SOPHOS

simple + secure

The Koobface malware gang exposed

An investigation by **Jan Drömer**, independent researcher, and **Dirk Kollberg**, SophosLabs

Sophos Exclusive Research Unmasks Koobface Malware Gang

Following media reports that Facebook has identified five people as responsible for the Koobface worm, IT security and data protection firm Sophos releases its independent and exclusive research into the Koobface gang, identifying the same alleged perpetrators as Facebook: Anton K., Alexander K., Roman K., Syvatoslav P., and Stanislav A.

Names and other details have been omitted to protect the privacy of the suspects and their families. Further, some URLs within this document might contain offensive material or malicious content not safe for browsing.

SophosLabs malware expert Dirk Kollberg and independent researcher Jan Droemer worked with an extensive team across the industry. Droemer and Kollberg's wealth of findings include the perpetrators' nicknames, online activities, physical locations and business dealings.

Koobface (an anagram of "Facebook") spreads via social networking sites, infecting PCs and building a botnet of compromised computers. It is so sophisticated it can even create its own social networking accounts, so that it can aggressively post links helping it to spread further.

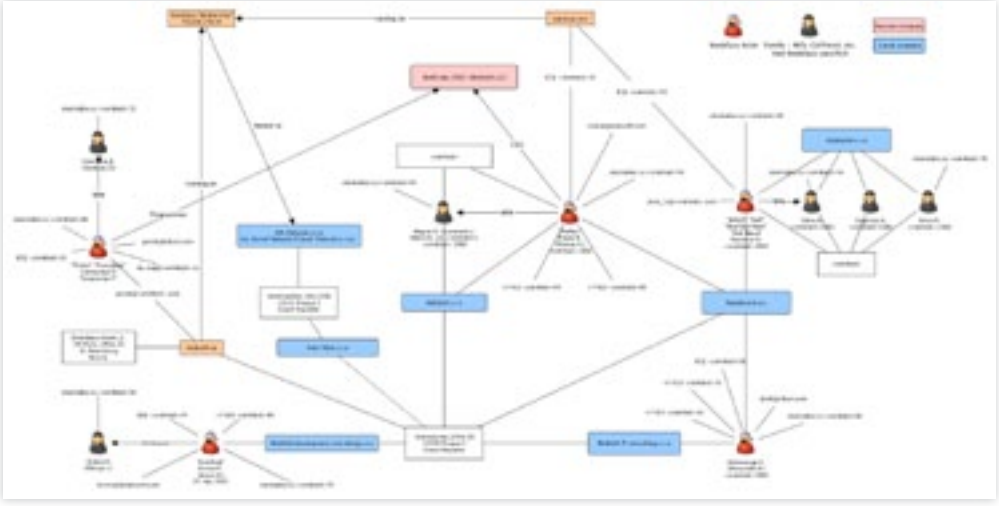
The creators of Koobface, whose names have not been public until now, earn millions of dollars every year by compromising computers.

Not a perfect (cyber)crime

The Koobface botnet—a product of the self-proclaimed "Ali Baba & 4" or "Koobface Gang"—has been terrorizing millions of internet users since mid-2008 and continues to do so up to the present day, despite multiple takedown efforts.

This research, conducted by independent researcher Jan Drömer and Dirk Kollberg of SophosLabs, is focused on the suspects behind one of the largest cybercrime threats in recent years and how they were identified.

The main research into the suspects was conducted from October 2009 until February 2010 and has been available to international law enforcement agencies since then.



See enlarged graphic next page.

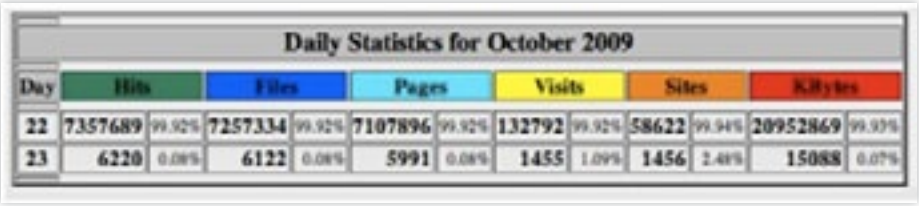
As in real life, a perfect cybercrime is a bit of a myth. The simple truth is that today's cybercrime landscape is aimed at achieving maximum revenue with minimal investment, which implies a certain level of imperfection. It's this imperfection, paired with a sense of "criminal arrogance" and an uncontrollable threat environment such as the internet, that ultimately led to the identification of multiple suspects forming the "Koobface gang".

The Koobface gang makes a mistake, and then another..

With every cybercrime attack, there can be vast amounts of technical information such as IP addresses, domain names, etc. available which usually form the starting point of an investigation. The Koobface investigation was no different. Upon identifying one of the Koobface Command & Control (C&C) servers used to steer the attack, the gang made its first mistake.

Turns out that the Apache web server on one of the active Command & Control servers (captchastop.com, 67.212.69.230) had the mod_status module enabled. With this module enabled, any visitor has public access to a live view of requests made to the web server, revealing file and directory names.

Although this mistake was corrected at the end of October 2009, days later the gang made yet another mistake by installing the Webalizer statistics tool in a publicly accessible way, allowing even better insight into the structures of their Command & Control system.



Daily Statistics for October 2009

Day	Hits		Files		Pages		Visits		Sites		KBytes	
22	7357689	99.92%	7257334	99.92%	7107896	99.92%	132792	99.92%	58622	99.94%	20952869	99.93%
23	6220	0.08%	6122	0.08%	5991	0.08%	1455	1.09%	1456	2.48%	15088	0.07%

A major breakthrough in the technical investigation came in December 2009 when the Webalizer statistics tool showed an unusual request to a file named "last.tar.bz2," which turned out to contain a full daily backup of the Koobface Command & Control software. During the investigation similar backups were obtained from various other Koobface Command & Control systems.

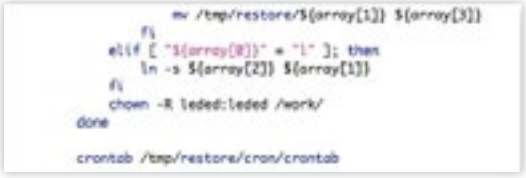
While these backups allow for a detailed technical analysis, they were mainly used to identify the entire system landscape forming the Koobface Botnet as well as any information (usernames, source code comments, log-files showing IP addresses, etc.) that could help identify the main actors. This led to various domain names and IP addresses, out of which one system stood up in particular.

This "Koobface Mothership" was hosted on the IP address 78.108.178.44, located within a network of UPL Telecom in Prague (Czech Republic) and used to store statistics, monitor C&C and used within the restore process in case C&C servers become unavailable.

Two of the found domain names (babkiup.com and service.incall.ru) were also hosted on the Koobface Mothership server. While incall.ru appeared to be a legitimate VoIP service, babkiup.com was greeting users with a service description that matched exactly the behaviors of the Koobface Botnet, including a short question and answer section for interested customers and ICQ contact details for two individuals going by the nicknames "PoMuC" and "LeDed".

Back to the backups, probably the most stunning information was found within a PHP script used to submit daily revenue statistics via short text messages to five mobile phones. The international prefix +7 identifies these numbers to be Russian telephone numbers.

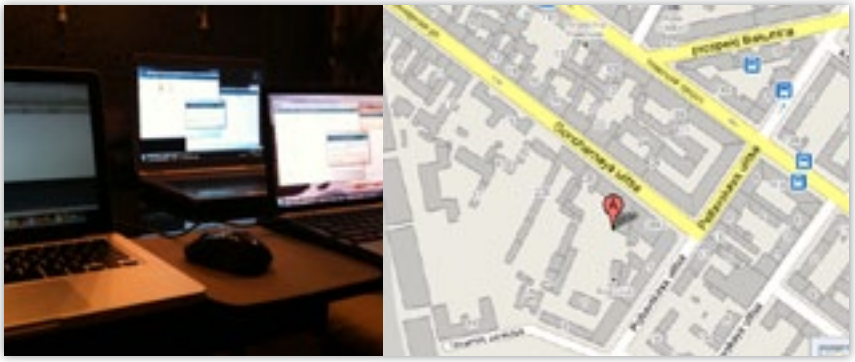
Note that one phone number has been commented out from receiving SMS messages, which either means that this gang member simply wasn't interested in these statistics or it may also be an indication that one member left the group.



The nickname "LeDed", named as a contact point on the "babkiup.com" website, reappears as a Unix username within a script used to restore defunct Koobface C&C servers. It is of particular note that within this script "LeDed" shows up as user/groupname within the Unix chown command.

"Krotreal" is another nickname that can be found within a script called "gen_service.php". Circumstances suggest that the source code comment made within the script, was made by "Krotreal" itself, likely implying that this individual had access to the source code of the PHP script(s) making up the Koobface Command & Control system.

Furthermore an image named "IMG_0121.JPG" was found within one of the backups. This picture is completely unrelated to the function of the Koobface botnet itself but may have been placed there by a Koobface gang member.

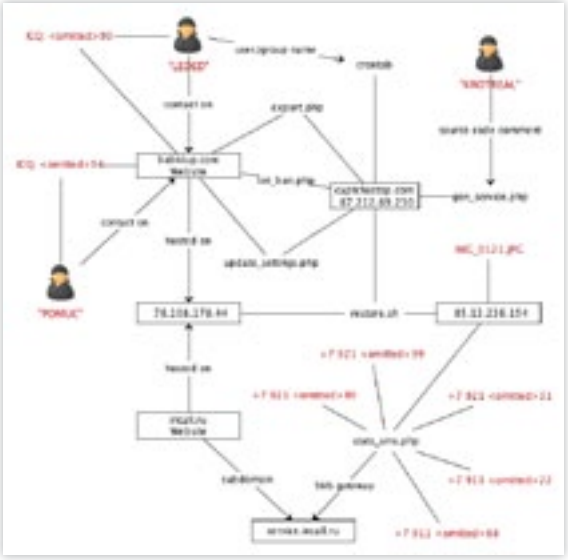


According to the Exif metadata contained within the photo it was taken with an Apple iPhone on September 15, 2009 with a Latitude of N 59° 55.66' and a Longitude of E 30° 22.11'. This directly points into the center of St. Petersburg, Russia.

Though this information may not be accurate enough to identify a single address, it supports the earlier presumption that the actors might be located in Russia and that one or more are probably located in the St. Petersburg region.

However, it is important to point out that this observation is rather speculative, considering that the photo could be entirely unrelated to the Koobface actors.

The following graphic depicts key information derived so far from the Koobface backups and websites.



Of cars and kittens..

Any further research would obviously start with the telephone numbers, since these are the most likely way to obtain identities of potential suspects. Different notations of telephone numbers were used as search strings, as well as look-ups made against the online telephone book of St. Petersburg, Russia.

One number was found on an online market platform for cars, one was selling a BMW 3 Series with the cars number plate "H <omitted> 98" in 2008.

The very same telephone number also appeared in another forum post from September 2007, this time trying to selling kittens. Even more important in this context is the email address "Krotreal@<omitted>.com" and the name Anton listed as contact.

As the telephone number search came to a dead end, the next most likely source of information would be the three nicknames ("Krotreal", "LeDed", "PoMuC").

"Krotreal"—or what's in a nickname?

Just as first and last names are the key to a person's identity in real life, so nicknames serve that purpose online.

Usually nicknames are life-long once chosen, and often have trust and reputation associated with them. This holds especially true for the underground economy were no-one is using their real identity in communications, yet there is a need to distinguish between those that offer reliable cybercrime services and those who don't.

Although some criminals use multiple nicknames or variations, they are forced to retain them to a certain extent to remain identifiable within the cybercrime ecosystem.

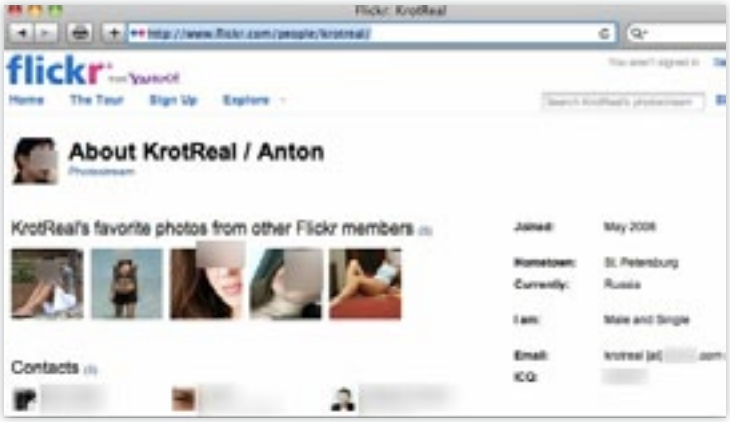
One may think that cybercriminals would "clean" all their profiles, but this is often not the case. There are several contributing factors to this, the most simple being for example that old profiles might have been simply forgotten or others may have all of a sudden become public due to a terms-of-service change.

Identifying such profiles at various social or Web 2.0 websites is easily possible through search engines or services like namechk.com or knowem.com. While these website are intended to help users with choosing a unique nickname not occupied by other users or to maintain their digital identities, they are in turn highlighting all those services used by a particular nickname.

This is exactly what we can use to our advantage in order to identify potential profiles containing additional information. Care must be taken during the analysis, of course, as profiles may belong to other individuals using the same nickname, or may even be intentionally forged.

In the case of the nickname "Krotreal" profiles at Flickr, Netlog, LiveJournal and later during the investigation vkontakte.ru, YouTube, FourSquare, Twitter, etc. could be identified.

This shows the importance of a repeatedly searching over several weeks.



All of these profiles were investigated for information leading to the real identity of "Krotreal". Profiles time and time again showed the name Anton, various email addresses, hobbies, references to St. Petersburg and an ICQ number.

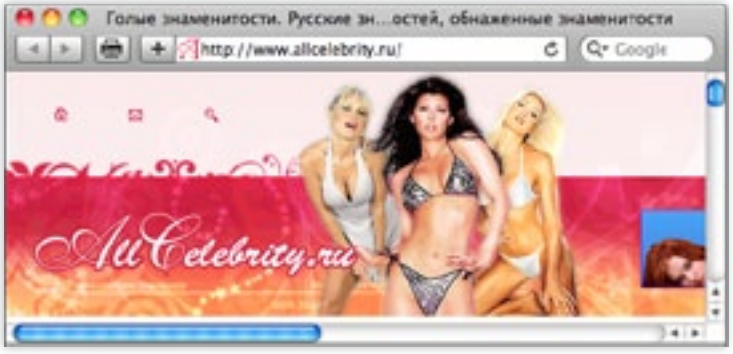
Some of these profiles even contained portraits of "Krotreal", providing another linking pin between the profiles, similar to the reappearing avatar pictures used within the profiles.

Access levels to individual profiles generally varies. The Flickr photo streams, for instance, aren't publicly accessible in this case. Nonetheless it is generally advisable to perform tailored searches against the profile using various search-engines, as there might be historic information cached by the search engine, or deep-links to profile information not show as it is the case with Flickr. One of the images turned up by a search showed a car with the same numberplate as discussed above and a caption "My little beauty :)".

Images in themselves may contain vital information, e.g. in this case the licence plate is framed with the name and and phone number of a German car-dealer, which could be used to trace the ownership chain of the car from that dealer towards it current owner.

Yet another photo of his Flickr profile shows him holding a Sphynx cat, which is an additional indication to the identity of "Krotreal" with regards to the kitten forum post discussed above.

While most of the profiles contain similar information, one is of additional interest as it references the website "www.<omitted>.ru" as belonging to "Krotreal" with the same holding true for his ICQ account.



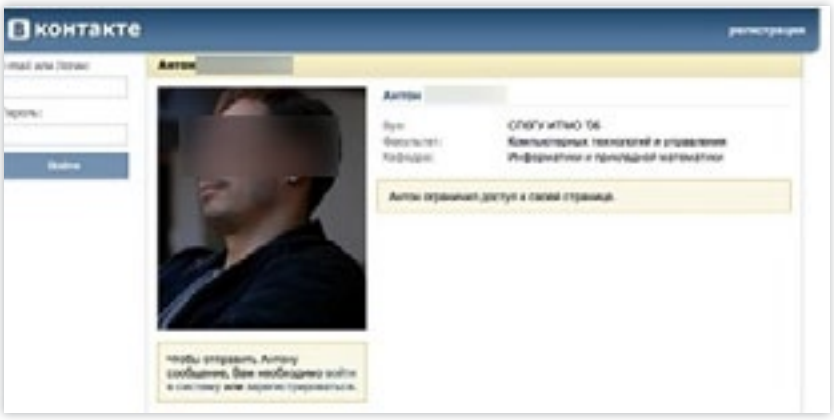
This page is an adult website. Surprisingly enough it appears the Whois details of the website had not been concealed, listing an Anton K., with a St. Petersburg telephone number as owner of the domain. Yet the accuracy of Whois details must be treated with care.

Querying Whois data for the Domain verybest.org, which is used to provide name services for www.<omitted>.ru, reveals yet another email address ("Krotreal@mobsoft.com") indicating that "Krotreal" was in one way or the other affiliated with this company.

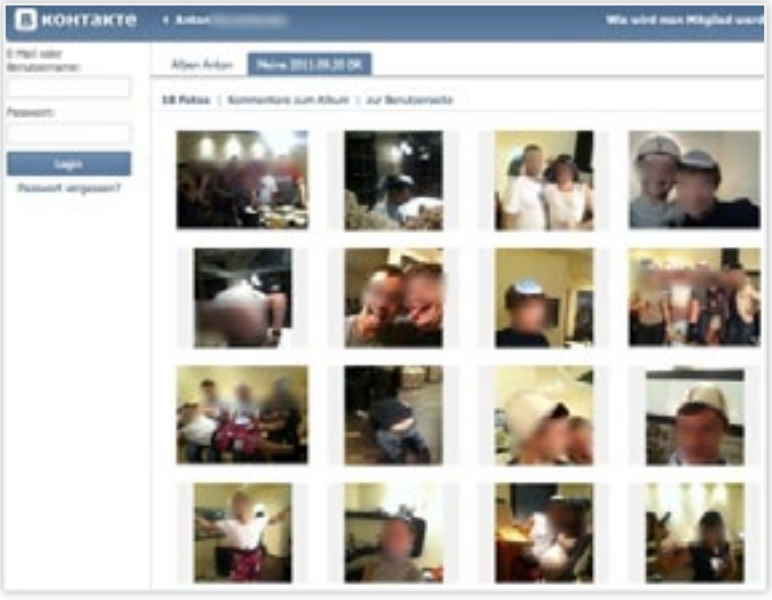
Note: Later during the investigation hosting of www.<omitted>.ru moved to the IP address of the Koobface Mothership—78.108.178.44.

Of special interest are of course social networks like Facebook or vkontakte.ru as they allow the identification of family members, friends and colleagues in case the profiles are publicly accessible.

The profile of "Krotreal" was initially very restricted, only allowing access by his friends. This situation changed over time, again a reminder for investigators to recheck such profiles from time to time.



Although the profile wasn't accessible initially, "Krotreal" posted links to photos within his profile on his Twitter account, thereby making these pictures publicly available.



Although the pictures are interesting by itself, given that they reveal travel activities, etc., more interesting are the comments made by other vkontakte.ru users.

Considering that the profile itself is restricted to the effect that only his friends have full access, these comments are especially useful to determine social relations and may thus provide clues related to the other actors behind Koobface, assuming that they know each other and are probably connected via social networks.

Unfortunately no such references could be found, however one comment made by Olesya L. is of particular interest due to the fact that she has a more accessible vkontakte.ru profile with several accessible photo albums. Further analysis of these photo sets portrayed both Anton K. and Olesya L. together on several occasions, suggesting that they are a couple.

While it was possible to elaborate "Krotreal's" social relations in more detail, no additional evidence confirming his identity could be obtained. Although it is suggested that "Krotreal" is in fact Anton K. further proof is necessary to substantiate this conclusion.

Obtaining proof of an identity is a difficult task, given that profiles, Whois data, etc. can be forged. Fortunately enough one of the found email addresses suggests that Anton K. was or is affiliated either as freelancer, employee or even as owner with a company called MobSoft.

Inside the Koobface firm

The Koobface gang rent offices on the top floor of this St Petersburg building. Note that there are other companies based in the building who have nothing to do with cybercrime.

Companies are an interesting research subject during an investigation, given that they usually need to be registered with the government or the tax service and fall under specific legislation mandating reports, etc.

Furthermore they usually keep public websites, eventually providing information about their history, the former and current management or also interesting employee testimonials on the careers pages.

In cases where a suspect is believed to be the owner or shareholder of a company, chances are that it will likely be possible to obtain valid identity information, as a company registration processes normally require valid identity documents, etc. to be shown.

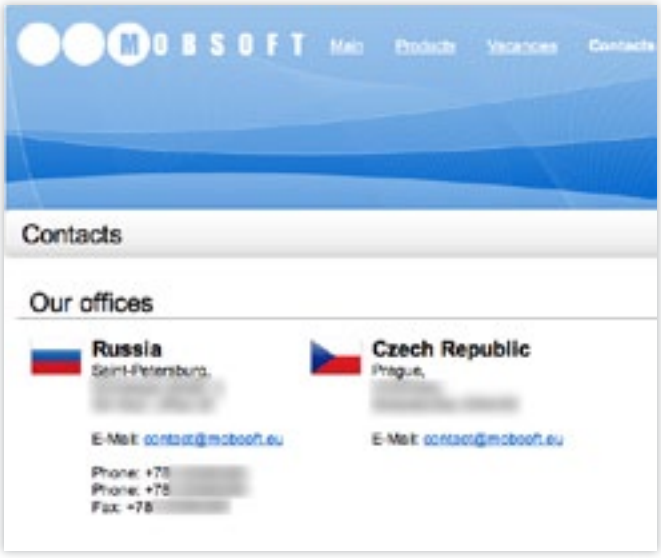
Even though employees or owners of a company might be involved in malicious activities, this does not automatically imply any whatsoever involvement of the company as such.

The research on MobSoft came to an early end, however, as the domain mobsoft.com was no longer resolving to a corporate website. Querying search engines also remained inconclusive and even complicated matters with multiple entities operating under the name MobSoft.

However, one lead was remaining with a copyright noticed placed on the website incall.ru, claiming the service to be a joint development between UPL Telecom s.r.o and MobSoft Ltd., with the name MobSoft Ltd. pointing to the website mobsoft.eu.

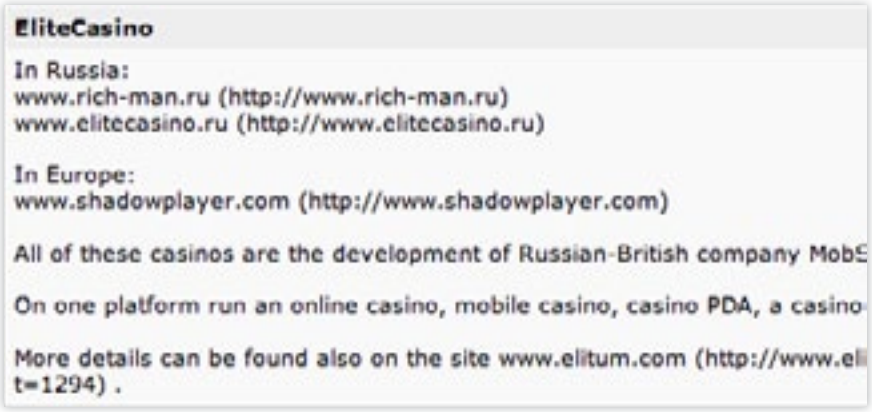
UPL Telecom s.r.o is a Czech company and was either directly or indirectly the hosting provider of the Koobface mothership server.

Reviewing the www.mobsoft.eu website, MobSoft Ltd. presents itself to be a company specialized in software development and distribution of mobile applications and services. According to its website it is operating from two offices, one located within the Czech Republic and one located in St. Petersburg, Russia.



Even though mobsoft.eu was also hosted on the Koobface Mothership server there was no proof that both mobsoft.com and mobsoft.eu were related to each other.

Additional research however revealed cached artifacts from the defunct mobsoft.com website such as the company logo as well as product descriptions such as the "Mobile Casino Management System" suggesting both to be owned by the same company.



The St. Petersburg address listed on the MobSoft website isn't providing any additional insights, unlike the Czech address. Google Streetview shows the address to be located in a residential area of Prague, and search results suggest a flurry of companies are registered at this address, including three Mobsoft entities.

The Czech government maintains an online portal providing easy access to company details such as the business purpose, registered address as well as details about shareholder and owners.

Registered persons are listed including their dates of birth and passport ID numbers. Reviewing the company details, we found Anton K. as proprietor of one of these companies, suggesting "Krotreal" is indeed Anton K. from St. Petersburg, Russia.

Similar searches were performed against the St. Petersburg company register, as well as the UK and Isle of Man registers. The latter two, due to the fact that forum posts were suggesting a joint UK & Russian company, with other information suggesting that Compact Disc India acquired MobSoft (Mobile Software Limited) with development centers in both the UK and St. Petersburg. These traces, albeit interesting, remained inconclusive.

Language matters—МобСофт

The Koobface case clearly has strong ties to Russia or Eastern Europe, meaning that language becomes an important factor in our investigation.

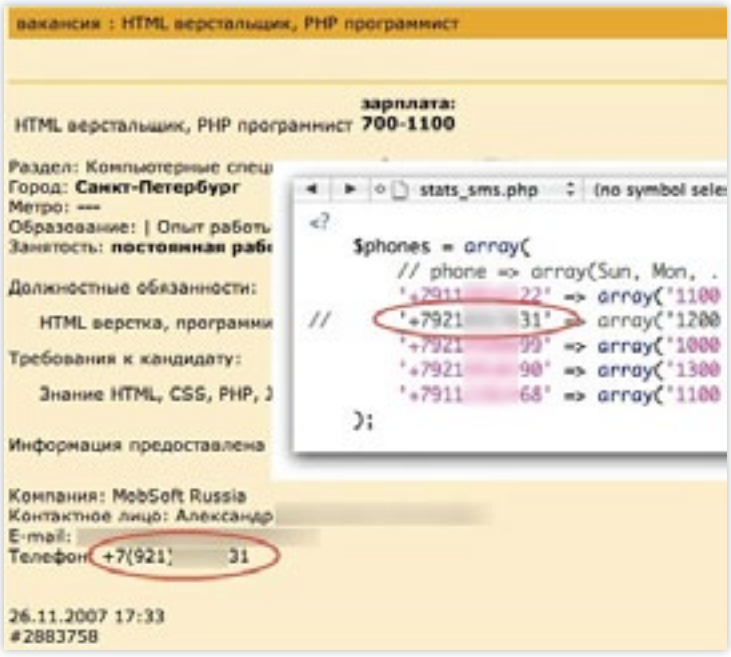
A simple search for MobSoft with the Russian Federal Tax Server resulted in no matches, but a search using the correct Cyrillic characters "МобСофт" provides the desired result.

The very same is true for search engines, such as Google or Yandex, or for searches within social networks. It is also important to understand that automatic translations of suspect names or even their sometimes self-chosen translations may result in no or even wrong results.

Research using the term "МобСофт", not only confirmed the existence of a company registered in St. Petersburg, but also lead to a Russian portal selling information about business. This portal lists Roman K. as the owner of Mobsoft LLC based in St. Petersburg.

We already know about this name from the Czech company register in connection with Mobsoft s.r.o. Continued research also led to various job portals identifying former employees of MobSoft such as for example a graphics designer. While this person is unrelated to the Koobface threat, the website provides various artwork such as the MobSoft corporate design.

Most remarkably however was a job advert, listing someone called Alexander K. as the company's contact with a mobile phone number that matches one of the numbers found within the Koobface SMS statistics script!



Details about Alexander K. are sparse. Just like the case with "Krotreal" access to Alexander's vkontakte.ru profile is unfortunately restricted.

Although it is inaccessible it presumably shows a photo of him. Alexander K. was also found commenting on various vkontakte.ru walls of other potential Koobface gang members. Attempts to locate more information about him and his precise involvement remained inconclusive.

Several profiles suggest that he also operates under the nicknames "floppy", "megafloppy" or "darkfloppy". Profiles using these nicknames can be found on various social networks, for example on LiveJournal.

Given the user profile picture, the birth date, the reference to St. Petersburg and the interests in various programming languages, he might have been involved in programming activities for the gang.

It is, however, of importance that it is his mobile phone number that has been commented out from the SMS statistics script. Like "PoMuC" he is also shareholder of Paytelecom a.s. another Czech company found while searching through the Czech company register.

Further research led to another job offer, again made by Alexander K. this time listing a St. Petersburg number "+7 (812) <omitted> 31".

PHP programmer coder

Salary:
800-1400

Category: Computer specialists: programmers
City: **St. Petersburg**
Metro: **Narva** , on the subway for 10 minutes.
Education: **irrelevant** | Experience: **1 year** | Age: **20 to 40**
Employment: **permanent job in the office full-time**

Job Responsibilities:

development of PHP code, template SMARTY, AJAX development scripts, coding

Requirements:

Good knowledge of PHP, HTML, JS, AJAX, CSS, Smarty

Information provided by the site boss.jlt.ru

Company: MobSoft Russia
Contact: Alexander
E-mail:
Phone: +7 (812) 31

03.12.2007 14:13
2908083

This number is exactly the same compared to the mobile phone number except that the St. Petersburg area code is used instead of the mobile network code. While this might be just a typo or pure coincidence, mobile phone numbers using the regular area code instead of the mobile network are considered to be more prestigious and are as such known to exist.

Following this train of thought, it was possible to link another number from the Koobface statistics script to Roman K., given that this number is listed within the Whois details for the domain highspeed.ru, owned by him.

```
domain: HIGHSPEED.RU
nserver: ns.masterhost.ru.
nserver: ns1.masterhost.ru.
nserver: ns2.masterhost.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Roman K.
phone: +7 812 <omitted>99
e-mail: andrew@elitum.com
registrar: RUCENTER-REG-RIPN
created: 2003.09.26
paid-till: 2011.09.26
source: TCI
```

Similarly vkontakte.ru was searched using the term "МобСофт" which led to the identification of two profiles, one belonging to "Vladimir XD" (about whom no further information could be retrieved) and the other one belonging to Svyatoslav P.

Friends and family—a weak link for the Koobface gang

With Anton K. ("Krotreal"), Alexander K. and Roman K. identified as suspected Koobface gang members, a few nicknames and individuals remain to be researched.

One of them is "PoMuC", listed with his ICQ number as a contact on the babkiup.com website. His ICQ profile already provides a wealth of information.

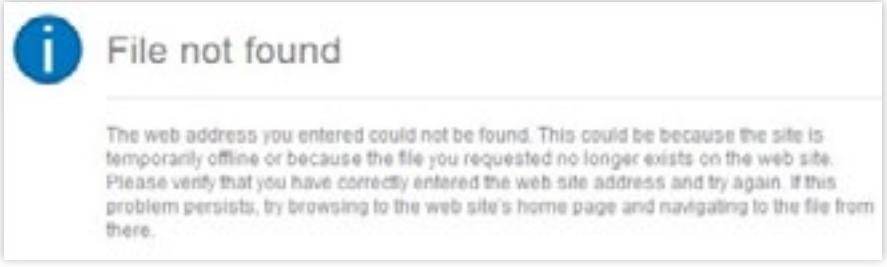
We begin with the first name "Roman" and a connection to MobSoft, combined with a birth date and a reference to St. Petersburg. The first name and date of birth match those of a Roman K., according to the Czech company register.

There were only a handful of profiles related to "PoMuC", and those that were likely to be linked to him, were sparse on details.

Besides some email addresses, a link to a company called "Elitum Ltd." was found, which was devoted to the development of mobile phone applications (casino games, etc.), very similar to MobSoft.

Some of Elitum's products, such as ElitePassword, may still be found on the internet.

The company itself, however, seems to be dissolved, and its website is no longer being available.



Nonetheless a few email addresses can still be found such as {andrew|psviat|akolt|support|4spam}@elitum.com.

The nickname "psviat" was also used to register the domain "mobsoft.eu". The name used in the registration was Syvat P., which may stand for Svyatoslav P.

Another profile confirmed the nickname "akolt", to be Alexander K., owner of MobSoft IT consulting s.r.o. Finally, the address andrew@elitum.com was used by Roman K. to register the highspeed.ru domain.

With details sparse, a search for the name Roman K. was performed on vkontakte.ru and the resulting profiles reviewed.

Unfortunately, none of the profiles seemed to match, or were simply inaccessible.

It might have seemed that a dead end had been reached, but you shouldn't underestimate friends and family.

It is known from the Czech company register that a Maria K. is listed as a co-owner of of one of the MobSoft entities.

Searching for Maria K. on vkontakte.ru returned just one hit. Luckily, her profile allows public access to the greatest possible extent; including photo sets, lists of friends etc.

Not only do we find Roman K. on the friend list and on several photos, but for example also Anton K. From the profile it becomes clear that Maria and Roman K. are married and have one daughter.

Now having a face of Roman K. it is furthermore possible to link two followers of "Krotreal's" Twitter account (spb_roman and ru_roman) to Roman K., given that both avatar pictures of these accounts show him.

This also provides us with two possible nicknames used by Roman K. which can be further investigated.

Upon investigation of the photo sets shared by Maria K., it was furthermore discovered that the family spent their holidays together with Anton K., suggesting a fairly close relationship between them.

Family and friends in social networks also play a role during the investigation of Svyatoslav P., alias "psviat". Even though his vkontakte.ru profile is publicly accessible, his photos are not. Even if Svyatoslav P. isn't sharing photo sets himself, more than 95 photos have been tagged by others, linking to him and his profile.

This is an inherent feature of social networks and shows the difficulty of maintaining a low-profile on these networks, because if one does not provide information such as photos himself, family and friends may do so. The analysis of these photos for instance show, that not too long ago, he married Svetlana D. who in turn is an acquaintance of Maria K.

His friend list showed that he is an acquaintance of both of the previously discussed Maria and Roman K. as well as Anton K.

Linking the nicknames "psviat" and "PsycoMan" to Svyatoslav P. was possible through the investigation of various profiles. Although his exact involvement in the Koobface threat isn't yet known, circumstances are suggesting that he might have been involved with programming tasks.

He can be also linked to the email address "ha-xep@.ru" which was used in connection with various malicious activities, such as for example the domain setup.bestmanage.org which used to be hosted on the same IP address as the old mobsoft.com website, within a network of UPL Telecom.

Sex sells

With a picture of Svyatoslav P. and his wife from the vkontake.ru photo albums, it was possible to identify them on pictures as having participated in the AWM (Adult Web-Master) Open 2009 conference in Cyprus.

The website "FUBAR Webmaster" contains archived photo sets from various adult industry events on which the couple was identified.

Svyatoslav P. was pictured using the nickname "PsycoMan" on his badge.

The porn industry, especially in Russia, is a frequently appearing linkpin when investigating cybercrime, as suspects are often found to be involved in the "adult entertainment" business.

There are likely several reasons for this, and it should by no means imply that the adult webmaster scene as a whole is involved in malicious activities.

As it is highly unlikely that cybercriminals start their criminal careers just out of the box, a more commonly observed pattern is individuals entering and getting involved in the internet porn industry, getting to know affiliate models, traffic trading, etc.

The somewhat shady nature of the scene, and the criminals' desire to make even more money fast, might be what makes some slowly cross the line and get involved in more malicious activities.

Additionally one should not forget that trust is equally important to the underground market as it is in legitimate business. Several porn industry events throughout the year are providing an excellent platform to establish such trust and business relationships in person, which might be another reason that the porn industry repeatedly shows up during the investigation of cybercriminals.

The adult webmasters of St Petersburg

Born in 1962, Stanislav A. (also known as "LeDeD", "DeD", "Ded Mazai" or "zoro_ru") is some 20 years or more older than the other members of the Koobface gang, and is the last and possibly most interesting suspect in this investigation.

While several profiles could be found on various shady forums such as crutop.nu, master-x and umax to name but a few, these profiles are not containing much useful information besides his ICQ number and claims to be "in service since 1999".

One of the postings made by "DeD" at www.master-x.com contained a link to a webpage on a site called 99livecam.

Accessing this link takes a visitor back to the ancient history of the St. Petersburg Adult Webmaster scene, namely to the homepage of "The United Club of Adult Webmasters of St. Petersburg", dating back to the year 2000.

The website includes some pictures from their very first club meeting. In addition to this, the Club-Website contains a picture-section called "Ded Mazai", the same term found within the ICQ profile of "PoMuC".

It may be assumed that the term "Mazai Team" references some group of (presumably) adult webmasters in St. Petersburg.

The website also contains a link to a discussion forum linked to the infamous CoolWebSearch (CWS) spyware activities. Further analysis of the forum posts provided some historic insights into the CWS activities as well as information about the Russian Adult Webmaster scene, again repeating the pattern previously discussed.

It is no surprise to find Stanislav A. connected to the nefarious CWS activities, as well as exploits, PPC (Pay per click) fraud, etc

Research of historic profiles and Whois records ultimately revealed his name, such as for example a historic whois entry of the dnserror.org domain, which was named in various discussions about malicious websites. One of these discussions contained a historic Whois entry for dnserror.org, listing an Stanislav A. in Prague:

```
Registrant Name:Stanislav A.
Registrant Organization:no
Registrant Street1:P5,
Registrant City:Prague
Registrant State/Province:CZ
Registrant Postal Code:15200
Registrant Country:CZ
Registrant Phone:+420<omitted>
Registrant Email:zoro_ru@<omitted>.com
```

The name Stanislav A. also showed up during the research of Roman K. and Alexander K. as all of them are shareholder of Paytelecom s.a., another Czech company.

Querying the Czech company register for the name Stanislav A., reveals another company. Owners of this company are Stanislav A., his wife and daughters.

You may wonder why the entire family is registered as company owners, but owning a company within the Czech Republic apparently eases the Visa application process, even granting permanent residence rights at some point in time, which might be the reason in this case.

Given this information one can now establish an obvious link between "Ded Mazai" and Stanislav A. The "Ded Mazai" profile on vkontakte.ru lists both his daughter and his wife as friends, next to Anton K. and Roman K.

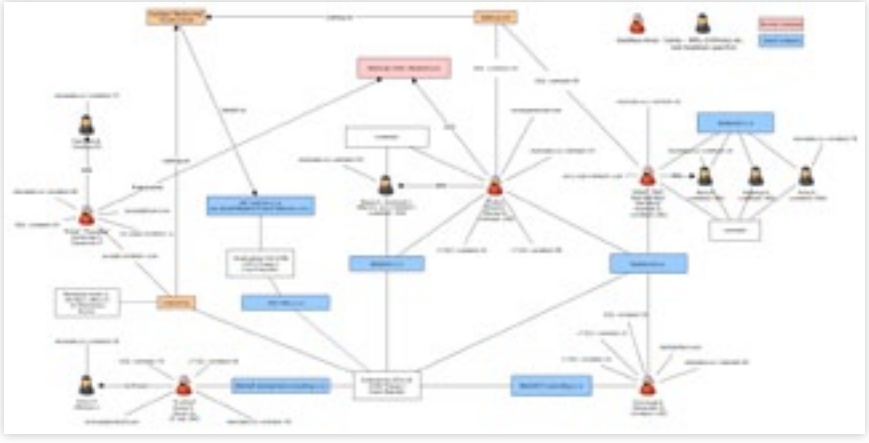
Stanislav A. even shares some photos. One for instance documenting his attendance at the AWM Open 2005 conference. Stanislav A. also maintains a publicly accessible photo album with hundreds of photos at Google Picasa.

One of these photo sets was of particular interest as it shows all of the previously discussed suspects together with their wives and girlfriends at a "fishing event".

Seeing the suspected members of the Koobface gang travelling together—even with their families, is a re-occurring pattern throughout many of the photo albums shared by them.

One of their documented tours shows them on a journey through Europe visiting Spain, Nice, Monte Carlo and ultimately ending in a casino in Baden-Baden, Germany—most likely gambling with the money stolen from their victims.

Roman K., Svyatoslav P., Alexander K., Anton K. and Stanislav A. Living the life of the rich and famous.



It's important, of course, to recognise that the individuals identified above have not been charged in relation to Koobface, and have not been found guilty of any crimes.

The full evidence is in the hands of the law enforcement agencies, and we wait to see what—if any—actions are taken to bring down the Koobface gang.

Thanks:

The authors of this investigation would like to thank people from different organisations for the joint effort collecting information about the Koobface threat, especially:

- Facebook Security Team
- Gary Warner - UAB Center for Information Assurance and Joint Forensics Research
- Claudio Guarnieri - iSIGHT Partners
- Trend Micro Threat Research
- Infowar Monitor
- Thomas from CERT-Bund
- CSIS Security Group A/S
- and various law enforcement agencies around the globe.

Further reading:

Naked Security's Paul Ducklin answers some questions about the Koobface virus:
http://nakedsecurity.sophos.com/questions-and-answers-about-koobface/

Koobface: Inside a Crimeware Network [PDF]

The Real Face of Koobface: The Largest Web 2.0 Botnet Explained [PDF]

The Heart of Koobface: C&C and Social Network Propagation [PDF]

Web 2.0 Botnet: Koobface Revisited [PDF]

More Traffic, More Money: Koobface Draws More Blood [PDF]

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

A Sophos Article 1.12v1.dNA

SOPHOS