The Market for Malware

Dr. Thomas J. Holt
Assistant Professor
Department of Criminal Justice
University of North Carolina at Charlotte
tjhol@uncc.edu
704-687-6081

Copyright 2007. All references to this work must appropriately cite the author, Thomas J. Holt.
Digital Crime Markets

• The problem of malware and computer based theft is increasing and becoming more complex
  – IC3 reports that spam and phishing complaints have increased over the past two years

  – CSI/FBI reports that virus contamination cost businesses $15 million and bot damages were estimated at $923,700 in 2006

  – Law enforcement agencies have begun to crack down on malware users and data thieves
    • Operation Firewall, Operation Bot Roast
TJX faces new suits over data breach

BY MARK JEWELL

BOSTON

TJX Cos. faces federal lawsuits in five additional states over a data theft that exposed at least 43 million credit and debit card numbers to potential fraud, according to a regulatory filing Thursday by the owner of stores including T.J. Maxx, Marshalls and A.J. Wright.

A quarterly filing said TJX was named in nine new lawsuits filed since the company's March 20 update on a theft believed to be the largest in the U.S. based on the number of customer records compromised.

The company filed suits Thursday in the Securities and Exchange Commission says complaints seeking class-action designation on behalf of customers were filed in Arizona and the federal courts of five additional states: Michigan, Missouri, Ohio and Texas.

Three new lawsuits were filed over the past two months, which are previously been brought earlier in the year. The suits in Alabama, California, Massachusetts, Pennsylvania and Massachusetts cases against Framingham-based TJX.

In addition to being TJX as a defendant, some of the suits listed T.J. Maxx, which processes some payment cards.

TJX said in Thursday's filing that it looks to a federal court.

TJX has said it will file a lawsuit to recover those credit cards.

The Associated Press

FBI finds over 1 million botnet victims

A series of recent attacks has uncovered additional incidents in which botnets have been used to facilitate criminal activity.

Michael Conney, NetworkWorld

Wednesday, July 13, 2007 11:03 AM EDT

The Department of Justice and FBI Wednesday said ongoing investigations have identified more than a million botnet crime victims.
Digital Crime Markets

• There are a range of websites, forums, and IRC channels devoted to malicious computer activity
  – Malware, carding, and stolen data

• These sites can provide direct information on current and emerging threats and the individuals responsible for their creation
  – Provides a snapshot of computer crime
Data

• Data generated from public web forums and studies actively involved in
  – Carding
  – Malware
  – Hacking and security

• Posts were examined along with any available materials provided in each forum
  – Machine translations
  – Human translators
Forum Structure

• The forums are structured to act as advertising spaces for the sellers and writers
  – Individuals post their products or services
  – Moderators review and verify products
  – Buyers post feedback or questions
  – Sellers answer and address comments
Customer Reviews of Malware

• Oleg
  – Thank you for a FreeJoiner, is the best program in its class I have ever seen, the result of the use was not long in coming, weaknesses and suggestions on the work simply no!

• f0rd
  – It is like this Joiner. The best of me once or seen many useful Fitch, Joiner make this one of the most powerful products on the market.

• Zolden
  – Anticipate just super, which was bought at the height. Works well, connects all the files without exception, to find a new attacker.
    P.S. Huge RESPECT sponsors of the programme.

• -=Humi™=-
  – Purchased a freejoiner 2 and left very happy….for each user, it's different ...
    Super Easy, Words can not explain.
    P.S. Greater Respect author of a remarkable tool!
Bots: Suicide DDoS Bot

- Suicide DDoS Bot by RKL a.k.a. Cr4sh
  - Control through web access and IRC
  - Botmaster controls can be separated at root user level in explorer.exe
  - ICMP, SYN, HTTP Flood
  - Injects code into trusted processes
  - SOCKS4 Proxy
  - Bindshell
  - Disguises itself in system through API intercept
  - Frequency ping bot
  - The bot is not detected by AV and can use any sort of packer for compression
Bots: Illusion DDoS Bot

- Illusion DDoS bot by Cyber Underground Project (CUP)
  - Is sold for up to $400, but older versions are available for free to members of some forums
  - Can control zombie machines through web access and IRC
  - Can be used for SYN, ICMP echo, UDP and HTTP GET Flooding
  - Can spoof IPs and use any source IP for flood command
  - Frequency ping bot
  - Multiple commands can be sent in one line via IRC separated by “|” symbol
  - Injects code into trusted processes
  - Disguises itself in system through API intercept
  - Bot password is coded by MD5 encryption to prevent “evil enemy” from learning your password and controlling the botnet
  - Has easy to use command interface
Bots: Illusion DDoS Bot

Binary: C:\Documents and Settings\Winux\Рабочий стол\BOTBINARY.EXE

IRC Administration
1) Host: 10.0.0.1 Port: 6667 Chan #chan Pass: 4test
2) Host: 10.0.0.1 Port: 6667 Chan #chan Pass: 4test

WEB Administration
1) Host: 10.0.0.2 Port: 80 Path: /webadmin/ Refresh time: 5 sec.
2) Host: 10.0.0.2 Port: 80 Path: /webadmin/

Default services:
- Socks4 port: 2240
- Socks5 port: 5420
- FTP port: 21
- Random range: 1025 - 2000
- Random range: 2001 - 3000
- Socks4
- Socks5
- FTP

IRC Access
BOT PASSWORD: qwerty

Options
- Install Kernel Driver
- Save services state in registry
- Colored IRC messages
- Auto OP admin on IRC channel
- Inject code if driver fails
- Add to autoload
- IRC server need password
- Bypass XP SP2 Firewall
- Flood Values

2006
Exit Save About
Trojans: Nuclear Grabber

• **Nuclear Grabber created by Corpse** ([http://corpsespyware.net](http://corpsespyware.net))
  
  – Can be purchased from corpse, but cracked versions are available

  – Practically UNIVERSAL TAN (Transaction Authorization Number) grabber
    • Any bank you choose can be a target

  – “Technology makes it possible to effectively gather TANs and more”

  – “Entire process of collection is realized without pop-ups, false pages, false communications and crashed browser at the critical moment.”

  – Product CAN make transfers (with another tan) and does not require immediate use

  – Also acts as a consummate phishing tool
Trojans: Nuclear Grabber

Nuclear Grabber drags forms, captures check and scroll box menus, and defeats virtual keypads.

All captured information is split into three data streams and sent instantly to both a selected server and redirected to the original domain.
Trojans: Nuclear Grabber

• There are limited instances of individuals selling data stolen using Nuclear Grabber

• D34th (posted 1.31.07)
  – At the given moment there is by 103 mb.
    Traffic - USA business. Nothing it touched from the lairs.

    I sell by the pieces:
    8 MB = 6.5 wmz
    13.0 MB = 10 wmz
    26.1 MB = 20 wmz
    26.8 MB = 21 wmz
    29.0 MB = 23 wmz

    I work only through the guarantee, or the patronage on 999 days.
Trojans: Pinch

• Pinch is a well known trojan that is frequently used for data theft

• The tool has gone through a variety of iterations
  – Originally sold by the creator, Coban2k, then the code was posted for free on-line
  – Latest version and custom builds can be purchased
Trojans: Pinch

• Pinch 2.99
  – Written in Assembler and is about 20K in size
  – No special knowledge is needed to use Pinch
  – Obtains passwords from over 33 different programs including RDP, Outlook, and The Bat!
  – Sends passwords to you encoded in a pass.bin file by HTTP, SMTP, FTP, or file on local machine.
  – Supports Socks5 and command shell via telnet.
  – Compile statistics about the machine.
  – Changes icons, binds itself to another executable, set starting page for internet browser.
  – Creates favorites in IE, kill processes or services
Trojans: Pinch

• Pinch 2.99
  – Adds listings information to the hosts file.
  – Cleans IE
  – Can turn into IRC-bot
    • Set server, port, channel and channel password
  – Starts as service, process, dll or other methods.
  – Hides itself from msconfig.
  – Start when online, specific time, or other.
  – Adds itself to Windows XP SP2 firewall allow list.
  – 4 Packers to choose from: MEW, UPX, UPACK, FSG
Trojans: Pinch

• Pinch can be customized for you and built for $30.
  – Guarantees that it will not be detected by antivirus when you buy it.

• Contact 123555 to buy a copy.
  – Revisions $5
  – Statistics server software bought separately ~$100.
  – Didn’t buy from 12355? Don’t contact for support
Trojans: Pinch

- New threads regularly appear with individuals selling stolen data obtained through Pinch
  - In a one week period in March of this year, five individuals sold stolen data obtained through Pinch
  - V-and-h-e
    Sales of data from Pinch,
    100 pieces of data= 3wmz
  - Aerot'ismo
    I sell the reports of pinch on the track to the price of 100- 2 Traff:
    Us, Uk, Ru, De, It.
    Bonus:
    * to the permanent buyers of reduction!
    * with purchase 500 (or more) reports, you obtain 100 more!
    iccQ - 947490
  - Kot777
    I sell the reports of pinch from 100 pieces for 2 wmz... traffic of miks, during the day there is near 2k- 5k of reports...
    ICQ 328498627
Trojans: Pinch

- Trojan Pinch.I Exim.
- You see our tariff plans to log (Records), the famous Trojan Pinch.
- We sell two types of logs:
  1) Information "booty" the main parser: passwords, auto IE and others.
  2) the information intercepted from the IE window, and others (very often hosting accumulators, with $ accumulation, etc.)

Price:
For one type of reporting: 100 pieces $ 1.5
the minimum order of 200 cards (ie, for $ 3)
The two types of reports: 1 mb., $ 0.3
Minimum order 20 mb. (ie $ 6)

Traffic reports:
Mostly Russian origin, in the direction of Europe about 39%, USA 15%.

Working through code protection or guardian. Reports are delivered in one hand.
Trojans: PG Universal Grabber

- **Power Grabber v1.8 Posted by Admin on 3.27.07**
  - Works with IE and browsers with IE based engine.
  - Works as loader, establishes necessary files, records in registry and deletes itself.
  - Invisible in processes, detours firewalls, invisible to AV.
  - Sends logs immediately after POST.
  - Loads files (Loads on UID bot. Can provide loading on other certain bot)
  - Updates old bots by new build (without restarting).

- **The full build costs $700 with antivirus protection for another $30**
  - Standard updates, bug fixes and optimization are free of charge.
  - Essential updates are charged (50 % from the added cost).
Trojans: PG Universal Grabber

Grabbing:
- http/https inquiries (paypal, ebay, banks, trade, etc...).
- FTP connections (Paths are saved in a separate file).
- Virtual FLASH/J.S. keyboards (By transfer POST’s inquiry, not ciphered).
- Keys Bank of America, and also keys of those banks which use system c *****keys (Deletes keys, answers to confidential questions are retrieved).
- Protected Storage (IE/Outlook, Autocomplete Passwords, Fields)

Work with E-Gold:
- Auto loading in e-gold
- Sends info (UID, IP, DateTime, Payee_account, Payer_account, amount) in a log and in admin right after loading.
- Knocks on icq after loading.
- Account number is retrieved from admin.
- After loading site is inaccessible.
*Trojan waits when holder accesses his account, then transfers 98 % on the account specified by you.
Trojans: PG Universal Grabber

**Work with TAN:**
- Uses remote access and adjustment from the administrator’s panel.
- TAN’s on DE are registered by default.
- Technology works everywhere with the similar work approach (Poland, Lithuania, Netherlands, etc). It is necessary to register name_site + name_TAN.

**Work with Redirect:**
- Uses remote control from the admin panel.
- Works with redirect using UID bot (After loading establish redirect on a page with a mistake).
- Page substitution (http: // Original/login.html => [you are a guest, you cannot view the page. Registration / Login].
- URL Substitution in an address line, the status of bar and page properties.

* By default the trojan is completed by fake Wellsfargo, BOA, cajamadrid, lloydstb, barclays.
Binding Tools: Free Joiner

• **Free Joiner Polymorphic by GIOFF**
  – First polymorphic joiner “without equal and worthy competitors in the network”

• The overall functionality:
  + Glued unlimited number of files of any format and content.
  + Glued to the minimum files (with the default values is 1K).
  + Glued file individual keys (transfer hidden files).
  + Dynamic of stabilizing the body (boot) in the process of compilation.
  + Location stabilizing the body, glued files and information on their location in one section of the file (complexity detects virus).
  + Very high speed unpack files at startup, regardless of their size.
  + The conservation options and settings last glue.
  + You can edit the resulting file to reflect information from other files (.exe, .dll)

General optional settings:
+ Select interface language (or Rus Eng).
+ The change icons (.ico, .exe, .dll).
+ Integrated package goes file (UPX, FGS, MEW, Petite, Upack).

• The full build costs 30 wuz, though a free download is available with less functionality.
Binding Tools: Free Joiner
Encryption Tools: SimbiOZ Cryptor

- **SimbiOZ Cryptor 1.x by 3xpl01t**
- Good day.
  I suggest you cryptor privacy. It is unique in the features
  Key features :
    - Encryption-executable files
    - Hiding file by intercepting API
    - Hiding process by intercepting API
    - Firewall not hang a change in the memory usage of injected code.
    - Source methodology for the selection of code injection can hide file
      and the process even under the unprivileged user, and not just
      under admin.
    - Hiding interception API some anti-rootkit programs (such
      RootkitRevealer)
    - Bypassing personal firewalls by masking agent under the annex
      (Svchost.exe)
    - Perhaps compress already encrypted file type Packers FSG.
    - The kit will include private Joiner.

Price : 10 WMZ, 2 updates for free.
Encryption Tools: SimbiOZ Cryptor
DDoS Services

- DDoS Service from hack-shop.org.ru

Competitors have started to press?
Someone stirs (prevents) to your business?
It is necessary to put out of action a site of "opponent"?

We are ready to solve yours
We offer service on elimination of not desired sites for you.

BOT-NET constantly increases!
Our bots are in different time zones that allows to hold constantly in online
Numerical army of bots, and in difference from other services - it is impossible to
close our attack on the country (for example to China :)).

1 hour - 20 $
24 hours from 100 $
Large projects - from 200 $ depending on complexity of the order.

Complexity of the order is defined/determined by width of the channel, filters, a
configuration of a server.
Forward the full sum undertakes...
Spam Services

- **Spam services from iNFEccTED-TeAM**
  - Respected ladies and gentlemen!
    we propose to your attention
    the straight post distribution of the letters of the advertising
    or information nature.

  Our address base: legal persons, organization, enterprise, the producers of goods and services,
  the specialized address base of data (personal selection, and also the start in it of your contacts).
  *Distribution is produced on exclusive software, developed by our command*

  iNFEccTED-TeAM

  It is professional, it is operational, it is qualitative.

  *our valuations:*

  **USA**

  1) US the partner
  Quantity --1 200 000
  Exclusive base.

  2) the physical persons
  Quantity --3 000 000
  Exclusive base.
ICQ Numbers

Individuals also regularly buy and sell ICQ numbers and tools

- **.ka$ta [ ICQ ] - 5d, 6d, 7d, 8d.**
- **5d:**
  - 4444x [ clean ] - $1500
- **6d:**
  - 4x444x [ clean ] - $150
  - 666xx6 [ clean ] - $300
  - 11x111 [ pm ] - $450
  - x22222 [ clean ] - $750
  - x00000 [ pm ] - $2500
- **7d-8d:**
  - 11111xx [ clean ] - $65
  - 1x111x1 [ inv ] - $55
  - 4444xx4 [ inv ] - $50
  - xx8888x [ inv ] - $50
  - 5x5555x [ inv ] - $50
  - x6x6666 [ inv ] - $50
  - 11Oct. 1111 [ clean ] - $170
  - 2222X22 [ pm ] - $160
  - 55X5555 [ i ] - $170

- **Tags from MakZer 'a**
- **XYZ**
  - 922242 - 20 wmz
  - 778717 - 17 wmz
- **Stairs**
  - 543-002 - 9 wmz
  - 313-789 - 8 wmz
  - 6-654-25 - 6 wmz
  - 475-234 - 5 wmz
  - 15-321-7 - 5 wmz
  - 6-345-06 – 4.5 wmz
- **XYZA**
  - 504242 – 6.5 wmz
  - 508804 - 6 wmz
  - 692009 - 6 wmz
  - 313108 - 6 wmz
  - 785572 - 5 wmz
  - 409477 - 5 wmz
  - 383404 - 5 wmz
Free Tools

• Many sites also provided access to free downloads
  – Older bots and malware
  – Password scanners
  – FTP checkers
  – ICQ tools
  – Proxy checkers
  – Articles
  – Exploits
  – Warez
Purchasing

• Individuals interested in purchasing products from a seller must contact them privately
  – ICQ
  – E-mail
  – Private messages in forum

• Buyers place orders and pay for services
  – E-gold
  – Web money (WM)
  – Western Union
  – Escrow payments
Organization of Market Actors

- There is an organizational continuum of sellers in malware markets based on seller reputation.

- Some forums maintain white and black lists to indicate who is trustworthy.
  - Rippers Database is also an important resource.
Market Forces in Malware Forums

• Four market forces shape relationships and actions in malware markets
  – Quick turnaround
  – Low prices
  – Reliable products
  – Customer service
Neutralizing Behavior

• Some sellers and writers made comments to negate their involvement in illegal activity

  – “the bot is a means of testing its network to the object of vulnerabilities, but not the tool for the attacks and other incorrect actions. For its use for any illegal purposes the author does not bear responsibility.”

  – “The programme was created for informational purposes and to check your own protection (security). The author is not liable.”
Discussion

• All manner of malware and information are being sold or made freely available

• Prices are generally low and the services available allow anyone to engage in computer crime and identity theft

• These markets operate much like legitimate businesses

• Malware writers and carders justify their actions much like other criminals
Complex Issues

- Law enforcement interdiction appears to have a small impact on the black market for malware

- May be difficult to attribute the creation of tools to any one individual or group

- The language barriers involved can obfuscate the content of forums

- A good deal of time, and skilled personnel are needed to monitor and analyze posts

- Transitory nature of forums and communications generally
<table>
<thead>
<tr>
<th>Russian</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Форум</td>
<td>forum</td>
</tr>
<tr>
<td>скачать</td>
<td>download</td>
</tr>
<tr>
<td>Закупка</td>
<td>purchase</td>
</tr>
<tr>
<td>Покупка/Продажа</td>
<td>purchase/sale</td>
</tr>
<tr>
<td>карт/кардинг</td>
<td>card/carding</td>
</tr>
<tr>
<td>счетов</td>
<td>account</td>
</tr>
<tr>
<td>Свалка</td>
<td>dump</td>
</tr>
<tr>
<td>Спам</td>
<td>spam</td>
</tr>
<tr>
<td>трояны</td>
<td>trojan</td>
</tr>
<tr>
<td>Личинка</td>
<td>bot</td>
</tr>
<tr>
<td>Червь</td>
<td>worm</td>
</tr>
<tr>
<td>Халява</td>
<td>warez</td>
</tr>
<tr>
<td>программа</td>
<td>program</td>
</tr>
<tr>
<td>хакер</td>
<td>hacker</td>
</tr>
<tr>
<td>wmz</td>
<td>web money (US)</td>
</tr>
</tbody>
</table>
Relevant Literature

- www.cybercrime.gov
Relevant Literature


