Bot Generator Analysis

July 27, 2007

n0fate@xstone.org

Warning

본 문서는 침해 대응 목적으로 제작되었습니다. 본 문서를 예방의 목적으로만 사용해주기를 바라며 문서에 기술되어 있는 프로그램을 이용한 불법적인 행위에 대해서 저자는 책임을 지지 않습니다. 본 문서를 사용하는 것은 이러한 내용에 동의함을 의미합니다.

Copyright

Document History

Version	Release Date	Amendent Contents
Ver 1.0	2007-07-27	Release

Special Thanks To

이 프로그램을 최초 포스팅하여 위험도를 알려주신 Coderant님과, 해당 프로그램의 분석을 위해 지원해주신 ZIZI님에게 감사드립니다.

목 차

그 림 목 차

I. 개요

1. 사건의 발단

7/26 일 경,Coderant 님의 블로그에 일에 다음과 같은 내용이 포스팅 되었다.

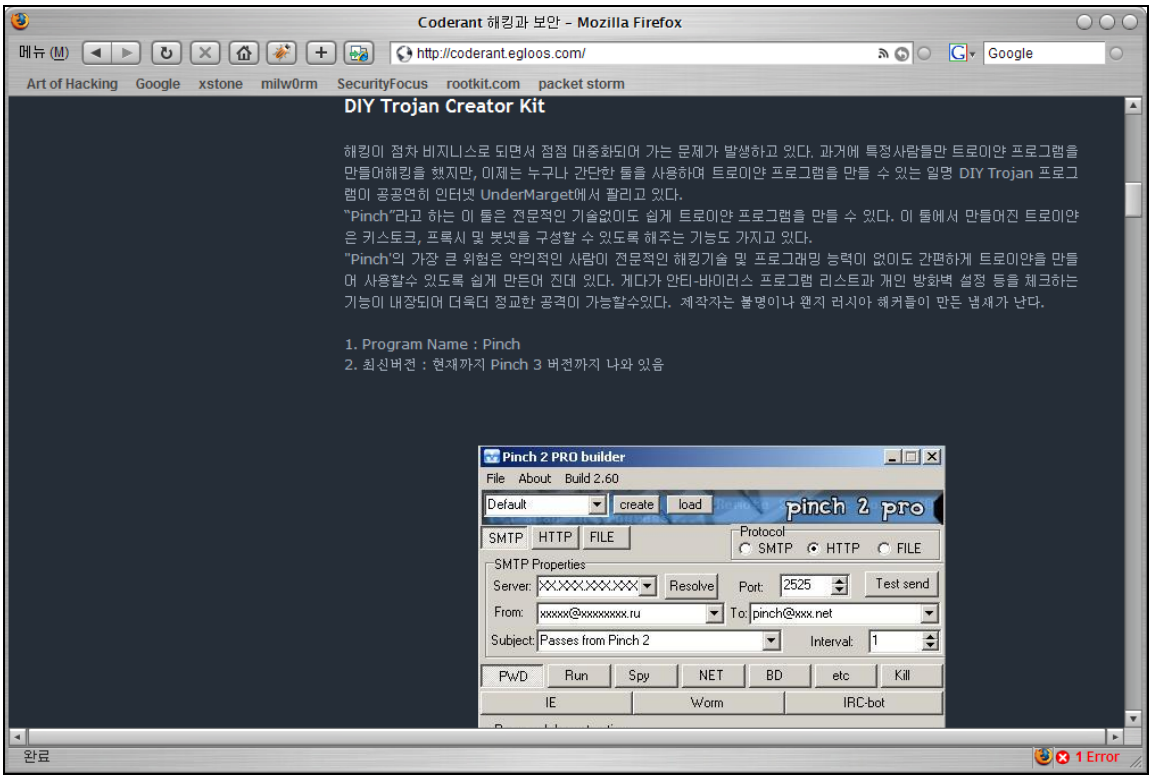

그림 1 - Coderant님 블로그에 포스팅된 내용

내용만 보면 저번 Download_Trojan_Generator(예명)이후 충격적인 일이 아닐 수 없었다. 단순 메뉴명 만을 봐도 키로거 기능, 백도어기능, 패스워드 추출 기능, 웜 기능, IRC-BOT 기능을 확인할 수 있다.

IRC-BOT 이란?

IRC-BOT 을 알기 전에 IRC(Internet Relay Chat)을 알아야 한다. IRC 란 일반적인 PC 통신과 비슷하지만, PC 통신은 개인적인 성격이 강한 반면에 IRC 는 IRC 클라이언트프로그램이나 IRC 클라이언트를 제공하는 서버에 접속하기만 하면 전세계의 어떤 사람과도 대화가 가능하다. (해당 채널 명이 없을 경우)각각이 채널을 생성할 수 있으며, 해당 채널이 있을 경우엔 해당 채널에 Join 하여 같은 채널에 있는 사용자와 대화, 파일전송 등의 일을 할 수 있다.

IRC-BOT 의 원래 의미는 해당 채널을 관리하기 위해 존재하였으며, IRC 는 기본적으로 해당

채널에 들어오는 유저들에게 guest 의 권한을 준다. 그리고 권한을 수작업으로 부여해야 한다. 만약 사용자가 잊어버리고 부여를 안 하게 되면 관리자가 없는 채널이 되어버릴 수도 있는 것이다.(실제로 이런 일이 많이 벌어진다.) 이런 현상을 막아주기 위해 Bot 은 몇몇 채널의 관리자가 들어왔을 경우 해당 관리자에게 권한을 할당해주는 등의 일을 수행하였다.

하지만 여기서 나타내는 IRC-BOT 은 조금 다른 의미로, 악의적인 사용자가 상대방의 PC 에서 실행된 IRC-BOT 이 공격자가 원하는 채널에 접속, 해당 BOT 에게 명령을 내려, 사용자 마음대로 조종할 수 있게 되는 것을 뜻한다.

해당 툴을 찾기 위해 Googling 을 실시, 해당프로그램의 신 버전을 구했지만, Public 버전으로 거의 테스트용 기능만이 사용 가능하였다.

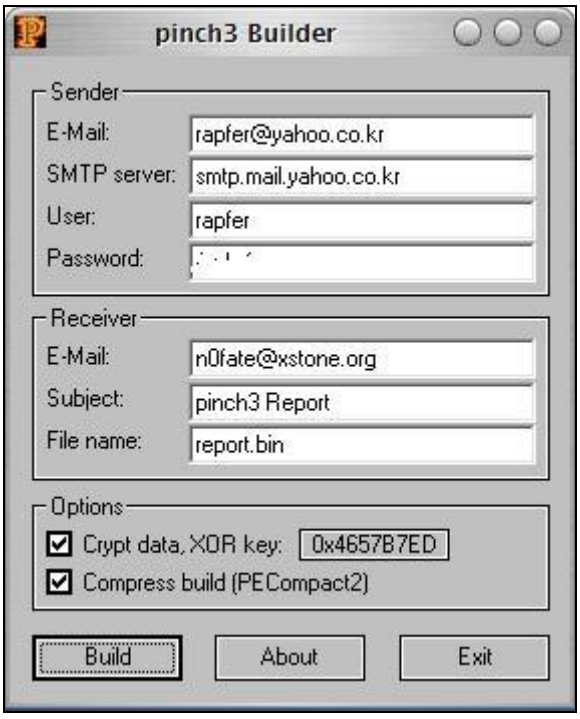

그림 2 - 간단한 기능만을 구현하는 Pinch3

이 Pinch3 는 간단하게 감염된 시스템의 드라이브 정보와 주요폴더의 위치정도만을 bin 파일로 제공한다.(Bin 파일은 Parser 라는 프로그램으로 내용을 확인할 수 있다.)

이 툴은 UnderMarket 에서 판매하는 툴이다 보니 모든 기능을 가진 툴을 구하기가 상당히 힘들었다. 그러던 중 ZIZI 님에게 모든 기능을 구현한 Pinch 버전을 받을 수 있었다.

II. Pinch 분석

1. 사전작업

우선 해당 프로그램의 구성을 확인할 필요가 있다.

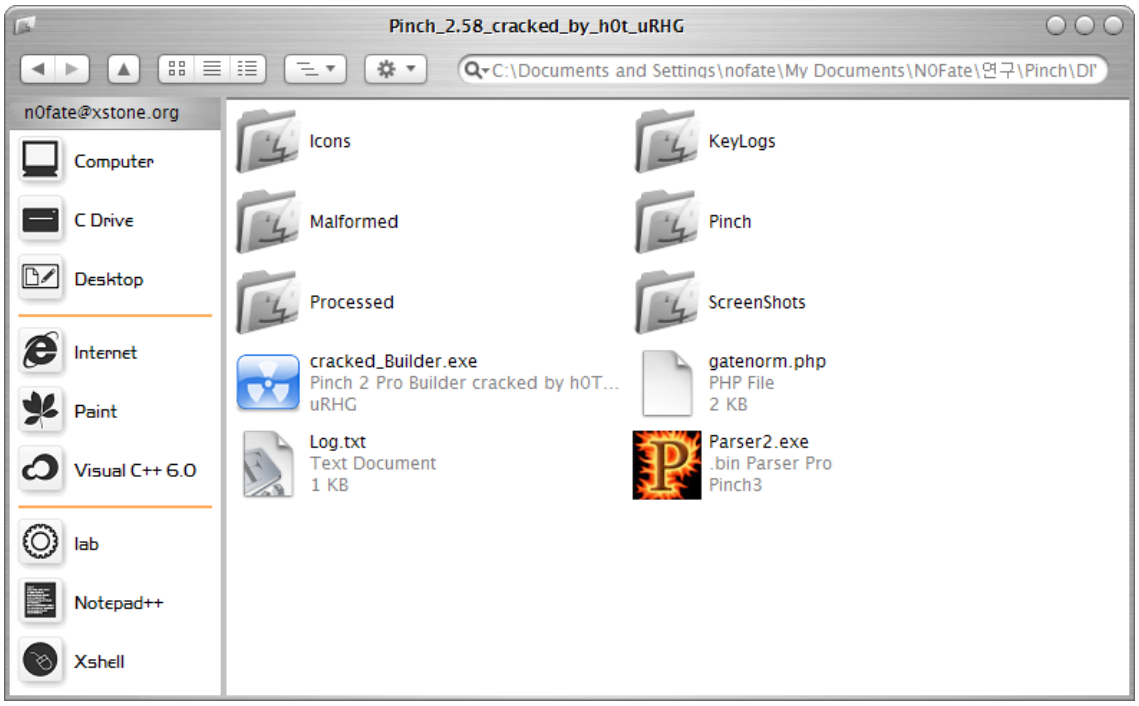

그림 3 - Pinch의 주요구성내용

각 파일의 내용은 아래와 같다.

Builder.exe : 실제적으로 악성코드를 생성시키는 역할을 하는 프로그램이다.
Parser2.exe : Builder 로 생성한 악성코드가 Victim System 에서 수행되면서 수집된 정보를 *.bin 파일로 제공하며 이 파일의 내용을 볼 수 있게 해주는 프로그램이다.
Gatenorm.php : Builder 생성시 해당파일의 경로(인터넷상의 경로)를 지정해주면 공격자 시스템으로 메일로 보내지 않고 Upload 방식으로 파일을 전송시키는 등의 일을 수행하게 해주는 파일이다. 물론 메일링 기능도 제공한다.

각각의 폴더에는 패커나, 각 세팅에 대한 설정체크파일(asm) 등이 들어있다.
이제 파일 내부를 들어다 보도록 하자.

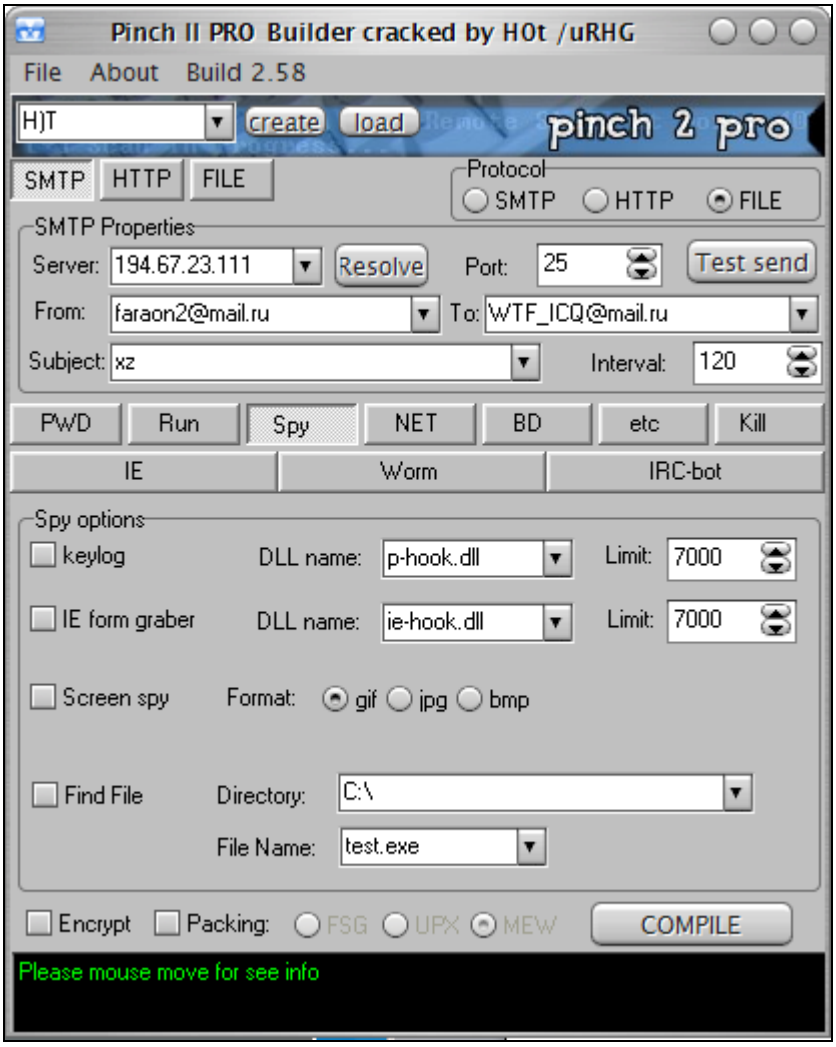

그림 4 – 해당 프로그램의 모습

위 화면에서 보면 알 수 있겠지만, 여러가지 기능을 가지고 있으며 각 내용은 아래와 같다.

PWD → 해당시스템의 프로그램 패스워드 획득 및 전송

Run → 실행프로그램에 등록기능

Spy → 키로거, IE form(아이디 패스워드 자동저장기능) 획득,

NET → 실행 시 해당파일다운로드 기능, PHP 파일을 이용한 파일 다운로드 기능 등

BD → Backdoor 설정

Etc → 아이콘이나 버전설정 등.

Kill → 실행시 Process Kill 기능을 실시한다.

IE → 피해자 피시의 Internet Explorer 설정을 변경한다. 신뢰하는 사이트와 즐겨찾기 추가, Host 파일 추가, 시작페이지, 검색페이지 설정 등의 기능을 설정한다.

Worm → 웜의 기능 수행

IRC-Bot → 봇 기능을 수행한다.

위와 같이 그 동안 많이 알려졌던 악성코드의 기능을 입맛대로(?) 선택하여 설치할 수 있는 것은 이 프로그램이 얼마나 위험한지를 알려준다. 당연히 저 위에 거론한 모든 기능을 수행하게 설정할 수도 있다. 간단히 check/input 을 수행한 후 COMPILE 버튼 한번으로 exe 파일 하나에 모든 기능이 들어가게 된다.
또한 Encrypt 와 Packing 기능을 통해 악성코드의 리버싱을 힘들게 하는 기능도 포함되어 있다.
위의 기능을 통해 빼낸 정보는 *.bin 이라는 파일명으로 smtp 방식의 메일전송이나, HTTP 로 remote Script 를 이용한 전송으로 설정할 수 있다.

2. 분석실시

위의 내용을 토대로 간단한 악성코드를 생성하여 확인해 보도록 하겠다. 이 악성코드에는 다음과 같은 기능을 심어 놓았다.

악성코드에 넣은 기능

IRC-BOT기능(채널 : #n0fatetest, 봇패스워드 : 1234)

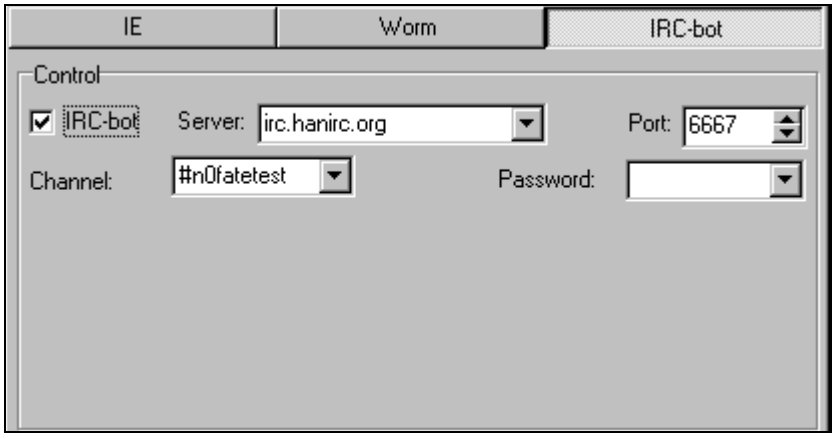

그림 5 - IRC-BOT기능 설정중

FTP BackDoor기능(12321 포트)

IE/Messanger KeyLogger

SMTP전송기능

피해시스템은 Windows 2000 Server Non-ServicePack(ENG) Version 이다.

VMWARE 에서 해당 악성코드를 실행하고 상태를 확인하였다. 우선 포트정보를 확인하였다.

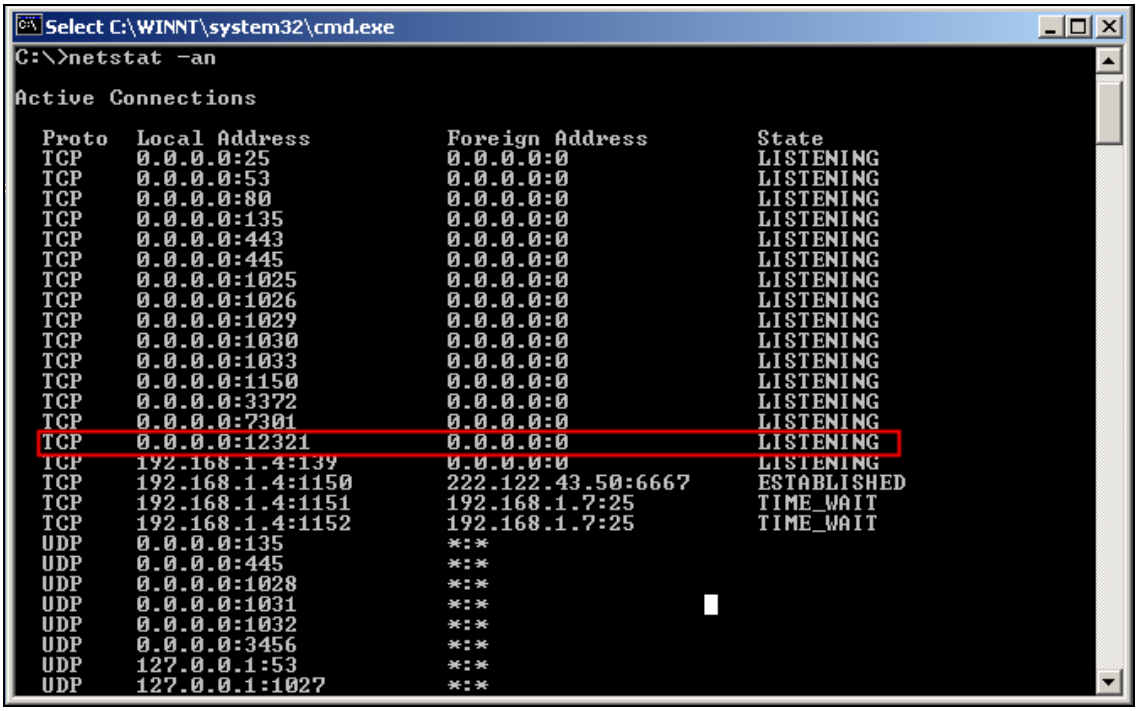

그림 6 - 오픈된 FTP Port

위와 같이 FTP 포트를 열려있는 모습을 확인할 수 있다. FTP 접속프로그램을 이용하여 확인해 보도록 하였다.

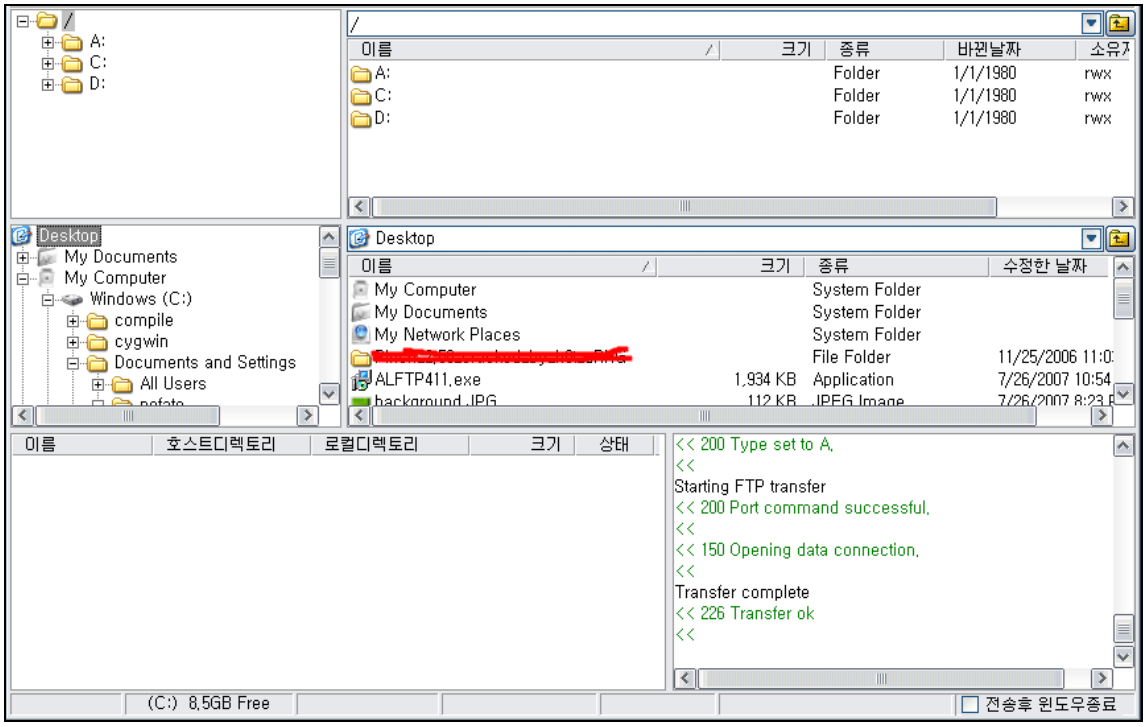

그림 7 - FTP클라이언트프로그램으로 접속한 모습

또한 실행 후 봇이 해당 IRC 채널에 접속하는 모습을 볼 수 있었다.

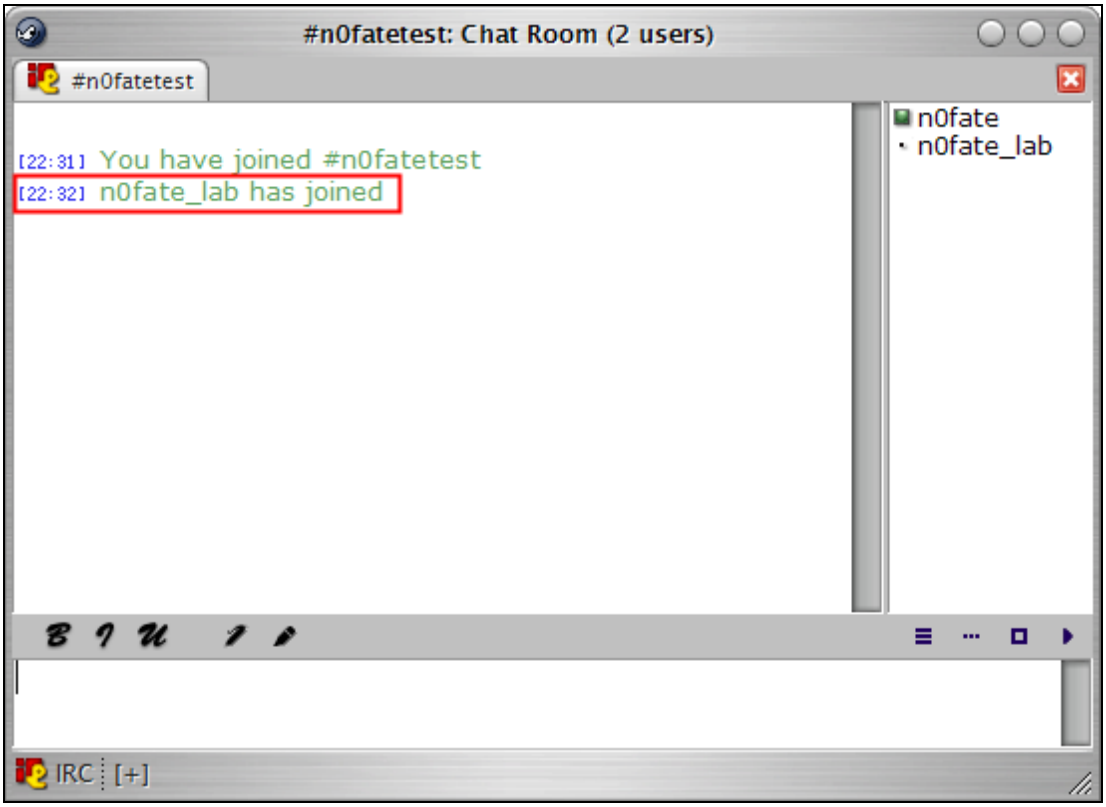

그림 8 - 접속한 BOT의 모습

해당 BOT 의 주요명령어는 아래와 같다.

.login <pass> ← 최초 로그인 후 봇 인증(설정했던 password 입력)
.die ← 봇을 죽인다.(봇을 제외한 임무를 수행한다.)
.download <url> ← 해당 url에서 프로그램(추가 공격코드 등)을 다운로드 한다.
.httpd <file> <port> ← 웹 서버에 지정한 port에 해당 파일을 올린다. 접속 시 자동으로 다운로드 창이 나타난다.
.proxy <id> <port> ← 해당 id 만을 허용하는 프록시 활성 포트 설정
.raw <text> ← 텍스트 내용을 출력한다.
.remove ← Bot을 제거한다.(자기자신을 삭제한다.)
.restart ← 자기자신을 재시작 한다.
.run <command line> ← 해당 console명령어를 실행시킨다.
.status ←현재 피해자 시스템의 정보를 보여준다.
.update <url> ← 해당 주소에서 Bot을 업데이트 한다. 동일한 파일명일 시 가능.
.visit <url> ← 해당 사이트에 방문한다.
.sp <url> ← IE의 시작페이지를 해당 url로 설정한다.
.msg <msg> ← msg에 입력한 내용을 메시지박스로 Victim에 보여준다.

.link <url> ← 해당 url을 즐겨찾기에 추가한다.
.scan <start address> <port> <delay> ← 해당 주소의 오픈 된 포트를 스캔한다.
.killthread <thread> ← 해당 쓰레드를 종료시킨다.
.shell <port> ← 해당 port번호에 Remote Connection을 대기한다.

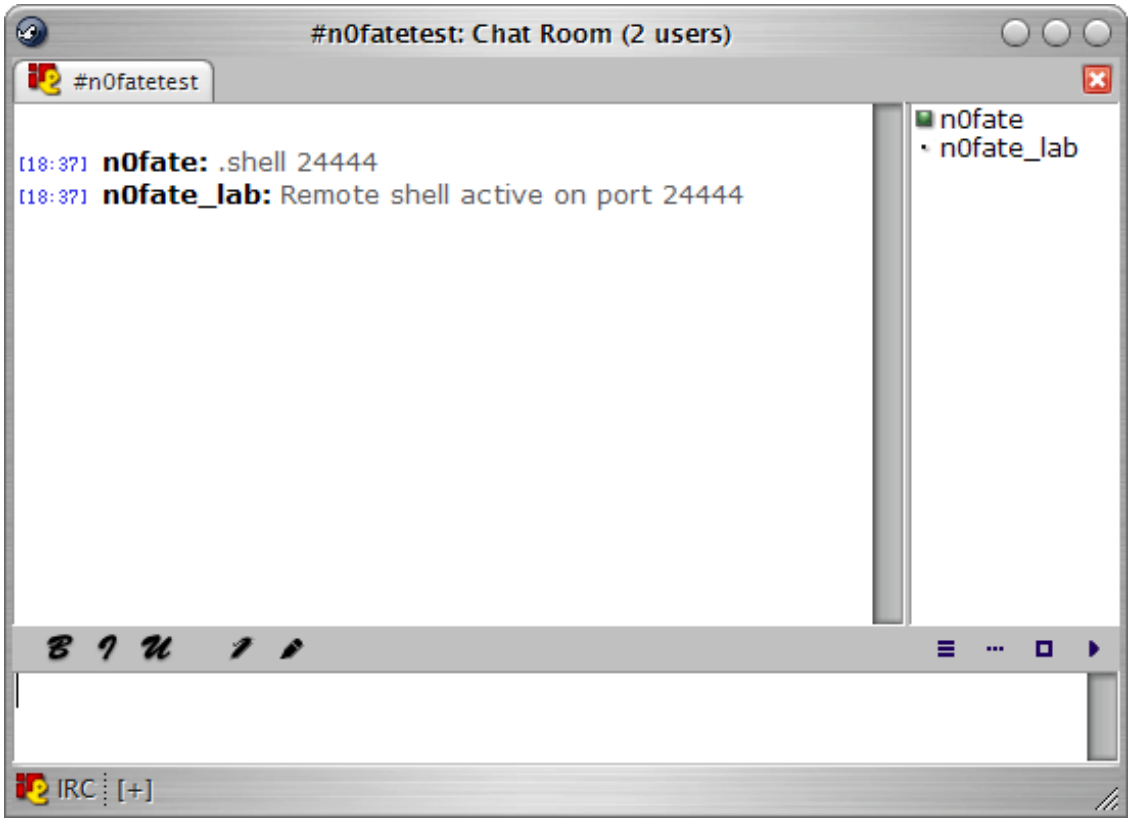

그림 9 - 명령어를 수행하는 모습

위에 나타난 것과 같은 많은 명령어가 존재하지만, 여기서는 간단하게 Bot 에게 명령을 내려, 리모트 쉘(.shell 명령어)을 이용한 접속을 확인해 보았다.

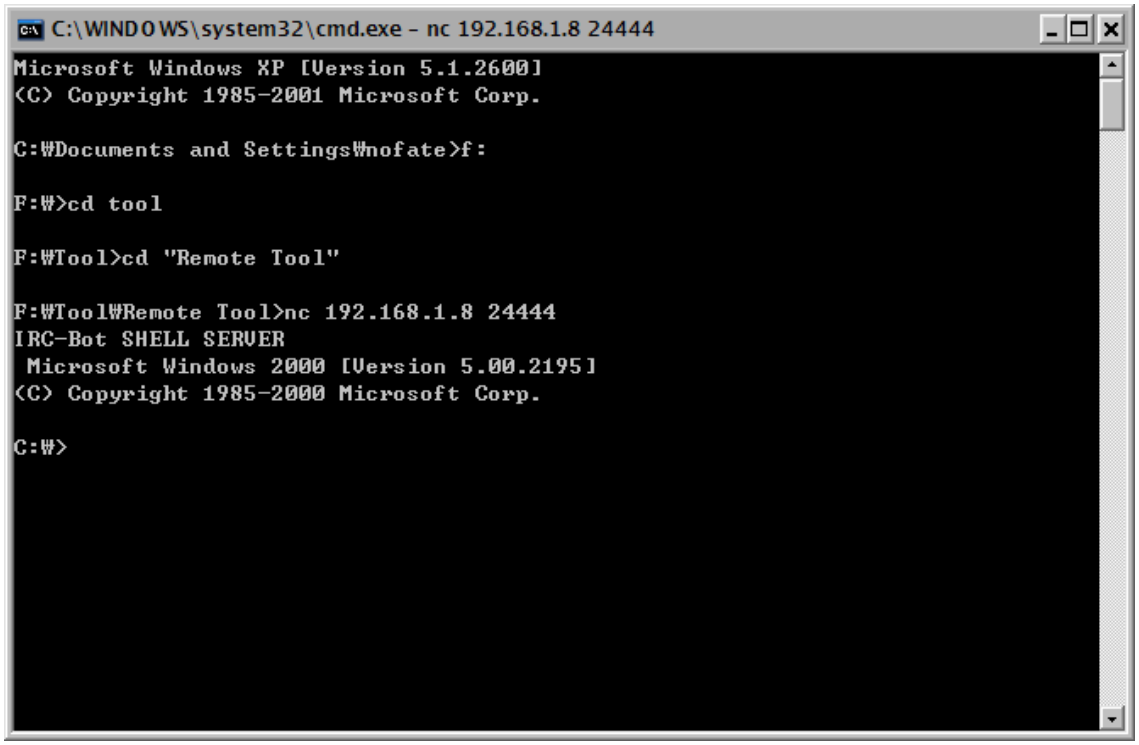

그림 10 - Remote Connection을 실시한 모습

위의 화면에도 나타난 것처럼 매끄러운 접속이 가능하였다.

또한 공격자의 메일서버로 지속적인 접속을 실시하여 메일을 보내는 모습을 볼 수 있다.

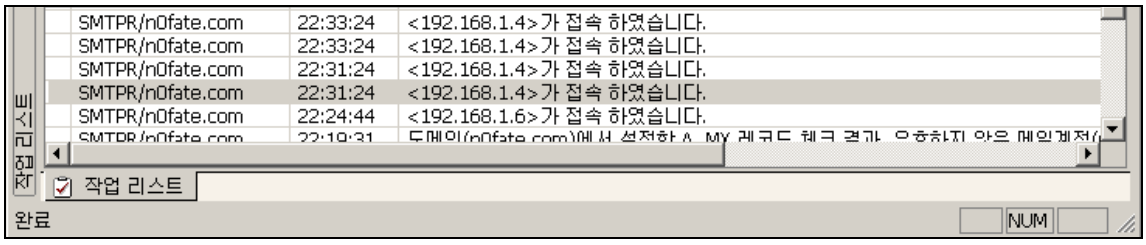

그림 11 – Victim System에서 SMTP접속로그내용

위와 같이 지속적인 접근을 하는 이유는 실행한 후 동일폴더에 ielog.txt 파일을 생성하여 인터넷 익스플로러의 키로깅 내역을 기록한다. 또한 처음에 설정해준 각 메신저/FTP 등의 키로거한 내용도 pass.bin 으로 저장해둔다. 즉, 이 파일들을 지속적으로 메일로 보내주기 위한 것이다..

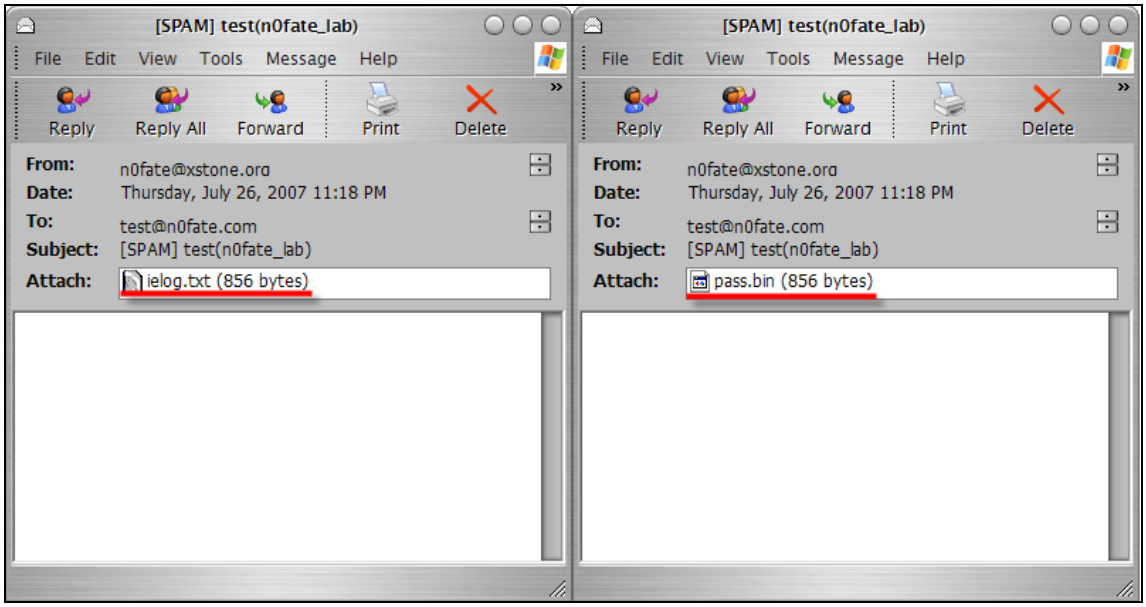

그림 12 - 넘어온 메일

ielog.txt 의 내용을 확인해보자.

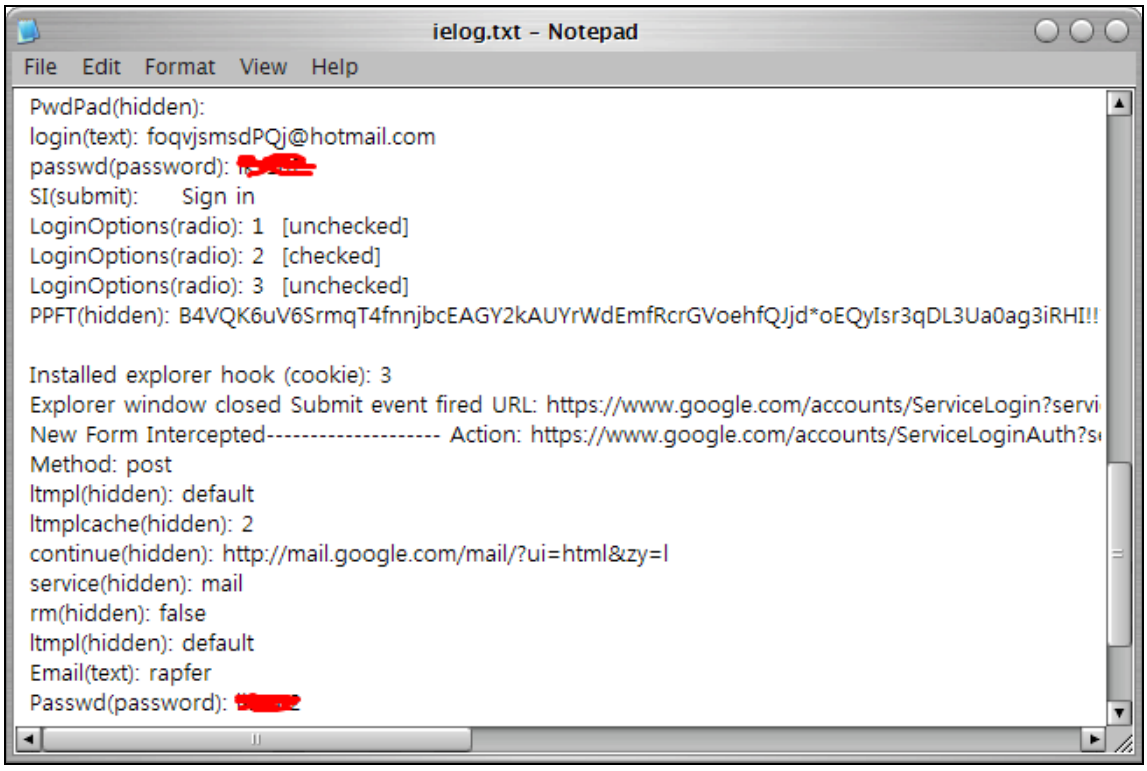

그림 13 - ielog.txt의 내용

위의 그림과 같이 인터넷 브라우저의 키 입력내용 및 쿠키을 후킹하여 획득하는 모습이다.

또한 pass.bin 을 이용하여 지정해준 메신저/FTP 서버의 아이디와 비밀번호를 확인할 수도 있다. 아래는 외국에서 ICQ 정보를 획득한 모습을 가져온 것이다.

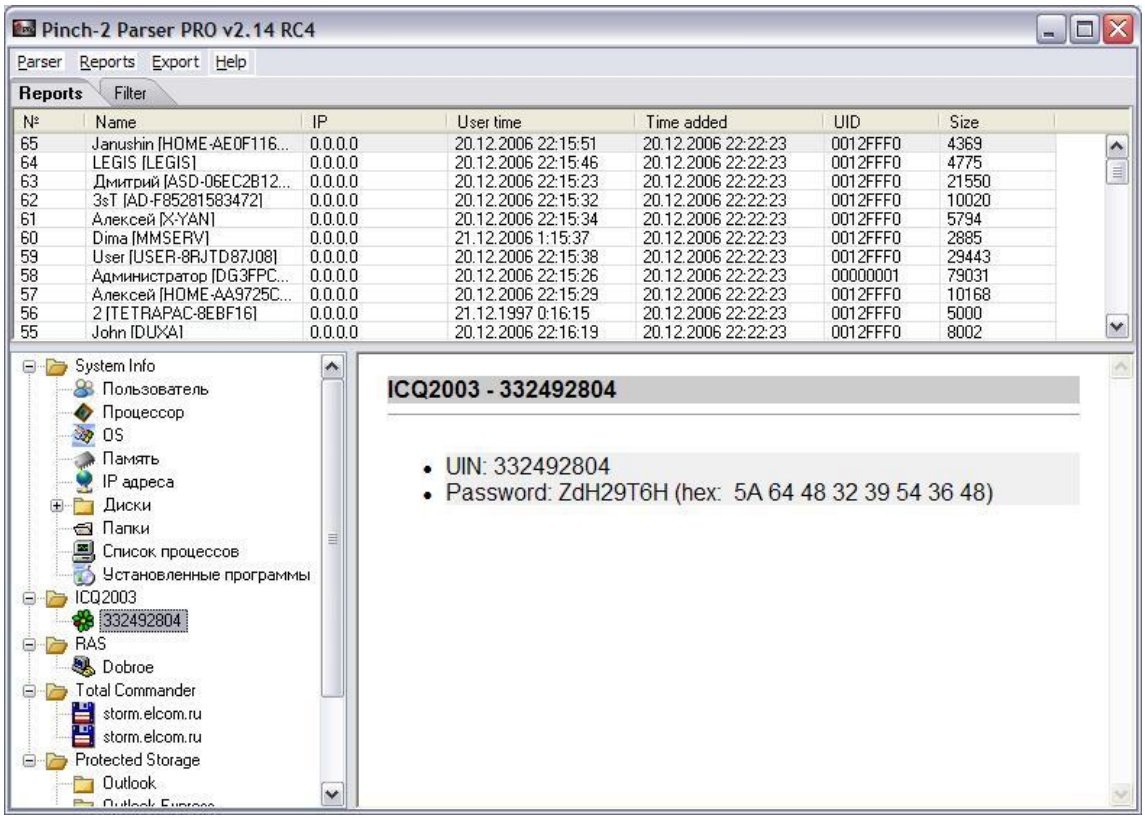

그림 14 - ICQ 계정정보획득

위 그림에 나와있지만, Parser 프로그램을 이용하여 해당 내용을 데이터베이스화 해서 보관을 하여, 지속적인 정보획득 등 계속된 피해를 입힐 수 있게 된다.

III. 결론

KISA 에서 2006 년 인터넷침해사고 동향 및 2007 년 전망(07.02.01 기재)에 대한 글이 있었다. 이 글의 내용을 보면,

"2007 년에도 봇넷을 이용한 악성행위는 지속될 것이다. 그중에서도 금전취득을 목적으로 하는 봇넷의 악용사례가 증가할 것으로 보이며, 이런 봇넷을 관리하는 악성 봇 C&C 서버를 그룹화해 운영하는 사례가 늘어날 것으로 예상된다. 또한 악성 봇의 전파방법의 변화가 예상되는데, 네트워크트래픽을 발생시켜 관리자에 의해 비교적 쉽게 발견·차단될 가능성이 높은, 스캔을 통한 전파방법은 감소하는 반면 악성코드 유포사이트 등을 통한 다운로드 전파방법이 증가할 것으로 보인다.
이 와 함께 악성 봇 자체의 기술적 변화도 2007 년에는 일어날 것이다. 그간 악성 봇은 IRC 기반이었지만, 보다 감지를 어렵게 하기 위해 변형되거나 암호화된 IRC 가 이미 발견되기도 했다. 이런 행위는 2007 년에도 지속될 것으로 보이며, 특히 Http 기반 악성 봇의 활성화 여부가 이슈로 등장할 것이다. 노명선 | 상황관제팀 팀장 nmsnms@kisa.or.kr
"

라고 기재되어 있다. 현재 이 봇 또한 동일 시스템에 악성코드를 다운로드 할 수 있는 시스템이 구현되어 있고, IRC 기능을 사용하지 않을 수도 있는 등, 다양한 방식의 공격이 가능하게 해준다. 또한 dll 파일을 이용, 후킹을 이용한 키로거의 기능도 가지고 있다. 즉 이 작은 프로그램 하나로 모든 악성코드의 기능을 다양하게 조합이 가능 한 것이다.

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.7.27.0	2007.07.26	Win32/IRCBot.worm.Gen
AntiVir	7.4.0.50	2007.07.26	TR/PSW.LdPinch.RW
Authentium	4.93.8	2007.07.25	Possibly a new variant of W32/IRCBot-based!Maximus
Avast	4.7.997.0	2007.07.26	Win32:Trojan-gen. {Other}
AVG	7.5.0.476	2007.07.26	-
BitDefender	7.2	2007.07.26	-
CAT-QuickHeal	9.00	2007.07.25	(Suspicious) - DNAScan
ClamAV	0.91	2007.07.26	Trojan.Fak
DrWeb	4.33	2007.07.26	DLOADER.IRC.PWS.Trojan
eSafe	7.0.15.0	2007.07.24	-
eTrust-Vet	31.1.5004	2007.07.25	-
Ewido	4.0	2007.07.26	-
FileAdvisor	1	2007.07.26	-
Fortinet	2.91.0.0	2007.07.26	-
F-Prot	4.3.2.48	2007.07.25	W32/IRCBot-based!Maximus
F-Secure	6.70.13030.0	2007.07.26	Trojan-PSW.Win32.PdPinch.gen
Ikarus	T3.1.1.8	2007.07.26	Trojan-Proxy.Win32.Webber.U
Kaspersky	4.0.2.24	2007.07.26	Trojan-PSW.Win32.PdPinch.gen
McAfee	5083	2007.07.26	New Malware.b
Microsoft	1.2704	2007.07.26	PWS:Win32/Ldpinch.gen
NOD32v2	2423	2007.07.26	a variant of Win32/PSW.LdPinch.RG
Norman	5.80.02	2007.07.26	-
Panda	9.0.0.4	2007.07.26	Suspicious file
Rising	19.33.32.00	2007.07.26	Trojan.PSW.LdPinch.e
Sophos	4.19.0	2007.07.26	Troj/LDPinch-JP
Sunbelt	2.2.907.0	2007.07.26	-
Symantec	10	2007.07.26	Infostealer.Ldpinch
TheHacker	6.1.7.154	2007.07.26	-
VBA32	3.12.2.1	2007.07.24	MalwareScope.Trojan-PSW.Pinch.1
VirusBuster	4.3.26:9	2007.07.26	-
Webwasher-Gateway	6.5.3	2007.07.26	Trojan.PSW.LdPinch.RW

Additional information

File size: 247808 bytes

MD5: a6b0ec181f58859dcf0d29cb857e4c89

SHA1: 74ea71658ca7199a62933d074acf011b5ab128d8

그림 15 - VirusTotal검사결과

필자가 테스트한 악성코드의 경우 VirusTotal 검사결과 31 개의 백신 중 20 개의 백신이 검출하였으며, 그중 몇몇 백신은 Bot 기능을 삭제하면 잡지 못하는 모습을 확인할 수 있었다.

문제는 이런 자동화된 생성 프로그램이 초보자, 소위 말하는 스크립키드(Script Kid)들도 손쉽게 강력한 악성코드를 제작할 수 있게 된다는 것이다. 현재 몇몇의 백신회사들의 경우엔 해당 툴을 구해서 분석, 모든 패턴에 대한 대응책을 준비했다는 것을 확인하였다.(위의 통계에서도 볼 수 있듯이 바이러스이름에 "Pinch"라는 이름이 들어감을 확인할 수 있다.) 이번 봇 제작프로그램은 필자가 블로그에 포스팅 한 내용처럼 언젠가는 백신 없이는 컴퓨터를 사용할 수 없는 시대가 올지도 모른다는 생각을 가지게 해준다.