

A Novel Trojan Detection and Defense System

Ting Liu

XJTU InfoSec Society



OUTLINE

- Background
- Trojan Detection and Defense System
- Testing Result

Background

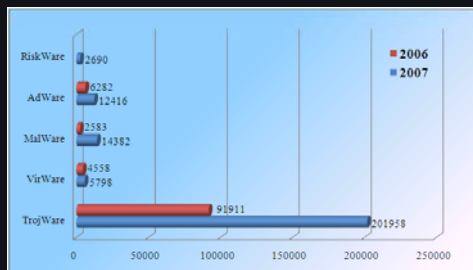
Underground Economy has been established

Sale, request and price of underground goods and services

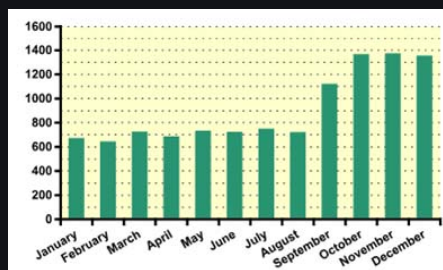
Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
Bank account credentials	18%	14%	\$10-\$1,000
Credit cards with CVV2 numbers	16%	13%	\$0.50-\$12
Credit cards	13%	8%	\$0.10-\$25
Email addresses	6%	7%	\$0.30/MB-\$40/MB
Email passwords	6%	2%	\$4-\$30
Full identities	5%	9%	\$0.90-\$25
Cash-out services	5%	8%	8%-50% of total value
Proxies	4%	3%	\$0.30-\$20
Scams	3%	6%	\$2.50-\$100/week for hosting; \$5-\$20 for design
Mailers	3%	6%	\$1-\$25

Background

Numerous unknown Trojans



Frequent Anti-virus update



1350 updates in October, once per half hour

“The number of new threats will again have doubled by the end of 2008” -- Kaspersky

Signature-based security product is not a good solution

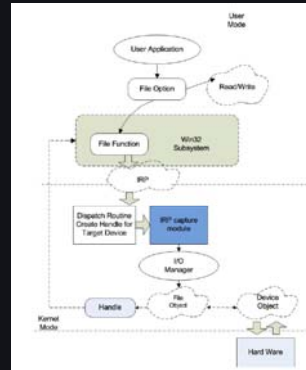
IRP Monitor Module

IRP (I/O request packet) monitoring

key information's data structure:

(Time, PI, FP, TR, RO, OI)

- ✓ Time: packet's creation time.
- ✓ PI: Information of the Process.
- ✓ FP: Path of the File.
- ✓ TR: Type of the Request.
- ✓ RO: Result of the Operation.
- ✓ OI: Other Information



API Evaluation Module

Feature Selection

API Names	Process Names										
	360Safe	Nero	ACDSee	KMPlayer	Maxthon	Trojan-Dropper Win32.VB.rj	Backdoor.Win32.Hupigon.bhes	Backdoor.Win32.Hupigon.bhof	Trojan.Win32.Buzus.gfl	Trojan.Win32.Agent	
CLSIDFromString	1	1	0	1	1	0	0	0	0	0	
SetCursor	1	1	0	1	1	0	0	0	0	0	
HeapFree	1	1	1	1	0	0	0	0	0	0	
ReleaseSemaphore	0	1	1	1	1	0	0	0	0	0	
Escape	1	1	1	0	1	0	0	0	0	0	
capGetDriverDescriptionA	0	0	0	0	0	1	1	1	1	1	
capCreateCaptureWindowA	0	0	0	0	0	1	1	1	0	1	
mouse_event	0	0	1	1	0	1	1	1	1	0	
SetLocalTime	0	0	0	0	0	0	0	1	1	0	
CreatePipe	0	0	0	0	0	1	1	1	1	0	

