This document contains a compilation of all the Threat Summaries released by F-Secure Labs during the years 2007 to 2011, in reverse chronological order.

This document is preceded by Threat Summaries Volume 1: 2002 - 2006.

For threat landscape coverage and malware research details from the years after 2011, see the Threat Reports and Mobile Threat Reports available from F-Secure Labs: Whitepapers.
THREAT SUMMARY

Overview

2011 saw rapid growth and significant shifts in the global smartphone market, with Google’s Android and Apple’s iOS dominating the battle between mobile operating systems. Malware threats continued to proliferate on the Android platform throughout the year.

Despite the increasing visibility and media attention on mobile malware, desktop machines remain the most targeted devices, and desktop PC based malware remain the most prevalent threats. This year also saw the rise of three major forces in online threats – online criminals, hacktivists and nation-states.

In terms of malware development, the most significant milestone in 2011 is the discovery of Duqu, successor to 2010’s Stuxnet. Also of interest is a rash of malware on the Mac OS X platform in the later months of the year.

Emergence of major players

Organized criminals continue to use online attacks as money-making activities, mainly by using malicious programs or online scams to infect computers, target bank accounts or hijack online transactions. According to Mikko Hypponen, F-Secure’s Chief Research Officer, “[today], it’s more likely for any of us to become a victim of crime online than here in the real world. And it’s very obvious that it’s only going to get worse. In the future, the majority of crime will be online.”

2011 was the year when ‘hacktivism’ – as performed by the amorphous Anonymous collective and its counterparts – also proved capable of organizing significant off-line political protests. Unlike previous outbreaks of online activism, these groups were able to move beyond attacks against government or commercial databases to successfully organizing multiple real-world protests.

Nation-states have also become heavily implicated or suspected actors in a number of online attacks, in particular sophisticated, targeted campaigns against perceived ‘dissidents’, ‘rogue nations’ or even simple corporate espionage.

These trends are presented in more detail in Hypponen’s presentations, in various public forums:

- [Mikko@TedxBerlin](#)
- [Fight Cybercrime, But Keep The Net Free (CNN)](#)
- [Mikko Hypponen: Fighting viruses, defending the net (www.ted.com)](#)
Perhaps not coincidentally, the latter half of 2011 also saw the emergence of a number of new threats on the OS X platform, including the Revir and Flashback trojans, the Tsunami IRC bot and DevilRobber backdoor.

Of particular technical interest are the Flashback trojans, which include a routine to abort itself if an active virtualization environment is found on the machine. According to the Labs analysts, this behavior is “a common anti-research technique used within the Windows ecosystem, but not yet so in Mac’s. It appears that Mac malware authors are anticipating that researchers will begin to use virtualized environments during analysis, and are taking steps to hamper such efforts.”

While we have seen more threats on the Mac platform this year than at any time prior, overall it appears that the most recent run of malware have been ‘testing the waters’, as these threats mostly used attack strategies, techniques or even code that have previously proven successful on other platforms.

No threats on this platform have successfully monetized their operations so far, with the possible exception of DevilRobber.A, which took the most direct money-making route by using infected computers to mine the digital Bitcoin currency.

Steve Jobs passes away
The death of Apple founder and former CEO Steve Jobs in 2011 presents a challenge for Apple, as it must now find a way to continue its incredible record of innovations without the charismatic figurehead many saw as both its driving force and ultimate arbiter.

As on countless previous occasions when a celebrity passed away, the event triggered a wave of spam and SEO poisoning attacks capitalizing on users looking for news.

Windows 7 overtakes XP
2011 is the year when Windows 7 finally overtook Windows XP[1] as the leading desktop operating systems (OS), with 40.5% of the global web market. Despite the decline in market share however, at 38.5% market share Windows XP remains one of the most common operating systems installed worldwide, particularly for home users, and as such continues to be the favored target for online criminals.

Sean Sullivan, Security Advisor at F-Secure says: “People seem to be adding new systems without necessarily abandoning their old XP machines, which is great news for online criminals, as XP continues to be their favorite target.”

As the increased market share makes the platform a more attractive target to attackers, a likely development in 2012 will be the development of threats targeting Windows 7.

Duqu follows in Stuxnet’s footsteps
In purely technical terms, the most interesting development of 2011 is the appearance of Duqu, which appeared almost one year after its predecessor, Stuxnet, was discovered.

Given strong code similarities between the two malware, there is a strong probability that the two malwares were created by the same party. The similarities between the two extend to the use of stolen certificates to sign their driver files, though the details of the certificates differ.

According to Mikko Hypponen, F-Secure’s Chief Research Officer, “unlike Stuxnet, [Duqu] does not target automation or PLC gear. Instead, it’s used for reconnaissance. Duqu collects various types of information from infected systems for a future attack. It’s possible we’ll eventually see a new attack based on the information gathered by Duqu.”

Though speculation is rampant about the origins and intentions of this new malware, like Stuxnet before it, no one has claimed responsibility for Duqu.

OS X Lion gains market share and malware
Desktop OS market share figures also shifted to reflect the release of Mac OS X Lion in July, which rapidly gained over 16% of the Mac user base in the US[4]. For the first time, Mac OS X machines topped 6% of the worldwide desktop market, and just over 13% in the US[5].

Perhaps not coincidentally, the latter half of 2011 also saw the emergence of a number of new threats on the OS X platform, including the Revir and Flashback trojans, the Tsunami IRC bot and DevilRobber backdoor.

Of particular technical interest are the Flashback trojans, which include a routine to abort itself if an active virtualization environment is found on the machine. According to the Labs analysts, this behavior is “a common anti-research technique used within the Windows ecosystem, but not yet so in Mac’s. It appears that Mac malware authors are anticipating that researchers will begin to use virtualized environments during analysis, and are taking steps to hamper such efforts.”

While we have seen more threats on the Mac platform this year than at any time prior, overall it appears that the most recent run of malware have been ‘testing the waters’, as these threats mostly used attack strategies, techniques or even code that have previously proven successful on other platforms.

No threats on this platform have successfully monetized their operations so far, with the possible exception of DevilRobber.A, which took the most direct money-making route by using infected computers to mine the digital Bitcoin currency.

Tablets
In 2011, tablets became firmly established as a must-have item for businesses and schools as well as personal use, which in turn has driven interest in both the consumer device and application development for it. Apple’s iOS blazed the trail in this field and still holds the title of the most sought after platform, for users and developers alike (iPad 2 currently claims 68.3% of the global market)[2].
That lead is predicted to hold through most of next year, and most likely even the year beyond, though the December 2011 launch of the highly anticipated Android 4.0 OS version (Ice Cream Sandwich or ICS) is likely to drive more shifts in market share in 2012.

The new Android OS release promises to solve or mitigate a range of concerns that has so far stymied app development for tablets using that platform. If the new release proves popular with users, Android would finally become a compelling alternative for app developers, who have thus far mostly preferred to work within Apple’s more streamlined development environment.

Other competitors in the tablet OS space have been struggling to keep up with the two giants and have had hard year, with HP’s webOS ending 2011 in limbo as all related hardware development is halted, Microsoft’s Windows 7 yet to gain significant traction and Blackberry’s Playbook essentially taking a distant third place in the competition for market share. Looking forward to 2012, the development of Windows 8 and its new ‘Metro’ UI for tablets is the only new entrant into this market.

Despite the significant growth in tablet usage, a malware targeting this device type has not yet been discovered. Though standard online or browser-based attacks—phishing, spam, click-jacking, social networking worms, etc— are still viable, these are not actually tablet-specific.

**Shifts in the mobile market**

2011 also saw Android emerge as the most popular smartphone platform, with 52.5% of the global market at the end of Q3, followed by Symbian (16.9%) and iOS (15%) [3]. The rapid change in market share between the mobile platforms is also closely tied with another phenomenon—growth in smartphone ownership, particularly outside developed markets such as the United States and Europe.

Even though changes in market share currently favor Android, major developments expected in 2012 may tip the scales again. Most significant among these changes is Nokia’s partnership with Microsoft to put Windows Phone 7 as the native OS on its smartphones. It therefore seems likely users will migrate from Symbian to either one of the current competitors or to Windows Phone 7, leading to more shifting in market share.

Following the announcement of the partnership, and the sharp drop of interest in Symbian app development that resulted, the eventual demise of Symbian seems likely and of course with it, Symbian malware, which have traditionally been the most numerous mobile threats. Whether a drop in malware activity on Symbian simply means more malicious attention being transferred to iOS or Android – or even to Windows Phone 7 – remains to be seen.

**Mobile malware development**

Growth in smartphone ownership has been particularly strong in Russia and China, and in the last two years, we have seen growth in mobile threats specifically targeted to users in these two markets, including premium-SMS trojans, spyware and grayware (apps that skirt the boundaries of legitimate usage).

Mobile developments in these two countries is particularly significant because a number of circumstances specific to Russia and China – including, among other factors, huge domestic audiences, relatively strong levels of technical expertise and uneven law enforcement – have made them ‘development hotbeds’ for mobile malware.

The most prevalent mobile threat we’ve seen targeting users in these two markets have dealt with premium-SMS trojans. In most cases, these threats have exploited country-specific or even network-specific issues in order to monetize their operations. As such, these threats have been strongly localized and have had little impact on users beyond their borders or network coverage areas.

It is however a likely possibility that an enterprising criminal will eventually develop and distribute a ‘kit’ or utility program that would allow attackers outside these countries to run similar operations, targeted to users in their own geographical region.

Though not an absolute certainty, such a development has strong historic precedence, as we’ve already seen a number of other attack patterns (spam floods, Distributed Denial of Service attacks, worm outbreaks, etc) similarly evolve from a manually-run operation requiring technical expertise into automated attacks launched using a simple kit that requires minimal skill.

**References**


5. Chris Smith, Apple Insider: Mac OS X install base grows to over 6% worldwide, 13% in the US; [http://www.appleinsider.com/articles/11/09/03/mac_os_x_install_base_grows_to_over_6_worldwide_13_in_the_us.html](http://www.appleinsider.com/articles/11/09/03/mac_os_x_install_base_grows_to_over_6_worldwide_13_in_the_us.html)

SECURITY FORECAST FOR 2011

Copycat attacks based on Stuxnet

Stuxnet may be the most significant malware development of the last decade.

“Stuxnet can attack factory systems and alter automation processes, therefore making cyber sabotage a reality by causing actual real-world damage,” says Mikko Hypponen, Chief Research Officer at F-Secure.

The financial and R&D investment required combined with the fact that there’s no obvious money-making mechanism suggests only a terror group or a nation-state could have created Stuxnet. And it’s not likely that a terror group would have such resources.

But now that the proverbial cat is out of the bag, similar attacks can be engineered with less effort. “And unfortunately it’s likely that we will see Stuxnet copycats in the future,” says Hypponen.

More mobile malware targeting the Android platform and jailbroken iPhones

Android apps do not go through an approval process like those required by the iPhone App Store or the Signed by Symbian programs.

In 2010, we saw Android apps that posed as games while spying on users, apps posed as banking apps with no official connection to the banks, and apps that attempted to steal users banking credentials. In 2011, the assault on Android phones by individuals with an excellent understanding of mobile applications and social engineering will only get worse.

Jailbroken iPhones also present a unique opportunity for malware writers.

In summer of 2010, two vulnerabilities in the iPhone made it possible for users to “jailbreak” their phone by simply visiting a website. Jailbroken phones can perform functions that were not intended by manufacturer—such as using the still camera on older iPhone models as a video camera. However, the exploit that made easy jailbreaking possible could have easily been modified for malicious purposes.

“If a worm had infected your iPhone, it could do anything you can do on your phone, and more. So it could destroy or steal all of your data. Track your location. Spam your friends. Listen to your phone calls. Dial the presidents of every country in the world. Anything. And you would pay for all the charges it would create, too,” says Hypponen.

Luckily, Apple patched the vulnerabilities before such a crisis occurred.

A large number of iPhone users have purposely jailbroken their phones and are opening themselves to increasingly complex threats. F-Secure does not recommend jailbreaking any device for any reason. The only iPhone worms we’ve seen so far only affect infected jailbroken devices and we expect that trend to continue or get worse in 2011.

Facebook spam goes global

Amidst news that global email spam levels have fallen suddenly, there has been an explosion of spam on social networks. Spam has become so prevalent that many Facebook users in the United States and United Kingdom have begun to ignore it.

“As English speakers become increasingly desensitized towards Facebook spam, the spammers are using language localization as a way to reach new audiences,” says Hypponen.

F-Secure Labs has already seen Facebook spam runs localized into Finnish along with runs that were popular in Sweden and Malaysia. A recent F-Secure survey found that as many as 78% of Facebook users think that spam is a problem on the site. And as Facebook increases its anti-spam efforts, expect to see the spammers change their tactics and targets.

For more about the unique scourge of social spam, visit the F-Secure Labs blog: [Social Spam Q&A](http://www.f-secure.com/about/news/social-spam-q-a)
2010 SECURITY WRAPUP

Overview

Though the security news of the last months of 2010 has been dominated by Wikileaks and the politically motivated online attacks carried out by its opponents and supporters, 2010 will be most remembered as the year when the theoretical threat of cyber sabotage became possible.

Wikileaks and DDoS made easy

During the last months of 2010 Wikileaks and the politically motivated online attacks carried out by its opponents and supporters made international news—but the methods the attackers used were far too familiar to security experts.

Mikko Hypponen, Chief Research Officer at F-Secure, says, “There is nothing new in the type of distributed denial of service (DDoS) attacks that were used to target companies like Mastercard, Visa and Paypal, which had dissociated themselves from Wikileaks. But today DDoS attacks have become so easy to carry out that almost anyone can participate.”

The first DDoS attacks took place in 2000 and since then technology has become so simplified that many of those so-called Hacktivists participating in the attack may be unaware that they are breaking the law.

“Most of the attackers who are part of the so-called Anonymous group are not really computer experts at all but people who want to participate in the attack because they believe in the cause,” says Hypponen. “So they download the tool and let others use their computers to mount the attack. I’m quite sure most of the people participating in these attacks don’t really realize that these are serious crimes.”

Preventing such attacks is a complex, costly endeavor, and typically companies don’t think about prevention until the assault is underway.

“These attackers have succeeded in shutting down the online payment credit card verification systems of both Visa and Mastercard and disrupted part of the PayPal service, immediately causing losses to credit card companies,” says Hypponen.

While these attacks certainly have global political significance, they do not live up to the definition of “cyber war”. “War isn’t just nameless attacks between parties that are not nation-states to begin with,” says Hypponen. “WikiLeaks is not a country. MasterCard is not a country.”
Stuxnet: the most significant malware development of the decade?

The most significant malware development of the year—and perhaps of the whole decade—has been the highly sophisticated Stuxnet worm.

“Stuxnet can attack factory systems and alter automation processes, therefore making cyber sabotage a reality by causing real world damage,” says Mikko Hypponen.

A Windows worm most likely spread through USB device, Stuxnet infects a system, hides itself with a rootkit and sees if the infected computer is connected to a Siemens Simatic factory system. If it finds a connection, it then modifies commands sent from the Windows computer to the PLC Programmable Logic Controllers, i.e. the boxes that actually control the machinery. Once running on the PLC, it looks for a specific factory environment. If this is not found, it does nothing.

Hundreds of thousands of computers around the world have been hit by Stuxnet. Siemens has announced that 15 factories were known to be infected. But Stuxnet is not limited to industrial plants. Most of the infected machines are collateral infections, i.e. normal home and office computers. But the fact that Stuxnet was designed to target a very specific facility or facilities points to the revolutionary nature of the threat.

Unusually large at 1.5 MB, Stuxnet exploited 5 vulnerabilities (4 of which were zero-days—all have been patched by Microsoft), employed a stolen signature and installed its own driver. F-Secure Labs estimates that it would take more than 10 manyears of work to complete Stuxnet.

This complexity and the fact that it could be used to impair the ability of a centrifuge to enrich uranium while providing no monetary gain suggest that Stuxnet was probably developed by a government—though which government is unclear.

For more information about the clues that may suggest who created Stuxnet, visit the F-Secure Labs weblog: Stuxnet Redux: Questions and Answers

Best year for arresting cybercriminals

2010 has been the best year ever in terms of the number of people arrested and convicted for committing online crimes.

Malware, which used to be written by hobbyists, became a vast profit-driven business controlled by criminals around 2003. However, for years the transition of malware from an online annoyance to criminal activity was not reflected by the number of arrests and convictions of the perpetrators. In the rare cases that people were caught and prosecuted, the sentences were hardly punitive. But in 2010 F-Secure saw what we hope is the beginning of a shift in the ability of law enforcement to identify, capture and prosecute cybercriminals.

In a landmark case in March 2010, Alfredo Gonzales received a 20 year jail sentence for being the ringleader of a gang that hacked tens of millions of credit card records from TJ Maxx and several other US retailers. This is the longest sentence ever passed in a cyber crime case. Gonzales and his gang members gained access into the authentication systems of the retailers’ cash registers by hacking into their wi-fi. Millions of credit cards had to be re-issued as a result.

The FBI revealed in October that it had arrested more than 90 suspected members of an international cyber crime ring, accused of stealing about $70million from bank accounts in the United States.

More arrests were also made in the UK and the Ukraine, from where the operation was directed. The criminals had gained access to people’s online banking details by sending infected spam messages. According to the FBI, the arrests were part of “one of the largest cyber criminal cases we have ever investigated”.

An interesting case involving spytools installed on mobile phones was reported by The Register in July, in which Romanian authorities had arrested 50 people accused of using off-the-shelf software to monitor the mobile phone communications of their spouses, competitors and others.

The Romanian Directorate for Investigating Organized Crime and Terrorism also arrested Dan Nicolae Oproiu, a 30-year-old IT specialist who allegedly sold the spyware for handsets running the iPhone, Blackberry, Symbian, and Windows Mobile operating systems, according to The Register.

Mikko Hypponen says, “Antivirus companies are not the police but we always provide the material uncovered by our investigations into cybercrime to the authorities so they can take action. It’s great to see this is having an effect and we hope that the new level of arrests and punitive sentencing represents a permanent shift in the way cybercrime is tackled.”
Windows XP still the major target

The Windows 7 operating system has been lauded as a safer operating system than its predecessor Window Vista. Despite overtaking Vista in terms of market share this year, Windows 7 is still far behind Windows XP, which remains the most popular operating system and the biggest target for malware writers.

“Cybercriminals will always look for the easy targets,” says Mikko Hypponen. “It’s likely that XP attacks will still be around for a number of years.”

In July 2010, Microsoft stopped issuing updates for Windows XP Service Pack 2. At that time, we estimated that 10% of our customers were still using XP SP2, potentially leaving them open to exploitable vulnerabilities.

The security implications of using outdated operating systems have been demonstrated by reports that the oil spill in the Gulf of Mexico could in part have been caused by the failure of computers that were still using Windows NT 4 from 1996.

Hypponen says, ”It is irresponsible that a billion dollar oil drilling operation did not bother to keep its computers up-to-date and as secure as possible.”

Mobile security developments

The number of mobile malware has not increased dramatically in 2010 but this year saw some developments that may provide insight to future trends.

The year opened with several banking apps being removed from the Android Marketplace. The applications were not developed or authorized by the banks themselves and could not do real online banking from the Android device. Apparently they only opened the web interface of the online bank for the user and could have stolen user credentials.

In April, a trojanized version of the Windows Mobile game 3D Anti-terrorist action was uploaded to several Windows Mobile freeware download sites. Infected phones made secret calls to expensive premium rate numbers, resulting in big phone bills for the victims.

In August, it turned out the Android app Tap Snake wasn’t just a game but a client for a commercial spying application called GPS SPY. The game looks like an average “Snake” clone. However, there are two hidden features.
2010 JUNE - SEPTEMBER SECURITY THREAT SUMMARY

Social Networks

F-Secure sees malware and spam in social networks on the rise

Spam in social networks reached a record high level May to September 2010. Malware and spam are appearing more frequently on social media like Twitter and Facebook. So far, most of the attacks on Twitter have been made for testing purposes or for fun to see how quickly they replicate. However, when hobbyists create social networking worms, profit-driven criminals often try to adapt them for making money.

“A deal you just can’t refuse!”, “Do not pay for a new iphone 4, get one for free one for no cost!”, “Whoa, check this out everyone” – spam on Facebook runs under numerous creative tag lines. In June the following string of text tried to lure Facebook fans: “I am shocked!!! The teacher nearly killed this boy: http://bit.ly/aWeBMl - Worldwide scandal!” People who clicked on the link, were directed to an application.

We had a closer look at the case and found more than 140 thousand clicks within the first day and the applications page indicated almost 59 thousand active users. This means that more than 40% of the users exposed to this lure were falling for it.

In August we found another, more popular spam about an unlucky McDonald’s Happy Meal. This spam used bit.ly links to spread itself on Facebook. The links led to h t t p://happytruthblog.co.cc and there were just over 32,000 clicks within a few hours. The ‘clicks to likes’ conversion rates were around 40% and about 48%. These are excellent results for spammers, and much better than e-mail spam. However, the 32,000 clicks were far less than similar spam from June when we saw several examples of viral links that yielded hundreds of thousands of clicks. Returns are diminishing as people are exposed, develop a resistance, and recognize Facebook spam for what it is. In fact, the spammers themselves seem to know this and are working harder to convince people. This version of the Happy Meal spam promises “no need to complete surveys”. But it was the same old spammer lie and the page had an anti-spam bot “test”, which is just a survey by another name.

Social networking spammers don’t need to dupe very many people in order to be rewarded for their efforts. Many of the surveys lead to SMS subscriptions (particularly outside of the USA) and there’s good money to be made. And because the conversion rates are better than e-mail spam, you can be certain that it won’t be going away any time soon.

Facebook has actually made things easier for the spammers and scammers by not implementing the restrictions on landing pages which it first announced in May 2010. Unfortunately, it’s a rather simple task to create a page on Facebook and the bigger problem is that of “landing tabs”, the first tab that’s shown to someone who doesn’t already like the page. Originally, Facebook announced in May to restrict landing pages to “authenticated pages” or to pages with more than 10,000 fans. One day later Facebook back-pedaled and didn’t implement the limitations because small businesses complained. The 10,000 fan requirement was seen as too difficult to achieve. The major use for landing tabs is to build the page’s base, so perhaps it was too much to ask. But having nothing in place opened up a deluge of scams and spam. Some kind of compromise must be possible.

In early September a clever spammer discovered a Facebook vulnerability that allows for auto-replicating links. Until then, a typical Facebook spam required the use of some social engineering to spread. But clicking on any of the application spam links is now enough to “share” the application to the user’s Wall.

Malware in the cloud presents new security problems. Mikko Hypponen, Chief Research Officer at F-Secure, says, “When you start using cloud services more and more, this also means that you are giving up control over your data. As long as your documents and communications are on your own computer, it is possible to encrypt and secure them. Once they are in the cloud, you can only hope that someone else is doing it on your behalf.

Twitter Targeted

Twitter targeted – antibodies fight back

Opportunistic spammers have also been quick to pounce on the newly discovered XSS vulnerabilities in Twitter in an attempt to lead users to dubious surveys and websites. Most of the worms are using onmouseover techniques, meaning it’s enough to simply move your mouse on top of
a malicious (mischievous) Tweet to resend the malicious message to your followers. Though the XSS vulnerability has been fixed, we expect problems to continue. It’s perfectly possible that there will be more malicious attacks, possibly combining this technique with browser exploits.

Mikko Hypponen suggests that Twitter establishes a bounty for finding major new security vulnerabilities in their system, as an incentive to potential hackers to stop breaking into their system. Twitter worms are quite different from the more sinister trojans we see attacking the Windows operating system. Most of the Twitter worms are made just for testing, or for fun. Very few try to steal information or to make money. They are created by the same kind of curious tinkerers that 10 years ago would have been writing Internet worms, just to see how quickly they would replicate.

While social networks are increasingly attractive to malware writers because they can spread information so quickly, this also means that Twitter and Facebook users can stop the spread of malware faster than before. Sean Sullivan, Security Advisor at F-Secure, says, “Social networks have built-in antibodies – their users. Whereas the malicious attacks of yesteryear took weeks or even months to develop, the recent Twitter attacks peaked and ebbed in just two and a half hours.

For more information, here are some posts from the F-Secure Labs Weblog related to social network spam:

- Twitter Attack
- Warning on Facebook worm “FBHOLE”
- Facebook Spam App Du Jour
- All Your Farm Are Belong To Us
- Should Facebook limit landing tabs?
- Two Steps Away from a Free iPad
- Facebook Recommends Spam Profiles
- What’s the success rate of Facebook spam?
- I May Never Text Again: More Facebook Spam
- CPAlead Spam on YouTube
- When do 258 tweets equal nearly half a million dollars?
- Twitter Spam and the OAuthcalypse
- New Spam Worm on Facebook
- Facebook Spam Worm Links to “Mobile Entertainment”
- Twitter onMouseOver Spam
- Twitter Antispam: Media not displayed
- Voi Paska, Facebook Spam Localized in Finnish

**Stuxnet**

**Stuxnet worm targets industrial infrastructure**

The Stuxnet Windows worm is one of the most significant malware cases in recent times. Discovered in June 2010, Stuxnet is the first malware to target specific industrial systems. The Stuxnet worm is highly complex and has required considerable resources to develop it, leading to speculation that a government or governments are behind it. Stuxnet has infected hundreds of thousands of computers around the world but the large number of infections in Iran suggests that the motive of the people behind the worm is to attack Iran’s nuclear program.

Stuxnet spreads via USB sticks and can also spread by copying itself to network shares if they have weak passwords once it is inside an organization. The LNK vulnerability used by Stuxnet would still infect your computer even if AutoRun and AutoPlay are disabled. The current versions have a “kill date” of June 24, 2012, which means the worm will stop spreading on this date.

After infecting the system, Stuxnet hides itself with a rootkit and checks if the infected computer is connected to a Siemens Simatic (Step7) factory system. Stuxnet can make complex modifications to the system; for example it could adjust motors, conveyor belts and pumps. It could even stop a factory and, with the right modifications, cause things to explode.

So far only a few factories have been hit and most of the infected machines are collateral infections of normal home and office computers that are not connected to SCADA systems. Stuxnet does not cause any damage unless it finds the specific factory system it is looking for.

So how can the attackers get a trojan like this into a secure facility? One method could be by breaking into a home of an employee, finding his USB sticks and infecting them. When the employee takes the USB sticks to work, they infect his work computer and the infection spreads further inside the secure facility, eventually hitting the target.

Stuxnet is a very complex and unusually large in size at 1.5Mb. It uses multiple vulnerabilities and drops its own driver to the system because the Stuxnet driver was signed with a certificate stolen from Realtek Semiconductor Corp. The stolen certificate was been revoked by Verisign on 16th of July 2010. A modified variant signed with a certificate stolen from JMicron Technology Corporation was found on 17th of July.
Stuxnet exploits five different vulnerabilities, four of which were 0-days:

- **LNK (MS10-046)**
- **Print Spooler (MS10-061)**
- **Server Service (MS08-067)**
- **Privilege escalation via Keyboard layout file**
- **Privilege escalation via Task Scheduler**

The two Privilege escalations have not yet been patched.

There is a reference to “Myrtus” (which is a myrtle plant) in Stuxnet. “Myrtus” could also mean “My RTUs” – RTU is an abbreviation for Remote Terminal Units, used in factory systems. However, the reference is not “hidden” in the code. It’s an artifact left inside the program when it was compiled. Basically this tells us where the author stored the source code in his system. The specific path in Stuxnet is: \myrtus\src\objfre_w2k_x86\i386\guava.pdb. The authors probably did not want us to know they called their project “Myrtus”, but thanks to this artifact we do. We have seen such artifacts in other malware as well. The Operation Aurora attack against Google was named Aurora after this path was found inside one of the binaries: \Aurora_Src\AuroraVNC\Avc\Release\AVC.pdb.

Stuxnet knows that it has already infected a machine as it sets a Registry key with a value “19790509” as an infection marker. This is actually a date: 9th May 1979. This could be the birthday of the author, or it could refer to the date that a Jewish-Iranian businessman called Habib Elghanian was executed in Iran. He was accused of spying for Israel.

### Arrests in UK

**Arrests in multi-million pound online bank fraud case in the UK**

In September 2010, a police investigation into the theft of at least £6m from online bank accounts has resulted in globally more than 100 arrests and charges against ten people for conspiracy to defraud and money laundering. According to reports from the BBC and Daily Mail, the accused used the Zeus trojan to get access to the online banking login details of at least 600 accounts with HSBC, the Royal Bank of Scotland, Barclays Bank and Lloyds TSB.

Infected weakly protected computers, the gang was able to steal the online credentials and manipulate the web browsing sessions of their victims by creating an additional page that requested passwords, PIN and card numbers. After gaining access to their victims’ accounts, the gang transferred several thousand pounds at a time to the accounts of specially recruited money mules, who allowed their bank accounts to be used for money laundering in return for payment. The accused are from the Ukraine, Estonia, and Latvia. According to the charges, the gang targeted British banks from 13 October 2009 until 28 September 2010.

### Zeus Trojan

**Zeus trojan used to target online banking**

Zeus continues to be one of the most common malware we run into. There was an interesting Windows+mobile case in September involving a ZeuS variant that steals mTANs, using a Symbian (.sis) or Blackberry (.jad) component. An mTAN is a mobile transaction authentication number, sent via SMS, and is used by some banks as a form of single use one-time password to authorize an online financial transaction. The SMS message may also include transaction data that allows you to ensure that nothing has been modified (via a Man-in-the-Browser attack).

Windows OS based online banking is constantly under attack from phishing, pharming, cross-site scripting, and password stealing trojans. Adding an “outside” device to the process is a useful security countermeasure; one that we thought might be technically challenging enough to dissuade any would-be attackers. However, online security is a constant cat-and-mouse game, and we have often predicted that it is only a matter of time before some banking trojan is targeting phones.

S21sec, a digital security services company, recently published information about the ZeuS variants they have discovered, see **Zeus Mitmo: Man-in-the-mobile**. This malware asks for mobile phone details and then send an SMS with a download link based on the answers given by the victim. It is difficult to get the complete picture of this emerging threat vector as the C&C used by the Zbot. PUA is no longer online, but based on the analysis and their configuration files, this attack is not a one-off by some hobbyist. It has been developed by individuals with an excellent understanding of mobile applications and social engineering. We expect that they will continue its development.
Mobile Security Developments

Mobile security developments – jailbreaks, anti-terrorists, snakes and spies

The biggest security story on the mobile front has been the jailbreakme.com website, which made it possible to jailbreak an iPhone, iPad or iPod Touch simply by visiting the website with the device. Jailbreakme.com used an exploit to execute code on the device. Anyone could have used the same vulnerability to execute malicious code on iPhones and iPads, which could have resulted in the first global mobile worm outbreak. Luckily this did not happen and Apple released a new version of iOS to patch the vulnerability on most of their platforms," says Mikko Hypponen. The jailbreaking community also put out their own patch which also closed the security hole for operating systems not supported by Apple.

Some Windows Mobile smartphone users have been affected by the 3D Anti-terrorist trojan, which makes expensive calls to international premium rate numbers, including countries like Somalia and Antarctica. A Russian hacker removed copy protection from the 3D Anti-terrorist Action game and uploaded the trojanized version download sites where people search for free games. “It’s a way of stealing money directly from infected smartphones and the victims only realise what has happened when they receive their next phone bills,” says Mikko Hypponen.

Another malicious application has been found from the Android Market. A game called Tap Snake turns out to be a client for a commercial spying application called GPS SPY. The Tap Snake game looks like an average “Snake” clone. However, it has two hidden features. First, the game won’t exit. Once installed, it runs in the background forever, and restarts automatically when you boot the phone. Secondly, the game secretly reports the GPS location of the phone to a server every 15 minutes.

GPS SPY is a simple mobile spying tool and only costs $4.99. When bought, the application advises you to download and install the “Tap Snake game” to the phone you want to spy on. During installation, the game is registered with a keycode to enable spying. This means that the spy has to have physical access to the phone he wants to spy on. In many ways, GPS SPY / Tap Snake can be seen as a little brother of mobile spying tools like FlexiSPY. GPS SPY is developed by a Russian developer based in Texas, Mr. Max Lifshin (“Maxicom”). GPS SPY and Tap Snake are no longer available in the Android Market.

F-Secure expects to see more malware attacks targeting smartphones. Jarno Niemelä, Senior Researcher at F-Secure, says, “Since 2004 there have only been 517 families of mobile viruses, worms and trojans, but as some mobile malware authors have now made money, we expect to see a lot more activity. Most of the mobile malware we have seen in 2010 has been profit motivated rather than hobbyist activity.” So far the malware monetization methods used by criminals include premium SMS messages, premium voice calls, subscription scams, banking attacks, ransomware, and fake applications.

See Mikko Hypponen’s video on mobile security developments at the FSecure News Video Channel: Mobile Security Review September 2010
2009

Q4 2009 THREAT SUMMARY

2009’s Worm of the Year: Conficker

Major security developments in 2009 included Conficker, the most pervasive networking worm in years.

Conficker spread fast in computers using the Windows XP operating system which had not been patched with a late 2008 Microsoft update. Infection rates peaked at more than 12 million computers worldwide, causing major problems for companies, hospitals, airports and other public institutions around the world.

Unlike many previous worms that were released in the wild for personal fame, Conficker was designed to call home and create a botnet of infected computers — a potentially profitable commodity for the authors of the worm. The Conficker Working Group, composed of several anti-virus companies including F-Secure, prevented the worm from reporting home and establishing a powerful botnet. Nevertheless, millions of computers still remain infected with Conficker at the end of 2009. It is still a mystery who wrote the Conficker worm.

- Conficker Working Group

Windows 7

This year saw the launch of the Windows 7 operating system as a replacement for Windows Vista and Windows XP, which were both affected by major security concerns. Windows 7 shows promise as a leaner, more secure operating system, and also has an improved user security experience compared to Vista.

The focus on a better user experience and improved security is also one of the important trends in 2009, coinciding with the emergence of Netbooks.

- Windows 7

Social Networking

Facebook, MySpace, Linked-In, Twitter — social networking sites have been all the rage in 2009.

On December 1st, Facebook announced that it has 350 million user accounts.

Social Networks have also become a major target for online criminals who are misusing the high level of trust involved in communities of friends and contacts to carry out phishing attacks and spread links to malicious websites. Compromised social networking accounts provide the ideal cover for online criminals to develop new money-making activities. People are much more likely to click on a link that seems to be coming from a trusted friend or relative, than an attachment or a link in an e-mail from someone they don’t know.
Sites such as Facebook are now working to implement greater privacy controls and are attempting to simplify the user experience in an attempt to limit mis-use of trust.

- An Open Letter from Facebook Founder Mark Zuckerberg

**Mobile Security**

**Curse** – The “Curse of Silence” exploit against several current versions of Symbian S60 phones was demonstrated at the end of December, 2008. The exploit was very easy to utilize and a video demonstrating how to perform it was quickly distributed on the Web. The resulting effect of the exploit jams the victim’s SMS messaging.

Many network operators reacted quickly and started filtering their SMS traffic so as to prohibit the exploit message. Nokia later released a free recovery utility called “SMS Cleaner”. The exploit was, at best, a potential nuisance with little profit motive, and has not been widely reported to have been used.

**Latitude** – In February, Google Latitude was introduced for the very popular mobile Google Maps application. Google Maps has the ability to locate the phone based on GPS or cell tower positioning. The Latitude add-on allows users to “broadcast” their location to approved individuals using their Google account IDs. The service is easy to use and is a likely forecaster of things to come. Location based applications are in high demand and many other service providers seek to offer solutions with a Social Networking focus. The introduction of Latitude has alarmed some privacy advocates, but so far users have control over their own information.

**FlexiSpy** – A well known Spy Tool began offering an iPhone version during Q1, 2009. FlexiSpy for iPhone requires the phone be “jail broken”. The software’s features include hiding the interface icon as well as hiding the fact that the phone itself has been jail broken. FlexiSpy tracks the phone’s usage (SMS, e-mail, GPS, etc.) and sends the collected data to FlexiSpy’s website from where the phone’s owner, or another party, can view the logged reports.

**Sexy View** – Worm:SymbOS/Yxe.A was the most significant mobile malware case of Q1. The Yxe worm is the first discovered SMS worm, and is spread largely in China. Yxe is also the first malware that is compiled to run on Symbian S60 3rd Edition phones. The S60 3rd Edition platform is greatly protected by requiring applications to be Symbian Signed. In the case of Yxe, a leaked, valid certificate was used to sign the worm. Thus, very minimal user interaction was required for installation.

When Yxe infects a phone by sending an SMS message to the victim that promises a “sexy view” and celebrity gossip. The SMS links to a website that then prompts the victim to install the Yxe worm. If the victim does so, the worm uses the victim’s Contact list to spread itself further. The victim’s Contact will receive a message that appears to be coming from their friend, and so the worm continues to spread via Social Engineering. On installation, the worm reports the phone number back to the website from which it was downloaded.

SMS spam is a large problem in China with hundreds of billions of spam messages reported. This harvesting of phone numbers is very similar to the harvesting of e-mail addresses seen on PCs in 2002. Several network operators have been fined as China works to shut down access points that allow the sending of SMS spam.

**SEO Attacks and Rogue Scareware**

Much of the traffic for malicious websites is generated by search engine optimization (SEO) attacks where the attackers seed the search engines with popular search topics like the names of celebrities in the news. When people end up on these sites their computers are taken over.

The installation of rogue security products has been a favorite tactic used by criminals in 2009 and the case of File Fix Professional is a good example of this. In fact, the writers of this software do not push the product themselves and all the work is done by their botnet master affiliates. File Fix Pro encrypts some of the files in the My Documents folder and then confronts the user with what seems like a realistic error message, saying that Windows is recommending them to download a special tool to fix the files. When the user clicks on the message he gets a download of File Fix Pro which does “fix” the files – in order words decrypts them — if the user pays $49.99 for the product.
It is a clever social engineering trick because the user does not realize that the files have been taken hostage and the purchase of the rogue security product is a ransom payment to recover the files. The user may even recommend this seemingly useful software to others. The real software vendor is not actually doing anything illegal because it is the botnet holders who are encrypting people’s files and making them purchase the tool.

- YouTube Video: Tiger Woods SEO Attacks

**iPhone Worms**

In 2009 smartphones have become more popular and more powerful than ever. Smartphones are increasingly used for Internet based activity, including social media. Much of this has been driven by the iPhone and other touchscreen smartphones. The iPhone already has more than 10 percent share of the smartphone market and its popularity is inevitably attracting the attention of malware writers.

At the end of 2009 jailbroken iPhones became a target for the first profit-motivated malware on this platform. The speed of the malware evolution for jailbroken iPhones is a telling sign of the times. The news of a Dutch hacker exploiting a jailbroken iPhone vulnerability was quickly followed by an Australian hobbyist writing the Ikee worm that tried to “teach people a lesson” for not changing their default SSH password. The worm changed the wallpaper on infected iPhones to a picture of Rick Astley.

The first profit driven worm for jailbroken iPhones then emerged almost immediately in the Netherlands, which was designed to create a mobile botnet and gain access to online banking details. The worm tried to redirect the customers of a Dutch bank to a phishing site when they were trying to access their online bank from the iPhone.

We fully expect this kind of organized criminal activity involving smartphones to increase next year.

- First iPhone Worm Found
- Malicious iPhone Worm

**Cloud Security in 2009**

While criminals are busily churning out an unprecedented volume of malware, the security industry is also developing ever more sophisticated technologies to meet the threats. In 2009 “cloud computing” emerged as an important advance against the constantly evolving malware threats.

F-Secure has been among the pioneers of developing antivirus in the cloud. This means that all the information we have about all the possible malicious programs and all the possible good programs is now stored “in-the cloud”, i.e. in our data centers, with no limits to the amount of data.

The benefits of real-time access to this vast amount of information are substantial. For example, antivirus databases no longer eat up the memory and hard drive space on people’s computers. Protection in the cloud also means that when we tag a file as “bad”, all our customers around the world are protected against the threat in a matter of seconds.

- YouTube Video: Evolution of Security
Leaner Operating Systems

Broadband Internet access continues to increase but computing resources have not kept pace with software demands. As a result, lighter software and optimized performance have become a major focus for the software industry. Both Microsoft and Apple “realized that the pile-on-features model is unsustainable”, wrote David Pogue in the New York Times in August. “Both are releasing new versions of their operating systems that are unapologetically billed as cleaned-up, slimmed-down versions of what came before.”

Apple | The August release of Mac OSX 10.6 Snow Leopard showed the way with an installation that left 7GB more free space on the hard drive than its predecessor. It also included some antivirus functions against trojans.

Microsoft | Microsoft’s Windows 7 operating system, to be released in October, is also set to be leaner and more secure than its predecessor Windows Vista. Vista’s insistent user access control feature actually prompted many users to turn it off completely.

Google | Google is also developing its own Google Chrome OS which is an “open source, lightweight operating system that will initially be targeted at netbooks”, according to the official Google Blog.

More Secure Browsing

During this quarter, Firefox introduced its new private browsing feature and Firefox 3.5.3 introduced a notification for outdated versions of Adobe Flash Player.

According to the Mozilla Security Blog, “Old versions of plugins can cause crashes and other stability problems, and can also be a significant security risk.” Mozilla is also promising to work with other plugin vendors to provide similar checks for their products in the future.
Search Engine Competition Good for Security

At the end of July Microsoft and Yahoo signed a 10-year deal whereby the Yahoo search engine will be replaced by Bing in a bid to challenge Google’s dominance of the search-based advertising business. Microsoft hopes to compete with Google by offering new features in Bing, such as adult content filtering. Safe search results are now an important feature for consumers.

According to Tom Krazit from CNET, “Microsoft has tweaked the search filters on its new Bing search engine following criticism that its smart motion video feature allowed Web surfers to watch porn without visiting adult Web sites.”


Search Engine Optimization Attacks

The deaths of Michael Jackson, Farrah Fawcett and Patrick Swayze were quickly exploited by criminals through Search Engine Optimization (SEO) attacks, often pointing people to rogue antivirus products. The H1N1 flu has also been used as an emotional “hook” to lead Internet users to scam sites.

F-Secure’s web analysts saw the first wave of celebrity spam within hours of the reported death of movie star Patrick Swayze, which was followed by fake videos that came up in Google’s search results for his funeral. Clicking on the ‘video’ took the victim to a different website and another video, where a click downloaded a rogue AV.

• Labs Weblog: Swayze Spam
• Labs Weblog: More Swayze-Baited Traps

Social Media and Networks Under Attack

Facebook | As Facebook reached 300 million accounts in September, social networks and social media have continued to attract criminal and political interest.

Personal networking connections offer trusted authentication and accounts compromised by criminals have been used to abuse that powerful trust by linking to malicious sites. F-Secure reminds Internet users about the importance of strong passwords and that Facebook passwords should be different from the primary e-mail used to logon to Facebook.

Twitter | As Twitter has grown in popularity, it has been increasingly targeted by worms, spam and account hijacking.

In August it also emerged that Twitter has been used to direct botnets. According to a report in The Register, a security analyst accidentally stumbled across a Twitter account being used by botherders as a cheap and effective way of directing infected computers to websites where they can get further instructions. This appears to be the first time Twitter has been used as part of a botnet’s command and control structure.


Twitter accounts are also being used to push rogue AV products. All the tweets sent by these accounts are auto-generated, either by picking up keywords from Twitter trends or by repeating real tweets sent by humans. The links eventually lead to fake websites trying to scare you into purchasing a product you don’t need.

• Labs Weblog: Mass-Generating Fake Twitter Accounts for Profit

Politically Motivated DDoS Attacks

In August, the Twitter, Facebook, LiveJournal, Google Blogger and YouTube accounts of a Georgian blogger called Cyxymu were jammed by a politically motivated DDoS attack, as reported by Elinor Mills on CNET.

• http://news.cnet.com/8301-27080_3-10305200-245.html

Launching DDoS attacks against services such as Facebook is the equivalent of bombing a TV station because you don’t like one of the newscasters. The amount of collateral damage is huge. Millions Twitter, Livejournal and Facebook users experienced problems because of this attack. Whoever was behind this attack had significant bandwidth available.

• Labs Weblog: Silence Cyxymu

In another coordinated DDoS attack during Malaysia’s National Day on August 31st, hackers targeted a Malaysian-based web host and defaced over 100 websites, including those belonging to Malaysia’s national institutes, universities, media and business.

• Labs Weblog: Cyber Attacks on Malaysian Websites
Mobile Threats Make A Comeback

In the world of mobile phone security, this quarter witnessed the re-emergence of the SMS worm Yxe (aka Sexy View), now in the form of Sexy Space, which performs much like the original. The new variant Yxe.D is Symbian Signed with a certificate from a different company in China than the earlier version.

- Labs Weblog: Q & A on “Sexy View” SMS worm

The old ‘missed call scam’ is also making a comeback. This involves a call from an unknown international number which is immediately dropped when answered. When the curious person calls back to the number, he hears a ‘busy tone’ audio file, when in fact the call is being charged at a premium rate. F-Secure recommends a Google or WhoCallsMe search on any unusual numbers before calling back in order to avoid nasty surprises in the phone bill.

- Labs Weblog: Received an SMS message from a service number with link in it?
- Labs Weblog: Missed Call Scammers Are on the Move

Q2 2009 THREAT SUMMARY

Securing the Cyber Infrastructure

On May 29th, the President of the United States, Barack Obama, announced the creation of a new White House office to be led by a Cybersecurity Coordinator. The President began his speech by acknowledging the significance of virtual space.

President Obama:

“It’s long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world — cyberspace — is a world that we depend on every single day. It’s our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives.”

“So cyberspace is real. And so are the risks that come with it.”

Cyberspace is indeed real. Corporate information, personal data, network resources, and virtual commodities have been under constant attack for years. The law is only just beginning to catch up with the criminals and the reality of cyberspace. Most governments are still catching up to the reality of what needs to be protected.

President Obama also discussed the costs involved with eCrime:

“According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion.”

“[W]e’ve had to learn a whole new vocabulary just to stay ahead of the cyber criminals who would do us harm — spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion.”

Eight billion dollars is only a fraction of the global costs. While it is impressive that President Obama knows terms such as “malware and spoofing” it remains to be seen if the United States government is “ahead of the cyber criminals”. In the constant battle to protect consumer’s computers, just keeping up with newly emerging threats is a daily challenge.
On May 29th the Pentagon (United States Department of Defense) submitted their cyber defense plan to the White House. On June 23rd, Defense Secretary Robert M. Gates, announced the creation of Cybercom. The new organization will be to coordinate the day-to-day operation of military and Pentagon computer networks.

F-Secure Chief Research Officer Mikko Hyppönen contributed the following to the New York Times on the 29th:

“The creation of a White House office for cyberdefense is a step in the right direction. Serious cyberthreats definitely exist — I see evidence of global eCrime daily. Attack technologies are growing in complexity and strength, and civilian government efforts will definitely need to be prepared for an unauthorized breach. Maybe people shouldn’t be so dependent on Internet technologies, but the fact is that they are.

In his remarks today, President Obama emphasized the global nature of the Internet and the security threats involved. This means that protecting the Internet cannot be done without international cooperation. A White House office will also have to address some important political and military questions. For example, it’s typical that online attacks are rerouted through various countries to make it harder to locate the attacker’s origin. So it will be important to work with other countries in combating these attacks. Moreover, because laws differ from country to country, cooperative enforcement of laws will be crucial.

Cyberwarfare will certainly be asymmetrical warfare. The enemy uses compromised computers belonging to consumers for their dirty work. As a result, the United States needs to think carefully about whether it is willing and committed to counterattack malicious proxies inside the U.S. or inside allied nations. If an attacker launches a wide attack through thousands of infected home computers in Asia and Europe, the U.S. will need to think carefully about how it will protect itself and what attempts to deal with this situation are justified.

There are no easy answers. But the good news in all of this is that President Obama has now clearly and convincingly brought the importance of this matter into the spotlight. It’s about time.”

This new effort to secure America’s cyber infrastructure, if successful, could finally produce the global organization and cooperation needed to curb the growth of eCrime and other emerging cyber threats. It will be a daunting challenge to undertake.

- Obama’s speech: Securing Cyberspace

Green Dam Youth Escort

China has mandated that all computers sold in China, including imports, will need to be pre-installed with a software application called “Green Dam Youth Escort”. The requirement takes effect on July 1, 2009. The software’s intended purpose is to filter pornographic or violent material. Green Dam is designed for Microsoft Windows.

Response to Green Dam has been diverse. Privacy advocates state that Green Dam will act as spyware allowing for the monitoring of millions of Chinese computers. China has defended Green Dam against these claims stating that it is nothing more than filtering software.

In addition to censorship and monitoring concerns, there are claims that Green Dam infringes on copyrights belonging to Solid Oak Software Inc. The Wall Street Journal has reported that Solid Oak would file injunctions on U.S. manufacturers to stop them shipping machines with Green Dam.

On June 11th, researchers from the University of Michigan published a report called “Analysis of the Green Dam Censorware System”. The report demonstrated various security vulnerabilities in Green Dam Youth Escort that could allow “malicious sites to steal private data, send spam, or enlist the computer in a botnet”. At least one of the reported vulnerabilities was patched on June 13th.

The security implications of millions of computers running Green Dam cannot be ignored. Vulnerabilities in Green Dam could suddenly introduce a “low hanging fruit” to be exploited on July 1st.

- University of Michigan: http://www.cse.umich.edu/~jhalderm/pub/gd/
- Internet Storm Center: http://isc.sans.org/diary.html?storyid=6571&rss
June’s Iranian Presidential Election

The disputed Iranian presidential election of June 12, 2009 has led to large political protests and a wave of social networking media use. Twitter, Facebook, YouTube and other sites are being heavily utilized to distribute information and to circumvent government censorship. Facebook now offers a Persian language interface. Google Translate launched a “Persian ALPHA” tool. Twitter.com has been used to such an extent that the site was asked by the United States State Department to delay any network maintenance that might take the site offline.

This use of social media sites is a favorable development. Information wants to be free. On the other side of technology, there are also calls for Distributed Denial of Service (DDoS) attacks and targeted hacks against Iranian government servers.

More information from The World Tech Podcast:

- [http://64.71.145.108/pod/tech/WTPpodcast247.mp3](http://64.71.145.108/pod/tech/WTPpodcast247.mp3)

Some of these attacks are much like the Estonian DDoS attacks of two years ago. Those that could not take part in physical protests turned to cyberspace in order to take action. In Iran’s case, calls to DDoS government servers could create collateral damage to the networks being used by protestors. As cyberspace continues to integrate itself with our daily real world activities, we will see more political cyber attacks in the future. These attacks will not be carried out by military forces but rather by self-organized groups.

The Future

Technology does not discriminate between just and unjust causes. Hopefully the move to create a unified defense of the American cyber infrastructure will help generate the tools and organizations to maintain a global virtual world where information can flow freely and yet people will be defended against cyber attacks. As President Obama stated, cyberspace has become “woven into every aspect of our lives.” It must be protected.

Conficker Remains in the Wild

The threat landscape in the first quarter of 2009 was dominated by the Conficker worm, which has proved to be the most significant malware outbreak in recent years.

The Conficker Working Group, a multi-vendor effort, was a great success and is an excellent example of international cooperation within the Internet security industry. Conficker created a great deal of media interest especially around April 1, 2009, at the start of Q2, when the Conficker C variant was due to modify its behavior. Nothing significant really changed on or after April 1st. Variant C began “dialing home” larger numbers of potential domains, but it simply did not have the same number of vulnerable machines to infect. The success of Conficker B exposed the problems that needed to be addressed and variant C did not have enough of a foothold to expand the worm further.

The Conficker case once again demonstrated the emotional interest in outbreaks. Despite the subsequent loss of media interest, the Conficker worm is still out there and there are no answers as to what it was designed to do.
Millions of unique IP addresses are currently being logged by the Working Group’s sinkhole project.

- Post April 1st Conficker Q&A
- New Conficker Action

**Twitter Worms**

The popularity of social networking sites continues to grow in 2009 and sites such as twitter.com are transforming the way in which traditional media reports news and information.

A Twitter cross-site scripting worm and spam outbreak occurred in April during the Easter period. Large numbers of Twitter profiles were affected. The messages initially read “I love www.StalkDaily.com!”. The messages morphed several times to include “Wow... www.StalkDaily.com” and “Join www.StalkDaily.com everyone!”. Many people followed the links to stalkdaily.com, as they believe the messages to be genuine Tweets from their friends. A cross-site script on the site then caused new users to start to Tweet the same messages. Not surprisingly, the entire worm was a publicity stunt by stalkdaily.com by one Michael Mooney AKA mikeyy. There were several variants during April 12th and 13th and a follow up worm on April 17th that Mike Mooney also admitted to writing.

All these attacks were JavaScript-based. Turning off JavaScript, or limiting JavaScript to only trusted sites will mitigate such worms. As social networking tends to include a level of trust, consumers will increasingly need new technologies to protect them against an abuse of trust.

Twitter spam has become a challenging issue for the site. http://www.twitter.com/spam is Twitter’s official response to the issue.

**Search Engine Optimization**

While the mikeyy Twitter worms were largely an annoyance, the rapid outbreak and subsequent interest in “mikeyy” did not go unnoticed by cyber criminals. They quickly seized the opportunity and search engine results for “twitter worm” or “mikeyy” soon led people to sites hosting malware.

Malicious search results based on trending news stories are becoming commonplace. Knowing the reputation of sites yielded by search is becoming increasingly important.

**Targeted Attacks**

Targeted attacks continue unabated. Exploits in popular file types are used.

We’ve covered targeted attacks many times in the past and we’ve also covered PDF and vulnerabilities in Adobe Acrobat/ Adobe Reader being used to install malware. We decided to take a look at targeted attacks and see which file types were the most popular during 2008 and if that has changed at all during 2009.

In 2008 we identified approximately 1968 targeted attack files. The most popular file type was DOC, i.e. Microsoft Word representing 34.55 percent.
Targeted Attacks 2009
As of the middle of Q2, 2009 we have discovered 663 targeted attack files and the most popular file type is now PDF. Why the change? Primarily because there has been more vulnerabilities in Adobe Acrobat / Adobe Reader than in the Microsoft Office applications.

Update Cycle
Adobe recognizes that its popularity makes it a target. During Quarter 2, 2009, Adobe began a Quarterly Update Cycle.

This is a promising move as it helps to highlight the need to keep Adobe applications up-to-date. A quartely update schedule is more likely to be noticed by those that need to patch.

F-Secure Health Check
Statistics from our Health Check application show that during the month of May, 1 in 3 computers scanned were vulnerable to an Adobe Reader flaw reported in the month of February. It takes time for consumers to security update their systems. Adobe’s new quarterly schedule should help to raise attention to the issue.

Q1 2009 THREAT SUMMARY

The Conficker Worm
Quarter 1 of 2009 has been dominated by the Conficker network worm.

The sustained growth of malicious software (malware) during the last few years has been driven by crime. Theft – whether it is of personal information or of computing resources – is obviously more successful when it is silent and therefore the majority of today’s computer threats are designed to be stealthy. Network worms are relatively “noisy” in comparison to other threats, and they consume considerable amounts of bandwidth and other networking resources. Worms spread very aggressively and can be quite difficult to control. They are not generally the weapon of choice for today’s eCriminal.

Infamous worms of the past such as Blaster, CodeRed, Melissa, and Nimda were authored more by hobbyists than by professional criminals. The Conficker worm, also known as Downadup, is quite different and may perhaps be an indication of threats to come. Analysis of its code reveals that it has in fact been authored by today’s “professional” class of malware authors. While some of it is disorganized, the code is clearly not something that was written by an amateur. It is complex code and demonstrates a sophisticated understanding of the security systems that must be circumvented for the worm to spread. Conficker utilizes server-side polymorphism and Access Control List (ACL) modifications to make network disinfection particularly difficult. When Conficker infiltrates a Local Area Network (LAN), removal can be a very time consuming and possibly frustrating task.

Conficker exploits vulnerabilities (MS08-067) in the Windows Server service. (The Windows MS08-067 vulnerability was patched in an out-of-cycle update in October 2008.) It also does much more than this. Conficker uses autorun-worm techniques, spreading itself via removable USB thumb drives. Once it has infected a computer, it attempts to access Network Shares and also attempts to crack local account passwords. If Conficker compromises an administrator account, it uses the Windows Task Scheduler service to spread itself to non-infected computers. Those computers, having received the Scheduled Task from an “administrator” account, proceed to execute and run the worm without question.
Regarding the MS08-067 vulnerability, the Conficker worm needs to determine what language version of Windows it is attacking in order to exploit its victim. Earlier versions of Conficker were somewhat limited in their ability to make this distinction as they made a GeoIP location query via the Internet. The responding GeoIP database then converted the IP addresses, used by all computers, into a geographic location. When attacking a computer located in the USA, the worm attempts to exploit the English language version of Windows. If the IP address of the computer under attack is located in China, the worm then attempts to exploit the Chinese language version of Windows, and so on.

The providers of the GeoIP database being used by Conficker.A renamed and moved their database in order to deny Conficker the ability to locate its victims. Conficker.B responded to this change by integrating a small GeoIP database within its own code. Other small improvements in the worm’s code lead to significant results.

The B variant of the Conficker worm spread rapidly during the months of January and February, infecting millions of computers worldwide. Countries such as China, Brazil, Russia, and India topped the list of infection counts. During the same period, there were many reported instances of European networks that were compromised. The out-of-band Windows MS08-067 vulnerability October update shortly before December’s holidays helped contribute to a lack of testing resources, and many organizations failed to implement the necessary updates by the time variant B became a serious threat.

With a swiftly growing number of infections and the potential threat of the worm “calling home” to its authors, a number of companies within the antivirus industry, including F-Secure, banded together to form the “Conficker Working Group”. The group has successfully worked together with Internet Domain Registrars from many countries to block the domain address to which Conficker attempts to communicate. Blocking the worm’s attempts to call home limits the worm’s authors from using the infected computers for criminal purposes. This successful monitoring of the worm continues against the current variant, Conficker.C, which greatly increased the number of domains to which it attempts to call home.

More information about Conficker is available from our Security Labs Blog:

- MS08-067 Worms
- MS08-067 Worm, Downadup/Conficker
- How Big is Downadup? Very Big
- Downadup, Good News / Bad News
- Conficker Q&A
- Post April 1st Conficker Q&A

Social Networking

Facebook has become the leading Social Networking website, growing to 175 million accounts during Q1 2009. Estimates project Facebook reaching 300 million accounts by the end of 2009. As its user audience grows, Facebook has become a more attractive target to eCriminals and fraudsters, leading to the development of Facebook specific threats, such as:

Facebook 419 scams – Numerous incidences of 419 style “advance fee frauds” are being reported. Password compromised accounts, resulting either from phishing or password stealing malware, are being used to scam social networking friends of the victim. Typically the compromised account sends out a request for help and assistance, claiming that money is needed. The victim is supposedly stuck abroad without any cash. There have been a number of confirmed reports in which friends have wired money to the scammers.

Error Check System – Some unscrupulous application developers using Facebook’s API have attempted to trick users into installing their applications, such as “Error Check System”. When installed, “Error Check System” sent messages to the victim’s friends. The notification message prompted Facebook users to resolve an “Error” by clicking the notification link. Spam is the likely goal of the people behind the application, though spreading links to malicious external sites is another possibility. Facebook’s recent layout changes appear to have limited this issue.

Group defacements – Facebook began to allow the changing of Group names during the month of March. There are already reports of hijacked and defaced groups. Fox News reported in early April that a Group centered on Judaism was defaced with a name referencing Adolf Hitler. There are many other claims of religious focus Groups being renamed. As websites are defaced, hackers also attempt to steal the passwords of Group administrators in order to cause offense.
Other Social Networking sites are emerging and growing rapidly, such as Twitter. These sites are contributing to a rapid sharing of links and other information. What remains to be seen is whether all of the links being shared can be trusted, or if criminals will attempt to inject malicious links into such systems.

Data Breaches
Identity theft and credit card fraud issues continue with two notable database breaches that occurred during Q1.

Monster UK (monster.co.uk) was compromised as a result of malware targeting the corporate recruiters. From these corporate accounts, the malware was able to access the applications of those submitting their CVs/resumes. Tens of thousands of individuals had their personal data scraped from the job search site.

In January, Heartland Payment Systems Inc. reported a massive data breach. Heartland processes payments for a large number of U.S. retailers, thus potentially compromising an enormous number of accounts.

Mobile Security
Curse – The “Curse of Silence” exploit against several current versions of Symbian S60 phones was demonstrated at the end of December, 2008. The exploit was very easy to utilize and a video demonstrating how to perform it was quickly distributed on the Web. The resulting effect of the exploit jams the victim’s SMS messaging.

Many network operators reacted quickly and started filtering their SMS traffic so as to prohibit the exploit message. Nokia later released a free recovery utility called “SMS Cleaner”. The exploit was, at best, a potential nuisance with little profit motive, and has not been widely reported to have been used.

Latitude – In February, Google Latitude was introduced for the very popular mobile Google Maps application. Google Maps has the ability to locate the phone based on GPS or cell tower positioning. The Latitude add-on allows users to “broadcast” their location to approved individuals using their Google account IDs. The service is easy to use and is a likely forecaster of things to come. Location based applications are in high demand and many other service providers seek to offer solutions with a Social Networking focus. The introduction of Latitude has alarmed some privacy advocates, but so far users have control over their own information.

FlexiSpy – A well known Spy Tool began offering an iPhone version during Q1, 2009. FlexiSpy for iPhone requires the phone be “jail broken”. The software’s features include hiding the interface icon as well as hiding the fact that the phone itself has been jail broken. FlexiSpy tracks the phone’s usage (SMS, e-mail, GPS, etc.) and sends the collected data to FlexiSpy’s website from where the phone’s owner, or another party, can view the logged reports.

Sexy View – Worm:SymbOS/Yxe.A was the most significant mobile malware case of Q1. The Yxe worm is the first discovered SMS worm, and is spread largely in China.

Yxe is also the first malware that is compiled to run on Symbian S60 3rd Edition phones. The S60 3rd Edition platform is greatly protected by requiring applications to be Symbian Signed. In the case of Yxe, a leaked, valid certificate was used to sign the worm. Thus, very minimal user interaction was required for installation.

When Yxe infects a phone by sending an SMS message to the victim that promises a “sexy view” and celebrity gossip. The SMS links to a website that then prompts the victim to install the Yxe worm. If the victim does so, the worm uses the victim’s Contact list to spread itself further. The victim’s Contact will receive a message that appears to be coming from their friend, and so the worm continues to spread via Social Engineering. On installation, the worm reports the phone number back to the website from which it was downloaded.

SMS spam is a large problem in China with hundreds of billions of spam messages reported. This harvesting of phone numbers is very similar to the harvesting of e-mail addresses seen on PCs in 2002. Several network operators have been fined as China works to shut down access points that allow the sending of SMS spam.
Mac OS X

In January, “cracked”, yet fully working copies, of iWork 2009 were distributed on popular file sharing websites. Those seeking a “free” version of iWork 2009 also received a nasty surprise included with the installation package. Downloading and installing the pirated copy of the software installed a backdoor application called iWorkServ.A.

Installation of software on Mac OSX requires the user to supply his administrative password. Any malicious software must therefore provide some kind of social engineering pretext to trick the user into entering that password. In this case however, the user is already prepared to enter the password in order to install the “free” software. Additionally, the installation does provide functional software as promised, giving the victim very little clue that his system has been compromised.

A version of Adobe Photoshop for Mac was also used as bait by this malware gang.

There is increasing evidence of malware gangs that are interested in and prefer to target Macs.

- Backdoor:OSX/iWorkServ.A
Q4 2008 THREAT SUMMARY

Another record breaking year in the growth of malicious software

- Growth in amounts of malicious software
- Growth in infections
- Growth in the number of botnets
- Growth in criminal profits
- Call for growth in punishment

Detection numbers have tripled

The silent acceleration of malicious software (malware) continues and 2008 has been another groundbreaking year. The year 2007 doubled our overall detection count and that count has now tripled during the year 2008. An additional one million database signatures were added during the year, bringing our total number of signature based detections to approximately 1.5 million.

Historical Detection Count

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Total Number of Detections</th>
<th>Detection Signatures Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>1987 - 2006</td>
<td>250,000</td>
<td>250,000</td>
</tr>
<tr>
<td>2007</td>
<td>500,000</td>
<td>250,000</td>
</tr>
<tr>
<td>2008</td>
<td>1,500,000</td>
<td>1,000,000</td>
</tr>
</tbody>
</table>

Explosive sample growth

Coupled with the rapid growth of signature detections has been a corresponding growth in our sample collections. Adding signature based malware detections to our databases first requires that copies of the malicious applications be collected for analysis. We have seen vast amounts of suspicious files discovered during 2008.

Our current malware sample management system contained many millions of suspicious applications at the end of last year. During this
year, our unique malicious sample totals increased by almost 350 percent. Tens of millions of suspicious samples have been imported, scanned, indexed, classified and categorized by our Response Lab systems. There were well over ten million unique samples collected this year, and there were tens of millions more redundant samples that our systems were required to handle. Our Lab Development team has been very busy maintaining and enhancing the system infrastructure to handle the load. This raw number of incoming samples shows no signs of decreasing anytime soon.

**Test file expansion**

Such rapid growth of malicious software has demanded an expansion of our database test collection files. Releasing quality databases to our customers is one of our most important responsibilities and we are today testing with five times the amount of files compared to one year ago. This trend will definitely continue into 2009 and we fully expect to expand our test collection by another 500 percent next year.

**White list collections**

With the introduction of DeepGuard 2.0 into our product line, our non-malicious (clean) file collection is an increasing priority. DeepGuard 2.0 moves part of our security technologies into our cloud based Real-time Protection Network.

Network lookups now allow our DeepGuard behavioral engine to query for the reputation of applications that are being launched on our customers’ computers. Good applications are allowed to launch and malicious applications are blocked. Unknown applications undergo behavioral analysis. This technology has altered our processes and our Security Labs are now collecting legitimate files as fast as they are collecting malicious files. Our aim is to expand our clean file collections by ten times the current amount during 2009. Having a huge set of known good applications will allow our behavioral engine heuristics to act more aggressively against the ever increasing amounts of unknown malicious threats.

**Exponential growth curves**

All of our systems, collections, and databases experienced exponential growth during 2008 and we fully expect this trend to continue into next year.

**Malware 2008**

**Busy Botnets**

2008 saw increasing amounts of botnet activity around the world. Botnets are a remotely controlled “robot network” of infected computers, also known as zombies. Botnets are very typically made up of infected consumer computers. The infected zombie computers very often do not display any local symptoms, except possibly lower performance. Just how many bots are there in existence? There are no exact measurements but the potential numbers are staggering.

Worldwide, there are now approximately 1.2 billion computers in use. One of the largest ISPs in Finland estimates that one percent of its customer base exhibits some bot-like behavior. Finland ranks among the safest countries in the world with very low malware infection rates. Finnish ISPs actively police their networks and there are strong regulatory controls provided to authorities. One percent is an extremely low figure compared to worldwide infection rates. Applying just a one percent bot infection rate to 1.2 billion computers yields 12 million potential bots in active operation. This is a very
conservative estimate and we would not be at all surprised to discover that the actual figure is many times higher.

It is important to note that not all active bots actually have botmasters (a controlling remote server telling the bot what to do). Many of the world’s bots are orphans without a master, their command and control servers having been discovered, abused, and taken out of service. However, even without a master, the bots continue to exist and they do still attempt to call home. They may also attempt to continuously carry out their last assignment and to defend themselves. These orphaned bots are a plague of wasted computing resources and bandwidth.

As for the bots that are still under criminal control - they are a dangerous and growing threat to consumers and businesses everywhere.

During 2008 our Response Lab conducted a small research project focusing on approximately 60 orphaned botnets. Listening to the communication attempts of these bots yielded over 200,000 unique IP addresses within a 24 hour period. We know that 200,000 is just the tip of the iceberg and are planning for more extensive research and anti-bot services during 2009.

**Recent outbreaks**

Three London area hospitals experienced a worm outbreak this November.

The Register (November 19, 2008):

Computer systems at three major London hospitals are largely back online on Friday morning, three days after a major computer virus outbreak forced staff to disconnect the network.

IT systems at St Bartholomew’s (Barts), the Royal London Hospital in Whitechapel and the London Chest Hospital in Bethnal Green were taken down on Tuesday following infection by the Mytob worm. The three hospitals make up the Barts and the London NHS Trust.

The US Department of Defense has banned USB drives.

Wired (November 20, 2008):

The decision to terminate use of removable rewritable media is a key component in the strategy to defend against attacks and establish a baseline for information system protection. Memory sticks, thumb drives and camera flash memory cards have given the adversary the capability to exploit our poor personal practices and have provided an avenue of attack,” the e-mail continues. “Malicious software (malware) programmed to embed itself in memory devices has entered our systems. Only through a layered defense of training, technology, procedures and personal recognizance, can we regain the high ground.
Malware even made its way into space during 2008.

BBC News (August 27, 2008):

NASA has confirmed that laptops carried to the ISS in July were infected with a virus known as Gammima.AG.

**Scareware scams on the rise**

Rogue security software scams have grown to become a major consumer issue during 2008. Fake security products using strong-arm fear tactics have been produced in bulk. New websites to promote their installation and purchase appear every day.

Scareware affiliates, who are paid a large percentage of the sale for each purchase, use very nasty techniques to ensure installation. Rootkit techniques are common and variants will attack and uninstall rival affiliates.

The unfortunate consumers who enter into the trap can spend hours trying to remove the rogues. Many surrender and attempt to resolve the issue by making the purchase.

The situation has created enough concern that Microsoft and Washington State are suing scareware pushers in the United States.

Washington Post (September 29, 2008):

Microsoft Corp. and the state of Washington this week filed lawsuits against a slew of “scareware” purveyors, scam artists who use fake security alerts to frighten consumers into paying for worthless computer security software.

“We’re absolutely certain that consumers across the country have been deeply affected by this.”

We know of consumers worldwide that have been affected.
SQL injection attacks targeted Chinese language sites

Our mid-year security summary noted the use of SQL injection attacks to inject sites with malicious code. As hosts to the 2008 Olympics, China saw a surge of such attacks focused on Chinese language sites.

News from the Lab (August 8, 2008):

With all the attention on China these days, especially in conjunction with the Beijing 2008 Olympics Games, and with “China” being one of the more popular search engine keywords at the moment, it makes sense for malware writers to focus their attention on the Chinese web - and we’ve been seeing some interesting examples of SQL injection attacks specifically targeting websites designed for a Chinese audience, whether from the mainland or overseas.

Like most SQL injection attacks, these attacks begin with a compromising script being injected into a legitimate site, compromising it and redirecting its users to a malicious website. This website then takes advantage of the vulnerabilities available on the user’s computer to download and execute malicious programs.

Malware is driven by profit and we can clearly see that criminals will focus their efforts on a new audience if it develops enough of a market presence.

Attacks continue against high profile targets

Our previous security summaries have noted targeted attacks. During the recent presidential election in the United States the computer systems of both candidates were hit by targeted attacks.

Newsweek (November 5, 2008)

At the Obama headquarters in midsummer, technology experts detected what they initially thought was a computer virus [...]. But by the next day, both the FBI and the Secret Service came to the campaign with an ominous warning: “You have a problem way bigger than what you understand,” an agent told Obama’s team. “You have been compromised, and a serious amount of files have been loaded off your system.

On the morning after Obama’s win, there were massive amounts of malicious e-mails using the election and fictitious videos of the President-elect as bait to tempt people to click on a link and install malware.

Such targeted attacks are not new and are expected to continue to be carried out in 2009.

Crime and punishment

Cyber Victories

Our earlier security summaries have highlighted the challenges involved in bringing cyber criminals to justice. The second half of this year has seen some moderate successes against the business of online crime.

EstDomains

For several years the Estonian domain registrar EstDomains was the largest registrar used by online criminals for their domain name registration needs. In October, the Internet Corporation for Assigned Names and Numbers (ICANN) pulled the plug on EstDomains, and started removing EstDomains from the list of ICANN-accredited registrars.
We first encountered EstDomains in 2005, while we were investigating the infamous WMF vulnerability. Initially the main site distributing malicious WMF files, unionseek.com, was registered via this, then new, Estonian registrar.

Since 2005, tens of thousands of malicious domains have been registered with EstDomains. They included drive-by-download sites, botnet command-and-control servers, spammed domains and so on. Many of the recent fake antivirus tools as well as rogue codecs have been running via EstDomains.

The EstDomains operation was run by Mr. Vladimir Tšaštšin, from the EstDomains office in downtown Tartu. Vladimir Tatin was sentenced earlier this year to six months of jail for credit card fraud, money laundering, and related charges.

This conviction allowed ICANN to exercise its authority and start the termination process. There were some small interruptions to that process, but at this point EstDomains is no longer accredited. Certainly there are other registrars that will be willing to take on dubious domains, but we at least will not miss EstDomains.

Rogue service providers

In September the criminal enabling ISP Atrivo / Intercage had its upstream service access terminated. The result was a noticeable drop in worldwide spam output.

The take down of Atrivo helped to end the life of the infamous Storm worm botnet which lost a few key components during the termination. Storm was a very successful botnet which utilized an advanced structure and innovative technologies.

A reporter from the Washington Post, Brian Krebs, almost singlehandedly got rid of 2/3 of e-mail spam on the Internet in November. The San Jose (California, USA) based Internet service provider McColo hosted the Command and Control (C&C) servers for several large botnets that were used to send massive amount of spam to millions of users around the world. Mr. Krebs gathered evidence against McColo and convinced the companies providing bandwidth to the ISP to shut down the connections. In a matter of hours the amount of spam being distributed worldwide dropped by 66 percent.

However, the botnet owners were able to update the network and change the location of the command and control servers to an ISP in Russia. The amount of spam being sent remained at a low level for two weeks but by the end of November they were back up to 70 percent of the original level.

As noted earlier, killing the botmaster doesn’t disinfect the bot. The cyber criminals involved are now attempting to reestablish control or to build new botnets. Spam volumes will eventually return to previous levels.

Nevertheless, anything that disrupts the operations of cyber criminals and reduces their profits is a win. More actions like this should be taken. Investigative journalism armed with information from security experts pushed McColo’s upstream providers to kill its connections. F-Secure believes that it is time for a professional, authoritative, investigative group to be established.

Dark Market

In an example of what aggressive law enforcement action can accomplish, the FBI announced in October the conclusion of a two-year undercover operation targeting an online carding forum (a criminal service dealing with e.g. stolen credit card information), resulting in 56 arrests. The operation was conducted in cooperation with law enforcement agencies around the world. The sting also resulted in over USD 70 million in fraud being prevented.

FBI (October 16, 2008):

The FBI, in conjunction with many partners in international law enforcement, today announced the conclusion of a two-year undercover operation targeting members of the online “carding” forum known as Dark Market.

Cyber criminals using this forum represented a virtual transnational criminal network spanning numerous countries who were involved with the buying and selling of stolen financial information including credit card data, login credentials (user names and passwords), as well as equipment used in carrying out certain financial crimes. At its peak the Dark Market website had over 2,500 registered members.

With the take down of Dark Market, there have been numerous arrests, including many in the U.K.

With all of the growth in malware and in online crime, we would like to see growth in the number of arrests and jail sentences for cyber criminals during 2009.
Predictions

Crimeware
There will be continued growth in the quantity of online threats with a continued incremental evolution of the malware involved. Crimeware is firmly established. Online crime is a business and we do not predict radical shifts in tactics. There are likely to be hundreds of millions to billions of dollars lost each year to crime. A good percentage of that is involved with online transactions in one form or another. With such a record of successful growth, we don’t expect the formula to change very much.

Smartphones
The number of smartphones globally has grown from approximately 300 million in 2007 to approximately 475 million by end of 2008. These figures are expected to continue growing, meaning there is an increasing number of people with both personal and business related information such as contacts, photos or e-mails, stored on their smartphones. Even thought there has not been a significant increase in malware for mobile phones, it is important to secure the data in case the smartphone is lost or stolen with anti-theft solutions.

Apple
We have seen a small but increasing number of Mac OSX trojans during 2008. The latest, Trojan-Downloader:OSX/Jahlev.A, includes functionality to install future malware components.

We predict that we’ll see additional Mac trojans during 2009, and that we will also see new security solutions and vendors entering the Mac OSX market.

Botnets
Botnets will grow and will adopt new technologies such as the Peer to Peer (P2P) functions exhibited by the Storm worm. Recent successes against rogue ISPs will prompt malware authors to develop disaster recovery plans.

Additional successes in cutting off command and control servers could incite an online territory war as online gangs compete for existing resources.

Punishment
We predict that authorities will recognize the value in fighting online crime and the need will increase for the establishment of an international agency tasked with enforcement knowledge or investigative assistance. The call for the establishment of “Internetpol” by Mikko Hypponen, Chief Research Officer at F-Secure, has been received with great interest internationally.
Q3 2008 THREAT SUMMARY

Challenge of bringing cyber criminals to justice

• As courts and law enforcement struggle to stem the mounting Internet crime wave,
• F-Secure’s Chief Research Officer Mikko Hypponen calls for the establishment of “Internetpol” to bring online criminals to justice
• Phishers exploiting international banking crisis
• US presidential election spam
• Return of the malicious attachment

During the last quarter there have been several interesting legal cases involving Internet crime, which highlight the challenges of bringing cyber criminals to justice.

In the United States, a prolific spammer who had received a long prison sentence saw his conviction overturned by the Virginia Supreme Court in September. Jeremy Jaynes was the first person to be tried and sentenced under an anti-spam law enacted in 2003. Following an appeal, Virginia Supreme Court decided that the state Anti-Spam Law violated the First Amendment to the United States Constitution concerning the right to free and anonymous speech.

The Court documents show that there was no question about Jaynes’ guilt. He used several computers, routers and servers to send over 10,000 e-mails within a 24-hour period to subscribers of America Online, Inc. (AOL) on three separate occasions. He intentionally falsified the header information and sender domain names before transmitting the e-mails.

While searching Jaynes’ home, police discovered CDs containing over 176 million full e-mail addresses and 1.3 billion e-mail user names. They also confiscated storage discs which contained private account information for millions of AOL subscribers. The AOL user information had been stolen from AOL by a former employee and was in Jaynes’ possession.

Just six months ago, the same court upheld the Anti-Spam Law and determined that there is no First Amendment right to spam. The latest reversal has provoked many questions from Internet security commentators.

Teenage Kiwi botmaster has bright future

In New Zealand, Owen Thor Walker, 18, known online as “AKILL” and dubbed as the “Kiwi botmaster king” in the international media, escaped a jail sentence in July despite pleading guilty to developing banking trojans that earned an estimated USD 15.4 million to a criminal gang.

The court ordered the teenager to pay damages and costs of about USD 10,800, with the judge describing him as a young man with a “potentially outstanding future” after he cooperated with the police. The judge stated that Walker, who suffers from Asperger’s Syndrome, a mild form of autism, was hacking from curiosity rather than criminal intent.

Walker was arrested after an 18 month investigation by New Zealand, Dutch and American authorities. According to TVNZ, Walker collaborated with an American student to infect 1.3 million computers, costing the victims around USD 20 million. Walker is now reportedly being wooed by major computer companies overseas. Local police also said that Walker’s “talents” could come in handy.

Lawsuits against scareware merchants

The Attorney General’s Office in Washington, United States, and Microsoft recently announced that they are filing new lawsuits targeting scareware purveyors. One of the cases is against James Reed McCreary IV, who is accused with sending incessant pop-ups resembling system warnings to consumers’ personal computers. The messages read “CRITICAL ERROR MESSAGE! - REGISTRY DAMAGED AND CORRUPTED,” and instructed users to visit a Web site to download Registry Cleaner XP.

“Consumers who visited the Web site were offered a free scan to check their computer - but the program found ‘critical’ errors every time,” said Senior Counsel Paula Selis, who leads the Attorney General’s Consumer Protection High-Tech Unit. “Users were then told to pay USD 39.95 to repair these dubious problems.” Microsoft has said that 50 percent of its customer support calls related to computer crashes can be blamed on spyware.

F-Secure notes that Registry Cleaner XP is just one of the increasing number of rogue security applications which also include Antivirus 2009, Malwarecore, WinDefender, WinSpywareProtect and XPDefender.
Call for establishment of “Internetpol”

While applauding efforts by the courts and police forces of different countries in challenging cyber crime, Mikko Hypponen, F-Secure’s Chief Research Officer, believes that there should be an international agency with the enforcement power to get a grip on the organized online crime.

“The Internet has no borders and online crime is almost always international, yet local police authorities often have limited resources for investigations. Even if the locations of online criminals are discovered, the investigations rarely uncover the full scope of the crime. The victims, police, prosecutors and judges cannot see the full picture and therefore don’t know the true costs of the crime,” says Hypponen.

“Antivirus and security companies are not law enforcement, nor should they be. They are protecting their customers’ computers but little can be done directly by non-governmental organizations to fight the criminals at the heart of the matter. We should consider the creation of an online version of Interpol - ‘Internetpol’ - that is specifically tasked with targeting and investigating the top of the crimeware food chain,” says Hypponen.

Hypponen recognizes that such an organization would clearly face a number of legal and other challenges. For example, malicious code is often created from countries where it is not illegal or not prosecuted. “But if we do not act now to fight the source of crimeware, it will continue to grow stronger and threatens to destroy the current model of Internet business, banking and commerce,” he says.

US Federal Trade Commission warns about “Phisher-man’s special”

As the international banking crisis shakes up the world economy, leaving consumer’s confused as to which bank might be holding their savings account or mortgage this week, phishers are taking advantage of the situation to obtain personal information such as bank account details or credit card numbers.

The US Federal Trade Commission issued an alert last week urging Internet users to be on guard against e-mails that look as if they come from a financial institution that has recently acquired a consumer’s bank, mortgage lender or savings and loan association.

"Currently there only seem to be e-mails related to Wachovia Corporation’s sale to Citibank being used as bait. The phish is attempting to get the recipient to download a new ‘certificate’ from a Wachovia phishing site. However, instead of collecting information, this attack will also install a banking Trojan,” explains F-Secure Security Advisor Sean Sullivan.

Presidential election spam

As the presidential election in the United States nears its climax, criminals are busy devising sensational headlines related to the candidates in order to persuade people to click on spam e-mails. A recent spam run has already set the tone by claiming to reveal a sex scandal involving Senator Barack Obama, the Democratic candidate. The e-mail with the fake news contains an attachment that links to a pornographic video.

In order to conceal the primary intent of the e-mail - which is to infect computers with a trojan that collects information about bank transactions - the video starts playing when the malicious file is downloaded and executed. Consequently, every time Internet Explorer is launched and the user connects to certain banking sites, especially well-known banks in Germany, the trojan collects the information and posts it to the website of a fictional “Medved Hotel” in Finland. The layout of the website looks convincing to unsuspecting users because it has been stolen from a real Finnish hotel.

We expect much more spam with a presidential election theme in the run-up to polling day.
Return of the malicious attachment

During the third quarter of 2008 we saw a sharp increase in malware being delivered as e-mail attachments. This was surprising as malicious attachments in e-mails are usually not successful in reaching the recipient because they are automatically removed by the Internet Service Provider or by the e-mail client. As a result, malware authors stopped using this approach and moved on to using links in e-mails or automatic downloads via exploits from websites.

The recent attachments were inside an archive, typically a ZIP file which unfortunately isn’t filtered by most security solutions. Some of the archives even required a password, making it more difficult for anti-virus solutions to scan them.

The different themes that were used to trick the user into running the file included bills or receipts from a variety of companies like JetBlue and UPS and greeting cards. This approach is not unlike phishing scams where the risk of losing money is used to trick the user into running the file and getting infected.

Q2 2008 THREAT SUMMARY

Silent Growth of Malware Accelerates

The number of malware detections seen during the first half of 2008 has exceeded the growth rate experienced during 2007. We ended 2007 with 500,000 total detections. By the end of June 2008 this number is around 900,000. The growth rate has never been faster.

This recent explosion of malware doesn’t necessarily represent new types of threats. It is largely the packing, encryption, and obfuscation of existing families of trojans, backdoors, exploits, and other threats. What the increasing use of self-defense technologies in malware represents is the ever growing professionalism within the crime-ware community.

Criminals are adapting and utilizing enterprise level systems and code within their operations. The complexity and quality of their IT infrastructure and systems continues to increase, providing them with the power to silently flood the Internet with their menace.

Targeted Attacks

Trend towards More Targeted Attacks

The first half of 2008 has witnessed a growing number of targeted malware attacks on individuals, companies, and organizations.

In a targeted malware attack, the attacker profiles his victim and sends an e-mail using the recipient’s name, title, and perhaps references to his job function. The message’s content is typically something that the recipient would expect to receive via e-mail.
The content will seem like an ordinary Word or PDF document, or other common file type, but infects the recipient’s computer with a hidden payload. Often this is a backdoor that gives the attacker access to the information stored on the computer without any outward sign of infection.

As an example of an attack during the month of May, high-level executives were targeted with an e-mail mentioning a supposed complaint made to the Better Business Bureau (USA) about their company. By researching their chosen targets, the criminals were able to use real company and individual names. This made the approach much more credible to the recipients, who were then more likely to follow the on-screen instructions and put their computer at risk. The technique used a high degree of social engineering and specialized malware to infect the would-be victims.

In this case the e-mail message linked to www.us-bbb.com in order to download the “complaint”. The real Better Business Bureau is located at www.us.bbb.org. The supposed complaint allegedly required an Adobe Acrobat update to be read and the download claimed to require Internet Explorer and an ActiveX component. Once the ActiveX application was installed, a backdoor opened the system and provided access to confidential information.

In this case the e-mail message linked to www.us-bbb.com in order to download the “complaint”. The real Better Business Bureau is located at www.us.bbb.org. The supposed complaint allegedly required an Adobe Acrobat update to be read and the download claimed to require Internet Explorer and an ActiveX component. Once the ActiveX application was installed, a backdoor opened the system and provided access to confidential information.

Targeted Political Motives

Targeted malware attacks are also being used for political and military motives. During the recent clashes between Tibetans and the Chinese military, the battles on the streets were accompanied by political espionage on the Internet. Human rights groups, pro-Tibet organizations and individuals supporting the freedom of Tibet were attacked with a carefully targeted and technically advanced e-mail campaign that attempted to infect their computers in order to spy on their actions.

The content of the e-mails was crafted from the real announcements and messages of the pro-Tibet groups. Some e-mails purported to include pictures of Tibetans shot by the Chinese army. The e-mails were forged to look like they were coming from trusted persons or organizations, making it more likely that they would be opened by the recipients. They were sent to mailing lists, private forums and directly to persons working inside pro-Tibet groups. Some individuals received targeted attacks several times a month. The attacks used many “trusted” file types including DOC, XLS, PPT, PDF, and CHM.

For example, one document seemed as if it was sent by the Unrepresented Nations and Peoples Organization (UNPO) but the e-mail headers were forged and the e-mail was coming from somewhere else altogether. The e-mail issued a statement of solidarity for the people of Tibet and contained a modified version of a PDF-encoded vulnerability to exploit Adobe Acrobat. If the recipients opened the document, they were infected with a keylogger that collected and sent everything typed on the affected machine to a server running at a DNS-bouncer system. The exploit inside the PDF file was even crafted to evade detection by most antivirus products at the time.

We have seen some of the same malware applications used for both political and corporate attacks. This supports the conclusion that those with the political motives to attack free Tibet groups are also involved in attacks on businesses, notably businesses within the defense industry.

Defense

Guarding against such personalized attacks requires great individual vigilance and a strong security culture within an organization. Most security education is designed to inform people of online threats directed at millions of Internet users and is not nearly as effective in protecting individuals who have been specifically targeted.

F-Secure has developed proactive DeepGuard technology to fight attacks such as these targeted attacks. DeepGuard is shipping in all of F-Secure’s current workstation products.

Spear Phishing

The same tools and information that are helping criminals to collect data on individuals is also being used to collect profiles on groups. Phishing a particular group is known as spear phishing. The attackers only send phishing bait to those that match the data profile. A spear phishing attempt may even attempt to address the recipient by name by analyzing the e-mail address. For example, “john.smith @ jsmithfamily.com” becomes “Dear John” rather than “Dear Customer” as is used by most generic phishing.

Increasingly Sophisticated Malware

Not all of the malware seen during the first half of the year were repackage known threats. There were also some notable developments.
**Mebroot**

The flexibility of current malware attacks demonstrates that some criminals have considerable resources and expertise at hand. Creating advanced backend systems requires serious time and investment.

This year we have seen a very advanced Master Boot Record (MBR) rootkit, known as “Mebroot”, which is probably the stealthiest malware produced so far.

It keeps the amount of system modifications to a minimum and is very challenging to detect from within the infected system. The F-Secure team that developed our defense against Mebroot estimates that it took several months of development.

**Storm**

The Storm worm has been dubbed malware 2.0 for its sophisticated sense of timing and social engineering methods, as well as the complexity of its design. It utilizes peer-to-peer technologies, creating a decentralized botnet that fights back against detection.

Storm has played a major role in the evolution of the online threat towards the current trend of drive by downloads.

Microsoft Corporation reported in April that its Malicious Software Removal Tool (MSRT) has been very successful in disinfecting Storm’s bots, remotely controlled components in the criminal Storm gang’s network of infected computers.

Nevertheless, there has recently been an upswing in e-mails being sent out attempting to trick people into visiting Storm websites. The Storm botnet certainly isn’t as big as it used to be, but it’s unlikely that we have seen the last of it.

**Criminal Injections**

During the first half of 2008 we’ve seen online criminals using powerful tools to locate websites using SQL servers hosting insecure pages. The SQL servers themselves are not insecure; the tools seek out web forms that allow unchecked/unfiltered malicious input. Using the vulnerable forms these tools automatically injected the site with malicious code.

More and more web sites are using database back-ends to make them faster and more dynamic. From a security perspective, this means that it’s crucial to verify what information gets stored in or requested from those databases — especially if a web site allows users to upload content themselves which happens all the time in discussion forums, blogs, feedback forms, and so on. Unless that data is sanitized before it gets saved, it’s not possible to control what the web site will show to the users. SQL injection is all about exploiting weaknesses in these controls.

Such mass SQL injection attacks are increasing in number and we’re seeing more domains being injected and used to host the attack files. Tens of thousands of hacked sites are actively affected. Millions have been hacked. We believe that there is now more than one criminal group using a set of different automated tools to inject malicious code. There is no longer any such thing as a “trusted site”. Any site running a vulnerable form is at risk.

The SQL attacks inject iframes that attempt to use several exploits to infect visiting computers. Infection by drive-by-download is more common than ever before.

**Browser Wars**

New versions of popular web browser have been released during the month of June. Firefox version 3 was released on June 18th with a very large marketing push in the United States. Millions of copies were downloaded and installed within the first 24 hours.

Opera 9.5 was released on June 12th. Internet Explorer 8 is in beta development.

All of these browsers contain enhanced security features that promise more of a challenge to malware.

**Third Party Applications**

As browsers are become hardened, much of the “lowest hanging fruit” has become the third party applications that have a large installed base.

Adobe Flash is one example. Flash is installed on nearly all Windows based computers. The Response Lab received sizable numbers of malicious Flash files during May and June. Such Adobe Flash exploits have been used in combination with the SQL injection attacks mentioned above. All but the current version of Flash 9.0.124.0 are at risk and many, many computers do not have the current version installed.
The powerful automated tools employed by malware wielding criminals have made it ever more important to update all of the application installed on one’s computer.*

**Mobile Phone Security**

During the first half of 2008 there were no significant mobile malware outbreaks. There was one new S60 2nd Edition worm called Beselo, more proof-of-concept type malware, and new commercial spy tools.

**Jailbreaking**

Mobile phone “modding” - the recreational hacking or modifying of phone hardware/handsets - has been very dynamic during the January to June period. Mobile phone enthusiasts are drawn to popular hardware and are eager to unlock any restrictions that exist. It’s very similar to the modding culture that exists among the video game community.

Jailbreak is a UNIX term that refers to the placing of files outside of a restricted folder structure. Once files have access to and are located in such restricted folders - privileged locations - the operating system can be altered.

The term jailbreak recently entered popular culture thanks to the Apple iPhone. Enthusiasts have developed easy to use tools with which to jailbreak the iPhone. The popularity of the device has led to rapid growth in iPhone security research.

**Symbian**

Perhaps some of this mobile activity has fueled the Symbian modder community as well. The Symbian operating system is the market-leading open operating system for mobile smartphones. Sales and market-share for Symbian based phones far exceed those of the iPhone. It is now possible to “Jailbreak” the Symbian S60 3rd Edition operating system with a single easy to use application.

Recent hacking techniques have targeted Symbian’s debugging interface, thus giving modders full control of the device without having to touch the firmware which can be risky. It also appears that all versions of the current Symbian operating system may be vulnerable to the techniques used. A graphical SISX application has only been developed for S60 3rd Edition however.

The privilege escalation allows the phone’s owner to install completely unsigned applications. Only signed or self-signed applications are possible with the security model intact. The hack limits the launching of new applications, but combined with another application, the hack can be toggled on or off at will following the first configuration.

It’s possible that Cabir, Commwarrior, or Beselo source code could be updated to run on S60 3rd Edition phones and with the addition of this privilege escalation they could cause similar problems as they do on 2nd Edition phones. However, Nokia and Symbian have worked on more S60 security features than just the platform security capabilities model. Current user interfaces would present more of a social engineering challenge than with 2nd Edition phones. We predict that someone will produce malware for 3rd Edition phones at some point just to prove that it’s possible, but don’t yet foresee any widespread threat.

More likely we’ll see a small but growing subset of enthusiasts running homebrew applications in much the same way as with the iPhone. Those users who are willing to risk the security consequences will run free applications from developers that skip the expense of the Symbian signing process. This subset of enthusiasts will continue to grow and will present more and more of a challenge to IT administrators attempting to enforce security policies within their organizations.
Q1 2008 THREAT SUMMARY

Windows 7

The amount of new malware has never been higher. Our labs are receiving an average of 25,000 malware samples every day, seven days a week. If this trend continues, the total number of viruses and Trojans will pass the one million mark by the end of 2008.

While there are more viruses being created than ever before, people often actually report seeing less of them. One reason behind this illusion is that malware authors are once again changing their tactics in how to infect our computers.

A year or two ago, most malware was spread via e-mail attachments, which resulted in mass outbreaks like Bagle, Mydoom and Warezov. Nowadays sending .EXE attachments in e-mail doesn’t work so well for the criminals because almost every company and organization is filtering out such risky attachments from their e-mail traffic.

The criminals’ new preferred way of spreading malware is by drive-by downloads on the Web. These attacks often still start with an e-mail spam run but the attachment in the e-mail has been replaced by a web link, which takes you to the malicious web site. So instead of getting infected over SMTP, you get infected over HTTP.

Drive-by downloads

Infection by a drive-by download can happen automatically just by visiting a web site, unless you have a fully patched operating system, browser and browser plug-ins. Unfortunately, most people have some vulnerabilities in their systems. Infection can also take place when you are fooled into manually clicking on a download and running a program from the web page that contains the malware.

There are several methods criminals use to gather traffic to these websites. A common approach is to launch an e-mail spam campaign containing messages that tempt people to click on a link. Messages like “There is a video of you on YouTube”, or “You have received a greeting card”, or “Thank you for your order” have been popular baits.

Another method used by criminals is to create many web pages with thousands of different keywords which are indexed by Google, and then simply wait for people to visit these sites. So when you do a search for something innocuous like “knitting mittens” (as a random example), and click on a search result that looks just like all the others, you are actually getting your computer infected. Typically, an infection by an automatic exploit happens without you realizing it or seeing anything strange on the computer screen.

The third method of distributing malware involves the criminals hacking into existing high profile, high traffic web sites. Unlike the joke defacements that some hackers played on the front pages of prominent web sites in the past, today’s criminal hackers don’t change the front page at all. They simply insert a line of javascript on the front page which uses an exploit to infect your machine when you go there. Everything works and looks as normal.

This has happened to the web sites of some popular magazines which can have a million users every single day. People trust sites that are part of their daily routine, and they couldn’t suspect that anything bad could happen when they go there.

Another vector for drive-by downloads are infiltrated ad networks. We are seeing more and more advertising displayed on high-profile websites. By infiltrating the ad networks, the criminals don’t have to hack a site but their exploit code will still be shown to millions of users, often without the knowledge of the webmaster of those sites. Examples of where this has happened include TV4.se, Expedia, NHL, and MLB.

It is important to be aware of this shift from SMTP to HTTP infections, which can be exploited by the criminals in many ways. Companies often measure their risk of getting infected by looking at the amount of stopped attachments at their e-mail gateway. Those numbers are definitely going down, but the actual risk of getting infected probably isn’t.

Individuals and companies should therefore be scanning their web traffic for malware - as well as filtering their FTP traffic. In parallel to the switch from SMTP to HTTP as a way of spreading malware, we are now also seeing more and more malicious e-mails that link to malware via FTP links.
**Advanced rootkit emerges**

A MBR rootkit - known as Mebroot - is probably the stealthiest recent malware we have observed, and has so far been distributed by drive-by downloads.

Mebroot replaces the infected system’s Master Boot Record (MBR), which is the first physical sector of the hard drive and contains the first code loaded and executed from the drive during the boot process. It keeps the amount of system modifications to a minimum and is very challenging to detect from within the infected system.

MBR viruses used to be the most common form of viruses at the time of the DOS operating system about 15 years ago. Recently there were academic papers published in conferences discussing whether this kind of MBR stealth could ever happen in the age of Windows. We have been very surprised to see it happening for real now in 2008.

This means that the criminals have both the funds and the high level expertise to develop such complex attacks. They have succeeded in developing code that loads from the boot sector of the hard drive, stays alive while Windows boots up, then loads parts of itself and injects to the operating system when Windows is up and running, and manages to hide all this very effectively.

We are likely to see this technique being used by quite a variety of malware. These first MBR rootkits are banking Trojans targeting several online banks, where the criminals are clearly seeing an opportunity to make a return on their investment.

**First mobile ransom Trojan**

Making money is what today’s malware is all about and the first ransom Trojans for smartphones have been found in China. We have already seen similar Trojans on the PC side before which infect your computer, take your data ‘hostage’ or somehow disrupt your computer’s capabilities, and then offer to restore everything back to normal if you pay out the ransom money. Typically, the ransom Trojan first encrypts your hard drive and then sends you a password after you have sent money to the criminals via an online money transfer system.

In the case of Kiazha, the first smartphone ransom Trojan, you get infected by downloading a shareware lookalike program on your phone, which then drops several known older viruses on your phone. Next it sends a message explaining that you can only get the phone fixed by transferring the equivalent of seven dollars to the attackers through an online payment system. Today’s smartphones are so important to many people that they are prepared to pay a ransom to get back their phonebook, calendar and mobile emails, so we might well be seeing much more of this type of malware in the future.

**More mobile trouble**

The Beselo worms spread via MMS and Bluetooth by using a novel form of social engineering to trick users into installing an incoming SIS application installation file. What makes Beselo interesting is that instead of a standard SIS extension, the Beselo family uses common media file extensions. This leads the recipient to believe that he or she is receiving a picture or sound file instead of a Symbian application. The recipient is then far more likely to answer “yes” to any questions the phone prompts after clicking on such an incoming file.

The filenames used by Beselo are beauty.jpg, sex.mp3, and love.rm. So if you have a Symbian S60 phone and receive a media file, answer “no” to any installation prompt that appears when trying to open the file. There is no reason for any image file to ask installation questions on the Symbian platform, so any image or sound file that does something else than play immediately is definitely not what it claims to be.

Beselo worms are compiled for S60 2nd Edition phones. Attempting to open the file on a 3rd Edition phone will probably cause an error message rather than an installation prompt.

HatiHati.A is another troublemaker, a worm-like application that spreads via MMC cards. Once the worm has copied itself to a new device, it starts sending SMS messages to a predefined number which can prove very expensive.

For a video about mobile threats, please go to our video channel.
H2 2007 THREAT SUMMARY

What previously took twenty years to accumulate - was now accumulated in just one year.

At the start of 2007 - our number of malware detections equaled a quarter-million. At the end of 2007, the estimates are to be equal to half-a-million.
Malware 2007

There was a great deal of volume seen during 2007. Malware authors are producing variants in bulk. Genuine innovation appears to be on the decline and is currently being replaced with volume and mass-produced kit malware. But while new techniques weren’t developed - the existing techniques were refined and adapted for much greater effectiveness. There are some very dangerous faces in the big crowd.

Windows Vista was on the horizon at the end of 2006 and the question was - would Vista be the end to malware threats? Not this year at least - The year 2007 ends with Windows XP still dominating the world’s installed base leaving Vista little opportunity to make an impact. The potential strength of Vista has not yet been tested in full force. And much of the malware in the wild running on XP machines is stronger than ever. We predict that the situation will not change very soon looking at Vista’s current sales.

Storm - Botnet 2007

Our Data Security Wrap-Up for the first half of 2007 (later referred to as H2) noted the birth of the “Storm Worm” - Storm being the umbrella name for a collection of backdoor trojans and e-mail worms.

On Friday, January 19th 2007, e-mail messages with subject lines based on actual news began to circulate. The subject line of “230 dead as storm batters Europe” coined the name Storm. There were in fact dozens of real deaths related to European storms during that time.

Using sensationalized versions of real headlines as a template proved to be a very clever bit of social engineering and was initially very successful. However, during H2 the headline technique’s success declined as it was repeated too often. So the gang behind Storm adjusted their procedures. During the second half of 2007 (H3), they have continuously updated their social engineering tactics. Targeting the U.S. - they have used holidays such as Labor Day and seasonal events such as the beginning of the National Football League (NFL) season. Targeting others - the gang keeps up-to-date with popular trends and sites. One of their tricks was the promise of seeing “yourself” in a supposed YouTube video in a message pointing to a fake YouTube site.

The gang has also altered Storm’s infection vector as detection of Storm increased and e-mail attachments were blocked. Instead of attaching the malware to the e-mail messages as before, they spammed messages with links to malicious Web pages. When the detection of the Web pages increased, they cleaned up the pages and instead linked to the malware from the page. So the vector evolution moved from e-mail attachments to Web pages pushing files to Web pages linking to files. (And those files are modified on the fly…) The evolution continues and adjusts as needed.

It is interesting to note that we have seen iFrames (inline frames) used by some Storm sites offering 16 versions of Storm to U.S. based IP addresses rather than the 9 that were offered to IP addresses outside the United States.

September’s Malicious Software Removal Tool, part of Microsoft’s monthly updates, made a dent in the size of the Storm botnet - the tool removed a good number of Storm’s bots during the update process - but the botnet remains and the dent hasn’t muted its overall strength.
Another special feature of the Storm botnet is that it protects itself. Repeat requests from a single source of one particular machine will result in many members of the botnet retaliating with a Distributed Denial of Service (DDoS) attack. Researchers must use caution during investigations or the botnet gets aggressive.

October brought evidence of Storm variations using unique security keys. The unique keys will allow the botnet to be segmented allowing "space for rent". It looks as if the Storm gang is preparing to sell access to their botnet. The end of H3 2007 finds Storm in a very strong position and utilizing only a fraction of its potential processing power.

**Malware Trends During H2**

**Banking Trojans**

While there are greater numbers of phishing sites online, it is most likely the result of kits such as Rock Phish. It is as easy to host multitudes of phishing sites as it is to host one. This ease of creation contributes to saturation and so there is a gradual reduction in the overall effectiveness. People are a bit more wary of phishing bait.

So what to do if you want to steal banking information? Use banking trojans.

Banking trojans sit and patiently wait for any banking activity. Trojans, by definition, use a decoy or ploy to get installed. Bank names are not mentioned. If the decoy uses clever social engineering, the victim may never realize what they have really installed on their computer.

Monitoring browser activity (URLs) for banking keywords is the Trojan’s task. When banking is discovered, a number of different techniques can be employed to steal the data.

- Form grabbing
- Screenshots and video capture
- Keylogging
- Injection of fraudulent pages or Form fields
- Pharming
- Man-in-the-middle attacks

See [The Trojan Money Spinner](#) (PDF file) for additional details. VB Conference September 2007.

Banking trojans are not a new phenomenon. But we have seen definite growth in 2007.

There is growing evidence of banking malware injecting itself into the browser. This allows some of the techniques above to be done as Man-in-the-Browser (MitB) attacks. These types of attacks allow the malware to use the browser as its platform. Encrypted banking sessions occur within the browser, so that’s where banking malware wants to be, before the banking session leaves the browser. We’ll see more of this trend in 2008.

**Trojan Password-Stealers and Online Games**

Another segment of interest this year has been Trojan password-stealers, specifically those that target online games. Online games continued to grow in popularity throughout the year 2007. More importantly - revenues continued to increase. More revenues means customers are spending more money, that’s the reason online game customers are increasingly becoming targets.

The economics are relatively straightforward even if the market is a bit of a novelty. Virtual commodities exist in the virtual worlds of online games. Many players of such games are willing to spend real money on these virtual commodities. So the value of these goods is real even if they are not physically real. And things of real value are the targets of theft. The stolen commodities get auctioned off and the thieves are difficult to identify because the crime is completely online.

In short, the money being spent within virtual games and communities has increased - so we’ve seen a corresponding increase in the growth of this segment during 2007.

The family Trojan-PSW:W32/OnlineGames was founded in September 14th, 2006. By the end of that year, we had around 150 detections. By the end of 2007, we will be near to having twenty thousand detections for this family. And there are numerous other families targeting the online games segment as well.

**Zlob - Fake Video Codecs and DNSChangers**

One of the most successful pests of 2007 is Zlob. It’s spyware that often claims to be a needed “video codec” to view copy-protected media.

Once installed, Zlob variants typically show fake error messages designed to convince the computer user into installing and buying rogue antispyware products.
Other pests from the Zlob gang such as DNSChanger silently reconfigure the computer’s DNS server settings. DNS servers are responsible for converting people friendly text URLs into computer friendly numeric IP addresses. Once the DNS settings are changed to their servers - the Zlob gang is in control of the Web browser’s destination.

They generate money by redirecting Web searches. Should the victim search for “air fare”, Zlob’s sponsored revenue-generating link will be put at the top of the results.

Zlob makes money by acting as a parasite. Stealing data from their victims is not the goal, and they don’t steal the computer’s resources to build a botnet either. What the Zlob gang prefers is to use their victims. As the victim does not suffer undo harm, many may not even realize how they are being used.

The Zlob gang expanded their target audience base late October with the introduction of DNSChangers for the Mac OSX platform.

**Apple Security**

The year 2007 was a banner one for Apple - their hardware is more popular than ever. More Apple hardware equals a greater installed base of Apple software.

**Trojan DNSChangers for Mac OSX**

As mentioned above, DNSChangers have started targeting Mac OSX. Social engineering is used to persuade users to enter their admin password for the install - not a big problem for clever social engineering. Getting a Mac user to type his password for an easily installed “video codec” isn’t a significant challenge to overcome, at least it hasn’t been a challenge for password protected Windows malware. And we’re seeing a growing number of Mac DNSChanger variants. The previous lack of Mac OSX malware could be a distinct disadvantage for its users. Social engineering can short-circuit a false sense of security.

Apple Mac’s market share is now significant enough for the Zlob parasites to target, as malware gangs don’t make an effort to develop something without the promise of a profitable return.

Apple’s Safari browser for Windows likely contributed to this development. Released in mid-June, researchers seized upon the Safari for Windows Beta and many security flaws were discovered. Many of those flaws were mirrored in the Mac version of Safari.

Web sites pushing DNSChangers determine the OS and the browser version being used by the visitor. The appropriate version of the malware is dynamically provided - visit with a Mac and you’ll get Mac malware.

**iPhone**

The Apple iPhone boasts an impressive design and a distinctive user interface. It was released in the U.S. at the end of June and becomes available to Europe during the fourth quarter of this year.

In just six months the iPhone has become a very well understood device.

It uses a version of Mac OSX, which is in turn based on Unix. If you understand Unix security, then you can relatively easily “port” your knowledge and understanding to the iPhone.

The iPhone also comes installed with the Safari browser and provides full rights to it. With the portability of understanding and the known Safari flaws mentioned above, coupled with the excellent hardware design, focus greatly intensified on the iPhone. Including the fact that the iPhone is a “locked” device and you have a perfect combination of factors leading to iPhone exploit research.

H.D. Moore added iPhone support for the Metasploit framework in September making security and attack research much easier.
Exploits for the iPhone are sought as a means to unlock the device. But in revealing those exploits there’s a security consequence.

**Leopard**

Mac OSX 10.5, code-named Leopard, was released at the end of October. It’s a major release for Apple.

It’s been well received for its features and sales are good but with increased popularity come increased focus on security flaws.

There have already been numerous updates made available. Research has suggested that old security flaws may have been reintroduced; Leopard’s new Firewall received criticism for its implementation and thus may affect Apple’s aura of perfect security.

**QuickTime and iTunes**

On the topic of popular Apple applications, there’s iTunes. The installed based of iTunes reaches far into the Windows platform. Even those without iPods use the application. And with iTunes comes QuickTime player.

QuickTime player is one of a growing number of applications targeted by malware. Previously, third-party applications were targeted as low hanging fruit as the Windows OS was hardened.

By the end of 2007 we’re seeing more and more exploits for third-party applications. Is it because they are the low hanging fruit? Or perhaps it is because the applications have reached such popularity as to become as ubiquitous as Windows itself.

**Mobile Security**

Symbian S60 3rd Edition has done an excellent job in curbing malware. Symbian leads the world’s market share of smartphones. Mobile malware discovered during the second half of the year affects older S60 2nd Edition phones.

What we continue to see on 3rd Edition platforms are spy-tools. The application vendors are able to get their spy-tools signed by submitting them as “back-up” software. The signed application is then also marketed for dubiously legal purposes. This trend matches what we saw during H2 and we expect it to continue.

S60 3rd Edition is more tightly controlled than previous versions and thus the lack of malware so far. However, the iPhone demonstrates that some users of tightly controlled devices want to “unlock” those devices. During October there were Symbian platform “hacks” posted. The hacks used a bug in the firmware update package software to completely unsecure Symbian 3rd Edition phones. If more users opt to unsecure their phones, it will have an effect on the future of mobile security.

One additional thought, as commercial vendors use what amounts to social engineering to get their questionable software signed, can malware authors be far behind? With a system that relies on humans to sign software, humans are, as with PC malware, the weak link.

**Database Breaches**

Reports of database breaches and data losses are becoming routine. There are massive amounts of personal data vulnerable to theft stored in databases worldwide.

January started the year with a bang. Reports revealed that TJX Companies exposed 45.7 million credit card numbers and transaction details. Poor WiFi security configurations and outdated WEP encryption was the culprit.

November caps off the year nicely in the U.K. with the HM Revenue & Customs (HMRC) losing 25 million names, addresses, and national insurance numbers. Two CDs containing information on parents, their children, and some portion of their bank account information was lost in the mail.

The use of personal data for ID theft is one obvious concern. Another newer concern is mass targeted attacks and mass spear phishing. Targeted attacks and spear phishing employ very detailed personal information as part of its social engineering. The target is called by name and the details of the message match their own personal details.

Spam addressed to “Dear Customer” is not nearly as effective as spam addressed to an individual using correct job titles and locations. Include additional factual details and the victim lowers their guard exposing themselves to phishing, trojans, backdoor, and more.

A November 6th letter from Salesforce.com acknowledged the leak of the company’s contact list. The result of the leak was spear phishing attacks made on their customers.
Late November also brought news of a mass targeted attack using the U.S. Department of Justice as the bait. Recipients were addressed by name and their company name was used. The spam message claimed that the company had received a DOJ complaint. The supposed complaint, a trojan-downloader, was attached to the message.

Personal information available for exploit is everywhere. With the popularity of social networking sites it’s ever more readily available to the bad guys.

We’ll see more bulk targeted attacks via spam as database leaks are used to enhance social engineering during 2008.

**Web Exploits**

Besides targeted spam, as “spray and pray” spam waves decrease in effectiveness, there is an increase in Web based threats. As noted in the Storm section, once Storm attachments were blocked, the malware executables were moved to the Web.

There’s an increase in use of ready-made kits for vulnerabilities such as MPack, IcePack and Neosploit that include easy to use web-based admin interfaces. These kits not only target Windows and Internet Explorer vulnerabilities but also other browsers, QuickTime, Real Player, WinZip, et cetera. These kits even come with support packages and updates for the right price.

Some other trends:

- **Use of pay ads (Flash exploit) affecting high profile websites (NHL, MLB).**
- **Use of search engine manipulation to direct people to malicious sites.**
- **Criminals continuously searching for sites to compromise. (Bank of India, CSIRT in China).**

**Conclusion and Predictions**

What we saw during H3 and the whole of 2007 was volume. Malware authors are criminals and as time passes they are becoming increasingly professional at their “business”. Kits and commodities markets are the result. The tools of online crime are being produced professionally. The purchased kits are producing malware in bulk. The stolen data is traded as commodities on underground auction sites. It’s easy money with plenty of cover from law enforcement.

What will we see in 2008? More of the same - lots more of the same but better, stronger, faster. The criminals have the technology. Everything will continue in bulk to ensure broad coverage. And as the bulk increases individual security awareness, new improved technology powered social engineering will strip that awareness away again. 2008 will be a challenge of endurance.
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.

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.

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. Microsoft 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.

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:
- Labs Weblog: Masters of Their Domain

**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:

“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:

- (Ministry of Economic Affairs and Communications): unreachable
- (Website of the prime minister): unreachable
- (Estonian Parliament): unreachable
- (Ministry of Internal Affairs): unreachable
- (Estonian Government): unreachable
- (Ministry of Foreign Affairs): unreachable
- (Ministry of Agriculture): reachable
- (Ministry of the Environment): reachable
- (Ministry of Finance): reachable
- (Ministry of Justice): reachable
- (Ministry of Culture): reachable
- (Ministry of Defence): reachable
- (Estonian Police): reachable
- (Party of the prime minister): reachable
- (Ministry of Social Affairs): reachable
Estonia

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.


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

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.

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

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.

![Service message](image)

**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.

![Install NetCompressor?](image)

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:

Spy tools have been born for both Windows Mobile and Symbian S60 3rd Edition devices.

We anticipated these spying tools, 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.
F-Secure is an online security and privacy company from Finland. We offer millions of people around the globe the power to surf invisibly and store and share stuff, safe from online threats.

We are here to fight for digital freedom.

Join the movement and switch on freedom.

Founded in 1988, F-Secure is listed on NASDAQ OMX Helsinki Ltd.