기업정보 온라인유출 유형 및 사례 분석

NCSC-TR050010

국가사이버안전센터
National Cyber Security Center

기업정보 온라인유출 유형 및 사례 분석

최원혁 | (주)하우리 엔진개발실장

I 서 론

기업이 많은 연구개발비를 투자해 획득한 기술 관련 정보, 생산에서 판매까지의 전략 등 각종 기업정보를 제3자가 부정한 방법으로 얻는 경우, 또는 정당한 방법으로 이를 획득했다 해도 자신의 이익을 위해 유용하는 경우나 혹은 남에게 피해를 주기 위해 부정하게 유출시키는 경우에는 문제가 된다. 물론 이 정보(비밀)는 '공공에 알려져 있지 않고 독립된 경제적 가치를 가지는 것으로 상당한 노력에 의해 비밀로 유지된 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상 정보'를 의미한다.[1]

컴퓨팅 환경이 발달하기 전에는 기업의 모든 정보는 튼튼한 금고 속에 깔금하게 철이 된 문서로 고이고이 모셔져 있었다. 하지만, 지금과 같이 컴퓨팅 환경이 발달하면서 점점 그러한 문서들은 중앙 서버에 모여지게 되었고 이들 정보에 접근하는 것도 특정인들만이 몇몇 보안 단계를 거쳐서 정보를 열람하고 나오는 방식으로 바뀌어지게 되었다. 더군다나 예전에는 경제적 가치로 인정받지 못했던 기업정보가 정보화산업 발달로 그 중요성이 높아지게 되고 이를 지키고자 하는 자와 빼내고자 하는 자 사이의 치열한 공방이 벌어지게 되었다. 결국 기업정보를 노리는 산업스파이들은 이런 정보를 빼내기 위해 해킹을 시도하기도 하고 그 조직에 잠입을 시도하여 그 정보에 근접하려고 노력을 하게 되었다. 결국 이런 이유로 기업은 보안관리자를 두고 각 부서별로 각각의 정보 접근권한을 부여함으로써 기업정보의 유출을 방지하고 있다.

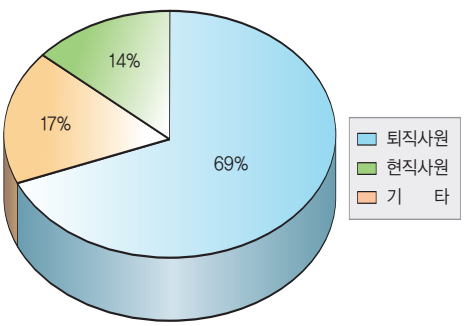
1 윤선희, "기업비밀 중요성", 전자신문-벤처포럼, 2002. 7.11

Ⅱ 기업정보 유출 주체

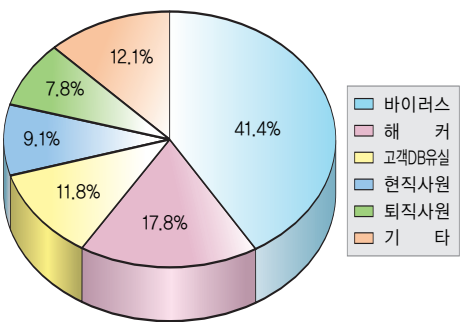
오늘날 기업정보 유출의 주체자를 외부자(해커)보다는 내부자로 보는 경우가 많아지고 있는데 이는 인터넷 시대에 이르러 더 심각한 수준에 이르렀다. 이것은 인터넷이 가지고 있는 즉각성과 개방성에 기인한다. 이메일과 메신저로 정보를 내보내는 것은 외부에서 들어와서 정보를 가지고 가는 것보다 몇 배는 쉽기 때문이다. 따라서 국내 보안산업의 패러다임이 외부자보다는 내부자에 의한 정보유출을 막는 방향으로 확대되고 있다

실제로 FBI가 2001년에 실시한 '기업의 기밀정보 유출실태조사'에 따르면 기업정보 유출이 외부해커에 의해서라기보다는 내부직원에 의해 일어나고 있음을 알 수 있다.[2] 또한, 정보통신부 산하 한국정보통신수출진흥센터(ICA)가 2004년 6월 1일부터 7월 20일까지 771개 기업을 대상으로 조사한 'IT기술 해외유출 방지 실태조사 보고서'에 따르면, 유출을 시도하는 사람은 [표 1]과 같이 내부자중 퇴직사원에 의한 것이 70%에 육박, 기업체 인사관리의 취약성이 드러나기도 했다.[3]

대한상공회의소가 2003년 국내 243개 기업을 대상으로 실시한 '국내기업의 정보보안 위기관리에 대한 실태조사'에 따르면 과거에 경험했던 정보보안 위기의 유형에 대해서는 41.4%가 바이러스에 의한 사내전산망 감염을 꼽았으며, 다음으로 △해커의 공격에 의한 사내 서버침투(17.8%) △고객정보 데이터베이스 손실(11.8%) △현직사원에 의한 사내 중요문서 외부유출(9.1%) △퇴직자에 의한 기업비밀 유출(7.8%) 순으로 나타났다. 이같은 결과는 기업들 사이에서 인터넷 사용이 보편화되면서 온라인상의 정보보안 피해가 오프라인보다 더욱 심각해지는 양상을 보이고 있는 것으로 풀이된다.[4]



[표 1] 내부자 자료유출 비율



[표 2] 과거 정보보안 위기 유형

2 최성호, "사내정보유출 문제점과 해결책", Ahnlab's CEO Report : Market Place, 2003.8.29

3 "IT기업 45%, 산업보안 위협", 디지털타임스, 2004. 7.21

4 "국내기업 70%, 정보보안 무방비", 머니투데이, 2003. 6.18

[표 1]은 2004년을 기준으로 하였고 [표 2]는 2003년을 기준으로 하였는 바 1년 사이에 퇴직사원에 의한 기업정보 유출피해가 급증한 것을 알 수 있는데, 통상 퇴직사원들은 현직시절 스카우트제의를 받은 후 이직을 전제조건으로 자신이 참여한 프로젝트나 접근 가능한 회사기밀 등을 수집하게 된다.

Ⅲ 온라인을 통한 기업정보 유출 유형

1. 내부자

영국의 보안리서치 전문기관인 BISS의 통계를 보면 기업기밀정보유출의 80%가 이메일을 통해서 일어나고 있다. 이라크전이 임박했던 2003년 3월 미군은 기밀 유출을 우려해 병사들의 이메일을 단속하기 시작했다. 일부 병사들이 부대의 안전을 해칠지 모를 디지털 이미지 등 민감한 정보를 이메일을 통해서 가족에게 보내는 일이 잦아지자 이를 단속하고 차단하기 시작한 것이다.[5] 물론, 기업도 마찬가지이다. 또한, 메신저는 이메일로 발송하기 어려운 용량의 문서도 전달이 가능하고 어떤 대화든 실시간으로 할 수 있기 때문에 기업정보 유출의 단속 대상이 되었다. 이런 이유로 지난해 10월에는 서울시 공무원들에게도 메신저 금지령이 내려졌는데 근무시간내 메신저를 이용한 채팅을 비롯 유해 인터넷 사이트 이용을 금지시킨바 있다.[6,7]

2. 외부자

가. 해킹

내부자가 아닌 외부자에 의해서 기업정보가 유출되는 경우라면 쉽게 산업스파이를 생각하게 된다. 이들이 기업의 내부가 아닌 외부에서 기업정보를 유출하는 방법으로 해킹을 시도하게 된다. 해킹은 불특정 다수의 시스템을 공격하는 웜 · 바이러스와는 달리 해커가 목표로 하는 시스템만을 공격하게 된다.

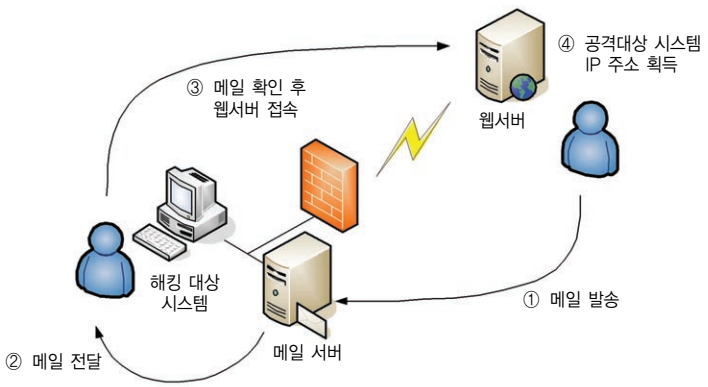
5 "미군, 병사들 e-메일 단속", YTN, 2003.3.12

6 "메신저 못하는게 없다", 제일경제, 2004.4.18

7 "서울시 공무원에 메신저 금지령 ", 연합뉴스, 2004. 10.22

1) 패스워드 공격

가장 쉽게 공격대상 시스템에 접근하는 방법은 해당 시스템의 계정과 패스워드를 알아내는 것이다. 물론 내부자라면 해당 시스템의 계정과 패스워드를 획득하는 것이 쉬운 일이지만, 외부자의 경우 이를 알아내는 방법은 그렇게 쉽지만은 않다. 또한 해당 시스템을 외부에서 찾아내기도 쉽지가 않다. 결국 해커는 외부에서 공격대상 시스템을 알아내기 위해 그 시스템의 IP 주소를 알아내는 것이 가장 중요하게 된다. 먼저 해당 시스템의 IP를 알아내기 위해서는 인터넷 게시판을 활용하는 방법과 알고 있는 이메일을 활용하는 방법을 생각할 수 있다. 해커는 해킹하고자 하는 시스템의 소유자에게 이메일을 보낸다. 첨부파일을 포함해서 백도어 등을 보낼 수도 있겠지만, 최근 웜 · 바이러스의 대표적인 방법과 유사해 쉽게 사용자들이 첨부파일을 실행하지 않는다는 것을 이해해야 한다. 따라서 접속을 유도할 만한 광고로 사용자를 웹사이트로 끌어들여 접속한 사용자 시스템의 IP 주소를 획득하면 된다.



[그림 1] 웹서버를 활용한 IP 주소 획득 과정도

이메일을 통한 해커의 접근은 방화벽 및 침입탐지시스템(IDS)에서 조차 발견하지 못하는데, 이는 지극히 정상적인 인터넷 사용으로 보기 때문이다. 지난해 6월에 발생했던 국가 · 공공기관 해킹사건이 대표적인 예라고 할 수 있다. 이때 해킹당한 시스템들은 국회, 해양경찰청, 원자력연구소, 국방연구원 등 국가기밀을 취급하는 주요 기관의 사용자 컴퓨터들이었으며 사용된 백도어는 Backdoor.Win32.PeepViewer였다. PeepViewer는 대만인이 제작하여 인터넷에 공개되면서 해커들이 사용하기 시작한 원격제어 프로그램이지만 이메일이나 네트워크로 확산되지는 않는다.[8] 그러나 이들 시스템이 감염될 수

8 "Backdoor.Win32.PeepViewer 바이러스 정보", 하우리, 2004.6.19

있었던 것은 바로 국가 · 공공기관의 이메일 주소로 세미나 안내 메일 및 설문조사 또는 안부 메일 등을 보내어 수신자가 이를 확인하였기 때문이다. 물론 국적미상의 해커가 보내긴 했지만 메일의 내용은 한국어로 되어 있었기 때문에 피해를 본 시스템의 사용자들은 PeepViewer가 첨부된 이메일을 아무 거리낌 없이 받아들였다.

공격대상 시스템의 IP 주소를 알아냈다면 이제 계정과 패스워드 공격을 시도할 차례다. 대부분의 사용자가 OS의 Administrator 또는 Admin 등의 계정을 기본적으로 사용하는 경우가 많기 때문에 해커는 패스워드를 찾아내기 위해 노력한다. 사용자 대부분이 간단한 패스워드를 사용하는 것을 이용해 [표 3]과 같은 취약 패스워드 대입법을 통해 시스템을 해킹하게 된다.[9]

!@#$	devil	rooted	TEST
!@#$%	dick	SERVER	Test
!@#$%^	dude	server	tim
!@#$%^&	erik	share	tom
!@#$%^&*	fanny	sql	UNIX
000000	feds	stacey	user
00000000	fish	stacy	User
111	fool	Standard	Verwalter
11111111	freak	stefan	wh0re
12	fucked	steve	whore
123	Gast	steven	win
1234	gay	student	windows2k
12345	george	super	windows98
123456	Guest	sybase	windowsME
1234567	hax	SYSTEM	WindowsXP
12345678	home	teacher	windoze
123456789	idiot	TEMP	wwwadmin
123asd	Internet	temp	xp
123qwe	Inviter		xyz
2004			

[표 3] 취약 패스워드

2) 원격 제어 프로그램 이용

인터넷이 보편화되면서 가장 큰 문제점중 하나가 해킹에 관련된 자료를 마음만 먹으면 쉽게 구할 수 있다는것이다. 원격제어 프로그램을 구했다면 해커는 이 프로그램을 공격

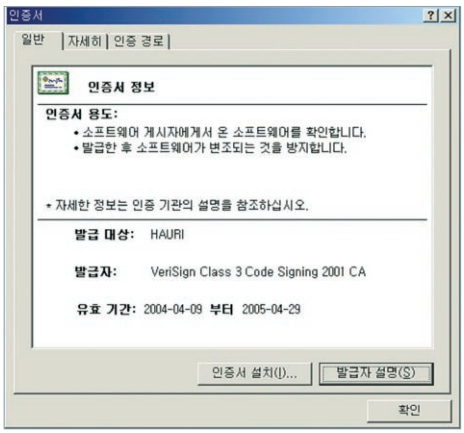
9 "PC속의 개인정보 누군가 엿보고 있다", 동아일보, 2004.7.19

대상 시스템에 보내게 된다. 이는 앞서 패스워드 공격때와 동일한 방법 즉, 이메일 및 웹 게시판을 통해서 배포할 수 있게 된다. 단, 웹 게시판을 통해서 배포할 때에는 대부분 보안 경고창이 나타나지만, 사용자의 인테넷 익스플로어의 옵션 설정에 문제가 있거나 사용자가 보안 경고창에서 [예]을 선택할 경우 자칫 원격제어 프로그램이 설치될 수 있다. 자신이 소유한 시스템의 인터넷 익스플로어 옵션 설정에 문제가 있는지를 체크하려면 [도구]→[인터넷 옵션]→[보안]→[인터넷]→[사용자 지정 수준]→[ActiveX 컨트롤 및 플러그 인]에서 아래내용을 확인하면 된다.

- 서명 안 된 ActiveX 컨트롤 다운로드 : 사용안함
- 서명된 ActiveX 컨트롤 다운로드 : 확인
- 안전하지 않는 것으로 표시된 ActiveX 컨트롤 초기화 및 스크립트 : 사용안함
- 안전한 것으로 표시된 ActiveX 컨트롤 스크립트 : 사용
- ActiveX 컨트롤 및 플러그 인 실행 : 관리자 승인

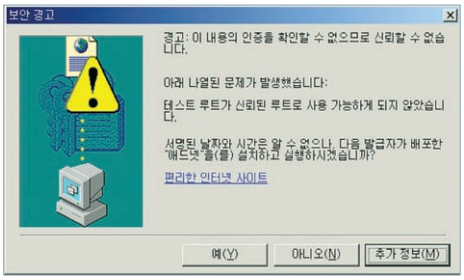
보안 경고창이 뜰 때 주의해서 보아야 할 사항은 바로 발급자이다. 발급 대상은 누구나 될 수 있지만 발급자는 대부분 정해져 있기 때문이다.

[그림 2] 보안 경고창

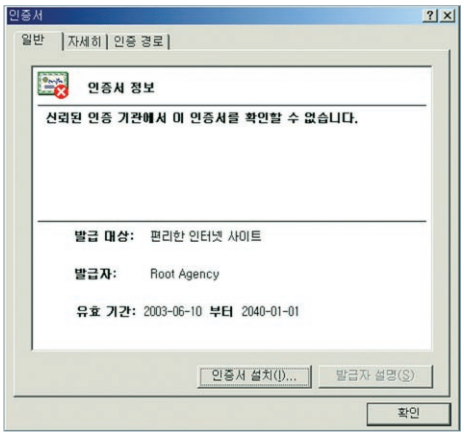


[그림 3] 발급자 정보

[그림 2]에서와 같이 보안 경고창에서 파란색의 하이퍼링크(Hyper Link)를 선택하면 [그림 3]과 같은 인증서 화면에 발급자의 정보가 나타나며, 우측하단에 발급자 설명을 통해서 어떤 발급자에 의해서 발급 대상자가 인증되었는지 자세하게 알 수 있다.



[그림 4] 신뢰할 수 없는 발급 대상임을 경고하는 보안 경고창



[그림 5] 발급자 정보를 찾아볼 수 없는 인증서

[그림 2], [그림 3]과는 달리 [그림 4]의 보안 경고창은 이미 신뢰할 수 없는 발급 대상임을 경고한다. 또한 하이퍼링크를 선택하여 자세한 발급자 정보를 찾아볼 수 없다. [그림 5]의 우측하단에 발급자 설명 버튼이 비활성화 되어 있을 뿐 아니라, 일반적인 발급자들이 제공하는 인증서의 유효 기간은 통상 1년인데 반해 [그림 5]에는 약 40년간의 유효 기간을 가지고 있다.

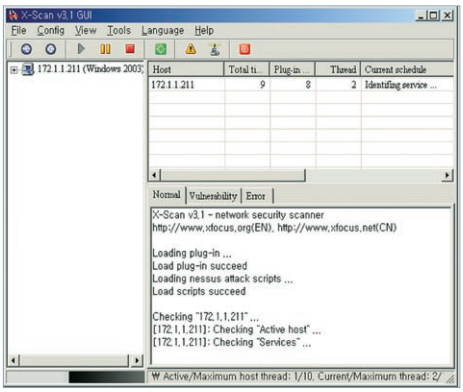
3) OS 취약점 이용

OS(운영체제)도 하나의 프로그램이다. 프로그램이라는 것은 사람에 의해서 개발되었고 언제나 버그가 존재할 가능성이 있다는 것을 의미한다. 조그만한 프로그램을 개발하더라도 수많은 버그가 존재하는데 하물며 커다란 OS를 설계하고 프로그램하는데 얼마나 많은 버그가 존재하겠는가? 따라서 MS는 항상 보안전문가들이 지적한 윈도우의 취약점을 제거하기 위해 노력하고 있으며 보안 취약점을 해결할 수 있는 패치 프로그램을 인터넷에 공개하여 윈도우 사용자들 누구나 다운로드하고 패치하여 보안에 안전한 최상의 윈도우 OS 환경을 만들고 있다. (http://windowsupdate.microsoft.com)

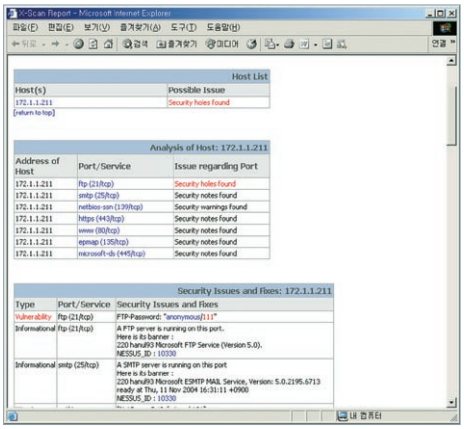
하지만, 아무리 MS사에서 보안 패치를 매번 내놓더라도 이를 사용자들이 제때에 설치하지 않는다는데 문제가 있다. 다소 귀찮고 대부분의 보안 패치 실행 이후 재부팅을 해야하기 때문에 웹서버, 메일서버 등 서비스가 중단되어서는 안될 시스템들은 보안관리자가 보안 패치를 강조하더라도 실제 서버 책임자는 패치를 하지않기도 한다. 결국 이런

이유로 해커는 보안 취약점을 스캐닝하는 툴을 활용해 쉽게 OS의 관리자 권한을 획득하려고 한다.

보안 취약점을 스캐닝하는 도구의 대부분은 해킹이 주목적이 아닌 보안 관리자가 많은 시스템을 일일이 살피지 않고 한꺼번에 보안 취약점들을 알아내어 위기 관리를 하기 위한 목적으로 사용하는것이다. 하지만, 일부 해커에 의해서 이런 프로그램들이 해킹도구로 전락되면서 오히려 해당 프로그램 개발자들이 더 좋은 기능의 관리도구 개발을 중단하게 만드는 이유를 제공하기도 한다.



[그림 6] 보안 취약점을 스캐닝하는 도구



[그림 7] 보안 취약점을 스캐닝하는 도구가 발견한 보안 취약점

[그림 6]은 보안 취약점 스캐닝 도구가 172.1.1. 211 시스템의 보안 취약점을 스캐닝하는 장면이고, [그림 7]은 최종 스캐닝한 시스템에 대한 보안 취약점 분석 보고서이다. 이 결과에 따르면 172.1.1.211 시스템에는 FTP에 보안 취약점이 존재하며, 계정이 anonymous이면서 패스워드가 111이라고 지적하고 있다.

나. 웜 · 바이러스

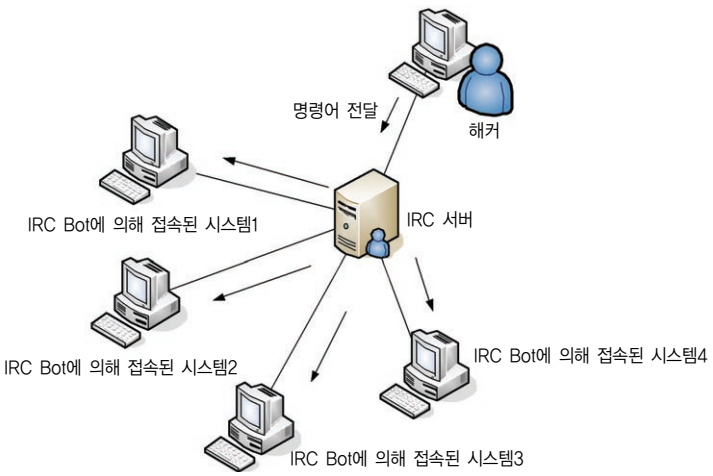
웜 · 바이러스를 통해 해킹을 하고자 하는 해커는 특별히 해킹하고자 하는 특정 시스템이 존재하지 않는 경우가 많다. 즉, 해커는 불특정 다수를 대상으로 해킹을 하여 기업 또는 개인의 정보를 유출하려고 하는 경우 웜 · 바이러스를 활용하게 된다. [10]

10 "Worm.Win32.Agobot 바이러스 정보", 하우리, 2004. 9.16

1) Bot을 이용한 공격

Bot(봇)은 "로봇"의 준말로, 사용자나 다른 프로그램 또는 사람의 행동을 흉내내는 대리자로 동작하는 프로그램을 의미한다. 인터넷상에서 가장 보편적으로 존재하는 봇들은 '스파이더', '크로울러'라고 불리는 프로그램들로써, 웹사이트를 주기적으로 방문하여 검색엔진의 색인을 위한 콘텐츠를 모아오는 일을 한다.[11] 하지만, 최근 이 Bot의 기능을 이용해 불특정 시스템의 보안 취약점을 분석하고 분석된 결과를 통해 시스템에 침투하여 해커가 관리자 권한을 얻는다.

가장 대표적인 Bot으로 IRC Bot을 예로 들수 있다. IRC(Internet Relay Chatting)는 일종의 채팅 서비스이며 대화를 위해서는 IRC 서버에 접속해야 한다. IRC 서버에 접속하는 프로그램은 IRC 클라이언트라 부르며 윈도우에서는 mIRC가 가장 널리 사용된다. 보통 IRC 클라이언트에는 스크립트를 처리할 수 있는 기능이 있고 mIRC 클라이언트에도 막강한 스크립트 기능을 포함하고 있다. 악성 IRC Bot에 감염된 시스템은 보통 이름이 변경되거나 실행 압축된 mIRC 클라이언트가 설치되며, 윈도우 시작 시 자동으로 실행되어 사용자들에게 들키지 않고 실행 중인 프로세스를 숨기는 프로그램 등으로 자신을 숨긴 후 사용자 모르게 IRC 서버의 특정 방(채널)에 접속한다. 이후 [그림 8]과 같이 해당방(채널)에 접속한 시스템들은 운영자(해커)가 내리는 다양한 명령어에 의해 IRC Bot들은 동작하게 된다. 이들 명령어 중에는 시스템의 정보를 획득하는가 하면, 중요 문서들을 유출할 수 있다.



[그림 8] IRC Bot의 명령어 전달

11 "Bot: 봇의 정의", http://www.terms.co.kr/bot.htm

물론 IRC Bot들은 웜 · 바이러스로 간주되기 때문에 Anti-Virus 프로그램들에 의해 진단되고 치료되어지게 된다. 하지만, 해커는 IRC 서버의 특정방(채널)에 접속한 시스템은 Anti-Virus 프로그램이 실행되지 않은 시스템으로 생각할 수 있고 그 방(채널)에 접속한 시스템의 숫자가 급격히 줄어들게 되면 Anti-Virus 프로그램에 의해 자신이 배포한 IRC Bot이 진단/치료된다고 간주하여 새롭게 설계한 IRC Bot 변종을 다시 감염된 시스템에게 업그레이드 하도록 명령을 내리고 다시 IRC Bot은 감염되지 않은 시스템을 찾아내어 감염시켜 IRC 서버의 특정방(채널)에 접속하게 하여 해커에게 정보 유출의 발판을 마련하게 한다. 따라서 최근 IRC Bot의 변종이 많이 등장하는 것도 이 때문이다.

IRC Bot이 가지는 주요 기능은 다음과 같다.[12]

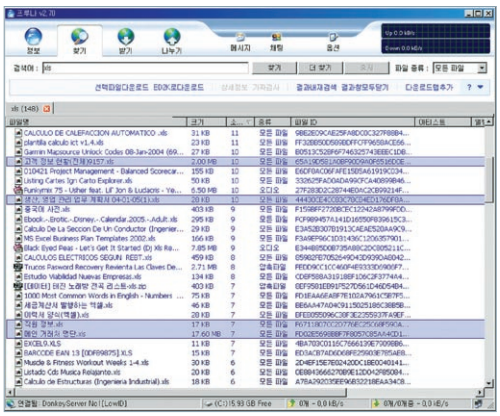
- 특정한 IRC 서버 및 채널로 재 접속
- 트로이 목마가 설치된 시스템의 IP 대역의 회선속도 확인
- 트로이 목마가 설치된 시스템의 트로이 목마 환경 재설정
- 트로이 목마가 설치된 시스템을 찾기 위해 임의의 IP 대역을 스캔
- 트로이 목마가 설치된 시스템의 트로이 목마의 버전확인
- 트로이 목마가 설치된 시스템의 프로세스 중지 및 삭제
- 트로이 목마가 설치된 시스템의 정보(H/W, S/W) 확인
- 트로이 목마가 설치된 시스템에서 rconnect.exe를 이용하여 FTP 서버 기능 on/off
- 트로이 목마가 설치된 시스템에서 mIRC Web 서버 추가 기능을 이용, Web 서버기능 on/off
- 트로이 목마가 설치된 시스템의 파일복사기능 또는 Dropper 파일 복사, 삭제기능
- 트로이 목마가 설치된 시스템들을 이용하여 DDoS 또는 ICMP 패킷 공격기능
- 트로이 목마가 설치된 시스템에서 다른 버전의 트로이 목마를 다운 받을 수 있는 기능
- 트로이 목마가 설치된 시스템의 임의의 포트 Open/Closed 기능
- 트로이 목마가 설치된 시스템에서 자신을 삭제하는 기능
- 그 외 mIRC 기본적인 기능들..

2) P2P를 활용한 공유 공격

초기에 P2P 서비스는 단순하게 음악 파일(주로 MP3)이나 동영상, 그림 파일 등을 주고받는 데 사용되었지만, 최근 들어 실행 파일뿐만 아니라 모든 파일을 공유할 수 있는 방식으로 발전하고 있다. 이는 자신이 원하지 않는 파일이 공유되거나 다른 사람에게 받는 파일의 안전성이 떨어질 수 있다는 것을 의미한다. 실제로 P2P가 실행 파일을 포함한

12 차민석, "악성 IRC봇의 의미와 동작원리 : 보안/바이러스정보", 안철수 연구소, 2003.12.3

모든 파일에 대한 공유가 가능해짐으로써, P2P 프로그램의 설정을 변경해 C드라이브 전체나 기밀문서 폴더 등이 공유될 수 있으며, 이는 곧바로 사용자가 원하지 않는 정보의 외부 유출로 이어질 수 있다. 악성코드가 많이 퍼지는 메일의 경우 많은 메일 서비스에서 메일에 대하여 백신으로 안전성을 검사해주지만 P2P는 이러한 부분이 모두 개인에 맡겨지므로 사용자 부주의에 의한 악성 코드 공유가 문제시 되는 것이다. 다행히 메일에 비해 아직 사용자 수가 적고 단시간에 악성코드가 전파되는 경우는 없어 피해는 적은 편이다. 하지만, 앞으로 P2P 서비스가 더욱 대중화되고 사용자 수가 늘어난다면 문제가 커질 수 있다. 특히 최근 발견되고 있는 웜은 메일, 공유 폴더, 메신저에 이어 P2P 서비스를 자신의 전파에 활용하고 있는 추세이기 때문에 P2P 서비스에 대한 안전 문제를 더 이상 간과할 수 없는 것이다.[13] 국내에서 많이 사용하는 P2P 프로그램은 “소리바다”, “구루구루”, “당나귀” 등을 들 수 있다.



[그림 9] P2P 프로그램으로 검색한 화면

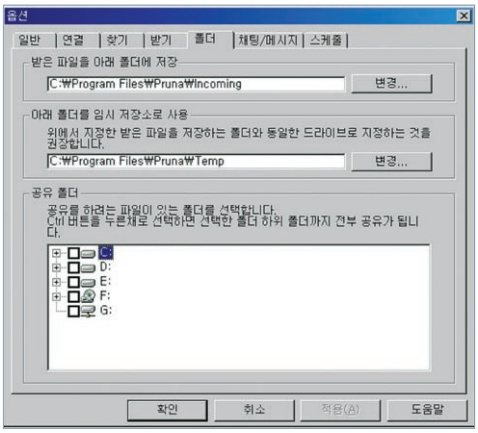
[그림 9]는 P2P 프로그램으로 xls 문서를 검색해본 화면이다. 여기에 검색된 것들 중에는 기업의 정보가 담겨있는 문서로 추측되는 것들이 다수가 포함되어 있다.

웜 · 바이러스는 실행되면 시스템에서 사용하고 있는 P2P 프로그램을 검색하고 P2P 프로그램이 공유하는 폴더에 웜 · 바이러스를 복사하여 누구나 접근할 만한 파일명으로 변환하여 다른 사용자로 하여금 다운로드 받게 한다. 다음은 P2P 프로그램을 이용하여 확산되는 Worm.Win32.Doep가 사용하는 파일명의 일부로 게임패치나 시디키생성기 등을 가장하고 있다.

13 차민석, “Peer to Peer(P2P)와 악성 코드 : 보안/바이러스정보”, 안철수 연구소, 2002.7.23

- Starcraft BroodWar LAST Official Patch.zip
- Diablo KeyGen.zip
- The Sims 2 Full Downloader.zip
- Baldurs Gate 2 KeyGen.zip

물론 현재까지 P2P를 활용하여 정보를 유출하는 웜 · 바이러스의 예가 아직 보고된 바 없다. 하지만, P2P 프로그램이 가지고 있는 공유의 범위만 변경하는 웜 · 바이러스가 등장한다면 이는 어려운 일이 아니다. 예를 든다면, 앞서 사용했던 "프루나" P2P 프로그램의 경우 [그림 10]에서 보는 바와 같이 옵션 항목을 선택하면 공유의 범위를 지정하는 곳을 볼 수 있다. 만약 웜 · 바이러스가 이 같은 설정을 전체 공유로 변경하게 된다면 누구나 사용자의 자료를 가져 갈 수 있게 된다.



[그림 10] P2P 공유의 범위를 지정하는 옵션 창

3) 메일 확산시 정보 유출 공격

흔히 웜 · 바이러스가 메일로 확산될 때는 웜 · 바이러스 본체만 확산된다. 하지만, 이메일 웜으로 대표적인 I-Worm.Win32.Sircam은 감염된 PC에 존재하는 DOC, XLS, ZIP 파일중 하나를 웜 파일 끝부분에 붙여 자체적으로 내장되어있는 SMTP를 이용하여 메일을 보내는 특징을 갖고 있다.[14] 즉, I-Worm.Win32.Sircam 웜의 끝부분에 붙는 파일이 대체로 문서 파일들이기 때문에 정보 유출 가능성이 크다. I-Worm.Win32.Sircam에 의해 정보가 유출된 대표적인 사례로 우크라이나 정부의 비밀 문서가 인터넷 사이트인 www.for-ua.com을 통해 누출된 사건을 들 수가 있다.[15] 물론 현재 알려진 것은 우크라

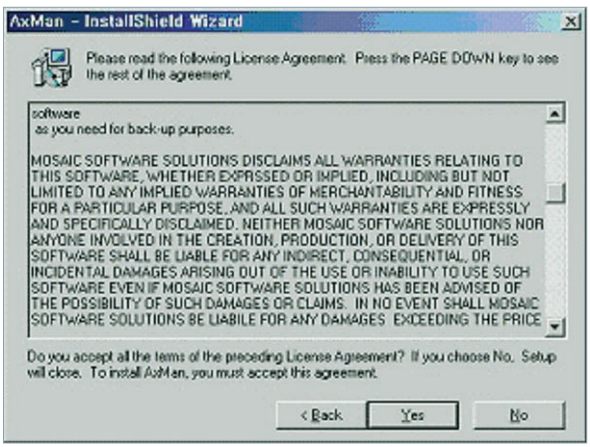
14 "I-Worm.Win32.Sircam 바이러스 정보", 하우리, 2001.7.19

15 "서캠바이러스, 코드레드보다 잠재위험성 더 커", 매일경제, 2001.8.3

이나 정부뿐이지만 분명 수 많은 기업들의 비밀 문서가 같이 누출되었음에 의심의 여지가 없다. 정보를 중요시 하는 요즘 이런 유형의 웜 · 바이러스는 계속적으로 나올 가능성이 크다.

다. 스파이웨어/애드웨어

스파이(spy)와 소프트웨어의 합성어로, 본래는 어떤 사람이나 조직에 관한 정보를 수집하는 데 도움을 주는 기술을 뜻한다. 광고나 마케팅을 목적으로 배포하는 게 대부분이어서 애드웨어(adware)라고도 불린다. 그러나 최근에는 다른 사람의 컴퓨터에 몰래 숨어들어가 있다가 중요한 개인정보를 빼가는 프로그램을 지칭한다. 대개 인터넷이나 PC통신에서 무료로 공개되는 소프트웨어를 다운로드 받을 때 함께 설치된다. 비교적 유용한 소프트웨어를 무료로 제공하므로 일반 해킹프로그램과는 성격이 다르다. 미국의 인터넷 광고전문회사인 라디에이트(Radiate)에서 개인 사용자의 취향을 파악하기 위하여 처음 개발되었다. 처음에는 사용자의 컴퓨터에 번호를 매겨 몇 명의 사용자가 광고를 보고 있는지를 알기 위한 단순한 것이었다. 그러나 최근에는 사용자 이름은 물론 IP주소와 즐겨찾는 URL, 개인 아이디, 패스워드까지 알아낼 수 있게 발전되어 악의적으로 사용될 소지가 많다. 문제는 사용자가 동의 절차에 민감하지 않는데 있다. 대부분 사용자들은 [그림 11]과 같이 프로그램을 설치할 때 보여지는 동의절차에 별 생각 없이 [예]를 클릭하는데 있다. 물론 영문일 경우 더 관심 있게 보지 않는다.



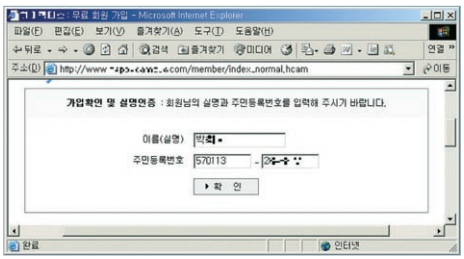
[그림 11] 프로그램 설치 동의 절차 화면

대부분 자신이 받고 있는 스팸(spam) 메일이 스파이웨어와 애드웨어에 의해 자신의 정보가 광고업체에 노출되었다고 할 수 있다.

라. 검색엔진에 의한 정보 유출

인터넷 검색엔진은 방대한 정보를 쉽게 찾을 수 있도록 하는 나침반임은 분명하다. 하지만, 인터넷 검색엔진의 대부분은 방대한 정보를 사람이 직접 인터넷을 돌아 다니며, 정보를 가공/분류하는 것은 아니다. 이때 사용되는 것이 웹봇(WebBot)이다. 웹봇은 자동으로 인터넷을 돌아다니며 정보를 가공/분류한다. 최근에는 정보의 가공/분류 기술이 발전하여 웹페이지 뿐만 아니라 pdf, doc, xls, hwp 등 문서 파일을 가공 분류하기에 이르렀다. 그런 이유로 검색엔진에서는 적절한 검색어만으로 기업의 정보를 유출할 수가 있다. 다음은 간단한 예로 최근 가장 많은 사용자가 사용하고 있다는 구글(www.google.co.kr)에서 주민등록번호중 앞부분에 해당하는 생년월일만 임의적으로 입력해본 것이다. [그림 12]에서 보는 바와 같이 쉽게 개인 정보로 추측되는 문서를 발견하였고 이를 통해 획득한 개인의 정보가 실명인지를 확인하고 있다. 인터넷에 문서를 잠시동안만이라도 올릴 때에는 해당 문서를 압축하여 암호를 설정해두는 것이 좋을 것이다. 그렇지 않다면 금방 웹봇이 지나가면서 해당 문서를 검색엔진에 정보로써 등록될 것이다.

[그림 12] 검색엔진에서 발견한 이름과 주민등록번호



[그림 13] [그림12]에서 얻은 정보로 실명 인증

Ⅳ 대안책

지금까지 기업정보 유출 유형 및 간단한 사례들을 살펴 보았다. 그렇다면 기업정보 유출을 막을 수 있는 최소한의 방법은 어떠한 것들이 있는가 알아보자.

1. 내부자 방어

내부자의 정보 유출이 외부자보다 위험한 것이 사실이지만, 내부자는 특별한 해킹 기술을 요하지 않고 쉽게 정보 유출이 가능함을 앞서 살펴보았다. 이런 내부자의 경우 그룹을 두어 정보에 접근하는 권한을 단계별로 설정해 둘 필요가 있다.

가. Secure OS

정보의 접근을 운영체제에서부터 조절하여 사용자별 권한을 두는 방안을 제시하는 운영체제이다. 운영체제 자체가 지원하면 좋겠지만, 현재의 운영체제보다 보안이 강화된 운영체제 플러그인 같은 프로그램을 구입, 설치해야지만 가능해진다. 보안이 강화된 운영체제는 사용자의 권한을 계속적으로 승계하여 작업하므로 부적절한 접근을 미연에 막아주기 때문에 내부자 보안에 효과적이라 하겠다.

나. DRM

DRM(Digital Rights Management)은 '디지털 저작권 관리'를 의미한다. 즉, 기업에서는 문서에 저작권을 부여하여 읽기가 허용된 사람에게만 문서가 공개되는 구조이다. 즉, 개발실에서 만들어진 프로그램 소스를 영업부에서 참조할 상황은 거의 없을 것이다. 따라서 이 프로그램 소스에 읽기 권한은 개발실로 한정한다는 의미이다. 물론 읽기 권한 뿐만 아니라 쓰기 권한, 프린터 권한 등 세세한 권한 부여가 가능하며, 회사에서 인가한 시스템에서만 해당 문서에 대한 권한을 가지게도 할 수 있다. 즉, 문서를 회사에서 인가한 시스템이 외부로 문서를 유출하여 문서 읽기를 시도할 경우 문서가 읽혀지지 않는다.

다. 메일 보안

메일은 업무에 있어서 상당히 중요한 부분을 차지한다. 따라서 메일을 사용하지 못하게

막을 수는 없겠지만, 첨부 파일에 대해서 적절히 조치를 취함으로써 기업정보 유출을 막을 수 있겠다. 이런 경우 동료간의 문서 교환은 메일이 힘들 수 있겠으나, 메일 서버의 적절한 셋팅을 통해 내부 메일 계정은 첨부파일을 허용하는 등의 방법을 사용하면 될 것이다.

라. 메신저 보안

메신저의 경우 가장 외부와 쉽게 연락이 되는 통신수단이다. 따라서 보안 관리자에게 민감하게 받아들여진다. 이 경우 공개된 메신저가 아닌 기업내 사설메신저를 도입하는 방법을 고려하는 것이 좋을 것이다. 이렇게 되면 기업내 동료간에 대해서만 메신저가 허용되므로 외부로 나갈 수 있는 정보 유출을 막을 수 있다.

마. 별도의 내부자 교육

기업정보 유출은 아무리 기술적인 측면에서 막더라도 내부자가 마음만 먹으면 얼마든지 가능한 일이 될 수도 있다. 따라서 기술적인 측면만을 고려하여 기업정보 유출을 막는 것에 무조건적으로 의지하기 보다는 내부자의 윤리 교육 등을 통해 처음부터 기업정보 보호에 대한 경각심을 갖도록 하는 것이 중요하다.

2. 외부자

가. 윈도우 보안 업데이트

해킹, 웜 · 바이러스는 제일 먼저 보안 취약점을 이용해 시스템 접근을 시도한다. 따라서 윈도우 보안 업데이트는 외부자에 대한 가장 기초적인 보안점검 사항 중 하나다. 윈도우 보안 업데이트에 접속하여 항상 보안 패치 프로그램을 확인하는 것이 가장 좋으며, 적용할 보안 패치가 없는 상태를 만들도록 노력해야 한다.

나. 최신 Anti-Virus 프로그램 사용

웜 · 바이러스를 가장 확실하게 차단할 수 있는 것은Anti-Virus 프로그램뿐이다. 따라서 항상 최신 버전을 유지하는 것이 무엇보다도 중요하다. 최근에는 하루에도 몇십개의

웜 · 바이러스가 등장하기 때문에 출퇴근에 맞춰 Anti-Virus 프로그램을 업데이트 하게끔 스케줄 기능을 활용하는 것도 좋은 방법이다.

다. 개인 방화벽 사용

임의적으로 해킹 시도를 차단하기 위해서 개인 방화벽 사용을 권장한다. 최근에는 Anti-Virus 프로그램의 일부 기능으로 개인 방화벽을 탑재하는 경우도 있기 때문에 개인 방화벽 기능이 탑재된 Anti-Virus 프로그램을 활용하는 것이 효과적이겠다.

지금까지 기업정보 유출의 유형 및 사례를 통해 적절한 기업정보 유출의 대안책을 살펴보았다. 물론 여기에서 제시한 대안책은 아주 일부분에 해당하는 것으로 이 밖에도 많은 대안책들이 존재하며, 더 좋은 기술적 접근을 통해 기업정보 유출을 막을 수 있을 것이다. 하지만, 앞서에서도 밝혔듯이 분명 기술적인 접근이 아무리 좋다고 하더라도 내부자의 보안의식 향상이 가장 중요하므로 수시 교육을 통해 이를 제고하여 기업정보 유출을 막는 방법이 제일 확실하다.