Future Trends of Malware

By Dancho Danchev (dancho DOT danchev AT hush.com)

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, things were entirely different from what they are today. Trojans used to have fixed ports, 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 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". 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/

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 is a malicious code (standalone or file-infecting), that propagates over a network, with or without human assistance. Malware 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 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, 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 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 solutions should be mentioned, and December's 2005 discovered vulnerabilities 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 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 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, 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. 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 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 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, 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, or external hard drives, 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 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. 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. TrendMicro also managed to compile a list of victims posed by the Sasser event back in 2004.

Cases of damages included the following:

public hospitals in Hong Kong

one-third of Taiwan's post office branches

British Airways - 20 flights were delayed for 10 minutes

Sydney train system

Scandinavian banks

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 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

http://www.whitedust.net/view.php?PageID=45