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 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)

Serious money can buy serious expertise

- Spam vendors are employing professional linguists to bypass filters
- Phishers use psychology graduates to scam victims
  - They have better experts than we do!
- Talented employees can earn $200,000+ per year
  - Remote root zero-days can go for $50-100,000

The Malware Industry (ctd)

Obtaining new recruits

- Russian script kiddie runs a botnet
- ISP notices this and reports it to their mafia contacts
- Mafia visits the kid and makes him an offer he can't refuse
- Kid is now working for the Russian mafia

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

- Windows Vista (-1)-day was available for $50K before Vista was even released!

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 ⇒ it's not there

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

  — Anti-virus vendor support call

Malware Economics

"Since Firefox now has appreciable market share, it will be targeted by malware authors"

- Only if you ignore the money factor

Let's do the maths…

- Assume MSIE has 80% market share, Firefox has 20% market share
- Assume successful exploit probability in MSIE is 3 out of 4 (75%), in Firefox is one in ten (10%)
- Do you want a 75% chance at 80% of the market (60% return) or a 10% chance at 20% of the market (2% return)?

Commercial attackers will expend effort to get the biggest market share, not short-lived bragging rights

Malware via the Affiliate Model

Pay others to infect users with spyware/adware/trojans

Business model was pioneered by `iframedollars.biz`

- (IFrames: Browser attack vector of choice)
- Pays webmasters 6 cents for each infected machine
- Alternative payment model is weekly fixed-rate payouts with bonuses for clean installs

  If your traffic is good, we will change rates for you and make payout with new rates

Malware via the Affiliate Model (ctd)

Since extended to a vast mass of adware affiliates (mostly porn)

- `12clickscash.com`, `camazoncash.com`, `gammacash.com`, `trafficcashgold.com`, … (way too many to list)
- `dollarrevenue.net` pays 30 cents for each install of their adware in the US, 20 cents in Canada, 10 cents in the UK, and one or two cents elsewhere
- T&C generally claim that they'll terminate affiliates who do anything unethical
  - Yeah, right

See `www.klikteamparty.com` for one company's end-of-year party (Mercedes C-Class, Vaios, strippers…)

Malware via the Affiliate Model (ctd)

Adware spams ads in a context-sensitive manner

- User Googles for something
- Adware spams the user with their affiliate's version of the product before they get a Google response
  - Variation: Rewrite the search results in the browser to favour your products
- Satanic version of the MS Office Assistant

  It looks like you're searching for dog food. Would you like to be spammed with penis enlargement ads instead?

Malware via the Affiliate Model (ctd)

A morass of grey-market and unethical practices

- Vendor puts an EULA on their adware so they can claim that they warn the user on install
- Affiliate uses OLE automation to click past the EULA without the user even seeing it

Piggyback malware on legitimate software

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

Malware as a Service

Standard commercial vendors are embracing SaaS

- Malware vendors have MaaS

MaaS is advertised and distributed just like standard commercial software

Iframe, pop under, накрутка счетчиков, постинг, спам
Также я советую если у вас нет сплоита и трафа, вы можете взять в аренду у здесь

Iframe exploits, pop-unders, click fraud, posting, spam

If you don't have it, you can rent it here

- Online video tutorials of the malware in action

Malware as a Service

Try-before-you-buy offers for malware

Трафик на сплоиты.
Для пробы всем Бесплатно 100 посетителей!!!
Цена
4 $ за 1000 посетителей - При заказе от 1000 до 5.000
3.8 $ за 1000 посетителей - При заказе от 5.000 до 10.000
3.5 $ за 1000 посетителей - При заказе от 10.000

Traffic for sploits
Free trial, 100 visitors!!!
Price
$4 per 1000 if buying 1000 – 5000
$3.80 per 1000 if buying 5000 – 10,000
$3.50 per 1000 if buying over 10,000

Malware as a Service (ctd)

Back-end databases and control systems managed via web GUIs

- Sophisticated, skinnable interfaces
- Briz/VisualBriz at right

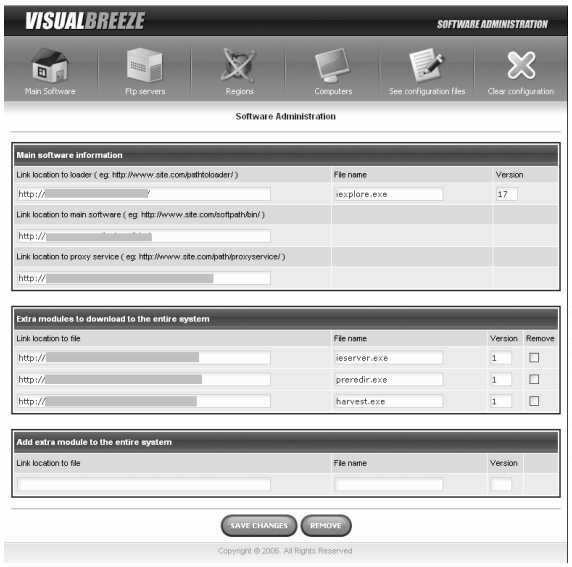


Image courtesy Alex Eckelberry, Sunbelt Software

Malware as a Service (ctd)

Buy the basic version for $1000-2000 (Gozi)

- Purchase add-on services at varying prices starting at $20

  Также вы може взять и другие страны на заказ.
  За подробной информацией обращайтесь к суппортам

  In other countries on request. Contact us for support

Prices vary by as much as 100-200% across sites – shop around

- Prices for non-Russians are often higher
- If you want the discount rate, buy via Russian sites

Malware as a Service (ctd)

Prices are generally advertised in wmz (USD-equivalent WebMoney currency)

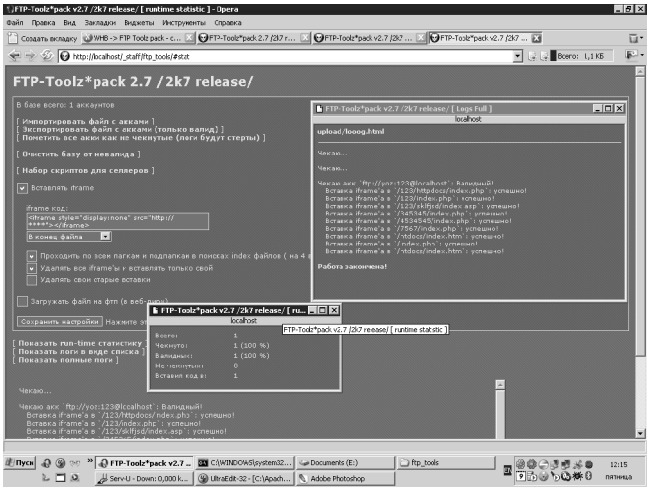
- WebMoney = more bulletproof Russian version of PayPal

  Icq спам по ONLINE номерам
  Для пробы всем Бесплатно 10.000 сообщений !!!
  10 000 сообщений - 0,5 wmz
  15 000 сообщений - 1,0 wmz
  50 000 сообщений - 3,0 wmz
  100 000 сообщений - 5 wmz
  200 000 сообщений - 9 wmz
  500 000 сообщений - 15 wmz
  1 000 000 сообщений - 20 wmz

  ICQ spam, free trial 10K messages, prices in wmz

Malware as a Service (ctd)

Server-compromise tools are sold in a similar manner



- Feed the tool a list of accounts and it does the rest

Malware as a Service (ctd)

Basic server-exploit tools typically go for $20-25

- Previous slide was FTP-Toolz, a front-end for the MPACK exploit toolkit
  - Automates deployment of MPACK
  - MPACK itself sells for ~$1000

Prime Exploit System - 20 $ (довольно неплохой сплойт)
Нуклеар - 40 $ (Хороший сплойт даже очень)
+ Ежемесечная оплата за польззования хостингом 10$

Prime Exploit $20 (not so bad sploit)

Nuclear (Grabber) $40 (very good sploit)

Additional $10 payment for hosting

Example: Information Stolen by Malware

Malware server found by investigators contained

- Information from 5,200 PCs
- 10,000 account records for 300 organisations
  - Top global banks and financial companies
  - US federal, state, and local government
  - US national and local law enforcement
  - Major US retailers
- SSNs and other personal information
- Patient medical information (via healthcare employees)

US regulations (HIPAA, GLBA, etc) made reporting this to the victims very difficult

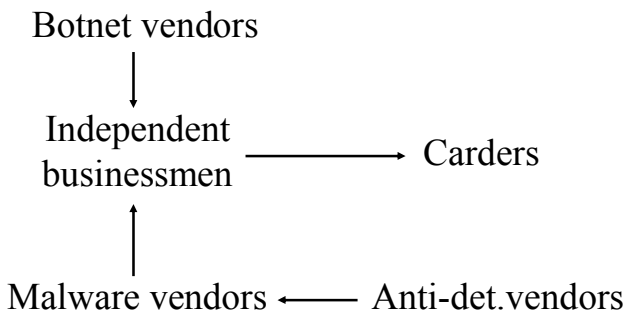
The Malware Business

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 Malware 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

Example: Gozi Trojan

Available as a service from iFrameBiz, `stat482.com`

- Gozi Trojan bought from HangUp Team, `hangup.da.ru`
- Trojan server managed by 76Service, `76service.com`
- Trojan server hosted by Russian Business Network, `www.rbnnetwork.com`
- Cashier details unknown

The Spam Business

Buy CDs with harvested addresses

- Prices vary depending on the quality
- Vacuum-cleaner for ~$50, verified for $*x*00

Send mail via spam brokers

- Handled via online forums like `specialham.com`, `spamforum.biz`
- $1 buys 1000–5000 credits
- $1000 buys 10,000 compromised PCs
- Credit is deducted when the 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
  - A "dump" in carder jargon, dump of the magstripe info
- 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

- Handled via web forums like `cardingworld.cc`, `darkmarket.org`, `talkcash.net`, `theftservices.com`
- "Need spammer to fill Hotmail boxes, will pay through percentage of phishing proceeds"
- "Will trade CVV2 for web site account"

Example: `carderplanet.net`

i can provide you with excellent credit cards with cvv2 code and without it. Minimum deal is a USD $200.00.

- USD $200.00 - there are 300 credit cards without cvv2 code (visa + mc) - USA (included credit card number, exp.day. cardholder billing address, zip, state).
- USD $200.00 - there are 50cc with cvv2 code (visa + mc) USA (included credit card number, exp.day. cardholder billing address & CVV code from the back side of the card).

Also i can provide cards with SSN+DOB. COST 40$ per one. Minimal deal 200$

- Also i can provide Europe credit cards, France, Germany + UK and many other contries around the globe.
- All credit cards with good exp day and it's work also so good.

Example: vendorsname.ws

On our forum you can buy:

- Credit cards with Change Of Billing (COBs)*
- Dumps of US and European credit cards (Platinum, Gold and Classic)
- Active eBay accounts with as many positive feedbacks as you need
- Active and wealthy PayPal accounts
- Drops for carding, cashing and money laundering
- Carded electronic and stuff for as low as 40 percent of market price
- PINs for prepaided AT&T and Sprint phone cards
- Carded Western Union accounts for safe and quick money transfers

… continues..

* COB = credit card with billing address changed to carder mail drop

Example: vendorsname.ws (ctd)

… continued…

- Carded UPS and FedEx accounts for quick and free worldwide shipping of your stuff
- Full info including Social Security Info, Driver Licence #, Mother' Maiden Name and much more
- DDoS attack for any site you need, including monsters like Yahoo, Microsoft, eBay

Come and register today and get a bonus by your choice:

- One Citybank account with online access with 3k on board, or
- 5 COB' cards with 5k credit line
- 10 eBay active eBay accounts with 100+ positive feedbacks
- 25 Credit Cards with PINs for online carding

Be in first 10 who register today and get the very special bonus from Administration of Forum.

The Carding Business (ctd)

Obvious: Get 25 PCs shipped to eastern Europe via intermediaries (re-shipping rings)

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

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

The Carding Business (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

The Carding Business (ctd)

Everything can be monetised

Obvious accounts: Banks, PayPal, …

Less obvious accounts: Stock brokerage accounts

- Dump the existing portfolio
- Buy microcap stocks to drive up prices in pump-and-dump
  - Cuts out the need to pump the stock

The Carding Business (ctd)

No accounts at all: Botnets used for click fraud

- Advertisers like clicks, they get feedback on effectiveness
  - Researchers estimate that 10-15% of clicks are fraudulent, representing ~$1B in billings
- Google and others boost revenue by recycling ads to other sites
  - Example: Domain parkers fill parked domains with ads
- PTC/PTR (pay-to-click/pay-to-read) rings or clickbots fill the sites with clicks
- Handled via brokers like `adspacedepot.com`, `clicksmania.net`, `clixmedia.biz`, `paid4clixonline.com`, `puppiesptr.com`
  - c.f. Terry Pratchett's fire-fighting economy in Ankh-Morpork

The Carding Business (ctd)

In 2006 the US government passed its Money Laundering Enabling Act

- Amendment to the Safe Port Act bans financial transactions to gambling sites
  - – Gambling continues, but now it's via illegitimate channels
- All gamblers become money launderers
- Vastly increases the noise level of money laundering
  - – Fraud-related laundering hides in the noise

Spam Technical Mechanisms

Bulletproof hosting

> Spam hosting from $20 per month, fraud hosting from $30 per month
>
> — 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)

Cost of a compromised system

- Cisco router: US$5
- Unix box: US$1-5
  - Can easily turn a Unix box into a router using built-in tools
- Windows box: Too cheap to meter

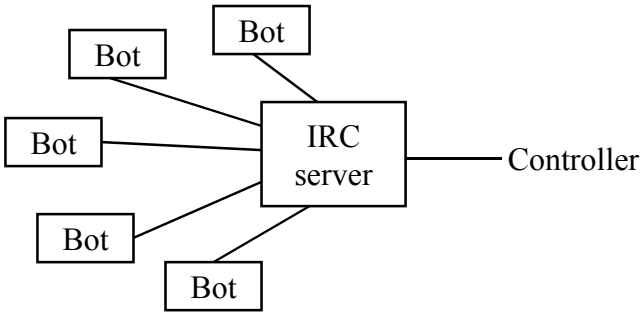
Email security firm MessageLabs reports that

- *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…

Spam Technical Mechanisms (ctd)

IRC-based botnet



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

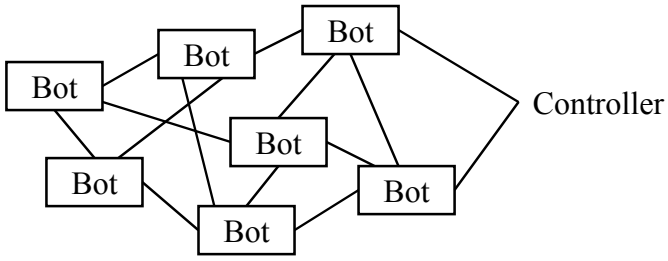
Spam Technical Mechanisms (ctd)

DSNX is an advanced, open source, modular, non-interactive IRC client (An irc robot). It provides the subsystem for a versatile internet technology deployment across multiple systems. Through the patented DSNX technology dataspy dot net INC can provide your fortune 500 company with the ultimate solution

— DataSpy Network X promotion

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
- GPLd

Exists in many variants

- Agobot, Phatbot, Forbot, Gaobot, Xtrmbot, Polybot, …
  - Hundreds of variants (depending on how you count them)
- Originally used IRC
- Some variants use P2P control, e.g. WASTE, `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

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

Other commands

`.keylog on`	Start keylogger
`.getcdkeys`	Get registration keys for commercial software
`.sysinfo`	Report system capabilities
`.netinfo`	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: Agobot (ctd)

Agobot variants added further commands, e.g. Gaobot

`bot.unsecure`	Enable shares, DCOM
`ddos.`*`type`*	Start assorted DDoS attacks
`http.visit`	Visit a web site
`http.execute`	Update from remote site
`inst.asadd`	Add an autostart entry
`inst.svcadd`	Add a service
`pctrl.kill`	Kill process

- Some are extensions of existing Agobot commands

Example: Spybot

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

`cachedpasswords`	Retrieve passwords via WNetEnumCachedPasswords
`get` *`file`*	Retrieve file
`killprocess` *`name`*	Kill a process (e.g. antivirus)
`passwords`	Retrieve RAS passwords
`startkeylogger`	Start keylogger
`sendkeys` *`keys`*	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 (numerous)

Email address harvesting (several)

DDoS on spam-blockers (numerous)

- DDoS other botnets
- Much DDoS traffic is actually botnet internecine warfare

Spamware Functions (ctd)

Worms act as special-purpose spam relays (e.g. Hogle, MyDoom, many others)

- 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)

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

Worms act as reverse HTTP proxies

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

Spamware Functions (ctd)

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

- 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

Spamware 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)

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 ("resuscitators") (Semisoft, Chiton, Lovegate)

Use error-correcting codes to repair the virus body if any portion is patched out (RDA Fighter)

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

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

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

Rewrites user-created Yahoo IM or MIRC messages to propagate itself (Browsesafe)

Injects itself into existing AIM, Google Talk, and Yahoo IM sessions (Peacomm)

Other Malware Functions (ctd)

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

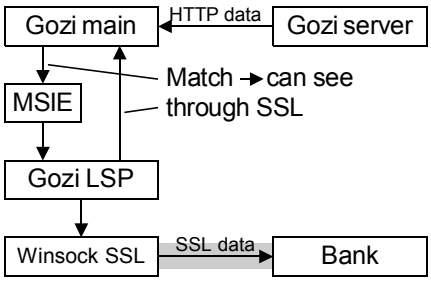
- Windows .PWL files (Dumaru)
- PGP secret keyrings (Caligula)
- CuteFTP password files (Melissa)
- UBS account and PIN files (LoveLetter)
- …

Hooks into the Javascript engine to grab AJAX-based authentication data (Gozi)

- After FFIEC required US banks to use two-factor auth, they redefined "two-factor" to mean "twice as much one-factor"
- "Hey, it uses AJAX, now it's secure!"

Other Malware Functions (ctd)

Register as a Winsock LSP to bypass SSL (Gozi)



- Bypasses SSL encryption in MSIE and other Windows apps (but not ones with built-in SSL)
- Blah blah monoculture blah blah

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”
- …

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

Steal client keys and certificates and other secrets from Windows Protected Storage (Gozi)

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 0wns the machine for use in botnets, spamming, DDoS, keystroke logging, etc

Example: Glieder trojan (ctd)

Multi-phase approach bootstraps a fast-moving zero-day into an arbitrary-sized malware payload

Q: How can a mere 376 bytes (SQL Slammer) be a threat?

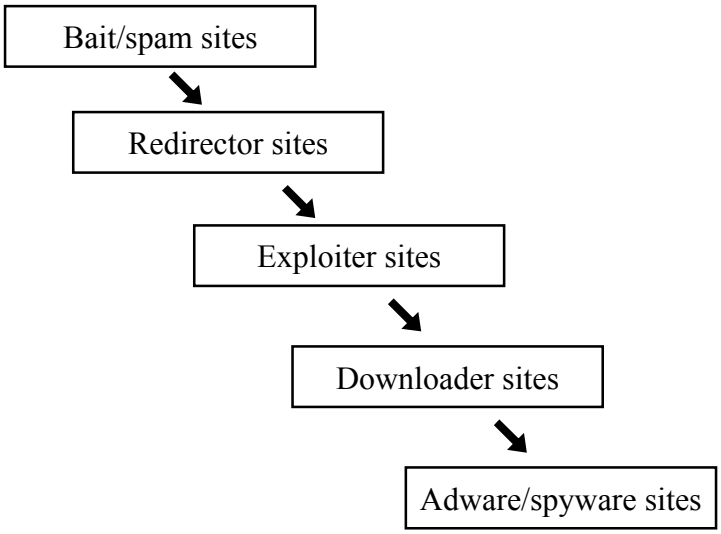
A: It doesn't have to be, all it has to do is clear the way for the *real* threat

Cascading file droppers of this kind are a standard mechanism for staying ahead of AV tools

- Glieder is relatively simple, some malware uses 10-15 stage infection strategies

Example: Glieder trojan (ctd)

Web sites are also set up using multi-stage strategies



Example: Hybris worm

Plug-in modules are encrypted with XTEA and digitally signed using a Davies-Meyer XTEA hash and a 1024-bit RSA key

- Modules are obtained from web sites or newsgroups
- Creates a so-called "programmable virus"

Modules ('muazzins') included

- Windows help file infector
- Polymorphic Windows executable infector
  - Could also infect executables 'through' a CRC16/CRC32/CRC48
- DOS .EXE infector

Example: Hybris worm (ctd)

- RAR/ZIP/ARJ infector
- Word, Excel infectors
- SubSeven backdoor dropper
- 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

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

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

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

Other Malware Functions (ctd)

Provide situation-specific payloads ("programmable viruses") (Cheeba)

- Capabilities are built in, but encrypted
  - Other programmable viruses use digitally signed plugins
- Virus compares a hash of disk filenames to built-in hash values
  - When a hash matches, it uses the filename as the key to decrypt the file-specific payload
- Allows a virus to carry custom payloads for specific files, URLs, applications…
  - You can't tell what will happen to you until it's too late
  - Mostly superseded by the easy ability to distribute plugins, see the discussion of Hybris, Babylonia, …

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

Adware vendors DirectRevenue have a 'Dark Arts' division dedicated to techniques like removing competing malware

> You also acknowledge that such software and updates to software may without further notice to you, remove, disable or render inoperative other adware or spyware programs including but not limited to competing products
>
> — DirectRevenue EULA

Other Malware Functions (ctd)

Record user geolocation information

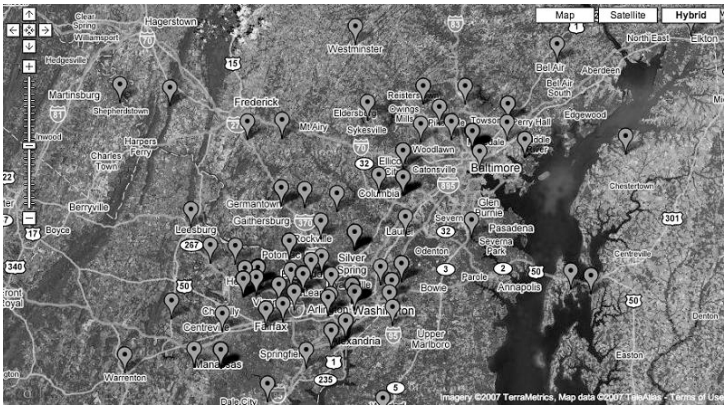


Image courtesy Brian Krebs, Washington Post

- Used to defeat anomaly-detection software used by CC companies
  - Use the card from a botnet node near the victim's registered location to evade transaction location tracking

Other Malware Functions (ctd)

Disable System Restore, patch SFC.DLL and SFC_OS.DLL to disable Windows File Prot (PWS-Satiloler, Sdbot)

Perform targeted attacks on specific groups of users

- SpamThru trojan contacts controlling servers for information for victim-specific attacks, for example pump-and-dump scams for users performing stock trading

Hijack Windows Update (BITS) to download updates (Jowspry)

- Bypasses Windows Firewall and other security measures

Other Malware Functions (ctd)

Use standard Windows popups for nefarious purposes

- Install malware via fake Windows Update notifications (Antispysolutions.com, via Myspace)
- Request CC details for Windows product activation (Kardphisher)

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

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

Anti-detection Mechanisms

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

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

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

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

Won't run if the system contains SoftICE, Filemon, Regmon, Visual Studio, Ethereal, … (Numerous)

Won't run under a VMM (Many)

Anti-detection Mechanisms (ctd)

Tricks with processor features (AMD64 memory-type-range registers) can even defeat hardware-based monitoring

Joanna Rutkowska's proof-of-concept "replacing attack" shows a different image to a PCI monitoring card than what's actually there

- Bounce access to physical memory address to I/O address space (memory-mapped I/O)
- Point some device's base address register into the target I/O space
- Fill device memory with whatever you want the hardware monitor to see

Anti-detection Mechanisms (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

Randomised decryption (RDA) was introduced in the RDA Figher virus

- Outer layer: Polymorphically-generated layer with up to 16 sub-layers
- Inner layer: Encrypted with random 16-bit key
  - Second level of IDEA virus also uses RDA with 18-bit key
- Virus needs to brute-force break its own encryption, making detection even harder

Anti-detection Mechanisms (ctd)

Polymorphism and RDA rendered pattern-based scanning ineffective 5-10 years ago

- Current scanners use behavioral analysis via heuristics and symbolic execution
- Zmist virus requires 2M code cycles to detect reliably
  - Emulated x86 may multiply this by a factor of 100
  - Then multiply again by *x*0,000 files on a system
- Virii using techniques like this are effectively undetectable

  A quick solution delivery for metamorphic virus detection should become a huge team effort at AV companies. Exact identification becomes a problem even for humans

  — Virus Bulletin

Anti-detection Mechanisms (ctd)

- Etap/Simile uses spread-spectrum style decryption
  - Maximum-sequence RNG identifies the next byte to decrypt
  - Avoids triggering memory-access-pattern detection
- Etap/Simile decryptor contains anti-emulation code
  - Metamorphic RDTSC-based header causes the virus to not trigger 50% of the time
  - Half the infected files won't be detected as a virus under emulation

Anti-detection Mechanisms (ctd)

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

- These are VX'ers checking for detectability

  The most popular brands of antivirus on the market […] have an 80 percent miss rate. That is not a detection rate that is a miss rate. So if you are running these pieces of software, eight out of 10 pieces of malicious code are going to get in

  — Graham Ingram, General Manager, AusCERT

Anti-detection Mechanisms (ctd)

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

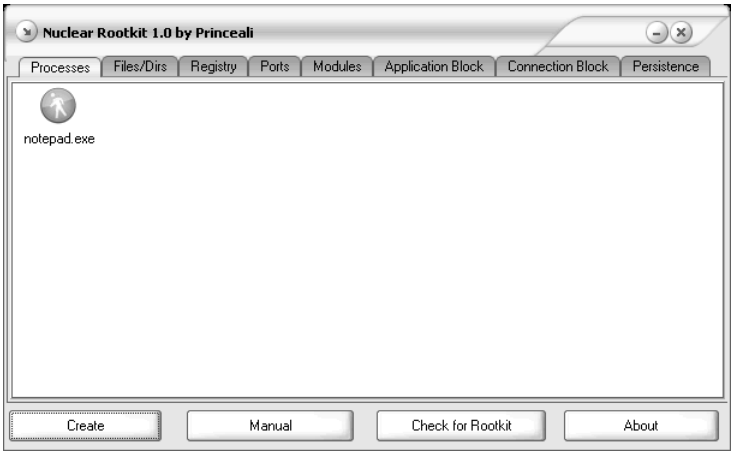
AFX Rootkit 2005 by Aphex

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

Anti-detection Mechanisms (ctd)



The professionalism of these rootkits is coming to another level

— Allen Schimel, StillSecure

Example: Hacker Defender rootkit

Available as Bronze/Silver/Golden/Brilliant Hacker Defender, `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

Example: Hacker Defender rootkit (ctd)

Author "Holy Father" was killed in a car accident, New Year 2007

- Has proven the business model
- Others have followed, e.g. HangUp Team in Russia, `hangup.da.ru`

Other types of malware are also available for purchase

- Example: WebAttacker malware kit sells for $15-20, `www.inet-lux.com` (Russian site)

Phishing Mechanisms

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

Phishing Mechanisms (ctd)

- Script in phishing email rewrites the victim's `hosts` file
  - As for direct DNS compromise
- Many DNS providers ignore TTL's
  - Invalid DNS entries can take weeks to correct

Trojans control the victim's PC

- Sniff keystrokes and mouse clicks
- Use screen scraping to get around graphical keyboards and PIN-pads
  - Mostly popular in Europe and South America, US banks haven't even got past unencrypted logon pages yet
- Render copies of genuine bank pages from the browser cache

Phishing Mechanisms (ctd)

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
- Uses HTML injection to capture TANs (one-time PINs) for banking sites (MetaFisher)

Phishing Mechanisms (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: 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 `IHTMLElement::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

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`
- $45 from `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` 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`
- 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

What Should I Do? (Non-geeks)

Put your head between your legs and …

What Should I Do? (Geeks)

Disable all Windows networking and RPC services (about 2/3 of all Windows services)

- No noticeable effect on system usability
- Closes all ports
- Total Windows kernel memory usage should be ~100MB
- Need to hack the registry and other obscure things

Browse the web from a browser running on a locked-down Unix box with 'nobody' privileges

- Use a graphic-image-only forwarding protocol to view the result under Windows
- Use NoScript (or equivalent) set the maximum blocking

What Should I Do? (Geeks) (ctd)

Read mail on a locked-down Unix box using a text-only client that doesn't understand MIME

Run all Internet-facing programs (Word, etc) under DropMyRights as 'Guest' or (standard, non-Power) 'User'

Conclusion

These aren't script kiddies any more

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

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