The Underground Economy of the Pay-Per-Install (PPI) Business

Kevin Stevens, Security Researcher
SecureWorks Counter Threat Unit (CTU)℠

History of the PPI Business

The Pay-Per-Install business model (PPI) has existed for years. When the PPI business first started, it was used to distribute advertisements. Today it is mainly used to spread spyware and malware. PPI starts with an “affiliate” interested in building a network of infected computers or earning money. The affiliate signs up to a PPI site and receives a file from the PPI provider. The PPI-provided files were originally a variant of adware program. The affiliate “binds” the PPI-provided file with another program that they might host on their site. A binder is a program that can combine the adware provided by the PPI site with a known program. Whoever downloads the program gets the adware installed on their computer. The affiliate is paid per install of that adware that the PPI site sent them.

PPI Goes From Pushing Adware to Spyware and Malware

The PPI business has seen significant and malicious changes over the years. It has gone from having victims unknowingly download and install adware to having them download and install spyware and malware. While some PPI sites are still distributing adware, the majority push malware and spyware to unsuspecting users. These PPI sites create an underground economy that profits from installing malware. This economy is so widespread that there is even a side business selling programs to make it more difficult for computer users to detect that they are installing something malicious.

We will first look at www.pay-per-install.org. This site hosts a forum where affiliates come together to discuss the PPI business and how to make money. This site is used for a variety of reasons:

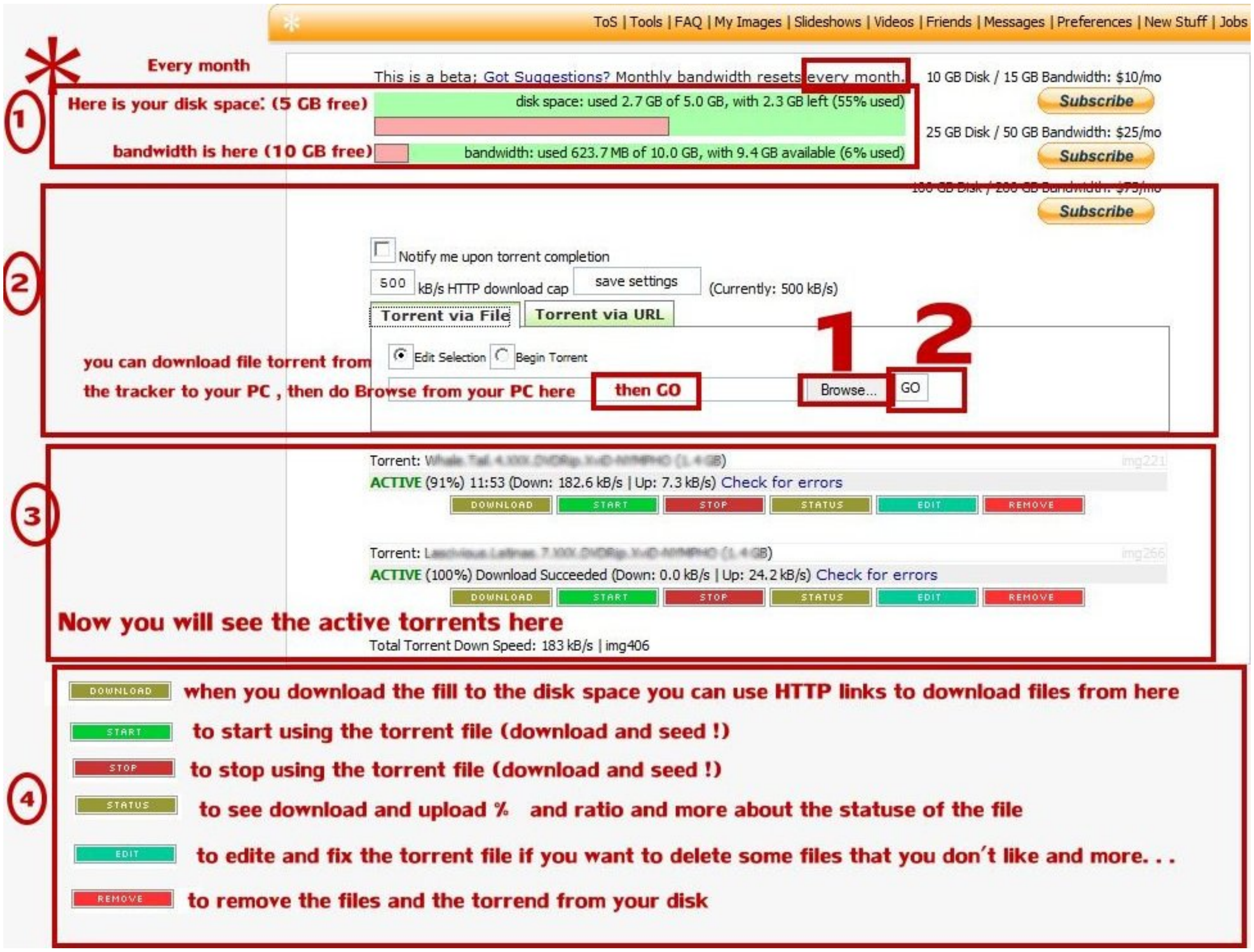
- Lists affiliate programs organized in a way that affiliates can get an idea which PPI business is paying the most and paying reliably for installs.
- Provides a forum for affiliates to discuss how to make money the fastest and how to advertise their links to get victims to download their installs.
- Tutorials and guides to get affiliates started in the PPI business.

Methods and Tools

Many affiliates of the different PPI sites have various methods and tools they use to maximize the effectiveness of their malware-packed download. One suggested method is the use of peer-to-peer (P2P) networks. Affiliates recommend using BitTorrent or eMule, two of the most popular P2P networks. Once the affiliate signs up with the PPI site and receives the malicious file, the affiliate must choose a file to “bind” to the malicious file. Most affiliates access BitTorrent and download a legitimate program or game crack, bind the malicious file with the legitimate program that they downloaded, upload the bundled file to the torrent sites and advertise that file as the original non-modified file. The goal is to have computer users download the malicious bundled file and execute it, thinking that they are actually installing a useful program and not malware. The affiliate gets paid after the file is installed on the victim's computer.

Seedboxes

One challenge affiliates encounter is that they must perform hundreds to thousands of installs to receive any significant income, which is why sites like www.pay-per-install.org exist to provide guidance. To address this challenge, many affiliates use a seedbox, or a private dedicated server used for the uploading and downloading of digital files. Affiliates use a seedbox to rapidly spread their malware-infected files using BitTorrent and eMule, avoiding the need to host the files on their computer. This can be a labor intensive process because once a P2P site discovers the malware in the uploaded affiliate file, that file is deleted or gets banned from the P2P network. Many affiliates take precautions to avoid this scenario by using special tools such as crypters to hide their files.


ToS | Tools | FAQ | My Images | Slideshows | Videos | Friends | Messages | Preferences | New Stuff | Jobs

Every month

This is a beta; Got Suggestions? Monthly bandwidth resets every month.

10 GB Disk / 15 GB Bandwidth: $10/mo

25 GB Disk / 50 GB Bandwidth: $25/mo

100 GB Disk / 200 GB Bandwidth: $75/mo

1 Here is your disk space: (5 GB free)

disk space: used 2.7 GB of 5.0 GB, with 2.3 GB left (55% used)

bandwidth is here (10 GB free)

bandwidth: used 623.7 MB of 10.0 GB, with 9.4 GB available (6% used)

2

□ Notify me upon torrent completion

500 kB/s HTTP download cap [save settings] (Currently: 500 kB/s)

● Edit Selection ○ Begin Torrent

you can download file torrent from the tracker to your PC , then do Browse from your PC here then GO

3

Torrent: [redacted]) img221

ACTIVE (91%) 11:53 (Down: 182.6 kB/s | Up: 7.3 kB/s) Check for errors

Torrent: [redacted]) img266

ACTIVE (100%) Download Succeeded (Down: 0.0 kB/s | Up: 24.2 kB/s) Check for errors

Now you will see the active torrents here

Total Torrent Down Speed: 183 kB/s | img406

4

DOWNLOAD when you download the fill to the disk space you can use HTTP links to download files from here

START to start using the torrent file (download and seed !)

STOP to stop using the torrent file (download and seed !)

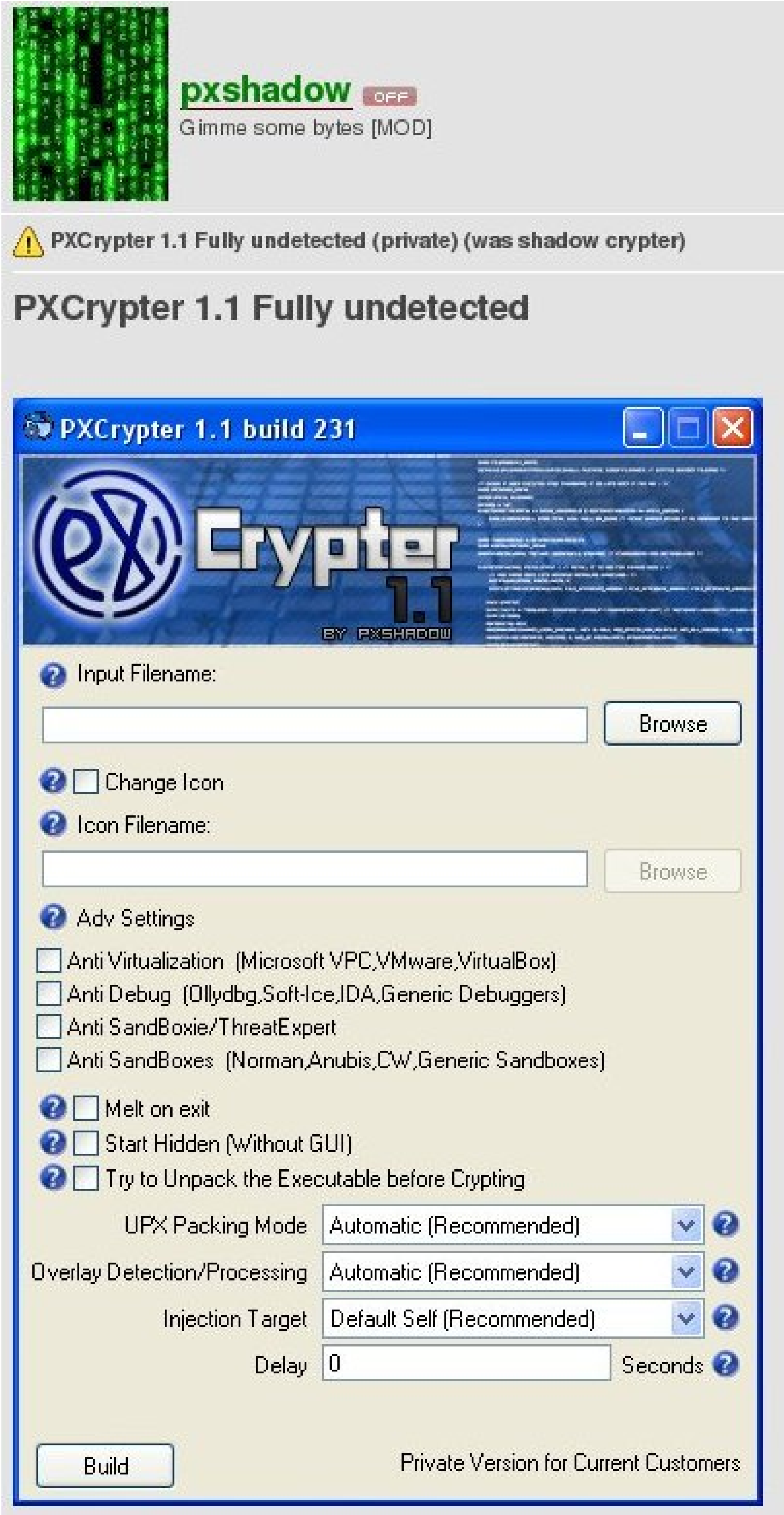
STATUS to see download and upload % and ratio and more about the statuse of the file

EDIT to edite and fix the torrent file if you want to delete some files that you don't like and more. . .

REMOVE to remove the files and the torrend from your disk

Crypters

One type of program that www.pay-per-install.org sells is called a crypter. Crypters are programs that hide malicious files from anti-virus (AV) solutions intended to protect your computer. Crypters are used to make a malicious file fully undetectable (FUD). Making files FUD is a money-making business in the world of malware. For example, the crypter on www.pay-per-install.org is called PXCrypter and is currently on version 1.1. Affiliates usually receive free upgrades when the author updates the crypter. This crypter sells for $75 and includes 1 stub; additional stubs are $25. The stub is the code that decrypts the rest of the program when it is executed. Because the stub must be available to perform the decryption, it can't be encrypted and is eventually identified by AV programs as malicious. To avoid this situation from occurring, crypters are sold with several stubs, with more available for an additional price.



pxshadow OFF

Gimme some bytes [MOD]

⚠ **PXCrypter 1.1 Fully undetected (private) (was shadow crypter)**

PXCrypter 1.1 Fully undetected

PXCrypter 1.1 build 231

Input Filename:

Browse

□ Change Icon

Icon Filename:

Browse

Adv Settings

□ Anti Virtualization (Microsoft VPC,VMware,VirtualBox)

□ Anti Debug (Ollydbg,Soft-Ice,IDA,Generic Debuggers)

□ Anti SandBoxie/ThreatExpert

□ Anti SandBoxes (Norman,Anubis,CW,Generic Sandboxes)

□ Melt on exit

□ Start Hidden (Without GUI)

□ Try to Unpack the Executable before Crypting

UPX Packing Mode: Automatic (Recommended)

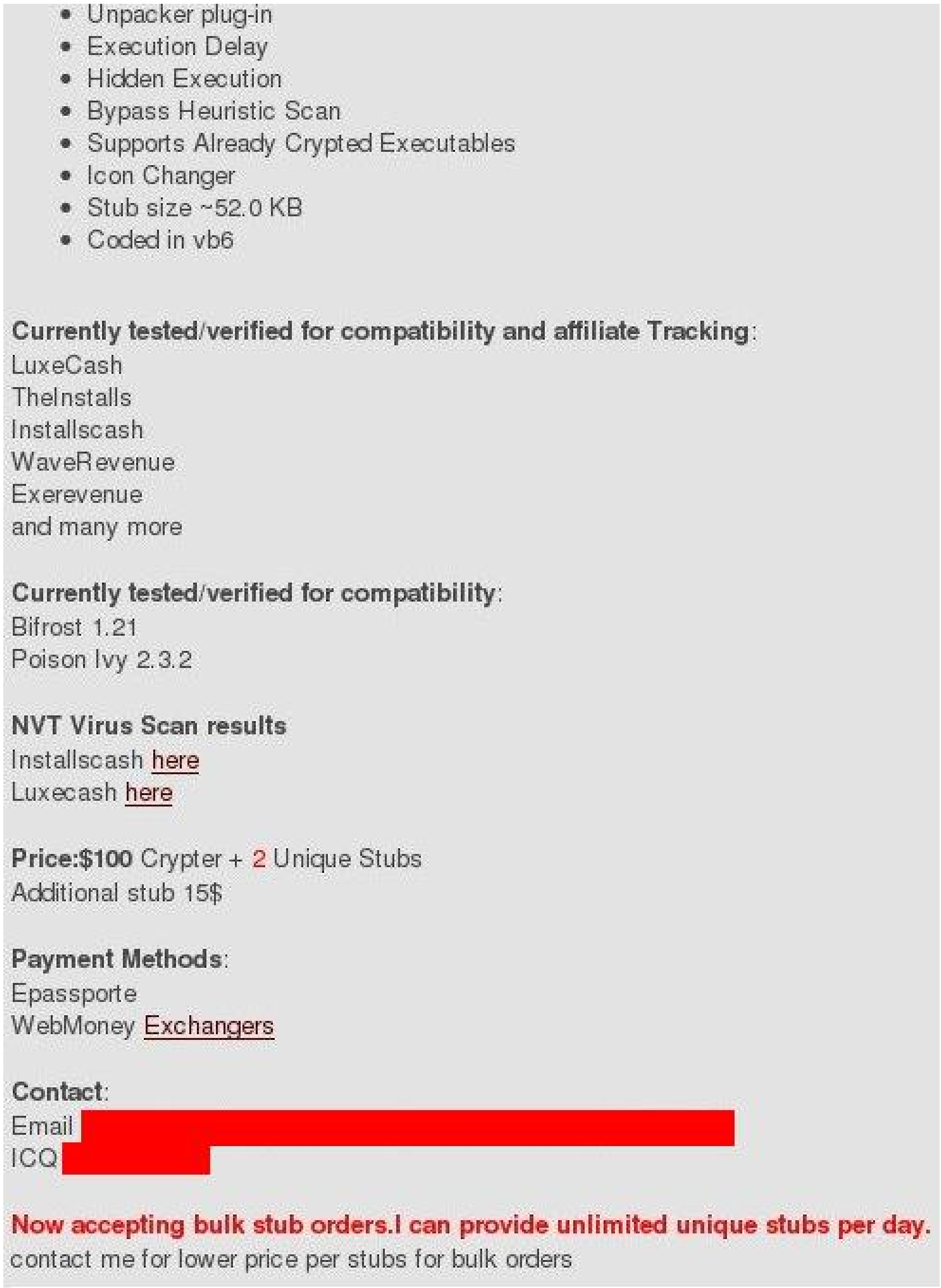
Overlay Detection/Processing: Automatic (Recommended)

Injection Target: Default Self (Recommended)

Delay: 0 Seconds

Build

Private Version for Current Customers



- Unpacker plug-in
- Execution Delay
- Hidden Execution
- Bypass Heuristic Scan
- Supports Already Crypted Executables
- Icon Changer
- Stub size ~52.0 KB
- Coded in vb6

Currently tested/verified for compatibility and affiliate Tracking:
LuxeCash
TheInstalls
Installscash
WaveRevenue
Exerevenue
and many more

Currently tested/verified for compatibility:
Bifrost 1.21
Poison Ivy 2.3.2

NVT Virus Scan results
Installscash here
Luxecash here

Price:$100 Crypter + 2 Unique Stubs
Additional stub 15$

Payment Methods:
Epassporte
WebMoney Exchangers

Contact:
Email [redacted]
ICQ [redacted]

Now accepting bulk stub orders.I can provide unlimited unique stubs per day.
contact me for lower price per stubs for bulk orders

PXCrypter has been written to work with many PPI affiliate files, has many features to avoid detection by AV software and prevents a malicious file from running in a sandbox. Sandboxes are often used by security researchers to create a virtual environment where malicious programs can run and be observed without causing damage to the computer or its operating system. Sandboxing is a good way to determine malware behavior and design effective protection techniques and countermeasures.

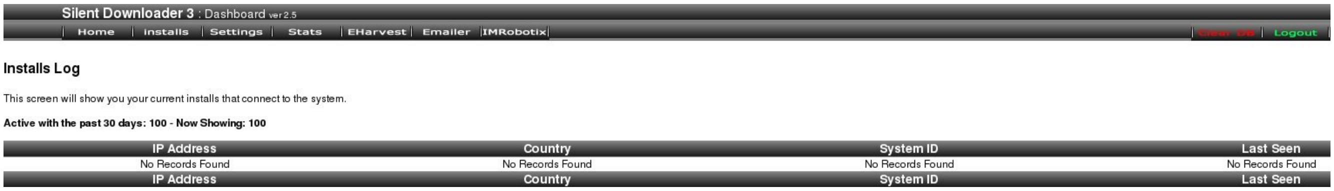
Trojan Download Manager

Another type of tool used by affiliates is a Trojan Download Manager. A Trojan Download Manager is commonly seen in the blackhat malware communities because it allows an attacker to update any malware that has been downloaded by a victim’s computer, install additional malware, and perform any other functions that the Trojan Downloader Manager software author has designed.

The www.pay-per-install.org site has a Trojan Downloader Manager program for sale called SDdownloader or Silent Downloader. SDdownloader normally sells for $300; however, it is currently on special for $225. It is at version 3, with version 4 being developed and includes:

- One unique stub to decrypt the malware and minimize its visibility to antivirus software
- Binder software to combine the malware file with another file sought by a victim
- A web interface to track statistics for infected computers
- An interface to make the infected PC a SOCKS proxy, allowing an attacker to funnel malicious network traffic through the infected computer
- Tools to download more malware to the already infected computer

Trojan Download Managers are popular because they not only allow attackers to infect the computer, but they can also force the computer to download and install any PPI files or malware at the attacker’s command.



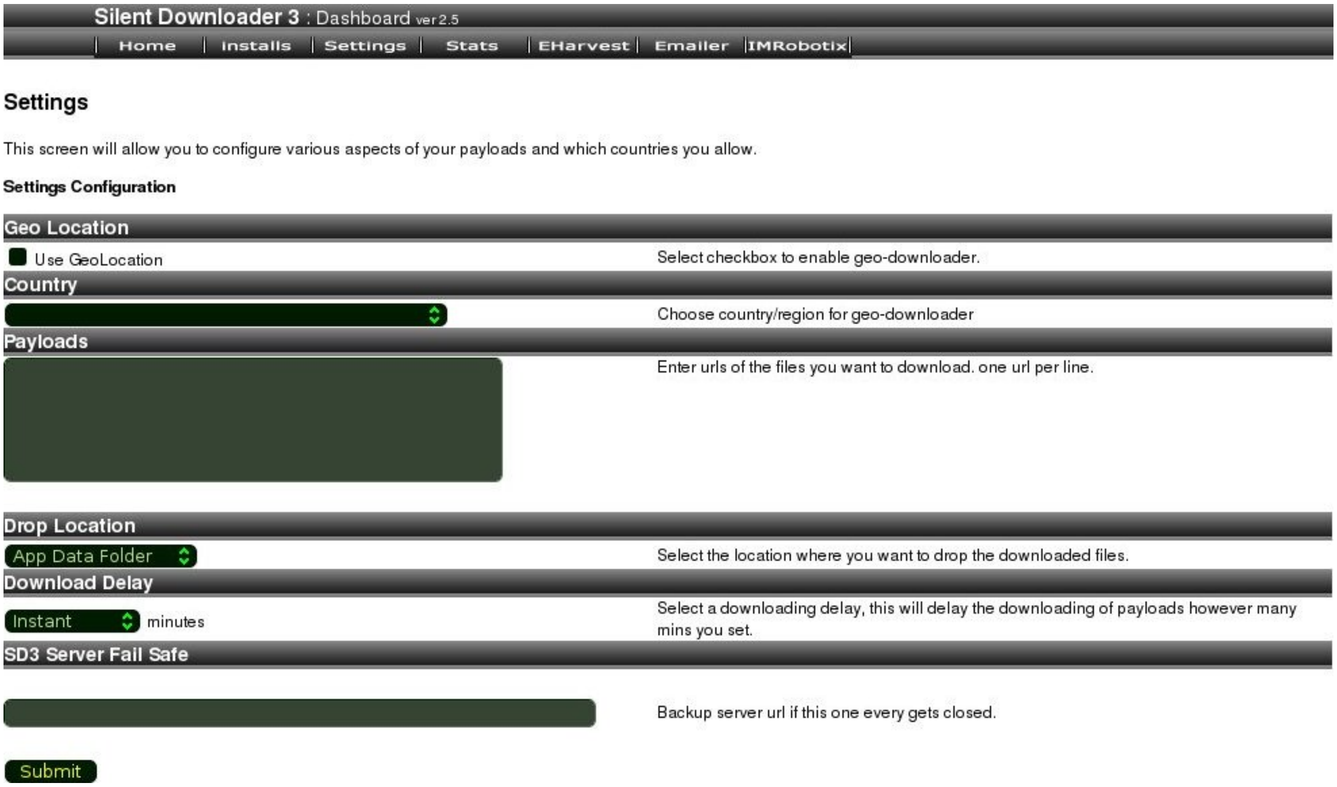
Installs Log

This screen will show you your current installs that connect to the system.

Active with the past 30 days: 100 - Now Showing: 100

IP Address	Country	System ID	Last Seen
No Records Found	No Records Found	No Records Found	No Records Found
IP Address	Country	System ID	Last Seen

This is the interface that displays how many bots are installed.



Settings

This screen will allow you to configure various aspects of your payloads and which countries you allow.

Settings Configuration

Geo Location

■ Use GeoLocation — Select checkbox to enable geo-downloader.

Country

Choose country/region for geo-downloader

Payloads

Enter urls of the files you want to download. one url per line.

Drop Location

App Data Folder — Select the location where you want to drop the downloaded files.

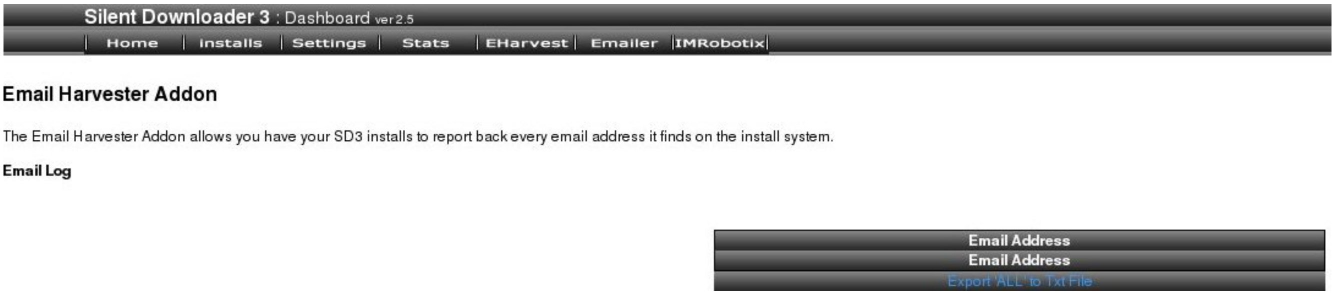
Download Delay

Instant minutes — Select a downloading delay, this will delay the downloading of payloads however many mins you set.

SD3 Server Fail Safe

Backup server url if this one every gets closed.

This interface shows the settings for the files to be installed. Bot operators can put a delay on files to be installed, switch out payloads, define where the payloads are installed, create server failsafes, and even use geolocation to choose which countries get which malware.



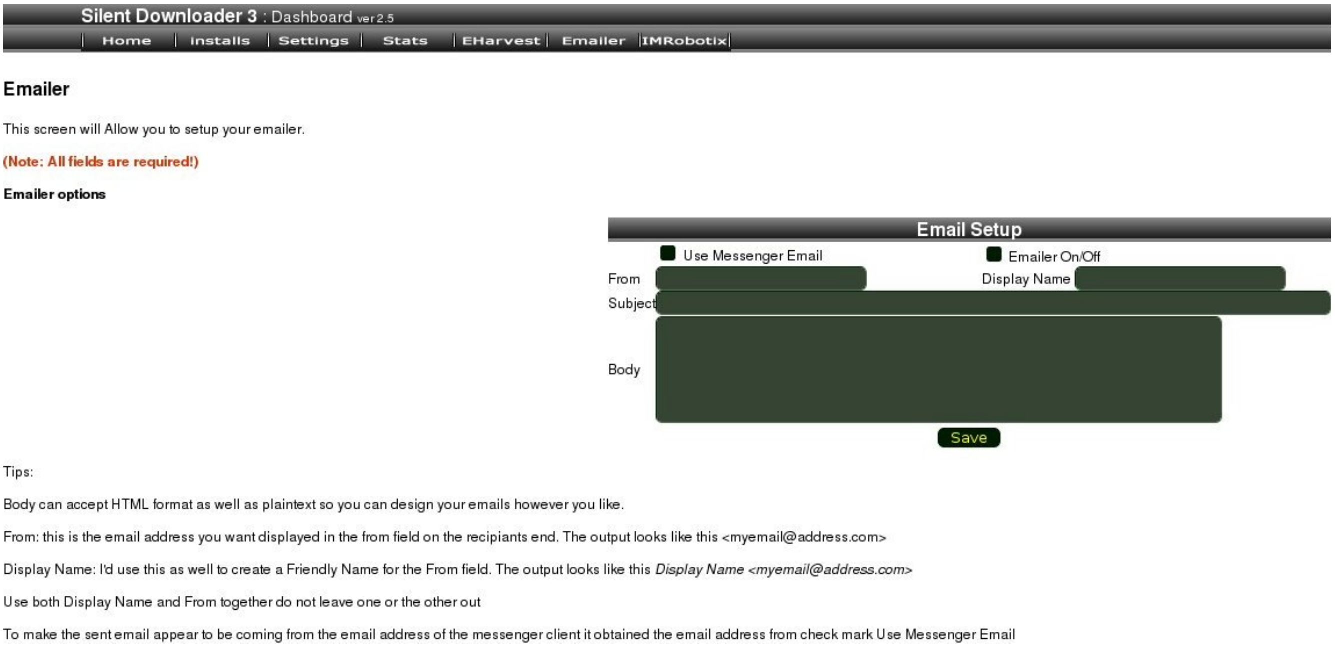
Email Harvester Addon

The Email Harvester Addon allows you have your SD3 installs to report back every email address it finds on the install system.

Email Log

Email Address
Email Address
Export 'ALL' to Txt File

This screenshot shows the email harvester addon. This addon allows SDdownloader to harvest all email addresses on an infected system.



Emailer

This screen will Allow you to setup your emailer.

(Note: All fields are required!)

Emailer options

Email Setup

■ Use Messenger Email ■ Emailer On/Off

From Display Name

Subject

Body

Save

Tips:

Body can accept HTML format as well as plaintext so you can design your emails however you like.

From: this is the email address you want displayed in the from field on the recipiants end. The output looks like this <myemail@address.com>

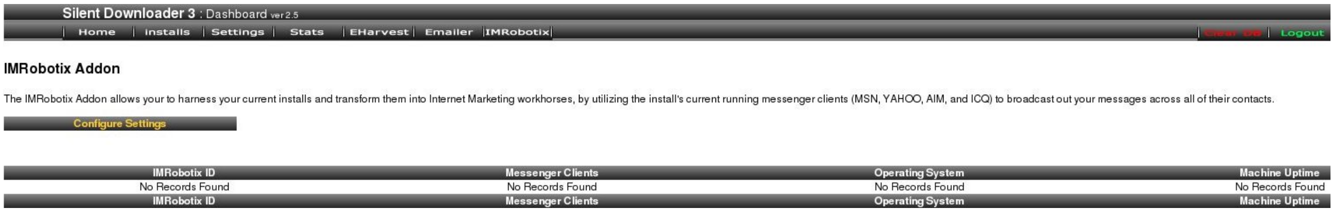
Display Name: I'd use this as well to create a Friendly Name for the From field. The output looks like this *Display Name <myemail@address.com>*

Use both Display Name and From together do not leave one or the other out

To make the sent email appear to be coming from the email address of the messenger client it obtained the email address from check mark Use Messenger Email

This screenshot shows a setup interface for sending emails or spam from the bot(s). Provided on the web page is a list of tips for this addon:

- Body can accept HTML format as well as plaintext so you can design your emails however you like.
- From: this is the email address you want displayed in the from field on the recipiants end. The output looks like this <myemail@address.com>
- Display Name: I'd use this as well to create a Friendly Name for the From field. The output looks like this *Display Name <myemail@address.com>*
- Use both Display Name and From together do not leave one or the other out
- To make the sent email appear to be coming from the email address of the messenger client it obtained the email address from check mark Use Messenger Email



IMRobotix Addon

The IMRobotix Addon allows your to harness your current installs and transform them into Internet Marketing workhorses, by utilizing the install's current running messenger clients (MSN, YAHOO, AIM, and ICQ) to broadcast out your messages across all of their contacts.

IMRobotix ID	Messenger Clients	Operating System	Machine Uptime
No Records Found	No Records Found	No Records Found	No Records Found
IMRobotix ID	Messenger Clients	Operating System	Machine Uptime

This figure displays the IMRobotix addon page. The IMRobotix Addon allows the bot controller to use the bot as an Instant Messaging (IM) spam computer. It will use IM clients such as MSN Messenger, Yahoo! Instant Messenger, AIM, and ICQ to spam all of the available bots' contacts.

Black Hat Search Engine Optimization (SEO)

A scammer who doesn't want to use P2P but wants traffic directed to their site that hosts malicious files can use black hat SEO techniques. Black hat SEO increases the volume of traffic to a web site by manipulating search engines. The user clicks the link in response to their search query and the victim's computer visits the site, where exploits hijack vulnerable computers using a technique known as drive-by downloads. After the site compromises the victim's computer, an attacker can successfully transfer and install as much malware as they want.

Attackers use tools such as XRumer to perform these tasks. XRumer is an auto-submitter program that posts messages to forums, guestbooks, bulletin boards and catalogs. An auto-submitter's purpose is to announce the attacker's site URL throughout the Internet to increase search engine rankings and display the site at or near the top of search engine results. This software also helps advertise the attacker's site URL so more people might be willing to click on it in a guestbook or forum posting.

Doorway Pages

Another method used by attackers to increase traffic so more victims will visit their site and download malicious files is the use of a doorway or doorway pages. Doorway pages are similar to SEO, but the goal is to increase the search ranking of the doorway page instead of the attacker's site. The doorway is simply a web page that may list many keywords in an attempt to increase the search engine ranking. This doorway page will not contain any malicious files to download, so it will not be removed from search engines or blacklisted. Instead, the doorway page contains scripts that redirect the victim's computer to the attacker's malicious or scamming adware page, where malware or adware may be downloaded to vulnerable computers.

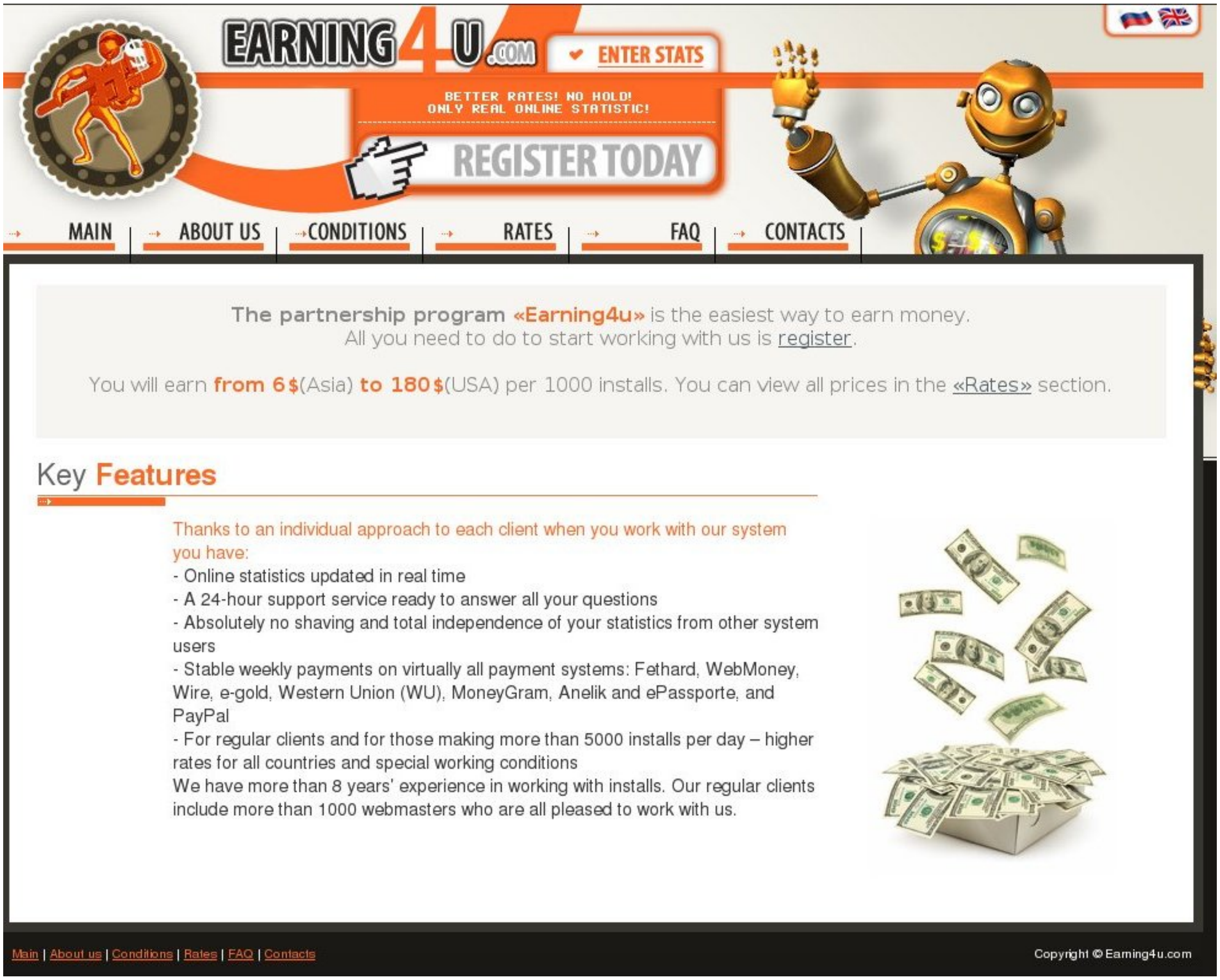
The PPI sites

Pay-per-install.org references a number of PPI sites that offer to pay affiliates to install programs on victims' computers. Most affiliates judge PPI sites by two main criteria: how much they pay and how honest they are. In PPI jargon, 'shaving' is the act of not counting some installations by affiliates. Some PPI sites are accused of shaving a portion of installations from the affiliates' total. Most affiliates want to sign up to a PPI site that has a good reputation and pays on time. Affiliates can work with many different PPI sites simultaneously to maximize their income.

Earning4u.com (formerly InstallsCash)

The Earning4u site is a startup that is reportedly a descendent of the InstallsCash web site. InstallsCash disappeared around the same time Earning4u became active. Earning4u.com only pays in increments of 1000 installs. The screenshots of the web site display pricing that is similar to that of InstallsCash, which shows that some things have not changed. The look and feel is different for the Earning4u site, but it has the same language options as InstallsCash of Russian and English. Earning4u has a Russian IP claims they are registered to a software company in China.

The site claims to have been in business since 2001, allegedly employs a team of 20 professionals, and claims to have over 1000 registered affiliates. The site processes payments using the same payment systems as InstallsCash in addition to e-gold and PayPal. One item of interest is that they refuse to pay for installations on Russian or any CIS-based (Commonwealth of Independent States, or former Soviet Republic) computers.



The partnership program «Earning4u» is the easiest way to earn money.
All you need to do to start working with us is register.

You will earn from 6$(Asia) to 180$(USA) per 1000 installs. You can view all prices in the «Rates» section.

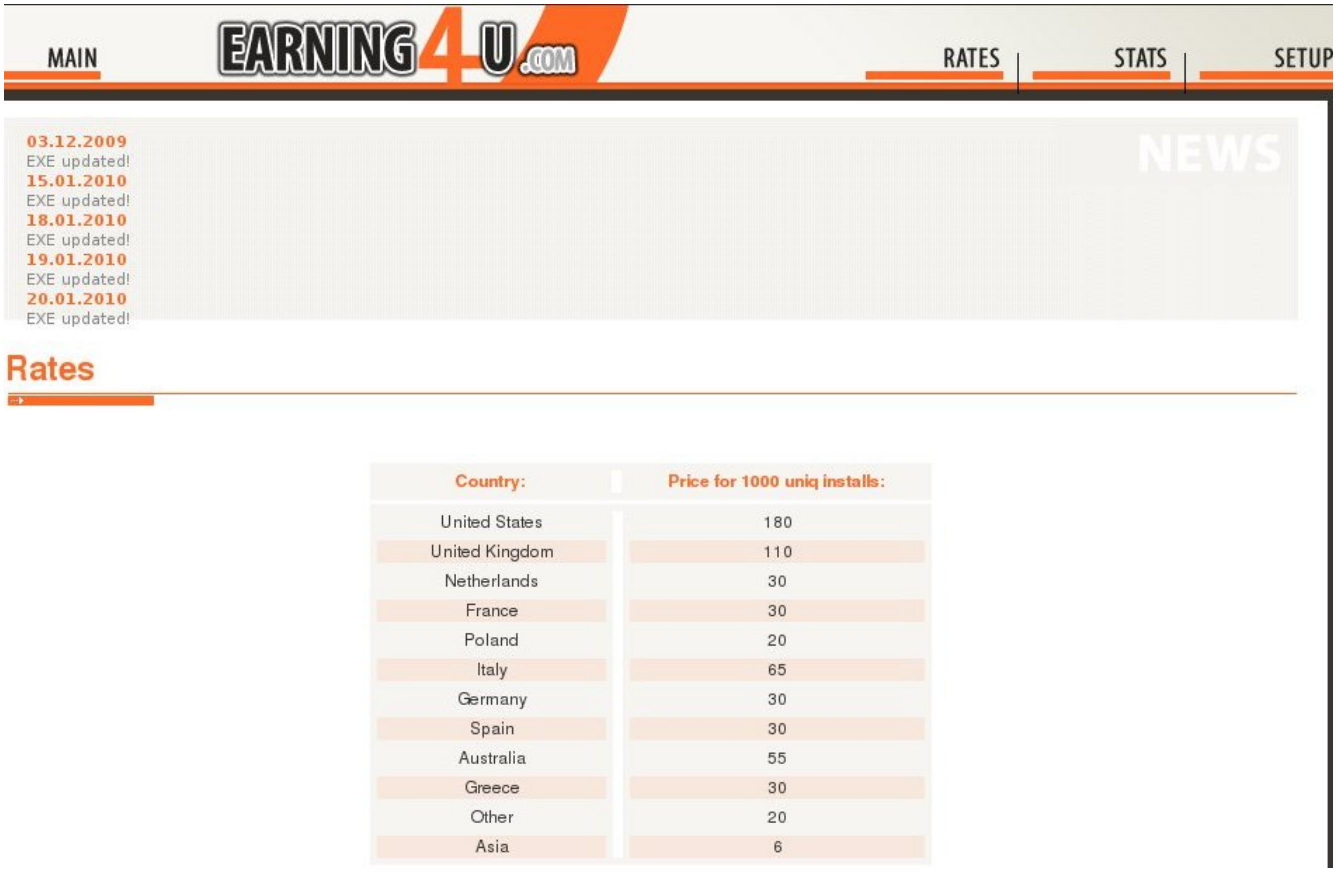
Key Features

Thanks to an individual approach to each client when you work with our system you have:
- Online statistics updated in real time
- A 24-hour support service ready to answer all your questions
- Absolutely no shaving and total independence of your statistics from other system users
- Stable weekly payments on virtually all payment systems: Fethard, WebMoney, Wire, e-gold, Western Union (WU), MoneyGram, Anelik and ePassporte, and PayPal
- For regular clients and for those making more than 5000 installs per day – higher rates for all countries and special working conditions
We have more than 8 years' experience in working with installs. Our regular clients include more than 1000 webmasters who are all pleased to work with us.

Main | About us | Conditions | Rates | FAQ | Contacts

Copyright © Earning4u.com

This is the home page for earning4u.com. It lists what they consider the key features of their service that puts them above what other affiliate programs offer.

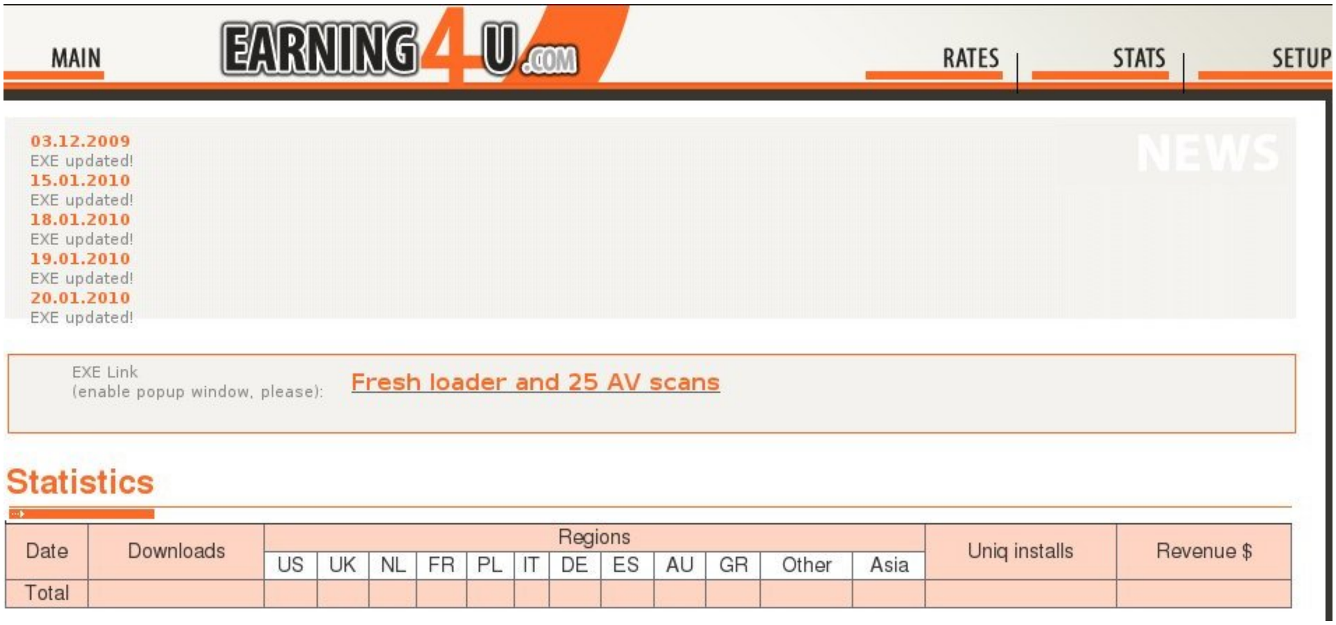


03.12.2009
EXE updated!
15.01.2010
EXE updated!
18.01.2010
EXE updated!
19.01.2010
EXE updated!
20.01.2010
EXE updated!

Rates

Country:	Price for 1000 uniq installs:
United States	180
United Kingdom	110
Netherlands	30
France	30
Poland	20
Italy	65
Germany	30
Spain	30
Australia	55
Greece	30
Other	20
Asia	6

The rates page lists prices per 1000 unique installations. The highest paid installs are for the U.S. at $180 and the United Kingdom at $110. At the bottom of the list is Asia at $6 per 1000 installations.



03.12.2009
EXE updated!
15.01.2010
EXE updated!
18.01.2010
EXE updated!
19.01.2010
EXE updated!
20.01.2010
EXE updated!

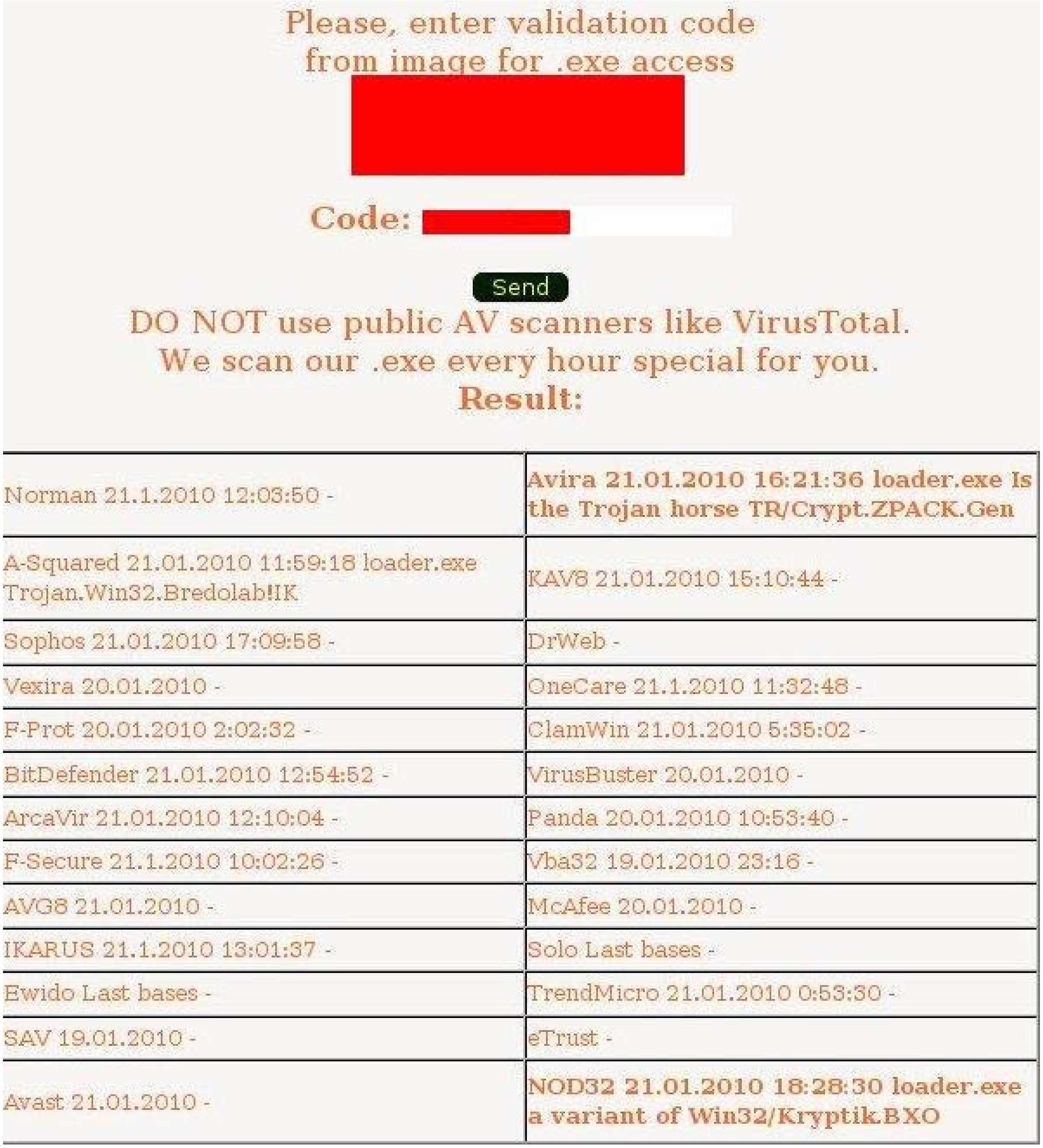
EXE Link
(enable popup window, please): Fresh loader and 25 AV scans

Statistics

Date	Downloads	Regions												Uniq installs	Revenue $
		US	UK	NL	FR	PL	IT	DE	ES	AU	GR	Other	Asia		
Total															

The “silent loader” software that can be downloaded and distributed by the affiliate will download and install a nasty malware combination. The initial executable file is the Piptea

Trojan horse downloader. Piptea’s main purpose is to download multiple malware programs onto the infected system.



Please, enter validation code
from image for .exe access

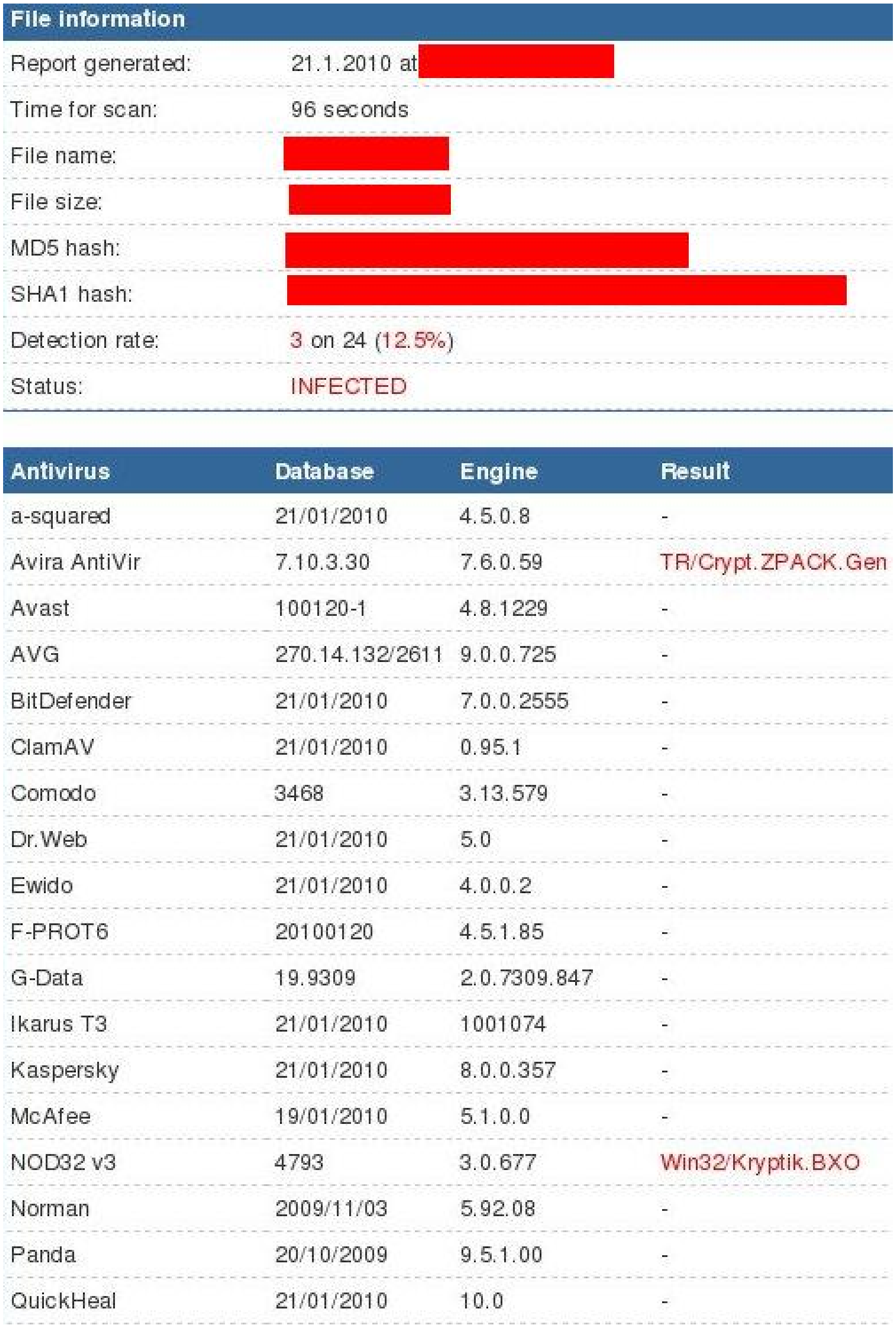
[redacted]

Code: [redacted]

DO NOT use public AV scanners like VirusTotal.
We scan our .exe every hour special for you.
Result:

Norman 21.1.2010 12:03:50 -	**Avira 21.01.2010 16:21:36 loader.exe Is the Trojan horse TR/Crypt.ZPACK.Gen**
A-Squared 21.01.2010 11:59:18 loader.exe Trojan.Win32.Bredolab!IK	KAV8 21.01.2010 15:10:44 -
Sophos 21.01.2010 17:09:58 -	DrWeb -
Vexira 20.01.2010 -	OneCare 21.1.2010 11:32:48 -
F-Prot 20.01.2010 2:02:32 -	ClamWin 21.01.2010 5:35:02 -
BitDefender 21.01.2010 12:54:52 -	VirusBuster 20.01.2010 -
ArcaVir 21.01.2010 12:10:04 -	Panda 20.01.2010 10:53:40 -
F-Secure 21.1.2010 10:02:26 -	Vba32 19.01.2010 23:16 -
AVG8 21.01.2010 -	McAfee 20.01.2010 -
IKARUS 21.1.2010 13:01:37 -	Solo Last bases -
Ewido Last bases -	TrendMicro 21.01.2010 0:53:30 -
SAV 19.01.2010 -	eTrust -
Avast 21.01.2010 -	**NOD32 21.01.2010 18:28:30 loader.exe a variant of Win32/Kryptik.BXO**

Earning4u scans the malware to demonstrate how undetected it is and so that the affiliate will not upload it to a virus scanning site and potentially compromise its stealth.



File information	
Report generated:	21.1.2010 at [redacted]
Time for scan:	96 seconds
File name:	[redacted]
File size:	[redacted]
MD5 hash:	[redacted]
SHA1 hash:	[redacted]
Detection rate:	3 on 24 (12.5%)
Status:	INFECTED

Antivirus	Database	Engine	Result
a-squared	21/01/2010	4.5.0.8	-
Avira AntiVir	7.10.3.30	7.6.0.59	TR/Crypt.ZPACK.Gen
Avast	100120-1	4.8.1229	-
AVG	270.14.132/2611	9.0.0.725	-
BitDefender	21/01/2010	7.0.0.2555	-
ClamAV	21/01/2010	0.95.1	-
Comodo	3468	3.13.579	-
Dr.Web	21/01/2010	5.0	-
Ewido	21/01/2010	4.0.0.2	-
F-PROT6	20100120	4.5.1.85	-
G-Data	19.9309	2.0.7309.847	-
Ikarus T3	21/01/2010	1001074	-
Kaspersky	21/01/2010	8.0.0.357	-
McAfee	19/01/2010	5.1.0.0	-
NOD32 v3	4793	3.0.677	Win32/Kryptik.BXO
Norman	2009/11/03	5.92.08	-
Panda	20/10/2009	9.5.1.00	-
QuickHeal	21/01/2010	10.0	-

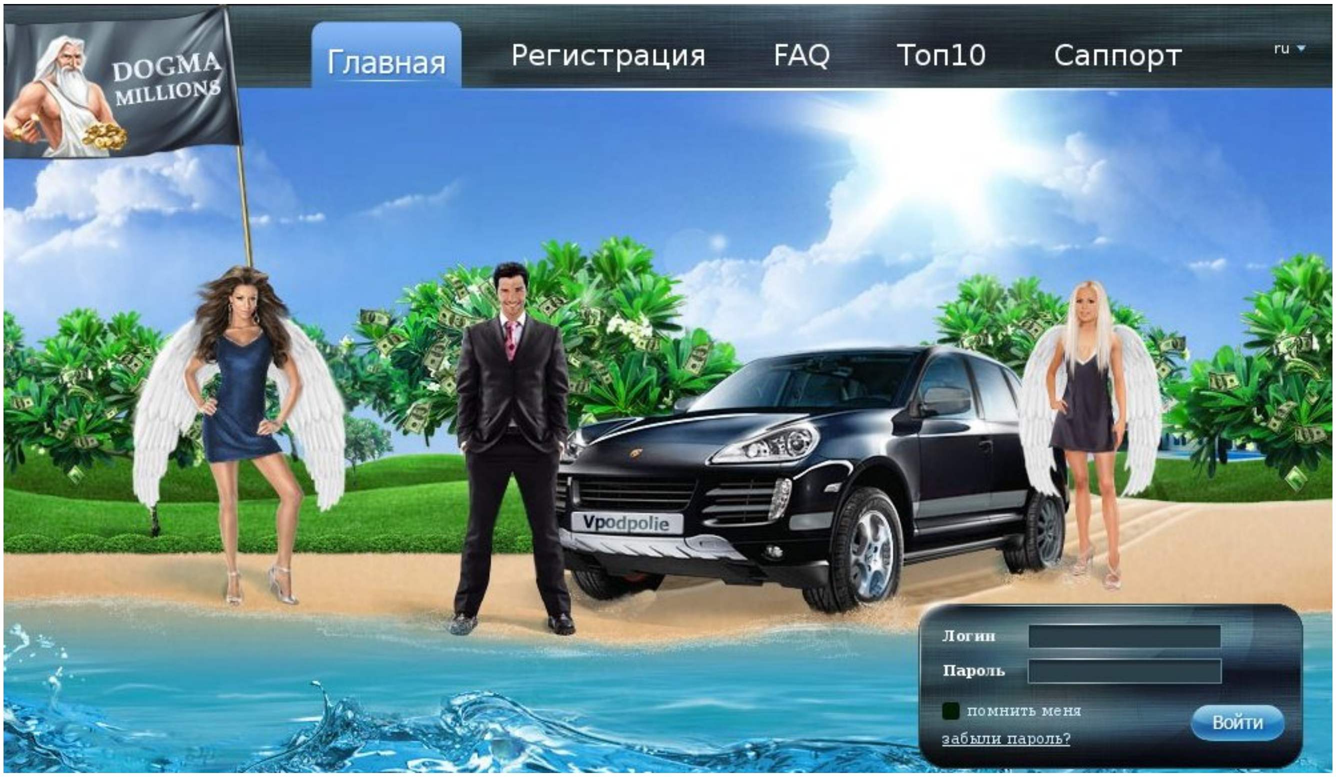
At the time of this writing, this malware is pretty much fully undetected (FUD). It is detected by only 12% of the scanners.

Earning4u.com makes the same claims for the installer as the InstallsCash installer. They claim that it is not harmful and only changes the web browser's homepage, as well as setting up a dialer to contact web sites. After the victim's computer executes the Piptea, the program phones home to http://certlxxxxx.com located in Russia.

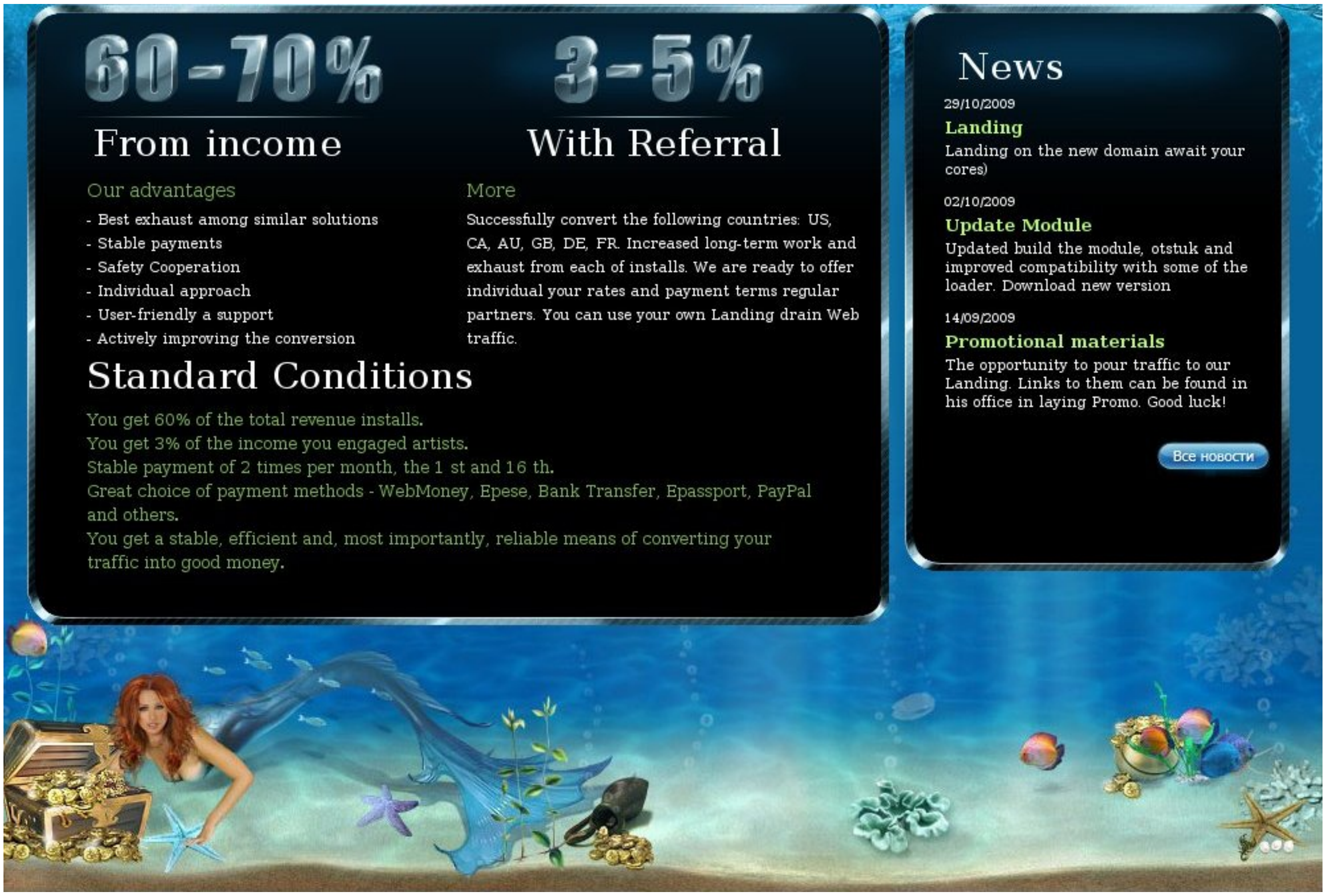
The phone home traffic to http://certlxxxxx.com consists of HTTP GET requests to download multiple pieces of malware, as well as phone home traffic that lets the malware check in with the C&C server. The other malware downloaded by Piptea consists of Ertfor downloader trojan, Butterfly Bot, Wimpixo downloader trojan, Tibs/Harnig, TDSS, an undetermined Trojan clicker, and many more.

Dogma Millions

Dogma Millions is a Russian-only PPI site that requires an invitation code to join. Affiliates have to send a message to one of the two ICQ numbers to ask for an invitation code. Just like earning4u.com, Dogma Millions does not accept Russian installations. They do not quote the going price is for installations, but instead state that affiliates receive 60% of the going price for the installation.



This is the homepage for the Dogma Millions web site. Notice how the site gives the impression that money grows on trees and features both sexy men and women.



60-70%

From income

3-5%

With Referral

Our advantages

- Best exhaust among similar solutions
- Stable payments
- Safety Cooperation
- Individual approach
- User-friendly a support
- Actively improving the conversion

More

Successfully convert the following countries: US, CA, AU, GB, DE, FR. Increased long-term work and exhaust from each of installs. We are ready to offer individual your rates and payment terms regular partners. You can use your own Landing drain Web traffic.

Standard Conditions

You get 60% of the total revenue installs.
You get 3% of the income you engaged artists.
Stable payment of 2 times per month, the 1 st and 16 th.
Great choice of payment methods - WebMoney, Epese, Bank Transfer, Epassport, PayPal and others.
You get a stable, efficient and, most importantly, reliable means of converting your traffic into good money.

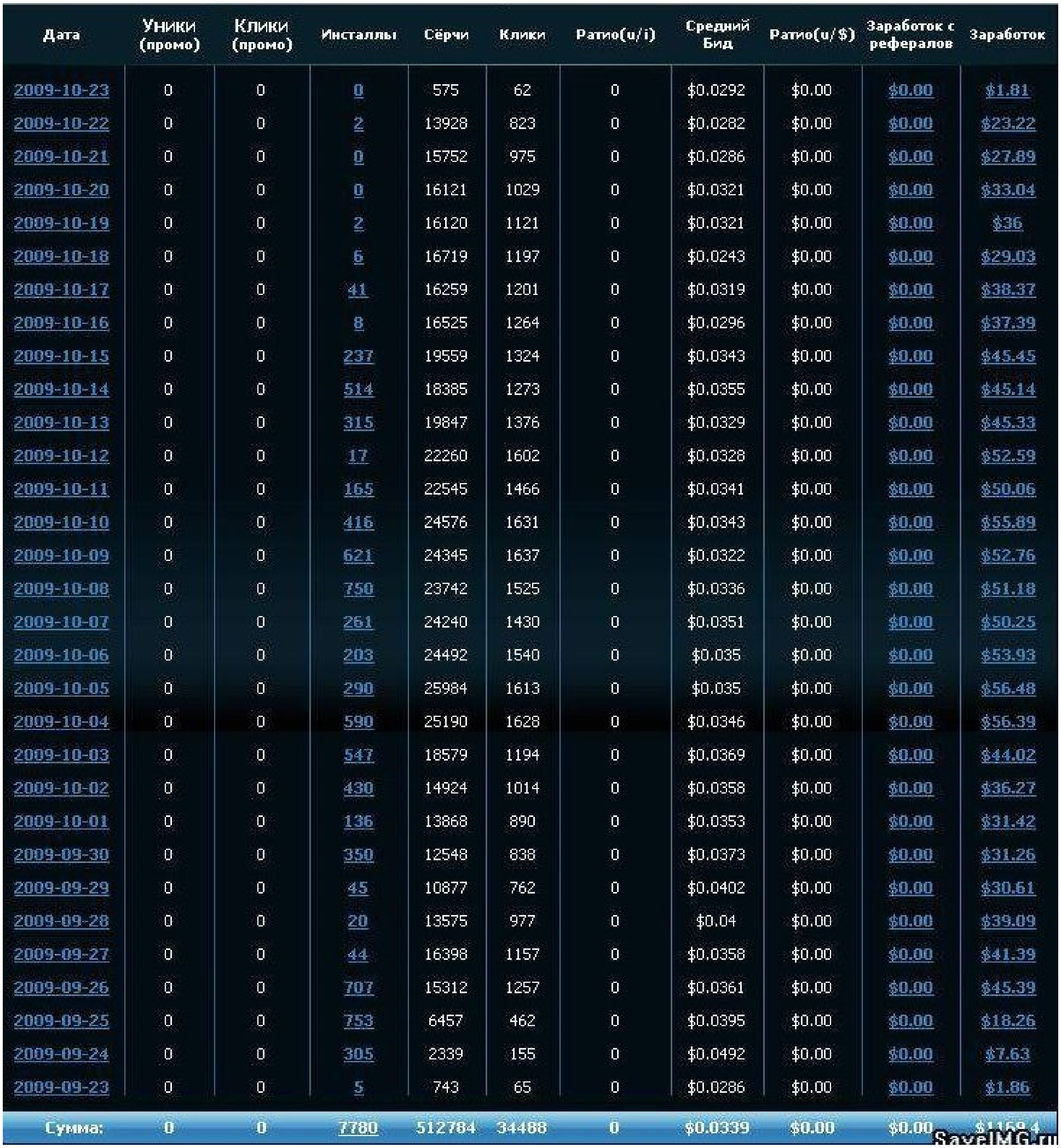
News

29/10/2009
Landing
Landing on the new domain await your cores)

02/10/2009
Update Module
Updated build the module, otstuk and improved compatibility with some of the loader. Download new version

14/09/2009
Promotional materials
The opportunity to pour traffic to our Landing. Links to them can be found in his office in laying Promo. Good luck!

This web page from Dogma Millions states that affiliates receive 60-70% of install prices and 3-5% from referrals. The site lists its key features similar to the earning4u.com web site.



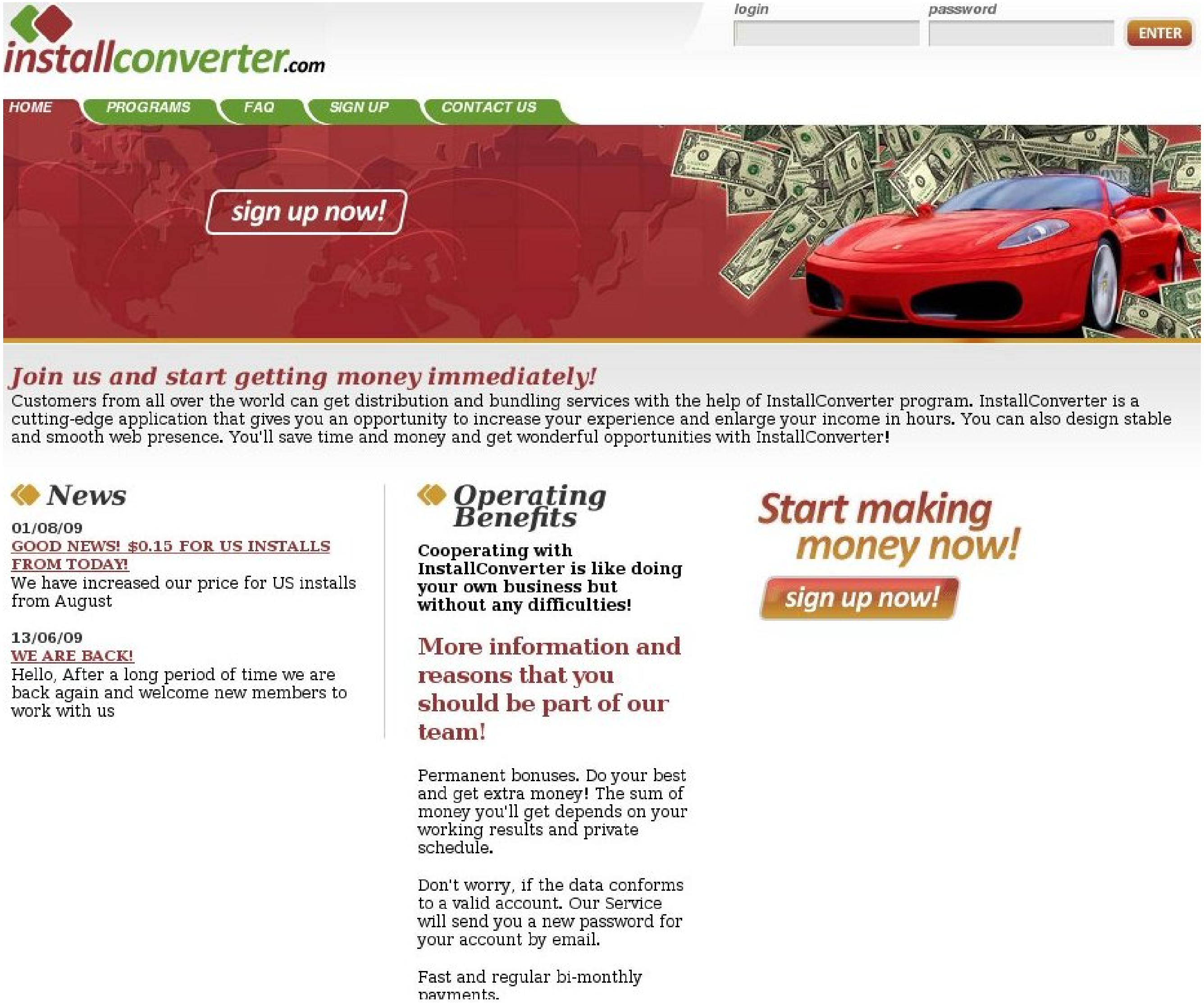
Дата	Уники (промо)	Клики (промо)	Инсталлы	Сёрчи	Клики	Ратио(u/i)	Средний Бид	Ратио(u/$)	Заработок с рефералов	Заработок
2009-10-23	0	0	0	575	62	0	$0.0292	$0.00	$0.00	$1.81
2009-10-22	0	0	2	13928	823	0	$0.0282	$0.00	$0.00	$23.22
2009-10-21	0	0	0	15752	975	0	$0.0286	$0.00	$0.00	$27.89
2009-10-20	0	0	0	16121	1029	0	$0.0321	$0.00	$0.00	$33.04
2009-10-19	0	0	2	16120	1121	0	$0.0321	$0.00	$0.00	$36
2009-10-18	0	0	6	16719	1197	0	$0.0243	$0.00	$0.00	$29.03
2009-10-17	0	0	41	16259	1201	0	$0.0319	$0.00	$0.00	$38.37
2009-10-16	0	0	8	16525	1264	0	$0.0296	$0.00	$0.00	$37.39
2009-10-15	0	0	237	19559	1324	0	$0.0343	$0.00	$0.00	$45.45
2009-10-14	0	0	514	18385	1273	0	$0.0355	$0.00	$0.00	$45.14
2009-10-13	0	0	315	19847	1376	0	$0.0329	$0.00	$0.00	$45.33
2009-10-12	0	0	17	22260	1602	0	$0.0328	$0.00	$0.00	$52.59
2009-10-11	0	0	165	22545	1466	0	$0.0341	$0.00	$0.00	$50.06
2009-10-10	0	0	416	24576	1631	0	$0.0343	$0.00	$0.00	$55.89
2009-10-09	0	0	621	24345	1637	0	$0.0322	$0.00	$0.00	$52.76
2009-10-08	0	0	750	23742	1525	0	$0.0336	$0.00	$0.00	$51.18
2009-10-07	0	0	261	24240	1430	0	$0.0351	$0.00	$0.00	$50.25
2009-10-06	0	0	203	24492	1540	0	$0.035	$0.00	$0.00	$53.93
2009-10-05	0	0	290	25984	1613	0	$0.035	$0.00	$0.00	$56.48
2009-10-04	0	0	590	25190	1628	0	$0.0346	$0.00	$0.00	$56.39
2009-10-03	0	0	547	18579	1194	0	$0.0369	$0.00	$0.00	$44.02
2009-10-02	0	0	430	14924	1014	0	$0.0358	$0.00	$0.00	$36.27
2009-10-01	0	0	136	13868	890	0	$0.0353	$0.00	$0.00	$31.42
2009-09-30	0	0	350	12548	838	0	$0.0373	$0.00	$0.00	$31.26
2009-09-29	0	0	45	10877	762	0	$0.0402	$0.00	$0.00	$30.61
2009-09-28	0	0	20	13575	977	0	$0.04	$0.00	$0.00	$39.09
2009-09-27	0	0	44	16398	1157	0	$0.0358	$0.00	$0.00	$41.39
2009-09-26	0	0	707	15312	1257	0	$0.0361	$0.00	$0.00	$45.39
2009-09-25	0	0	753	6457	462	0	$0.0395	$0.00	$0.00	$18.26
2009-09-24	0	0	305	2339	155	0	$0.0492	$0.00	$0.00	$7.63
2009-09-23	0	0	5	743	65	0	$0.0286	$0.00	$0.00	$1.86
Сумма:	0	0	7780	512784	34488	0	$0.0339	$0.00	$0.00	$1159.4

This figure displays an example list of one affiliate’s installations for one full month from September to October 23, 2009. This affiliate had 512,784 total installations, but only 34,488 unique installations. They successfully infected 34,488 computers in just one month and from just one affiliate. Dogma Millions has hundreds of affiliates and probably collects over 500,000 unique installations each month.

InstallConverter

InstallConverter is another PPI site, but it’s a bit more bland and not as flashy.

InstallConverter is unique because they offer site content to help affiliates build your own site to successfully spread installations. Quoting from their site: “Syndication is the best way to get free content and get paid for it! You can choose from different games, audio, software, multiple free videos for your website. For every new InstallConverter install produced from any country we credit for, InstallConverter gives you money.”



Join us and start getting money immediately!

Customers from all over the world can get distribution and bundling services with the help of InstallConverter program. InstallConverter is a cutting-edge application that gives you an opportunity to increase your experience and enlarge your income in hours. You can also design stable and smooth web presence. You'll save time and money and get wonderful opportunities with InstallConverter!

News

01/08/09

GOOD NEWS! $0.15 FOR US INSTALLS FROM TODAY!

We have increased our price for US installs from August

13/06/09

WE ARE BACK!

Hello, After a long period of time we are back again and welcome new members to work with us

Operating Benefits

Cooperating with InstallConverter is like doing your own business but without any difficulties!

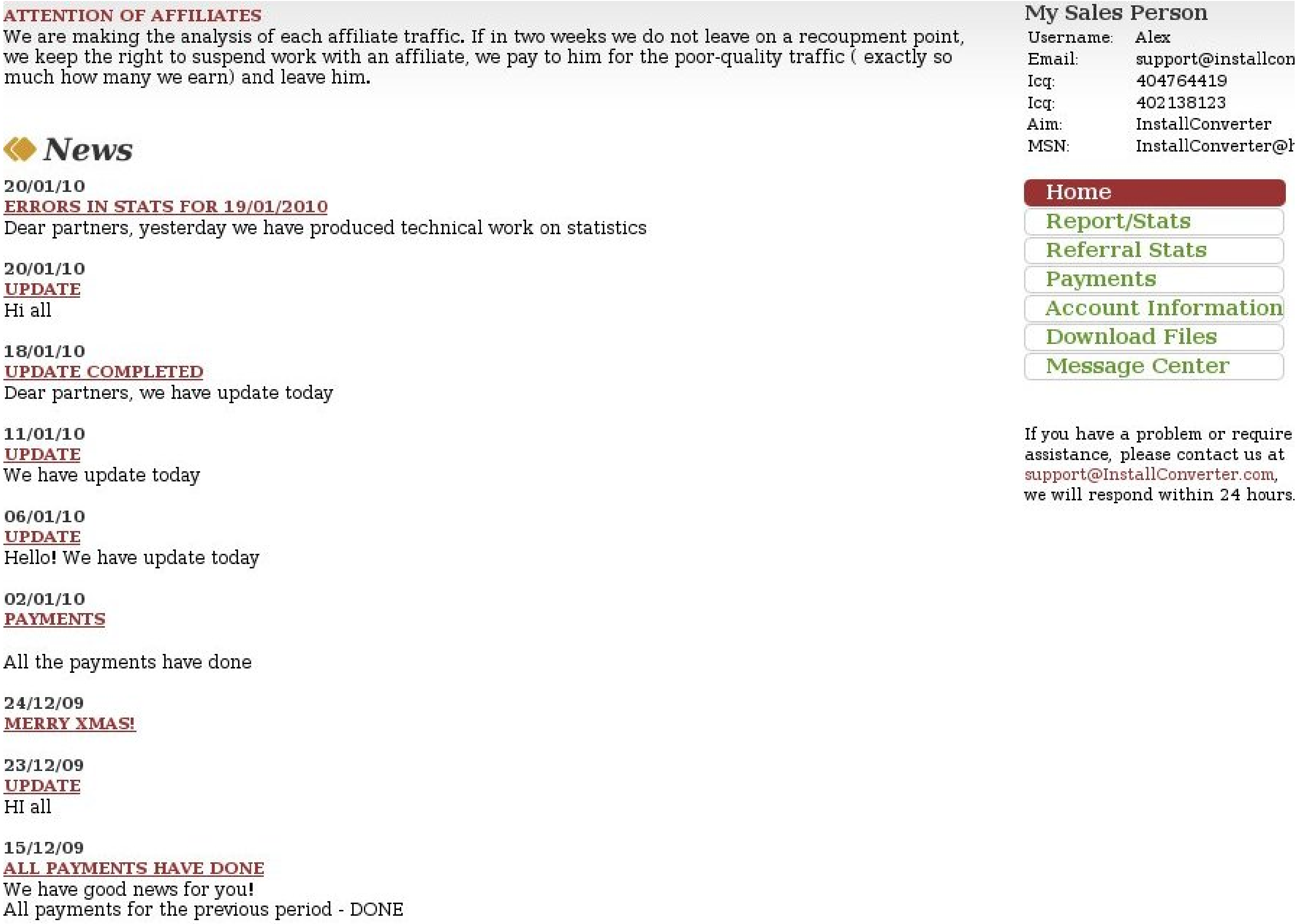
More information and reasons that you should be part of our team!

Permanent bonuses. Do your best and get extra money! The sum of money you'll get depends on your working results and private schedule.

Don't worry, if the data conforms to a valid account. Our Service will send you a new password for your account by email.

Fast and regular bi-monthly payments.

Here’s the home page for the InstallConverter web site.



ATTENTION OF AFFILIATES

We are making the analysis of each affiliate traffic. If in two weeks we do not leave on a recoupment point, we keep the right to suspend work with an affiliate, we pay to him for the poor-quality traffic (exactly so much how many we earn) and leave him.

News

20/01/10
ERRORS IN STATS FOR 19/01/2010
Dear partners, yesterday we have produced technical work on statistics

20/01/10
UPDATE
Hi all

18/01/10
UPDATE COMPLETED
Dear partners, we have update today

11/01/10
UPDATE
We have update today

06/01/10
UPDATE
Hello! We have update today

02/01/10
PAYMENTS

All the payments have done

24/12/09
MERRY XMAS!

23/12/09
UPDATE
HI all

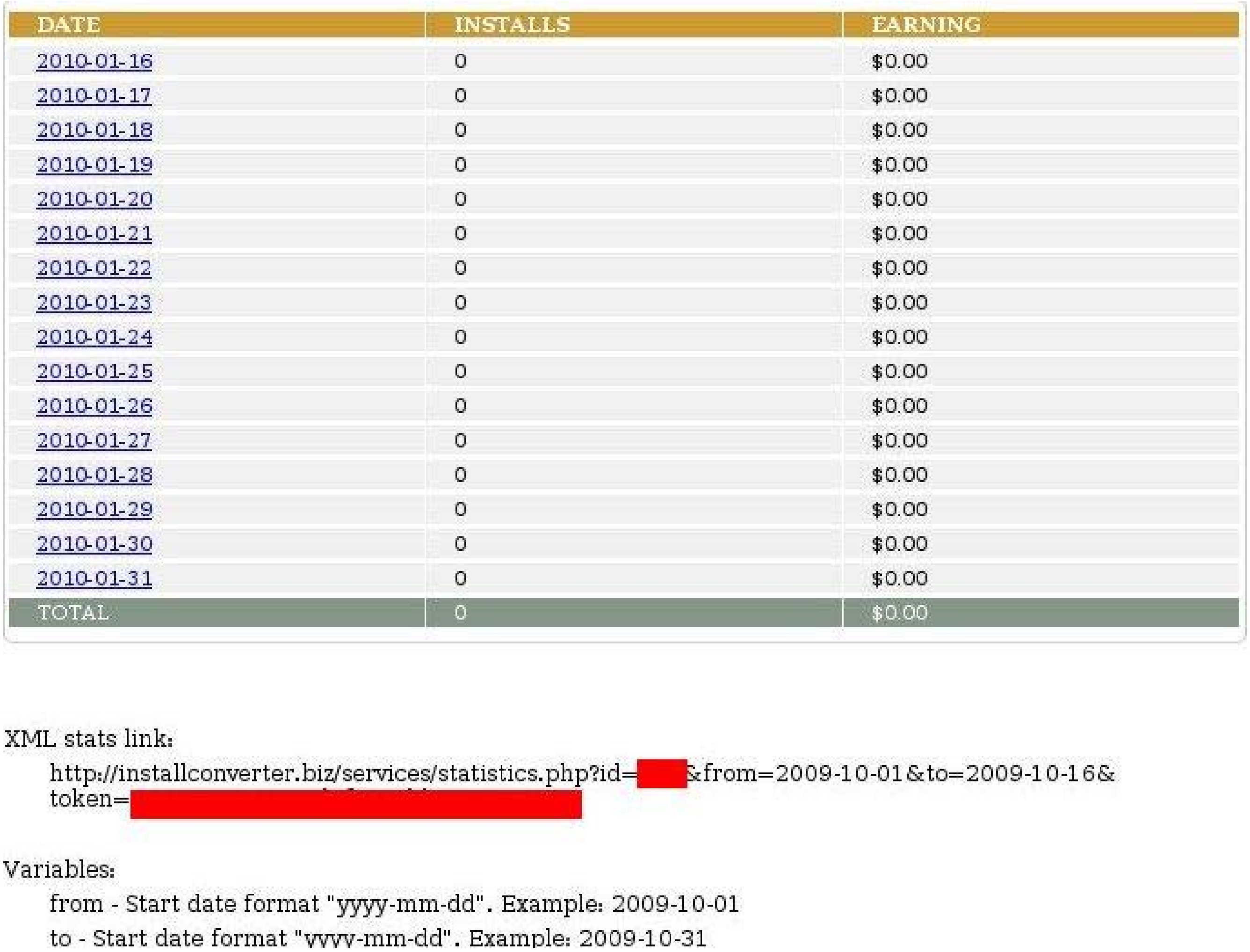
15/12/09
ALL PAYMENTS HAVE DONE
We have good news for you!
All payments for the previous period - DONE

My Sales Person

Username:	Alex
Email:	support@installcon
Icq:	404764419
Icq:	402138123
Aim:	InstallConverter
MSN:	InstallConverter@h

If you have a problem or require assistance, please contact us at support@InstallConverter.com, we will respond within 24 hours.

This page displays the most recent news for the InstallConverter site and how often they update their executable file to make it FUD. They also list a “Sales Person” that should be able to assist affiliates with any problems they might encounter. My personal experience with their sales person was horrible…he never wanted to talk to me.



DATE	INSTALLS	EARNING
2010-01-16	0	$0.00
2010-01-17	0	$0.00
2010-01-18	0	$0.00
2010-01-19	0	$0.00
2010-01-20	0	$0.00
2010-01-21	0	$0.00
2010-01-22	0	$0.00
2010-01-23	0	$0.00
2010-01-24	0	$0.00
2010-01-25	0	$0.00
2010-01-26	0	$0.00
2010-01-27	0	$0.00
2010-01-28	0	$0.00
2010-01-29	0	$0.00
2010-01-30	0	$0.00
2010-01-31	0	$0.00
TOTAL	0	$0.00

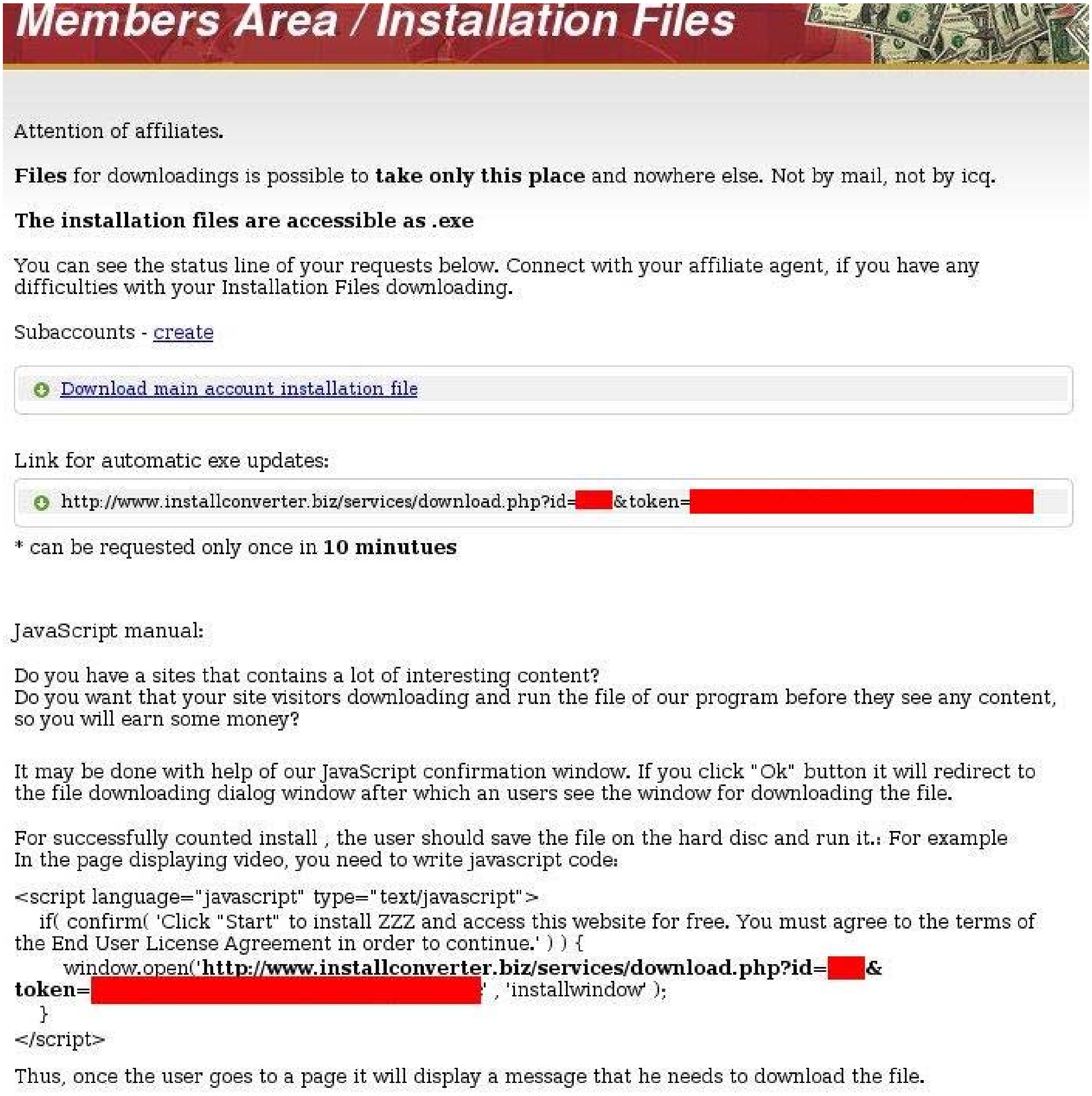
XML stats link:

http://installconverter.biz/services/statistics.php?id=[redacted]&from=2009-10-01&to=2009-10-16&
token=[redacted]

Variables:

from - Start date format "yyyy-mm-dd". Example: 2009-10-01
to - Start date format "yyyy-mm-dd". Example: 2009-10-31

This page displays how many installs an affiliate has for the 15 day pay period. This example has none listed. The XML stats link listed allows an affiliate to post the link in an iframe or use some other method to infect victims' computers.



Members Area / Installation Files

Attention of affiliates.

Files for downloadings is possible to **take only this place** and nowhere else. Not by mail, not by icq.

The installation files are accessible as .exe

You can see the status line of your requests below. Connect with your affiliate agent, if you have any difficulties with your Installation Files downloading.

Subaccounts - create

Download main account installation file

Link for automatic exe updates:

http://www.installconverter.biz/services/download.php?id=[redacted]&token=[redacted]

* can be requested only once in **10 minutues**

JavaScript manual:

Do you have a sites that contains a lot of interesting content?
Do you want that your site visitors downloading and run the file of our program before they see any content, so you will earn some money?

It may be done with help of our JavaScript confirmation window. If you click "Ok" button it will redirect to the file downloading dialog window after which an users see the window for downloading the file.

For successfully counted install , the user should save the file on the hard disc and run it.: For example
In the page displaying video, you need to write javascript code:

```
<script language="javascript" type="text/javascript">
   if( confirm( 'Click "Start" to install ZZZ and access this website for free. You must agree to the terms of
the End User License Agreement in order to continue.' ) ) {
       window.open('http://www.installconverter.biz/services/download.php?id=[redacted]&
token=[redacted]' , 'installwindow' );
   }
</script>
```

Thus, once the user goes to a page it will display a message that he needs to download the file.

This web page displays the main download links for an affiliate to download the installation file, along with the link that can be used to infect victims’ computers.

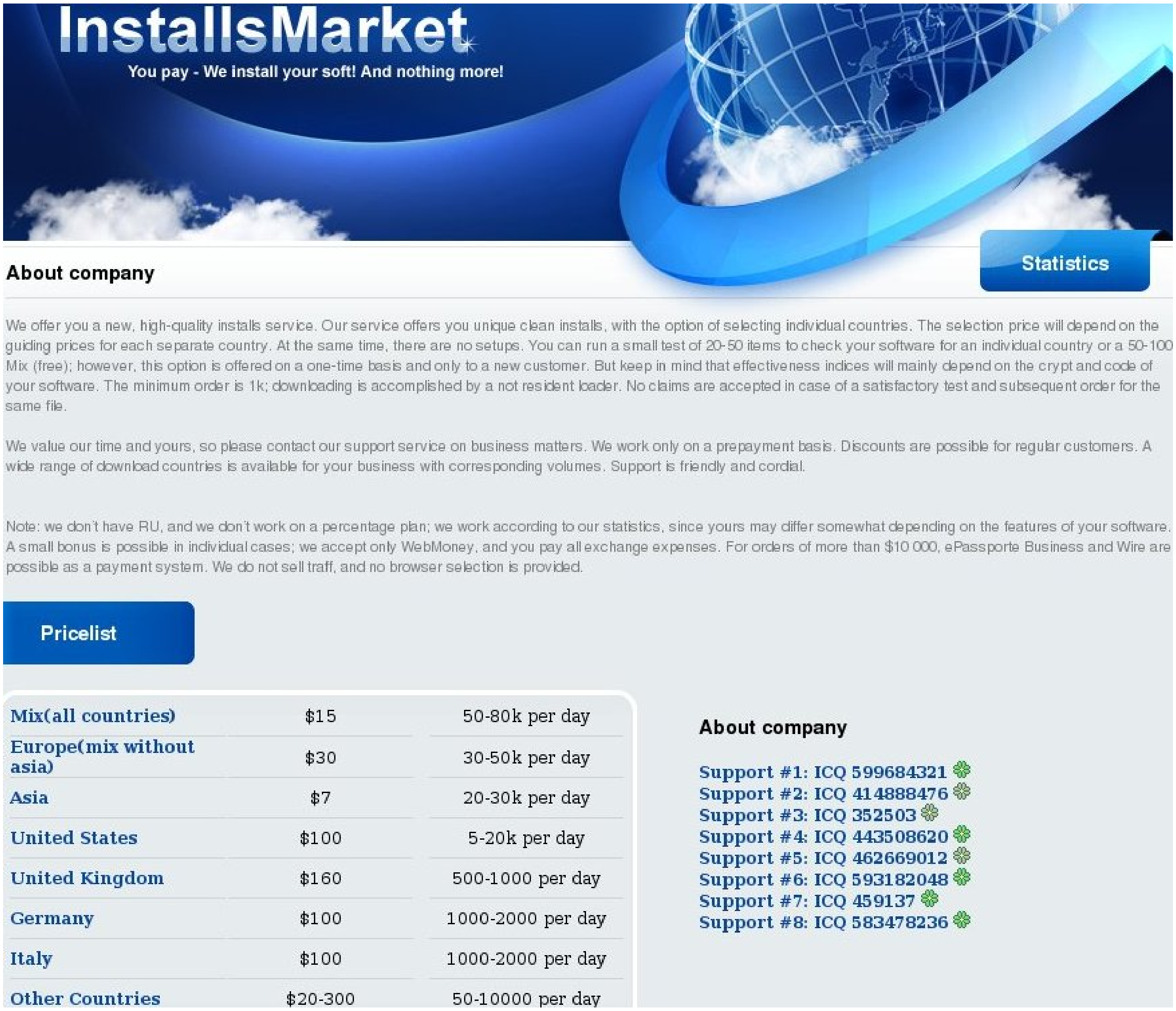
Installs Market

The Installs Market web site is the “opposite” of PPI: the web site offers to do installs for a price. They receive executable files from attackers, and they recommend that senders crypt executable files to remain undetectable for a longer time. Quoted from their web site: “We offer you a new, high-quality installs service. Our service offers you unique clean installs, with the option of selecting individual countries.

The selection price will depend on the guiding prices for each separate country."
For example:

- U.S.-only installs command $100 per 5 to 20 thousand installs per day.
- For Europe, they charge $30 per 30 to 50 thousand installs per day.
- Asia costs only $7 per 20 to 30 thousand installs per day.

Like many other similar web sites, Installs Market will not install files on computers in Russian geographic regions or domains. The domain for Installs Market is registered in China, which seems to be a trend among Russian cyber criminals. They register domains in China and then register the actual IP addresses outside of Russia or in some other Eastern European country.



InstallsMarket

You pay - We install your soft! And nothing more!

About company

We offer you a new, high-quality installs service. Our service offers you unique clean installs, with the option of selecting individual countries. The selection price will depend on the guiding prices for each separate country. At the same time, there are no setups. You can run a small test of 20-50 items to check your software for an individual country or a 50-100 Mix (free); however, this option is offered on a one-time basis and only to a new customer. But keep in mind that effectiveness indices will mainly depend on the crypt and code of your software. The minimum order is 1k; downloading is accomplished by a not resident loader. No claims are accepted in case of a satisfactory test and subsequent order for the same file.

We value our time and yours, so please contact our support service on business matters. We work only on a prepayment basis. Discounts are possible for regular customers. A wide range of download countries is available for your business with corresponding volumes. Support is friendly and cordial.

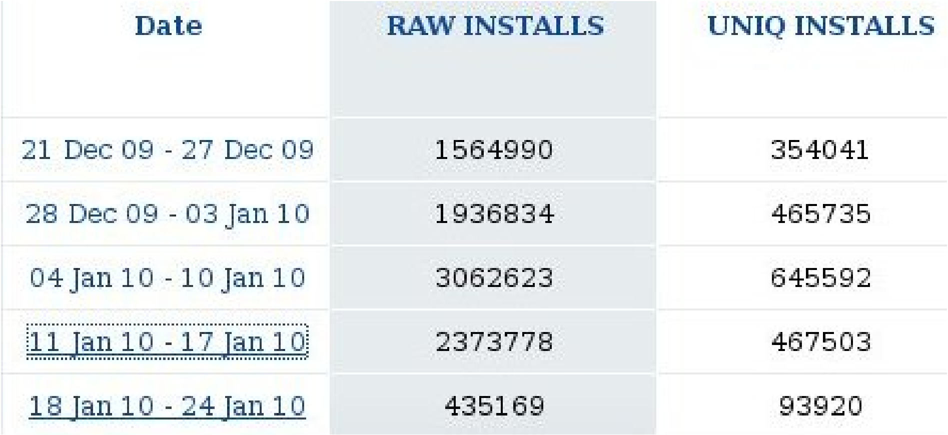
Note: we don't have RU, and we don't work on a percentage plan; we work according to our statistics, since yours may differ somewhat depending on the features of your software. A small bonus is possible in individual cases; we accept only WebMoney, and you pay all exchange expenses. For orders of more than $10 000, ePassporte Business and Wire are possible as a payment system. We do not sell traff, and no browser selection is provided.

Mix(all countries)	$15	50-80k per day
Europe(mix without asia)	$30	30-50k per day
Asia	$7	20-30k per day
United States	$100	5-20k per day
United Kingdom	$160	500-1000 per day
Germany	$100	1000-2000 per day
Italy	$100	1000-2000 per day
Other Countries	$20-300	50-10000 per day

About company

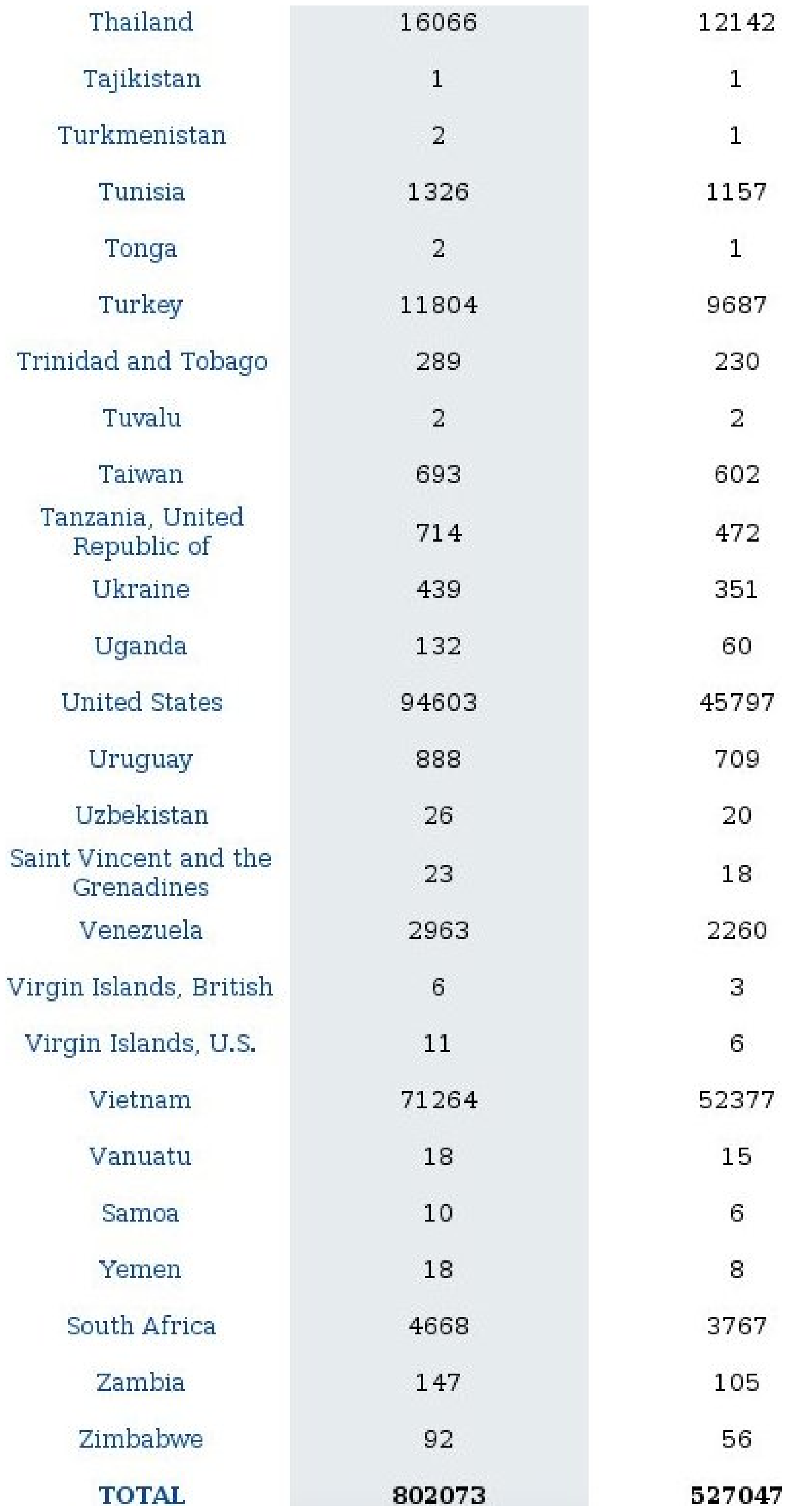
Support #1: ICQ 599684321
Support #2: ICQ 414888476
Support #3: ICQ 352503
Support #4: ICQ 443508620
Support #5: ICQ 462669012
Support #6: ICQ 593182048
Support #7: ICQ 459137
Support #8: ICQ 583478236

Displayed is Installs Market home page with their listed prices.



Date	RAW INSTALLS	UNIQ INSTALLS
21 Dec 09 - 27 Dec 09	1564990	354041
28 Dec 09 - 03 Jan 10	1936834	465735
04 Jan 10 - 10 Jan 10	3062623	645592
11 Jan 10 - 17 Jan 10	2373778	467503
18 Jan 10 - 24 Jan 10	435169	93920

This chart displays how many computers Installs Market can infect within a selected time frame. Each entry is for seven days (excluding for the last entry, because its week was not complete at the time of this publication), averaging 483,217 unique installs for the first four weeks, or 69,031 installs per day.



Thailand	16066	12142
Tajikistan	1	1
Turkmenistan	2	1
Tunisia	1326	1157
Tonga	2	1
Turkey	11804	9687
Trinidad and Tobago	289	230
Tuvalu	2	2
Taiwan	693	602
Tanzania, United Republic of	714	472
Ukraine	439	351
Uganda	132	60
United States	94603	45797
Uruguay	888	709
Uzbekistan	26	20
Saint Vincent and the Grenadines	23	18
Venezuela	2963	2260
Virgin Islands, British	6	3
Virgin Islands, U.S.	11	6
Vietnam	71264	52377
Vanuatu	18	15
Samoa	10	6
Yemen	18	8
South Africa	4668	3767
Zambia	147	105
Zimbabwe	92	56
TOTAL	**802073**	**527047**

Here is a breakdown per country of the seven day period from January 11 to January 17, 2010. Notice that besides Vietnam, the highest amount of installs is for the United States.

Conclusion

To protect your computer and your company from these types of threats, your organization needs to have strong Information Technology (IT) policies and user education in place. IT policies should not allow any kind of peer-to-peer (P2P) usage because file sharing can easily lead to the downloading of malicious files. Users should also be prohibited from installing pirated or unlicensed software, as this software often contains malware.

Use caution when using search engines to find software downloads. Only download software from reputable sites, as SEO techniques are often used to display malicious download sites in search engine rankings.

Depending on your organization’s security and business needs, consider preventing end users from installing any programs on their work computer. Users should be educated on the reasons for these policies, as well as common scams used to con them into running Trojan programs (such as tempting movies, fake codecs, fake AV programs, and spam-based Trojans).

Because many of these PPI programs install the Zeus Trojan and other similar financial and credential-stealing Trojans on victims’ computers, CTU recommends that businesses handling online banking and financial transactions adopt a strategy to isolate the workstations, used for these activities, from possible Zeus or other data-stealing Trojan infections.

Operating system and antivirus software should be updated frequently. The PPI business threat is rapidly growing and attackers use more tools and methods to trick computer users into downloading malware that can result in millions of computers being compromised.