The "Kneber" Botnet, Spear Phishing Attacks and Crimeware

by Nart Villeneuve
(Chief Research Officer, SecDev.cyber)

Introduction

Targeted attacks, known as “spear phishing,” are increasingly exploiting government and military themes in order to compromise defense contractors in the Unites States. [1] In 2009, the Washington Post reported that unknown attackers were able to break into a defense contractor and steal documents pertaining to the Joint Strike Fighter being developed by Lockheed Martin Corp. [2] Google was compromised in January 2010 along with other hi-tech companies and defense contractors. [3] The problem is becoming increasingly severe. [4] In fact, the Department of Defense recently released a memo with plans to protect unclassified information passing through the networks of various contractors. [5] The memo recognizes the severity of the ongoing threat and seeks to:

> Establish a comprehensive approach for protecting unclassified DoD information transiting or residing on unclassified DIB information systems and networks by incorporating the use of intelligence, operations, policies, standards, information sharing, expert advice and assistance, incident response, reporting procedures, and cyber intrusion damage assessment solutions to address a cyber advanced persistent threat.

Netwitness revealed the existence of a Zeus-based botnet that had compromised over 74,000 computers around the world. Zeus is not a single botnet, rather it is a malware kit that allows anyone to easily create a botnet. It sells for $400 - $700 although there are older (and pirated) version that cost considerably less or are publicly available for download. [6] Typically, the Zeus malware is used to steal banking credentials. [7] Because of the proliferation of the Zeus kit there are a wide variety of actors using Zeus – there is no single Zeus botnet, there is no one group behind the attacks. [8] In fact, botnet operators will often use multiple types of malware. [9]

Netwitness found that the command and control infrastructure for this botnet was primarily based in China and most of the compromised computers were in Egypt, Mexico, Saudi Arabia, Turkey and the United States. In addition to stealing banking credentials, attackers are now targeting the social networking credentials of members of the government and military as well as the employees of Fortune 500 companies. Netwitness revealed that many of the US compromises included government networks as well as Fortune 500 enterprises. [10] News reports revealed that ten U.S government agencies were compromised and several high profile companies were named including Merck, Cardinal Health, Paramount Pictures and Juniper Networks. [11]

The use of crimeware infrastructure for spear phishing attacks is certainly not a new development. Anti-Virus (AV) companies and members of the security community have downplayed the Kneber

botnet suggesting that there has long been AV protection for this type of attack and that there is nothing particularly new about this botnet. [12] Furthermore, they argue that Kneber is not a particularly large Zeus-based botnet either, implying that the Kneber botnet is not deserving of the attention it has received. [13] While the media attention paid to the Kneber botnet has often been alarmist and sometimes inaccurate, the anti-virus coverage of the malware used in this attack was low (18/41 on Virustotal) -- despite the fact that it was the well known Zeus malware kit. The way in which some are suggesting that AV has long protected users from this threat is troubling. Moreover, focusing solely on Zeus and not additional malware downloaded after Zeus obscures the relationship between generic and targeted attacks.

These events indicate that attacks that are often considered to be criminal in nature, such as the targeting of banking credentials of individuals, also pose persistent threats to those in the government and military sectors. Moreover, it is well understood that these attackers aim to maximize their financial gain from such attacks. If the data ex-filtrated is not simply bank account and credit card numbers but also credentials that can be used to access the internal networks of the victims, why wouldn't they also sell that information? [14] As Netwitness states:

> They are well organized, have demonstrated technical sophistication on par with many intelligence services and do not forgo the opportunity for financial gain with the the information they collect. If they are collecting network credentials, it means they are using or selling them in an active underground economy – which may include sponsoring foreign intelligence services. What is easier? Designing a campaign like Operation Aurora, or simply purchasing access to your target companies? [15]

Moreover, Netwitness suggests that the attackers may have been after data other than simply banking, credit card or social networking credentials. In response to the critique from the security and AV community, Netwitness stated that “trivializing the damage done is simply disingenuous by anyone who has seen the types of data stolen from threats such as these.” [16] This implies that the data ex-filtrated by the attackers may have been particularly sensitive. In fact, the Wall Street Journal reported that:

> At one company, the hackers gained access to a corporate server used for processing online credit-card payments. At others, stolen passwords provided access to computers used to store and swap proprietary corporate documents, presentations, contracts and even upcoming versions of software products. [17]

One can understand the AV and security communities skepticism. Zeus, after all, is very well known. However, our investigation found that not only were there high profile compromises, as suggested by Netwitness, but that the focus of the attack appears to have been the extraction of sensitive information, not just banking credentials.

IWM Investigation

Our investigation focused on a spear phishing campaign that is linked with the Kneber botnet that represents only a small portion of the Kneber botnet. We focused on a case in which the attackers took portion of blog posts by authors Brian Krebs and Jeff Carr (two prominent members of the security community) and used them as the content of their malicious emails. Numerous individuals with .gov and .mil email addresses were sent these spoofed emails that prompted them to download a security fix for Microsoft Windows. Our investigation revealed that Zeus was being used to infect targets within the

government and military sectors with second instance of malware designed to ex-filtrate data from the compromised computers.

Instead of simply stealing banking, credit card and social networking credentials, the Zeus malware downloaded an additional piece of malware on to the compromised machines which focused on ex-filtrating sensitive documents. We found that at least 81 compromised computers that had uploaded a total of 1533 documents to the drop zone. We found sensitive contracts between defense contractors and the U.S. Military, documents relating to, among other issues, computer network operations, electronic warfare and defense against biological and chemical terrorism. We found the security plan for an airport in the Unites States as well as documents from a foreign embassy as well as a large UN-related international organization. In addition, the personal computers of employees with security clearances who work for a variety of companies and government agencies were compromised.

The sensitive data obtained from these attacks will likely be used to exploit these targets further as well as those within the targets' social network. The contact information and documents obtained by the attacker will likely be used for further “spear phishing” attacks. But these attacks may signify the growing involvement of crimeware in targeted malware attacks for the purposes of extracting sensitive information that can be exploited for intelligence purposes . The profile of the organizations that were compromised and the nature of the ex-filtrated data indicate that the goal of these attacks was not simply stolen banking credentials - the typical target of the Zeus malware.

Furthermore, this case poses challenges to methods of attribution that interpret the geo-political motivation of the attackers and assess the geographic location of the attackers' command and control infrastructure. Were these attacks simply part of an ongoing Zeus crimeware campaign? Or does the composition of the targets and the content of the ex-filtrated data indicate that this is less a case of crimeware and more a case of espionage? There is no easy answer.

A more detailed examination of our investigation

On February 6, 2010, Brian Krebs reported that attackers using the Zeus trojan targeted a variety of .gov and .mil email addresses in a spear phishing attack that appeared to be from the National Security Agency and enticed users to download a report called the “2020 Project.” [18]

Following the publication of the article by Brian Krebs, attackers took portions of his article and used them as lure in further spear phishing attacks. [19] Sophos Labs analyzed the sample that used Kreb's post. [20] A post on Intelfusion.com by Jeff Carr regarding the spear phishing attack was also used in another attack. [21] The attackers used the blog posts of these individuals and spoofed their email addresses in order to make their malware seem convincing to the recipients of the spear phishing attack.

Spear Phising Email

From: jeffreyc@greylogic.us [mailto:jeffreyc@greylogic.us]
Sent: Wednesday, February 10, 2010 7:34 AM
To: [REDACTED]
Subject: Russian spear phishing attack against .mil and .gov employees

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft(r) Windows(r) and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://fcpra.org/downloads/winupdate.zip

or

http://www.sendspace.com/file/tj373l

_____

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us

According to a further post on Intelfusion.com, the header information from the email reveals that there were two email addresses used to send the malicious email nobody@abe.enixns.com and w63697@uw03.uniweb.no. [22]

This email was sent to .mil and .gov email addresses, including those at the following locations: [23]

Executive Office of the President
Office of the U.S. Trade Representative
US Agency for International Development
Dept of Agriculture
Department of the Interior
Department of Transportation
Federal Aviation Administration
Department of State
Department of Justice
US Marine Corps
Marine Corps Intelligence Activity
US Navy
Advanced Traceability and Control Program
Department of Defense
US Joint Forces Command

White House Military Office Defense Logistics Agency Defense Security Service US Pacific Command Joint IED Defeat Organization Defense Logistics Agency Defense Intelligence Agency Defense Finance and Accounting Service

Malware Analysis

The following is an analysis of the malware sample downloaded from:

http://fcpra.org/downloads/winupdate.zip

(The malware samples at http://www.sendspace.com/file/tj373l and http://mv.net.md/update/update.zip were identical).

The malware sample was contained in a ZIP file:

MD5: 4fc8bb3fd8634085423e6e25448acfe1
Filname: winupdate.zip
Virustotal: 6/41 (14.63%)
http://www.virustotal.com/analisis/907f50968b1c324dd37cf545959b119a75fc93aee35a4b92d5b51803ecbfa4f5-1265821180

Opening the ZIP file reveals an executable:

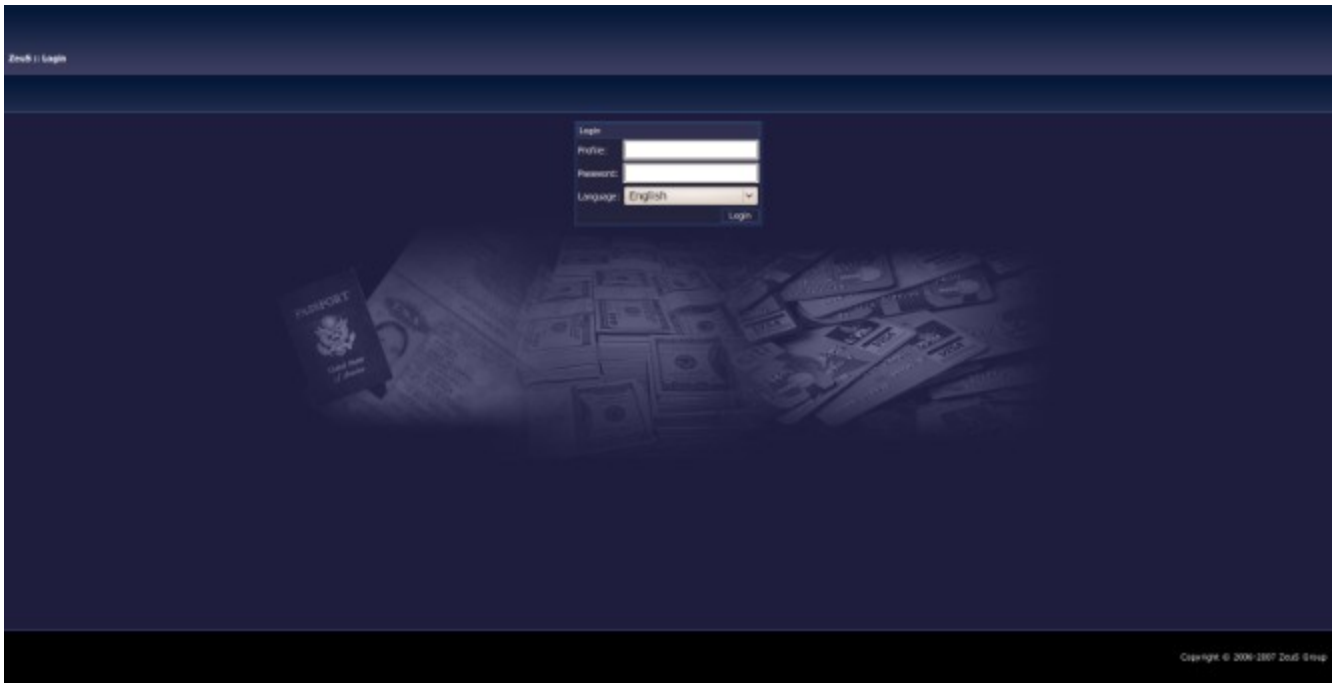
MD5: 7c0d0a771a39a83a691ffb2e3b810e0a
Filename: KB823988.exe
Virustotal: 18/41 (43.90%)
http://www.virustotal.com/reanalisis.html?907f50968b1c324dd37cf545959b119a75fc93aee35a4b92d5b51803ecbfa4f5-1265991887
http://www.threatexpert.com/report.aspx?md5=7c0d0a771a39a83a691ffb2e3b810e0a

After running the executable, attempts are made to connect with a command and control server located in China over HTTP:

updatekernel.com
115.100.250.105

Registration Information	WHOIS Information
Name: Sport Co LTD Organization: Sport Com LTD Address: Volodarskiy City: Izjevsk Province/state: IZJEVSK Country: CN Postal Code: 519000 Phone: +84.4562425583	IP: 115.100.250.105 Netname: YYNET Descr: Beijing qi shang zai xian rate communications Technology Co., Ltd. Langfang Branch Descr: West Side to the da guan di ,Langfang Development Zone Country: CN

Fax: +84.4562425583 Email: abuseemaildhcp@gmail.com	



Screen capture of Zeus login page on updatekernel.com.

The command and control server is a known Zeus C&C server. [24] There are a wide variety of malware kits and associated domain names hosted on this server, as well as several neighbouring servers.[25] The following are active domain names on the same server (115.100.250.105).

www.adjamadja.cn	justin_dickerson@ymail.com
www.antidopings.cn	abuseemaildhcp@gmail.com
www.avatar-agency.com	contact@privacyprotect.org
www.aviavavilons.net	abuseemaildhcp@gmail.com
www.banner3.biz	d_brih23@gmail.com
www.bidon.in	alparytechno@hotmail.com
www.camforuss.com	abuseemaildhcp@gmail.com
www.lusia777.com	cuitiankai@googlemail.com
www.men-secret2010.info	markstevenson.main@hotmail.com
www.olypoos.com	abuseemaildhcp@gmail.com
www.paycc.org	_wmz_@mail.ru
www.pinpinpongs.com	abuseemaildhcp@gmail.com
www.poolst.in	bondarenkoip1@gmail.com
www.realtybestus.com	krekivoshki@live.com
www.restiabuildholding.com	abuseemaildhcp@gmail.com
www.socks5servic.cn	abuseemaildhcp@gmail.com
www.stable-trading.com	abuseemaildhcp@gmail.com

www.transfertraff.cn	abuseemaildhcp@gmail.com
www.updatekernel.com	abuseemaildhcp@gmail.com
www.valentinsss.info	andrejjm@yahoo.com
www.vodkalv.com	abuseemaildhcp@gmail.com

Dancho Danchev has linked the email address “abuseemaildhcp@gmail.com” to a variety of criminal enterprises including “money mule recruitment” operations. [26] Netwitness indicated that there is a link between the “Kneber” botnet. The Knerber botnet is named after the email address used to register the command and control domain names, “hilarykneber@yahoo.com”. This email address has been linked to past crimeware activity as well. [27] The link between the domains registered to “abuseemaildhcp@gmail.com” and those registered to “hilarykneber@yahoo.com” appears to be a common command and control infrastructure.

There are two domain names www.globalunitrack.com and www.aeroninc.com both resolve to 59.53.91.102 which is where portions of the Kneber botnet are hosted. These domain names are also hosted on 115.100.250.105 which is where updatekernel.com is hosted.

There are also domain names registered by both email addresses hosted on the same IP addresses.

91.213.174.50
netname: VolgaHost
descr: PE Bondarenko Dmitriy Vladimirovich
country: RU

91.213.174.50	shashacn.cn	hilarykneber@yahoo.com
91.213.174.50	sebastijans.com	abuseemaildhcp@gmail.com

61.235.117.72
netname: CRGdSzS
country: CN
descr: China Railcom Guangdong Shenzhen Subbranch

61.235.117.72	stallvars-11.cn	hilarykneber@yahoo.com
61.235.117.72	stallvars-1.com	abuseemaildhcp@gmail.com

There are a variety of other interesting connections between “stallvars” domain names and other email addresses which indicate that there are further connections between the domain names and IP infrastructure used by the attackers. [28] This particular botnet extends beyond just the domains registered by “hilarykneber@yahoo.com.”

Configuration File

The compromised machine downloads a Zeus configuration file. In this case the file was downloaded from:

GET /imgpic/x18d2/d8x16/x98x10.bin
Host: updatekernel.com

The decrypted contents of this file contain the typical banking services that Zeus targets. When visiting these sites Zeus adds additional fields to capture information from the compromised user. It also changes DNS setting for the domains of antivirus products to prevent users from receiving updates.

```
http://updatekernel.com/dbbck/fts.exe
http://updatekernel.com/templtes/a16ext/int3xs/s.php
http://updatekernel.com/imgs/clprof/rbs28.bin
https://www.gruposantander.es/*
https://internetbanking.gad.de/*/portal?bankid=*
https://www.vr-networld-ebanking.de/index.php?RZKZ=*&RZBK=*
https://finanzportal.fiducia.de/*?rzid=*&rzbk=*
https://*.banking.first-direct.com/*
https://banking.*.de/cgi/ueberweisung.cgi/*
*&tid=*
*&betrag=*
https://internetbanking.gad.de/banking/*
KktNrTanEnz
https://cipehb*.cdg.citibank.de/HomeBanking*?_D=WorkArea&*
https://www.vr-networld-ebanking.de/ebanking*Action=*
Schmetterling
https://finanzportal.fiducia.de/ebanking*Action=*
Schmetterling
https://finanzportal.fiducia.de/ebbg2/portal?token=*
*decBetrag=*
value_*
https://onlinebanking.norisbank.de/norisbank/*.do?method=*
https://www.dresdner-privat.de/servlet/*
*&CMD=stapelFreigeben&*
https://brokerage.comdirect.de/servlet/*TAN*
*transactionID=*
```

After the “check in” with the command and control server, another executable was downloaded:

MD5: fb82af794544359ee89c17d096fa35b7
Filename: stat.exe
Virustotal: 5/41 (12.20%)
http://www.virustotal.com/analisis/1336bca82ba370c8cf0967ed192cb1865e4f943fbb4ea4e2f6c2c9b98eb43723-1265964848
http://www.threatexpert.com/report.aspx?md5=fb82af794544359ee89c17d096fa35b7

Drop Zone

After running the executable, attempts are made to connect with a drop zone located in Belarus over FTP:

packupdate.com
86.57.246.177

Registration Information	WHOIS Information
NOSPAM ASSOCIATION Email: domains@atservers.com Organization: Private person	IP: 86.57.246.177 rDBS: by104.activeby.net Netname: BELTELECOM-DATACENTER

Address: 11-2 Nezavisimosti ave., office 320 City: Minsk State: BY ZIP: 220030 Country: BY Phone: +375.172099191 Fax: +375.172099191	Descr: Minsk, Belarus Country: BY

After connecting to the drop zone, the following files were uploaded from the compromised computer to the drop zone:

- _C.dll - list fo files and directories in the “C:\” directory
- EXCEL9.XLS - blank excel document
- _hslib.dll - unique id for compromised computer
- _users.dll - list of users on the compromised computer
- WINWORD8.DOC - blank word document

The FTP server revealed that there were at least 81 compromised computers that had uploaded a total of 1533 documents to the drop zone.

While we did not find any classified data, there was sensitive information regarding contracts with private firms as well as government/military entities and project information including budgets and supplementary documentation from government/military sources. The data includes unclassified, but sensitive, documents on latest threats from law enforcement services around the world. There were also procedural documents, such as an airport's security plan.

There were also several computers compromised that belong to individuals that hold Top Secret (SSBI) clearances. In addition, computers were compromised that belong to individuals that contain documents regarding “privileged” military documents. The personal computer of an investigator that conducts security clearance investigations was also compromised.

Conclusions

Despite the fact that no classified information appears to have been obtained, the data captured is valuable to the attackers. At a minimum the attackers can use the contacts and information in these documents to further exploit the targets. Social engineering, rather than technical proficiency, is what enables attackers to compromise these high value targets. Expect to see these documents used as malicious exploits targeted those who would be familiar with or interested in them.

The identity of the targets compromised in this attack, the focus on ex-filtrating data, and the content of the documents indicates that crimeware may be moving into the espionage industry and/or providing command and control infrastructure for those engage in such activities. While Zeus is normally associated with capturing banking and other credentials, it is being used to deliver a payload that focuses on extracting sensitive data. The use of a well known malware kit such as Zeus and crime-focused command and control infrastructure may be obscuring the nature and intent of the attackers. If this trend is in fact occurring, the use of crimeware infrastructure significantly impacts traditional methods of determining motivation and attribution in espionage investigations.

About Information Warfare Monitor

The Information Warfare Monitor is an advanced research activity tracking the emergence of cyberspace as a strategic domain. We are an independent research effort. Our mission is to build and broaden the evidence base available to scholars, policy makers, and others. We aim to educate and inform.

The Information Warfare Monitor is public-private venture between two Canadian institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto and The SecDev Group, an operational think tank based in a Ottawa (Canada). The Secdev Group conducts field-based investigations and data gathering. Our advanced research and analysis facilities are located at the Citizen Lab.

---

[1] http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

[2] http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html

[3] http://www.wired.com/threatlevel/2010/01/google-hack-attack/

[4] http://www.businessweek.com/technology/content/jul2009/tc2009076_873512.htm

[5] http://www.dtic.mil/whs/directives/corres/pdf/520513p.pdf

[6] http://www.damballa.com/downloads/d_pubs/WP%20Many-to-Many%20Botnet%20Relationships%20(2009-05-21).pdf

[7] For a technical discussion see http://www.abuse.ch/?p=1192 , http://blog.threatexpert.com/2009/09/time-to-revisit-zeus-almighty.html and http://www.m86security.com/labs/i/Zbot-In-Your-Inbox,trace.1005~.asp

[8] http://www.fortiguard.com/analysis/zeusanalysis.html

[9] http://www.darkreading.com/security/client/showArticle.jhtml?articleID=217800596

[10] http://www.netwitness.com/resources/kneber.aspx

[11] http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html http://www.nytimes.com/2010/02/19/technology/19cyber.html http://blogs.zdnet.com/security/?p=5508

[12] http://www.symantec.com/connect/fr/blogs/kneber-zeus

[13] http://www.krebsonsecurity.com/2010/02/zeus-a-virus-known-as-botnet/, http://blogs.zdnet.com/security/?p=5508, http://pandalabs.pandasecurity.com/kneber-another-bot-yet/, http://blog.scansafe.com/journal/2010/2/18/zeus-kneber-botnet-cache-discovered.html, http://www.sophos.com/blogs/gc/g/2010/02/19/zeus-kneber-botnet-unmasked/, http://blog.threatfire.com/2010/02/a-zbot-botnet-dubbed-kneber.html, http://www.symantec.com/connect/fr/blogs/kneber-zeus, http://www.f-secure.com/weblog/archives/00001887.html

[14] See, comment by Brian Krebs, http://www.krebsonsecurity.com/2010/02/zeus-a-virus-known-as-botnet/

[15] http://www.networkforensics.com/2010/02/18/move-over-china-here-comes-russia/

[16] http://www.networkforensics.com/2010/02/19/kneber-update/

[17] http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html

[18] http://www.krebsonsecurity.com/2010/02/zeus-attack-spoofs-nsa-targets-gov-and-mil/

[19] http://www.krebsonsecurity.com/2010/02/warning-about-zeus-attack-used-as-lure/

[20] http://www.sophos.com/blogs/sophoslabs/?p=8654

[21] http://intelfusion.net/wordpress/2010/02/08/russian-spear-phishing-attack-against-mil-and-gov-employees/

[22] http://intelfusion.net/wordpress/2010/02/11/define-irony-a-phishing-attack-disguised-as-a-warning-from-an-infosec-

author-about-a-phishing-attack/

[23] http://intelfusion.net/wordpress/2010/02/19/u-s-government-departments-and-agencies-hit-by-the-zeus-trojan/

[24] https://zeustracker.abuse.ch/monitor.php host=updatekernel.com&id=7f6a3e6d82935254f0eafd9dc4fa450a

[25] http://www.malwaredomainlist.com/mdl.php?search=115.100.250.&colsearch=All&quantity=50

[26] http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html, http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html, http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

[27] http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

[28] http://www.malwareurl.com/search.php?domain=&s=stallvars&match=0&rp=50&urls=on&redirs=on&ip=on&reverse=on&as=on