

The Commercial Malware Industry

Peter Gutmann

University of Auckland

(An Introductory Note)

For those reading the slides rather than going to the talk:

The information was gathered over time and prices and offerings of malware authors change rapidly; all figures and information is/are representative only...

Since this is an ongoing work, information is taken from different eras to illustrate changes in the industry and technology; this isn't how everything works at the current time

Malware as a Service

Standard commercial vendors are embracing software-as-a-service, 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 spoits

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 control systems managed via web-based GUIs

- Sophisticated, skinnable interfaces
- Briz/VisualBriz at right



Image courtesy Alex Eckelberry, Sunbelt Software

Malware as a Service (ctd)

Companies producing malware are standard commercial IT operations

A receptionist greeted visitors at the door of the company [...] as business boomed, the firm added a human resources department, hired an internal IT staff and built a call center to dissuade its victims from seeking credit card refunds. Employees were treated to catered holiday parties and picnics with paintball competitions

— “Perks and paintball: life inside a global cybercrime ring”

A researcher with antivirus software maker McAfee [...] estimates that the business generated revenue of about US\$180 million in 2008, selling programs in at least two dozen countries

— “Perks and paintball”

Malware as a Service (ctd)

There are even support bureaus available for your cybercrime operation

- One operator, callservice.biz, provided support for over 2,000 identity thieves

[The bureau] provided the services of English- and German-speaking individuals to persons who had stolen account and biographical information to defeat the security screening processes. The callers would confirm unauthorized withdrawals or transfers from bank accounts, unblock accounts, or change the address or phone number associated with an account

— “Operator of ‘Support Center’ Assisting over 2,000 Identity Thieves Pleads Guilty”

Malware as a Service (ctd)

See “Anatomy of a Malware Scam” for a (long) step-by-step walkthrough of how sophisticated the malware front-ends on victim’s PCs are

- Spoofed Windows Security Center for fake “security” software
- Spoofed Vista UAC including the greyed-out background
- Spoofed taskbar notification area/system tray popups
- Online help forums
- EULAs
- Fake anti-virus scans
- ...

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 можете взять и другие страны на заказ.
За подробной информацией обращайтесь к суппортам
In other countries on request. Contact us for support

Malware is rented in 30-day billing cycles ('projects')

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)

Following the discussion (in Russian) is very difficult

- Transliteration of English words with totally different meanings
 - Based on semantic/visual/contextual puns and other tricks
 - Bonus points if it has obscene connotations
- The more obtuse the reference, the more l33t it is
- Terms are used in a context-dependent manner, e.g. relative to a particular piece of software
- Even native speakers can have difficulty following it

Malware as a Service (ctd)

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

- WebMoney = more bulletproof Russian version of PayPal

Ісq спам по ONLINE номерам

Для пробы всем Бесплатно 10.000 сообщений !!!

10 000 сообщений - 0,5 wnz

15 000 сообщений - 1,0 wnz

50 000 сообщений - 3,0 wnz

100 000 сообщений - 5 wnz

200 000 сообщений - 9 wnz

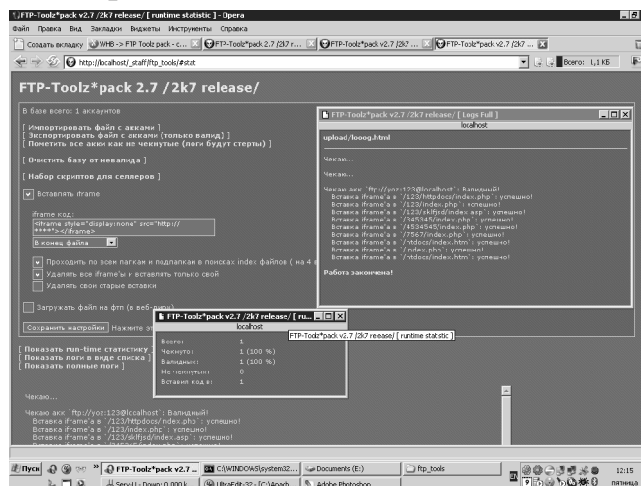
500 000 сообщений - 15 wnz

1 000 000 сообщений - 20 wnz

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

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 спloit)

Нуклеар - 40 \$ (Хороший спloit даже очень)

+ Ежемесячная оплата за пользования хостингом 10\$

Prime Exploit \$20 (not so bad sploit)

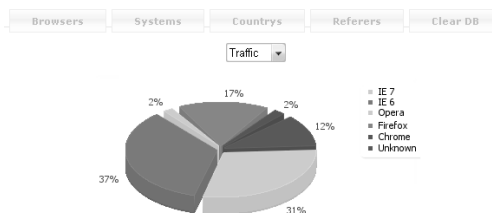
Nuclear (Grabber) \$40 (very good sploit)

Additional \$10 payment for hosting

Malware as a Service (ctd)

Exploit packs provide sophisticated reporting of attack and vulnerability statistics

- google-analytics for the bad guys



Browser	Uniques	Downloads	Percent
Total (100 %)	3029	555	18.32 %
IE 6 (37.07 %)	1123	397	35.35 % (13.11 %)
IE 7 (30.57 %)	926	89	9.61 % (2.94 %)
Firefox (16.64 %)	504	54	10.71 % (1.78 %)
Unknown (11.89 %)	360	2	0.56 % (0.07 %)
Chrome (2.01 %)	61	9	14.75 % (0.3 %)
Opera (1.82 %)	55	4	7.27 % (0.13 %)

Source: malwareint.blogspot.com

Malware as a Service (ctd)

Vendors provide money-back guarantees

Cvv2 = UK, EU, ASIA,CA and AU

VBV (Verified By Visa) = UK and US only

VISA CLASSIC|MASTERCARD \$5 <> \$3 per 30

VISA PLATINUM|BUSINESS \$10 <> \$7 per 30

[...]

ANY CVV&FULLZ WILL BE REPLACED IF NOT WORKING
BUT NOT LATER THAN 72 HOURS

DECLINED/HOLD-CALL/PICKUP dumps we replace in 48hrs
after purchase. If you like checked stuff - we can check, before
you receive it, so only 100% Approval

Malware as a Service (ctd)

Escrow agencies act as guarantors for sales

As you know there are a lot of rippers in world who don't
believe in trading nicely. For this purpose we are introducing
our own service just like www.escrow.com but our commission
is going to be only 4%

— “Crimeware Business Models”, David Cole

- This looks like a good business model, rippers are a far more
serious problem than the banks' security measures

(Destabilising the market would be a good way to attack it,
but requires a considerable investment of effort and
ongoing commitment)

Malware as a Service (ctd)

Accounts are sold with quality guarantees

BANK LOGIN / TRANSFER

UK US CA

\$10.000 Maximum

£5.000 Maximum

I have Paypal verifi balance > 20.000\$

sell 2000\$

Malware as a Service (ctd)

Buying in bulk is cheaper

Visa Classic, MasterCard Standart

Amount: 10-50 -- \$20 per 1 dump

Amount: 50-100 -- \$18 per 1 dump

Amount: 100 -- \$14 per 1 dump

Visa Gold | Platinum | Business, MasterCard Gold | Platinum

Amount: 10-50 -- \$36.5 per 1 dump

Amount: 50-100 -- \$34.5 per 1 dump

Amount: 100 -- \$25 per 1 dump

Malware as a Service (ctd)

Online cybercrime “universities”...

CASH PARADISE UNIVERSITY
ТВОЙ КЛЮЧ К БОГАТСТВУ
YOUR KEY TO WEALTH

ICQ 48-777777-8
JABBER: CPUONLINE@THESECURE.BIZ

VISA MasterCard

skype Poker Stars.com WESTERN UNION ups

MAIN STUDY PROGRAMS RULES CONTACT US

Malware as a Service (ctd)

... with a variety of courses

[1] HELLO WORLD or SKYPE CARDING - 2-3h - 75\$

**for those who passed the basic.*



Skype Carding. The first practical experience, bringing a steady income, it is recommended for those who passed basic course on security in the network.

Material for the work included:

Credit Card USA (no VBV/MCSC)
Dedicated Server USA
DoubleVPN for security in network

Invest 10\$/day. Get 100-150\$.

Advice: sell skype accounts not only on one board, try to sell this on RU-boards

Result: You learn SKYPE carding, get an account with a balance \$ 50 (live long), you can immediately sell on the forum for 7-8\$, or you can try to sell it to other (legal) sites for 30-40 \$.

GET YOUR OWN DROPS

[2] How to get your own DROPS for STAFF and TRANSFERS 4-6h - 250\$

Malware as a Service (ctd)

In the last few years services have moved from DIY to online clearinghouses

Nearly every aspect of the underground economy that supports commercial crime operations has been automated
— Washington Post

- See service-specific examples in later slides

As in the real world, corporate mergers and takeovers occur

- After initial rivalry, Zeus development and support was taken over by the SpyEye developers
- (This is a standard technique used by malware authors to start afresh when their existing product has attracted too much publicity)

Malware as a Service (ctd)

Whatever this is, we've got lots more of it

- Arrest one spam gang and three more drop in to fill the gap
I don't believe it [widely-publicised bust of "the largest spam operation in the world"] has made any statistically significant difference to spam levels at all. If one spammer disappears there are plenty more to take up any slack
— Paul Ducklin, Sophos

Malware as a Service (ctd)

Pay-per-install (PPI) sites pay affiliates to install malware

EARNING4U.COM ENTER STATS

BETTER RATES! NO HOLD!
ONLY REAL ONLINE STATISTIC!

REGISTER TODAY

→ MAIN → ABOUT US → CONDITIONS → RATES → FAQ → CONTACTS

The partnership program «Earning4u» is the easiest way to earn money.
All you need to do to start working with us is [register](#).

You will earn from **6\$(Asia) to 180\$(USA)** per 1000 installs. You can view all prices in the «Rates» section.

Key Features

Thanks to an individual approach to each client when you work with our system you have:

- Online statistics updated in real time
- A 24-hour support service ready to answer all your questions
- Absolutely no shaving and total independence of your statistics from other system users
- Stable weekly payments on virtually all payment systems: Fethard, WebMoney, Wire, e-gold, Western Union (WU), MoneyGram, Aneik and ePassporte, and PayPal
- For regular clients and for those making more than 5000 installs per day – higher rates for all countries and special working conditions

We have more than 8 years' experience in working with installs. Our regular clients include more than 1000 webmasters who are all pleased to work with us.

Malware as a Service (ctd)

Standardised PPI rates for different geographic regions

Our Rates

Country:	Rate in \$ for 1000 installs:
United States	180
United Kingdom	110
Netherlands	30
France	30
Poland	20
Italy	65
Germany	30
Spain	30
Australia	55
Greece	30
Other	20
Asia	8



* We also reserve the right to delete any account
* And remember – all SPAM is prohibited!

- Except Russia, Ukraine, etc
- Most sites explicitly exclude targets in these regions

Malware as a Service (ctd)

Alternatively, pay someone else to do your installs for you



The screenshot shows the InstallsMarket website. At the top, there is a header with the logo "InstallsMarket" and the tagline "You pay - We install your stuff! And nothing more!". Below the header, there are two tabs: "About company" and "Statistics". The "About company" tab is active, displaying a paragraph of text and a "Pricelist" button. The "Pricelist" button is also active, showing a table of services and prices. To the right of the table, there is another "About company" section with a list of support IDs.

InstallsMarket
You pay - We install your stuff! And nothing more!

About company

We offer you a new, high-quality installs service. Our service offers you unique clean installs, with the option of selecting individual countries. The selection price will depend on the pricing prices for each separate country. At the same time, there are no setups. You can run a small test of 20-50 items to check your software for an individual country or a 50-100 files (free); however, this option is offered on a one-time basis and only to a new customer. But keep in mind that effectiveness indices will mainly depend on the crystal and code of your software. The minimum order is 1k; downloading is accomplished by a not resident loader. No claims are accepted in case of a satisfactory test and subsequent order for the same file.

Statistics

Pricelist

Country/Region	Price	Installs per day
Mix(all countries)	\$15	50-80k per day
Europe(mix without asia)	\$30	30-50k per day
Asia	\$7	20-30k per day
United States	\$100	5-20k per day
United Kingdom	\$160	500-1000 per day
Germany	\$100	1000-2000 per day
Italy	\$100	1000-2000 per day
Other Countries	\$20-300	50-10000 per day

About company

- Support #1: ICQ 599684321
- Support #2: ICQ 352503
- Support #3: ICQ 443598620
- Support #4: ICQ 462669012
- Support #5: ICQ 593182048
- Support #6: ICQ 583478236
- Support #7: ICQ 414888476

Malware as a Service (ctd)

Stats for one site...

Date	RAW INSTALLS	UNIQ INSTALLS
26 Jul 10 - 01 Aug 10	3324062	757220
02 Aug 10 - 08 Aug 10	3345175	783291
09 Aug 10 - 15 Aug 10	3016733	765660
16 Aug 10 - 22 Aug 10	3246990	745198
23 Aug 10 - 29 Aug 10	268351	63227

Malware as a Service (ctd)

If you have a pulse, you're a target

- Phish children on Neopets
What's the point of stealing a 12 year old's information? You can sell their account/neopoints/rare items on Ebay. The user may have an [Xbox Live] account you can take
- Offer them Neopets e-gadgets/toys
- Link to external web sites with programs to install to get the toys...
i love it sooo much. i'm gonna get on this like now. stupid 12 years olds
- Their parents do their online banking from the same family PC, so...
im tying this definatly but with my botnet

Example: Information Stolen by Malware

Malware code is often written very simply and quite securely, server administration isn't nearly as good

The person that operated this server had no clue on security, he had no clue how to configure a web server. He just took a toolkit and started to use it and in three weeks he managed to have this treasure trove on his server

— Yuval Ben-itzhak, CTO, Finjan

- More recent updates contain IDS-style defence mechanisms to keep out the good guys
- IDS is based on tracking of bot unique IDs, history of data submitted from that source, ...

Example: Information Stolen by Malware (ct)

A single malware server scanned 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 once the researchers had recovered it

Example: Information Stolen by Malware (ct)

During [the infection peak], attacks using only modestly successful distribution methods — email or six-month-old browser exploits, for example — collect more than 1 GB (gigabyte, or approximately one billion characters) of stolen data from infected users' PCs each day

— Don Jackson, SecureWorks

(Russian malware industry is very careful not to soil its own nest. Stealing from foreigners is fine)

- More recently there has been limited targeting of Russian businesses
- Possibly newbies who don't know the rules
- Many bots contain code to specifically avoid hitting Russian hosts, e.g. by checking system locales or using GeoIP

Example: Information Stolen by Malware (ct)

Another server investigated by a security company contained 1.4GB of

- Patient data
- Bank customer data
- Business-related email
- Outlook files containing email records

Yet another server was investigated by security firm SecureWorks

- Single botnet C&C server contained 50GB (!) of data
- Everything was neatly indexed in an SQL database
 - Talk about business intelligence!

Example: Information Stolen by Malware (ct)

University of Mannheim researchers tracked information captured by two bots, Limbo/Nethell and ZeuS/Zbot/Wsnpoem

- 33 GB of data
- 11,000 stolen bank accounts
- 150,000 stolen email accounts
- This was less than a third of the total (only a subset of the information harvested could be accessed)

Example: Rock Phish

Industry-leading innovators in phishing...

- So-called because they used to store their content in a `/rock` directory on compromised servers

Owned nameservers and wildcard DNS

- Avoids blacklists
- Each target gets their own personal phishing URL to go to

Register huge numbers of domains like `abc123xyz.com`

- Send out phish for `http://www.bankname.com.[...]abc123xyz.com`
- Defeats blacklisting since it's impossible to track and blacklist all those domains

Example: Rock Phish (ctd)

Everything is done via redirectors

- Nothing to target or take down

All data is stored in memory

- No files on disk or other traces to recover

Example: Rock Phish (ctd)

Estimated US\$0.5 – \$1B/year revenue

- No-one's sure where these figures come from. Rock Phish don't publish an SEC filing

We sell all you need to hack, shop & cashout.

Cvv2 = UK, EU, ASIA, CA and AU

VBV (Verified By Visa) = UK and US only

VISA CLASSIC|MASTERCARD \$5 <> \$3 per 30

VISA PLATINUM|BUSINESS \$10 <> \$7 per 30

VISA SIGNATURE \$20 (when available)

Bank Details e.g Acct #, Routine and so on... and Background details e.g SSN, DL, MMN, DOB and PIN

Example: Rock Phish (ctd)

Some of the people behind this are really, really scary

- This is established, organised crime

Example: Anti-cybercrime investigator in Russia working with the St.Petersburg police

- One of his teenage daughters, living in a western country, is kidnapped
- “If you drop the case, the rest of your children might be OK”
- Five years later she's located in Kazakhstan
She was fed drugs and used to service men
— Joseph Menn, author of “Fatal System Error”

These are people you don't ever want to mess with

Malware via the Affiliate Model

Pay others to infect users with spyware/adware/trojans

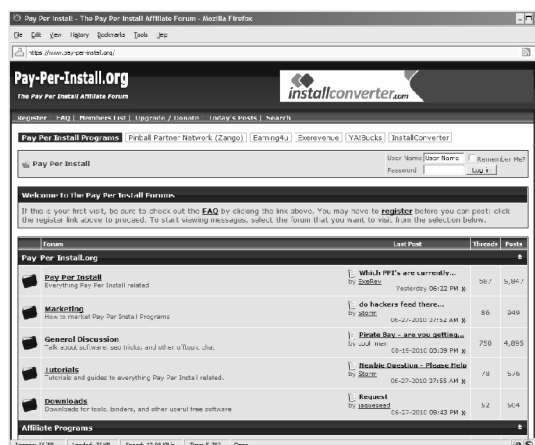
Business model was pioneered by
`iframedollars.biz`

- Pays webmasters 6 cents for each infected machine
- Alternative payment model is weekly fixed-rate payouts via PayPal, e-Gold, Western Union
 - Fixed-rate deals require a minimum of 1,000 installs
 - Bonuses paid 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)

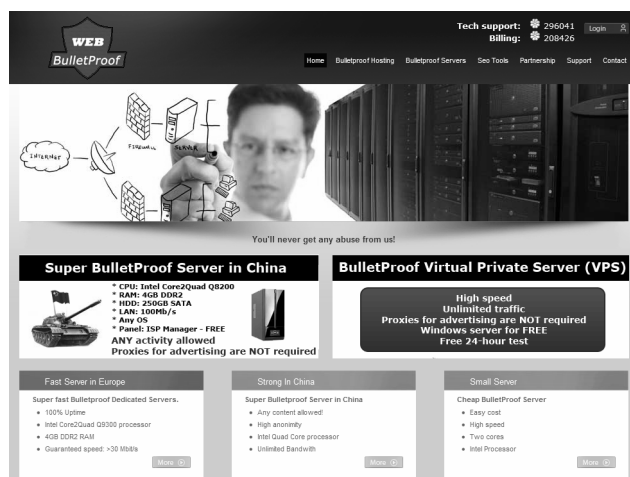
Malware distribution is also a standardised service



- Note the use of SSL – because organised crime deserves CA recognition as well

Malware via the Affiliate Model (ctd)

But who would actually host something like this?



The screenshot shows the BulletProof website interface. At the top, there is a navigation menu with links for Home, Bulletproof hosting, Bulletproof Servers, Site Tools, Partnership, Support, and Contact. The main content area features a large banner with a man looking at a server rack and a diagram of a network. Below the banner, there are several server hosting options:

- Super BulletProof Server in China**: CPU: Intel Core2Quad Q8200, RAM: 4GB DDR2, HDD: 250GB SATA, LAN: 100Mbps, Any OS, Panels: ISP Manager - FREE. ANY activity allowed, Proxies for advertising are NOT required.
- BulletProof Virtual Private Server (VPS)**: High speed, Unlimited traffic, Proxies for advertising are NOT required, Windows server for FREE, Free 24-hour test.
- Fast Server in Europe**: Super fast Bulletproof Dedicated Servers, 100% Uptime, Intel Core2Quad Q8300 processor, 4GB DDR2 RAM, Guaranteed speed >30 Mbps.
- Strong in China**: Super Bulletproof Server in China, Any content allowed, High anonymity, Intel Quad Core processor, Unlimited Bandwidth.
- Small Server**: Cheap BulletProof Server, Easy cost, High speed, Two cores, Intel Processor.

- Ah yes, someone like that...

Malware via the Affiliate Model (ctd)

iFrames: The browser attack vector of choice

- MPACK automated the deployment process to create ~10,000 iFrame-infection sites in a single day
- iFrames are often cascaded over multiple levels of redirection to improve fault-tolerance/flexibility

Anti-virus vendor Sophos reports 8,000 new iFrame webpages per day

- 70% are on legitimate websites (via compromised machines)

Malware via the Affiliate Model (ctd)

This type of exploit is yet another reason why blacklists will never work...

- 70% of phishing victims are caught in the first 12 hours of a phishing site's life

Example: In August 2007, the Bank of India website was compromised

- Served 22 pieces of malware to anyone visiting it
- Most of the online trust rating organisations (Netcraft, McAfee SiteAdvisor, Google Safe Browsing, ...) reported it as safe to visit during that period

Malware via the Affiliate Model (ctd)

Even uninfected legitimate sites have ended up serving malware via third-party paid ads

TV viewers are accustomed to adverts getting in the way of what they want to watch. They're probably not as used to adverts on their favourite TV websites delivering unwanted code straight to their desktops

— "Poisoned TV website adverts lead to PC and Mac scareware"

Q: What's the widest-coverage way to get your malware onto people's desktops?

A: Google adwords

Malware via the Affiliate Model (ctd)

This doesn't affect just Google though...

Malware that exploits holes in popular applications is being delivered by big ad delivery platforms including those run by Yahoo, Fox, and Google [...] Users don't need to click on anything to get infected; a computer becomes infected after the ad is loaded by the browser

— CNET News

- The technical term for this is 'malvertising'

Use Javascript in banner ads to infect machines (Prontexi)

- Affects yieldmanager, doubleclick, fimservice, xtendmedia, vuze, specificclick, bidsystem, ...

In one case it was done by impersonating a legitimate advertising company to the ad networks

Malware via the Affiliate Model (ctd)

The scope of some of these automated infections is staggering

At the time of writing, Google searches showed almost 520,000 pages containing the [malware] infection string

— The Register

- One of the infected sites was the Department of Homeland Security

Interacts badly with user education telling people that they're OK on "safe" sites

- Real-world studies have shown that users don't bother about security in these cases, for example by disabling anti-virus scans ("risk compensation")

Malware via the Affiliate Model (ctd)

Malware: AJAX' killer application

- Use Google to locate vulnerable web applications
 - About half of all reported vulnerabilities in 2007 were in web apps (SANS Institute)
- Vulnerabilities were reported at the rate of several hundred (!) a week

Deployment scripts turn the web app into a malware server (drive-by downloads, phishing, ...)

- Search worms of this kind provide fast, massive-scale propagation
- One web-app honeypot measured 368,000 attacks from 29,000 hosts over a two-month period

Example: Asprox botnet

Use Google to search for servers running ASP.net

Run automated SQL injection attacks on any servers found

- Injected SQL payload searches the web server for web pages
- Injects an iframe into the pages
- Redirects site visitors to (constantly-changing) attacker-controlled servers
 - Redirection is masked through various tricks such as conditional redirection, redirection only for external visitors coming from search engines, redirection based on client browser type, ...

Example: Asprox botnet (ctd)

Google analysed the subset of Asprox-infected sites that their search covered

- 153,000 different web servers
- Six million URLs across those servers

Malware via the Affiliate Model (ctd)

The iFrameBiz business model incentivises customers to register large numbers of domains

- Drop the exploit on each site and hustle visitors

Malware distribution handled via online brokers

LoadsForYou - это приемлимые цены, оперативность, надежность и быстрая скорость отгрузки всех стран. Имеются разные предложения для Вашего бизнеса, для крупных заказов предусмотрена удобная система скидок

- Efficient, reliable, fast delivery to all countries. Discounts for bulk orders

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
 - DollarRevenue were very successful in their day because they paid reliably, and had a reputation for paying (no honour among thieves)

Malware via the Affiliate Model (ctd)

T&C generally claim that they'll terminate affiliates who do anything unethical

- Yeah, right
 - Blame for improper behaviour was diffused over a complex web of affiliate relationships where the guilty party was always one elusive step away
 - “Crimeware Business Models”, David Cole

Seized IRC logs from DollarRevenue show they knew exactly what they were doing, even though they claimed in public to be unaware of abuse

Malware via the Affiliate Model (ctd)

See www.klikteamparty.com for one company's end-of-year party (NSFW!)



- Mercedes C-Class and Vaio laptops as prizes, strippers...

Malware via the Affiliate Model (ctd)

Completely automated exchanges/clearing houses for click fraud exist

Robotraff is the first automated stock exchange of the traffic, here you can buy the traffic by criteria interesting you and also to sell - under the price favorable to you.

Tasks of our resource include creations of comfortable conditions both for sellers and for buyers, maintenance of the account of the traffic, money resources, guarantees for buyers of receipt of the traffic, and for sellers of duly payment

— robotraff.com

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 (Gumblar)
 - Anti-adwords, sell terms to redirect users to malware sites
- 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)

Use compromised high-pagerank sites to redirect users to a fake Google site

- Users click on a link from the real Google and are switched to an indetical (fake) Google
- Fake Google links only to attacker-controlled sites
- All implemented as a complex interlinked mesh ("constellation")
- Highly damage-resistant/fault-tolerant

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 via the Affiliate Model (ctd)

Bundle malware alongside legitimate software scraped from distribution sites

Syndication is the best way to get free content and get paid for it! You can choose from different games, audio, software, multiple free videos for your website. For every new InstallConverter install produced from any country we credit for, InstallConverter gives you money

- Use black-hat SEO techniques to get your site rated highly
- Victims hit your malware-laced copy of Ashampoo Studio before they get to the real one

Dogma Millions has hundreds of affiliates and probably collects over 500,000 unique installations each month

— “The Underground Economy of the Pay-per-Install Business”

Malware via the Affiliate Model (ctd)

Selling adware as a service

- Develop or license various dancing-bunnies applets
- Distribute them as free, ad-supported software
- EULA allows installation of additional software
- Once you have x million installs, go to every other adware distributor and offer to install their adware at 10 cents a machine

The Malware Business

Entire attacks can be commissioned via clearinghouses or brokers (e.g. the Russian UPLEVEL group)

- Send out an RFP for a job
- Vendors submit bids
- Winner is awarded the contract

Exactly like standard IT contracting, only in broken English

The Malware Business (ctd)

We sell balances in CHASE, BOA, CREDIT UNION, HALIFAX, HSBC, ABBEY, SMILES, COMPASS, WELSFARGO, WACHOVIA BANKS. Contact us for other.

BALANCE 1K TO 20K 150\$

BALANCE 20K TO 50K 250\$

BALANCE 50K TO 80K 350\$

BALANCE 80K TO 150K 520\$

BALANCE OVER 150K 800\$

PAYPAL VERIFIED 40\$

PAYPAL VERIFIED with 2000\$+ BALANCE 160\$

Example: Russian Business Network

Originally run as a standard malware business network
hosting various services

- The more attention your operations drew to the RBN, the more they charged you for hosting

The RBN as a whole became too high-profile, and various attempts were made to shut them down

- Response: Reorganise, reroute, and rearrange
- The whack-a-mole effect

Example: Russian Business Network (ctd)

Most of the RBN's hosted services are still hosted, but now everything's distributed, decentralised, diffused...

Killing one source results in five more harder-to-kill ones popping up

- With the original RBN at least you knew where it was

RBN is significant enough that it's tracked via a dedicated blog, rbnexploit.blogspot.com

Example: Russian Business Network (ctd)

Other malware groups maintain backup links owned by shell companies

- When malware host McColo was forced offline, it waited until the weekend and then fired up a backup link via another ISP to relocate the control infrastructure for the Rustock botnet to the RBN
- 12 hours of traffic at up to 15 MB/s before that too was shut down
- The host is gone, but the malware has moved elsewhere

Other McColo-hosted botnets like Srizbi were built to be immune to blacklisting/takedowns and were barely affected at all

Example: Russian Business Network (ctd)

Another McColo-hosted botnet, MegaD, survived the shutdown equally well

- It then survived a second attempt at a takedown that specifically targeted it
In both cases MegaD initially ground to a halt, but then quickly bounced back with greater vigor
— Insights from the Inside: A View of Botnet Management
- Second takedown attempt was probably avoided by using PPI to reboot the botnet

Example: Russian Business Network (ctd)

Shutting down the host doesn't shut down the botnet

- One honeypot experiment observed that nearly half of their attacks were from orphan botnets
- Controller is gone, but the botnet keeps on infecting

It's the attack of the undead malware zombies!

Example: Prg trojan/Zunker botnet

Implemented as part of a complex micro-economy

- c.f. Photoshop industry: Plugins, filters, clip art, books, training, consulting, artists for hire, ...

Prg is a malware delivery agent and client for the Zunker botnet

- Evolved and mutated over time, Zeus, Zupacha, Zbot, ...

Some variants are generic, some are targeted

- Banker
- Broker

Example: Prg trojan/Zunker botnet (ctd)

Prg/Zeus trojan is the basic framework, customisation is done via plugins

Distributors (e.g. the Russian UPLEVEL group) tailor solutions for individual clients

- Collect customer requirements
- Provide attack profiles for the botnet client
- Provide plugins to exploit this
- Deliver it to customers alongside referrals to affiliates for services like hosting, cashiers, etc

Like the RBN, Zeus has its own site that tracks it

<https://zeustracker.abuse.ch/statistic.php>

Malware Then and Now

People expect Hollywood-style effects from malware

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

Viruses always have visible symptoms. The respondents spoke of computer viruses mucking with their data, viruses that slowed down or broke the computer, and viruses that cause strange new behaviors like popups or spam email. Only one respondent talked about viruses that might go unnoticed by the user of the computer

— “Mental Models of Home Computer Security”

Malware Then and Now (ctd)

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

Malware Then and Now (ctd)

“My computer’s misbehaving, it must be a virus”

- If it was a virus, you wouldn’t notice anything
Worms like Storm [...] spread more subtly, without making noise. Symptoms don’t appear immediately, and an infected computer can sit dormant for a long time. If it were a disease, it would be more like syphilis, whose symptoms may be mild or disappear altogether, but which will eventually come back years later and eat your brain
— Bruce Schneier

Malware Economics

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

- Only if you ignore the money factor
Firefox has a community of web developers and hobbyists who build cool applications for it while most of the folks extending Internet Explorer in the Windows world are writing spyware and other kinds of malware
— Dare Obasanjo

Malware Economics (ctd)

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)?

Malware Economics (ctd)

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

Most adware targets Internet Explorer (IE) users because they're the biggest share of the market and they tend to be the less-savvy chunk of the market. If you're using IE then either you don't care or you don't know about all the vulnerabilities that IE has

— Matt Know, DirectRevenue adware developer

Malware Economics (ctd)

Internet prime directive (the end-to-end principle):

Intelligence is concentrated at the network edges

Market reality: Users control their own computers

Intersection of the two: Users control the Internet in terms of viruses, spam, malware, etc

- Backbone provider AT&T reports detecting a *million* new bots a month using their backbone traffic logs

Red Queen Effect

- The good guys have to run as hard as they can just to keep up with the bad guys

Malware Economics (ctd)

When you hear about “the XYZ botnet” it’s referring to a product class like “Windows Server 2008”, not a particular instance

There isn’t just one Zeus botnet out there, there are hundreds if not thousands of them

— Roel Schouwenberg, Kaspersky Labs

- Users buy a copy of the XYZ botnet software and use it to run their business

– c.f. “ ” “ ” “ ” “ Windows Server 2008 ” “ ” “ ” “ ”

When you look at the Zeus business model, it’s a package that anyone can purchase to conduct attacks that can be monetized in one way or another

— Roel Schouwenberg, Kaspersky Labs

Malware Economics (ctd)

The vendors of these business tools run into the same problems that more legitimate vendors do

- Users pirate their products
By involving professional programmers, many of whom have University diplomas, malware development becomes a very expensive process. Thus, the malware kit price climbs up, and then its developers need protection from piracy
— Sergei Shevchenko, PC Tools
- Some vendors responded with node-locked licenses and similar license management tools
[The Zeus vendors] introduced a hardware-based activation process similar to Windows activation, to make sure only one purchased copy of the ZeuS kit can run on one computer
— Sergei Shevchenko, PC Tools

Example: Torpig trojan

US Federal Financial Institutions Examination Council (FFIEC) required that banks use two-factor authentication

- Banks redefined “two-factor authentication” to mean “twice as much one-factor authentication”
- Could be “compliant” without having to do anything

Torpig trojan doesn't just steal the victim's credentials but also

- Obtains browser information
- Fetches stored cookies
- Sets up HTTP and SOCKS proxies on the victim PC

Example: Torpig trojan (ctd)

Has a knowledge base of 2,700 banks and e-commerce sites used to customise the attack

- Injects new content into web pages requesting further user data
- The later Clampi trojan contained custom profiles for at least 4,600 different web sites

Example: Torpig trojan (ctd)

Pretend two-factor authentication uses as a second factor

- Browser cookies
- IP address/browser agent
- Other, similar trivia

Torpig defeats this pretend authentication without even trying

- Trojans were doing this even before the FFIEC ruling had been implemented by banks, so the pretend auth was defeated before it was even deployed

The Spam Business (ctd)

Historically done via

- Open relays
- Pink contracts

More recently botnets

- Easily available
- Defeats blacklists

Even more recently spam has moved to Hotmail, Gmail, ..., again to defeat blacklisting

The Spam Business (ctd)

Mass account signup is done via commercial CAPTCHA-breaking operations

I m from Bangladesh. We r a group worker who solve captcha image for money. We are working on another captcha project, too and deliver 50000 captchas/day. Let us working4you. our rate is \$ 8 for per 1000 captcha solved. I m waiting for ur response.

Thanks, admin, Raki IT Group

I'm from VietNam. We have a group with 20 person. We working some site rabot, rubl, look... Our rate just 4\$ for per 1000 captcha solved. We hope work you
Best Regard, QuangHung

The Spam Business (ctd)

CAPTCHA-breaking for spam purposes is handled via online clearinghouses

According to some of the statistics obtained [CAPTCHA breakers] earn over ten times more while solving CAPTCHAs than through their legitimate data processing jobs

— Dancho Danchev, ZDNet

Post requests for service, receive back work bids

Hi! I need professional work team for data entry (captcha job). Team must be online 24/7. Must provide capacity minimum 100K daily. Payment E-Gold or WebMoney only. Payment weekly or every 48 hours. Happy bidding!

The Spam Business (ctd)

Ready to provide 24/7 service for 100K captcha entries daily @ US \$1.5 per 1000 Entries

We are the team of more than 106 people (Members are increasing in). We have experience data entry, captcha entry 2 years, working available 60 hours per week, 24 hours 7 days a week if needed. IP can be converted. We can finish min 100k captcha per day

hi, my team is composed of experienced captcha encoders, we were working for several projects already from various employers. we can start soon if given the opportunity, we bid for 6USD/1000 captcha. assurance of accurateness per transaction

- Targeted towards westerners, e.g. India/Pakistan/Bangladesh-based companies rate in 100K rather than lakh

The Spam Business (ctd)

There are even specialised sites set up just for the CAPTCHA-breaking business



The Spam Business (ctd)

The investments made in purchasing the PCs, the web proxies, the training and education of the staff, as well as the sophistication of the web based applications aiming to empower non-technical users, clearly explain why India remains the market leader in CAPTCHA solving, with thousands of legitimate data processing workers converted to CAPTCHA solvers

— Dancho Danchev, ZDNet

The Spam Business (ctd)

Spamming 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

Example: Zeus Banking Trojan

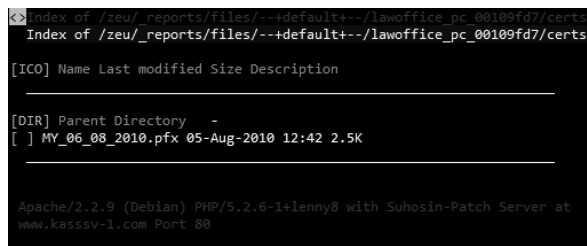
Basic Zeus kit does the usual

- Steals client-side credentials
 - Steals HTTP form data
 - Redirects victims to attacker-controlled web pages
 - Locates and uploads files from the victim's PC
 - Screen-scrapes content, takes snapshots of the victim's screen
 - Downloads and executes binaries
- Zeus is sold in the criminal underground as a kit for around \$3000-4000, and is likely the one malware most utilized by criminals specializing in financial fraud
— “Zeus Banking Trojan Report”

Example: Zeus Banking Trojan (ctd)

Additional functionality

- Steals X.509 certificates and keys
- Allows back-connects from the victim's PC to defeat location/address-based checks
- Uses Jabber IM protocol to notify botmaster of credentials in real-time to defeat time-based OTP tokens
- Allows complete control of a victim PC via VNC
- Uses node-locked licensing to tie it to the machine for which the license is purchased



```
Index of /zeu/_reports/files/---default---/lawoffice_pc_00109fd7/certs
[ICO] Name Last modified Size Description
[DIR] Parent Directory -
[ ] MY_06_08_2010.pfx 05-Aug-2010 12:42 2.5K

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch Server at
www.kasssv-1.com Port 80
```

Example: Zeus Banking Trojan (ctd)

Support for Vista and Windows 7 infections costs extra

- Default is XP only

Special support for ACH fraud

- On-demand scripts work like SQL triggers to perform given takes when the victim takes a certain action
The CTU [SecureWorks Counter Threat Unit] has observed ZeuS databases for sale on various underground black markets. Their size is typically over 10GB
— “ZeuS Banking Trojan Report”

Example: Zeus Banking Trojan (ctd)

Hi all,

we offer unlimited access to running Zeus banking trojan control panel. You can use all features including the control panel like searching in database, socks, scripts, etc.

The Botnet started on the 29.10.2009 and is still raising. Now it has 560 Bots included

Countries are mainly GB and Europe.

System does still load new bots by drive by exploits. We guarantee about 100 new bots a day.

The rate is for one month 150 US\$. Minimal time is three month.

If interested PM me.

Greets, dapin

--BotNetService>Netherlands--

The Carding Business

Prices are openly published or subject to private negotiation

- A “dump” in carder jargon, dump of the magstripe info

DUMPS+PIN:-

US Classic, Platinum, MC Standard \$250

US Gold, Purchasing, Signature \$300

US MC World, Business, Corporate \$350

DUMPS+PIN:-

EU/ASIA Classic, MC Standard \$150

EU/ASIA Gold, Platinum \$250

EU/ASIA Business, Corporate, Infinitive \$350

The Carding Business (ctd)

Advertising is done via hijacked online forums

- Find a web board discussing cars, clothes, planting tips, children's toys, ...
- Post your ad with appropriate carder keywords
- Wait a few days for Google to find it

We Supply Dumps, Fullz, Cvv2, Logins....

Cvv2 = UK, EU, ASIA, CA and AU

VBV (Verified By Visa) = UK and US only

FULLZ COME WITH : CC Details e.g CC #, Address, Cvv and

rest Bank Details e.g Acct #, Routine and so on... and

Background details e.g SSN, DL, MMN, DOB and PIN

Dumps/Cvv2 checking service also available.

BANK LOGINS FOR SALE TOO, CONTACT ME WITH THE BANK COUNTRY AND THE BANK NAME.

The Carding Business (ctd)

Discounts available for buying in bulk

Discount : Correct discount ask in icq.

100 pcs usa classik 1800\$

100 pcs usa platinum 3500\$

100 pcs usa amex 1800\$

100 pcs usa discover 2500\$

100 pcs canada classik 2300\$

100 pcs canada gold 4500\$

100 pcs europa classik 7000\$

100 pcs europa platinum 9000\$

Payment by wu, mg, wnz.

The Carding Business (ctd)

Carders have ebay-style reputation rating systems

- #rippers on carder IRC nets
- (Free samples are also used to prove that you're not a ripper)

Malware forums also have rating systems for malware, but it's less of a deal than with carders

dont buy from goldkingz@yahoo.com
i sent 200 dollars to him he ripped me

The Carding Business (ctd)

Cards can be bought by region and/or BIN

- BIN is the issuing bank prefix
 - Banks refused to let anti-malware researchers see these “for security reasons”
 - Security researchers got the BIN lists from malware instead

No-charge card validity checks are typically done through pre-auths

- Formerly done mostly for hotels and rentals, but now commonly used when buying petrol with a swipe-only transaction

The Carding Business (ctd)

Funds are moved into drops

- Compromised bank accounts used to launder funds

BANK TO BANK TRANSFER TO ANY COUNTRY

>RECEIVE 1000\$ 200\$

>RECEIVE 2000\$ 380\$

>RECEIVE 5000\$ 900\$

>RECEIVE 1K 1300

– (Last is probably a typo for 10K)

The Carding Business (ctd)

Scammers are big fans of online banking, especially via other people's accounts

Transfer OnLine

1000\$ 50\$egold

2000\$ 100\$egold

3000\$ 150\$e-gold

4000\$ 200\$e-gold

5000\$ 250\$e-gold

6000\$ 300\$e-gold

7000\$ 350\$e-gold

8000\$ 400\$e-gold

9000\$ 450\$e-gold

10,000\$ 500\$e-gold

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
 - Or buy WU accounts and do it yourself
 - WU BUG \$300
 - WU ADMIN + PIN 1MONTH \$150
 - WU ADMIN + PIN 3MONTHS \$350
 - WU ADMIN + PIN 1YEAR \$1000
- (WU ADMIN allow you to cash out \$3000 per order. WU BUG will only allow 900\$)

The Carding Business (ctd)

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

Use of modified gift cards is popular

- Write the credentials from a high-value stolen card onto the gift card
- Cards are anonymous and signature-less, no checking by merchants

The Carding Business (ctd)

Perfect copies of cards can be mail-ordered

Manufacturing plastic of bank quality is made on the newest equipment with use of own technologies.

We make following kinds of cards:

MasterCard / Visa / AMEX

We guarantee a correct bank microfont, with an excellent strip of the signature. Quality card 2800 dpi. The design of a card is identical to the bank original. Holograms on cards are IDENTICAL to the presents. The price 120 USD for 1 ready card. Cost is not included in cost of plastic dumps. Minimal order of 4 products of the given type.

Payment Webmoney, Westernunion, E-gold. Sending made at the first 24 o'clock after reception of money.

The Carding Business (ctd)

You can even run your carding business from prison!

- All you need to do is have accomplices outside cashing out the accounts

[The] gang would purchase stolen credit-card information from websites based overseas. Using inexpensive credit-card encoders, [outside affiliates] then programmed the information onto the magnetic strips of credit cards

— “Rikers Island inmate’s alleged credit card scam netted \$1 million from iPads and Apple computers”

The ring spanned 13 states and the District of Columbia. It was so easy and lucrative that one gang member who was a shopper branched out to form his own syndicate

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 prepaid 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.

Example: vendorsname .ws (ctd)

One possible way to handle COBs is via Address Verification System (AVS) spoofing

- AVS only checks the street number and Zip code (if the country uses Zip codes)
- 100 Foo Ave, Fooville, CA 90210 and
100 Bar Ave, Barville, CA 90210
are identical for AVS purposes

Alternative is to use standard social engineering

Sell COB/price here

USA 50\$

CANADA 50\$

UK 100\$

(COB minimum order 50\$)

The Carding Business (ctd)

Recruit money mules via job sites like monster .com

- Work from home! Earn up to \$xxx/week!
The mule recruiters also have perfected the art of impersonating established online businesses. In nearly every money mule scam, the fraudsters build fake store fronts by copying the names, trademarks and Web content of legitimate online companies
— Brian Krebs, Washington Post

The Carding Business (ctd)

I'm Seller for: CC, US, UK, CA, EURO, AU, Italian, Japan, France, ger, asian...all cc (all Country). Paypal verify, Software Spam mail + mail list, code PHP,Shop Admin and CC fullz info, CC DOB, cc Dump, Pri sock....Domain hosting.

UK FULLZ 10\$ / US FULLZ 5\$ / EU FULLZ 15\$ / CA FULLZ 5\$

Fullz Have the following Information:

- * CardTipe / * CC Name / * CC Number / * CC Expiry / * CVV2 / * CC PIN
 - * First & Last Names / * Address & City / * State & Zip/Postal code / * Country (US) / * Phone #
 - * MMN / * SSN / * DOB
 - * DSL
 - * Bank Acc No / * Bank Routine No
- (Fullz MINIMUM ORDER 50\$)

The Carding Business (ctd)

Victims are offered jobs as “financial managers”, “re-shipping agents”, “*\$countryname* representative”, or “funds transfer agents”

- Receive payment via PayPal, cash out, forward via Western Union
- Mules get 10% commission on transfers

Some are genuine dupes, some are fully aware of what they're getting into

We have large amounts of funds on numerous bank accounts which needs to be laundered. We need your help to do that

Monetising your Stolen Data

Everything can be monetised

Obvious accounts: Banks, PayPal, ...

Less obvious accounts: Stock brokerage accounts

- Buy stolen accounts at E-Trade, TD Ameritrade, JP Morgan Chase, Charles Schwab, ...
- Dump the existing portfolio
- Set up an E-Trade account and buy microcap stocks
- Use the stolen accounts to drive up your microcap stock prices in pump-and-dump
 - Cuts out the need to pump the stock
- Implements a proxy transfer of funds from the brokerage account to your account

Monetising your Stolen Data (ctd)

Target “worthless” databases containing no sensitive information

- Just names, addresses, contacts, etc
 - Monster.com job-seeker lists
 - Salesforce.com customer lists
- Vendors issue soothing press releases that there’s nothing to worry about
 - “The stolen information did not include any sensitive information such as social security numbers or credit card information”

Monetising your Stolen Data (ctd)

Use your newly-acquired “worthless” information to perform social phishing/spear-phishing attacks

- Additional information “that only a legitimate source would know” greatly increases the chances of success

The end result is that a far higher percentage of recipients actually open the poisoned attachments, and in some cases even forward the message on to a trusted friend, co-worker, or subordinate

— Brian Krebs, Washington Post

Monetising your Stolen Data (ctd)

No accounts at all: Botnets used for click fraud
(Clickbot.A)

- Advertisers like clicks, they get feedback on effectiveness

Redirect Google searches to a fake Google page (Bahama)

- Search-result links are masked cost-per-click ads

In its worst-case scenario, the Bahama botnet has turned as much as 30 percent of an advertiser’s CPC [Cost-per-Click] budget into click fraud

— IDG News

Monetising your Stolen Data (ctd)

Indirect click fraud

- Malware replaces affiliate ID in cookies with its own
- As soon as a cookie is set, it gets the desired affiliate ID added to it
- Merchant site checks cookie for the referrer, affiliate gets paid

Google claims that about 10% of clicks are fraudulent, representing ~\$1B in billings for just Google alone

- Others have put the fraud rate as high as one third of all click-throughs

Monetising your Stolen Data (ctd)

Google and others boost revenue by recycling ads to other sites

- Example: Domain parkers fill parked domains with ads

Dell lawsuit over trademark-infringing domains used for this purpose reveal how much money is involved

Google [...] was ordered to hold in a special account the first \$1 million collected on behalf of the defendants each month. The second \$1 million that accrues in the account every month will be given to the defendants. If more than \$2 million accrues in one month, the money is split between the defendants and the Google account

— IDG News

Monetising your Stolen Data (ctd)

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
- Hordes of commercially available clickbots like Fake Hits Wizard, I-Faker, FakeZilla, Magic Traffic Bot, Professional Proxy Clicker, and Clickmaster can manage this for you

Monetising your Stolen Data (ctd)

The relentless quest for ad impressions is skewing the entire Internet economy

- Anything to drive clicks to your site

Trivial example: Google arbitrage

- Buy cheap ads on Google to get people to visit your site
- Have them leave via expensive ad links
 - Little incentive for anyone involved to fix this

But that's barely scratching the surface...

- You can do much better than this

Monetising your Stolen Data (ctd)

Example: The software awards racket

- Author submits software to a download site
- Many sites automatically give the software a five-star rating
- Some of them look quite impressive, but none of them are worth the electrons it takes to display them
 - “The software awards scam”, Andy Brice
- Author puts the rating on their site with a link back to the download site
- Increases the download site’s page rank and traffic/number of ad impressions



Monetising your Stolen Data (ctd)

Example: Pingback ad-hosting

- Set up fake blogs in ephemeral domains (e.g. domain-tasting domains)
 - Or use long-term domains, e.g. `www.247blogging.info`
- Search for genuine blogs containing keywords matching the material that you’ll host on your fake blog
- Scrape the articles from the target blog(s) to your blog
 - Add a pingback on the target blog, which provides a link to your blog

...continues...

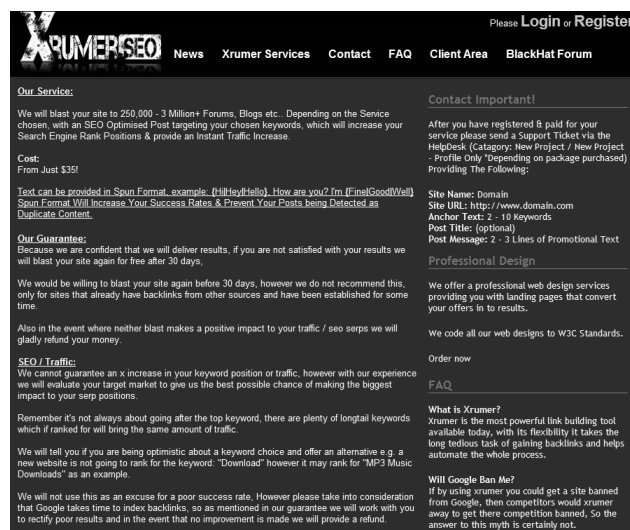
Monetising your Stolen Data (ctd)

...continues...

- You now have a high-pagerank site linking to your site that conveniently contains material similar to the original highly-ranked site
- Host ads on your now well-ranked fake blog until the ephemeral domain expires
 - Use user access stats from your fake blog to guide you in setting up new fake blogs
- With appropriate SEO techniques your scraped blogs will rate higher than the original on Google (!!)

Monetising your Stolen Data (ctd)

Supported by standard (black-hat) commercial tools...



The screenshot shows the Xrumer website interface. At the top, there is a navigation bar with the Xrumer logo and links for News, Xrumer Services, Contact, FAQ, Client Area, and BlackHat Forum. A 'Please Login or Register' link is also present. The main content area is divided into two columns. The left column contains sections for 'Our Service', 'Cost', 'Text can be provided in Spun Format', 'Our Guarantees', 'SEO / Traffic', and a disclaimer. The right column contains sections for 'Contact Important!', 'Site Name', 'Professional Design', 'FAQ', and 'Will Google Ban Me?'. The text in the screenshot is as follows:

Our Service:
We will blast your site to 250,000 - 3 Million+ Forums, Blogs etc. Depending on the Service chosen, with an SEO Optimised Post targeting your chosen keywords, which will increase your Search Engine Rank Positions & provide an instant Traffic Increase.

Cost:
From Just \$39!

Text can be provided in Spun Format, example: {Hi!Hey!Hello}. How are you? {m {FinalGood!Well} Spun Format Will Increase Your Success Rates & Prevent Your Posts being Detected as Duplicate Content.

Our Guarantees:
Because we are confident that we will deliver results, if you are not satisfied with your results we will blast your site again for free after 30 days.

We would be willing to blast your site again before 30 days, however we do not recommend this, only for sites that already have backlinks from other sources and have been established for some time.

Also in the event where neither blast makes a positive impact to your traffic / seo serps we will gladly refund your money.

SEO / Traffic:
We cannot guarantee an x increase in your keyword position or traffic, however with our experience we will evaluate your target market to give us the best possible chance of making the biggest impact to your serp positions.

Remember it's not always about going after the top keyword, there are plenty of longtail keywords which if ranked for will bring the same amount of traffic.

We will tell you if you are being optimistic about a keyword choice and offer an alternative e.g. a new website is not going to rank for the keyword: "Download" however it may rank for "MP3 Music Downloads" as an example.

We will not use this as an excuse for a poor success rate. However please take into consideration that Google takes time to index backlinks, so as mentioned in our guarantee we will work with you to rectify poor results and in the event that no improvement is made we will provide a refund.

Contact Important!
After you have registered & paid for your service please send a Support Ticket via the HelpDesk (Category: New Project / New Project - Profile Only) Depending on package purchased Providing The Following:

Site Name: Domain
Site URL: http://www.domain.com
Anchor Text: 2 - 10 keywords
Post Title: (optional)
Post Message: 2 - 3 Lines of Promotional Text

Professional Design
We offer a professional web design services providing you with landing pages that convert your offers in to results.
We code all our web designs to W3C Standards.

Order now

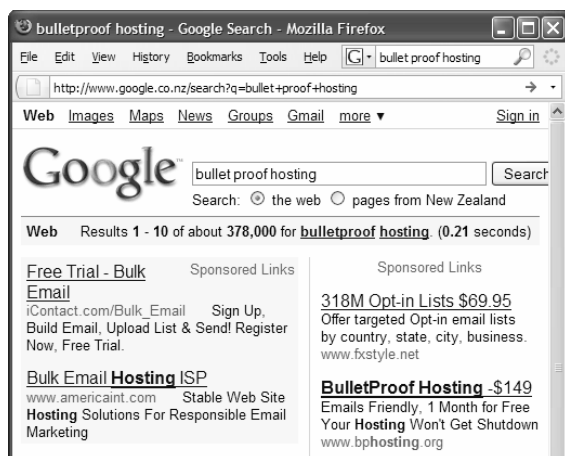
FAQ

What is Xrumer?
Xrumer is the most powerful link building tool available today, with its flexibility it takes the long tedious task of gaining backlinks and helps automate the whole process.

Will Google Ban Me?
If by using xrumer you could get a site banned from Google, then competitors would xrumer away to get there competition banned. So the answer to this myth is certainly not.

Monetising your Stolen Data (ctd)

Or cut out the middleman and advertise your malware services directly with Google adwords...



Monetising your Stolen Data (ctd)

Or just insert your spam into legitimate posts via malware

- Add URLs for porn sites to legitimate message-board postings (Submithook)

As with everything else, online clearinghouses are taking over from individuals

Robotraff.com is the first automated stock exchange of the traffic, here you can buy the traffic by criteria interesting you and also to sell - under the price favorable to you.

Tasks of our resource include creations of comfortable conditions both for sellers and for buyers, maintenance of the account of the traffic, money resources, guarantees for buyers of receipt of the traffic, and for sellers of duly payment

Monetising your Stolen Data (ctd)

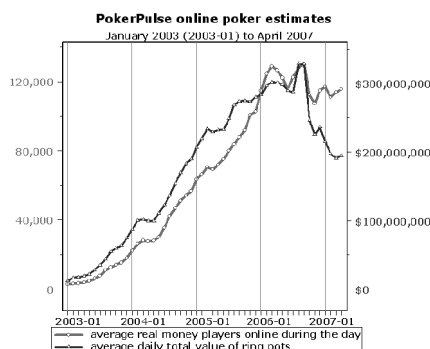
Clearinghouses provide better quality of service, oversight, value for money

- # Simple and clear system for sale of the traffic on a stock exchange
- # The detailed statistics including not only on - country the contents but also such parameters as, speed of a stream of the traffic, percentage of the version of browsers, etc.
- # Presence of elements of a stock exchange allow to organize original “game” of the prices for buyers and sellers where the market wins the most successful

Monetising your Stolen Data (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



If you're not Part of the Solution...

US banks: Make credit available as easily as possible

- People have obtained credit cards for pets, dead people, inanimate objects, ...
 - You are sending an application to a dog
 - Written on a credit card application for Clifford Dawg
 - Dog's don't chase us, we chase them
 - Chase Manhattan after issuing the dog a Platinum Visa
- ... using torn-up taped-together application forms with obviously fake/doctored information
 - Fraud starter kits
 - Police term for pre-approved credit card applications
- (See: Subprime mortgages)

If you're not Part of the Solution... (ctd)

US credit-card management is riddled with additional fee triggers and high-interest rate conditions

- Even conscientious users who always settle on time are tripped up using a whole range of tricks
- Double-cycle billing
- Banks preferentially paying off low-tier interest balances before high-tier ones
- Banks not declining over-the-limit transactions but allowing them and charging a huge penalty rate
- ...

See GAO report GAO-06-929, "Increased Complexity in Rates and Fees Heightens Need for More Effective Disclosures to Consumers"

If you're not Part of the Solution... (ctd)

Consumer redress in case of errors in credit reports is almost impossible

- US Public Interest Research Group (PIRG) found that 79% of consumer credit reports contained errors

So long as the mistakes about consumers make the consumers appear to be a worse credit risk than they really are rather than better, the credit industry has no incentive to improve the system

— Anthony Rodriguez, National Consumer Law Center

You've got to get a lawyer and hit them between the eyes with a two-by-four to get their attention

— Richard Feferman, FCRA (Federal Credit Reporting Act) lawyer

If you're not Part of the Solution... (ctd)

System is set up to ensure that nothing ever gets resolved and consumers give up

Equifax knew that the pointless [actions of pretending to investigate] was not going to resolve Plaintiff's dispute in a timely manner and only served to delay the matters until Plaintiff tired of the process or proceeded to litigation

— New Mexico district court judge M.Christina Armijo

I have never seen a credit bureau send supporting documents [in case of a dispute] to the creditor in fifteen years [...] They never send those documents because it's more profitable for them to not follow the law then it is to actually follow the law

— Mike Baxter, FCRA lawyer

If you're not Part of the Solution... (ctd)

Nothing must stand in the way of easy credit

- Getting six or seven of nine digits of the SSN and at least three letters of the first name (in any order) right are enough
- Surnames and date of birth aren't checked at all
 - Swapped first name and surname are OK too
- “Cynthia” = “Cindy” is OK, but then “Mark” = “Martha” and “David” = “Diana”
- Bad handwriting, nicknames, typos, or an inability to read instructions mustn't interfere with the process of obtaining credit
 - FRR must be 0% so FAR \approx 100%

If you're not Part of the Solution... (ctd)

If you want a copy of your credit report though, every detail has to be 100% accurate or the records “can't be found”

- Fraudulent entries with a letter or digit out of place “can't be located” and so are never reported to the consumer

Fraud is typically written off as a bad loan

- No-one looks bad
- No alarms are set off
- ID Analytics study found that 90% of ID theft cases were hidden as simple credit loss

No incentive to fix anything since “fraud is relatively low”

If you're not Part of the Solution... (ctd)

Entry barriers to credit fraud are very low, and there's no incentive among banks/credit agencies to fix anything

- Bank recovers the money via a chargeback to the merchant
- Bank can also hit the merchant with chargeback fees
- If done right, the bank can actually *make money* from the fraud
 - Talk about a perverse incentive!

The industry has fought tooth and nail against even the most cursory checks. Opting out of instant credit isn't an option for most people [...] the credit bureaus will not put a fraud alert on your account unless you've already been a victim of identity fraud. *Then* you can close the barn door and have a fraud alert put on your account

— “Phishing: Cutting the Identity Theft Line”

Malware 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

Malware 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

Malware 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

Use node-locked licensing to protect the malware creator’s IP (Zeus 2)

Malware Functions (ctd)

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

- Years ago it was possible to scan for viruses via the standardised code that they used to disable MSAV
- In 2008 there were 22 different malware families that specifically infected Microsoft's malware scanning tool

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)

Malware Functions (ctd)

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

Inject hostile code into anti-virus processes (Stuxnet)

- Enumerate running processes to find any running anti-virus applications
- Inject the malware into the application
- The malware is now running inside the anti-malware app

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

Malware Functions (ctd)

Fool anti-virus software into checking the wrong program code (Nebbett's Shuttle)

- Create a process in the suspended state
 - AV software checks the binary image and clears it
- Overwrite the image with a new image using VM functions
- Start the process executing
 - Classic ToC/ToU race

Functionality is available in SDK form to add to your current malware product (Prg)

Malware Functions (ctd)

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 (Srizbi, Rustock)
 - Load only the NDIS code fragments that it needs (“code pullout”), reducing the detectable footprint (Mebroot)
- Using your own binaries to avoid detection/logging is a common technique
 - MegaD spam botnet uses its own copy of BIND to avoid being found via traffic patterns in the system BIND logs

Many, many variations used by different rootkits, e.g.
FireWalk

Malware Functions (ctd)

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

- Even though Microsoft finally set somewhat safer defaults, the original unsafe ones are only a mouse click away

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)

Malware Functions (ctd)

Complex IDS-evasion techniques (Stuxnet)

- Hooks NTDLL.DLL
- Calls `LoadLibrary()` with a specially-formed nonexistent filename
 - IDS is satisfied, since the file doesn't exist and therefore isn't a threat
- Hooked NTDLL recognises the special file form passed to `ZwOpenFile()` and returns a mapped view of the binary image elsewhere in memory

Collect detailed PC information and state data to emulate the victim's footprint for avoid fraud-detection systems
(Tigger)

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`

Malware Functions (ctd)

Infect *outwards* from the kernel to userspace (Peacomm)

- Conventional thinking is that the kernel is the bit you can trust

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

Capture screenshots around the area of the screen where a mouse click has occurred

- Defeats graphical password-entry mechanisms

Scan for anti-malware software and report stats on which defence software is the most widespread and/or problematic (Pushdo)

Malware Functions (ctd)

Report statistics on the most effective exploits back to the controller (MPACK)

- Allows future exploit payloads to be adapted based on what's worked best in the past

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

Malware Functions (ctd)

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

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

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)
- ...

Malware Functions (ctd)

Target plugins rather than browsers

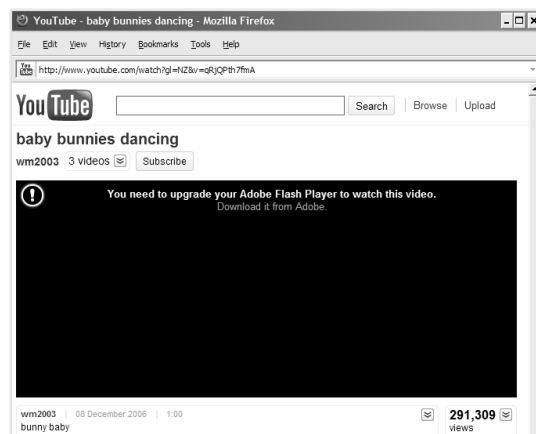
- Provides a high success rate against all browsers: IE, Firefox, Opera, Safari, Google Chrome, ...
- Most popular target: Adobe PDF
- Other popular targets: Java, Flash, ...

Some of the most successful exploits target vulnerabilities that were patched quite some time ago [...] The Java exploit was the second most successful attack (behind an exploit pack that attacks at least three different Adobe Reader flaws)

— Krebs on Security

Malware Functions (ctd)

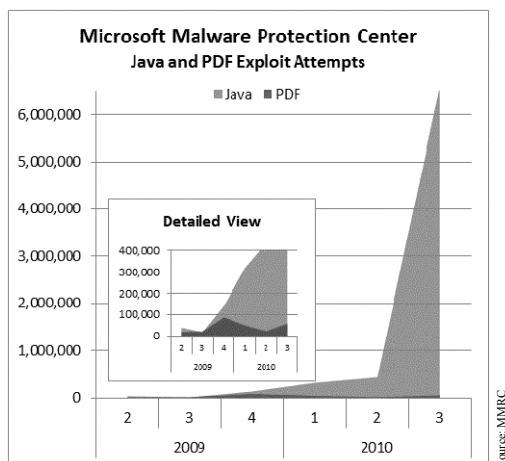
Use the plugin as the attack vector



- Users have been universally trained to do this by web sites
- Video “plugin” is a malware installer

Malware Functions (ctd)

Java, the malware VM environment of choice



Malware Functions (ctd)

Why Java?

- It's secure (by emphatic assertion!) so there's no need to worry about it
- Installed on 85% of all desktop machines
- Most users don't know that it's there
- Requires frequent updating to keep it secure
Java is ubiquitous, and [...] people don't think to update it. On top of that, Java is a technology that runs in the background to make more visible components work. How do you know if you have Java installed or if it's running?
— Holly Stewart, MMPC
- Oh, and anti-malware products have problems dealing with Java. Would you want to include a JVM in your scanner?

Malware Functions (ctd)

Hook into the Javascript engine to grab AJAX-based authentication data (Gozi), Firefox via XUL (Nuklus)

- 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!”

Steal client keys and certificates and other secrets from Windows Protected Storage and PFX/PKCS #12 files (Gozi, Nuklus/Apophis)

- Client cert-stealing malware could well outnumber client cert users

Malware Functions (ctd)

Perform distributed account-validity checking (Trojan.Loginck)

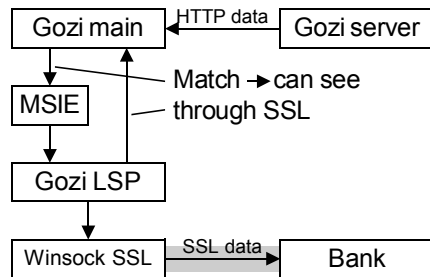
- If you have 40 million stolen accounts (as one botherder did), how do you check which ones are still valid?
- Use your botnet as a distributed validity-checking server

Generate pseudo-random domain names and connect to them in turn (Srizbi)

- Botherder preemptively registers the domains before the botnet connects to them
- Defeats domain blacklisting/takedowns

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

Malware Functions (ctd)

Steal user accounts via password-reset facilities

- Typical password-reset process
 - Go to site
 - Enter email address, click on “I’ve forgotten my password”
 - Wait for emailed link with cookie to enter new password
- Dump a spam list at obvious targets like Amazon, Gmail, eBay, ...
- Wait for return email containing the password reset code
- Amazon et al, for ^*&#’s sake add CAPTCHAs to your password-reset capabilities
 - Some already do this, e.g. PayPal, Gmail, eBay (sort of)
- Current mechanisms hand out accounts to anyone who can submit a POST and copy a link from the returned email

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”
- ...

Malware Functions (ctd)

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

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

Replace auto-update programs for popular software (e.g. Acrobat, Java) with malware updaters (Fakeupver)

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: 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?

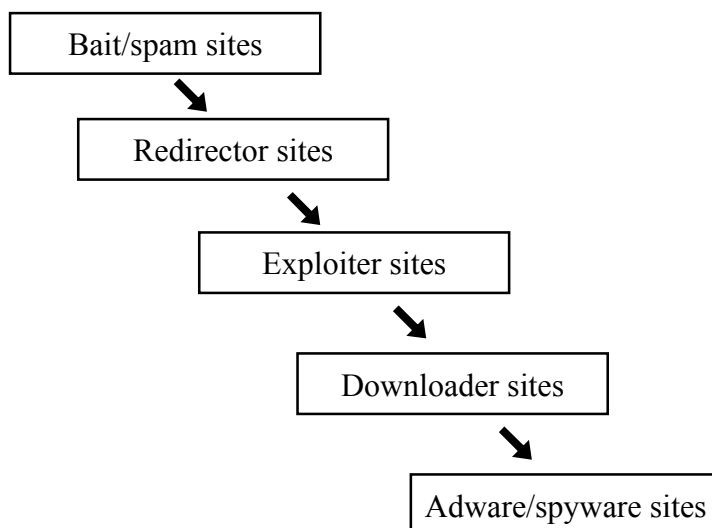
A: It doesn't have to be, all it has to do is clear the way for the *real* threat

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

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)

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, ...

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

That’s pretty cool that you kicked all the viruses [that were blocking the adware] off. Why don’t you kick the competitors off too?

— Matt Knox, DirectRevenue adware developer

Why should I be worried about being infected with Tigger, all the popups have disappeared and my computer runs much faster, it’s great!

— A/V researcher quoting a customer

Malware Functions (ctd)

This tactic is so common that malware authors occasionally go to war over it

- In mid-2007 the authors of Storm and MPACK briefly turned their malware on each other in retaliation for the other side removing the malware from their machines

This was in the early days

- More recently it's been handled via corporate takeovers
- See e.g. Zeus + SpyEye mentioned earlier

Malware Functions (ctd)

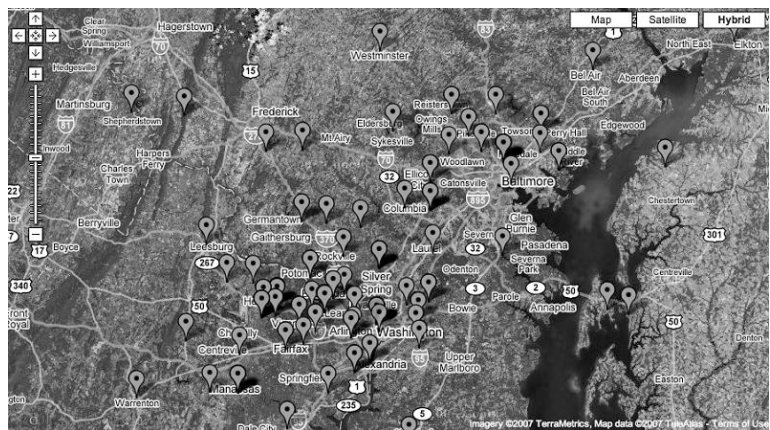
Adware vendors DirectRevenue have a 'Dark Arts' division dedicated to techniques like removing competing malware

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

Malware Functions (ctd)

Record user geolocation information



Malware Functions (ctd)

Used to defeat anomaly-detection software used by CC companies

- Can buy geolocated proxy from brokers do defeat location-based security
- Clampi trojan tunneled communications back through the victim's PC to defeat location-based authentication

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

Use stolen SMTP credentials to send authenticated spam (Waledac)

Malware Functions (ctd)

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

- Bypasses Windows Firewall and other security measures

Use Windows EFS to protect itself (Spy-Agent)

- Create an admin account with a random name and password
- Use EFS to encrypt its payload
- Create a service that uses the credentials of the random account to decrypt and run the payload

Intercept and lobotomise anti-malware applications as they start (Storm)

- Application is running, but it's brain-dead

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)

Modify the master boot record (MBR) to seize control of the machine before the OS loads (Mebroot)

- Patches the NTLDR OS kernel as it loads
- MSDOS called, it wants its boot sector viruses back!
- Pins disk clusters to prevent them from being relocated during a defrag
 - Newer versions use a monitoring thread to track relocations

Malware Functions (ctd)

Implement a custom encrypted filesystem to store the malware components (Mebroot)

- Stores binaries and stolen data at the end of the disk
- Uses a filter driver to make the infected portion of the disk appear normal
- Disinfects the copy of the driver in the system cache to prevent detection
 - An attempt to read the driver data will get the (clean) cached copy, not the (infected) in-memory one

Use UPnP messages to open holes in firewalls (Conficker)

Malware Functions (ctd)

Use Windows file-parsing peculiarities to bypass behavioral/signature-based checking (Stuxnet)

- Windows will parse a .EXE as a .INF, skipping the entire executable (hundreds of kB) until it eventually runs into the .INF commands at the end (!!!)
- IDSes don't really expect this sort of thing

Inject HTML code into login pages to acquire additional credentials (e.g. ATM PINs on bank login pages) (Infostealer.Banker)

- Rewrites the genuine HTML, no way to detect the modification

Malware Functions (ctd)

Use form grabbing to bypass alternative input methods (e.g. virtual keyboards) (Haxdoor, Goldun, Metafisher, Snatch, BankAsh, Torpig, PWS.Banker, ...)

- Hook functions like `HttpSendRequestW()` to intercept POST requests
- Bypasses SSL since the data hasn't go down to the SSL layer yet
- Can be done by any user (no admin privs required)

Malware Functions (ctd)

Use victims to defeat CAPTCHAs (Captcha Trojan)

- Victims (collaborators?) are shown progressive X-rated images in exchange for solving CAPTCHAs
- Much more reliable to just outsource it though, see earlier slides

Install rootkits that run even in Windows Safe Mode (Tigger)

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

Malware Functions (ctd)

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
- Other malware is distributed via pre-built Linux OS images
 - BIND, PHP, OpenVPN, nginx proxy, ...
 - Standardised image is customised via scripts at install

In the next generation, we will all do business with infected end points. Our strategy is we have to figure out how you do business with an infected computer. How do you secure a transaction with an infected machine? Whoever figures out how to do that first will win

— Chris Rouland, IBM Internet Security Systems

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)

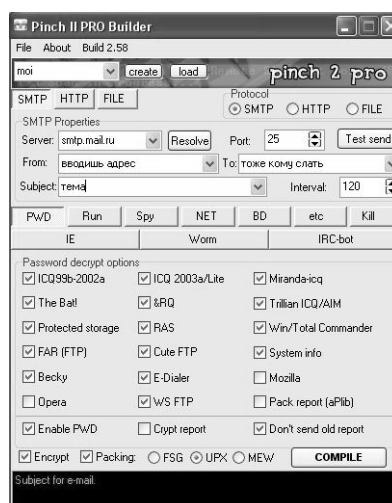
Spyware capabilities

- 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

Example: Pinch trojan construction kit

Point-and-click tool for creating trojans

- Configure data-stealing actions
- Configure defensive actions (e.g. disable firewalls, A/V software)
- Configure auto-run/rootkit capabilities
- Configure anti-detection mechanisms like encryption, compression, ...
- Configure means of exporting stolen data

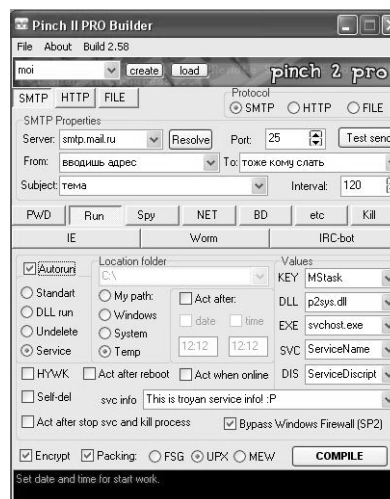


Example: Pinch trojan construction kit (ctd)

All aspects of the resulting trojan are highly configurable

- See sample at right for configuring SMTP export of data and autorun capabilities

Comes with a huge range of capabilities, e.g. for injecting links into the MSIE Trusted Sites zone, acting as various types of proxy to defeat location-based security, screens and screens of this stuff



Example: Pinch trojan construction kit (ctd)

Comes with its own visualisation tool, the Pinch Parser, for managing the volumes of data created

- Sophisticated tree-based browser
- Custom data filters, reporting, etc

Protected Storage
This module contains passwords from Windows protected storage: Outlook, IE, FTP
yo-cool-girl@list.ru
• Email: yo-cool-girl@list.ru
Sites
Passwords from sites (Basic Auth)
mp3.territory.ru/Protected Area
• Host: mp3.territory.ru/Protected Area
• login: ksunikum@rol.ru
• password: [REDACTED]
voffice.rol.ru/ROL restricted area
• Host: voffice.rol.ru/ROL restricted area
• login: ksunikum@rol.ru
• password: [REDACTED]
voffice.rol.ru/ROL Virtual Office
• Host: voffice.rol.ru/ROL Virtual Office
• login: ksunikum@rol.ru
• password: [REDACTED]
voffice.rol.ru:80/ROL Virtual Office
• Host: voffice.rol.ru:80/ROL Virtual Office
• login: chika15@rol.ru
• password: [REDACTED]

Example: Pinch trojan construction kit (ctd)

The Pinch creators (Ermishkin and Farhutdinov) were arrested by the Russian FSB (Federal Security Bureau, former KGB) in 2007

Now everyone's getting in on the act

- Want a Turkish malware construction kit? No problem...
- “Support your local malware in industry!”



Example: Pinch trojan construction kit (ctd)

Off the shelf technology gives anyone the ability to create a piece of malware and launch a banking trojan attack. For a few hundred dollars you can purchase a tool kit and create your own customized malware to target a financial institution of your choice

— Gunter Ollmann, IBM Internet Security Systems

Malware Functions (ctd)

Use every available attack vector to propagate (Nugache)

- Targets Windows security holes
- Spreads via email and IM social-engineering attacks
- Propagates via links on blog posts
- Uses a trojaned shareware application
 - Used click-fraud to boost the popularity of its propagation mechanisms, e.g. the shareware application's rating

Inject themselves into network clients to avoid HIDs

- Look for processes with names *explore*, *firefox*, *chrome*, *opera*, *safari*, ...
- Network access from these won't be flagged as suspicious by a host-based IDS

Malware Functions (ctd)

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
 - In any case this is overkill, form-grabbing works just as well
- Render copies of genuine bank pages from the browser cache

Malware Functions (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)

(What do people do when they realise that they've been infected by a trojan?)

- Go to AV vendor sites using the infected machine and enter their credit card number, CVV, ... to buy AV tools
– Paul Craig, Security-Assessment.com)

Malware Functions (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

I'm here to sell a working version of win32.grams trojan, [...]
The trojan has been tested successfully with Windows XP (all SP's) and works ONLY on IE (Internet Explorer). The price for this wonder trojan is only 1000 dollars

Example: Grams egold siphoner

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 `IHTMLInputElement::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

Example: PRG Trojan

Checks victim data for evidence of interaction with banking sites

They spear phish with a very well-crafted email that purports to be from their bank and is offering a new soft token, client certificate or security code. When they actually try and download the new token, certificate or security code, the trojan is downloaded to their computer

— Don Jackson, Senior Security Researcher for SecureWorks

- Provides a real-time alert of the victim interacting with a bank to the phishers to allow live interception

Example: PRG Trojan (ctd)

Sends information on bank(s) used to attackers

- Allows bank-specific attacks to be performed
- Message from your bank with your bank's logo and your account information, addressed directly to you

Trojan acts as a VM for control code on central servers

- C&C servers send out bank-specific code to run in the trojan VM
- Allows operations to be continually adapted without requiring changes in the trojan itself

Anti-detection Mechanisms

Inject themselves into the system via

- Import Address Table (IAT) hooking
- System Service Dispatch Table (SSDT) hooking
- Filter drivers
- Direct kernel object manipulation (DKOM)
- IRP hooking
- Inline function hooking
- VMM hooking
- Interrupt Descriptor Table (IDT) hooking
- ...

"It's rootkits all the way down"

Won't run under a VMM (Many)

Anti-detection Mechanisms (ctd)

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)

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

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 Fighter 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 $\times 0,000$ files on a system

Viruses 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)

This form of code-hiding is commercialised in the form of crypters

- Come with custom plugins (“stubs”) to bootstrap the decryption process
- Need a stub to begin decryption of the rest of the malware

Stubs are eventually identified by AV software

- Crypters are sold with an initial set of stubs, with more available for a fee
- Many crypters also detect sandboxing, to avoid analysis by anti-virus researchers

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
- Something as simple as adding zero bytes will fool many A/V programs
No AV on VirusTotal detects this malware obscured with 255 zero-bytes. But for IE this poses no problem [...] it still renders the page and executes the script
— “A000n000 0000O000l000d 00T0r000i000c0000k”

Anti-detection Mechanisms (ctd)

“Race to Zero” contest at Defcon 2008 demonstrated how easy it was to get malware past antivirus software

- Oldest piece of malware was the Stoned virus from 20 years ago
- Others included a who's-who of well-known malware
 - Bagel
 - Netsky
 - Sasser
 - SQL Slammer
 - Welchia
 - Zlob
- (These should be the most easily detected ones due to their prominence)

Anti-detection Mechanisms (ctd)

Malware was run against software from all major antivirus vendors

Fastest team took 2 1/2 hours to get the entire collection past every antivirus program

- Done using a custom packer, a technique popular with malware authors

AV is not a magic security pill. We respond to major computer security incidents for a living and AV products are always in place and usually deployed in the vendor-specified manner, yet the bad guys still are able to use slightly modified versions of popular tools to pull off everything from bank heists to stealing sensitive government information

— Nick Harbour, member of winning team

Anti-detection Mechanisms (ctd)

virustotal.com maintains statistics for malware detected by all antivirus products vs. malware not detected by at least one product

- For every one piece of malware detected by all products, *a thousand* are not detected by at least one product (<http://www.virustotal.com/estadisticas.html>)

Anti-detection Mechanisms (ctd)

Undetectability is a major selling point when advertising trojans

Файл dhdezdgzjzdgshstds.exe получен 2008.03.23 01:15:57 (CET)

Антивирус	Версия	Обновление	Результат
AbnLab-V3	2008.3.22.1	2008.03.21	-
AntiVir	7.6.0.75	2008.03.22	-
Authentium	4.93.8	2008.03.22	-
Avast	4.7.1098.0	2008.03.22	-
AVG	7.5.0.516	2008.03.22	-
BitDefender	7.2	2008.03.23	-
CAT-QuickHeal	9.50	2008.03.21	(Suspicious) - DNAScan
ClamAV	0.92.1	2008.03.23	-
DrWeb	4.44.0.09170	2008.03.22	-
eSafe	7.0.15.0	2008.03.18	-
eTrust-Vet	31.3.5633	2008.03.21	-
Ewido	4.0	2008.03.22	-
F-Prot	4.4.2.54	2008.03.22	-
F-Secure	6.70.13260.0	2008.03.21	-
FileAdvisor	1	2008.03.23	-
Fortinet	3.14.0.0	2008.03.22	-
Ikarus	73.1.1.20	2008.03.22	-
Kaspersky	7.0.0.125	2008.03.23	-
McAfee	5257	2008.03.21	-
Microsoft	1.3301	2008.03.23	ТроянDropper:Win32/Buzus.gen!A
NOD32v2	2967	2008.03.21	-
Norman	5.80.02	2008.03.20	-
Panda	9.0.0.4	2008.03.22	-
Prevx1	v2	2008.03.23	-
Rising	20.36.42.00	2008.03.21	-
Sophos	4.27.0	2008.03.22	-
Sunbelt	3.0.978.0	2008.03.18	-
Symantec	10	2008.03.23	-
TheHacker	6.2.92.252	2008.03.22	-
VBA32	3.12.6.3	2008.03.21	-
VirusBuster	4.3.26.9	2008.03.22	-
Webwasher-Gateway	6.6.2	2008.03.22	-

Дополнительная информация
File size: 23040 bytes

Anti-detection Mechanisms (ctd)

Some sites even do custom scans that go beyond what VirusTotal does

DO NOT use public AV scanners like VirusTotal. We scan our .exe every hour special for you

- Intent is to make the malware fully undetected (FUD)

Online malware/phishing rating sites will check your product or site for FUD-ability

- Report detectability by AV software and web-site blacklists

First action by the malware is to disable the anti-virus program

- Miss rate then goes from 80% to 100%

Anti-detection Mechanisms (ctd)

The more successful pieces of malware are continuously update with new, undetectable versions

- Trojans like Torpig continued their multi-year effectiveness via 60-80 new undetectable versions a month
- Zeus 2 MaaS offers free upgrades once the existing version becomes too detectable

The risk of getting infected by malware that antivirus protection doesn't detect is alarmingly high [... if users] visit the wrong Web site they probably won't be protected from infection

— “Fools Download Where Angels Fear to Tread”

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

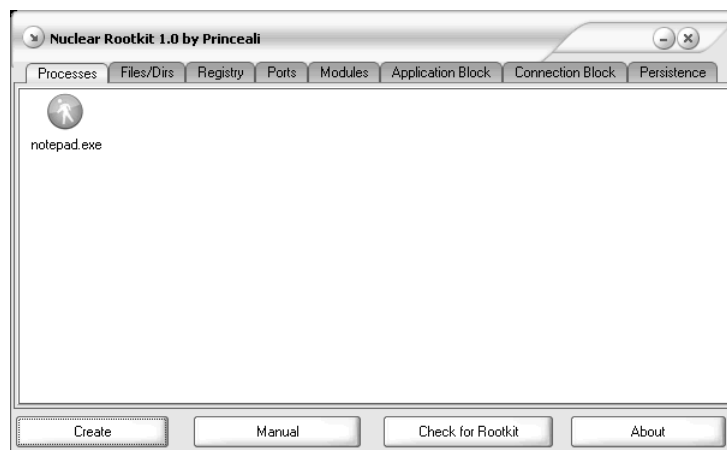
Just as AV companies reverse-engineer malware and develop countermeasures, so malware authors reverse-engineer the countermeasures and develop malware updates

Anti-detection Mechanisms (ctd)

Remove debug privileges from administrator accounts
(Spy-Agent)

- Prevents many rootkit detectors from running

Anti-detection Mechanisms (ctd)



The professionalism of these rootkits is coming to another level

— Allen Schimel, StillSecure

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

Availability of Private Data

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

There's so many stolen identities in criminal's hands that [identity theft] could easily rise twenty times. The criminals are still trying to figure out what to do with all that data

— Thomas Harkins, former Operations Director,
MasterCard Fraud Division

In 600 million years the sun will go out

- The fraudsters will have to finish cashing out their accounts in the dark

Availability of Private Data (ctd)

July '06: US Office of Management and Budget (OMB)
requires notification of data breaches exposing personal
(identity-theft) data

June '07: Incidents running at 14 per day

October '07: Incidents running at 30 per day

- Reporting rate is slowly catching up with the actual incident rate

Estimates are that > 50% of all Americans have been
exposed at some time

What Should I Do? (Non-geeks)

Put your head between your legs and kiss your ...

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
 - (No longer possible under Vista, Win7)
- Total Windows XP kernel memory usage should be ~100MB
 - Under Vista/Win7... ough
- Need to hack the registry and other obscure things
 - Gets harder and harder with newer versions of Windows

What Should I Do? (Geeks) (ctd)

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 to maximum blocking

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'

- Sort-of the default under Vista/Win7 with UAC

What Should Banks Do?

Implement proper usage controls at the bank

- Secure > 1 billion PCs or secure a few centralised banks, which do you think is more likely?

In their rush to cut costs, banks moved absolutely everything online

- Processes that were traditionally internal to the bank are now exposed via the public Internet
- A home PC really isn't a good substitute for an ATM, but is given more capabilities than one

Taking critical operations back offline is the single biggest change that banks can make to secure online finances

What Should Banks Do? (ctd)

Allow customers to set usage controls

- Customers know better than any banking fraud-guessing system what's right and wrong

Break up one-size-fits-all credit limit into overall credit limit + domestic spending limit + overseas spending floor limit

- Total limit = \$25K, domestic limit = \$5K, overseas limit = \$1K

Allow setting limits based on spending type

- Merchant category code (MCC) is already present for every transaction

What Should Banks Do? (ctd)

Allow card-present but not card-not-present for overseas spending

- If customer is on holiday in the UK, allow transactions in the UK but not the US

Decline transactions below a customer-set lower limit

- To a criminal doing a liveness check the card will appear invalid → move on to the next one
 - (Many merchants will refuse tiny transactions anyway because the card fees will destroy any profit they may make)

All of the reporting is already present in the payment clearing system, it's just never used (until it's too late)

What Should Banks Do? (ctd)

Unfortunately banks are too busy playing with fraud-guessing systems to consider this

- Newer malware includes built-in rule-based systems with user-configurable parameters to defeat these fraud-guessing systems

Crooks distribute stolen card data use in time and space to evade detection

- Like spread-spectrum botnet spamming, this automatically evades fraud-guessing systems without any special effort

Takes banks months before they even notice that there's something wrong

What Should Banks Do? (ctd)

Plenty of anecdotal evidence of guessing systems failing

What was amazing to me was that I would call the victims and they were retired people in California who'd never shopped in Wal-Mart and never been to Florida. So to me this screamed out how in the world did this happen? I mean people had \$20,000 charged to their credit card in one day from one location

— Jon Swartz, USA Today

- We'd be happy to authorise your 3am request to move your entire bank balance to Lagos
- Sure, simultaneously using the same credit card in Australia and Poland is no problem

What Should Banks Do? (ctd)

Death first!

- Any impediment to easy credit will never be accepted by the banks

No sign of the status quo ever changing

What Should Banks Do? (ctd)

Require physical presence with photo ID for COB, credit limit increase, additional cardholder, ...

- These are so rare (once every few years at most) that a brief bank visit is no impediment

What Should Banks Do? (ctd)

Properly implement SMS-based authorisation

- Business → Bank: Request transfer of \$1000 from savings account to Bob's Cameras
- Bank → User: Enter this code to authorise all further transactions until the account is empty

What *were* they thinking?!?

What Should Banks Do? (ctd)

Keep proper track of the problem to provide insight

- Number of US phishing victims in 2006: 2,300,000
- Number of US phishing victims in 2007: 3,600,000
- Number of attacks in the period January 2005 – May 2007 reported by US banks to the FDIC: 451

The data quality was so poor that it was impossible to draw any conclusions from it other than that the regulatory reporting on fraud attacks is severely lacking

— Avivah Litan, Gartner Group

What Should Banks Do? (ctd)

Adopt proactive defence measures

- Many card security measures are designed to defend against the previous year's/decade's attack
- Cards still have features present for legacy attacks from decades ago

Poison the source

- Attackers are in this purely for the money
- Hit them in the wallet

Create a lemon market for stolen credentials

- Seller (banks) know which credentials are lemons
- Buyers (crooks) can't tell

What Should Banks Do? (ctd)

Vendors offer guarantees on their wares

- Replacement/money back if a card declines within 48/72 hours

Make sure that 95% of their cards decline

- Forces them to spend time/money to fix things
- Loss of reputation with customers

Inject bogus data into phishing sites

- Valid-seeming CC details
- Appear to allow the small transactions used by crooks to check card validity
- Decline any real transactions

Crooks end up selling lemons to their customers

What Should Banks Do? (ctd)

Allows tracing of data flows

- Suppliers (banks) can associate alarms with their fake data
- We injected it in Canada, two weeks later it was used in Poland...
- Radioactive tracers for stolen credentials

Other Options

The Globus Grid toolkit is 450MB of source code (!!)

- The Globus Security Infrastructure component is 100MB of code (!!!!)

Hire Russian botnet authors (world authorities on grid computing) to rewrite Globus in, oh, 1MB or so

- Takes care of two problems at once

Conclusion

We now finally have (very good!) security metrics

- These aren't just educated guesses based on vulnerabilities per KLOC or similar metrics
- To see what's being attacked and what's most in demand, look at prices for malware, services, and product

We're not winning

- We're not even breaking even
- They already have countermeasures ready for security measures that we haven't even deployed yet
- Would require an Enron-scale debacle to get the banks/credit agencies to change

Conclusion (ctd)

It's all about the money

- No-one's exploiting e.g. the goldmine of 0days that is Safari because there's no money in it

Monoculture reloaded: Use unpopular software

Reading recommendation: Brian Krebs' "Security Fix" column in the Washington Post, later "Krebs on Security", <http://krebsonsecurity.com>

- Probably the best generally accessible source on the state of play in Internet crime

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