Malware – future trends

Dancho Danchev
dancho.danchev AT hush.com
ddanchev.blogspot.com

1. **Intro**
2. **Scope**
3. **Author's comments**
4. **The current state of the malware threat**
    - Where the metrics are!
        - Use and abuse of malware
            - DDoS extortion
            - DDoS on demand/hire
            - Botnets and zombie hosts
            - Pay-Per-Click-Hijacking
            - Cryptoviral extortion, Ransomware
            - Platform for dissemination of other junk
            - Mass identity theft and financial abuse
            - Around the industry
5. **Factors contributing to the rise and success of malware**
    - Documentation and howto's transformed into source code
    - Vulnerabilities, even patches, easily turned into exploits
    - Clear signs of consolidation on the malware scene
    - The media as a fueling factor for growth
    - Over 960M unique Internet users and their connectivity, or purchasing power
    - The demand for illegal services
6. **Future trends**
    - Mobile malware will be successfully monetized
    - Localization as a concept will attract the coders' attention
    - Open Source Malware
    - Anonymous and illegal hosting of (copyrighted) data
    - The development of Ecosystem
    - Rise in encryption and packers
    - 0day malware on demand
    - Cryptoviral extortion / Ransomware will emerge
    - When the security solutions ends up the security problem itself
    - Intellectual property worms
    - Web vulnerabilities, and web worms – diversity and explicit velocity
    - Hijacking botnets and infected PCs
    - Interoperability will increase the diversity and reach of the malware scene
7. **Conclusion**

01. Intro

Malware has truly evolved during the last couple of years. Its potential for financial and network based abuse was quickly realized, and thus, tactics changed, consolidation between different parties occurred, and the malware scene became overly monetized, with its services available on demand.

What are the driving forces behind the rise of malware? Who's behind it, and what tactics do they use? How are vendors responding, and what should organizations, researchers, and end users keep in mind for the upcoming future? These and many other questions will be discussed in this article, combining security experience, business logic, a little bit of psychology, market trends, and personal chats with knowledgeable folks from the industry.

02. Scope

This publication is in no way intended to be a complete future prediction or a reference, as future can never by fully predicted, that's the beauty of it. Instead, its intention is to discuss the possible future trends backed up by a little speculation, and also use some of the current ones as a foundation for future developments. Malware authors, and antivirus vendors would never stop playing a cat and mouse game, that's the nature of the market, but as in any other, there are core factors affecting all the participants, and variables whose movements shape the future direction of events. In this publication, I did my best to cover the most significant ones, expressing entirely my point of view as an independent security consultant.

03. Author's comments

Back in 2003 when I first wrote The Complete Windows Trojans Paper[1], things were entirely different from what they are today. Trojans used to have fixed ports[2], servers were open to anyone scanning and using the right client for the right trojan. Then, malware started getting smarter, and port 80 or anything else allowed by default started acting as a communication platform. Infected PCs started getting controlled over Web browsers, and SensePost's Setiri[3] concept deserves to be mentioned among the many other important ones back in those days.

Slightly highlighting the future potential of what used to be Remote Access Trojans (RATs) back in 2003, today this threat is represented by IP (intellectual property) worms, cryptoviral extortion schemes, or industrial espionage 0day cases like the Israeli's operation "Horse Race"[4]. Furthermore, many others trends and factors should also be considered. I greatly hope that this trend analysis will result in more constructive discussions, or perhaps, even expectations from any of your security vendors!

For others thoughts on security, you can also go through my blog posts at :

http://ddanchev.blogspot.com/

[1] http://www.windowsecurity.com/whitepapers/The_Complete_Windows_Trojans_Paper.html
[2] http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html
[3] http://www.informit.com/articles/article.asp?p=102181&seqNum=5&rl=1
[4] http://arik.baratz.org/wordpress/2005-05-29/trojan-horses-abound/

What will you learn after reading this paper?

- you will be able to easily graps the big picture and know where you, or your organization stands
- you will maker better purchasing decisions, and become a more informed opinion leader
- how the current threats affecting the scene will influence the trends to come?
- why malware will continue to be an inseparable part of the Internet?
- how malware turned into a cost-effective industrial espionage tool?
- and many more insights or topics to speculate on!

04. The current state of the malware threat

Let's start from the basics. A worm[5] is a malicious code (standalone or file-infecting), that propagates over a network, with or without human assistance. Malware[6] though, should be considered as "the gang" of malicious software, in respect to their unique features. Which is what I am going to talk about. That said, you should also consider today's malware as:

- modular - new features are easily added to further improve its impact, want it to have P2P propagation capability, add it, want it to disseminate over IM, done. The disturbing part is that what used to be tutorials and documents on the topic, is today's freely available source code, or specific modules[7] of it

- even more powerful and destructive - full control over infected host and network connection, blocks known firewalls, antivirus signatures updates and software, eliminates rival malware, encrypts host data and asks for ransom, has rootkit capabilities, generates revenue for its authors, and that's just the tip of the iceberg!

- monetized - acts as a source of revenue and not fun, or just intellectual exploration anymore. Huge profits are to be made out of malware, and individuals easily turn to the dark side. A great post I came across on the Incident Handler's Diary[8], mentioned that the world champions in web site defacements, Brazilian gangs, sell web servers access to phishers, but quite often, many get shot!

- on demand - in need of a specially crafted 0day malware, rent zombies for DDoS attacks or spamming? Look no further, services likes these are available, and ShadowCrew[9] were the first to realize an underground electronic market concept. There's a clear demand, and when there's demand, there's supply as well

- homogenous as always - Microsoft's OS(and IE of course) dominate the market, exploit them, and exploit pretty much everyone. Linux boxes or MAC's, are currently getting no attention at all, and they will later on, MS's "New Era" ad campaign "Your Potential(Host, Network), Our Passion(Malware)", can indeed be taken as a leading incentive for future generations of malware authors vision. My point is that, the so called monoculture is one of the leading factors for mass innovation during the 21st century, but even though, monopolistic sentiments in the security industry can cause damage with targeted attacks. For instance, Welchia's attacks on security

[5] http://en.wikipedia.org/wiki/Computer_worm
[6] http://en.wikipedia.org/wiki/Malware
[7] http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=257
[8] http://isc.sans.org/diary.php?storyid=724
[9] http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm

solutions should be mentioned, and December's 2005 discovered vulnerabilities[10] in Symantec's and McAfee's products as well. Vendors tend to have vulnerabilities as well. However, I feel any vendor should really, really, try to reach the proactive level of high-severity vulnerability research, than merely responding (whether later or not is yet topic though) on security vulnerabilities. In many cases, independent security researchers provide patches or policies on how to block certain security threats posed by the lack of vendor released patch in a timely manner. Irony, but it keeps the balance around the Net in a certain way.

- easily resetting its lifecycle by reintroduction of new exploits, or switching infection propagators – once enough "seed victims" are gathered, these easily act as a stepping stone for further infections. Furthermore, once a patch for a known vulnerability starts getting applied across networks, the malware authors simply "reset" their code's lifecycle, by reintroducing it under new infection propagators, and exploits database. So for the time being, I feel malware authors have the privilege in this tactical warfare

- **competitive -** rather ironical, but malware can, and is disinfecting against other malware. And given the competition for a larger share of the Internet's infected population as I refer to zombies, malware authors are waging cyberwars among themselves. The infamous virii wars[11] indicate that malware authors are facing challenges too, and while collaborating, they are also competing. So true for any market, isn't it?

- **sneaky -** namely, can propagate through content spoofing[12] or web vulnerabilities, auto-executing through client-side attacks(browser, any other software), and requires less end user's interaction resulting in a faster worm, and higher probability of infection

- **the main platform for disseminating spam, phishing or any kind of e-junk -** "Give me an email and I can move the Earth!" approaches easily turn into reality, and there's been a clear indication of how spammers, phishers and malware authors work together. That's just the beginning of these affiliations.

Further expanding the topic, the malware scene is overly mature, while on the other hand its "releases" usually tend to have extremely short lifecycles, and quickly become part of a family of variations. The ones with the longest lifecycles tend to dominate a higher proportion of the Internet's infected population, and these very same pieces of malware are actually the ones written for gains, be it intellectual or financial ones. They also tend to reach levels of sophistication outpacing the rest, make an impact (always the news!) as well as test the vendors' understanding and fast response to today's, even tomorrow's threats. Mind you, each and every malware is released with a specific purpose, namely it's life-cycle is anticipated by the authors themselves, but hijacking botnets, or vulnerable infected hosts could extend perhaps, not only its life-cycle, but its ownership as well, and that's already happening. What's also to note is how fast malware changes tactics whenever an opportunity appears, so basically, even over a short period of time, all propagation vectors get used.

It is impressive how huge the Internet has grown, its diversity in terms of countries participating, their regulations, understanding, and actually responding to Internet related threats. The overall Internet monetization acted as the most clearly highlighted factor for the early malware-for-profit experiments we have witnessed during the last two years. Be it, email address harvesting, "direct marketing", no wait, spam sending, phishing attacks, on demand services in respect to DDoS,

[10] http://www.redherring.com/Article.aspx?a=14981&hed=Symantec%2C+McAfee+Battle+Flaws&sector=Industries&subsector=Computing
[11] http://www.pcmag.com/article2/0,1895,1612207,00.asp
[12] http://www.webappsec.org/projects/threat/classes/content_spoofing.shtml

segmented attacks targeting particular country's businesses, or single company – it is happening right now, without the FUD! As a matter of fact, in this publication fear stands for "worst case scenario", uncertainty for "risk", and doubt with "uncontrollable external factors". It's also as "third-party research", as possible :)) There's been a lot of buzz on using RSS as an infection propagator, and that Microsoft's integration of RSS into future IE versions, would further fuel the developments in this field. The speculation originally came from a white paper released by TrendMicro[13]. On the other hand, content spoofing or pharming are the first scenarios that come to my mind. If an attacker is able to inject anything into a popular RSS feed, due to a web application vulnerability on the service, then we really have a problem, and the live feed circulation meter should be considered as the infected hosts one in this case! What about an IE vulnerability that would further improve the "effectiveness" of the build-in RSS reader? I wouldn't consider it to be the "next big thing" though. Can syndication also be considered as the biggest hit-list ever, one of the foundations for a Warhol[14] worm in this case? Every major dotcom darling has suffered a web application vulnerability, and with the percentage of Internet traffic they attract, these are constantly attacked on all fronts.

Another initiative that should also be mentioned, is the Common Malware Enumeration[15] whose aim is to minimize the confusion of malware cross reference names during public outbreaks. The guys from Av-test.org, have also taken the time and effort to compile a list of cross-reference malware names[16], a clear indication of the need for such a project. But how useful is the idea actually? It has been recently criticized for not linking to anti virus vendor site's technical descriptions of the related malware, an issue that they have already resolved.

During 2005 we have also witnessed a great deal of cases with preprogrammed malware coming over mp3 players[17], or external hard drives[18], and I consider it as a clear indication of the penetration of the Internet within important networks, as well as the interoperability effect these days. Malware could therefore easily reach everywhere, and any device.

Malware can also have national security implications, but discussions on these, you wouldn't hear or read in news, that's up to your sources of course. For instance, in June 2005, Japanese nuclear data was leaked[19] on the Internet through a virus on a personal computer. It exposed interiors, details of regular inspections of repair works, and names of workers. Yet another event that happened in December, 2005 was that of Japanese Airlines leakage of airport passcodes through malware infected PC[20]. Disturbing enough to comment, even if it's not done on purposely!

Going back to **2004's blackout in the U.S**, a lot of folks highlighted that the event was right in between another Blaster cycle around the net. In fact, some researchers tried to summarize the potential of Blaster's unconscious contribution to the blackout, overloading networks worldwide.[21] TrendMicro also managed to compile a list of victims posed by the Sasser[22] event back in 2004.

Cases of damages included the following:

---

[13] http://www.trendmicro.com/en/offers/global/outbreak-aug18-wp.htm
[14] http://www.cs.berkeley.edu/~nweaver/warhol.html
[15] http://cme.mitre.org/
[16] http://www.av-test.org/down/wildlist.zip
[17] http://jp.creative.com/corporate/pressroom/releases/welcome.asp?pid=12173
[18] http://www.cio-today.com/story.xhtml?story_id=39742
[19] http://search.japantimes.co.jp/print/news/nn06-2005/nn20050624a5.htm
[20] http://www.infoworld.com/article/05/12/09/HNairportpasscodes_1.html
[21] http://www.ists.dartmouth.edu/library/120.pdf
[22] http://www.virtual.com/whitepapers/TrendMicro_The_Sasser_Event_wp.pdf

1. *public hospitals in Hong Kong*
2. *one-third of Taiwan's post office branches*
3. *British Airways – 20 flights were delayed for 10 minutes*
4. *Sydney train system*
5. *Scandinavian banks*
6. *British Coast Guard – 19 control centers were forced to use traditional pen and paper for their charting routines.*

And given that's just a small part of the big picture, malware can be considered as a truly evolving menace!

Where the metrics are!

No metrics' quality should be taken for granted, but I have come across a great deal of similarities between vendor's research reports and the actual situation. Even though the diversity of their sensor networks and geographical regions covered can be questioned, yet another trend should be considered. Be it, out of professional solidarity, or social concerns, today's ever-lowering costs for building and maintaining honeyfarms infrastructure have resulted in hundreds of thousands of honeynets run by researchers or consultants. Their, often unique and timely discoveries are directly forwarded to all the major vendors for testing. This ongoing collaboration between anti virus vendors, independent researchers, and organizations, has helped spotting some of the most prolific threats the industry has seen, such as the Code Red worm for instance, a moment that sparkled further partnerships between anti virus vendors and vulnerability or intrusion detection ones.

Symantec's Internet Security Threat Report VIII[23] Edition indicates that :

Note : Symantec's data is based on more than 24,000 sensors monitoring over 180 countries across the world. It also integrates data from their 120M client, gateway, and server solutions customers that use the company's products, and the 2M decoy accounts spread across the world.

- In the first six months of 2005, on average there were identified **10, 352 bots per day**
- During Jan-Jun 2005, **the daily volume of phishing attacks was 5.70B messages**
- Between **Jan-Jun 2005 DdoS attacks grew by more than 680%, to 927 per day on average**, compared to 119 per day during the first half of 2004
- Educational institutions and small businesses(end users included) was the most targeted by industry

Kaspersky's overview of 2004 and 2005 indicates the following[24] :

[23] http://enterprisesecurity.symantec.com/content.cfm?articleid=1539
[24] http://www.viruslist.com/en/analysis?pubid=167798878

Behaviour	Growth rate 2004 against 2003	Growth rate 2005 against 2004
Email-Worm	-20%	8%
IM-Worm	^ (average = 1 per month)	^ (average = 28 per month)
IRC-Worm	-28%	-1%
Net-Worm	21%	29%
P2P-Worm	-50%	-36%
Worm	-1%	24%
Virus	-54%	-28%
VirWare	-37%	7%

Source : Kaspersky Labs : VirWare growth rates 2004 - 2005.

The lack of P2P worms is, I think, a logical consequence of the RIAA's busts around the U.S, and the global response towards P2P networks copyright infringement. The rest is pretty evident though.

Use and abuse of malware

DDOS extortion

Types of Electronic Crimes *(base: 342)*	
Virus or other malicious code	77%
Denial of service attack	44%
Illegal generation of SPAM email	38%
Unauthorized access by an *insider*	36%
Phishing	31%
Unauthorized access by an *outsider*	27%
Fraud	22%
Theft of intellectual property	20%
Theft of other proprietary info	16%
Employee identity theft	12%
Sabotage by an *insider*	11%
Sabotage by an *outsider*	11%
Extortion by an *insider*	3%
Extortion by an *outsider*	3%
Other	11%
Don't know	8%

Source : E-Crime Watch Survey 2004
cert.org/archive/pdf/2004eCrimeWatchSummary.pdf
cert.org/archive/pdf/ecrimesummary05.pdf

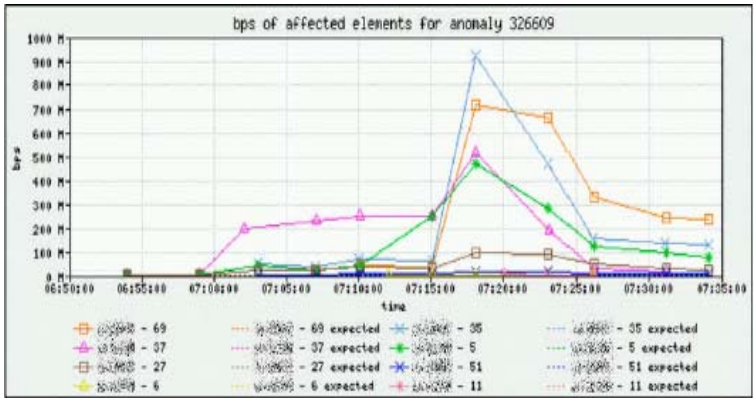
2004's E-Crime Watch Survey results match other research findings. Malware and DoS attacks occupy the top 3 positions(2005's version shows an increase in all crimes, but it is my opinion that extortion attempts do not even get reported!). Any web site could suffer a DdoS extortion attempt causing it direct revenue losses that's hard dollars, and the lost stakeholders' confidence in the business. Besides directly attacking business continuity and revenue streams, a lot of soft dollars, that is lost customers, partners, and overall stakeholders' loss of confidence in the business is what would follow, and is hard to quantify thoroughly. DdoS extortion happens when the botmaster, or his slaves, contact your requesting $ for not taking down your site. The web server, network, or other dedicated server may or may not be yet attacked prior to contacting the owners, and that should be considered the polite approach.

The other directly performs successful DDOS attack to demonstrate capability, and than demands, a clear psychological attack, that should provoke impulse paying. There's a clear indication of the obvious botmasters' dominance and motivation, and organizations paying are fueling the growth of this practice. For instance, Authorize.net[25] got under DDoS out of an extortion attempt, and perhaps the most decent reading I ever came cross on the topic is a CSO's article that's a very realistic one[26].

[25] http://www.theregister.co.uk/2004/09/23/authorize_ddos_attack/
[26] http://www.csoonline.com/read/050105/extortion.html

In the beginning of November 2004 until the end of January 2005, the folks from the Honeynet Project were able to observe 226 DdoS attacks[27] against 99 targets. Rather good sample for you to consider!

How severe can a DDoS attack get?



I came across a "great" 3GB/s (!?) graph(that's in 2004). Now you should ask yourself, would total cost of ownership of the business, the costs of the bandwidth, the DDoS attack protection solution, or the botmaster's deal with the devil style proposition can solve the situation. If you're thinking big, each and every time an organization pays, it not only risks a repeated demand, but is also fueling the growth of the practice in itself – so don't do it!

Source:
http://www.securite.org/presentations/ddos/COLT-SwiNOG9-ExpDDoS-NF-v1.pdf

A typical DDoS extortion letter's[28] tone usually sounds like this :

From: friends@compromised-email.com
To: <customer-service@hostremoved.com>
Subject: first letter

Your site is under an attack and will be for this entire weekend. You can increase your pipe all you want and it won't help. You have a flaw in your network that allows this to take place. You have 2 choices. You can ignore this email and try keep your site up, which will cost you tens of thousands of dollars in lost [business] and customers, or you can send us $40k to make sure that your site experiences no problems.

If you send the $40k your site will be protected not just this weekend, but for the next 12 months. This will let you enjoy business with no worry. If you choose not to pay for our help, then you will probably not be in business much longer, as you will be under attack each weekend for the next 20 weeks, or until you close your doors.

You can always choose to wait, see what happens, and then contact us for our help when you realize you can't do it yourself, however, then it will cost you more and your site will still be down. The choice is yours as we await your response

P.S. The sites that were attacked and paid last weekend are happy that they paid and are protected

What should also be taken into consideration when dealing with DdoS attacks, is how your position as the targeted victim will affect your ISP's other customers' performances, and how may the ISP actually react. Would your in-house, and off the shelf tools manage to protect you,

[27] http://www.honeynet.org/papers/bots/
[28] http://newsite.prolexic.com/downloads/whitepapers/Prolexic_WhitePaper-DDoS-Q4-2004.pdf

and should you, and most importantly how, deal with the extortionist without affecting business continuity?

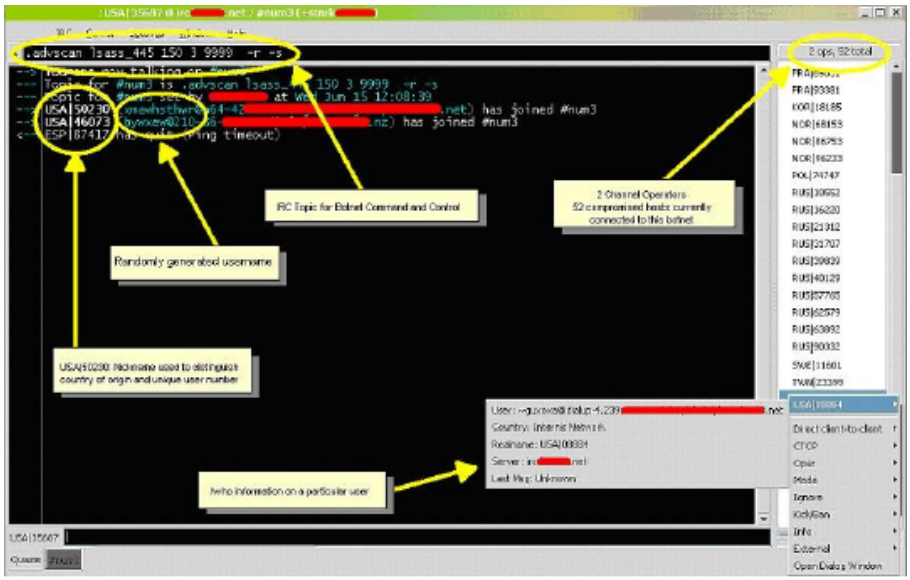
DDoS on demand/hire

There's a lot of demand for paying to teens to shut down your competitors and hoping they would go under the radar, and while ethics are excluded, given these get busted, they'll be the first to forward the responsibility to the buyer of the service. There's also a clear indication of market for such services, and sooner or later these individuals will improve their communication skills, thereby increasing the impact of these attacks. For instance, Jay Echouafni, CEO of TV retailer Orbit Communications, paid a group of botmasters to DDoS his competitors, where the outage costs were estimated at $2 million[29]. Another case of DDoS on demand occurred in March, 2005, when the FBI arrested a 17 year old and a Michigan man for orchestrating a DdoS attack, again causing direct monetary loses[30]. DDoS attacks, and the ease of gaining capability in this field are clearly increasing.

I wonder how many businesses would actually resist to such in a offer, and what if attackers start getting even more smarter and exploit the momentum of a certain situation, to further increase the value of their proposition?

Botnets and Zombie hosts

Botnets as a concept of utilizing all infected nodes at the same time, is causing the industry major damages. Hundreds of thousands of fully controlled Internet connected hosts, with amazing bandwidth, storage and sensitive information stored within could be easily utilized to perform the majority of security attacks we are witnessing these days.



A modest Botnet dominated IRC channel, courtesy of CERT
http://www.cert.org/archive/pdf/Botnets.pdf

[29] http://www.securityfocus.com/news/9411
[30] http://nj.gov/lps/newsreleases05/pr20050318c.html

I wouldn't go into details of what a botnet is, how it communicates, as I'm certain the majority of readers are pretty aware of the way it functions. In the long-term, encrypted or covert command and communication systems will appear, and the currently stripped IRCDs would seem like dinosaur practices for sure. Today's open source nature of malware, benefits malware authors to easily enter the scene though modifying publicly downloadable botnet sources and cause huge headaches and financial losses to everyone. A typical initiation of a DDOS attack against a victim can be seen in Honeynet Project's research on Botnets :

```
------------------------------------------------------------------------
[###FOO###] <~nickname> .scanstop
[###FOO###] <~nickname> .ddos.syn 151.49.8.XXX 21 200
[###FOO###] <-[XP]-18330> [DDoS]: Flooding: (151.49.8.XXX:21) for 200 seconds [...]
[###FOO###] <-[2K]-33820> [DDoS]: Done with flood (2573KB/sec).
[###FOO###] <-[XP]-86840> [DDoS]: Done with flood (351KB/sec).
[###FOO###] <-[XP]-62444> [DDoS]: Done with flood (1327KB/sec).
[###FOO###] <-[2K]-38291> [DDoS]: Done with flood (714KB/sec).
------------------------------------------------------------------------
```

Source : http://www.honeynet.org/papers/bots/

Of course, many other galleries[31] of botnets are available online.

Another growing trend is that of malware authors renting full access to botnets, so the temporary owner could do wherever his/her capabilities and intentions reach. The possibility to connect and control hundreds of thousands of infected hosts altogether and maintain the connection, is what malicious attackers are originally aiming for, besides the $$$, of course. Perhaps the biggest botnet publicly reported so far consists of (approximately) 1.5M compromised computers[32], so botnets can indeed be considered as a major threat to every Internet business or participant.

Pay-Per-Click-Hijacking[33]

Pay-Per-Click search advertising on a mass scale is the true financially sound solution to online ads, but Pay-Per-Click-Hijacking is a very commonly practice nowadays, and botnets take their shot. In fact, Google was recently sued for pay-per-click abuse practices[34] so you can consider that it's actually happening, and I'm sure given that their revenues comes primarily from AdWords, they are definitely taking it serious. However, many other pey-per-click ad providers can, and are easily targeted as well.

Pay-Per-Click-Hijacking is a fully realistic practice these days. For instance, an SDBot variant[35] detected by Eric at the MalwareBlog.com, is a suitable example of how malware is able to automatically generate revenue, vote, or count as a visit :

http:///ads1.revenue.net/r?site_id=13414&pplacement_id=1
http:///ads1.revenue.net/l?O_RANK=4&O_CREATIVE_ID=207892&O_SITE_ID=13414&
http:///ads1.revenue.net/l?O_RANK=2&O_CREATIVE_ID=208343&O_SITE_ID=13414&
http:///ads1.searchmiracle.com/ads/ad.php?country=1&pos=4
soundcheck.ninemsn.com.au
http:///soundcheck.ninemsn.com.au/vote.jsp?fvEntry=450&fvRank=5
http:///e.rn11.com/a/a369-ovc720spi

[31] http://swatit.org/bots/gallery.html
[32] http://informationweek.com/story/showArticle.jhtml?articleID=172303265
[33] http://www.lurhq.com/ppc-hijack.html
[34] http://www.fayettevillenc.com/article?id=221972
[35] http://www.malwareblog.com/?p=164

e.rn11.com
http:///www.mt-download.com/mbimg.gif

A recent publication, courtesy of CERT also gives a simple visualization of the feature :

<botherder> <bot12345>	.visit http://www.cert.org/ http://www.referingsite-URL.com/ site visited.

Source : *CERT, Coordination http://www.cert.org/archive/pdf/Botnets.pdf*

Clickable indeed equals fraudable in this case, and the very fact of "owning" someone's unique IP gives you the opportunity to influence any place where it's required as a guarantee of uniqueness. Is it just me, or I am spotting a great business opportunity in here for instance Sophos's ZombieAlert[36] service in direct combination with anti-click fraud solutions. But should a malware infected user by denied the right to generate revenue whatsoever? I am also a little surprised out of the lack of piggybacking on this feature, given the vast amounts of data on zombie PCs anti virus solutions have, of course, among pretty much every security vendor. Pay-Per-Click-Hijacking scams will continue getting even more sophisticated.

Cryptoviral extortion / Ransomware

The concept isn't new as it was first seen with the appearance of The Disk Killer virus[37] in June, 1989. But its weakness of using a weak encryption algorithm made it easy to restore the data. In fact, that's the current problem with this type of malware today, weak algorithms, and actual implementation. Though, my favorite is One_Half[38], which as a matter of fact I got infected with back in 1994. It encrypts folders prior to accessing them, until it encrypts half of the disk space. A recent variant was spotted in 2004, that's W32/GPcode[39]. It searches for specific file extensions, encrypts them and demands ransom. And given today's crucial availability of information, the trend will continue growing.

A cryptoviral attack basically takes data as a hostage, encrypted with the author's public key, naturally wiping out the unencrypted data, and demanding a ransom for it. Whether a retrovirus attack or a future trend, if well executed the possibilities and damage caused by such infections, would definitely test your security flexibility.

Adam Young's in-depth research on cryptovirology[40] provides an great overview of the concept. It opens up a discussion on "kleptographic attacks[41] ones that utilize subliminal channels to transmit things like: private signing keys, private decryption keys, symmetric keys, etc. outside of a cryptosystem (e.g., smartcard)". Future attacks would be definitely better planned and executed compared to the current situation.

However, I doubt cryptoviruses would be launched on a mass scale, as it would raise too much noise, which is why I believe the actual metrics on that type of malware aren't as extensive and they would be. It opens up yet another point to consider, and that is related to the momentum I've mentioned, would an organization pay the ransom if its last accessed files/folders for half of the work day are about to get deleted, not just held hostage? And what if they demonstrate it, since they got nothing to lose in this case?

[36] http://www.sophos.com/products/es/zombiealert/
[37] http://www.f-secure.com/v-descs/diskkill.shtml
[38] http://www.f-secure.com/v-descs/one_half.shtml
[39] http://www.viruslist.com/en/alerts?alertid=166119889
[40] http://www.cryptovirology.com/cryptovfiles/cryptovirologyfaqver1.html#whatiscryptovirology
[41] http://www.cryptovirology.com/cryptovfiles/cryptovirologyfaqver1.html

Platform for disseminating other junk

The odds are, that a percentage of the global spam sent today is coming straight from your PC. Botnets are actively utilizing their connectivity to the Internet for spreading spam, phishing, worms, do hosts' mapping, act as platform for spreading, or hijacking backdoored malware, that platform is functioning right there in front of us. An entry at the Incident Handler's Diary[42], for instance mentions that use of Brazillian defacers(the world champions) for hosting of phishing sites on defaced servers has been already happening, yet another indicator of the growing consolidation of different parties and a factor for growth.

The majority of these attacks, as well as malware in itself are getting increasingly localized, in both, their targets, and social engineering, even network vulnerabilities. Exploiting the momentum of local events, organization's reputation, and total impersonation of an organization/individual is getting even more popular, because it's successful. A recent, rather odd case related to localized malware, was when a person that happened to possess child-porn images, though he received an official police warning. That very same local police warning, was actually sent from a worm[43]!

Mass Identity theft and financial abuse

Keylogging, taking active screenshots of browser sessions (perhaps to better tailor future attacks), malware authors are also turning the usability of E-banking and its visibility, into easily categorized databases to keep an eye on. For instance, in may, 2005, the Trojan-PSW.Win32.Agent.aa[44], was found to steal data from over 2764 bank sites[45], from over 100 countries, that's not just a hobbyist. According to Valerie McNeven, advisor on cybercrime to the U.S Treasury, cybercrime yielded more revenues the drug trade's $105 billion for first time in 2004[46]. Even though this could be doubtful given the hard to quantify soft and hard dollars of cybercrime, I'm sure it indeed surpasses drug trafficking in respect to popularity and potential for gains, illegal, of course. Moreover, Kaspersky's TrojWare growth rates[47], indicate a 115% increase in Banker trojans(stealing banking/financial information) in 2005 against 2004, yet another indicator it's indeed a growing trend.

Around the industry

During the year, F-Secure built a Bluetooth viruses lab[48] that's indeed a serious commitment from their side on playing a future strategic role in this growing market segment that they seem so good at developing. Sophos introduced the ZombieAlert[49] concept, notifying companies or customers when and if there are part of a botnet. Symantec is getting deeper in storage with their Veritas acquisition[50], meaning even broader penetration of their security solutions. On the other hand vendors are starting to actively research, or directly license rootkit protecting technologies in order to remain competitive. Overall, compared to previous years, vendors are

[42] http://isc.sans.org/diary.php?storyid=724
[43] http://www.vnunet.com/vnunet/news/2147777/internet-worm-catches-child
[44] http://www.f-secure.com/v-descs/agent_aa.shtml
[45] http://www.f-secure.com/weblog/archives/agent_aa.txt
[46] http://www.itbusinessedge.com/item/?ci=9598
[47] http://www.viruslist.com/en/analysis?pubid=167798878
[48] http://www.f-secure.com/weblog/archives/archive-052005.html#00000568
[49] http://www.sophos.com/products/es/zombiealert/
[50] http://www.computerworld.com/securitytopics/security/story/0,10801,98269,00.html

releasing much more detailed, and sometimes scary, not biased malware statistics, while I greatly feel more attention should be paid to R&D, and anything theoretical, besides thinking that appliances are the natural evolution. They may be, but your "know-how" is what would prove most valuable in the long-term.

Another trend that I already mentioned, is the ongoing close collaraboration between independent researchers, system administrators and anti virus vendors, that is proving highly beneficial to improving their early reaction capabilities to new pieces "in the wild".

A report[51] released by Kaspersky Labs, gives a good overview of what antivirus vendors are up to compared to one another :

3.1 Summary Table of Proactive Technologies Used by Vendors

	Cisco	McAfee	Panda	Symantec	Trend Micro	BitDefender	Kaspersky
Heuristic Analyzer		•	•	•	•	•	•
IPS		•	•	•			•
Buffer Overrun		•					
Policy based					•		
Alerting system				•	•		•
Behaviour Blocker	•		•			•	•

Source: Kaspersky Labs, http://www.viruslist.com/

Mind you, rootkits capabilities would be able to reset the life cycles of many of the segments covered by malware (adware, spyware, trojans etc.) in the upcoming future, and so will solutions hopefully emerge.

Should we witness the consolidation between though to be main rivals in the upcoming future? I bet so, since anti virus industry is poised for success, and of course, very intense competition. With the time(the sooner the better of course), end users and corporate decision makers will educate themselves even more on what they should expect from a antivirus solution these days. And either get "it", a substitute, or switch vendors.

Particular events I didn't actually find amusing during 2005 were how fast and easy malware authors started using Sony's DRM technology[52], to extend it into rootkit capabilities in order to achieve their goals. This transparency in the security industry in respect to the open flow of information assists both sides, what's amazing is how the majority of vendors started taking credit one by one over who first started the research. So, for months, thousands of users were infected by Sony's strategy, without any vendor having a clue about it?! (Psst, no!) Lack of technology – nope, lack of threat awareness – nope, eventual bad PR fiasco – yep, at the bottom line this is Sony we are all talking about, a deep-pocketed, highly respected company, or at least used to be. Think vendors, if it was a malicious insider in a production facility that has managed to gain access and actually disseminate the malware in such a way – it would end up a story worth mentioning. But knowing that it's Sony, and not wanting to blow the whistle in the face of the company, it's obvious that sooner or later a researcher or someone will come across this, and put the majority of vendors in favorable, this time, protective position. What Sony did was up to

[51] http://www.viruslist.com/en/downloads/vlpdfs/wp_nikishin_proactive_en.pdf
[52] http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

their point of view, greatly underestimating the opinionated and the biggest think-tank of the world. Stuff like this could have worked years ago, if it happens today, sooner or later (a bit later in this case) will come across strange activities, and have the entire community express an opinion about.

Another important issue to note about Sony's case is that lawsuits will follow in only these countries whose law expertise in computer and network security is way too higher compared to the majority of others. It is an extremely unpleasant situation for the company, as more attention and awareness to the issue will also be brought by civil and digital liberties organizations.

Just for the record, F-Secure and Kaspersky are keeping it customer-friendly with team blogs, compared to the other players, playing it corporately, and sticking to reports and analyses only. Blogs save the momentum though, and the echo generated out of a discovery are always beneficial.

Of course, we can have an endless discussion on the advantages and disadvantages of anti virus solution, the point is that the industry has been pretty active for the past several years!

05. Factors contributing to the rise of malware

If I were to include them all, I would need another several weeks research. And quantity of the factors isn't of importance, but highlighting the major ones. Have a point of view? Drop a line!

- **Documentation transformed into source code**

Extremely easy entry on the scene, given that what used to be howto's and documentation on how to write worms turned into open source code that's can the theoretically be discussed and commented on every web forum out there. Source code of malware can be easily found online, or requested offline in the form of a CD/DVD. The globalized Internet allows the hosting of questionable in other countries materials, while a great deal of people are still convinced that security could be improved out of having source code freely available. IDS and anti virus filtering experiments with source code, both original, and modified, have always been an option, and so are wannabe authors. For instance, Fanbot.f was developed using the source code of Mydoom and the SbBot variants, and even left the message inside the code[53]. Though, malware's source code truly "wants to be free" these days.

- **Vulnerabilities, even patches, easily turned into exploits**

The current number of vulnerabilities reported, their severity and the use of security research tools for crafting exploits[54], are shrinking the anyway huge window of opportunity posed by released vulnerabilities and working exploits. Given all this, the modulation and impact of malware on an enormous number of hosts worldwide, today's malware is successfully evaluating the response of the Internet community towards dealing with 0day, or 1day vulnerabilities.

There's been recently a lot of media reports on 0bay vulnerability market[55], that I expressed an opinion on in one of my blog posts. Basically a malware could be constantly "loaded" with new modules, and besides exploiting witty social engineering vulnerabilities, authors prefer to exploit vulnerabilities mostly. There has always been and will always be a discussion on whether the

[53] http://www.viruslist.com/en/analysis?pubid=173190935
[54] http://www.metasploit.com/
[55] http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html

release of vulnerability (no exploit included) improves security or damage it. The thing is when? Now, or in the near future, because today's transparency and active discussions are still leaving the unaccountable by anyone vendors in a catch-up mode. And while they are fighting bugs on their solutions portfolio, the rest of the Internet in a "stay tuned" situation.

Software vendors release patches on a freewill basis in respect to time, given they are not legally obliged to do so, it's a connected world and security is the trade-off, some will say. We can though, argue as the current model of malware attacks abusing the Net as a whole quite often puts vendors and their stakeholders in a "catch-up" mode. For instance :

- *The time between the disclosure of the vulnerability and the release of an associated exploit was 6.0 days*

- *The average patch-release time for the first 6 months was 54 days. This means that, on average, 48 days elapsed between the release of an exploit and the release of an associated patch. I must also add that according to IronPort[56], a security appliance vendor, not only does vulnerabilities act as a growth factor, but the collaborative approach of the anti virus industry left your business exposed to risks in the wild for 56 days this year. Also, consider going through Av-test's statistics on the vendors' responses[57].*

- **Clear signs of consolidation on the malware scene**

One of the important events on the malware scene, that greatly changed, and made it much more dangerous, was the consolidation between different parties. The lack of misconfigured email servers acting as a platform for the dissemination of junk, made it necessary that malware authors start crawling around hard drives, successfully obtaining a huge number of fresh and valid email addresses. Web site defacers are offering the web servers for hosting of, both payload, and actual fake sites. And exactly the opposite. While thinking you're at citibank.com, you might be actually surfing someone else's hard drive, courtesy of a malware author. Each of these groups have advantageous approaches compared to the others, and uniting and exchanging updated information between one another is causing even more competitive fight with the criminals.

- **Over 960M unique Internet users their connectivity, or purchasing power**

To me, the penetration of the Internet in a Windows world, with millions of connected to the same highway hosts, actively taking advantage of E-commerce, is what lures malware authors to launch more attacks. What should also be noted, is that, it's not just someone's financial data, or non existent "top secret" information stored on their PC an attacker looks for these days. Instead, it's the overall Internet connectivity of the host, it's bandwidth, and even storage capacity, as illegal hosting on demand will emerge as a concept anytime now in my opinion.

It is not just the profit-maximization opportunity seekers that go through quarterly E-commerce data. Malware authors, and the rest of cybercriminals are also pretty aware of the growth of online advertising, and E-commerce as whole. Cybercrime as a concept is evolving, and cybercrimes are often a real-life criminal's cash cows.

A recent case with a drug raid in Oregon shred more light on the fact that real-life criminals are actively taking advantage of various online exploitation techniques[58]. While the

[56] http://www.silicon.com/0,39024729,39155160,00.htm
[57] http://www.av-test.org/down/ms05-039.zip
[58] http://www.securityfocus.com/brief/42

information can naturally be obtained through common identity theft tactics, such as dumpest diving, information gathering, impersonation, direct request, phishing, and stealing login information out of malware infected users for the purpose of illegal funding is a real possibility in the long-term.

- **The media as a fueling factor for growth**

Malware authors logically hate to get on the front page, it would ruin any temporary advantages against the vendors, and consequently the potential victims. Even though the media, as always, is actively reporting on each new variant, even speculating on what's actually going on, haven't been their core competency recently. I greatly feel, more attention should be paid to what matters in an anti virus solution, can a recent event directly affect me or my organization, and what to do about it, instead of emphasizing on malware names. Now, that's hell of an appropriate moment to mention the possible misunderstandings posed by cross-reference malware names, some even make the news too[59]. Don't get me wrong, it's the media that has the capacity to communicate all your values.

- **The demand for illegal services**

There will always be such a demand, and that's one of the core principles of economics, specialization, namely, a malware author doesn't have the background necessary to efficiently harvest/crawl for fresh email addresses, this is where the spammer and phishers come into place bring in know-how. People do impulse things like shutting down their competition over the Internet given with the false sense of security concerning the guy hired. Spammers also constantly need fresh hosts to spread their "message", and the same goes for phishers. For instance, cybercriminals forward responsibility(or do they actually?!) though renting access to the botnet, while I am certain the ease of developing and maintaining an electronic marketplace for pretty much anything illegal in this case, is a fully realistic scenario that the ShadowCrew actually realized for a little while.

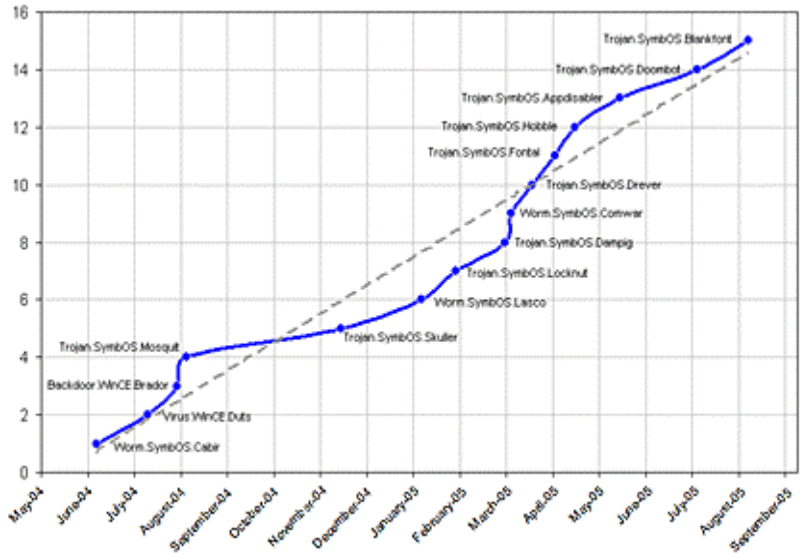
06. Future malware trends

The nature of trends covered here is in no way intended to be complete, simply because you would often find the scenarios for the future either too big, or too narrow. I have anyway tried to compile my point of view in the following way :

[59] http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1152377,00.html

- **mobile malware will be successfully monetized**

Generating buzz around mobile malware will again get rather common during 2006.



Source : Kaspersky Labs "Overview of Mobile Malware[60]*"*

According to vendors, it has already reached the 100 variants barrier. We are seeing it everywhere due to the fact that the number of mobile devices outpaces the number of PCs in the world, yes, that's true, and a bit of a common sense. I expect to see further research on mobile devices vulnerabilities, Symbian devices mostly, as this is where most top of the breed models come from. Fontal's ability to kill the phone, makes it particularly devastating if successfully disseminated. around an event/country.

CardBlock[61] should also be mentioned as the evil side of Fontal in a certain way. It deletes pretty much everything, and password-protects the card with a random password, as soon as the device is restarted of placed in another card. Mobile malware has a lot of "potential", and at the moment authors are just actively experimenting, lack of forensics as an incentive? On the other hand, MMS malware with a lot of social engineering involved, can also easily break the ice. I think timing is an important factor here. If users start receiving any kind of malware somehow related with the event they are current at, many will fell victims of course. We would on the other hand witness the inevitable monetization of mobile malware, such as the abuse of premium numbers, impersonation scams, ring tones and melodies revenue generators, voting/participation(sms) schemes and many others. As the world goes towards an increased use and interest in mobile banking, the GSM commerce that will emerge will again open up countless opportunities for malicious attacks to take advantage of. Would mobile phishing also emerge in that case?

Mobile malware will evolve, mainly because of the penetration of faster networks, and the levels of new features that come up on the market these days. Malware session keylogging, dissemination though the contact list, harvesting phone numbers are retro techniques that would inevitably reappear on this front, or at least authors will try to develop. Something else, to consider is the use of mobile malware as a propagation vector, in the form of a URL for instance, or successful social engineering approach, given enough numbers can and are collected. For instance, Commwarrior.C[62] immediately replies to incoming messages with an infected MMS that contains previous chats within, an improved effect of social engineering, and that's just the beginning in my point of view. SPIM, that is mobile spam, has been around for a while, and with

[60] http://www.viruslist.com/en/analysis?pubid=170773606
[61] http://www.f-secure.com/v-descs/cardblock_a.shtml
[62] http://www.f-secure.com/v-descs/commwarrior_c.shtml

Telecoms and Cellular providers building Internet gateways to further improve performance, I see a clear indication to worry about.

Key point :

The number and penetration of mobile devices greatly outpaces that of the PCs. Malware authors are actively experimenting and of course, progressing with their research on mobile malware.
The growing monetization of mobile devices, that is generating revenues out of users and their veto power on certain occasions, would result in more development in this area by malicious authors. SPIM[63] would also emerge with authors adapting their malware for gathering numbers. Mobile malware is also starting to carry malicious payload. Building awareness on the the issue, given the research already done by several vendors, would be a wise idea.

- **Localization as a concept will attract the coders' attention**,

By localization of malware, I mean social engineering attacks, use of spelling and grammar free native language catches, IP Geolocation, in both when it comes to future or current segmented attacks/reports on a national, or city level. We are already seeing localization of phishing and have been seeing it in spam for quite some time as well. The "best" phish attack to be achieved in that case would be, to timely respond on a nation-wide event/disaster in the most localized way as possible. If I were to also include intellectual property theft on such level, it would be too paranoid to mention, still relevant I think. Abusing the momentum and localizing the attack to target specific users only, would improve its authenticity. For instance, I've come across harvested emails for sale segmented not only on cities in the country involved, but on specific industries as well, that could prove invaluable to a malicious attack, given today's growth in more targeted attacks, compared to mass ones.

Key point :

The ability to tell more about the total number of infected hosts, in respect to their geographical location for future attacks, would continue to attract the author's attention. Picture an author that's aware of the exact locations of all the infected victims, and that their native languages. And these and various other system stats are spread among the other cyber criminals, in the ecosystem I see as a natural evolution. Localization would easily result in far more effective attacks, compared to the current mass mailings.

- **Open Source malware**

Have we reached the level where malware would be freely modifiable for anyone wanting to extend its functionality? I'm afraid it's already happening, and we can truly define it as open source malware, as people are actively modifying it, adding more features. Agobot/Sdbot and many other are released under the GPL license, and anti virus vendors are already counting thousands of variants produced under the same code.

Distributing the source code contributes to the increased anonymity of the real authors and the diversifying of the attention already gained over a particular variant. You'd better have you fans in the news, without even having to bother they'll ever compete with you on know-how, instead of getting all the attention at your malware. Making the source code public is a bit of a dirty, yet visionary trick from malware author's point of view, it brings many more newbies to be caught on the radar, instead of the experiences ones. The noise generated by the script kiddies and wannabe media heroes, creates a great environment for the real authors, to keep playing behind

[63] http://www.simplenote.com/images/PDFs/spim.pdf

the curtains, and theoretically, to hijack the most successful variants based on their very own code. Another very significant benefit of open source malware is how easily new features and concepts get added, thus benefiting the malware scene as a whole, and requiring more competitive play from the vendors.

Key point :

Open source malware is a real issue that's currently resulting in hundreds of copycats out there easily launching a bot on their own. And whether successful or not, this fact is responsible for the flood of variants of known families. That is, of course until an easily exploitable remote vulnerability appears, which happens rather often these days by the way.

- **Anonymous and illegal hosting of (copyrighted) materials**

Today's advances in transferring huge files across the Internet with the help of BitTorrent, get easily implemented in malware. And even though we are witnessing the decline of malware using P2P as a propagation vector, we would start witnessing the use of infected zombies for unauthorized hosting of any kind of content.

In the brief "future trends", that I included in The Complete Windows Trojans paper, I slightly opened up the question of illegal hosting service, so I was greatly surprised the idea hasn't been more popular, until recently of course.

We should see even more "utilization" of an infected host, and the way we are seeing how botnet master's verify the bandwidth availability of all PCs, that way they will easily start verifying the storage capacity, and get impressed for sure. Picture a huge distributed storage capability, where the loss of a single host, wouldn't affect the actual dissemination of the files in question, neither it would influence the rise of bandwidth usage. BitTorrent disrupted the concept of transferring huge files over the Net. As we've already witnessed during December, 2005, a relatively modest, still powerful enough botnet of 18, 000 computers[64] started using BitTorrent to transfer pirated files over the hosts. Certain users will definitely wake up as true porn kings :))

Key point :

The overall demand for illegal service that I already stated as one of the main factors fueling the growth of malware, would result in the abuse of an infected host's storage capacity. Given today's P2P concepts, and the disruptive BitTorrent technology, it is not longer required to on purposely slow down transfers to hide the activity on a user's host. Connections have evolved, and so have technologies, and taking even a broader note, I could argue a host's bandwidth speed, and storage capacity could be easily bargained on when renting botnets, or the service in itself.

- **The development of an Ecosystem**

Google, AOL, and Yahoo!'s affiliations can be clearly defined as an ecosystem. Google's search technology achieves explicit velocity, and it's advertising program's quality generates revenues using AOL's and Yahoo! massive audiences -- everyone's happy! A huge percentage of both, Google, AOL, and Yahoo!'s revenues are fairly distributed among them, simply because they wouldn't be able to survive on their own, or at least miss hell a lot of profitable opportunities.

[64] http://www.eweek.com/article2/0,1759,1904429,00.asp?kc=EWRSS03119TX1K0000594

The higher the pressure put on malware authors and other parties, the higher the chance of the development of such an ecosystem among them. Whenever a natural disaster happens, let's say in China, a phisher would seek localized email addresses, ones provided by both malware authors, and spammers. That very same ecosystem I'm talking about, would also bring sellers and buyers of "services" together. Imagine a database that keeps track of important variables such as IP, Browser version, host's OS, geolocates it, and passes it to everyone, or even worse zombies stats for rent. Taking into consideration reconnaissance and OS fingerprinting for compiling hit-lists, and we have a problem.

Now imagine a malware, such as Bagle, or any other implementing spamtool modules to harvest the victim's hard drive for email. In our case, one that goes through the most recent emails received, strips out the sender's IP addresses, and both confirms it as an active one, prior to including the client's version, and it's geolocation. Today's witty malware of spotting non existent domains on the hard drive, left on purposely through "poisoning" techniques, will inevitable evolve in its understandings of the opportunities.

Key point :

The true benchmark for serious commitment, perhaps investment in the malware scene in my opinion would be the development, and eventual discovery of such an ecosystem, the way ShadowCrew's electronic marketplace was tracked and shut down. In would emerge not only because the environment would become even more competitive for authors, but also because of the clear gains for all the parties, given they realize them. From another point of view, centralization is always a weakness, but that can also be questionable.

- **Rise in encryption and use of packers**

As far as packed malware is concerned, it would continue to gain even more popularity by malware authors looking for ways to make it harder to analyze their code. Looking at Kaspersky's metrics on packed malware, we see, a modest, but increasing trend in this field. And besides thinking that encryption is a logical development, today's huge number of commercial packers that are available get often purchased, or pirated copies are obtained.

Year	Increase in packed malware relative to other malware
2003	28.94%
2004	33.06%
2005 (forecast)	approx. 35%

Source : *Kaspersky Labs http://www.viruslist.com/en/analysis?pubid=167798878*

The use of the Hacker Defender[65], its Golden Hacker Defender edition, as the most popular ones, or any other packer to make it harder for a vendor to analyze the code, is allowing it to win necessary time to infect the seed victims that would improve the chances for success of the malware. We would definitely witness more development in this field any time now.

Key point : Winning time gives authors a crucial temporary advantage to infecting seed victims, making it hard to thoroughly analyze code and purchasing commercial tools or obtaining illegal copies of them, should be considered as a common practice. The interesting part is how developers of rootkits are adding protection against rookit detectors, and exactly the opposite, as pointed out in a post[66] at F-secure's Blog.

[65] http://hxdef.czweb.org/
[66] http://www.f-secure.com/weblog/archives/archive-102005.html#00000675

- **0day malware on demand**

We have already seen this, and we will continue seeing it ever more. A web site that I regularly used to peek at(now down, cjb.net domain though so it's up somewhere else!) was offering specially crafted, and of course undetected by antivirus vendors malware coding services, rootkit capabilities included. For instance, "**The Symantec DeepSight Threat analyst team** has uncovered evidence indicating that bot networks that can be used for malicious purposes are available for hire. In July 2005, in an Internet relay chat (IRC) discussion that the DeepSight team was monitoring, a self-proclaimed bot network owner revealed the size, capacity, and price of a bot network that he was making available. Customized bot binary code was also available for between U.S.$200 and U.S.$300"[67].

Key point : Having open source malware means knowing how to add modularity, make it truly undetectable, and perhaps even having build-in special features, seen nowhere else. Malware like this, if its well programmed, could bypass the majority of anti virus solutions, and in case any other perimeter based risk management solutions aren't in place, it would really do a lot of damage. What's also important to note, is the growing communication between such "sellers" and "buyers" would further make entries on the malware scene much easier, than they are right now!

The number of people capable of coding malware is growing(or copy and pasting!), and it's up to their social and moral obligations not to start offering their services to the great number of people looking for them. So treat your coders with respect, please :-)

- **cryptoviral extortions will emerge**

That's a bit of a creative in a nasty sense of humor type of malware, no regrets, no demands, the art of malware is battlefield :-) After ensuring what's most precious to an organization or individual is made useless by encryption, the desperate victim is the one having to initiate the contact and comply with the extortion. If you even got infected with a malware, lost something in one way or another, and had the chance to contact the author, what would be the first thing to say?? In this case, you will have to negotiate in one way or another and cut the physical damage part :)) Making sure the infected data hasn't actually leaked out of the organization, but is only remaining encrypted on its network, is a good sign. But in the future, authors will find ways to adapt, would another market for trade secrets emerge, that's a scary thought! Such kinds of attacks should be well researched as they will soon start appearing one way or another.

Key point : directly attacking the availability of information and successfully establishing a backend communication(infected victim contacts the malware author) is a witty approach malware authors are starting to use. The encryption algorithm, and its actual implementation are currently its weakest points, as well as given no data leaked out of the organization. And of course, clean, and very recent backups.

- **When the security solution ends up the security problem itself?**

Another fact worth mentioning that I haven't seen active discussions on, is what happens when the security solution turns into the security problem in itself? Naturally, having the solution would definitely limit the more serious security problem that would result without it, but what should also be considered is the possibility of worms directly exploiting a vulnerability in the solution. We have already seen this with the Welchia worm, 1 day from vulnerability to worm, successfully

[67] http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

attacked the majority of ISS's customers, that's as a matter of fact a huge number of the Fortune 500 companies. No way to respond to a threat like this given the timeframe, so imagine what could have happened if the payload caused both, hard and soft dollars losses. I should also mention Sony BMG's DRM solution that ended up first as a security threat in itself, and than as propagation vector for malware authors, though it is my opinion that the greatest benefit is the awareness that it built on rootkit technologies. An interesting fact was also pointed out by Mike Rash at SecurityFocus.com is that it could also mean you are doing a violation of the DMCI act for trying to get rid of Sony's DRM protection, now that's just "great"[68].

On the other hand given that some of MyDoom's versions block over 250 firewalls, as well as infected hosts from updating themselves, malware authors are clearly interested in attacking the vendors themselves. Both, directly and indirectly. Another frontline, perhaps a little bit of unpopular one is that of the vendors' or anyone providing security policies or updates and the transparency of their update locations/mechanisms. If we were to go through the known vulnerabilities of known antivirus vendors, we should also go deeper and find out their response time. Plenty of timeframes to abuse. In the future, either through 0day vulnerabilities markets(like the ones already emerging), or through extra efforts, malware authors will pay more attention to attacking the antivirus solution directly.

Another point to consider is that malware authors often think "the best defense as the attack", that also sounds like "hack or be hacked", but it's a weak practice namely, defined by some as retrovirus techniques, future malware will greatly emphasize on directly attacking anti-virus solutions, 0-day vulnerabilities abuse, killing the application, or blocking its most precious signatures update feature. Quite some malware, first disables the solutions, than downloads its payload with ease. I can argue that, the majority of malware authors update their signatures more often than the majority of end users and organizations tend to. Currently companies aren't paying serious attention to tackling this major threat to their effectiveness. The now out-of-development Trojan Defense Suite (TDS) was pretty aware of how fast authors would start targeting its functioning, that is why a randomly chosen process window, lack of default installation directories and other techniques were in place to safeguard against possible interference. I haven't recently come across great research on the topic, though SnakeByte's list[69] that I first featured in the Complete Windows Trojans paper, should be taken as an example. As a matter of fact, you can freely find, executables, process names etc. of products blocked/killed by malware that's already detected. Information that is too convenient to be available in such a way on any vendor's web site in my opinion.

Key point : Is it just me or I haven't seen a proactive vulnerability release by a vendor recently? Should vendors be held liable for Quality Assurance in respect to security, or is it the coders[70]?
The point for companies is to achieve security flexibility, and a great deal of appliance vendors already offer multiple anti virus solutions integration for the purpose. Moreover, policy based protecting, for instance, December's vulnerability in Symantec's over 40 products, could be tackled by blocking the use of RAR archives scanning at all. Security is taken care of, but what about productivity if N % of the organization's workforce have to adapt with the measure in the very last moment? What about the somehow inevitable lost of productivity due to security solutions, that although deals with risk of a real security event, is under great pressure to constantly improve performance of its solutions? "The wild", has gone even wilder these days, and you no longer need access to a commercial alerting service to know that. You could just plug yourself in, and see what's actually going on. HTTP scanning, host based scanning, on-the-fly scanning, hourly updates, is a load that vendors are greatly working on improving. I am not

[68] http://www.securityfocus.com/columnists/369
[69] http://www.snake-basket.de/e/AV.txt
[70] http://www.wired.com/news/infostructure/0,1377,69247,00.html

being a pessimist here, as in a "perfect world", productivity and world R&D spending will triple due to safer networks, malware-free :))

- **intellectual property theft worms**

The success of ransomware/cryptoviral extortion, is a clear indication of the authors' intentions to take more advantage of the intellectual property stolen on an infected host. Myfip[71] is that type of IP theft worm. It attempts to steal files with the following extensions :

.pdf – Adobe Portable Document Format
.doc – Microsoft Word Document
.dwg – AutoCAD drawing
.sch – CirCAD schmatic
.pcb – CirCAD circuit board layout
.dwt – AutoCAD template
.dwf – AutoCAD drawing
.max – ORCAD layout
.mbd – Microsoft Database

We've seen malware that attempts to steal PGP private keys, but we haven't heard of it successfully attacking an enterprise, or anyone else taking advantage of PKI for instance(everyone!). Should we also consider cd keys of software or games we've purchased as an intellectual property? We should, and these would start getting abused even more than they are now. Picture a highly segmented attack(country as the choice) with the idea to steal as much intellectual property as possible from a certain industry. Another fully realistic scenario would be the use of malware for industrial espionage, in this case, infecting a company's network and transferring it back to the attacker. Covert channels[72] implementation would emerge as well. As a matter of fact we've always seen this in the Israeli trojan espionage case. I made a comment in June, 2005[73] :

What's the easiest way to "catch up" or match your competitors propositions and even exceed them? No, it's not called competitive advantage or business intelligence, but taking advantage of remote access control tools to do industrial espionage. Even though major organizations are, at least believed, to be taking care of malware, the story clearly points out the devastating effects of what happens when you don't take your rivals into consideration. The Trojan, self-coded might somehow get ignored by the anti-virus scanners in place, but what's to note is a technique using the autostart feature of CD that I described in The Complete Windows Trojans Paper back in 2003 and thought it was outdated or at least enough awareness was build on its possible abusive use. Hopefully the case will raise even more awareness on the fact that private investigation companies are actively using Trojans to spy on individuals, and that companies striving to innovate or catch up are actually interested in these services, Ethics, E what?!

Would enterprise risk management solutions such as **Vontu**, **Reconnex**, or any other capture this data, what if it's tunneled, encrypted, and than disseminated through BitTorrent, a functionality that is already gaining grounds? Would malware authors find a way to adapt in here as well? In case, we extend the scenario even more, the way recently received emails get replied

[71] http://www.lurhq.com/myfip.html
[72] http://gray-world.net/projects/papers/cc.txt
[73] http://www.astalavista.com/media/archive1/newsletter/issue_15_2005.pdf

by a worm, and recently accessed files under extensions of interest, could further take advantage of the timeframe capability and lead to the success of intellectual property worms. I believe, that events like these are currently happening, and as always, it takes a little while for an organization to find out that it's been infected. Some never even find that information has leaked, until the media watchdogs pick up the story. That being said, it is important to highlight the way different organizations value security incidents. The majority, would for instance count the direct loss of productivity in hourly rate, and the incident recovery costs of the malware infection only. Quantifying intellectual property is still an academic concept, even though scientifically justified concepts and a little bit of marginal thinking, (they aren't 100% accurate of course), can do the job! It would also be wise to say that intellectual property is the only type of asset that can be at two different places at the same time!

Key point : Given the vast majority of sensitive, and ready to be abused by competitors, blackmailers, or hackers, intellectual property worms will emerge during the next couple of years. They would greatly benefit of the current malware trend of more targeted and less global attacks, acting as a 0day threat to corporate enterprises, a threat posed by cyber criminals, competitors, spies, or blackmailers. What that type of malware would have to bypass would be the enterprise wide risk management solutions such as Vontu, ReconneX, Vericept and Tablus, ensuring secret or sensitive information doesn't leak out through the network. In the upcoming future a great deal of efforts will be placed in finding ways to locate and leak intellectual property over the Net.

- **Web vulnerabilities, and web worms – diversity and explicit velocity**

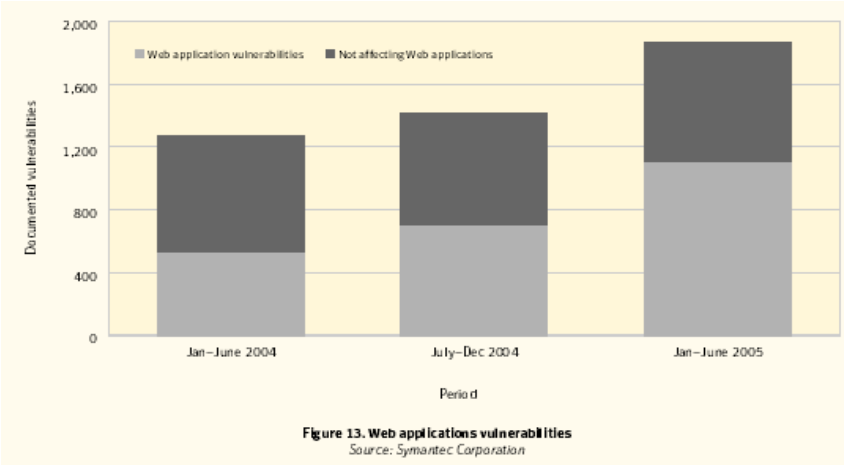


Figure 13. Web applications vulnerabilities
Source: Symantec Corporation

Web application vulnerabilities vs Not affecting Web applications
http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

Managing to unveil a vulnerability and actual exploit for an Internet community, of web forum, you could easily trick these people into thinking they are connecting to the right host, but get redirected, or have their PCs automatically breached into. Malware authors or pretty much anyone with a little knowledge could easily obtain.

Thus, exploiting the trust established between the victim and the host in question. How would a malware author be able to harness the power of the trust established between, let's say, ComScore's top 10 sites and their visitors? Content spoofing is the where the danger comes from in my opinion, and obvious web application vulnerabilities, or any bugs whose malicious payload could be exposed to their audiences. In case you reckon, a nasty content spoofing on Yahoo!'s portal resulted in the following possibility for driving millions of people at a certain URL, if I don't trust what I see on Yahoo.com or Google.com, why bother using the Net at all is a common mass attitude of course. Anyone with a web site full of web vulnerabilities could act as the intermediary in a malicious activity, both inside and outside the site or it's service in particular. If anyone can provide the biggest, relatively recent snapshot of the known Web, that's the most relevant search engine in the world, Google. What I am trying to imply is the possibility of creating and

maintaining huge hit-lists with relatively simple search techniques, an automation, with the use of "slow" worms, whose activities would usually go beyond the radar.

Key point : Any web property attracting a relatively large number of visitors should be considered as a propagation vector, for both, malware authors, and others such as phishers, or botnet brokers[74] for instance. The ease of exploiting web vulnerabilities, increases the probability of such an attack tremendously, so adequate audits for vulns should be regularly considered. Robert from CGISecurity.com once gave a prediction[75] on the possibilities of web worms as well.

- **Hijacking botnets and malware infected computers**

No code is perfect, even the malicious one! In case you reckon, W32/Doomjuice, W32/Bagle, and W32/Welchia attacked MyDoom compromised systems by abusing its weak update mechanism. Certain worms go in the wild based on vulnerabilities in other worms, so even in case full access to the botnet cannot be gained, another author could still abuse them. Theoretically, hijacking botnets is truly sound in my opinion.

Key point : The growing competition on the malware scene would result in far more unethical events, such as competing authors the virus wars, were an example of this growing trend. In consequence, future authors would look to piggyback on existing malware, by exploiting vulnerabilities in the known to dominate the Internet variants. Directly hijacking it though sniffing, flexibly techniques to acquire the botmaster rights, to both, further conduct illegal activities, or simply shut it down would represent a growing trend in the upcoming future from my point of view.

- **Interoperability will increase the diversity and reach of the malware scene**

The brave new world of IPv6

By interoperability I refer to namely, standardizing communication and data interfaces to further ease the communication between different devices. Think Symbian for instance. Yet another point to consider is the extend to which we are actually building networks of intercommunicating devices in our houses, even offices!

This trend called technology, and market forces, would result in a far more adaptive breed of malware this time infecting technologies and services we surround ourselves with, and not stay in front of them(PCs). For instance, during 2005, F-Secure trashed a PSP[76], and a Nintendo devices

[74] http://www.securityfocus.com/news/11195
[75] http://www.cgisecurity.com/articles/anatomy-of-web-app-worms.txt
[76] http://www.f-secure.com/weblog/archives/bricking_psp.wmv

with code that renders them useless just to show a demonstration. Even though many would argue these attacks are not poised for success in "the wild", these experiments will quickly evolve the way we've see it with any type of malware. Cars, gaming boxes, fridges even TiVos will definitely get connection, given they all do, or would, poses the necessary connectivity.

Keypoint:

While the majority of manufacturers and vendors are limiting the use of proprietary OSs for their devices, thus achieving higher penetration and adding more value to their offerings. This huge boost having huge impact on the society and businesses as a whole, isn't left unnoticed by malware authors, and the more lucrative the reach or severity of the attack, the higher the research efforts. My point is that, the benefits and disadvantages of standardization, as well as common data and communication protocols, will increase the diversity of the malware scene even more. Hopefully, vendors will be ahead of the threats as they appear.

Key summary points

- Malware authors update their multi-vendor anti virus signatures faster than most end users and enterprises do altogether
- The high pressure put on malware authors by the experienced vendors is causing them to unite efforts and assets, and realize that it's hard to compete on their own. Yet this doesn't stop them from waging a war in between
- Intellectual property theft worms have to potential to dominate in today's knowledge-driven society acting as tools for espionage
- Don't matter what you always wanted to do to ecriminals, in case of a cryptoviral extortion, you'll be the one having to initiate the contact
- The growing Internet population, E-commerce flow, and the demand for illegal/unethical services, would fuel the development of an Ecosystem, for anything, but legal
- The "Web as a platform" is a powerful medium for malware attackers understanding the new Web
- The unprecedented growth of E-commerce would always remain the main incentive for illegal activities

7.0 Conclusion

I hope that the points I have raised in this research, would prove valuable to both end users, businesses and anti-virus vendors. The Internet as a growing force shaping our ways of thinking and living is as useful, as easy to exploit as well. The clear growth in E-commerce, today's open-source nature of malware, the growing penetration of the Internet in respect to insecure connected PCs, are among the main driving factors of the scene. Do your homework and stay ahead of the threats, most of all, less branding when making security decisions, but high preferences! Please, feel free to direct your opinions, remarks, or any feedback to me, at dancho.danchev AT hush.com or at ddanchev.blogspot.com where you can directly comment on my publication. Nothing is impossible, the impossible just takes a little while!