받은 적 있는지도 확인하였다. 국내 국방기관과 방산업계를 대상으로 시도되고 있는 이메일을 활용한 사회공학적 공격에서의 멀웨어 배포 양상을 실사례들을 분석한 결과, 국내 방산업계 대상 공격의 의도는 불특정 다수에게 배포되어 단순한 좀비PC를

형성하는 것을 목표로 하고 있지 않다. 공격 대상자들의 메일 수신처는 국방특화연구센터가 설치되어 있는 대학 등의 연구기관과 방산업체, 정부출연연구기관, 방산업체의 협력업체, 국방SI 업체들로 그 메일 도메인이 한정되어 있다. 공격대상자들의 이메일과 이메일 도메인은 직접 공개할 수 없다. 여기서 다룬 내용 자체가 다시 공격 자료 수집에 활용 될 수 있기 때문이다. 방산업계에 대한 공격 의도는 특정 분야 종사자에 대한 목표대상에 대한 맞춤형의 의도적 공격으로 추정된다. 공격대상자의 PC에는 트로이목마, 백도어, 루트킷 등이 설치된다. 개별 설치 파일들은 외국의 특정 IP로 정보전송을 시도하는 구조이다. 이는, 공격 대상이 보유한 정보를 유출하려는 의도를 가지고 있음을 알 수 있다.

3.1 이메일 공격 사례 실증 분석

3.1.1 공격용 이메일 특성 분석

타 분야의 사례로써, 국내 보안업계의 경우에는 해당 업체에 지원하는 이력서를 빙자한 이메일 공격이 시도된 바 있다. 최근 6월의 경우 일반 공공기관에 대해서 해당 공공기관 공보실과 문화원이라는 제3의 기관을 사칭하여 동향정보를 배포하는 것처럼 멀웨어를 배포하고 있는 사례가 나타나고 있다. 반면에 국내 국방기관과 방산업계에 대해서는 이와는 전혀 다른 내용으로 공격이 이루어지고 있다. 그러므로 국방기관과 방산업계에 대한 공격들이 일반개인이나 타 공공기관에 대해 이루어지는 공격과는 다른 의도를 가지고 있거나 공격자가 다름을 알 수 있다. 멀웨어 배포를 위한 이메일은 주로 사회공학적 공격 요소를 가지고 있다. 각각의 이메일들은 피해자가 이메일의 첨부화일을 열어 보도록 유도 하고 있다. 이들이 주로 활용되는 이메일의 내용들은 최근 국방부, 방위사업청, 국방과학연구소, 국방기술품질원, 국방연구원의 공식 홈페이지에 공지되고 있는 공지사항 또는 주요 국방이슈들을 제목으로 삼고 있다. 해당 사항을 안내하거나 분석했다는 문서화일들이 멀웨어가 포함된 상태로 첨부 화일로 제공하고 있다. 각각의 공격 메일에 첨부된 해당 문서 화일들은 해당 문서 화일 포맷의 취약점을 활용하고 있다. 공격대상자가 첨부된 해당 멀웨어 문서화일을 열람하는 경우 자동으로 PC 등기 멀웨어에 감염되게 하는 단순하고 대표적인 유형이 사용되고 있다. 기존 타 공공기관에 대해서는 한글화일 공격이 주종을 이루고 있다. 반면, 국방기관 및 방산업계에 대해서는 현재까지 PDF 화일을 활용한 공격만이 공통적으로 활용되고 있다. 최근 3년간 사용된 공격 이메일들이 다루고 있는 안건을 정리하면, ‘국방융합기술 0000’,‘방산물자 및 방위산업체 규정/훈령 개정발령’, ‘0000 과제공모’, ‘0000 자료 제공 요청’, ‘00000 위원 명단’,‘00000 관련 명단’, ‘00000 사업 관련 소식’, ‘00000 사업 정보’, ‘00000 사업 현황’. ‘0000 사업 관련 참고자료’ 등의 방위산업 업무 관련 제목 군이 1가지 유형을 나타내고 있다.

한편, ‘0000 정책토론회’, ‘0000년 통일정책토론회 ’, ‘0000 대북 전략’, ‘0000 회담 결과’,‘0000 지시 사항’ 등의 통일 또는 군사 문제 관련 이슈와 관련된 제목군이 제2의 유형이 되고 있다. 기존 메일들의 분석결과에서 0000으로 대체된 내용은 유사내용이 계속 반복된 것을 의미한다. 향후에도 이런 2가지 유형의 경향성은 지속될 것이다. 이런 종류의 메일 제목들은 근거 없이 선정되는 것이 아니라, 최근 1~2달 이내 공공기관들의 공지나 보도 등에 나온 내용과 연계되어, 시의성을 가지고 활용되고 있다. 제1유형의 경우에는 1달 정도의 지연을 갖고 있다. 공지 및 요청 후 반응이 미비하여 추가 조사한다는 빌미나 마감시점과 맞물려 사회공학적 상승효과를 갖는다. 반면, 제2유형의 경우에는 뉴스 등에서 나온 후 1~2주 안에 배포되고 있다. 이런 공격 성향은 사회공학적 공격 역량을 가진 자의 의도적인 공격임이 드러나는 부분이다. 이와 연계되는 최근 예를 든다. 본 연구의 초고 제출 후 추가적으로 확인된 사항으로, 최신 공격 사례인 2012년 8월의 이메일 공격에서는 “공문 13년착수핵심SW개발사업과제소요공모계획안내.pdf”제목의 이메일을 발송하고 있다. 해당 공격은 기존의 대표적인 유형 중의 1가지인‘0000 과제공모’과 같은 내용에 구체적인 년도 등이 추가되어 있다. 해당 메일에 악성코드 포함 파일을 첨부하여, ‘학회’를 사칭하여, ‘cey3545@hanmail.net’라는 계정에서 메일이 발송하였다. 이 사례는 최근 6월 29일, 방위사업청이 2013년도 착수대상 핵심SW 개발사업과제소요공모계획을 방위사업청 등 국방관련기관에 일제히 공지하였음을 활용하여 8월 9일에 공격을 시

도한 내용이다. 1달 정도의 지연이 발생하고 있으며, 마감이 2~3주 남은 시점에 환기 전환을 하는 것으로 보이고 있다. 이 공격에서 유념할 점은 공격자가 학회를 사칭하고 있는 것이다. 이런 현상은 이런 종류의 공지 후에 공공기관들이 관련된 학회, 협회 등을 통하여 재공지하는 업무 협조요청 관습을 하는 것을 어느 정도 파악하고 있다는 의미이다. 해당 공격은 앞서 언급된 바와 같이 1달 이상의 기간 격차를 가지고 8월31일 마감인 공모에 대하여 1달 뒤 상기시키는 용도로 발송된 것으로 보일 수 있다. 이런 방법은 공격대상자에 대한 사회공학적 공격 효과가 있다. 이런 종류의 이메일이 기업의 간부에게 발송되는 경우에는 실무자에게 해당사항 진행하는지 확인하는 단계에서 재배포되는 것도 가능하다. 이런 공격유형은 상당히 효과적이며 치밀한 의도를 가지고 있음을 알 수 있다. 실제 위 공격의 경우 배포과정에서 최초 열람자가 백신에서 악성코드 포함 경고를 받았음에도 부서원에 재배포하여 해당 부서원이 모두 악성코드 있는 이메일을 열람하게 한 경우이다. 이와 같은 문제로 인해 향후 예상 유형에 대해서는 경각심이 필요하다. 이번 연구는 이와 같은 예방을 주목적으로 한다.

3.1.2 이메일 송신자 특성 분석

국방기관 및 방산업계에 대한 공격메일들에서 확인되는 제1유형의 메일 송신자는 주로 공공기관의 연구원, 공무원, 현역군인, 공공기관 직원을 직간접적으로 사칭하고 있다. 제2유형의 국방관련기관과 방산업체 직원들이 업무와 관련하여 가입하여 활동하는 군사관련 학회나 컨퍼런스 사무국 또는 직원을 사칭하고 있다. 여기서 각각의 유형에서 사칭되는 기관에는 국방부, 방위사업청, 국방SW산학연협회, 익명의 '협회'가 주종을 이루고 있다. 향후에도 이런 경향은 지속될 것이다. 방산업계를 대상으로 사회공학적 공격을 하기 위한 이메일 공격에서 주로 활용되는 이메일 계정으로 국내 포털사이트인 다음의 메일 서비스인 hanmail.net과 동일 서비스인 daum.net 계정들만이 사용되고 있다. 특정 도메인의 메일 서비스만 공격용 메일로 사용되고 있으므로, 현재까지는 타분야에 비하여 상대적으로 예방이 쉬운편이라고 할 수 있다. 다음의 메일서비스는 국내 무료 이메일 계정생성 사이트로 가장 오래되었고, 사용자 또한 많다. 공격자들이 다음을 가장 많이 사용하는 이유는 휴면계정 취득이나, 가입이 용이하기 때문인 것으로 추정된다. 다른 이유는 외국의 이메일을 활용하는 경우 스팸으로 걸러지기 쉽기 때문이다. 다음을 사용하는 또 다른 이유로는 공격용 정보 습득을 시도 할 때에 다음의 카페를 많이 사용하는 것도 이유일 것으로 추정된다. 최근 활용되었거나 자주 활용되는 공격자 이메일 계정에는 bultj@hanmail.net, kma0000@hanmail.net 등이 있다. 여기서 영문 약어인 kma는 Korea Military Academy를 의미한다. 한글번역으로는 '육군사관학교'를 나타내는 의미로 사용되고 있다. 그러므로 kma를 사용하는 것은 주로 육군사관학교 출신자를 사칭하는 의도가 뚜렷하다. 이는 국내 국방기관, 방산업체나, 방산관련 기관에는 육군사관학교 출신이 많이 있다는 사실을 공격자가 이를 이미 파악하고 있다는 의미이다. 실제로 육사출신자 중 상당수의 인원이 kma라는 영문약자에, 0000에는 2자리년도+2자리기수, 4자리수년도, 생일, 전화번호, 6자리수의 생년월일 등을 조합하여 이메일 계정으로 사용하고 있다. 공격대상자에 대한 메일 정보는 육군사관학교 동기회 카페나 각급 부대 카페 등의 가입을 통해, 공격용의 메일 정보를 획득하고 있는 것으로 추정된다. 기존에는 육사 출신 장교 까페에 대한 사회공학적 공격들에만 이런 계정이 사용되었다. 그러나 현재에는 국방기관 및 방산업계에 대한 공격에도 활용되고 있다. 이는 가장 흔하게 발견되는 공격자의 사칭수단으로 현역 군인을 사칭하는 의도로 추정된다. 일반 공공기관 공격의 경우에는 국방관련 공격에 비해, 한글의 사용이 미숙하고 불필요한 말이 많은 경향을 보인다. 그러나 국방 관련 공격에서는 짧고 간결한 지시형 말투가 사용되고 있다. 이는 송신자가 상급자인 인상을 주려는 의도가 있음을 알 수 있다. 이런 현상은 현재의 공격들이 단순하거나 우연한 것이 아님을 알려주는 증적 중의 하나이다.

3.1.3 공격대상 수신자 정보 획득 수단

기존 연구[1]에 따르면 가장 간단한 정보취득 수단은 학술대회 및 학회 등에서의 정보 절취이다. 그리고, SNS 정보수집과 포털 사이트, 정보사이트의 인명사전, 세계인명사전 등의 검색도 좋은 정보획득 수단이다.[1]

페이스북, 포탈사이트의 카페, 트위터, 싸이월드 등의 각종 SNS들은 매우 용이한 정보획득 수단이 된다. 이런 사이트들에서 간단한 검색만으로 특정부대출신과 군 동기 등에 대한 많은 정보가 노출되고 있음이 확인된다. 대량 정보를 수집하기 위한 가장 좋은 방법은 기술적 해킹이다. 목표가 되는 정보수집 웹사이트의 계정정보나 등록정보를 취득하는 등의 다양한 수단이 활용된다. 그러나, 기술적 해킹의 성공은 지속적으로 어려워지고 있어 위에 언급된 바와 같은 간접적인 자료수집이 주종을 향후에도 주요 수단이 될 것으로 추정된다. 전문적인 사회공학 툴에 의한 방법을 활용하거나 사회연결망 분석 툴들을 복합적으로 활용하는 경우에는 수집 대상 관리, 정보수집, 정보융합과 가공이 가능하다. 특정 화일을 활용하여 특정행위를 구현하는 악성코드의 구현하거나 공격용 타이틀을 설정하는 것도 가능하다.[4,5,10] 이들 툴을 활용한 구체적인 수집 절차는 본 연구의 범위를 넘게 되므로 이를 다루지는 않는다.

3.1.4 공격대상 수신자 특성 분석

이번 연구는 09년 1월부터 12년 8월까지의 국방 및 방산분야 분야 공격 메일을 수집하여 분석했다. 공격 메일 수신자 집단은 국내 국방기관, 국내방산업체, 국내방산관련 연구수행 대학, 특화연구센터 개설대학, 국방SI업체 등의 이메일 도메인들이 노출되고 있다. 매번의 공격메일에는 수신자 17명, 참고 33명으로 메일을 50명 단위로 발송하고 있다. 이런 수신자 특성은 hanmail.net의 이메일 발송 인원 제한 특성 때문으로 공격자는 수차례에 걸쳐 나누어 공격을 하고 있음을 나타내고 있다. 본 연구에서 분석 대상이 된 이메일은 총 40건이다. 40건에 대한 각각의 공격대상자 50명에 대한 공격대상자는 총 2000명이다. 그러나 각각의 모든 이메일에 사용된 메일계정 중복여부를 대조한 결과 본 연구에서 추적가능한 공격대상자는 348명으로 감소되었다. 본 연구에서는 348명에 대해 개별적으로 메일을 보내, 멀웨어 배포 공격이 있었음을 설명하였다. 추적대상자 348명 중 회신과 협조를 허락한 20명에 대해서는 추가적인 인터뷰와 이메일 증적 수집을 실시했다. 추가 이메일 조사결과 연구자가 당초 수집한 이메일 외에 추가 이메일은 발견되지 않았다. 응답자들에게서 받은 공격 메일의 경우, 연구자와 같은 메일링 리스트 같은 것이 확인되었다. 회신자를 기준으로 대조했을 때에는 추가적인 추적대상자는 확인할 수 없었다. 회신 인원 20명 중 8명은 최근까지 국방관련 공공기관에서 근무한 경험이 있는 인원들로, 메일송신자는 기존 국방관련 공공기관 소속인원으로 간주하고 공격을 시도하고 있는 것으로 추정된다. 분석 결과, 국방기관 공격과 방산업계 공격의 내용이 시기적 공격 유형이 동일하였다. 매번의 공격 메일 대상자 50명의 목록은 일치하는 경우와, 중복되는 경우, 전혀 다른 경우의 3가지 경우로 확인되었다. 이것은 공격용 수신자 메일링 리스트의 습득지가 다름에 따라, 발생하는 차이점으로 추정된다. 현재 공격은 개개인에 대한 분석까지 시행하지는 않고, 메일링리스트에 대한 일괄공격 유형으로 판단된다. 특이하게 같은 내용의 공격을 2~3번 이상 받은 인원의 메일이 전체 샘플 40건 중 3건이 있었다. 이는 수신자 메일링 리스트가 여러 곳에 등록된 경우로 분석되었다. 메일링 리스트상에 노출된 인원들에 대한 개별적으로 이메일 인터뷰를 시도하였고, 결과. 국방관련 기관 종사자, 학계 연구자, 방산업계 종사자이면서 이메일 공격을 받은 인원들은 국방기관 재직시와 방산업체 재직 시 주로 각종 대외 협의체 참석인원, 각종 대외 학술대회 참석 인원들이다. 이들의 정보 유출은 학회장 등에 있는 명단에서 유출되었을 수도 있으며, 이메일 정보가 집계된 특정 PC가 최초 공격을 받은 이후 이들에 대한 정보를 습득하여 지속적인 공격이 시도되는 것으로 예측할 수도 있다. 추적대상 이메일들을 활용하여, SNS 유사 아이디를 확인한 결과, 추적대상자의 85%는 메일계정과 SNS아이디를 유사한 아이디로 사용하고 있어, SNS 사용을 통한 공격용 개인정보의 수집이 용이함을 확인할 수 있었다. 분석결과로는 국내 국방분야 및 방산업계 사회공학적 공격대상자는 발생 빈도 분석을 통해 볼 때, 보직간부와 실무자를 가리지 않고 보내고 있는 것으로 추정된다. 사회연결망 분석을 통한 사회공학적 정보 수집의 경우, 보직간부와 실무자의 구분이 어렵지 않다. 그러므로, 정보수집과정에서 공격자가 습득한 정보가 정교하지 않아, 선택적 공격을 하지 않았을 가능성도 있다. 그러나 공격자의 기본적인 의도가 다수에 대한 공격을 통해, 공격 성공 가능성을 높이는 것이 주목적일 것으로

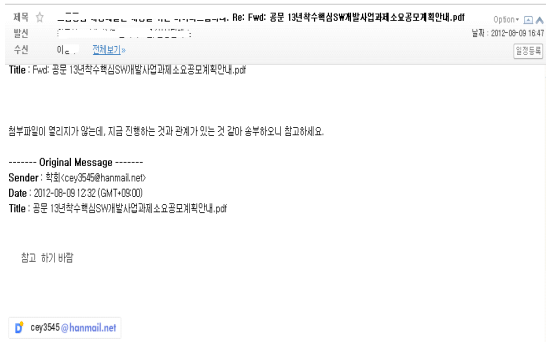
추정된다.

3.1.5 이메일의 구성 : 내용과 첨부

앞서 언급된 바와 같이 최근 3년간의 메일들을 분석해보면 매월의 주요 공지사항이나 이슈 사항들이 공격용 메일의 안건으로 활용하고 있다. 분석 결과 주목할 사항은 대부분의 이메일에서 해당 화일을 열어보라는 표현으로 '참고바람','참고할 것', '참고바람' 정도의 매우 짧은 표현만을 간략하게 사용하고 있다. 예를 들면 (그림 2)와 같이 '참고바람' 이라는 매우 짧은 표현을 사용하고 있다. 이 외의 일반적인 인사말과 자신을 드러내는 표현을 사용하지는 않고 있다. 공격 메일들에 드러나고 있는 공격자의 이런 행동 양식은 공격자의 사회공학적 역량 수준에 대한 위장 또는 상급자로 위장하기 위한 의도된 표현으로 추정되는 부분이다. 또한 학회 협회를 사칭하는 것만으로도 사회공학적 역량이 낮은 것을 확인할 수 있다. 사회공학적 역량이 높은 경우, 신뢰도를 향상시키기 위한 공감 확보를 위한 표현들과 전문용어, 공감향상 용어 등이 활용되고 있다. 현재까지의 공격들은 공감확보를 위한 표현을 사용하지 않고 있다. 이 것의 의도는 자세한 설명을 하지 않음으로써 공격대상자가 파일을 호기심으로 열게 하려는 의도로 추정된다. 이러한 동향은 지속적이고 공통적으로 사용된 것으로써, 단순한 것이 아닌 의도된 것으로 간주해야 한다. 여기서 이런 짧은 표현은 상급자가 하급자에게 하는 표현을 의도하고 있는 것으로 추정된다. 공격자는 자신이 사회적으로 우월한 지위에 있는 상급자로 보이려는 시도를 하고 있는 것으로 추정된다.

4. 공격 유형 예측

본 연구는 실제 발생한 사례들을 통해, 향후 발생될 것으로 예상되는 공격유형을 예측하는 것을 목표로 하고 있다. 우선, 향후 시도될 공격들이 다루려고 하는 안건들을 현재 기존의 공격 내용과 향후 예상되는 국방 및 방산 관련 이슈, 정기적으로 발생하는 안건 등과 연결하여 예측한다. 다음으로는, 공격의 기술적 변화를 예측한다. 현재는 단순하게 멀웨어인 첨부화일을 실행



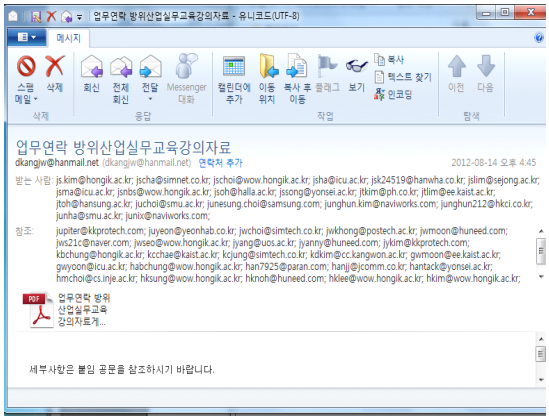
(그림 2) 예상된 공격 유형이 실제 발생한 경우 1

하게 유도하는 것이 공격의 주된 방법으로 나타나고 있다. 그러나, 향후에는 메일 확인만으로도, 감염이 되거나, 좀비PC와 같이 이미 저장된주소록을 활용한 메일링리스트 스팸공격 같은 것을 복합적인 공격이 시도할 것이 예측된다.

4.1 신규 메일 안건 예측

최근 3년간의 공격 메일 안건과, 최근의 국방, 방산분야 이슈를 분석하여, 향후 1년간 예상되는 이메일 공격 제목을 예측해본다. 매년 정기적으로 발생하는 사항인 'ACTD 과제공모', 'SW 과제 공모' 등의 정기적인 방산업계의 '연구개발사업 장려'공지관련 사항은 매년 공격에 활용되고 있는 것으로 이는 지속적인 재활용이 가장 유력한 예측 대상이다. 현재 국방부, 방위사업청, 국방기술품질원, 한국방위산업학회 등에 공지되거나, 공지된 사항을 통해 2012년 중에 발생할 것으로 예상되는 공격용 이메일에서 활용될 것으로 예측되는 안건은 다음과 같다. '방위산업교육관련','감항인증교육관련' '2012년 감항인증컨퍼런스', '국방과학기술전략서', '품질경영위원회 개최 결과', '국방품질경영업무규정','방산체계업체-협력업체 SCM 관리','핵심기술기획 추진계획','ACTD 과제검토 결과','국제기술협력기본계획 및 발전포럼','효율적인 국방과학기술진흥실행계획','차세대 전투기 도입사업 시험평가 결과'이다. 여기서 예측한 안건 외에 발생 가능한 사항은 시의적인 사항들로 남북관계나 군사관련 이슈 발생하는 경우의 해당 안건 관련 정보공유를 빙자한 공격들이 시도될 것이 예상된다. 위에 예측된 사항은 모두 국방 및 방산과 관련된 공지사항

으로, 공격자는 국방부 및 관계기관 홈페이지를 지속적으로 모니터링 하여, 공격용 안건을 지속적으로 생성하고 있음이 추정되고다. 그러므로, 위와 같은 사항이 올 하반기에 지속적으로 공격용으로 활용될 것이다. 위에 예측된 결과는 향후 지속적으로 실제 공격을 확인함으로써만 예측값의 정확성 평가가 가능한데, 위에 예측된 사항중 '방위산업교육관련'은 이번 연구 초고 제출 후, 발생한 (그림3)의 실제공격사례와 같이 '업무연락 방위산업실무교육강의자료'로 발생했다. 그 형태가 기존의 공격과 유사하여 버추얼 머신 상에서 확인 결과, 버추얼 머신 내부에 악성코드 실행의 특징적 현상인, 윈도우 시스템 폴더들에 파일 생성 현상이 발생했다. 해당 메일의 첨부화일은 메일 수신 당시, 악성코드 포함여부가 진단되지 않았다. 백신업체로 전송 후 통보된 내용은 전형적인 PDF 취약점을 활용한 공격의 변형으로 확인되었다.



(그림 3) 예상된 공격 유형이 실제 발생한 경우 2

이 공격 사례에서 확인되는 특이사항은 기존에 사용하지 않던 업무연락이라는 표현과 '바랍니다'라는 약간의 경어가 사용되었다는 것으로, 향후 사회공학적 공격 양상과 수단이 복잡해질 것임을 예측할 수 있다.

4.2 공격의 기술적 변화 예측

앞 장은 향후 이메일 공격에서 활용될 안건을 예측해보았다. 이와는 별개로 공격의 기술적 변화들도 예측할 수 있다. 본 연구에서 예상하는 신규유형은 기존의 이메일 격이 개별 사용자에 대한 단체 메일 개별 배포 방식과 조금 다른 공격 방식을 예측한다. 이는 공격의 생존성과 공격범위 확대를 동시에 만족할 수 있는 방법이다. 기존의 공격은 수집된 공격대상에게, 공격용 화일을 배포하고 해당 공격자 PC를 침해하는 것으로 이루어진다. 예상되는 변화 시도 유형은 공격용 메일에 스크립트 자동실행 통해, 공격대상자의 메일계정이 가진 메일주소록을 탈취하한다. 공격메일을 해당 메일주소록으로 자동 발송하는 것을 1차 공격으로 한다. 2차 공격으로 1차공격의 확실한 보장을 위한 보조수단으로, 공격용 파일은 같은 기능의 스크립트나 다른 용도의 스크립트를 포함시킨다. 이를 통해, 공격 시도자의 단일 피해자에 대한 1회 공격은 2회의 공격 효과를 가지게 된다. 단일피해자가 가진 메일 주소록의 수량에 따라, 수집된 목표물 외에 수십, 수백배의 공격이 가능하게 된다. 이 경우에는 공격 시도자가 목표한 공격 목표를 초과하는 공격 효과를 기대할 수 있게 된다. 예측된 신규 유형은 메일주소록 탈취 스크립트 작성의 어려움과 성공 가능성에 대한 제한사항이 발생할 수 있다. 이러한 문제는 다른 변화 시도를 통해, 스크립트의 작성 문제보다 단순하게 해결할 수 있다. 계정 확보나 메일주소록 확보, 메일자동발송 스크립트 프로그래밍 같은 것을 전혀 하지 못하더라도, '부서원간 회람바람', '전파바람' 정도의 사회공학적 문구를 사용하는 것만으로도, 원래 의도한 공격 시도자의 의도를 달성할 수 있을 것이 우려된다. 현재까지 발생 사례를 살펴보면,, 공문이나 메일을 수신하는 경우에 별도의 정본 확인 절차 없이 메일을 무분별하게 재전송하는 경우가 많기 때문이다. '회람, 전파'라는 표현에는 반사적으로재전송으로 반응할 경우에는 조직내 전파가 용이해지게 된다. 또한 바이러스나 악성코드가 걸린 것으로 검진 된 경우에도, 보안부서 신고 없이 재전송하는 경우가 있었다. 이러한 방법은 현재까지 충분히 위협적인 공격방법으로 예상할 수 있다. 이번 연구에서 예측한 신유형의 이메일 공격의 요점은 기존의 열람자 권한 확보와 아울러 열람자, 메일주소록 상의 관계자 이메일로 최초 열람자의 회람 요청 또는 확인 요청 메일 자동 전송을 통해 기관내 전체 인원을 악성코드에 감염시키거나 수동 재전송을 통해 감염범위를 넓히는 방식이다.

4.3 신 공격 유형들에 대한 대응 방안

국방기관과 방산업계에 대해 배포된 멀웨어들은 특정 국외 IP로 정보를 전송하는 기능을 보유하고 있다. 특정 분야에 대한 특정 공격이 지속되는 것으로 보아, 현재 국방기관과 방산업계에 배포되고 있는 멀웨어 공격들은 APT(Advanced Persistent Threaten)를 의도하고 있는 것으로 추정된다. 이런 종류의 지속적인 공격들에 대해서 정보보안 솔루션들이 개발되어 소개되고 있다. 그러나 그런 종류의 보안솔루션을 도입할 수 있는 기업이나 기관은 흔치 않다. 또한 현재 소개되고 있는 APT 보안솔루션들은 기존의 방화벽이나 IDS, IPS와 큰 차이를 가지고 있지 못한 문제도 있다. 납품 단가 상승을 위해, 랙 형태의 별도 서버를 SW제품과 함께 제공하는 형태로 소개되고 있는 현재의 APT보안 제품들이 투자비용대비 효과가 있을지에 대해서는 현재까지 검증된 바가 없다. 본 연구에서는 보다 현실적이고 용이한 접근법들을 제시한다. 먼저, 국방기관과 방산업계 관련된 이메일을 통한 자료 배포에 공공기관 배포 정본확인이 가능한 인식표나 인증서, 비표 등을 부여하는 방법이다. 인식표나 비표의 경우에는 각 공공기관별로 특정기간을 정하여 해당 기간 중에는 메일에 특정한 특수문자나 특정한 단어가 등장해야만 해당 기관에서 발행한 문서임을 증명하는 것이다. 인증서의 경우 공공기관에서 발송하는 모든 문서는 각각 인증서를 포함하여 발송하게 하고 개별인증서를 해당 공공기관에서 조회하였을 때에 적합성이 인증된 메일만이 적합한 메일로 분류하는 방법이다. 아울러, 본 연구에서는 국방분야 멀웨어 공격이나 사회공학적 공격을 예보하는 업종/전문 분야별 사이버테러 예보관 제도도 제시하고자 한다. 사이버테러 예보관 제도는 국방기관과 방산업계에 대한 이해도가 높고 정보보호에 대한 인식이 높은 인원을 활용하여, 앞서 언급된 것과 같은 사회공학적인 멀웨어 배포 동향을 예측하게 하는 제도이다. 현재 국가지역 수준에서의 사이버테러 위험수준 전반에 대해서는 백신업체와 공공기관 사이버수사대, 사이버안전센터 등에서 수준을 측정하여 공지하고 있다. 하지만, 특정 분야와 전문 분야, 특히 최근 지속적인 공격이 시도되고 있는 공공기관, 국방기관, 방산업계 등에 대한 별도의 관리는 이루어지고 있지 않다. 최근 사이버테러는 기존의 기술의존적 침해사고보다 사회공학적 공격 성향을 많이 띄고 있으므로, 기술적인 공격 분석을 중심으로 관제하는 방식에 아울러, 분야별 사회공학적 공격을 방지할 수 있는 비기술적 관점을 볼 수 있는 사이버테러 예보관 제도를 시행하는 경우 현재 발생하는 사회공학적 공격시도들을 방지하는데 도움이 될 것으로 예상한다. 앞서 언급된 신규 유형 중 수동 전파 공격의 경우에는 교육을 통해, 의심되는 이메일에 대한 재전송 금지만 전파가 되고 구성원간의 인지만 되어도 충분히 막을 수 있는 공격이다. 사회공학적 공격은 전적으로 교육을 통한 관리적 보안을 통해서 공격 대상으로 정보가 수집되는 것을 방지하고 발생하는 공격 시 의심스러운 사항에 대해 조치할 수 있는 능력을 가지는 것이 중요하다. 보안 또는 정보보호에서 전체수준은 가장 약한 부분의 수준이라는 표현이 있듯이, 구성원 중 1명이라도 취약성을 가지는 경우에는 취약성을 가진 1인에 대한 공격 때문에 기관전체에 대한 사회공학적 공격이 성공할 수 있기 때문이다. 이번 연구에서 분석되고 예상된 공격 유형은 관리적 보안대책 차원에서 교육훈련에 반영되어 전파되는 것이 큰 변화 없이 즉시 실행가능한 가장 효율적인 방지대책이 된다. 기존의 군사보안 규정에 대한 준수는 지속적으로 준수되어야 하며, 이에 대한 보완책으로 일반적으로 사용되고 있고 외부 변화에 대응이 용이한 정보보호관리체계(ISMS), 정부정보보호관리체계(G-ISMS) 등이 있다. 개정이 어려운 특수 기준의 활용만을 만족하기 보다는 변화에 따른 지속적인 개정과 관리가 빠르게 이루어지는 일반 기준을 활용하고 있는 정보보호 검증도 도입하여 지속적인 보안강화를 이루어가는 것도 필요하다.

4.4 예측에 대한 평가와 향후 과제

본 연구에서 제시하고 있는 예측은 과거 자료를 통해 귀납적으로 공통점을 도출하고, 그 공통점을 통해 연역적으로 향후 공격 유형을 예측하는 방식이다. 본 연구에서 제시하고 있는 예측들 중, 국방분야 공지사항을 활용한 사회공학적 이메일로 멀웨어를 배포에 대한 예측은, 실제사례 발생으로 입증이 되고 있다. 그러나 이에 대한 정량적인 검증 평가 방법이나, 정성적인 평가방법은 현재까지 찾기 어려운 실정이다. 본 연구의 정밀도를 높이고, 예측값의 정당성을 높이기 위해

서는 현재 연구에서 단순히 기존 자료를 분석하여 공통요소를 도출하여 예측을 하는 방식에서 보다 일반적인 접근법을 활용하는 것이 필요하다. 본 연구에서는 예측과정에서 예측에 대한 분석 모델링 프레임워크를 만들어내지 못한 한계가 있다. 향후에는 예측에 대한 분석 모델링 프레임워크를 가지고 접근할 필요가 있다.

5. 결 론

본 연구는 이메일을 활용한 사회공학적 공격 중 국내 국방기관 및 방산업계에 대한 이메일 활용 멀웨어 배포 동향을 분석했다. 이에 따른 새로운 공격 유형을 예측하였다. 국내 국방기관 및 방산업계 대상의 이메일 공격은 주로 수집된 이메일 정보를 바탕으로 악성코드가 포함된 문서 파일을 멀웨어로 배포하여 피해자 PC에 저장된 정보를 탈취하는 의도이다. 이번 연구는 새로운 공격 유형의 예측을 통해, 국내 국방기관 및 방산업계에 대한 해킹 시도에 대한 방지에 기여할 수 있다는 데 의의가 있다. 본 연구에서는 예방적 정보보호써 몇가지를 제시한다. 먼저 공공기관에서 발송하는 이메일의 정본성 확보를 위한 비표, 인증서, 인식표를 제정하여, 공공기관을 사칭하는 사회공학적 공격 메일을 방지하고자 한다. 다음으로 비기술적 관점의 사이버테러 분석관인 전문분야 사이버테러 예보관 제도를 제시한다. 현재 분석된 바와 같은 공격의 대응을 위해서는 기본적으로 기존의 보안업무시행규칙의 이행과 준수를 지속적으로 강화해야한다. 또한 관리적 보안 강화를 위하여 현재 타 공공분야와 업계에서 적용이 지속적으로 제시되고 있는 정보보호관리 프레임워크와 관리방법론과 인증심사 등의 다양한 수단 들을 활용하는 것의 검토도 필요하다. 이런 방법을 활용하여 관리적 보안을 지속적으로 향상시켜야 할 필요가 있다. 현재 국방부의 보안업무시행규칙을 적용하거나 준용하는 기관들이나 방산업계에 기본적으로 수행되는 보안감사와 보안규정을 엄밀하게 준수하는 경우에는 큰 문제가 없을 수도 있다. 그러나 어느 곳에나 허점은 발생할 수 있으므로, 보완책이 필요하다. 보완책으로는 일반적으로 사용되고 있고 외부 변화에 대응이 용이한 정보보호관리체계(ISMS), 정부정보보호관리체계(G-ISMS) 등이 있다. 개정이 어려운 특수기준의 활용만을 만족하기 보다는 변화에 따른 지속적인 개정과 관리가 빠르게 이루어지는 일반 기준을 활용하고 있는 정보보호 검증도 도입하여 지속적인 보안강화를 이루어가는 것도 필요하다.

참고문헌

[1] 최준성, 국광호, “국내방산업계 사회공학적 공격 동향과 대응방안”, 2012, 한국방위산업학회 논문지, 제19권1호 2012년 6월

[2] 장공수, “해킹 확산 예방체계 긴요 사회공학적 공격 위험성과 우리 군의 대응 방안”, 2009, 국방저널

[3] 최양서 외,“사회공학적 공격 방법을 통한 개인정보 유출 기술 및 대응방안 분석,”정보보호학회지, 제16권 제1호, 2006

[4] 송인철, “사회공학적 공격 위험성과 우리 군의 대응 방안에 관한 연구 군에서 발생 하는 공격 위험성과 효과적인 대응방안 중심으로”,2011,연세대학교

[5] Christopher Hadnagy,“Social Engineering The Art of Human Hacking”, 2010, Wiey Publishing

[6] Johnny Long,“No Tech Hacking, A Guide to Social Engineering Dumpster Diving & Shoulder Surfin”, 2008, Syngress

[7] Kevin Mitnick,“The Art of Intrusion”, 2005, Wiley Publishing

[8] Kevin Mitnick,“The Art of Deception”, 2002, Wiley Publishing

[9] Kevin Mitnick,“Ghost in the Wires: My Adventures as the World's Most Wanted”, 2012, Back Bay Books

[10] Shakeel Ali,“BackTrack 4: Assuring Security by Penetration Testing”, 2011, Packt Publishing

[11] Vivek Ramachandran,“BackTrack 5 Wireless Penetration Testing Beginner's Guide”, 2011, Packt Publishing

[저 자 소 개]

최 준 성 (Junesung Choi)

1999년 공군사관학교 산업공학사
1999년~2008년 공군군수사, 한미연합사, 국군지휘통신사, 국방부, 행정자치부
2008년~현재, 삼성탈레스(주)
2002년~2011년 한국방송통신대학교 법학과, 컴퓨터과학과 수료
2008년~2010년 한국방송통신대학교 대학원 정보과학과 정보통신이학석사
2011년~현재, 서울과학기술대학교 IT정책전문대학원 산업정보시스템공학전공 박사과정

email : where@seoultech.ac.kr

국 광 호 (Kwangho Kook)

1979년 서울대학교 산업공학사
1981년 서울대학교 대학원 산업공학 석사
1989년 美 조지아 공과대학교 대학원 산업공학박사
1989년 ~ 1993년 한국전자통신연구원 선임연구원
1993년 ~ 2012년 현재 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 교수

email : khkook@seoultech.ac.kr