

IT Security Threat Summary for H1 2007: Social Engineering, Bank Scams, Cyber War and Mobile Spyware

Spammed by Storm: New Trojan Small.DAM Spreads (With) Real News

A sophisticated social engineering trick (Storm-Worm) invited computer users to read breaking news about the severe January storms that caused havoc in Europe, as well as several other shocking events around the globe.

The new trojan, Small.DAM, spread the news in significant volumes via an attachment file. The run of the worm made a significant appearance on the F-Secure Tracking System as it reached hundreds of thousands of computers globally in just one night <http://www.f-secure.com/2007/images/stormworm.mwv>

The impact of the worm was based on the following types of shocking "headlines", often linked to similar real-life events making news headlines in the media:

230 dead as storm batters Europe
A killer at 11, he's free at 21 and...
British Muslims Genocide
Naked teens attack home director
U.S. Secretary of State Condoleezza...

Social engineers attempted to re-orchestrate the spam run with shocker headlines again throughout the following months. However, the effectiveness of this technique seemed to have declined with time and this time the impact was, luckily, much weaker.

2007-01-19 06:51:00	-	-	Email-Worm.Win32.Mydoom.m
2007-01-19 06:51:00	-	-	Email-Worm.Win32.Mydoom.m
2007-01-19 06:50:29	-	-	Net-Worm.Win32.Mytoob.u
2007-01-19 06:49:57	-	-	Trojan-Downloader.Win32.Small.dam
2007-01-19 06:49:26	-	-	Trojan-Downloader.Win32.Small.dam
2007-01-19 06:49:26	230 dead as storm batters Europe.	Video.exe	Trojan-Downloader.Win32.Small.dam
2007-01-19 06:47:52	A killer at 11, he's free at 21 and...	Full Clip.exe	Trojan-Downloader.Win32.Small.dam
2007-01-19 06:46:48	230 dead as storm batters Europe.	Read More.exe	Trojan-Downloader.Win32.Small.dam
2007-01-19 06:45:46	-	-	Trojan-Downloader.Win32.Small.dam
2007-01-19 06:45:45	British Muslims Genocide	Video.exe	Trojan-Downloader.Win32.Small.dam

More Secure Microsoft Windows Vista Challenges Hackers

Improved security was Microsoft's primary design goal for its new operating system, Windows Vista, released to consumers on January 30th, 2007. Several new security and safety features were introduced with its launch.

User Access Control (UAC); Keeping Strangers Away?

For instance, the new User Access Control (UAC) feature is designed to prompt the user for authorization when an application tries to perform an administrative task. In Windows XP, a default

user account - often shared by many users - was granted full administrative rights. A vast majority of malware applications today employ administrative level actions when attempting to compromise a system. When attempting to install itself on a Windows Vista system, such malware will generate UAC prompts that would allow the user to deny the compromising actions.

However, the above is only true if the user understands the UAC prompts. Resulting from extensive tests, security researches have redefined the concept of UAC. They reintroduced the feature as a "design choice" rather than a "security mechanism".

Overall, the new feature is not a bad thing at all, as implementation of this design choice makes running a system more practical as the number of users is limited, and therefore applications run in a restricted environment. But, as with security in general, UAC isn't a silver bullet. Even with the new functionality enabled, Windows Vista users are still vulnerable to social engineering tricks.

Address Space Layout Randomization (ASLR); Malware Becomes a Guessing Game?

Another new Windows Vista security feature is the Address Space Layout Randomization (ASLR). This technique takes key parts of an application's process (system code) and places them randomly into a process' address space. This feature makes it difficult for an attacker to predict target addresses, therefore forcing a malware application to "guess" the location of vulnerabilities.

To skirt around new security features, such as ASLR, malware authors are seeking out old exploits that remain in Vista as part of legacy support.

Windows Vista Security Patches; the Countdown begins

The first ever security patch for Windows Vista was an out-of-cycle patch, released in January. The patch addressed a WMF (Windows Metafile) exploit, associated with the way the operating system deals with graphics. Another similar exploit occurred in April, addressing a vulnerability in the animated cursor remote code execution (ANI).

While both the exploits affected Windows Vista, neither led to any significant compromising of such systems. The ANI exploit was indeed a more serious threat to Windows XP users.

As Windows Vista gains more market share, we expect to see the bad guys pushing to develop more sophisticated methods of attack. Inevitably, we expect that sooner or later they will be successful. That said, as web-based applications are the cool kids of the tech scene today, operating systems won't necessarily need to be the primary focus for hackers. There are softer targets to go after.

Bank Trojans - a Business Model?

Whatever the commodities, or even the place of trading, the bad guys continue to focus on separating people from their money.

As phishing defenses mature, attackers are also increasing and developing their use of banking trojans that are equipped with content filters to detect when people bank online. As soon as banking activity is detected, the malware begins to capture account details using methods such as form grabbing, screenshots and video capture, keylogging, injection of form fields as well as injection of fraudulent pages to attract more users. Not only are these trojans capturing data, they are also

intercepting local sessions and changing transactions details - all unbeknownst to the people just trying to go about their business and manage their finances.

[sidebar] Food for thought: Trust Your Finances with .bank?

Based on F-Secure's suggestion to establish a new top-level domain available exclusively to legitimate financial institutions, a discussion has emerged recently about whether such a new domain, for example .bank, could resolve the wide-spread phishing phenomenon, reaching more and more people every day via banking scams. So how would it work?

Put simply, anyone can register a domain name for as little as about \$5. Most banks operate online under the typical .com, or country-specific domain names such as .fi, .de, co.uk and so on. It is no rocket science, that authentic-looking domain names that replicate existing banking domains, are an easy hit for phishing fraudsters trying to collect financial information from unsuspecting consumers banking online.

One may wonder why banks and other financial organizations do indeed operate under typical commercial domain names. Wouldn't it make sense if the Internet Corporation for Assigned Names and Numbers, the body that creates new top-level domains, created a new, secure domain just for this reason, such as .bank?

Registering new domain names under such a top-level domain could then be restricted only to bona fide financial organizations. Instead of a fiver, the cost of registering such domains could be something like \$50,000. Most fraudsters contributing to the new malicious economy behind phishing would probably think (at least) twice, and give up, when faced with such fees. Banks would love this.

Read more on the topic of .bank at:



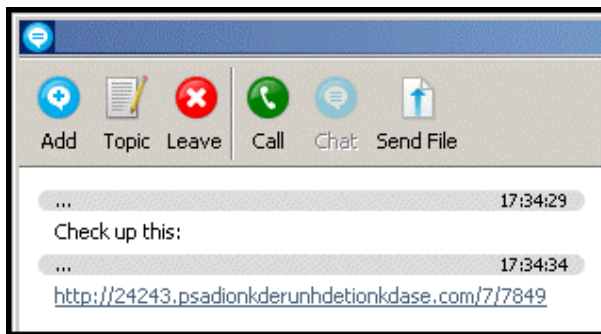
Worms Interrupt More IM Conversations

One of the usual e-mail worm suspects - WareZov - has expanded its attack vectors. No longer just content for spam e-mail attachments, the WareZov gang has adopted a new channel to spread malicious code.

Replicating a method similar to e-mail worms, Skype's chat features have proved to be an ideal vehicle for delivering such content to unaware recipients. Rather than an e-mail attachment, a Skype user receives a link in a chat window, which provides a direct gateway to malicious content.

The most recent variant of such an IM-Worm is cross-client by nature, and thus able to infect multiple Instant Messaging applications via one contact. Using their new "friend's" contact list, such clever IM-Worms can utilize a social engineering trick and craft messages to appear as though they're from a friend.

As web browsers' defenses are hardened, the bad guys are shooting for new targets with new, carefully disguised weapons. In order to equip users with tools to block such undesirable conversation intruders, user education now needs to include "do not to click on links", as well as "do not open attachments" if you aren't expecting them.



Declaration of Cyber War I: Distributed Denial of Service (DDoS) Attacks in Estonia

Coinciding with general unrest and riots throughout late April and mid-May, 2007, various Estonian websites (including sites owned by governmental organizations, banks, and media outlets) were targeted via centralized Distributed Denial of Service (DDoS) attacks. A vast amount of Web traffic, largely originating from Russia, was directed at the sites. Such traffic made many of them very slow, and sometimes even unusable. Slate Magazine coined a new term to describe the phenomenon: "Cyber War I" had begun (<http://www.slate.com/id/2166749/>).

The general unrest in Tallinn gained worldwide media attention, seeding the ground for cybercriminals to steal the limelight. CNN reported (<http://edition.cnn.com/2007/WORLD/europe/04/28/estonia.riots.reut/>):

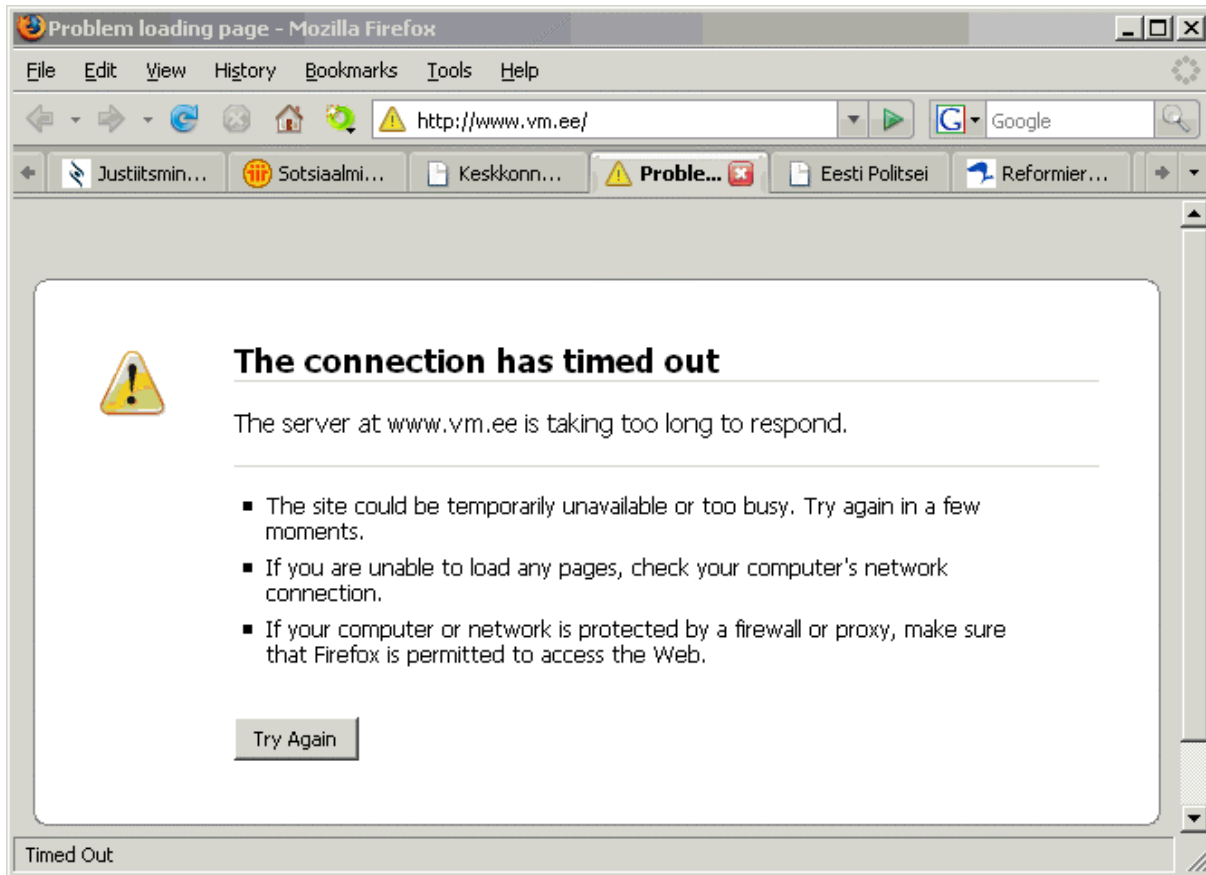
"Police arrested 600 people and 96 were injured in a second night of clashes in Estonia's capital over the removal of a disputed World War Two Red Army monument ... Russia has

reacted furiously to the moving of the monument ... Estonia has said the monument had become a public order menace as a focus for Estonian and Russian nationalists."

The next stage of the riots involved large-scale attacks against websites run by the Estonian Government. Some of the sites were rendered unreachable. Others were up, but did not allow any traffic from foreign/outside IP addresses.

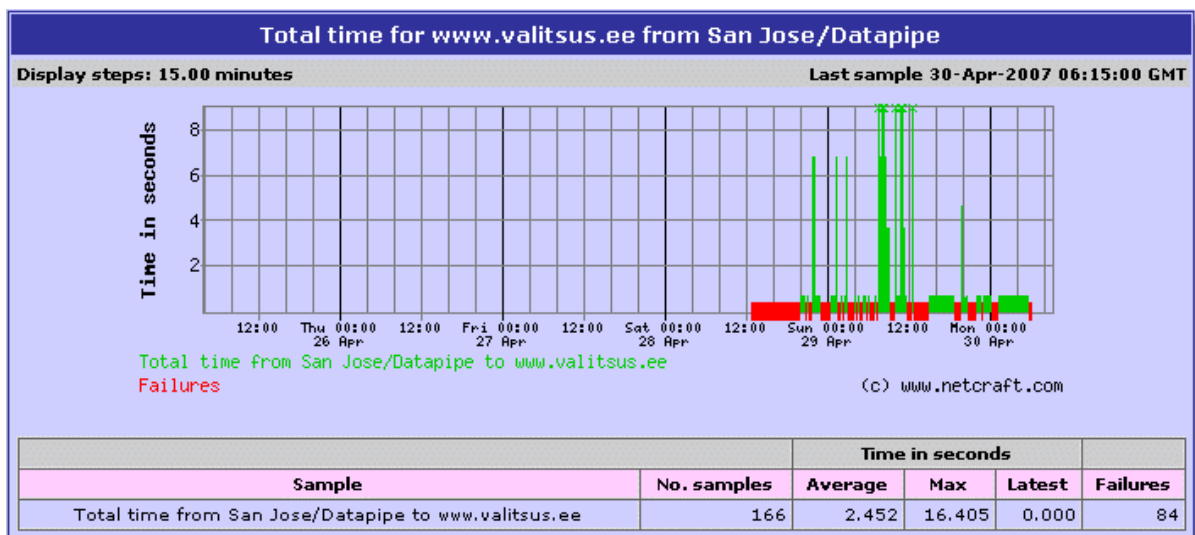
The sites that were attacked on Saturday, April 28th at 15:00 GMT, included:

- www.mkm.ee (Ministry of Economic Affairs and Communications): unreachable
- www.peaminister.ee (Website of the prime minister): unreachable
- www.riigikogu.ee (Estonian Parliament): unreachable
- www.sisemin.gov.ee (Ministry of Internal Affairs): unreachable
- www.valitsus.ee (Estonian Government): unreachable
- www.vm.ee (Ministry of Foreign Affairs): unreachable
- www.agri.ee (Ministry of Agriculture): reachable
- www.envir.ee (Ministry of the Environment): reachable
- www.fin.ee (Ministry of Finance): reachable
- www.just.ee (Ministry of Justice): reachable
- www.kul.ee (Ministry of Culture): reachable
- www.mod.gov.ee (Ministry of Defence): reachable
- www.pol.ee (Estonian Police): reachable
- www.reform.ee (Party of the prime minister): reachable
- www.sm.ee (Ministry of Social Affairs): reachable



Several of the Government websites monitored by the F-Secure Labs that weekend were still down the following Monday. Some of the sites were up but they could only operate in "light-weight" mode. For example, the site of the Estonian Police had to be maintained via just one text-only page.

See below for the Netcraft availability stats on the Estonian Government official home site, www.valitsus.ee. They are fairly alarming.



Here's an example of a Russian hacker site, offering Denial of Service tools, crafted for these particular attacks:



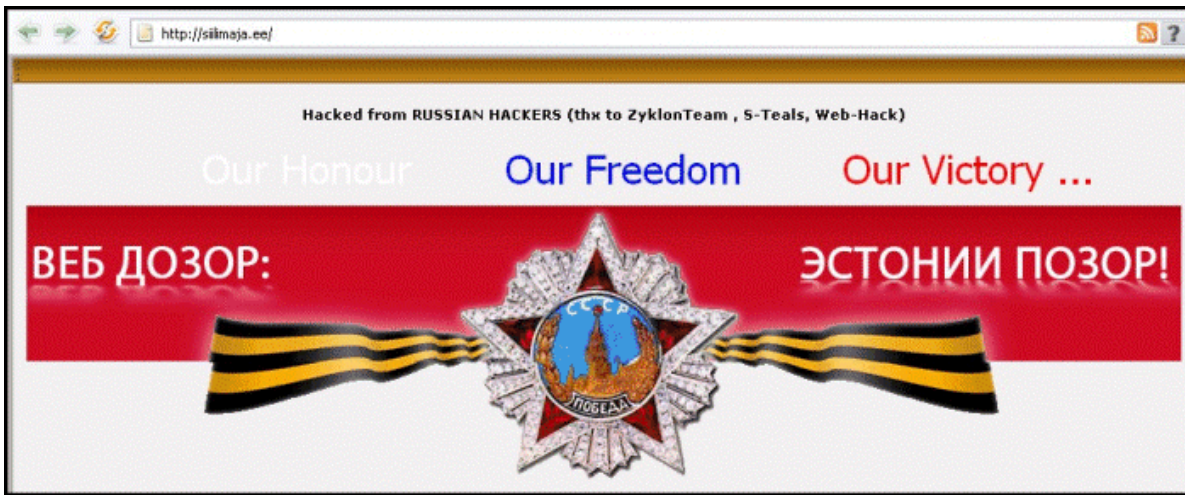
ZYKLON
security team

DDoS Attacker
Дата: 28.04.2007 Написал: zombiexе
релиз **DDoS Attacker** многопоточный, поддержка Socks 4, Socks 5.
Написан на Delphi
[Скачать TCP/IP DDoS Attacker](#)
Special for attacking fuc*ing Estonian sites.

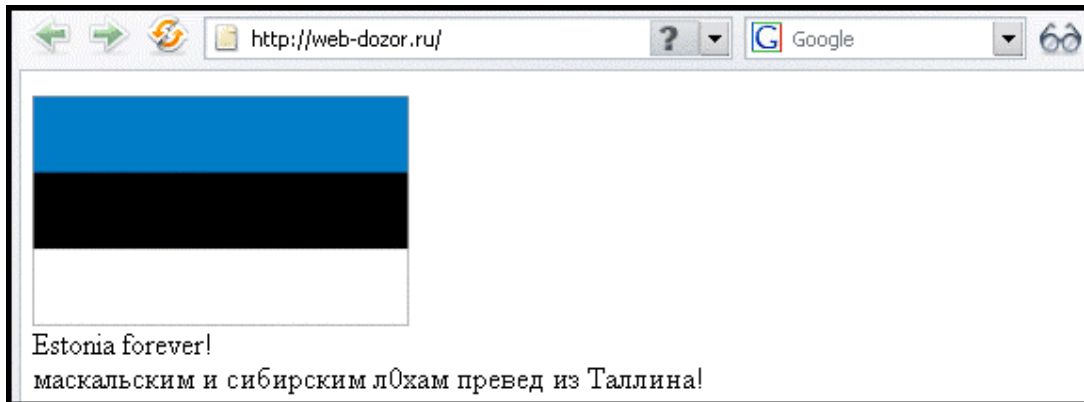
Новости команды
Дата: 12.04.2007 Написал: zombiexе
1. Craft покинул команду ...
2. Релиз MySQL Bruter - [Скачать](#)
3. Идет набор в команду (желающим вступить - связаться со мной по

Обновление FTP-informer
Дата: 18.01.2007 Написал: Craft

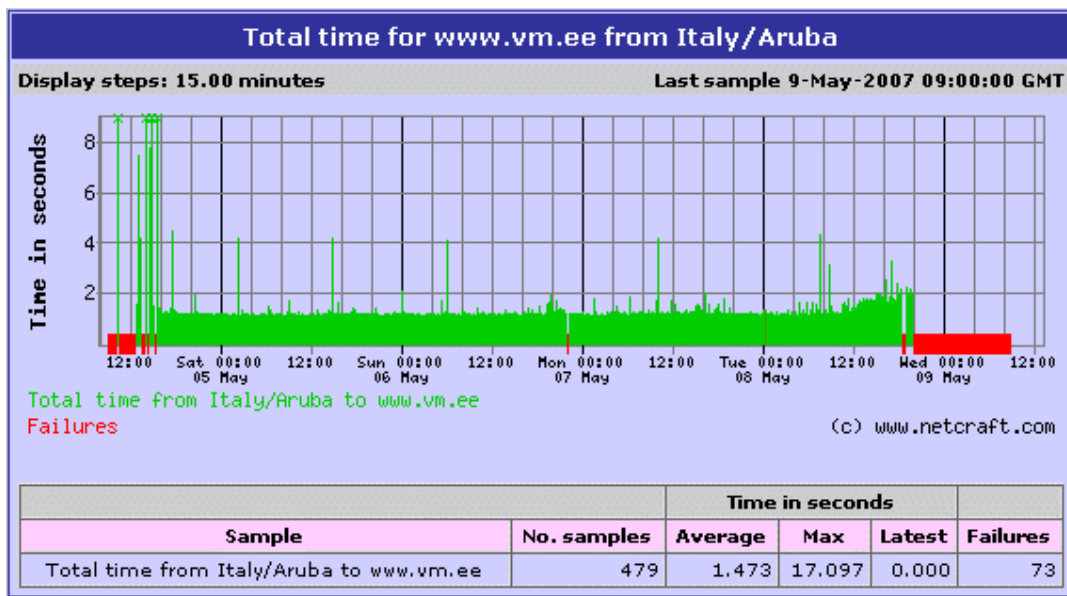
In addition to DDoS attacks, some defacement activity also occurred. For an example of an Estonian website, defaced by Russian hackers, see here:



And here's a Russian website, defaced by Estonian hackers:



The Russian Victory Day on the 9th of May was another key date in the series of riots, both on the ground, as well as in cyberspace. On many Russian-speaking forums, we saw discussions about instigating a massive attack. And sure enough, after three days of calm, just after midnight on the 9th of May, we saw a large botnet attack against multiple Estonian targets.



DDoS attacks have largely been a method of extortion and, fortunately, the recent trend with the occurrence of such attacks has been one of decline. However, it now seems that the latest gimmick in this category is adopting a new form via political protest.

Although not an ideal teaching method, security lessons have been widely learnt as a result of the recent DDoS attacks in Estonia. As a consequence, other countries will now be better equipped to deal with similar attacks in a predictive fashion. The other side of the coin, unfortunately, is that the bad guys will adapt as well.

It is also worthy of mention that besides using botnets to carry out DDoS attacks, we've also seen more and more evidence that vulnerabilities in P2P applications can also be exploited to slam websites with unmanageable amounts of traffic.

The Latest Attempts to Lure us to Expose Ourselves to Mobile Scammers

SMS Spam

The F-Secure lab received many reports of a fairly well-orchestrated SMS Spam campaign in Europe. The SMS messages arrived with a URL that could only be accessed via a WAP gateway. Entering the URL into a computer's web browser returned a page declaring that the service was unavailable. The URL in the SMS was also tied to the phone's receiving mobile device's number, implying that only that particular phone could use the link. Forwarding the message to another phone rendered it inaccessible.



SMS Phishing

We also saw noteworthy global SMS phishing scams. Many of our colleagues in Kuala Lumpur, for example, were "lucky winners" in lotteries organized under the pretense of local organization. The hefty financial reward could be collected by contacting a specified telephone number.

The message displayed on the "winning" mobile phone screens was the following:

"Announcement from PETRONAS MLSY. CONGRATULATIONS your phone number has won a prize of RM 11000. (About US\$3,200) Please contact the following number at 0062858853982xx tomorrow morning at 8.00am. Thank you".

\$M\$ Trojans

Our list of text intruders continues. Three new for-profit SMS trojans that affect mobile devices running Symbian S60 2nd Edition, as well as older devices, were discovered in May.



The Viver family of trojans, originating from Russia, masks itself under the pretense of utility programs for Symbian phones. A variety of such programs has been uploaded to at least one popular file sharing site in the hope that people will, totally unaware, download and install them. The consequences are unpleasant, to say the least.

Immediately after installation, the Viver trojans take it upon themselves to start sending SMS messages to premium-rate numbers (\$7USD). The messages are sent with proper international area codes, so they are able to reach the correct destination, even when activated outside Russia.

If Viver generates enough profit for its creators, we expect that there will be plenty more to come.

Mobile Spyware for Windows Mobile and Symbian 3rd Edition

Other than the above SMS issues, it has been rather peaceful on the mobile malware front (touch wood!). However, mobile spyware and spying tools have been raising their heads lately. In May, we received samples of two “interesting” new mobile spying tools – running on new platforms: spyware has been born for both Windows Mobile and Symbian S60 3rd Edition devices.

We anticipated that spyware, rather than malware, would make an appearance first on these platforms. Historically, hobbyists of varying skills have been behind most of the mobile malware that we have seen so far, and most mobile malware is rather simple. Quite the opposite, spyware is being developed by commercial companies that have a lot more resources, skills, and motivation to get their creations to work.

The recent developments in the mobile arena may be a further indicator that a whole new malicious economy, based on a variety of sophisticated Internet and mobile-based crime, is indeed developing towards unexpected dimensions.