KOOBFACE:

Inside a Crimeware Network

JR04-2010

By NART VILLENEUVE

with a foreword by
Ron Deibert and Rafal Rohozinski

November 12, 2010

MUNK
SCHOOL
OF
GLOBAL
AFFAIRS

TheSecDevGroup

INFOWAR
MONITOR

WEB VERSION. Also found here:
http://www.infowar-monitor.net/koobface

Foreword

There is an episode of Star Trek in which Captain Kirk and Spock are confronted by their evil doppelgängers who are identical in every way except for their more nefarious, diabolical character.

The social networking community Facebook has just such an evil doppelgänger, and it is called Koobface. Ever since the Internet emerged from the world of academia and into the world-of-the-rest-of-us, its growth trajectory has been shadowed by the emergence of a grey economy that has thrived on the opportunities for enrichment that an open, globally connected infrastructure has made possible.

In the early years, cybercrime was clumsy, consisting mostly of extortion rackets that leveraged blunt computer network attacks against online casinos or pornography sites to extract funds from frustrated owners.

Over time, it has become more sophisticated, more precise: like muggings morphing into rare art theft. The tools of the trade have been increasingly refined, levering ingenuous and constantly evolving malicious software (or malware) with tens of thousands of silently infected computers to hide tracks and steal credentials, like credit card data and passwords, from millions of unsuspecting individuals.

It has become one of the world economy's largest growth sectors—Russian, Chinese, and Israeli gangs are now joined by upstarts from Brazil, Thailand, and Nigeria—all of whom recognize that in the globally connected world, cyberspace offers stealthy and instant means for enrichment.

Affecting a digital break-in of a Manhattan victim at the speed of light from the slums of Lagos, or the terminal greyness of Kamchatka, is elegant and rewarding—certainly more so than pulling a knife in the slums for a fist full of cash.

It is a lot less risky too. Cybercrime has elicited so little prosecution from the world's law enforcement agencies that it makes one wonder if a de facto decriminalization has occurred. Not surprisingly, it is seen as a safe yet challenging way out of structural economic inequality by the burgeoning number of educated young coders of the underdeveloped world. Sitting in front of a glowing monitor thousands of miles away from the actual victims, practically immune from the reach of the law, it must feel more like a virtual crime—but one with real rewards.

Cybercrime thrives not just because of ingenuity and lawlessness, but also because of social media opportunities. Koobface (an anagram of Facebook) succeeds by mimicking normal social networking behavior. It is like a digital amoeba, living parasitically on our sharing habits. It leverages the most successful of all age-old criminal techniques—our readiness to extend trust—with our eagerness to click on links. We have become conditioned into a world of intense social interaction. We click on web site addresses and documents like mice clicking on pellet dispensers. And it is that conditioned tendency that Koobface exploits with precision.

We undertook this investigation as a continuation of our work on cyber espionage that began with *Tracking GhostNet* and *Shadows in the Cloud*. In both cases, we found that the attackers' systems were built upon off-the-shelf crimeware code and tradecraft, readily obtained and applied either by state-based actors or commissioned from criminals all too ready to serve as privateers to sell their wares to the highest bidder.

We were intrigued: if the criminal merchants of code were ready to engage in the high-end of the exploitation market—breaking into government systems to obtain sensitive documents—then what was going on in the streets, and the myriad of globalized pathways of cyberspace which now connect over two thirds of humanity?

As with those earlier cases, our lead technical researcher Nart Villeneuve was able to take advantage of mistakes made on the part of the attackers to secure their own infrastructure; our access was almost comprehensive, allowing us insight into their inner workings for a period of months.

What we found with Koobface gave us pause: clearly cybercrime is profitable, but equally clearly, there is little incentive or even basis for our existing institutions of policing to do much about it.

The entrée point for Koobface is almost irresistible: a link sent from a fake "friend" prompting a visit to a video site that purportedly reveals the recipient captured naked from a hidden web cam. Who wouldn't follow that link? But for the hapless recipient, that one click leads down a Kafka-esque rabbit hole of viruses and Trojan horses, and straight into the tentacles of the Koobface network.

The mechanisms put in place by Koobface operators to generate revenue walk a very fine line, and are at times so subtle that it is difficult, if not impossible to identify who, if anyone, is actually a victim.

Although our investigation determined the Koobface gang drew revenues of over US$2 million a year, the combined earnings were derived from thousands of individual micro-transactions on the order of a fraction of a penny each, spread across victims in dozens of national jurisdictions. Each commandeered computer that clicked on an online ad or downloaded a fake anti-virus package generated a cut for the gang. So meticulous were the attackers that they created an automatic text message alert to themselves each day summing up their spoils.

Without a victim, particularly a complainant, it is almost impossible for a police force to justify the resources to investigate a case like Koobface. Police officers ask: what's the crime? Prosecutors ask: what or whom am I supposed to prosecute? In the case of Koobface, it is almost as if the system were purposefully designed to fall between the cracks of both questions.

Even more debilitating is the international character of Koobface. Cybercrime networks succeed by hiding locally while leveraging a global infrastructure. Electrons may move at speed of light, but legal systems move at the speed of bureaucratic institutions, especially across national borders. Living in St. Petersburg, Russia, the Koobface gang might as well be living on Mars, so poorly developed are the mechanisms of international law enforcement cooperation.

Although we turned over the entire Koobface database we acquired as evidence to Canadian law enforcement, including evidence identifying the individuals behind it, we were not surprised that there has been no arrest or prosecution, for the reasons listed above.

We also worked with the broader security community who had studied Koobface to notify the hosting companies and service providers upon which Koobface had built its malignant enterprise: some 500,000 fraudulent Google blogger and Gmail accounts, and 20,000 Facebook accounts. The action to disable these accounts will temporarily bring the network to its knees, but not terminate it. Koobface will surely live to see another day as long as the individuals behind it roam free.

Some may argue Koobface earned its operators a few million dollars on a nearly victimless crime. Is that really something that warrants concerted international policing and attention? Maybe not. But here it is important to understand the broader ecosystem of which Koobface is just one small example.

A recent study by Bell Canada suggested that CA$100 billion out of $174 billion of revenue transiting Canada's telecommunications infrastructure is "at risk." The same operator measured over 80,000 "zero day" attacks per day targeting computers on its network—meaning, attacks that are so new the security companies have yet to register them. These are staggering figures, which if translated into physical terms—bank robberies and break-ins—would be prompting politicians into immediate action.

There is another element of that which Koobface represents that should give us even more pause. The Koobface gang had a certain charm and ethical restraint. They communicated with security researchers about their intents and their desire not to do major harm. They limited their crimes to petty fraud, albeit massive in scale and scope. But the scary part is that they could have easily done otherwise.

Thousands of compromised computers networked together with an invisible tether controlled by a few individuals can be employed to extract pennies from unsuspecting victims, as it was with Koobface, or sensitive national security documents from government agencies, as it was with *GhostNet* and *Shadows*. It can be used to direct computers to click on fake advertisements for Viagra or marshal them together to attack a meddlesome human rights website, as it is with increasing frequency from Iran and Kazakhstan to Burma and Vietnam.

Criminal networks such as these are growing as fast as the social networking platforms upon which they parasitically feed. Koobface is just one example of an entire ecosystem that threatens to put at risk the very entity on which it depends—a free and open cyberspace. How to clean up and control it, without undermining the positive characteristics of social networking we have all come to enjoy, is one of the major challenges of global security policy today.

Ron Deibert
Director, Canada Centre for Global Security Studies
and the Citizen Lab
Munk School of Global Affairs, University of Toronto

Rafal Rohozinski
CEO, The SecDev Group (Ottawa)
Senior Fellow, Canada Centre for Global Security Studies
Munk School of Global Affairs, University of Toronto

Acknowledgments

The Information Warfare Monitor (infowar-monitor.net) is a joint activity of the Citizen Lab, Munk School of Global Affairs, University of Toronto, and the SecDev Group, an operational consultancy based in Ottawa specialising in evidence-based research in countries and regions under threat of insecurity and violence. The blurring boundaries between cybercrime and cyber espionage that were explored in our previous *Tracking GhostNet* and *Shadows in the Cloud* reports led to an investigation that was undertaken to gain a better understanding of the malware ecosystem that enables and sustains both online criminals and cyber espionage networks. The Information Warfare Monitor wanted to follow due process with respect to law enforcement in order to educate ourselves further about the challenges posed by criminal organizations whose activities span multiple jurisdictions.

This report was made possible thanks to the guidance and encouragement of Ron Deibert and Rafal Rohozinski, the principal investigators of the Information Warfare Monitor. This report is built upon the research of members of the security community and I would like to thank all those who have documented the operations of Koobface over the years, especially Dancho Danchev and Trend Micro's Threat Research Team. I would like to acknowledge and thank Chris Davis and Jose Nazario for sharing their knowledge and providing advice. In addition, I would like to thank the RCMP, the FBI, the UK Police, and AusCERT for their assistance. Finally, a special thanks is due to Jan Droemer who discovered the same data and shared his analysis and insights.

The research of the Citizen Lab and the Information Warfare Monitor is supported by the Canada Centre for Global Security Studies (University of Toronto), a generous grant from the John D. and Catherine T. MacArthur Foundation, in-kind and staff contributions from the SecDev Group, and a generous donation of software from Palantir Technologies Inc. I am very grateful to Masashi Crete-Nishihata (Citizen Lab) for research assistance and to Jane Gowan (Agent 5 Design and Citizen Lab) for layout and design.

Author's Biography

Nart Villeneuve is the Chief Research Officer for SecDev.cyber and Psiphon Fellow at the Citizen Lab, Munk School of Global Affairs, University of Toronto, where he focuses on targeted malware attacks and politically-motivated distributed-denial-of-service attacks. Nart's technical investigations at the Information Warfare Monitor informed the discovery of two cyber espionage networks, GhostNet—which compromised diplomatic missions and ministries of foreign affairs around the world as well as the Dalai Lama's office, and the Shadow Network—which extracted secret, confidential, and restricted documents from the Indian government and military.

Nart is also the author of *Breaching Trust*, a report that discovered a surveillance network being operated by Skype and its Chinese partner, TOM Online, which captured millions of records, including contact details for any text, chat, and/or voice calls and the full text of sensitive chat messages.

Nart has testified before two United States congressional committees on China's Internet censorship and surveillance practices and corporate social responsibility. Nart is a graduate of the University of Toronto and the former Director of Technical Research at the Citizen Lab. As a part of the OpenNet Initiative, he analyzed the Internet filtering policies of over 40 countries and the methods used to bypass these restrictions.

Summary

Malicious actors are expanding their botnet operations by exploiting new propagation strategies and, in particular, have started to exploit Internet users by leveraging users' trust in social networking platforms. Botnet operators are able to obscure their activities by using countermeasures against efforts by the security community to understand their malware and shutdown their operations. Not only are botnet operators able to obscure the location of command and control servers by relying on compromised intermediaries, they are also using anti-malware products to determine whether their malware is detectable by security software in order to increase the chance that their malware will be able to slip past most defenses. Hence, although there is a wide variety of crime that occurs on the Internet, botnet creation is one of the most difficult to counter.

Botnet operations are conducted within a lucrative malware ecosystem that facilitates their expansion. In addition to contracting the services of other botnet operators to further propagate malware, cybercriminals rely on affiliate programs to enable profitable activities, such as defrauding advertisers and tricking Internet users into installing and purchasing fake security software. As a result, botnet operators are generating significant income from criminal activity.

From April to November 2010 the Information Warfare Monitor investigated the operations and monetization strategies of the Koobface botnet. We focused on Koobface because of its notorious misuse of social networking platforms that allows its operators to exploit the trust we have both in these platforms and in our friends that we use these platforms to communicate with. In addition, this investigation was undertaken in order to gain a better understanding of the malware ecosystem that enables and sustains cybercriminal activity.

Our botnet monitoring and research activities discovered a URL path on a well-known Koobface command and control server from which we were able to download archived copies of Koobface's command and control infrastructure. The contents of these archives revealed the malware, code, and database used to maintain Koobface. It also revealed information about Koobface's affiliate programs and monetization strategies. While the technical aspects of the Koobface malware have been well-documented, this report focuses on the inner workings of the Koobface botnet with an emphasis on propagation strategies, security measures, and Koobface's business model.

Koobface maintains a system that uses social networking platforms, such as Bebo, Facebook, Friendster, Fubar, Hi5, MySpace, Netlog, Tagged, Twitter, and Yearbook, to send malicious links. Malicious links to Blogspot blogs (often disguised by bit.ly's URL service) redirect users to false YouTube pages that are hosted on compromised Web servers. Koobface exploits Internet users' trust in these systems in order to trick users into installing malware. Koobface also leverages connections to other malware groups to propagate and has been found spreading in connection with botnets associated with Bredolab, Gumblar, Meredrop, and Piptea.

Koobface relies on a network of compromised servers that are used to relay connections from compromised computers to the Koobface command and control server. This tiered infrastructure makes it difficult to investigate and disrupt the operations of the botnet. The Koobface operators also employ counter-measures against security efforts to counter their operations. In addition to maintaining a "banlist" of Internet protocol addresses that are forbidden from accessing Koobface servers, Koobface operators carefully monitor whether any of their URLs have been flagged as malicious by bit.ly, Facebook, or Google.

The operators of Koobface have been able to successfully monetize their operations. Through the use of pay-per-click and pay-per-install affiliate programs, Koobface was able to earn over US$2 million between June 2009 and June 2010 by forcing compromised computers to install malicious software and engage in click fraud.

It is difficult to counter botnet operations because botnet operators employ technical countermeasures and leverage geography to their benefit. This makes it difficult to coordinate law enforcement and takedown efforts. In addition, while it is clear that the totality of the criminal activity by the botnet operators is significant, each criminal act is spread across multiple jurisdictions. As a result, the total amount of criminal activity in any one *local* jurisdiction is less significant than the *global* whole. Without an understanding of their operations as a whole, Koobface is unlikely to attract significant attention.

This investigation provides a glimpse of the inner workings of crimeware networks and contributes to the ongoing efforts to protect Internet users from malware attacks. It also demonstrates that it is possible to leverage the mistakes made by botnet operators in order to better understand the scope of their operations.

Table of Contents

Introduction

There are numerous computer systems around the world that are under the control of malicious actors. These compromised computers, often known as zombies, form a botnet that receives and executes commands from botnet operators who harvest passwords, credit card numbers, and sensitive information from the zombies.[1] Botnet operators also put the "zombies" to work by forcing them to send spam messages, create fraudulent accounts, and host malicious files. Rather than relying on sophisticated technical exploits, some botnet operators simply trick users into compromising themselves. Through fake Web sites, users are encouraged to download malicious software masquerading as benign. Sometimes, these fake, malicious Web sites are sent to users by their contacts on social networking sites. The rise of social networking tools has given attackers a platform to exploit the trust that individuals have in one another. People are much more likely to execute a malicious file if it has been sent to them by someone they know and trust.[2] The information that individuals post online and the interests contained within their profile information can also be used to lure individuals into executing malicious software.

Koobface is a botnet that leverages social networking platforms to propagate. The operators of the botnet (known as Ali Baba and 40 LLC) have developed a system that uses social networking platforms, such as Bebo, Facebook, Friendster, Fubar, Hi5, MySpace, Netlog, Tagged, Twitter, and Yearbook, to send messages containing malicious links. These links are often concealed using the URL shortening service bit.ly and sometimes redirects to Blogspot blogs that redirect users to false YouTube pages hosted on compromised Web servers. These pages encourage users to download malicious software masquerading as a video codec or a software upgrade.[3] Koobface also uses search engine optimization (SEO) techniques that allow these malicious sites to be listed highly in search engine results for popular search terms.[4]

In order to propagate malware using Blogspot, Facebook, and Google accounts, Koobface uses social engineering to convince the owners of compromised computers to solve CAPTCHAs. This allows the botnet operators to create fraudulent accounts.[5] The abuse of social networking tools is a critical component of Koobface's propagation efforts.

Botnet operators are increasingly implementing measures to counter the security community's anti-malware

[1] Jaideep Chandrashekar et al., "The Dark Cloud: Understanding and Defending Against Botnets and Stealthy Malware," *Intel Technology Journal* 13, no.2 (2009).

[2] Tom N. Jagatic et al., "Social Phishing," *Communications of the ACM* 50, iss.10 (2007), accessed October 4, 2010, http://portal.acm.org/citation.cfm?id=1290958.1290968&coll=GUIDE&dl=GUIDE&CFID=74760848&CFTOKEN=96817982.

[3] Jonell Baltazar, Joey Costoya, and Ryan Flores, "The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained," *TrendWatch*, July 2009, accessed October 4, 2010, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf; Jonell Baltazar, Joey Costoya, and Ryan Flores, "The Heart of KOOBFACE: C&C and Social Network Propagation," *TrendWatch*, October 2009, accessed October 4, 2010, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf; Jonell Baltazar, Joey Costoya, and Ryan Flores, "Show Me the Money! The Monetization of KOOBFACE," *Trend Watch*, November 2009, accessed October 4, 2010, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/koobface_part3_showmethemoney.pdf; and Jonell Baltazar, "Web 2.0 Botnet Evolution: KOOBFACE Revisited," *TrendWatch*, May 2010, accessed October 4, 2010, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/web_2_0_botnet_evolution_-_koobface_revisited__may_2010_.pdf.

[4] Phil Hay, "Malicious LinkedIn Campaigns Continue," *M86 Security Labs Blog*, September 30, 2010, http://www.finjan.com/MCRCblog.aspx?EntryId=2317.

[5] Ibid.; and Jason Zhang, "CAPTCHAs – Breaking into the Shadow Economy," *MessageLabs Intelligence*, July 15, 2010, http://www.symantec.com/connect/es/blogs/captchas-breaking-shadow-economy.

efforts.[6] Koobface has created a "banlist" of IP addresses that are forbidden from accessing Koobface servers. Koobface also monitors their malware links with the Google Safe Browsing API and checks whether their URLs have been flagged as malicious by bit.ly or Facebook.[7] Using these techniques, Koobface is able to stay one step ahead of the security community.

Koobface exists within a malware ecosystem designed to maintain the operations of botnets. The malware ecosystem consists of buyers and sellers of malicious software, stolen data and, increasingly, services. All of the tools and infrastructure required to maintain a botnet are available for purchase in the malware ecosystem.[8] Botnets are, as a consequence, playing an increasingly critical role in the malware ecosystem:

> It's botnets which unite all the disparate elements of cybercrime into an integrated system, and make it possible to transfer funds from those who make a profit from mass mailings and credit card thefts to malware writers and those who supply cybercriminal services.[9]

Botnet operators also rely on each other to support their operations. Koobface leverages connections to other malware groups in order to propagate and has been found spreading in connection with botnets associated with Bredolab, Meredrop, and Piptea.[10] Koobface has also been found propagating in connection with Gumblar[11] and has been hosted on a Gumblar-related server in the past.[12] These relationships allow Koobface to maintain a large network of compromised computers and spread through a variety of mechanisms other than social networks.

Botnets require a command and control infrastructure in order to maintain and manage a network of compromised computers. Consequently, botnet operators must rent or acquire servers for this purpose. There are a variety of crime-friendly hosting services that are known as "bullet proof" hosting because they protect their clients from abuse complaints and takedown requests.[13] The use of these crime-friendly services makes it very difficult to take down the botnet as providers will resist requests to disable botnet-related servers.[14] For instance, we discovered a file on a Koobface server that contained details of two complaints made about Koobface's activities. It appears that one of Koobface's previous hosting providers had forwarded complaints from the security community directly to the operators of Koobface. Koobface appears to rely on at least one crimeware host known as MiraxNetworks.[15]

Ultimately, operators of botnets, including Koobface, seek to monetize their activities through a variety of

[6] Brian Krebs, "Services Let Malware Purveyors Check Their Web Reputation," *Krebs on Security*, July 26, 2010, http://krebsonsecurity.com/2010/07/services-let-malware-purveyors-check-their-web-reputation.

[7] Koobface's use of these techniques is part of a trend in which malware is checked against a variety of security products in order to counter blocking and takedown efforts by the security community, see: Krebs, "Services Let Malware Purveyors Check Their Web Reputation."

[8] Alvaro A. Cardenas et al., "An Economic Map of Cybercrime" (working paper presented at the 37th Research Conference on Communication, Information and Internet Policy, Arlington, VA, September 25-27, 2010).

[9] Vitaly Kamluk, "The Botnet Ecosystem," *Secure List*, December 17, 2009. http://www.securelist.com/en/analysis?pubid=204792095.

[10] Atif Mushtaq, "Killing the Beast…Part II," *FireEye Malware Intelligence Lab*, June 17, 2009, http://blog.fireeye.com/research/2009/06/killing-the-beastpart-ii.html.

[11] Andrew Martin, "Inside the Massive Gumblar Attack," *Viewing InfoSec from the Trenches*, May 21 2009, http://www.martinsecurity.net/2009/05/20/inside-the-massive-gumblar-attacka-dentro-del-enorme-ataque-gumblar.

[12] Dancho Danchev, "Koobface – Come Out, Come Out, Wherever You Are," Dancho Danchev's Blog – *Mind Streams of Information Security Knowledge*, July 2, 2009, http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html.

[13] Alvaro A. Cardenas et al., "An Economic Map of Cybercrime."

[14] Ibid.

[15] See Part 2 of this report.

methods, including pay-per-click (PPC) fraud and pay-per-install (PPI) schemes.[16] PPC refers to a model in which webmasters display third-party advertisements on their Web sites and earn income whenever Internet users click on these advertisement links. PPI refers to a model in which the software of one company is promoted by a third party who is paid every time an Internet user installs the software. While there are legitimate users of these models for online advertising, online criminals have long sought to defraud such advertisers or use these models to install spyware and malware on compromised computers. Benjamin Edelman, a Professor at the Harvard Business School who has studied a variety of click fraud schemes, explains:

> More generally, it's easy to write software to fake a click – to make a user's computer request a paid search ad, as if the user had clicked the ad link, when the user did no such thing. Tens of millions of computers are infected with botnets that can fake ad clicks, and these infections have proven remarkably difficult to eradicate.[17]

Because botnet operators have numerous computers under their control, they can easily force compromised computers to click on advertisements or install malicious software. In addition to click fraud, botnet operators also leverage affiliate networks to earn income from PPC and PPI networks that advertise their own, often fake, products.[18]

Some of the most common PPI affiliate networks are those that pay for successful installations of fake Internet security software known as rogue security software. These software products purport to be legitimate security software, such as anti-virus programs, and use scare tactics to convince users to purchase the software. However, the software provides little to no actual security.[19] The software costs US$30.00 to $100.00 and has proven to be a very profitable enterprise, with affiliates earning 58 to 90 percent commission on sales of the software.[20]

Unlike other botnets, such as those that rely on the ZeuS malware, Koobface does not steal banking and credit card information from compromised computers.[21] In fact, in a message to the security community, the Koobface operators claimed that they would never steal such information:

> As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER.[22]

Despite this promise, Koobface has added a component that does steal password information relating to e-mail, instant messaging, file transfer protocol (FTP), and Facebook accounts. However, this appears to be an effort to

[16] Trend Micro Incorporated, "Unmasking Fake AV," *TrendWatch*, June 2010, accessed October 4, 2010, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/unmasking_fakeav__june_2010_.pdf.

[17] Benjamin Edelman, "The Dark Underbelly of Online Advertising," *HBR Now*, November 17, 2009, http://blogs.hbr.org/hbr/hbr-now/2009/11/dark-underbelly-of-online-ads.html.

[18] Dmitry Samosseiko, "The Partnerka – What is it, and why should you care?" (paper presented at the Virus Bulletin Conference, Geneva, Switzerland, September 2009).

[19] Trend Micro Incorporated, "Unmasking Fake AV."

[20] Symantec Corporation, "Symantec Report on Rogue Security Software July 08 – June 09," *Symantec Enterprise Security*, October 2009, accessed October 4, 2010, http://www4.symantec.com/Vrt/wl?tu_id=XuOB125692283892572210; and Joe Stewart, "Rogue Antivirus Dissected – Part 2," *SecureWorks*, October 22, 2008, accessed October 4, 2010, http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2.

[21] Ponemon Institute, "Growing Risk of Advanced Treats: Study of IT Practitioners in the United States," *NetWitness*, June 30, 2010, accessed October 4, 2010, http://www.netwitness.com/resources/kneber.aspx; AVG Technologies, The "Mumba" Botnet Disclosed, *AVG*, August 2010, accessed 4 October 2010, http://www.avg.com.au/files/media/avg_white_paper_mumba_botnet_02-aug-10.pdf; and Nart Villeneuve, "The Ambler Botnet," Nart Villenueve: *Internet Censorship Explorer*, August 4, 2010, http://www.nartv.org/2010/08/04/the-ambler-botnet.

[22] Dancho Danchev, "The Koobface Gang Wishes the Industry "Happy Holidays"," *Dancho Danchev's Blog – Mind Streams of Information Security Knowledge*, December 26, 2009, http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html.

facilitate propagation rather than monetization since Koobface monetizes their operations through PPC and PPI. The operators of Koobface have been able to setup a stable botnet infrastructure that allows them to maintain tens of thousands of compromised computers and profit immensely from PPC and PPI, earning a total of $2,067,682.69 between June 23, 2009 and June 10, 2010.

Outline of report

This report consists of three parts:

- **Part one** describes the operation of the Koobface botnet including its propagation strategies, command and control infrastructure, and the ways in which the Koobface operators monitor their system and employ counter-measures against the security community.
- **Part two** details the ways in which the Koobface operators monetize their activities and provides an analysis of Koobface's financial records. It details the affiliate relationships that Koobface maintains with PPC brokers and rogue security software vendors.
- **Part three** describes the challenges that the law enforcement and security community face in dealing with the threats posed by botnets such as Koobface.

PART 1:
THE BOTNET

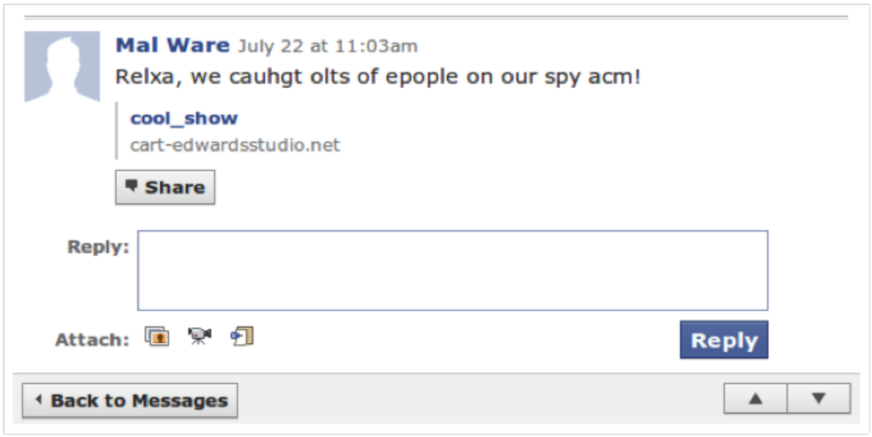
Part 1: The Botnet

In order to sustain a monetization strategy that relies upon click fraud and rogue security software, the Koobface botnet has been designed to continually propagate by exploiting Internet users' trust in social networking platforms. This propagation strategy relies upon URL shortening services (such as bit.ly) and Blogspot blogs in order to disguise malicious links. Koobface instructs compromised computers to send messages containing malicious links to friends on Facebook and uses compromised computers to create fraudulent Google and Facebook accounts. In addition, Web sites that host the Koobface malware, as well as servers that the malware connects to once a new victim has been compromised, are actually compromised intermediaries themselves. Koobface obscures its main command and control servers by using compromised FTP credentials in order to turn ordinary Web servers into relays used for command and control. The Koobface operators monitor their infrastructure to ensure that it is functioning correctly and to counter efforts by the security community that disrupt their operations.

Propagation

Koobface spreads through social networking platforms by using credentials on compromised computers to login to the victim's account and send messages that contain links to malware to friends that are linked to the account. Koobface targets a variety of social networking platforms, including Bebo, Friendster, Fubar, Hi5, MySpace, Netlog, Tagged, Twitter, and Yearbook. However, it has primarily focused on Facebook. Typically, a user's first encounter with Koobface is a Facebook message from a friend that contains a malicious link (see figure 1).

FIGURE 1:
An example of a message sent by Koobface to a compromised user's Facebook friends.

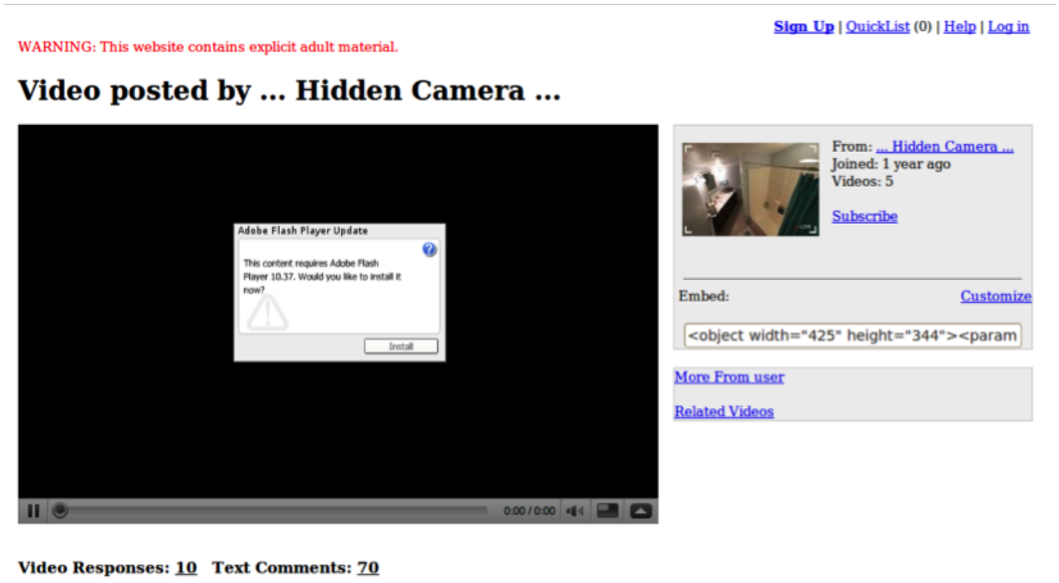


Mal Ware July 22 at 11:03am
Relxa, we cauhgt olts of epople on our spy acm!

cool_show
cart-edwardsstudio.net

The malicious link is often concealed using the URL shortening service bit.ly and sometimes redirects once again through a Blogspot blog to a malicious Web page that encourages the user to run the accompanying executable. Koobface has experimented with other mechanisms including Google Buzz and Google Reader. Often, these malicious pages purport to be YouTube pages that require a new codec or an Adobe Flash upgrade in order to view the video (see figure 2).

FIGURE 2: A fake YouTube page that Koobface uses to trick users into installing malware.



WARNING: This website contains explicit adult material.

Video posted by ... Hidden Camera ...

Adobe Flash Player Update

This content requires Adobe Flash Player 10.37. Would you like to install it now?

From: ... Hidden Camera ...
Joined: 1 year ago
Videos: 5

Embed: <object width="425" height="344"><param

Video Responses: 10 Text Comments: 70

The executable is actually the Koobface loader that gives the botnet operators control over the user's computer. Once compromised, the newly infected computer becomes part of the operations of the Koobface botnet and the user's friends are sent malicious messages. This cycle provides Koobface with a constant supply of new victims.

Infrastructure

Koobface maintains an infrastructure that integrates command and control capabilities (including zombie proxies that obscure the location of the command and control server), "landing pages" that encourage users to download malware (including bit.ly and Blogspot links used for redirection), a "mothership" for click fraud services, an installation tracker, a backup server, drop zones for stolen credentials, and a server known as "The Offis," from which the operators test their infrastructure.

- Command and Control: 85.13.206.115 (Coreix, GB); u07012010u.com (ofuztocxeaebmx@gmail.com)
- PPC/PPI Mothership: 85.13.236.154 (Coreix, GB); ze-biz.com (contact@privacyprotect.org)
- Install Tracker: 78.108.178.44 (UPL, CZ); babkiup.com (master@cookingluck.com)
- Backup Server: 95.143.192.205 (Servainet, SE); *.23sachenbacher02.com (contact@privacyprotect.org)
- Dropzones: 117.41.181.129 (CHINANET-JX, CN); insta-find.com (bigvillyxxx@gmail.com) and xtsd20090815.com (bigvillyxxx@gmail.com)
- The Offis: 85.13.200.59 (Coreix, GB) (and 85.13.200.58, 77.239.243.224, 93.190.141.160, 209.200.6.208, 93.190.142.49)

Command and Control

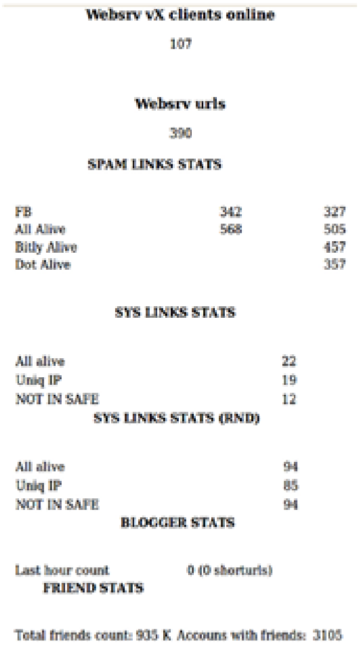
Koobface's main command and control server is hosted on 85.13.206.115 (Coreix, GB) and uses the domain name u07012010u.com (ofuztocxeaebmx@gmail.com). This server is the main component of the Koobface infrastructure. The Koobface command and control server maintains a database that contains information on the infrastructure of the Koobface botnet, including compromised hosts that have been turned into relays and used by the operators to proxy requests to the command and control server.

Based on data extracted from the Koobface command and control database, Koobface maintains a number of fraudulent accounts with third party services:

- 21,790 Facebook Accounts
  - Total friends count: 935,000/Accounts with friends: 3105
- 350,854 Total Blogger Accounts
- 522,633 Total Google Accounts
- 4,842 Google Reader Accounts
- 4,044 100mb Accounts

Koobface also appears to use compromised computers to host landing pages (pages from which the malware is downloaded) as well as compromised Web servers that are used as relays to proxy traffic from compromised computers to the command and control server. The live numbers associated with these Web servers and relays fluctuate significantly (see figure 3).

FIGURE 3: A screenshot of Koobface's statistics interface.



```
           Websrv vX clients online
                     107

                 Websrv urls
                     390
            SPAM LINKS STATS

FB                         342          327
All Alive                  568          505
Bitly Alive                             457
Dot Alive                               357

              SYS LINKS STATS

All alive                        22
Uniq IP                          19
NOT IN SAFE                      12
           SYS LINKS STATS (RND)

All alive                        94
Uniq IP                          85
NOT IN SAFE                      94
              BLOGGER STATS

Last hour count          0 (0 shorturls)
     FRIEND STATS

Total friends count: 935 K  Accouns with friends:  3105
```

The Koobface malware has a modular structure that allows the botnet operators to install additional components on compromised computers based on specific criteria. After the loader is successfully executed, the compromised computer connects to one of Koobface's relay Web servers, which act as proxies to the Koobface command and control server. The malware on the compromised host requests URLs that contain parameters which elicits responses from the Koobface command and control server.

"fbgen"

The relay proxy server receives the "fbgen" parameter from the compromised host and connects to a PHP file on the Koobface command and control server. This file determines the contents of the message and the Koobface URL to send to the Facebook friends associated with Facebook accounts found on the compromised computer. There are three main commands: "s," which sets the number of messages per target and reports the compromised hosts IP address; "m," which generates the title, text, and link to be sent to the user's Facebook friends; and "w," which instructs the compromised computer to wait.

"ldgen"

The relay proxy server receives the "ldgen" parameter from the compromised computer and connects to a PHP file on the Koobface command and control server. This file determines what further binaries the compromised host will download from the command and control server. If the compromised host has an IP address in a range assigned to Australia, Austria, Belgium, Canada, China, Denmark, France, Iceland, Italy, Ireland, Germany, Great Britain, The Netherlands, New Zealand, Norway, Puerto Rico, South Africa, Spain, Sweden, or The United States, Koobface will download p.exe, the search engine hijacker and dogma.exe, the binary for the affiliate program at dogmamillions.com.

If the compromised host has an IP address assigned to the United States, Koobface will download st934.exe, a RogueAV software, from the "weber" affiliate at affiliates.sftmasters.com. Based on a random number, Koobface will also download Koobface components v2newblogger.exe and v2bloggerjs.exe, which are responsible for creating new blogger.com accounts used in Koobface spam campaigns.

Next, Koobface instructs the compromised computers to download hostsgb3.exe, which modifies the HOST file on the compromised computers; migdal.org.il.exe (the filename changes with new domain names); an FTP credentials grabber (LDPINCH); and ws.exe, which installs a Web server for Koobface's use on the compromised computer. Finally, if Internet Explorer is not the default browser, Koobface will download gr.12.exe, which creates fraudulent Facebook accounts.

"ppgen"

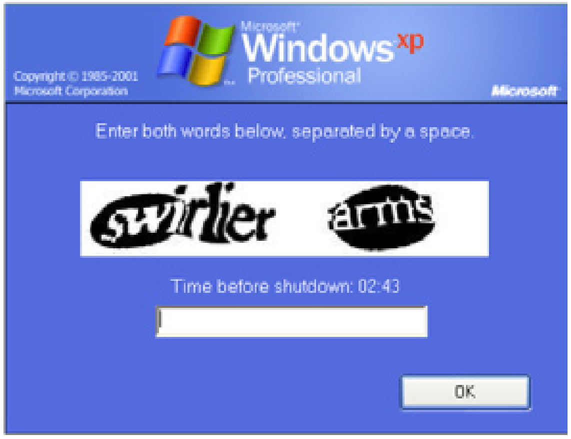
The relay proxy server receives the "ppgen" parameter from the compromised computer and connects to a PHP file on the Koobface command and control server. This file generates URLs that are used to create pop-up windows on the compromised computer. These URLs point to rogue security software affiliates on Google searches for keywords such as "antivirus," "best + spyware + remover," and "adware + spyware + removal," which triggers the search hijacker when the user clicks on any of the links returned by Google.

"CAPTCHA"

Koobface tasks compromised computers with creating fake Google and Blogspot accounts. Koobface uses random samplings of real Facebook profile information stolen from compromised accounts to create fictitious accounts. When presented with a CAPTCHA during the account creation process, Koobface causes a popup window to open on a compromised computer. The popup window suggests that the computer will shutdown if the CAPTCHA is not solved. When users solve the CAPTCHA, Koobface successfully creates a fictitious account.

The relay proxy server receives the "CAPTCHA" parameter from the compromised computer and connects to a PHP file on the Koobface command and control server. This file selects a CAPTCHA image from the database and passes the image back to the compromised computer.

FIGURE 4:
A screenshot of a Koobface popup that appears on compromised computers used to trick users into solving a CAPTCHA.


Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
Enter both words below, separated by a space.
swirlier arms
Time before shutdown: 02:43
OK

A popup window asks the compromised user to solve the CAPTCHA and indicates that the computer will shutdown if the user does not do so within a specified time period (see figure 4). The solved CAPTCHA is then relayed back to the command and control server so that an account, usually Facebook or Google, can be created.

Data Theft

With the introduction of an additional malware component LDPINCH, Koobface now steals credentials for a variety of accounts, including Web, FTP, instant messaging, and e-mail. Koobface has processing scripts to explicitly collect user names and passwords for FTP clients, such as Core FTP, CuteFTP, FileZilla, FlashFXP, SmartFTP, Windows Total Commander, WinSCP; IM clients, such as FreeCall, Google_Talk, ICQ2003 Lite, MSN Messenger, Paltalk, PSI, QIP, Windows Live Messenger, and Yahoo! Messenger; and mail clients and providers, such as IncrediMail, Outlook, and Windows Live Mail.

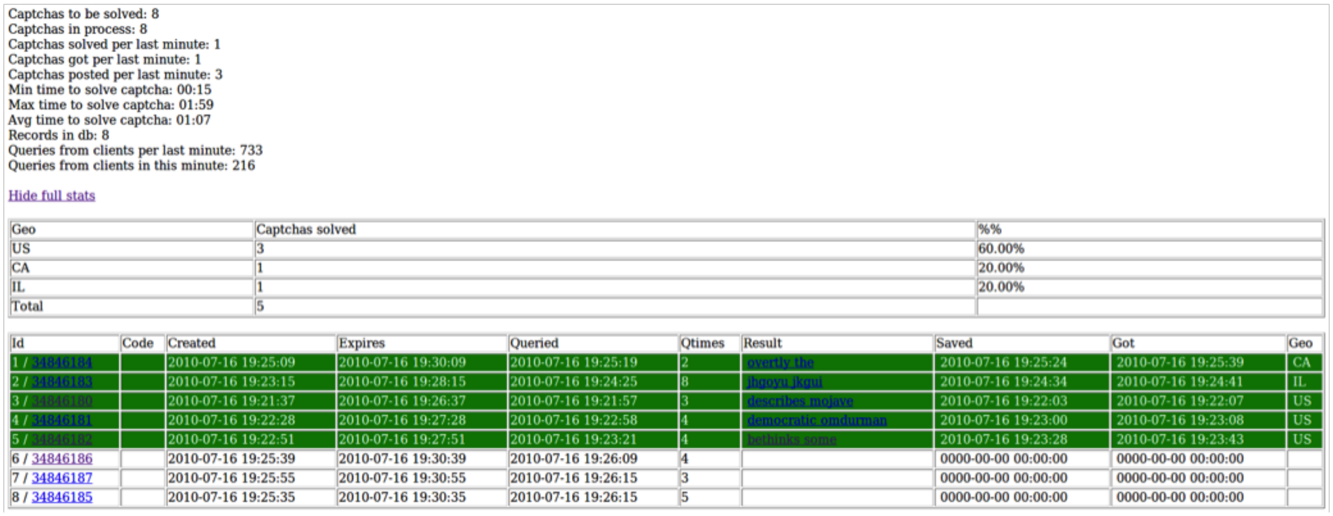
Monitoring & Countermeasures

The operators of the Koobface botnet have a system in place to monitor the operations of the botnet and to ensure that the system continues to maintain the infrastructure that is required to operate it. The Koobface operators have also created a variety of statistics pages that allow the operators to monitor the overall statistics as well as the speed and availability of the Web servers that host their landing pages.

In addition to monitoring the availability of the Web servers, Koobface also checks to ensure that the most recent versions of the malware loader are present along with the most recent landing pages.

Koobface also has an interface to monitor their CAPTCHA breaking system (see figure 5). Creating fraudulent accounts is an important component of Koobface's propagation strategy. This interface allows the operators to ensure that the system is functioning.

FIGURE 5: A screenshot of Koobface's statistics page for its CAPTCHA breaking system.



Captchas to be solved: 8
Captchas in process: 8
Captchas solved per last minute: 1
Captchas got per last minute: 1
Captchas posted per last minute: 3
Min time to solve captcha: 00:15
Max time to solve captcha: 01:59
Avg time to solve captcha: 01:07
Records in db: 8
Queries from clients per last minute: 733
Queries from clients in this minute: 216

Hide full stats

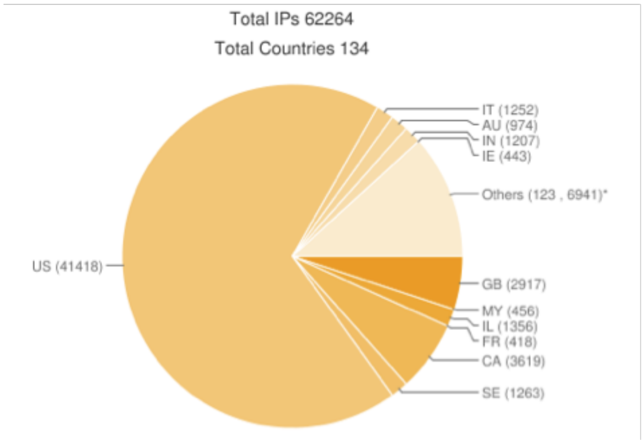
Geo	Captchas solved	%%
US	3	60.00%
CA	1	20.00%
IL	1	20.00%
Total	5	

Id	Code	Created	Expires	Queried	Qtimes	Result	Saved	Got	Geo
1 / 34846184		2010-07-16 19:25:09	2010-07-16 19:30:09	2010-07-16 19:25:19	2	overtly the	2010-07-16 19:25:24	2010-07-16 19:25:39	CA
2 / 34846183		2010-07-16 19:23:15	2010-07-16 19:28:15	2010-07-16 19:24:25	8	jhgoyu jkgui	2010-07-16 19:24:34	2010-07-16 19:24:41	IL
3 / 34846180		2010-07-16 19:21:37	2010-07-16 19:26:37	2010-07-16 19:21:57	3	describes mojave	2010-07-16 19:22:03	2010-07-16 19:22:07	US
4 / 34846181		2010-07-16 19:22:28	2010-07-16 19:27:28	2010-07-16 19:22:58	4	democratic omdurman	2010-07-16 19:23:00	2010-07-16 19:23:08	US
5 / 34846182		2010-07-16 19:22:51	2010-07-16 19:27:51	2010-07-16 19:23:21	4	bethinks some	2010-07-16 19:23:28	2010-07-16 19:23:43	US
6 / 34846186		2010-07-16 19:25:39	2010-07-16 19:30:39	2010-07-16 19:26:09	4		0000-00-00 00:00:00	0000-00-00 00:00:00	
7 / 34846187		2010-07-16 19:25:55	2010-07-16 19:30:55	2010-07-16 19:26:15	3		0000-00-00 00:00:00	0000-00-00 00:00:00	
8 / 34846185		2010-07-16 19:25:35	2010-07-16 19:30:35	2010-07-16 19:26:15	5		0000-00-00 00:00:00	0000-00-00 00:00:00	

Koobface relies on bit.ly links, Blogspot blogs, and Web servers to operate effectively. Koobface's ability to compromise new victims is affected when these components are reported as malicious. Therefore, Koobface carefully monitors these links through the Google Safe Browsing API and checks if any of their URLs have been flagged as malicious by bit.ly or Facebook.

Koobface maintains a banlist of IP addresses that are forbidden from accessing servers under Koobface's control. The majority of the banned IP addresses are in the United States (see figure 6).

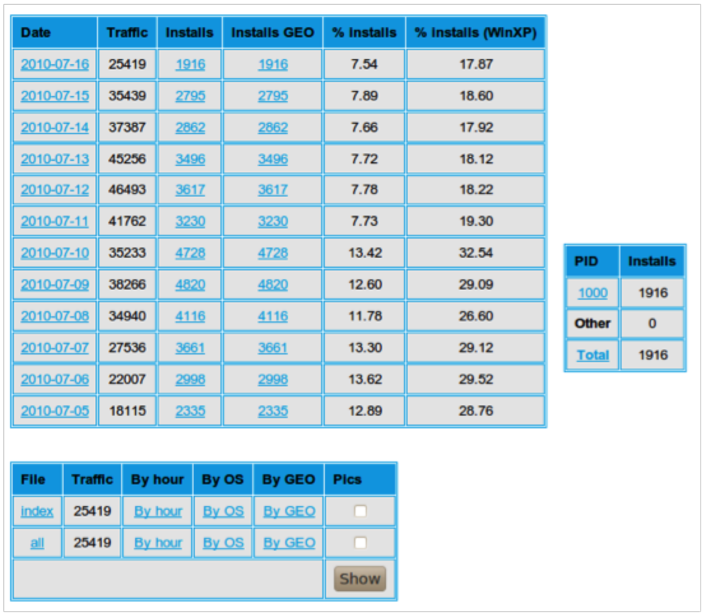
FIGURE 6: A geographical breakdown of the IP addresses banned from visiting Koobface infrastructure.



Monitoring Installations

Koobface keeps count of successful installations and traffic generated by the botnet (see figure 7). The Web site babkiup.com is used to synchronize records of Koobface installations across multiple servers.

FIGURE 7: A screenshot of Koobface's malware installation statistics page.



Date	Traffic	Installs	Installs GEO	% Installs	% Installs (WinXP)
2010-07-16	25419	1916	1916	7.54	17.87
2010-07-15	35439	2795	2795	7.89	18.60
2010-07-14	37387	2862	2862	7.66	17.92
2010-07-13	45256	3496	3496	7.72	18.12
2010-07-12	46493	3617	3617	7.78	18.22
2010-07-11	41762	3230	3230	7.73	19.30
2010-07-10	35233	4728	4728	13.42	32.54
2010-07-09	38266	4820	4820	12.60	29.09
2010-07-08	34940	4116	4116	11.78	26.60
2010-07-07	27536	3661	3661	13.30	29.12
2010-07-06	22007	2998	2998	13.62	29.52
2010-07-05	18115	2335	2335	12.89	28.76

PID	Installs
1000	1916
Other	0
Total	1916

File	Traffic	By hour	By OS	By GEO	Pics
index	25419	By hour	By OS	By GEO	□
all	25419	By hour	By OS	By GEO	□
					Show

When an Internet user visits a Koobface landing page and installs the malware, the malware connects through a relay server to the command and control server and sends the compromised user's IP address, geographic location, unique identifier, Koobface user identifier, and malware identifier. This data is recorded in a file on the command and control server and is then exported to the babkiup.com server. This allows Koobface to keep track of malware installations. After the search hijacker module is installed, connections are issued to the Koobface mothership, which is responsible for serving PPC and PPI links to the compromised hosts. The mothership records the compromised user's IP address, geolocation, unique identifier, Koobface user identifier, and malware identifier.

PART 2:
THE MONEY

Part 2: The Money

The Koobface operators maintain a server known as the mothership. The mothership acts as an intermediary between the PPC and rogue security software affiliates and the compromised victims. This server receives intercepted search queries from victims' computers and relays this information to Koobface's PPC affiliates. The affiliates then provide advertisements links that are sent to the user. When the user attempts to click on the search results, they are sent to one of the provided advertisement links instead of the intended location. In addition, Koobface will receive and display URLs to rogue security software landing pages or will directly push rogue security software binaries to compromised computers. As a result, Koobface operators were able to generate over two million dollars in a one-year period.

The Mothership

The Koobface mothership maintains daily records of the money earned from affiliate relationships. The daily total for the last seven days is sent to four Russian mobile phone numbers daily. The records of daily totals extend back for nearly one year, from June 23, 2009 to June 10, 2010. During this time, Koobface earned a total income of $2,067,682.69. The daily average income was $5,857.46. The highest daily total was on March 23, 2010, with a profit of $19,928.53. The lowest daily total was on January 15, 2010, with a loss of $1,014.11(see table 1).

TABLE 1: The total amount of money Koobface earned by month, including the specific days on which they earned their highest and lowest daily totals.

MONTH	TOTAL	DAYS	HIGH		LOW	
2009-06	$47,066.03	8	2009-06-23	$8,300.42	2009-06-28	$3,643.61
2009-07	$61,290.31	31	2009-07-02	$3,487.79	2009-07-17	$872.91
2009-08	$132,987.50	31	2009-08-18	$9,976.38	2009-08-02	$1,290.33
2009-09	$135,193.27	30	2009-09-02	$7,931.38	2009-09-14	$2,809.18
2009-10	$150,168.52	31	2009-10-25	$10,179.41	2009-10-10	$1,092.54
2009-11	$254,404.43	30	2009-11-24	$18,775.62	2009-11-05	$2,994.17
2009-12	$174,894.68	31	2009-12-02	$11,357.75	2009-12-10	$2,138.42
2010-01	$149,758.92	31	2010-01-27	$8,516.61	2010-01-15	-$1,014.11
2010-02	$137,256.44	28	2010-02-17	$7,899.96	2010-02-07	$966.84
2010-03	$379,942.73	31	2010-03-23	$19,928.53	2010-03-28	$6,918.67
2010-04	$292,189.29	30	2010-04-13	$17,328.02	2010-04-28	$4,298.34
2010-05	$126,204.67	31	2010-05-22	$7,451.72	2010-05-07	-$107.86
2010-06	$26,325.90	10	2010-06-09	$4,150.33	2010-06-04	$1,671.58

Paymer

There was an archive file on the Koobface command and control server that contained records of payments made through Paymer (paymer.com). Paymer is a payment service that integrates with WebMoney, a Russian payment system that is popular within the malware ecosystem. It is similar to PayPal, except that payments are not reversible. The archive contains records for 255 transactions. Payments were sent on May 13, 2010 and redeemed by the payees on May 14 and 15, 2010. The large number of transactions is due to the fact that payments were split into $200 chunks. A total of $47,779.67 was sent to 28 different WebMoney identities (see table 2).

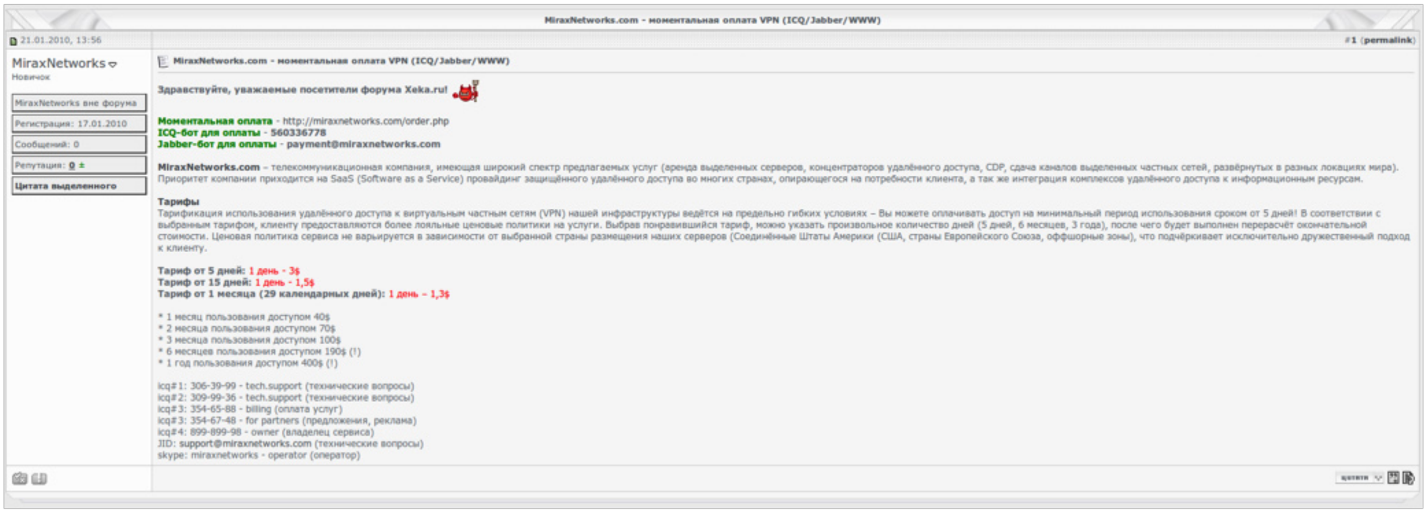
TABLE 2: WebMoney identities that Koobface made payments to in May 2010.

NAME	AMOUNT
Aalee	$1,460.98
Artem	$131.99
Dmitriy	$28.99
Eleutherios	$1,727.99
Fiore	$470.98
Forser	$3,188.99
Isay	$520.99
Jerry	$1,578.99
Kizilovan	$859.98
Ksandr	$831.99
Magic	$1,827.99
Mchammer	$802.99
MiraxNetworks	$3,199.99
Moloko	$281.99
MR	$9,446.99
Nemo	$570.99
Othercash	$448.99
Pipez	$338.99
Prostin.ivan	$1,515.99
Pushka	$400.00
Seo	$3,030.99
TTpu3paK	$1,947.99
Victor	$3,671.99
Webmoney24.in.ua	$80.99
Вася	$544.99
Ткаченко	$983.99
Алексей	$2,504.99
Дуля	$5,376.96

While the identities of the recipients and the purposes of the transfers remain unclear, the total transfer amount of $47,779.67 is close to the amount of Koobface's earnings between May 1 and May 13, 2010, which was $48,135.09. Therefore, it is possible that this file represents Koobface's bi-monthly payroll and accounting.

A payment recipient of significance is MiraxNetworks, which received $3,199.99. MiraxNetworks may be a crimeware friendly hosting provider that has advertised on Russian hacker forums (see figure 8). This transaction could be Koobface paying their Web hosting bill.

Figure 8: A screen shot of an advertisement for MiraxNetworks in an underground forum.



MiraxNetworks.com - моментальная оплата VPN (ICQ/Jabber/WWW)

Здравствуйте, уважаемые посетители форума Xeka.ru!

Моментальная оплата - http://miraxnetworks.com/order.php
ICQ-бот для оплаты - **560336778**
Jabber-бот для оплаты - **payment@miraxnetworks.com**

MiraxNetworks.com – телекоммуникационная компания, имеющая широкий спектр предлагаемых услуг (аренда выделенных серверов, концентраторов удалённого доступа, CDP, сдача каналов выделенных частных сетей, развёрнутых в разных локациях мира). Приоритет компании приходится на SaaS (Software as a Service) провайдинг защищённого удалённого доступа во многих странах, опирающегося на потребности клиента, а так же интеграция комплексов удалённого доступа к информационным ресурсам.

Тарифы
Тарификация использования удалённого доступа к виртуальным частным сетям (VPN) нашей инфраструктуры ведётся на предельно гибких условиях – Вы можете оплачивать доступ на минимальный период использования сроком от 5 дней! В соответствии с выбранным тарифом, клиенту предоставляются более лояльные ценовые политики на услуги. Выбрав понравившийся тариф, можно указать произвольное количество дней (5 дней, 6 месяцев, 3 года), после чего будет выполнен перерасчёт окончательной стоимости. Ценовая политика сервиса не варьируется в зависимости от выбранной страны размещения наших серверов (Соединённые Штаты Америки (США, страны Европейского Союза, оффшорные зоны), что подчёркивает исключительно дружественный подход к клиенту.

Тариф от 5 дней: 1 день - 3$
Тариф от 15 дней: 1 день - 1,5$
Тариф от 1 месяца (29 календарных дней): 1 день – 1,3$

* 1 месяц пользования доступом 40$
* 2 месяца пользования доступом 70$
* 3 месяца пользования доступом 100$
* 6 месяцев пользования доступом 190$ (!)
* 1 год пользования доступом 400$ (!)

icq#1: 306-39-99 - tech.support (технические вопросы)
icq#2: 309-99-36 - tech.support (технические вопросы)
icq#3: 354-65-88 - billing (оплата услуг)
icq#3: 354-67-48 - for partners (предложения, реклама)
icq#4: 899-899-98 - owner (владелец сервиса)
JID: support@miraxnetworks.com (технические вопросы)
skype: miraxnetworks - operator (оператор)

The WebMoney identification page of MiraxNetworks lists two other identities: PrettyMedia and MiraxFinance. MiraxFinance was profiled by bobbear.co.uk as a "money mule" recruitment Web site that attempts to recruit users into allowing criminals to use their bank accounts to transfer funds.[23]

Koobface's Affiliates

Koobface maintains a system for monitoring the income generated from their relationship with a variety of affiliate networks. These affiliate networks pay the Koobface operators for advertisement clicks generated by compromised computers and for installations of fake security software (see figure 9). The monitoring system contains account information for 18 affiliate networks. There are also daily records for earned income organized by affiliates. The data spans from June 21, 2009 to June 9, 2010, and indicates that a total of $1,994,355.86 was earned.[24]

There were considerable variations in the total amounts earned from affiliates, although not all affiliates were active over the entire time span. Overall, Koobface operators earned roughly the same amount from rogue security software affiliates as they did from PPC affiliates. However, the income generated from PPC affiliates was generally stable while the income generated from rogue security software affiliates was volatile (see table 3).

[23] Mirax Finance LLC (Mirax Finance Group, Inc.) Fraud," accessed October 4, 2010, http://www.bobbear.co.uk/mirax-finance-llc.html.

[24] The Koobface script ran multiple times per day. These figures were calculated from the last file created for each day and by using the calculated total in the "yesterday" section of each affiliate. This daily total differs from the daily income total that Koobface sent via SMS to the botnet operators. Not all affiliates are represented in these files.

Figure 9: A Palantir screenshot visualizing the payment flows from Koobface's affiliates.

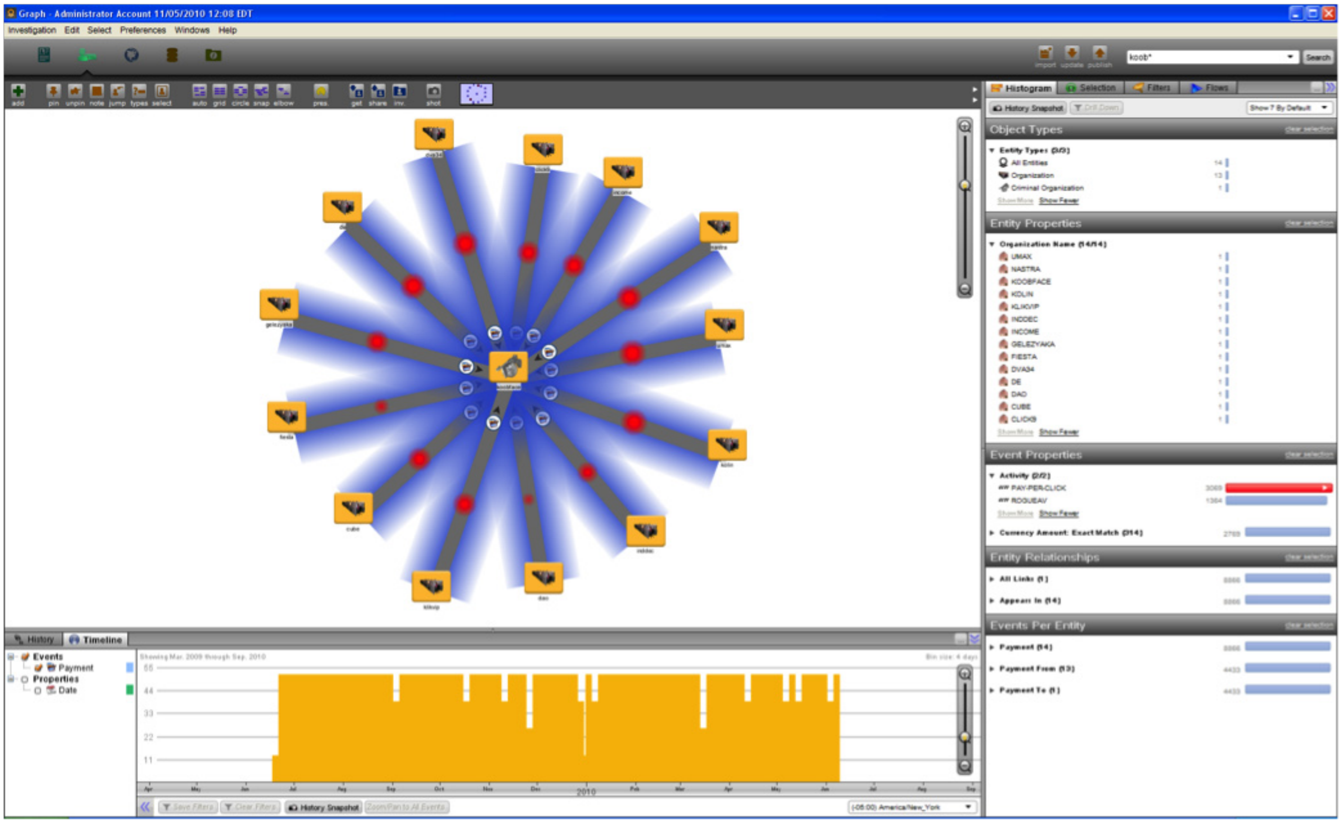


Table 3: Koobface's earnings from each affiliate.

AFFILIATE	WEBSITE	AMOUNT
Blackvendor	blackvendor.net	Unknown
Click9	click9.com	$88,552.24
Codec	adultadscash.com	Unknown
Cube	affiliatecube.com	$87,339.85
Dao	daoclick.com	$1,027.84
Dva34	old.dva34.com	$264,942.61
DE	feed-statistics.com	$476,674.00
Fiesta	fiestappc.com	$5,852.20
Gelezyaka	gelezyaka.net	$89,160.00
Income	incomeppc.com	$157,779.98
Inddec	inddecsoft.com	$39,000.00
Klikvip	klikvip.com	$86,607.37
Kolin	207.226.175.142	$209,470.00
Nastra	92.48.127.76	$278,585.00
Secash	se-cash.net	Unknown
Trafficconverter	trafficconverter2.biz	Unknown
Umax	umaxlogin.com	$209,364.77
Valary	valary.com	Unknown

Rogue Security Software

Rogue security software is distributed through “partnerka” networks, private affiliate groups that form to facilitate coordinated malware propagation. These networks are linked to similar networks that focus on “pharma” (fake pharmaceutical sites), pornography, and pirate software. The content is advertised through the use of SEO techniques that allow these Web sites to be listed highly in search engine results for popular search terms as well as distribution through well-known spam networks. Most, but not all, partnerka networks are private:

> Due to the openly criminal nature of these affiliate groups, the codec-partnerkas do not last very long. Most of them are exclusively private and require affiliates to have a certain reputation in the SEO world before they can be admitted as members.[25]

These networks provide support and encourage affiliates to distribute rogue security software through coordinated efforts known as “campaigns”.[26]

Income from rogue security software accounts for $1,003,729.00 or 50.3 percent of the income generated by Koobface’s affiliates.[27] Koobface’s relationship with “DE” (feed-statistics.com) has resulted in earnings of $476,674.00. Overall, the distribution of rogue security software was profitable. However, earnings were volatile. For example, Koobface earned as much as $8,010.00 on one day, but lost as much as $990.00 on another.

In total, Koobface has maintained relationships with at least seven rogue security software providers. Koobface developed a script that connects to a source location for rogue security software and retrieves URLs for rogue security software landing pages that attempts to scare users into installing the fake software.

“CUT”

Koobface has an affiliate account with “CUT” (exportmaindomain2010.com), which distributes rogue security software. The malware associated with this affiliate is Win Antispyware Center (winantispywarecenter.com).

Koobface retrieves new domain names from a URL supplied by CUT:

> Result: garrypotertds.com

Koobface appends its unique identifier as part of CUT’s affiliate program and redirects compromised computers to CUT’s rogue security software application.

“DE”

Koobface has an affiliate account with “DE” (feed-statistics.com), which distributes a rogue security software known as “Personal Security”.[28] This affiliate represents the largest source of Koobface’s income. Between October 22, 2009 and May 24, 2010, Koobface earned a total of $476,674.00, including a one-day total of $7,280.00.

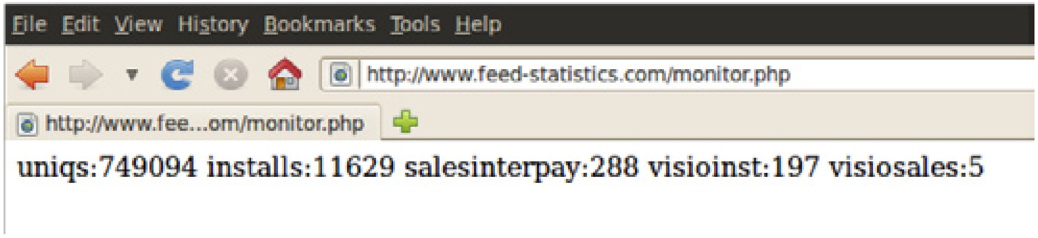
[25] Samosseiko, “The Partnerka.”

[26] Marco Cova et al., “Gone Rogue: An Analysis of Rogue Security Software Campaigns” (invited paper in the Proceedings of the 5th European Conference on Computer Network Defense, Milan, Italy, November 2009).

[27] There are a variety of Koobface’s rogue security software affiliates that are not included in these totals, either because they are no longer active or Koobface stopped propagating these links.

[28] “Malware Domain List,” *Malware Domain List*, accessed October 4, 2010, http://www.malwaredomainlist.com/mdl.php?search=195.5.161.210&inactive=on.

Figure 10: A screenshot of the "DE" affiliate's malware statistics page.


File Edit View History Bookmarks Tools Help
http://www.feed-statistics.com/monitor.php
http://www.fee...om/monitor.php

```
uniqs:749094 installs:11629 salesinterpay:288 visioinst:197 visiosales:5
```

A screenshot from feed-statistics.com's statistics interface on May 20, 2010 reveals that there were over 11,000 installations and 288 purchases on that date (see figure 10). However, this rogue security software vendor appears to have been disabled or discontinued on May 25, 2010.

Koobface retrieves new domain names from a URL supplied by DE:

Result: atechnologyscanner.com

Koobface appends its unique identifier as part of DE's affiliate program and redirects compromised computers to DE's rogue security software application.

"inddec"

Koobface has an affiliate account with "indecc" (inddecsoft.com), which distributes rogue security software Internet Antivirus Pro (iav-pro.com), General Antivirus (ga-site.com), and Live Security Suite (livesecsuite.com). Koobface retrieves new domain names from a URL supplied by inddec:

Result: golandscan.com

Koobface appends its unique identifier as part of inddec's affiliate program and redirects compromised computers to one of inddec's rogue security software applications. Koobface's total earnings from inddec were rather modest in comparison to other affiliates, totaling $39,000.00. However, indecc was a volatile income source. Koobface earned as much as $1,800.00 on one day, but lost as much as $1080.00 on another.

The campaigns surrounding this rogue security software have been well-documented. Dancho Danchev, a well-known security researcher and Koobface expert, has connected the activities of this group to the Crusade Affiliates, another affiliate network.[29]

"kolin"

Koobface has an affiliate account with "kolin" (207.226.175.142), which distributes a rogue security software known as "PrivacyCenter".[30] Koobface earned a total of $209,470.00 from kolin. However, kolin was a volatile income source. Koobface earned as much as $5,460.00 on one day, but lost as much as $2,790.00 on another.

Koobface retrieves new domain names from a URL supplied by kolin:

[29] Dancho Danchev, "Koobface Botnet's Scareware Business Model," *Dancho Danchev's Blog – Mind Streams of Information Security Knowledge*, September 16 2009, http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html.

[30] "Check Website Security Status," *MalwareURL*, accessed October 4, 2010, http://www.malwareurl.com/listing.php?domain=muoiy.in.

Result: muoiy.in

Koobface appends its unique identifier as part of kolin's affiliate program and redirects compromised computers to kolin's rogue security software application.

"nastra"[31]

Koobface has an affiliate account with "nastra" (92.48.127.76), which distributes rogue security software. Koobface earned a total of $278,585.00 from nastra. However, nastra was a volatile income source. Koobface earned as much as $8,010.00 on one day, but lost as much as $990.00 on another. Koobface retrieves new domain names from a URL supplied by nastra:

Result: 91.188.60.126

Koobface appends its unique identifier as part of nastra's affiliate program and redirects compromised computers to nastra's rogue security software application.

"RED"

Koobface has an affiliate account with "RED" (strangepassenger.com), which distributes rogue security software. Koobface retrieves new domain names from a URL supplied by RED:

Result: spyware-online-scaner.com

Koobface appends its unique identifier as part of RED's affiliate program and redirects compromised computers to RED's rogue security software application.

"weber"

Koobface has an affiliate account with "weber" (affiliates.sftmaster.com), which distributes a rogue security software known as "AV Security" (antivirprime.com). Koobface retrieves new domain names from a URL supplied by weber:

Result: business.one.strangled.net

However, the URL appears to be broken and as a result, Koobface is directly distributing the malicious executable:

st934.exe – MD5: df1d9e8a748c5f79a78ee74c758d8467

Koobface's PPC/PPI Affiliates

While some botnets focus on stealing information such as credit card numbers and PayPal credentials, many botnets monetize their operations through PPC schemes. There are a wide variety of PPC affiliates, including both public and private affiliates. Botnet operators create accounts with these affiliates and then force

[31] Dancho Danchev, "Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign," *Dancho Danchev's Blog – Mind Streams of Information Security Knowledge*, June 8, 2010, http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html.

compromised computers to click on the supplied links. The botnet operators earn money for each click they supply. Koobface accomplishes this by using a hijacker that intercepts queries to search engines and directs users to PPC links that they did not intend to visit. Trend Micro explains how browser hijacker Trojans operate:

> Browser hijacker Trojans refer to a family of malware that redirects their victims away from the sites they want to visit. In particular, search engine results are often hijacked by this type of malware. A search on popular search engines like Google, Yahoo!, or Bing still works as usual. However, once victims click a search result or a sponsored link, they are instead directed to a foreign site so the hijacker can monetize their clicks.[32]

Using this method, Koobface was able to earn $990,626.86 between June 21, 2009 and June 9, 2010.[33] In order to ensure that there are always active accounts, Koobface diversifies across a wide variety of PPC brokers.

- Click9 (click9.com): Click9 is a PPC affiliate that is available in both English and Russian. It has an open registration and pays out twice a month through bank wire transfer, ePassporte, Fethard, and WebMoney. Koobface earned an income of $88,552.24 from Click9. The average daily income was $259.68.

- Cube (affiliatecube.com): AffiliateCube is a PPC affiliate that is available in both English and Russian. It has an open registration and pays out bank wire transfer, ePassporte, EvoPlus, and WebMoney. Koobface earned an income of $87,339.85 from AffiliateClub. The average daily income was $256.13.

- Dao (daoclick.com): Daoclick is a PPC affiliate that is available in both English and Russian. Koobface earned an income of $1,027.84 from Daoclick. The average daily income was $3.01.

- Dogma (dogmamillions.com): Dogmamillions is a Russian PPI affiliate that pays affiliates 60 percent of install revenue and pays out twice a month.[34] They advertise on Russian hacker forums in order to attract affiliates.[35] It is estimated that Dogmamillions accumulate hundreds of thousands of installations per month.[36] Dogmamillions provides each affiliate with a TDSS rootkit to propagate and a personal manager to assist with any problems.[37] Koobface has a PPI affiliate account with dogmamillions.com and pushes dogma.exe (MD5: ef00741e9fcf1379e9e7554c1a12d609) to compromised computers.

- Dva34 (old.dva34.com): Dva34 is a Russian PPC/PPI affiliate that no longer appears to be actively accepting registrations but is still active through old.dva34.com. Koobface earned an income of $264,942.61 from Dva34. The average daily income was $776.96.

- Fiesta (fiestappc.com): Fiestappc is a PPC affiliate that may require an invitation. Koobface earned an income of $5,852.20 from Fiestappc. The average daily income was $17.16.

- Gelezyaka (gelezyaka.net): Gelezyaka is a private PPC affiliate. Koobface earned an income of $89,160.00

[32] Feike Hacquebord, "Making a Million, Part One – Criminal Gangs, the Rogue Traffic Broker, and Stolen Clicks," *Trend Labs Malware Blog*, August 9, 2010, http://blog.trendmicro.com/making-a-million%E2%80%94criminal-gangs-the-rogue-traffic-broker-and-stolen-clicks/#ixzz111GSacE7.

[33] The daily average numbers for PPC affiliates cover the entire time period of the logs, although it does appear that some affiliates started later than others or were discontinued during the time period.

[34] Since Koobface has only recently started distributing dogma.exe, the earnings from this affiliate are not available in the records obtained by Informwation Warfare Monitor.

[35] See: http://forum.blackhack.ru/showthread.php?t=11939, accessed July 27, 2010.

[36] Kevin Stevens, "The Underground Economy of the Pay-Per-Install (PPI)," *SecureWorks*, September 29, 2010, accessed October 4, 2010, http://www.secureworks.com/research/threats/ppi/?threat=ppi.

[37] Aleksandr Matrosov and Eugene Rodionov, "TDL3: The Rootkit of All Evil?," *ESET*, June 25, 2010, accessed October 4, 2010, http://www.eset.com/resources/white-papers/TDL3-Analysis.pdf.

from Gelezyaka. The average daily income was $261.47.

- Income (incomeppc.com): IncomePPC is a PPC affiliate that is available in both English and Russian. Koobface earned an income of $157,779.98 from IncomePPC. The average daily income was $462.70.

- Klikvip (klikvip.com): Klikvip is a PPC affiliate that is available in both English and Russian. It has an open registration and pays out through bank wire transfer, ePassporte, EPESE, PayPal, Stormpay, and WebMoney. Koobface earned an income of $86,607.67 from Klikvip. The average daily income was $253.98.

- Umax (umaxlogin.com): Umax is a popular PPC affiliate that is available in both English and Russian. It has an active Russian language forum. It has an open registration and pays out twice a month through bank wire transfer, CGPay, ePassporte, EvoPlus, Payoneer, PromSvyazBank, RUR bank wire transfer, UniStream money transfer, and WebMoney. Koobface earned an income of $209,364.77 from Umax. The average daily income was $613.97.

- Koobface uses a variety of other PPC affiliates including se-cash.net, trafficconverter2.biz[38], blackvendor.net, adultadscash.com, 92.48.127.76/PrivateCoin[39], dolcevitacash.com, tinyppc.com, and offersreal.com.

The diversity of PPC and PPI affiliates spread across both public and private affiliates ensures that the Koobface operators continue to generate income even if one or more of their accounts are suspended or if the security community identifies and blocks any malicious URLs distributed by these affiliates. As a result, even though the income generated from some affiliates was volatile, the Koobface operators were able to maintain a fairly steady income over the last year.

[38] Trafficconverter2.biz is related to the infamous BakaSoftware and reportedly pays out quite well. BakaSoftware was compromised and details of their operation were made public. See: John Markoff, “Antiviral ‘Scareware’ Just One More Intruder,” *New York Times*, October 29, 2008, accessed October 4, 2010, http://www.nytimes.com/2008/10/30/technology/internet/30virus.html; “Traffic Converter,” *Seo Blade*, accessed October 4, 2010, http://uaseo.net/soft-partnerki/111; and Joe Stewart, “Rogue Antivirus Dissected – Part 1, *SecureWorks*, October 21, 2008, accessed October 4, 2010, http://www.secureworks.com/research/threats/rogueantivirus-part-1/?threat=rogueantivirus-part-1.

[39] PrivateCoin is a private PPC affiliate, but has been publicly reviewed. See: http://uaseo.net/soft-partnerki/184.

PART 3:
THE TAKEDOWN

Part 3: The Takedown

Investigating the individual(s) responsible for operating botnets is an arduous task. These investigations focus on gathering evidence to meet legal standards[40] with the aim of prosecution, and they often take place over a considerable period of time.[41] Botnet operators leverage geography as well as the Internet's relative anonymity to avoid prosecution, and issues of overlapping jurisdictions and international politics often complicate investigations. Cross-border investigations are hampered by a lack of trust, priority, and willingness to respond.[42] This makes evidence collection and successful prosecution difficult. As Professor Roderic Broadhurst explains:

> Digital footprints are fragile or ephemeral, so swift action is often required. This becomes very difficult when an attack transits multiple jurisdictions with different regimes for preserving evidence. Traditional methods of law enforcement are therefore no longer adequate. A slow formal process risks losing evidence, and multiple countries may be implicated. Following and preserving a chain of evidence is a great challenge.[43]

There is a general consensus within the security community that a lack of international cooperation allows cybercriminals in Eastern Europe and Russia to operate freely.[44] However, there have been successful cases in these regions. In *Fatal System Error*, Joseph Menn describes the investigation and international cooperation that led to the arrest and imprisonment of Russian botnet operators involved in financial fraud.[45] There have been several other recent successes involving international cooperation. In November 2009, British police arrested individuals for using the well-known ZeuS/Zbot malware to steal information from numerous compromised computers.[46] In February 2010, the Mariposa Working Group, comprised of security companies, researchers, and the Spanish police, worked to identify and ultimately arrest three individuals for operating the Mariposa botnet.[47] In July 2010, Slovenian police arrested the author of the malware.[48]

The cooperation between the security community, including industry professionals, academics, and law enforcement, is critical to the successful investigation and arrest of global cybercriminals.[49] Therefore, we have notified and are working with law enforcement. During the course of this investigation we have been in contact

[40] Ricci S.C. Ieong, "FORZA - Digital Forensics Investigation Framework that Incorporate Legal Issues," *Digital Investigation* no. 3 (2006), accessed October 4, 2010, http://www.dfrws.org/2006/proceedings/4-leong.pdf

[41] Joseph Giordano and Chester Maciag, "Cyber Forensics: A Military Operations Perspective," *International Journal of Digital Evidence* 1, no. 2 (2002).

[42] Eleventh UN Congress on Crime Prevention and Criminal Justice, Bangkok, Thailand, 18-25 April 2005, *Press Release* (BKK/CP/15), April 15, 2005, accessed October 4, 2010, http://www.un.org/events/11thcongress/docs/bkkcp15e.pdf.

[43] Roderic Broadhurst, "Developments in the Global Law Enforcement of Cyber-Crime," *Policing: International Journal of Policy Strategy and Management* 29, no.2 (2006): 429.

[44] Brian Krebs, "From (& To) Russia, With Love," *Washington Post*, March 3, 2009, accessed October 4, 2010, http://voices.washingtonpost.com/securityfix/2009/03/from_to_russia_with_love.html.

[45] Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet* (New York, PublicAffairs, 2010).

[46] Jeremy Kirk, "UK Police Reveal Arrests over Zeus Banking Malware," *Computer World*, November 18, 2009, accessed October 4, 2010, http://www.computerworld.com/s/article/9141092/UK_police_reveal_arrests_over_Zeus_banking_malware.

[47] Omar El-Akkad, "Canadian Firm Helps Disable Massive Botnet," *Globe and Mail*, March 3, 2010, accessed October 4, 2010, http://www.theglobeandmail.com/news/technology/canadian-firm-helps-disable-massive-botnet/article1488838.

[48] Brian Krebs, "Alleged Mariposa Botnet Author Nabbed," *Krebs on Security*, July 28, 2010, http://krebsonsecurity.com/2010/07/alleged-mariposa-botnet-author-nabbed.

[49] Igor Muttik, "Cooperation Is Key to Internet Security," *McAfee Security Journal* iss.6 (2010): 20-24. accessed October 4, 2010, http://www.mcafee.com/us/local_content/misc/threat_center/articles/summer2010/msj_article05_cooperation_is_key_to_internet_security.pdf.

with the RCMP, the FBI, and the UK police. However, this process is taking place within a dynamic environment where the Koobface operators continue to profit from the exploitation of Internet users around the globe.

Given the obstacles to successful international investigations, disrupting the operations of the botnet itself is often the only available course of action. These "takedown" efforts generally involve contacting Internet service and hosting providers as well as domain name registrars to have malicious Web sites disabled. Brian Krebs describes two types of takedown efforts: "shuns" and "stuns".[50] A shun occurs when the security community ostracizes the peers of a malicious network to sever their connections, and a stun refers to efforts to disconnect the command and control infrastructure used by a botnet. This activity has often been referred to as a game of "whack-a-mole" because the criminals simply move their operations to other servers. It is understood that the botnet operators will likely reconstitute the botnet. However, as Krebs explains, these takedown efforts can impact botnet operations and can lead the botnet operators to make mistakes that can provide additional information about their operations:

> Shuns and stuns can not only be disruptive to online criminal operations, they also certainly increase costs and reduce profits for the perpetrators. And, when cybercriminals are forced to move their operations, the direction of that migration can provide important clues about allied hostile networks and actors that may deserve further scrutiny down the road.[51]

Prior to the publication of this report, notifications were delivered to the owners of the infrastructure that Koobface is abusing. They include: fraudulent and stolen Facebook and Google accounts, stolen FTP credentials, and dedicated command and control servers. We are working to synchronize notification to the operators of these elements in order to have an impact on the operations of the Koobface botnet.

[50] Brian Krebs, "Takedowns: The Shuns and Stuns That Take the Fight to the Enemy," *McAfee Security Journal* iss.6 (2010): 5-8, accessed October 4, 2010, http://www.mcafee.com/us/local_content/misc/threat_center/articles/summer2010/msj_article02_take_the_fight_to_the_enemy.pdf.

[51] Ibid.

Conclusion

This analysis of the Koobface botnet reveals that social networking platforms are being successfully leveraged to propagate malware. The personal information that is available in these networks provides botnet operators with significant leverage to exploit the "human factor" by abusing the trust between personal contacts.

After compromising users, Koobface was able to successfully monetize their operation through affiliate programs with PPC and PPI brokers. Through a combination of click fraud and the propagation of rogue security software, Koobface was able to generate over $2 million between June 2009 and June 2010.

Botnet operators, including those behind Koobface, rely on relationships with other botnet operators and online criminals to sustain and monetize their operations. The relationship between affiliate or partnerka programs and botnet operators is important. Just as the botnet operators diversify their operations across multiple affiliate programs, it is likely that each affiliate also has multiple botnet clients that propagate malicious software or advertising links. This provides a layer of redundancy within the malware ecosystem and allows botnet operators to continue monetizing their operations even if some partnerka programs are disrupted. This makes efforts to counter botnet operations difficult.

The countermeasures taken by botnet operators are aimed at the increasing efforts of the security community to understand their malware and shutdown their operations. Koobface maintains a banlist of IP addresses that are forbidden from accessing Koobface servers. In addition, Koobface operators carefully monitor whether any of their URLs have been flagged as malicious by bit.ly or Facebook and they also monitor their malware links with the Google Safe Browsing API. This is part of a trend where malware authors check their malicious software against a variety of security products to ensure that there is only limited protection.[52]

Botnets present significant, but not impossible, challenges for law enforcement. Botnet operators leverage geography to their advantage, often exploiting Internet users from all countries but their own. While the total amount of criminal activity that the botnet operators engage in may be significant, the distribution of that criminal activity across multiple jurisdictions means that the criminal activity in any one jurisdiction is minimal. In addition, botnet operators leverage Internet infrastructure around the world, making it difficult to interfere with their operations. Since relevant information and persistent monitoring can uncover the details of botnet operations, it is important that the law enforcement and security community continue to share information and work closely together. An understanding of the inner workings of crimeware networks allows law enforcement to pursue leads and the security community to develop better defenses against malware attacks.

[52] Brian Krebs, "Virus Scanners for Virus Authors, Part II," *Krebs on Security*, April 5, 2010, http://krebsonsecurity.com/2010/04/virus-scanners-for-virus-authors-part-ii.

Glossary

Affiliate programs: An e-commerce marketing program whereby a Web site is linked to an e-commerce Web site with the goal of making a commission for referred sales.

Botnet: A collection of compromised networked computers that can be controlled remotely by an attacker.

Browser hijacker Trojans: A family of malware that redirects their victims away from the sites they want to visit.

CAPTCHA: A response test used in computing to ensure that the response is not being generated by a computer.

Click fraud: Occurs in pay-per-click advertising and refers to when an automated script, computer program, or person clicks on an ad for the purpose of generating a profit.

Codec: A device or computer program that is capable of encoding and/or decoding a digital data stream or signal.

Command and control server: The network server that sends commands to compromised computers in a botnet.

Malware (malicious software): Software designed to carry out a malicious purpose. Varieties of malware include computer viruses, worms, Trojan horses, and spyware.

PPC (pay-per-click): An Internet advertising model where advertisers pay host Web sites for every time their ad is clicked by users.

PPI (pay-per-install): An Internet advertising model where advertisers pay publishers for every time their application, usually free and bundled with advertising-supported software, is installed by users.

Spyware: A type of malicious software that is installed on computers to collect bits of information at a time about the users.

Zombie (zombie computer): A computer that has been compromised by a hacker, computer virus, or trojan horse.