

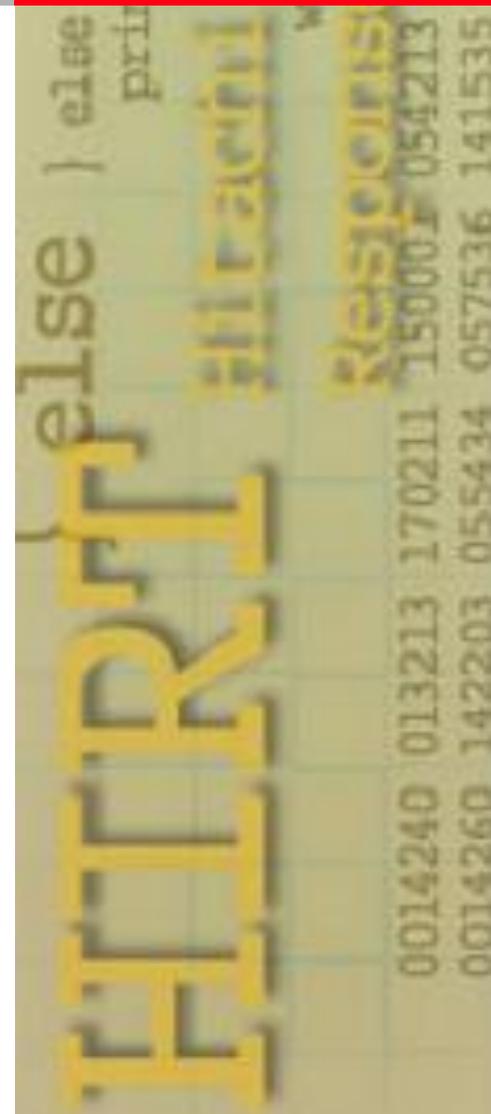
遠隔操作ツール RATの紹介

～Poison Ivy～

2012/05/25

Hitachi Incident Response Team

寺田 真敏



⇒ APT攻撃につながる機能改良

- 遠隔操作ツール (RAT) の進化
侵入したシステムを遠隔から操作するためのプログラム
潜伏活動や窃取活動で利用されている

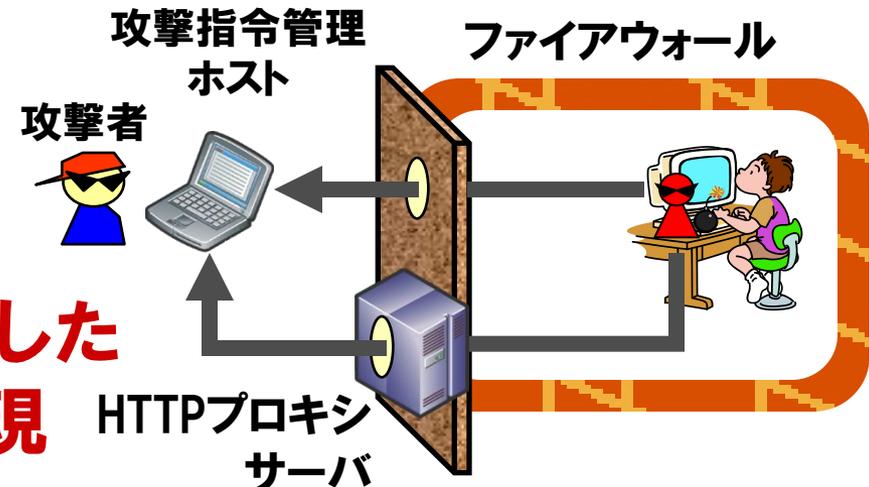
攻撃側発呼型から

- 2000年前後 BackOrifice、SubSeven など

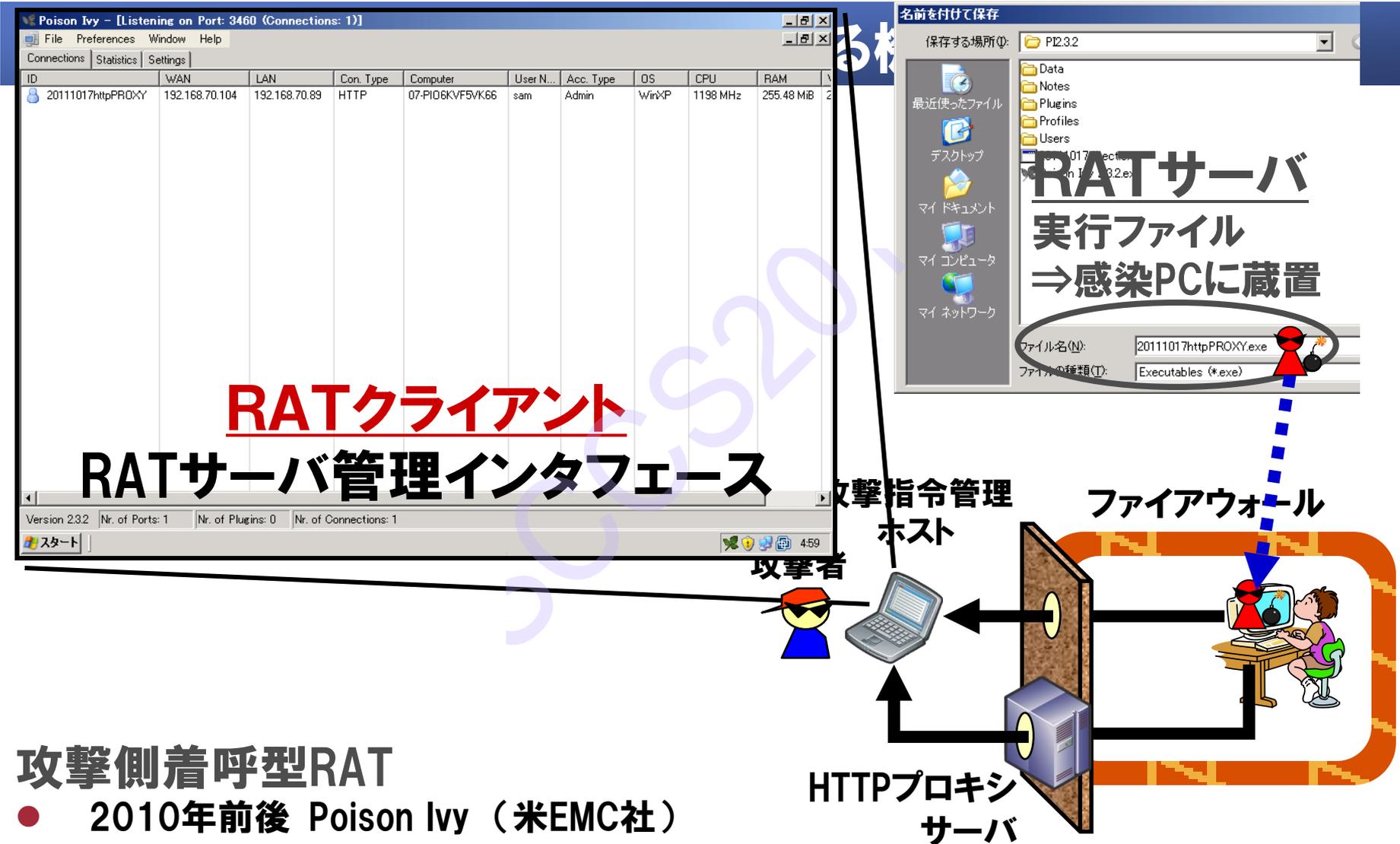


攻撃側着呼型へ

- 2010年前後 Poison Ivy (米EMC社)
MFC Hunter (三菱重工業)



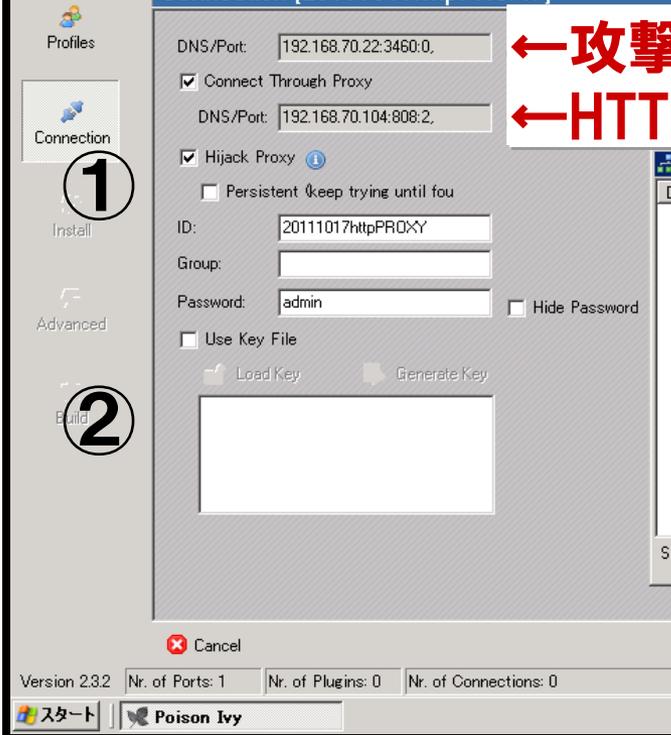
⇒ 潜伏中、ファイアウォールを介した
外部接続可能な通信環境を実現



RAT: Remote Access Trojan / Remote Administration Tool

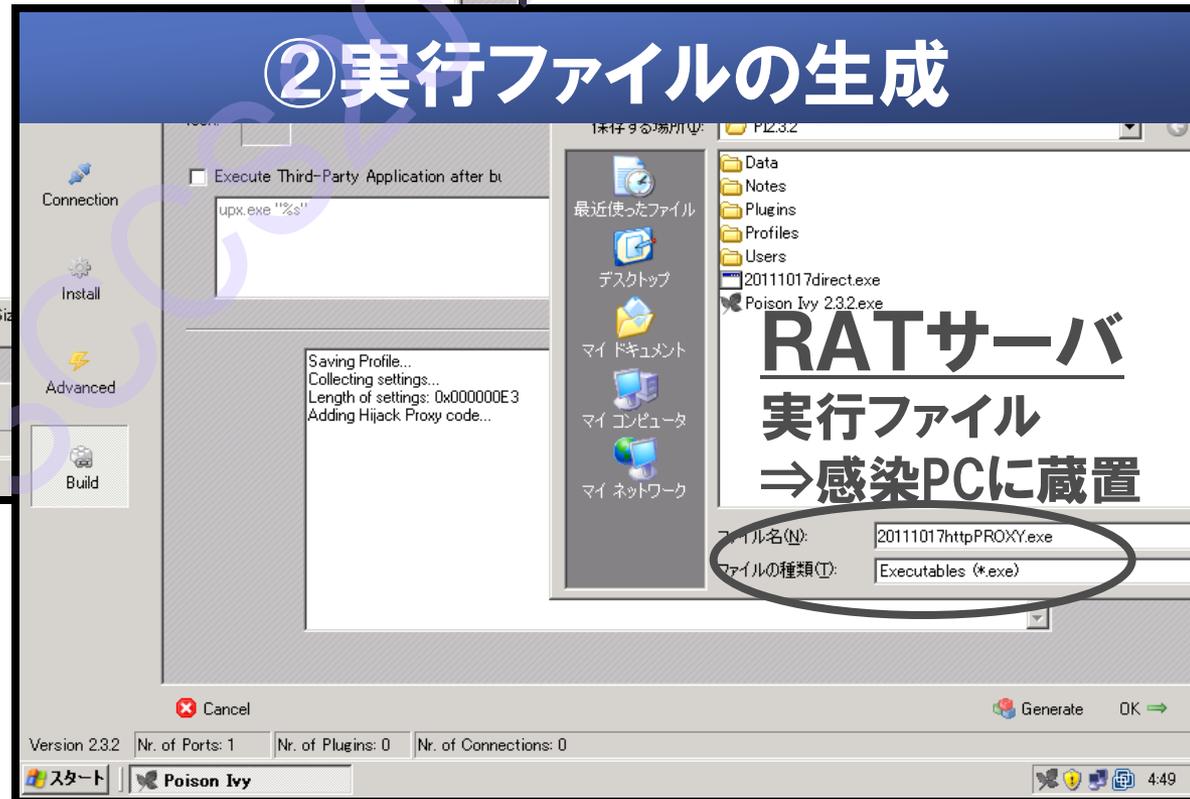
① 攻撃指令管理ホスト、中継の設定

← 攻撃指令管理ホスト
← HTTPプロキシサーバ

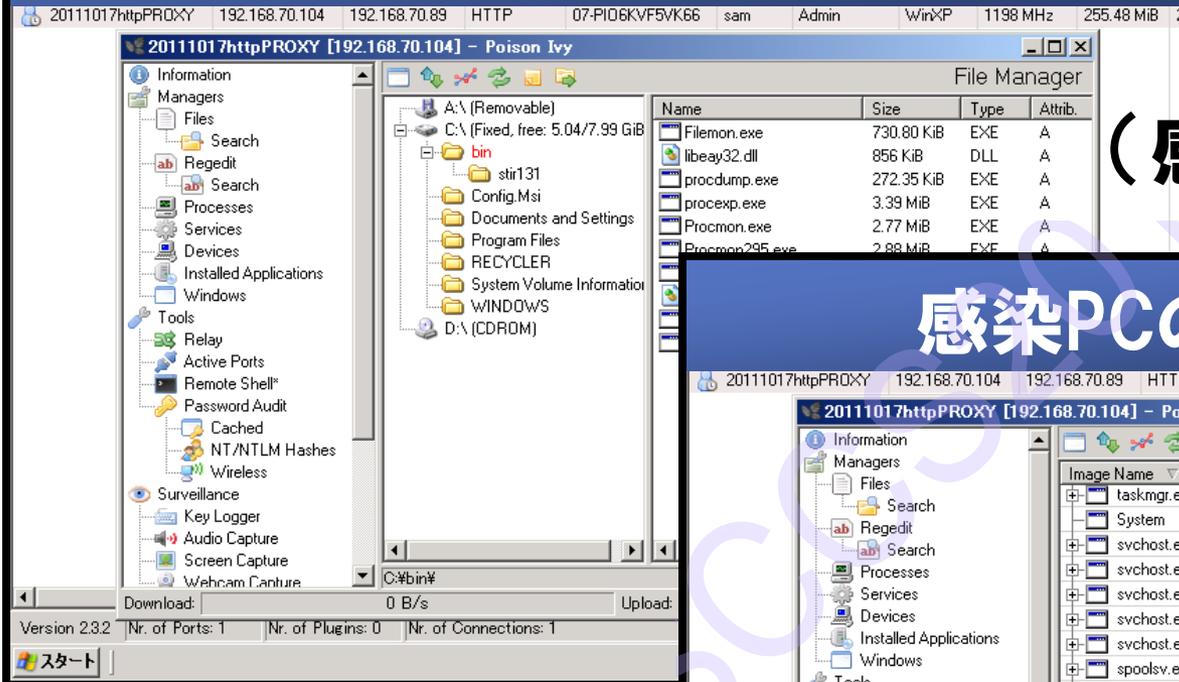


RATサーバの作成 GUIで2ステップ ほどの操作

② 実行ファイルの生成



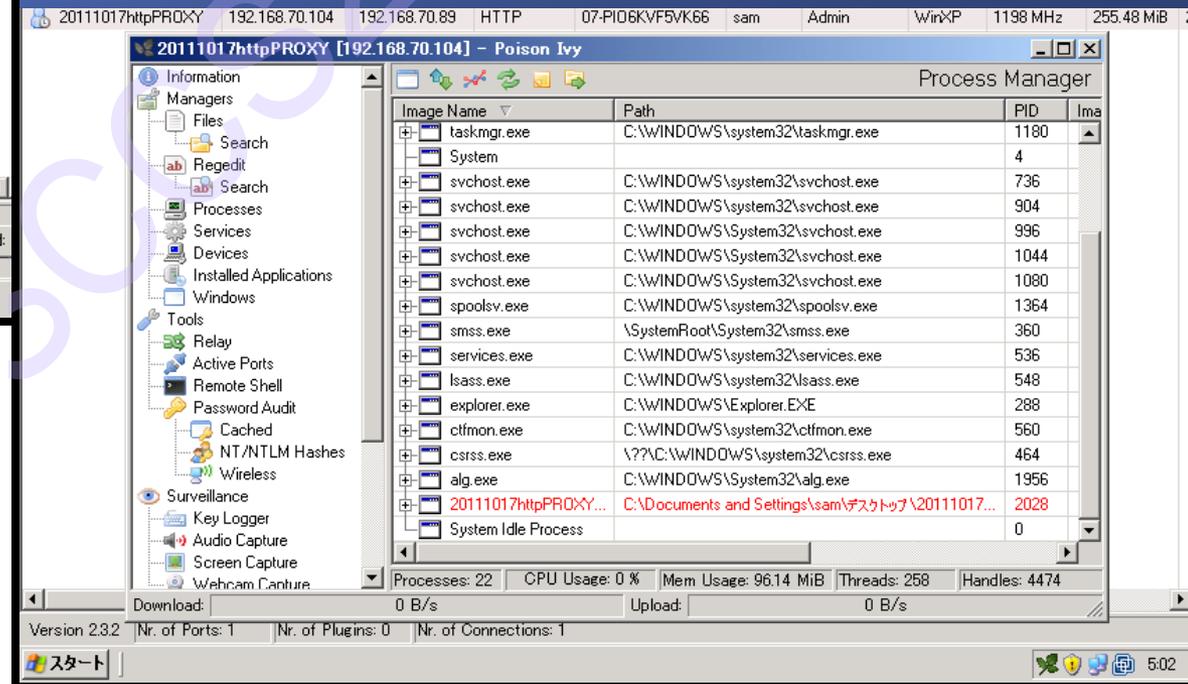
感染PCのファイル／フォルダ操作



RATサーバの 遠隔操作

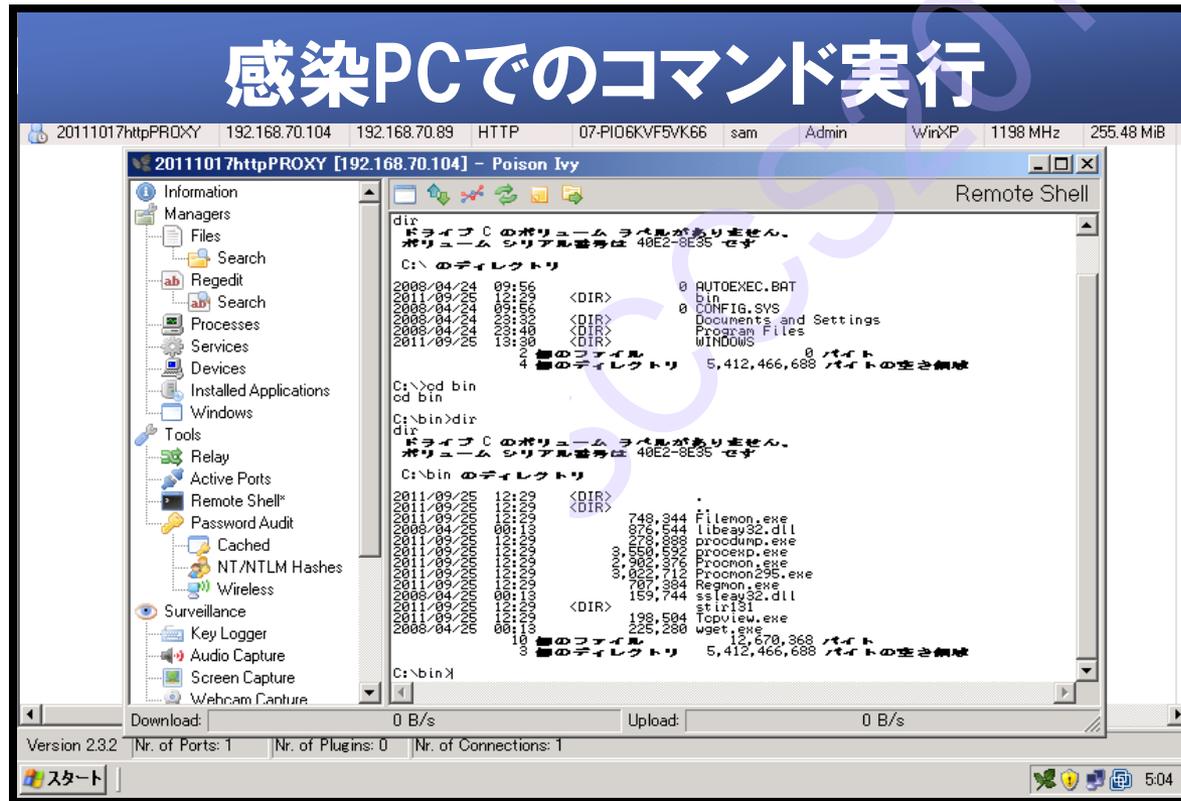
(感染PCの遠隔操作)

感染PCのプロセス操作



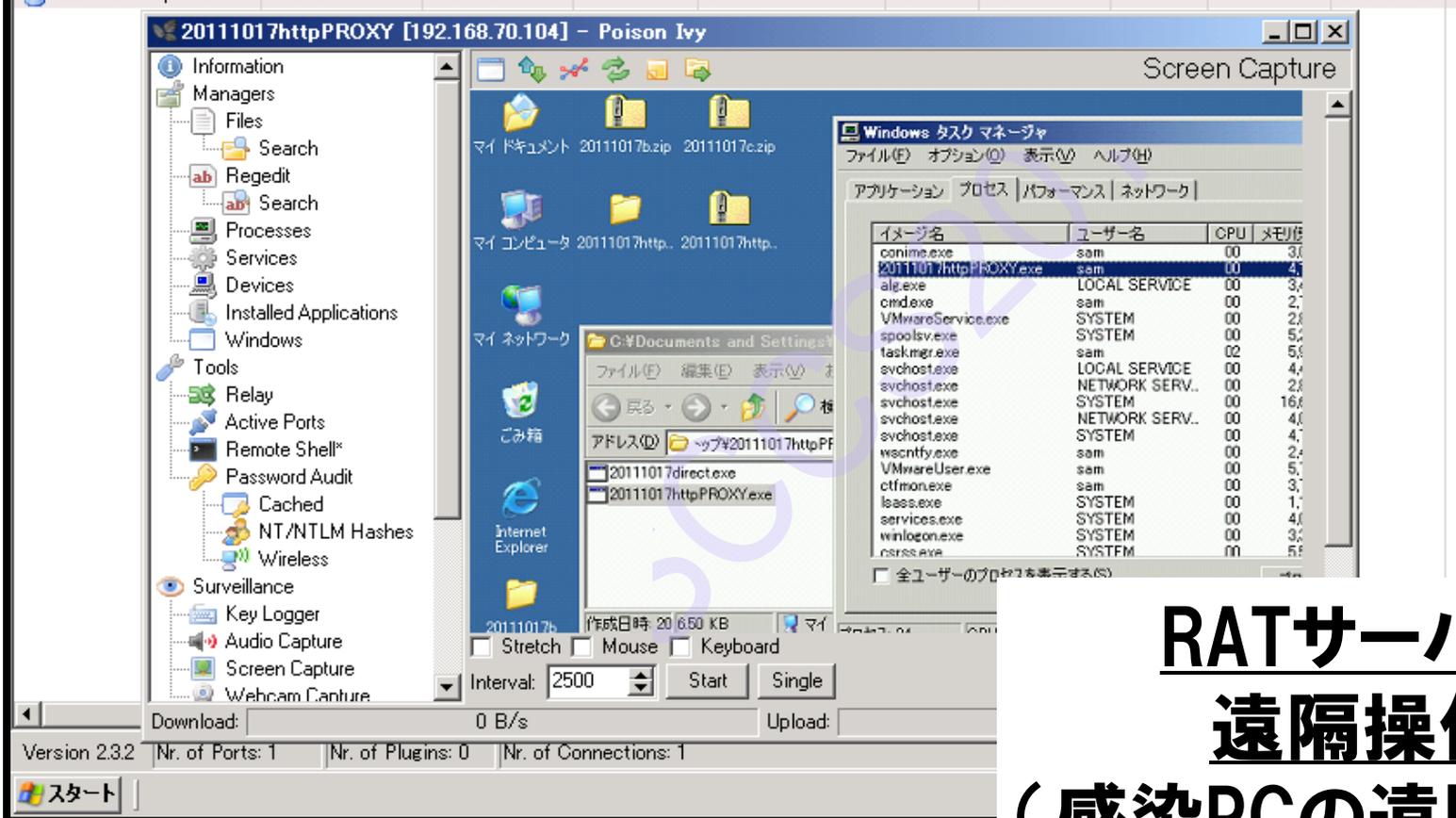
PCを直接操作して
いる状態と等価

RATサーバの 遠隔操作 (感染PCの遠隔操作)



感染PCの画面キャプチャ

ID	WAN	LAN	Con. Type	Computer	User N...	Acc. Type	OS	CPU	RAM
20111017httpPROXY	192.168.70.104	192.168.70.89	HTTP	07-PI06KVf5VK66	sam	Admin	WinXP	1198 MHz	255.48 MiB



20111017httpPROXY [192.168.70.104] - Poison Ivy

Windows タスク マネージャ

イメージ名	ユーザー名	CPU	メモリ
conime.exe	sam	00	3,0
20111017httpPROXY.exe	sam	00	4,0
alg.exe	LOCAL SERVICE	00	3,0
cmd.exe	sam	00	2,0
VMwareService.exe	SYSTEM	00	2,0
spoolsv.exe	SYSTEM	00	5,0
taskmgr.exe	sam	02	5,0
svchost.exe	LOCAL SERVICE	00	4,0
svchost.exe	NETWORK SERV...	00	2,0
svchost.exe	SYSTEM	00	16,0
svchost.exe	NETWORK SERV...	00	4,0
svchost.exe	SYSTEM	00	4,0
wscntfy.exe	sam	00	2,0
VMwareUser.exe	sam	00	5,0
ctfmon.exe	sam	00	3,0
lsass.exe	SYSTEM	00	1,0
services.exe	SYSTEM	00	4,0
winlogon.exe	SYSTEM	00	3,0
csrss.exe	SYSTEM	00	5,0

Screen Capture

Interval: 2500 Start Single

Download: 0 B/s Upload:

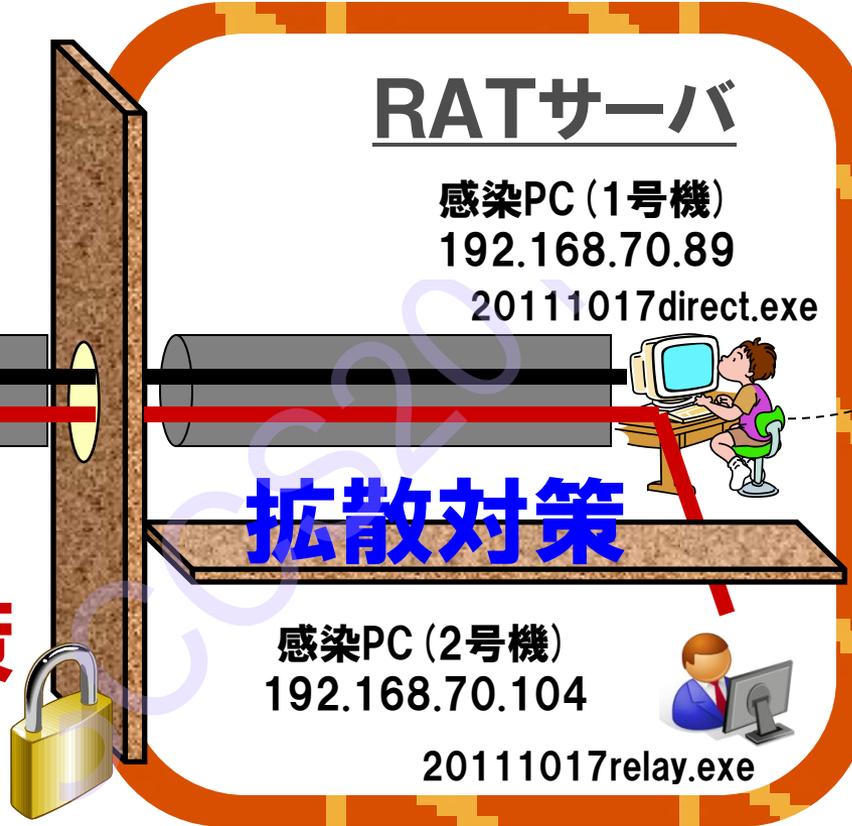
Version 2.3.2 Nr. of Ports: 1 Nr. of Plugins: 0 Nr. of Connections: 1

スタート

**RATサーバの
遠隔操作
(感染PCの遠隔操作)**

RATクライアント

攻撃指令管理
ホスト (RATc_adm)
192.168.70.22:3460



出口対策

感染PC (2号機) が直接外部と通信できない環境に設置されていても、攻撃指令管理ホストは、中継機能を使うことによって、攻撃指令管理ホストと感染PC (1号機) の通信路 (土管) を介して、感染PC (2号機) を遠隔操作できる。

出口対策例(設計での対策)

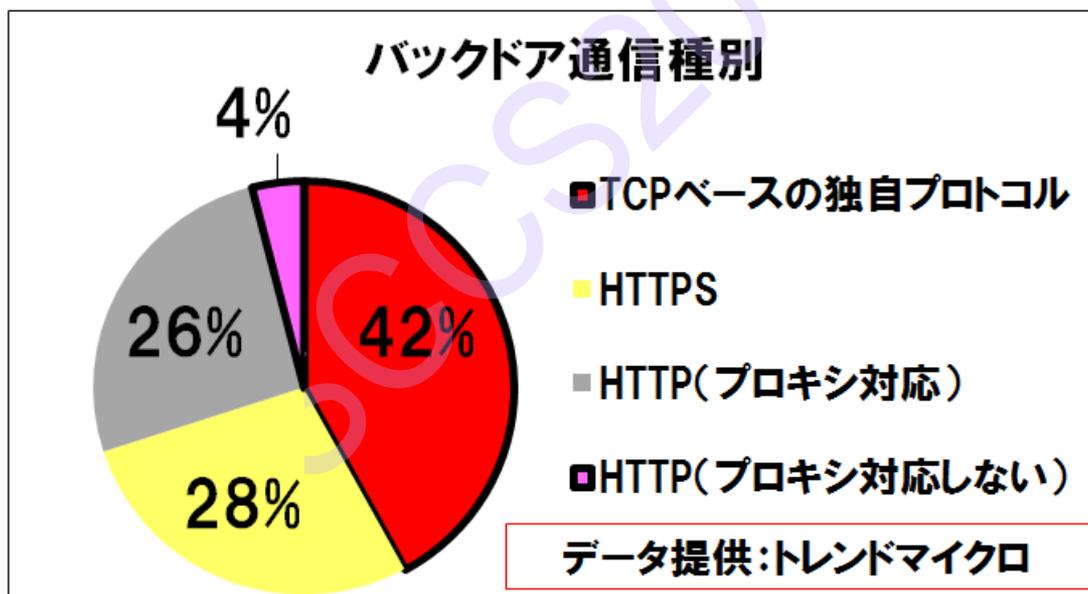
① サービス通信経路設計の効果

出口対策

IPA

■ FWでプロキシ経由以外の通信を遮断することで...

- TCPベースの独自プロトコルとHTTP(プロキシ対応しない)通信の46%のバックドア通信を遮断可能。



※2011年4月～10月国内で収集
標的型攻撃メールに添付されていたと思われるウイルス50個のバックドア通信サンプル

ivyrat-proxy_auth.pcap - Wireshark

No.	Time	Source	Destination	Protocol	Info
1	0	HTTPproxy	RATs_pc	HTTP	Continuation or non-HTTP traffic
20	35	RATs_pc	HTTPproxy	HTTP	CONNECT 192.168.70.22:3460 HTTP/1.0
21	35	HTTPproxy	RATs_pc	HTTP	HTTP/1.0 407 Unauthorized
22	35	HTTPproxy	RATs_pc	HTTP	Continuation or non-HTTP traffic
34	45	RATs_pc	HTTPproxy	HTTP	CONNECT 192.168.70.22:3460 HTTP/1.0
35	45	HTTPproxy	RATs_pc	HTTP	HTTP/1.0 407 Unauthorized
36	45	HTTPproxy	RATs_pc	HTTP	Continuation or non-HTTP traffic
48	55	RATs_pc	HTTPproxy	HTTP	CONNECT 192.168.70.22:3460 HTTP/1.0
49	55	HTTPproxy	RATs_pc	HTTP	HTTP/1.0 407 Unauthorized
50	55	HTTPproxy	RATs_pc	HTTP	Continuation or non-HTTP traffic
62	65	RATs_pc	HTTPproxy	HTTP	CONNECT 192.168.70.22:3460 HTTP/1.0
63	65	HTTPproxy	RATs_pc	HTTP	HTTP/1.0 407 Unauthorized

出口対策

10秒間隔

Frame 21 (182 bytes on wire, 182 bytes captured)

- 独自プロトコル。ただし、HTTPプロキシ越え(CONNECTコマンド使用)、Socks(v4対応)越えが可能である。
- **CONNECTコマンドで接続できるポート番号を80、443などに制限することも、接続性を妨害するという意味では、多少は効果がある。**
- Poison Ivy 2.3.2は、**認証型HTTPプロキシを越えることはできない。**
- **10秒間隔でHTTPアクセスがあることから、DENYログの監視も有効である。**

0060 0d 0a 50 72 bf 78 79 2d 41 75 74 68 65 6e 74 69 ..Proxy- Authenti
0070 63 61 74 65 3a 20 42 61 73 69 63 20 72 65 61 6e ..cater: Basic real