

# The Commercial Malware Industry

Peter Gutmann

University of Auckland

# Some History: The Numbers Racket

The numbers racket = Lotto before the government took it over

- Run through barber shops, groceries by local operators
- Bets were for cents
- Players chose a 3-digit number
- “Drawn” using the last 3 digits of the total amount bet on pari-mutuel racetrack betting machines

Seen as a harmless vice, no-one paid much attention to it

# Some History: The Numbers Racket (ctd)

Then organised crime moved in...

- Dutch Schultz took over from existing operators
- They weren't career criminals and were intimidated by explicit death threats

Dutch hired mathematician Otto "Aba Daba" Berman to fix the numbers racket

- Ensure that heavily-played numbers never won
- No-one had ever considered this level of attack
  - c.f. spammers hiring professional linguists
  - "We can't repel firepower of that magnitude"

# Some History: The Numbers Racket (ctd)

Once organised crime got involved, everything changed

The modern spam industry now is spread across the globe and has become infested by technically organised programmers from Russia and Eastern Europe, often in league with local organised crime syndicates

— Colin Galloway, *Asia Times*

Most of the big outbreaks are professional operations. They are done in an organised manner from start to finish

— Mikko Hypponen, F-Secure

Last year [2004] was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs [...] cybercrime is moving at such a high speed that law enforcement cannot catch up with it

— Valerie McNiven, US Treasury advisor on cybercrime

# The Spam Business

## Buy CDs with harvested addresses

- Prices vary depending on the quality
- Vacuum-cleaner for ~\$50, verified for \$x00

## Send mail via spam brokers

- Handled via online forums like [specialham.com](http://specialham.com), [spamforum.biz](http://spamforum.biz)
- \$1 buys 1000–5000 credits
- \$1000 buys 10,000 compromised PCs
- Credit is deducted when spam is accepted by the target MTA

# The Spam Business (ctd)

Broker handles spam distribution via open proxies, relays, compromised PCs, ...

- Sending is usually done from the client's PC using broker-provided software and control information
- Sources are obscured using spread-spectrum/frequency-hopping style techniques

This is a completely standard commercial business

- The spammers even have their own trade associations  
Nearly a third of users have clicked on links in spam messages. One in ten users have bought products advertised in junk mail [...] the fact that users are buying things continues to make it an attractive business, especially given that sending out huge amounts of spam costs very little

— BBC News

# The Carding Business

Prices are openly published or subject to private negotiation

- “CVV for \$1, CVV with SSN for \$10, bank account \$50, ...”
  - “CVV” implies full CC details down to the CVV level
- Some sources give bulk discounts for larger CVV purchases

Carders have ebay-style reputation rating systems

- #rippers on carder IRC nets

# The Carding Business (ctd)

Card checks are performed via IRC bots

- `!chk cardno expiry`
- `!cclimit cardno`
- `!cvv2 cardno expiry`
  - CVV is the 3-4 digit crypto checksum on the back of the card
  - Required as an extra check by some merchants
- This is more sophisticated than many merchants!

# The Carding Business (ctd)

User identities are hidden via IRC proxies (bouncers) on hacked PCs

The trade of BotNets on compromised machines is becoming an industry in itself. Organised crime is making use of this industry

— Detective Chief Superintendent Les Hynds,  
head of the UK National Hi-Tech Crime Unit

Funds are moved into drops

- Compromised bank accounts used to launder funds
- Scammers are big fans of online banking, especially via other people's accounts

# The Carding Business (ctd)

## Cashiers cash out the contents of the drops

- Take 50% of the funds to move the money out via services like Western Union
- Many, many ways to cash out the funds. Example: Find a business with \$10K of debt, agree to pay them \$20K if they cash out 50% of the funds

## System works like an open labour market

- “Need spammer to fill Hotmail boxes, will pay through percentage of phishing proceeds”
- “Will trade CVV2 for web site account”

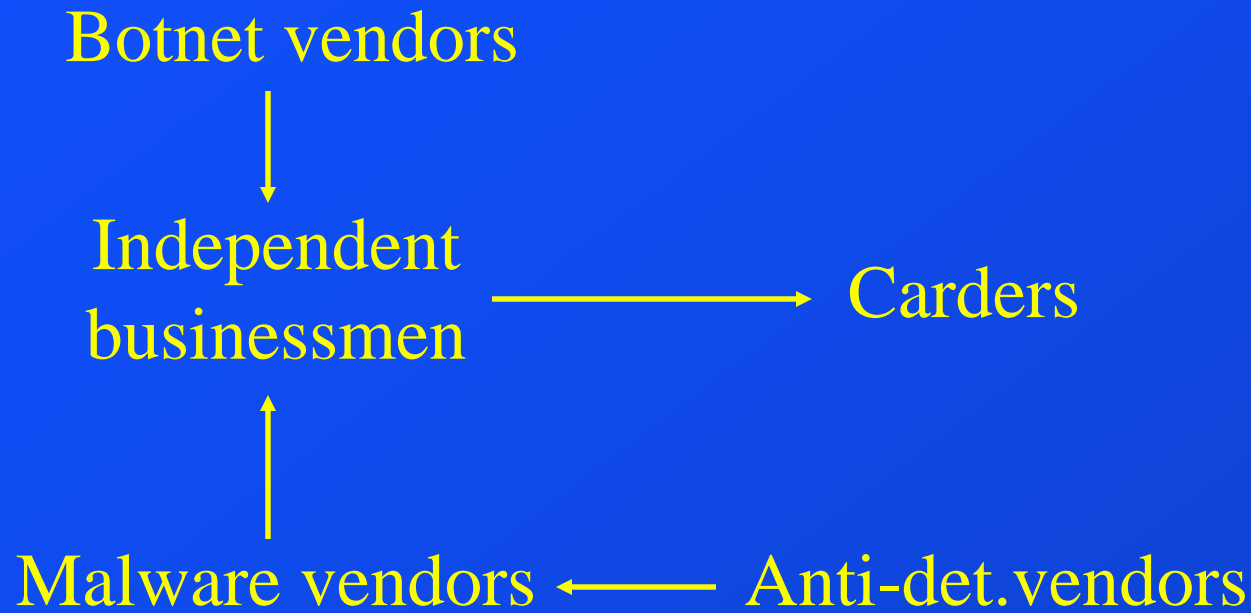
# The Carding Business (ctd)

## Everything can be outsourced

- Scammer buys hosts for a phishing scam
- Buys spam to lure the punters
- Buys drops to send the money to
- Pays a cashier to cash out the accounts

You wonder why anyone still bothers burgling houses when this is so much easier...

# The Carding Business (ctd)



The money seems to be in being the middleman

- If someone could figure out how to set up an automated clearing house (ACH), they'd really clean up
- Probably not possible since it breaks the decentralised model that makes the system fault-tolerant

# The Malware Industry

Publicity virus: Written by bored script kiddies

- Poorly tested, often barely works

Spam/phishing virus: Written by paid professional programmers

- Well-tested, can be quite sophisticated
  - The Babylonia virus used plug-in virus modules (VMODs) downloaded on-demand by the virus body
  - The Hybris worm uses digitally-signed encrypted updates propagated via web servers and newsgroups

The [Scob trojan] attack demonstrated the same skills required to design an entire software application

— Dan Frasnelli, NetSec

# The Malware Industry (ctd)

- Spam vendors are employing professional linguists to bypass filters
- Phishers use psychology graduates to scam victims
  - They have better experts than we do!

Kernel-mode rootkits can be bought from third-party developers

- Outsourcing the anti-detection code allows malware authors to concentrate on the payload

# The Malware Industry (ctd)

## Zero-days are sold online

There are dozens of these sites with hackers offering zero-day code for sale all the time. They even have a mechanism to test the code to make sure it is legitimate and will get past anti-virus software

— Jim Melnick, iDefense

This [WMF] exploit could be bought from a number of specialised sites. Hacker groups in Russia were selling this exploit for \$4,000

— Alexander Gostev, senior virus analyst, Kaspersky Labs

# Spam Technical Mechanisms

## Bulletproof hosting

Spam hosting from \$20 per month, fraud hosting from \$30 per month

— [carderportal.org](http://carderportal.org)

## Significant numbers of spam servers are located in China

- Highly advanced telecom infrastructure
- Cheaper bandwidth than in the West
- China has 30 – 50,000 Internet police in 700 cities...  
... who carefully investigate dangerous threats like pro-democracy web pages

# Spam Technical Mechanisms (ctd)

## Bullet-Proof server:

- Fresh IPs
- 1024MB RAM
- P4 CPU
- 72GB SCSI
- Dedicated 100M fiber
- Unlimited Data Transfer
- Any software
- Based China
- US\$599.00 monthly

## May use the server for:

- Bulk web Host
- Direct Mailing

We also supply e-mail list according to your order and sending out your message for you.

Hope to service for you.

# Spam Technical Mechanisms (ctd)

One experiment in blocking IP addresses originating worm/virus attacks ended up blocking

- China Anhui Province Network
- China Beijing Province Network
- China Fujian Province Network
- China Guangdong Province Network
- China Hangzhou Node Network
- China Hubei Province Network
- China Jiangmen Broadband Network
- China United Telecommunications Corporation, Beijing
- Oriental Cable Network Co, Shanghai
- Shanghai sichuan[...]gonsi Co.Ltd.

# Spam Technical Mechanisms (ctd)

Spammers can do whatever they want

They simply don't want to know — China Telecom doesn't care because they're government-owned, and there is no pressure coming from the government

— Steve Linford, Spamhaus

# Spam Technical Mechanisms (ctd)

Use BGP route injection/AS hijacking to steal an IP block

- Break into a poorly-secured router
  - NANOG 28 (June'03) ISP security BOF: 5,400 compromised routers
- Send a BGP route update announcing that your router is now responsible for some currently-unused block of IP addresses
  - In 5-10 minutes the entire Internet will know
  - This is all the time you need
- Spam like crazy from each IP address in the block until you get blacklisted

# Spam Technical Mechanisms (ctd)

## Advertise a huge netblock, e.g. a /8

- More specific prefixes advertised in the space, e.g. a /24, won't be affected (more specific takes precedence)
- Attacker gets the remaining space (unallocated, or allocated but unused)

## Advertise a legitimate netblock (someone else's)

- Routers who don't know or care will believe it
- Easy to spot, payoff is low, but then the cost is also low

## Works because routers/AS's are assumed to be trustworthy

- S-BGP (secure BGP) is high-overhead and little-used
- Only major peering points use it

# Spam Technical Mechanisms (ctd)

Spammers routinely break into legitimate users' PCs to send spam

“I don't bother securing my [games] PC, because I doubt spammers are interested in my savegames”

“They're not after your games, they're after your network connection”

— slashdot

- Largest observed single bot-net had 11,000 members
- In late '04 these were growing at 30,000 machines per day
- Peak rate was 75,000 per day during the MyDoom/Bagle virus group wars

# Spam Technical Mechanisms (ctd)

Email security firm MessageLabs reports that

- *Two thirds* of the spam it blocks is from infected PCs
- Much of the spam comes from ADSL/cable modem IP pools
- Distributed Server Boycott list reports 350,000 compromised hosts on the US RoadRunner network alone

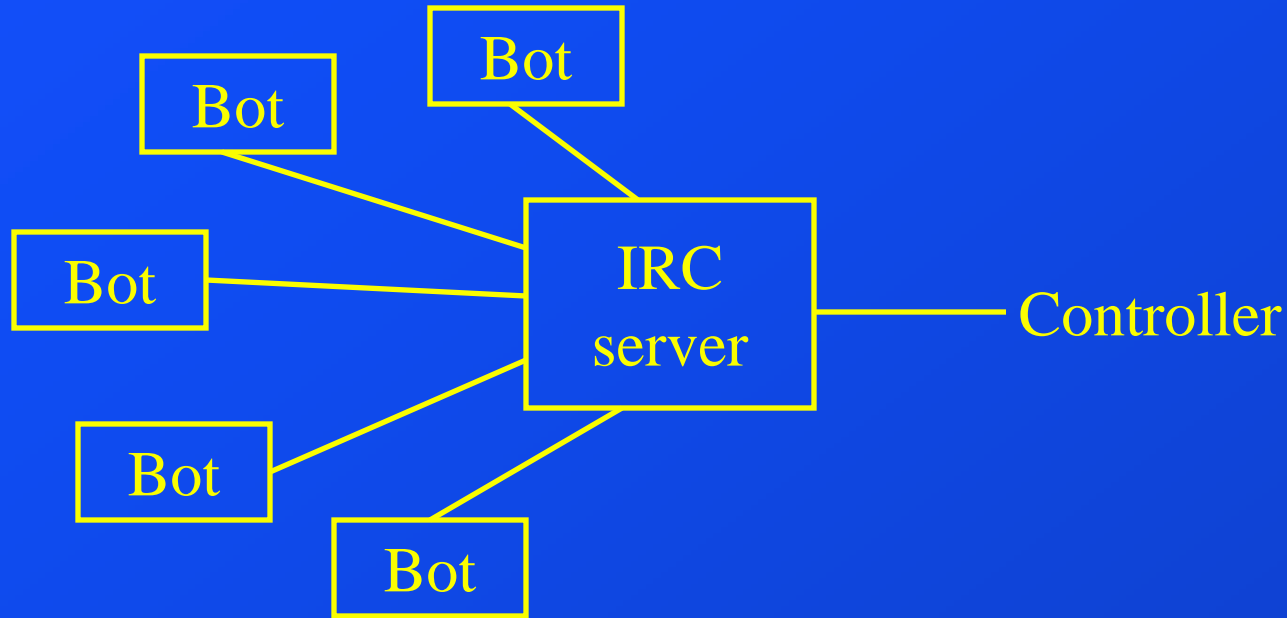
We have met the enemy and he is us...

Worms act as reverse HTTP proxies

- Provide a distributed fault-tolerant “web site” for spammers
- Backdoor.Migmaf changed the “site” every 10 minutes
  - c.f. email spam frequency-hopping

# Spam Technical Mechanisms (ctd)

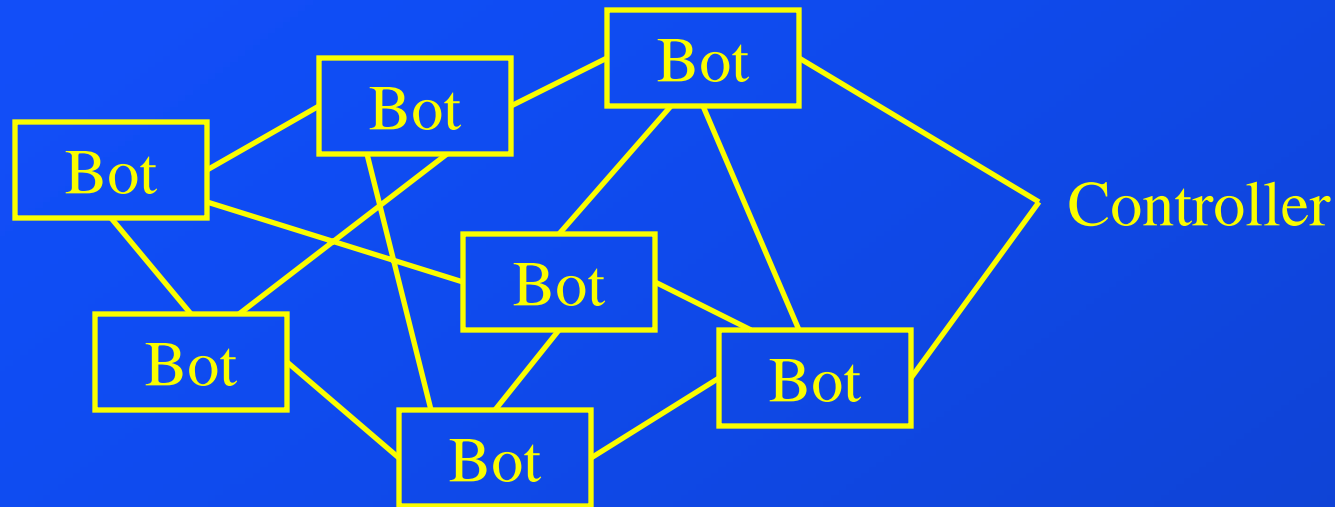
## IRC-based botnet



- IRC links may be encrypted (SSL)
- Communications may be over covert channels
  - DNS TXT records
  - HTTP

# Spam Technical Mechanisms (ctd)

## P2P-based botnet



- More damage-resistant than centralised IRC control

## Evolution follows that of file-sharing networks

- Centralised IRC-based system allows direct control, but provides a single point of failure → mitigate via IRC bouncers
- Mitigate even further via completely decentralised control

# Example: Agobot

Source code is freely available

- Well-written C++ implementation
- Cross-platform
- Modular design
- Easy to add new capabilities

Exists in many variants

- Agobot, Phatbot, Forbot, Xtrmbot, ...
- Originally used IRC
- Some variants use P2P control, e.g. WASTE,  
<http://waste.sourceforge.net>

# Example: Agobot (ctd)

## General capabilities

- Packet sniffing via `libpcap`
- Windows rootkit capabilities
- Detect debuggers and VMs
- Encrypt config data
- Disable anti-virus/firewall software
- Modify `hosts` file, e.g. to prevent access to antivirus sites

# Example: Agobot (ctd)

## Typical Agobot commands

<code>harvest.emails</code>	Harvest email addresses
<code>spam.setlist</code>	Download pre-harvested address list
<code>spam.settemptate</code>	Download email message template
<code>spam.start</code>	Start spamming
<code>spam.stop</code>	Stop spamming

## Other commands

<code>.keylog on</code>	Start keylogger
<code>.getcdkeys</code>	Get registration keys for commercial software
<code>.sysinfo</code>	Report system capabilities
<code>.netinfo</code>	Report network connection capabilities

# Example: Agobot (ctd)

Many additional commands are available

- Macro forms of spam commands to perform the above with a single command
- Display spoofed pages via browser help objects (BHO's)
- Web page redirection
- Spyware propagation
- Steal CD keys/registration codes for commercial software from the registry
  - Includes a database of registry locations for common commercial software
- Search the hard drive for sensitive files, e.g. \*.xls, \*finance\*

# Example: Spybot

Same pattern as Agobot, but oriented more towards spying/system manipulation

<code>cachedpasswords</code>	Retrieve passwords via <code>WNetEnumCachedPasswords</code>
<code>get <i>file</i></code>	Retrieve file
<code>killprocess <i>name</i></code>	Kill a process (e.g. antivirus)
<code>passwords</code>	Retrieve RAS passwords
<code>startkeylogger</code>	Start keylogger
<code>sendkeys <i>keys</i></code>	Simulate keypresses on PC keyboard

# Spamware Functions

## Worms install spamware

- Send-Safe.com and Direct Mail Sender (DMS) via SoBig, the first commercial spam virus
- Affects 80-100,000 new PCs a week
- Software hosted by MCI Worldcom (pink contract)

Act as an SMTP proxy to intercept outgoing mail (Taripox)

Run a SOCKS proxy for spammers (BID 9182 MSIE hole)

Email address harvesting (several)

DDoS on spam-blockers (numerous)

Run port redirectors to mask the true source of traffic

# Spamware Functions (ctd)

Worms act as special-purpose spam relays (e.g. Backdoor.Hogle, MyDoom.\*)

- MyDoom infected ca. 1,000,000 PCs (F-Secure)
- Infected PCs (“fresh proxies”) are traded in spammer forums
- Spamware sends either direct from end-user PCs or routed via an ISP’s mail servers
  - Spam comes from legitimate users or legitimate ISPs

Worm patches itself into WSOCK32.DLL (Happy99 etc)

- Intercepts the `connect ( )` and `send ( )` functions
- Checks for connections to the SMTP port
- Modifies outgoing mail as it’s sent
- Transparently converts legitimate mail into spam

# Spamware Functions (ctd)

Many additional ways to monetise malware...

Perpetrate click fraud on pay-per-click ads

- Botnet of 10K hosts each visit a pay-per-click site
- Site records visits from 10K unique IP addresses and pays for each click

# Other Malware Functions

## Disable anti-virus/firewall software (ProcKill, Klez, Bagle-BK)

- At one point it was possible to scan for viruses via the standardised code that they used to disable MSAV

## Bypass firewall software

- Walk the NDIS.SYS memory image or data structures and patch yourself in beneath the firewall hooks
  - Page in your own NDIS.SYS image from disk to avoid touching the live one
- Many, many variations used by different rootkits, e.g. FireWalk

## Other Malware Functions (ctd)

Modify anti-virus database files to remove detection of the malware (IDEA, AntiAVP)

- Alternatively, delete anti-virus database files

Block access to anti-virus vendor sites (MTX, Mydoom)

Modify anti-virus software to propagate the virus (Varicella)

Unhook the malware from lists of processes, threads, handles, memory, ... (FU rootkit)

Change scanners' abilities to view memory by hooking the virtual memory manager (Shadow Walker rootkit)

# Other Malware Functions (ctd)

Encrypt/obfuscate themselves to evade detection (too many to list)

- IDEA virus encrypts itself with the algorithm of the same name to evade detection

Pattern-based scanning stopped being effective 5-10 years ago

- Current scanners use heuristics and symbolic execution
- Second level of IDEA virus encryption uses randomised decryption (RDA) in which no decryption key is stored
  - Virus needs to brute-force break its own encryption, making detection even harder
- Zmist virus requires 2M code cycles to detect reliably

## Other Malware Functions (ctd)

Re-enable unsafe defaults in software, e.g. MS Office  
(Listi/Kallisti)

Lower browser's security settings to unblock pop-up ads  
(Mytob)

- Mytob author Diabl0 was paid per pop-up delivered

Run multiple instances/threads that resurrect each other if one is killed (Semisoft, Chiton, Lovegate)

## Other Malware Functions (ctd)

### Infect through CRC32-checksummed files (HybrisF)

- CRC32 isn't a cryptographic checksum mechanism
- Can modify the file without affecting its CRC32 value

### Install rogue CA root certificates (Marketscore)

- Because of the browser certificate trust model, Marketscore can usurp *any* SSL site

### Disable user rights verification by patching the kernel (Bolzano, FunLove)

- Two-byte patch to `SeAccessCheck ( )` in `ntoskrnl.exe`

## Other Malware Functions (ctd)

Engage users in IM chat sessions inviting them to download malware (IM.Myspace04.AIM)

- The worm will tell users that it's not malware if asked
- The typical AOL "lol d00d check this out" is hardly a Turing-test level challenge

Steal CD keys/registration codes for commercial software (Agobot)

Add registry entries to make an ActiveX control appear "safe" and digitally signed (Grew)

# Other Malware Functions (ctd)

Prevent anti-virus/malware removal programs from running

- Remove registry keys
- Block apps from starting
  - Register kernel-level load image notification callback via `PsSetLoadImageNotifyRoutine()`, prevent known images from loading
- Close windows with titles containing phrases like “virus” and “remove”
- ...

Use kernel-mode thread injection to hide from scanners  
(Rustock.A rootkit)

## Other Malware Functions (ctd)

Registers itself as a critical system process so it always gets loaded, even in Safe Mode (CoolWebSearch, HuntBar, VX2)

Worms attach themselves to Winlogon using the Winlogon notify function

- Winlogon always runs, and starts before anything else
- Malware can intercept any attempts to remove it at boot time

# Other Malware Functions (ctd)

Autostart mechanisms are used by almost all malware

- Fall into the general category of auto-start extensibility points (ASEP)
- Registry keys, startup folder, services, browser help objects (BHOs), layered service providers (LSPs), MSIE extensions, shell hooks, ...
- Several dozen (known) ASEPs in the Windows core OS alone

Use NT native API to create registry entry names that the Win32 API can't process

Pop up messages requesting payment of money and may disable your computer if you don't pay up (WGA)

- Disables PC with the only option being to pay up (SPP)

# Other Malware Functions (ctd)

## Remove competing malware from the system

- SpamThru includes a pirated copy of Kaspersky Antivirus to eliminate the competition
- Loads the Kaspersky DLL and patches the license check in-memory

## Spammers can do virtually anything to a victim's PC

- BroadcastPC malware installs 65MB (!! ) of .NET framework without the user being made aware of this

# Malware Then and Now

People expect Hollywood-style effects from malware

- Exploding panels
- Sparks flying from the case
- Crashing alien spacecraft

Modern malware is designed to be as undetectable as possible

- No visible effect  $\Rightarrow$  it's not there

I ran this Anna Kournikova thing and nothing happened. Why not?

— Anti-virus vendor support call

# Example: Haxdoor Identity-theft Trojan

## Advanced anti-removal and rootkit capabilities

- Hides itself by hooking the System Service Dispatch Table (SSDT)
- Auto-loads via WinLogon
  - It gets to load first
- Sets itself to run in SafeBoot mode
- Adds an autostart system service under various aliases
- Creates a remote thread inside Explorer
- Causes attempts to terminate it by AV software to terminate the AV program instead
  - Done by swapping the handles of the rootkit and the AV program

# Example: Haxdoor Identity-theft Trojan (ctd)

## Spyware capabilities

- Captures all information entered into MSIE
  - Recognises financial-site-related keywords on web pages (“bank”, “banq”, “trade”, “merchant”, ...)
- Steals cached credentials (RAS, POP, IMAP, ...)
- Feeds info to servers running on compromised hosts

One server held 285MB of stolen data from 9 days' logging

- 6.6 million entries, 39,000 distinct victim IP addresses
  - Probably much higher due to NAT'ing
- Full access details for 280 bank and credit card accounts
- Usernames and passwords for endless online accounts

# Example: Hacker Defender rootkit

Available as Bronze/Silver/Golden/Brilliant Hacker Defender, <http://hxdef.czweb.org>

- €150 (Bronze)/240 (Silver)/450 (Gold)/580 (Brilliant) layered add-on rootkit
- Commercial version of Hacker Defender

Anti-detection engine detects anti-virus software before it can detect the rootkit

- Works like a virus scanner in reverse
- Removes its kernel hooks if a rootkit-scanner is run to evade detection by the scanner

## Example: Hacker Defender rootkit (ctd)

Uses signature-based detection to detect anti-rootkit tools

- The same techniques that the anti-malware tools use to find rootkits, only the rootkit gets there first
  - Anti-rootkit tools are using rootkit-style stealth techniques to avoid this
- Updated on a subscription basis like standard virus scanners

Comprehensive real-time virus protection against all known  
Anti-Virus threats

# Convergence of Spam and Virus Threats

Anti-virus vendors notice users performing online scans of small variations on a theme

- These are VX'ers checking for detectability

Other rootkit vendors will modify their code to evade the virus scanner of your choice for a fixed fee (\$25-50)

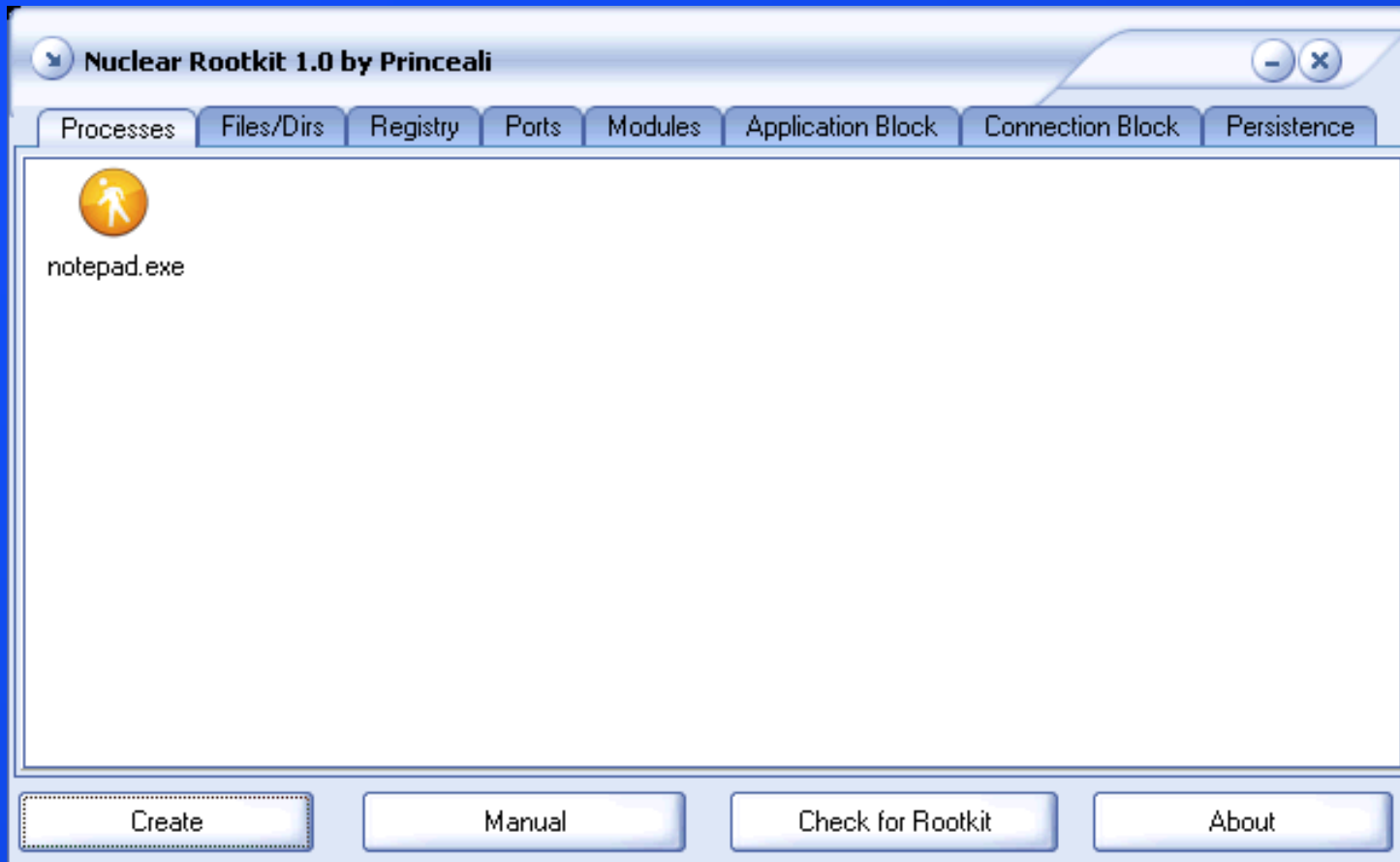
AFX Rootkit 2005 by Aphex

Undetected rootkits are on sale for \$100 each. Payment by paypal, egold, western union, check or money order!

Hackers working mutually on numerous rootkit projects are able to modify implementations to defeat detectors faster than corporations can offer a change

— Eric Uday Kumar, Authentium

# Convergence of Spam and Virus Threats (ctd)



The professionalism of these rootkits is coming to another level

— Allen Schimel, StillSecure

# Example: Grams egold siphoner

Invades the victim's PC via the usual attack vectors

Uses OLE automation to spoof the user's actions

- Uses the `IConnectionPointContainer` OLE object to register event sinks for the `IWebBrowser2` interface
- Checks for accesses to `e-gold.com`
- After user has logged on, uses `IWebBrowser2::Navigate` to copy the account balance window to a second, hidden window
- Uses `IHTMLInputHiddenElement::get_value` to obtain account balance
- Uses OLE to set `Payee_Account` and `Amount`
- Uses `IHTMLInputElement::click` to submit the form
- Waits for the verification page and again submits the form

# Example: Grams egold siphoner (ctd)

- Defeats any existing authentication method
  - Passwords, SecurID, challenge-response calculator, smart card, ...

This method of account looting bypasses all authentication methods employed by banking institutions, and is expected to become very popular [...] Since the trojan uses the victim's established SSL session and does not connect out on its own, it can bypass personal and corporate firewalls and evade IDS devices

— LURHQ security advisory on the trojan

# Phishing Attacks

Phishing: A broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt to trick individuals into revealing personal credentials that can be used fraudulently against them

— Financial Services Technology Consortium

Have gone from amateurish to very sophisticated, professionally-run operations

- Phishing toolkits allow criminals to select corporate logos, web site designs, site contents, ...
  - eBay's own fraud investigators were fooled by one phishing email, and endorsed it as legitimate
- Perfect copies of the original site
- Links lead back to the real site

# Phishing Attacks (ctd)

Phishers have started using self-signed certificates and similar techniques to fool users (“secured phishing”)

In self-signing, you become your own CA [...] most people don't know that self-signed certificates exist

— Susan Larson, Surfcontrol

- Security firm Netcraft recorded 450 cases of secured phishing in 2005, the first year that records were kept
  - Self-signed certs
  - Certs for soundalike domains
  - Cross-site scripting to insert content into banking web sites
  - Frame injection to " " " " " "
- Many bank sites (e.g. MasterCard, Barclays) are insecurely coded and allow these types of attack

# Phishing Attacks (ctd)

## Example secured phishing site: [visa-secure.com](http://visa-secure.com)

- Uses phishing email from [visa.com](http://visa.com) to send users to the site
- The real Visa uses similar naming, e.g. [verifiedbyvisa.com](http://verifiedbyvisa.com), [visabuxx.com](http://visabuxx.com)
- Site uses an SSL certificate to “authenticate” itself  
We use advanced SSL encryption technology to ensure confidential information cannot be viewed, intercepted, or altered  
— [visa-secure.com](http://visa-secure.com) phishing site
- Site is (was) hosted in Taiwan

# Phishing Attacks (ctd)

## Attacker controls the DNS

- Server compromise
  - 10% of DNS servers scanned in late 2005 were vulnerable to DNS cache poisoning
  - Used in one attack to redirect visitors to `cnn.com` and `msn.com` to spyware sites
- Bribing/blackmailing ISPs
- Virus changes the victim's DNS server entries ("pharming")
  - Can be used to disable security updates
  - (Fake) `windowsupdate.com`: Your system is up to date and doesn't need any security fixes
- Script in phishing email rewrites the victim's `hosts` file
  - As for direct DNS compromise

# Phishing Attacks (ctd)

- Many DNS providers ignore TTL's
  - Invalid DNS entries can take weeks to correct

## Trojans control the victim's PC

- Sniff keystrokes, mouse clicks, images of graphical “virtual keyboards”
- Render copies of genuine bank pages from the browser cache

## Trojan installs itself as a browser help object (BHO)

- Watches for access to a who's who of banking sites around the world
- Captures banking details before they go into the SSL layer

## Set up bogus blogs loaded with viruses/trojans

- Malware on blogs gets around email filters

# Phishing Attacks (ctd)

## Use typo-squatting to install malware

- `googkle.com` infects visitors with trojans, backdoors, and spyware
- Popups redirect to third-party sites loaded with downloader scripts
- Use assorted exploits to download more tools containing further exploit code
- Just one of these downloaded exploit packages contains two backdoors, two trojan droppers, a proxy trojan, a spyware trojan, and a further trojan downloader
- Another trojan dropper infects the Windows system folder and modifies the `hosts` file to prevent access to anti-virus sites
- Another generates a fake virus alert and directs the user to another trojan-riddled site

# Example: Glieder trojan

Phase 1, multiple fast-deploying variants sneak past AV software before virus signatures can be propagated

- Disable Windows XP Firewall and Security Center

Phase 2, connects to a list of URLs to download Fantibag malware

- Disables anti-virus software and other protection mechanisms
- Blocks access to anti-virus vendors
- Blocks access to Windows Update

Phase 3, Mitglieder malware contains the actual payload

- The attacker now owns the machine for use in botnets, spamming, DDoS, keystroke logging, etc

# Example: Hybris worm

Plug-in modules were encrypted with XTEA and digitally signed with a 1024-bit RSA key

- Modules were obtained from web sites or newsgroups

Modules ('muazzins') included

- Windows help file infector
- Polymorphic Windows executable infector
  - Could also infect executables 'through' a CRC16/CRC32/CRC48
- DOS .EXE infector
- RAR/ZIP/ARJ infector
- Word, Excel infectors
- SubSeven backdoor dropper

## Example: Hybris worm (ctd)

- Module to retrieve plugins from web servers
- Module to retrieve plugins from news servers
- General-purpose dropper
- WSOCK32.DLL infection stealth module
- DoS module
- Antivirus web-site blocker module
- Antivirus uninstall/database corruptor module
- SOAP-based email generator

# Phishing Attacks (ctd)

## Spyware via the affiliate model

- Pay others to infect users with spyware/adware/trojans
- `iframedollars.biz` pays webmasters 6 cents for each infected machine
- Their exploit drops at least 9 pieces of malware, including backdoors, trojans, spyware, and adware

## Piggyback malware on legitimate software

- CoolWebSearch co-installs a mail zombie and a keystroke logger
- Gathers credit card numbers, social security numbers, usernames, passwords, ...

# Availability of Private Data

Stolen personal information is so easily available that the best protection is that crooks simply can't use it all

- Number of identities stolen in an 18-month period from Feb'05 — Jun'06: *89 million* (Privacy Rights Clearinghouse)
- The smaller the breach, the greater the chance of the information being misused by crooks

Fraudsters [...] can use roughly 100 to 250 [stolen identities] in a year. But as the size of the breach grows, it drops off pretty drastically

— Mike Cook, ID Analytics

- A bit like recommending that all householders leave their doors unlocked and alarms disabled, since crooks won't be able to get around to robbing all of them

# Availability of Private Data (ctd)

Social security numbers (SSNs) and other information can readily be bought online

- \$35 from [secret-info.com](http://secret-info.com)
- \$45 from [iinfosearch.com](http://iinfosearch.com)

Several sites sell full Social Security numbers, potentially contributing to an epidemic of identity theft

— Washington Post

- Unisys study found that about half of all financial institutions use the SSN to verify customer identity

# Availability of Private Data (ctd)

## Prices for a CD or DVD of stolen data in Gorbushka market, Moscow

- Cash transfer records from Russia's central bank: \$1,500
- Tax records, including home addresses and incomes: \$215
- Mobile phone company's list of subscribers: \$43
- Name, birthday, passport number, address, phone number, vehicle description, and VIN for every driver in Moscow: \$100

## In Sao Paulo, Brazil, can buy a CD with full Brazilian tax records

- Due to the size of the required support infrastructure, tax records are fairly leaky in most countries

# Availability of Private Data (ctd)

Some of this information is also available in places like the US

- \$110 to [locatecell.com](http://locatecell.com) buys a month's worth of phone records
- Other sites sell similar information for \$90-150
  - Reputable firms work around problems in obtaining the information by farming it out to contractors and not asking questions

Information security by carriers to protect customer records is practically nonexistent and is routinely defeated

— Robert Douglas, privacy consultant

# Availability of Private Data (ctd)

To see how dangerous this could get, a blogger tried buying the call records for Supreme Allied Commander of NATO (SACEUR), General Wesley Clark

- Cost \$89.95 from [celltolls.com](http://celltolls.com)
- Required only the cellphone number and a credit card number
- This seems to be explicitly permitted by US law

A provider [...] may divulge a record or other information pertaining to a subscriber to or customer of such service [...] to any person other than a governmental entity

— 18 USC 2702

- Intent was to allow sale for marketing purposes, but limit government intrusion

# Credit Card Fraud

Obvious: Crime rings get 25 PCs shipped to eastern Europe

- Countermeasure: Merchants refuse to ship internationally
- Merchandise is shipped via US middlemen
  - “Earn big bucks working from home!”

Slightly less obvious: Set up CC processing on behalf of a legitimate company

- Legitimate company doesn't normally take CC orders and isn't aware of this (identity theft for companies)
- Make many small transactions at just under the floor limit using stolen cards
- Forward the funds to accounts controlled by the crime ring

# Credit Card Fraud (ctd)

Less obvious: Use online auctions for money laundering (triangulation)

- Advertise new \$1000 digital camera on ebay for \$800
- Buy with stolen card, get sent to ebay buyer
- Collect \$800 cash

Use bot-driven cliques to defeat trust rating systems

- Set up multiple accounts
- Sell zero-value items (e.g. background GIFs for web pages) for 1 cent each
- Provide positive feedback for each sale
- 100 positive feedbacks for \$1
  - Like business goodwill, trust can be monetised

# Conclusion

These aren't script kiddies any more

- Their experts are as good as anything we've got

More at <http://www.cs.auckland.ac.nz/~pgut001>