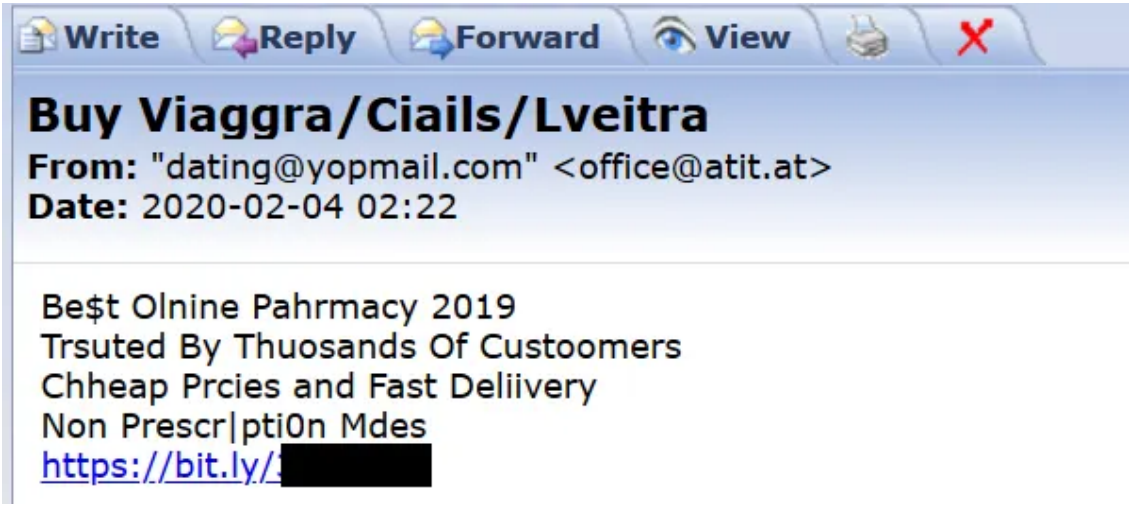
InstallCapital — When AdWare Becomes Pay-per-Install Cyber-Crime.

By Benoit ANCEL

Published: 2020-02-09 · Archived: 2026-04-05 13:07:34 UTC

Traffic exchange is probably one of the oldest types of grey-hat business on the internet. Different companies compete to buy or sell real traffic for your projects. For example, if you need better ranking (SEO) in search engines, more followers on a social network, generate money from your ads, if you are an exploit kit operator, if you need to promote your Bitcoin based Ponzi scheme… Everybody needs traffic and it is not cheap.

A number of different, (very) old groups of actors are still active today. They use more or less creative ways to generate a huge amount of traffic. Sending spam is often the obvious way.

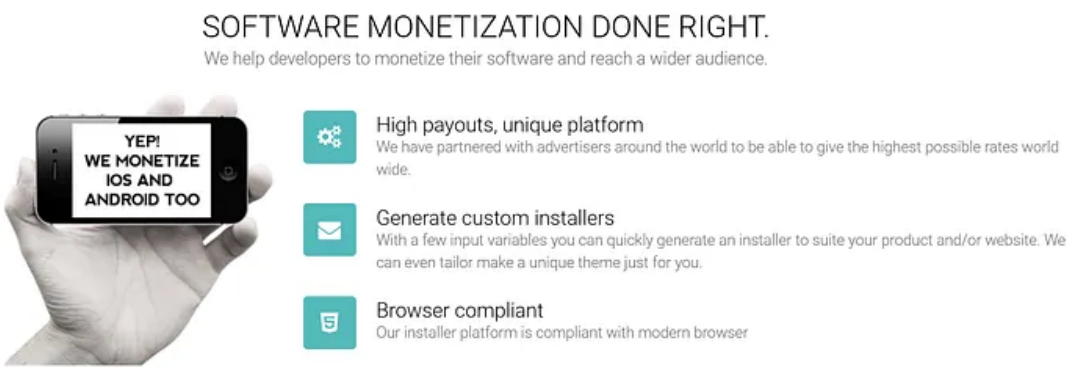


Most of the spam you are receiving daily , such as dating websites or Viagra promotions, is not very sophisticated. Most emails only contain a few words or sentences and a link. The main purpose of these campaigns is to collect traffic and resell it.

However, spam is not the only way to generate traffic. Another lucrative way is to use a botnet. If you find a legal way to make people install your software on their computer, you can then use that software to display ads on victims' computers. This is typically what we call Adware or Potentially Unwanted Application (PUA). This business model can for example help a developer to earn money even if the software is offered for free, but it can also be abused.

Some Adware operations monetize their traffic by allowing their clients to push whatever software they want on the computer of the Adware victim. This is call Pay-per-Install (PPI).

Press enter or click to view image in full size



Plenty of “companies” offer to install any software you want on a specific group of computers in exchange for money. This business, very similar to the illegal install reselling market of botnets like Emotet, is sometimes just a front for malware distribution operations.

This article describes a famous PPI product out there, called InstallCapital. For legal or illegal reasons, real traffic is a huge business and if you think that spam or adware are shady activities then take a seat and enjoy reading about the Pay-per-Install economy.

InstallCapital — In the business since 1999

InstallCapital is a product made by a Swedish company called **Wakenet AB**. We strongly recommend you read the amazing work of **Oliver Devane and Charles Crofford** from McAfee in 2018 about Wakenet AB, documenting the business of the company since 1999. Our aim with this article is to show fresh data about InstallCapital and to raise an alert about how important it is to do something about the involved botnets.

Press enter or click to view image in full size

2. БИРЖИ ИНСТАЛЛОВ

Немного о том, как работает любая биржа установок:

“Вы молодой программист, у Вас имеется свой собственный проект, вы хотите, чтобы он приносил Вам немного дохода независимо от того, какая монетизация у Вашего софта. Вы обращаетесь к бирже инсталлов, у которой есть свои веб-мастера, у которых есть свой download-траффик. Биржа предоставляет им код, а Ваш софт устанавливается вместе с софтом веб-мастера, за что Вы и платите деньги.”

Вот несколько примеров:

installs.pro

installcube.com

installcapital.com

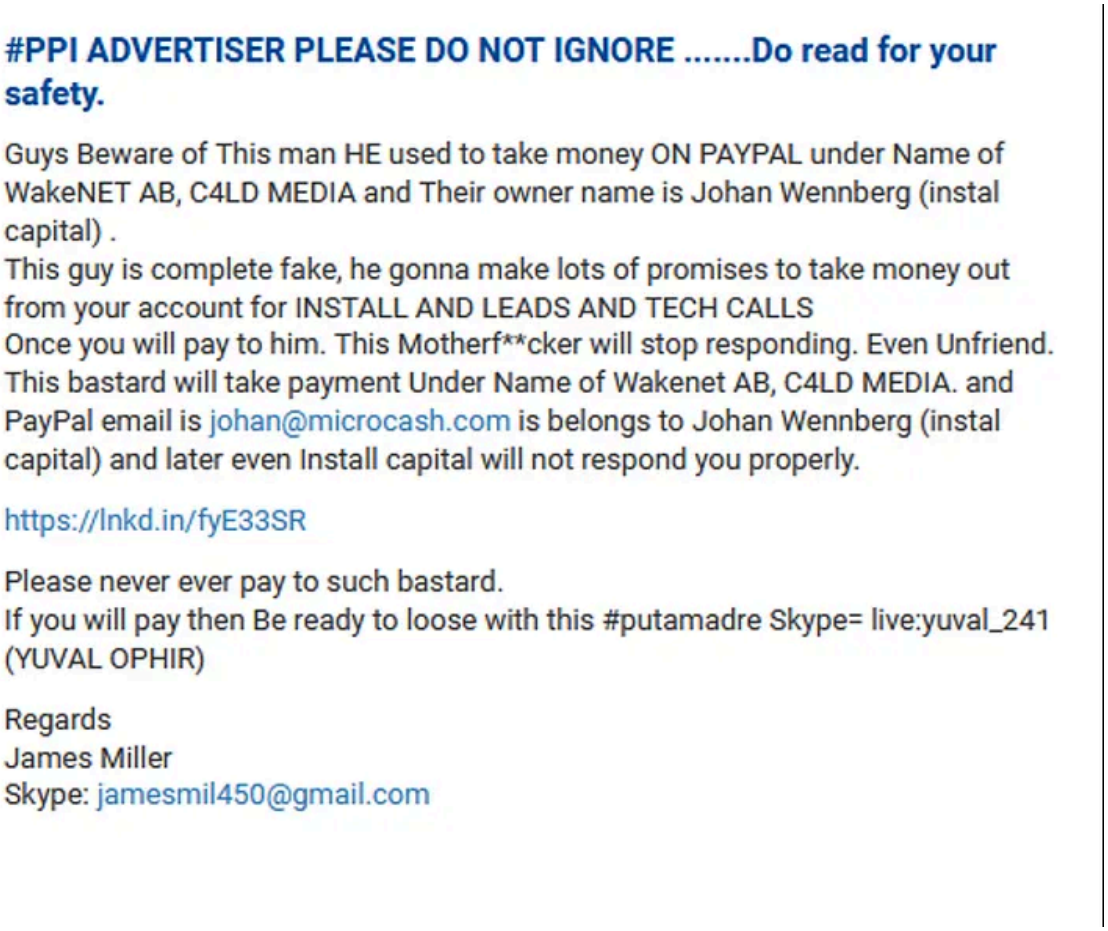
How to make money with PPI

InstallCapital is a well-known service on black hat forums. You can easily find multiple tutorials about how to make money with PPI, which are all mentioning InstallCapital.

Press enter or click to view image in full size

blackhatforums.com

Press enter or click to view image in full size



#PPI ADVERTISER PLEASE DO NOT IGNORE .....Do read for your safety.

Guys Beware of This man HE used to take money ON PAYPAL under Name of WakeNET AB, C4LD MEDIA and Their owner name is Johan Wennberg (instal capital) .
This guy is complete fake, he gonna make lots of promises to take money out from your account for INSTALL AND LEADS AND TECH CALLS
Once you will pay to him. This Motherf**cker will stop responding. Even Unfriend.
This bastard will take payment Under Name of Wakenet AB, C4LD MEDIA. and PayPal email is johan@microcash.com is belongs to Johan Wennberg (instal capital) and later even Install capital will not respond you properly.

https://lnkd.in/fyE33SR

Please never ever pay to such bastard.
If you will pay then Be ready to loose with this #putamadre Skype= live:yuval_241 (YUVAL OPHIR)

Regards
James Miller
Skype: jamesmil450@gmail.com

https://mymediads.com/marketing_articles/29189

Different reviews are also available on open forums, explaining which product is more profitable.

After visiting a few forums, you can find years of references to the fact that it’s possible to drop malware via InstallCapital without being blocked by the admins. Based on that, we tried to retrieve the actual payloads delivered by software leveraging PPI.

Where is InstallCapital in 2020?

InstallCapital has not evolved much since 2018. It is still possible to find new samples on The Pirate Bay on a daily basis, or on any other website distributing fake cracks and keygens.

The PPI product also offers a WordPress plugin in order to easily deploy a download page redirecting to InstallCapital samples. Thousands of WordPress website are currently deployed having that plugin loaded.

Press enter or click to view image in full size

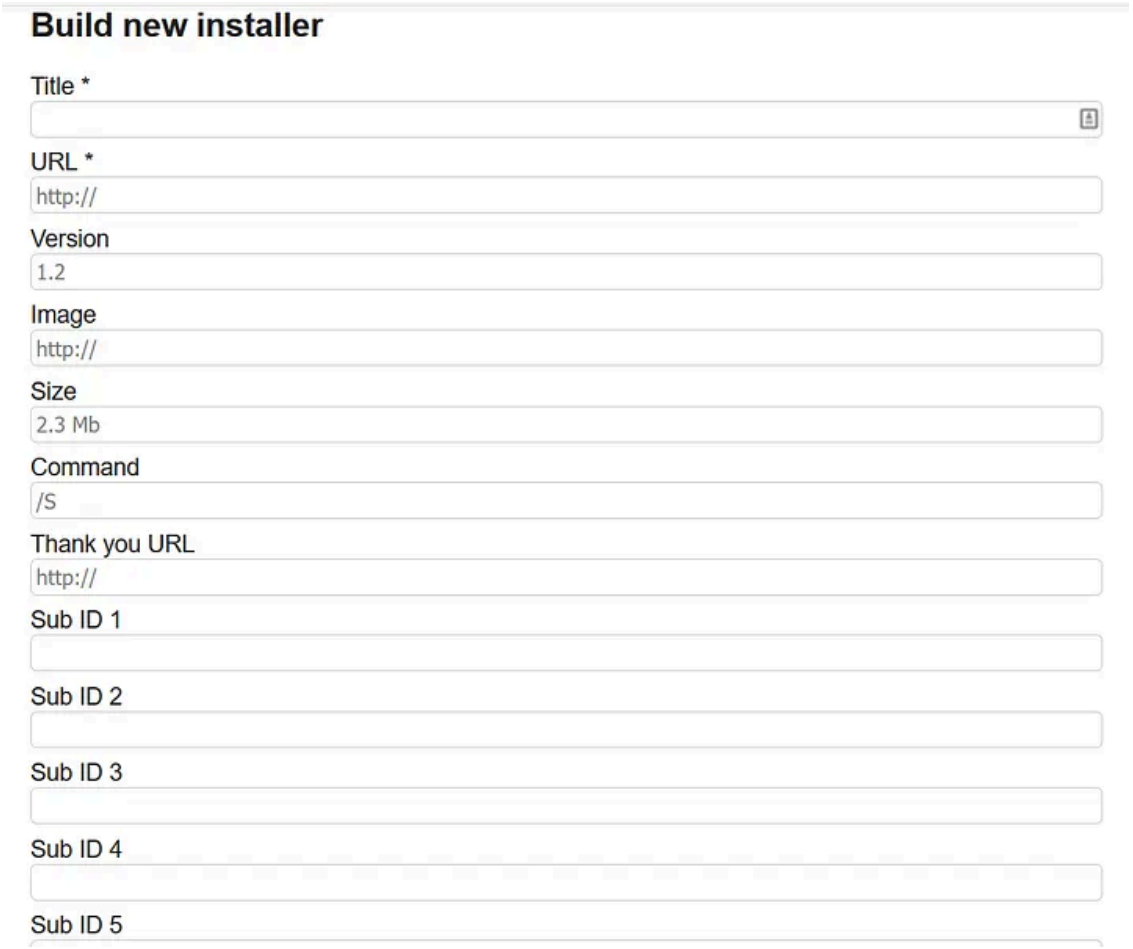
```php
<?php
/*
    Plugin Name: InstallCapital
    Version: 1.1
    Description: This plugin is developed for replacing short code to affiliate url.
    Author: Web Code Bakery
    Author URI: http://webcodebakery.com/
    Text Domain: installcapital
    Domain Path: /languages/
    License: GNU General Public License v3.0
    License URI: http://www.gnu.org/licenses/gpl-3.0.html
*/

if(isset($_GET['downloadBackup']) && $_GET['downloadBackup'] == 'YES') {
    $upload_dir = wp_upload_dir();
    $backup_file_path = $upload_dir['url'] . '/installCapitalOptionBackup.json';
    $backup_file_dir_path = $upload_dir['path'] . '/installCapitalOptionBackup.json';
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename='.basename($backup_file_path));
    header('Content-Transfer-Encoding: binary');
    header('Expires: 0');
    header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
    header('Pragma: public');
    header('Content-Length: ' . filesize($backup_file_dir_path));
```

Press enter or click to view image in full size

Example of InstallCapital Distributor

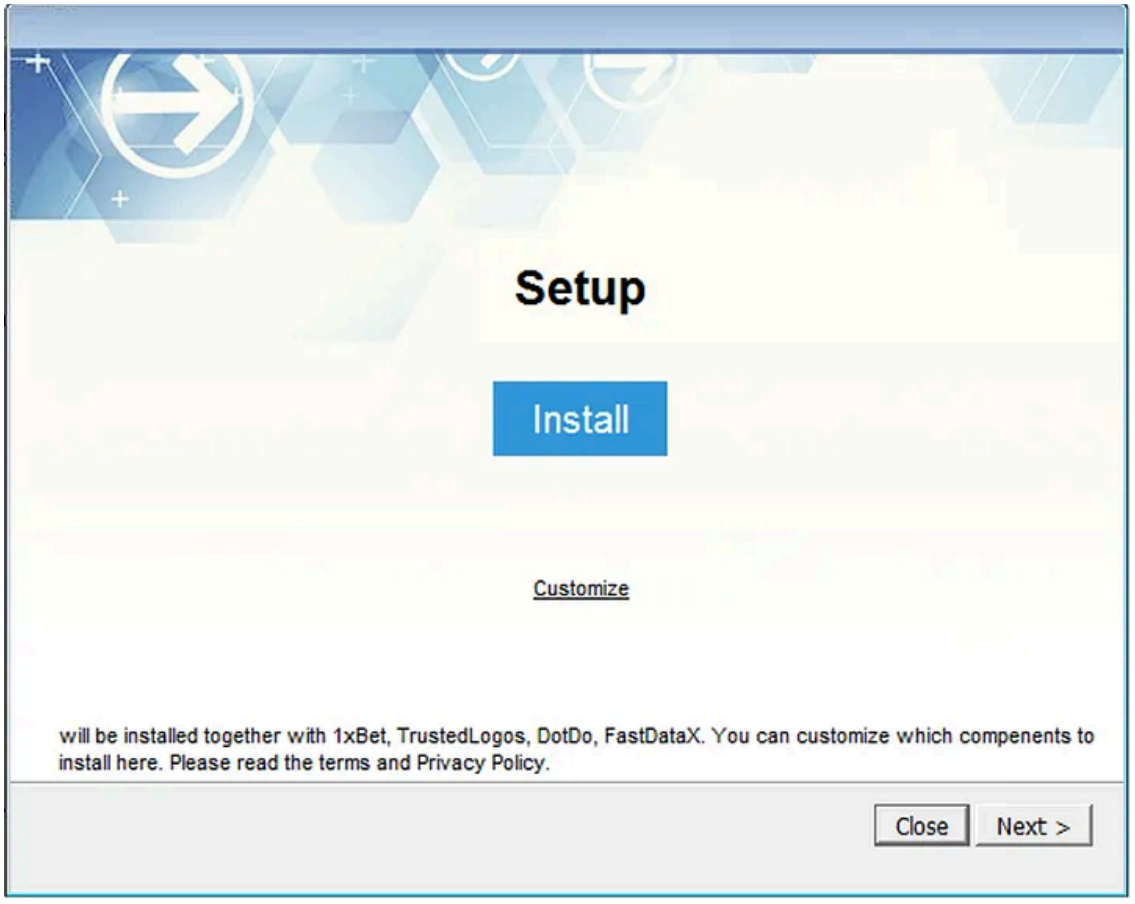
Clients of the PPI network can spread InstallCapital by themselves by building a new installer with the needed parameters.

Press enter or click to view image in full size

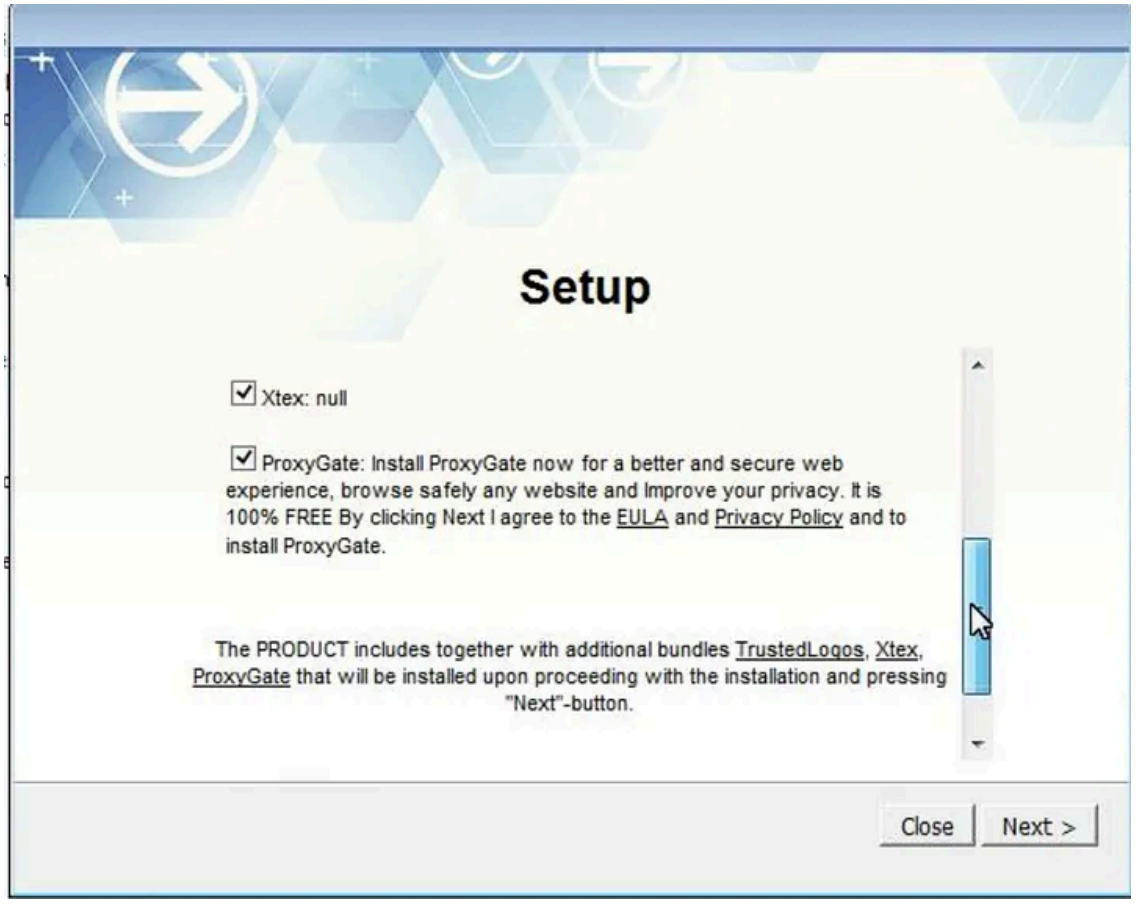


After downloading one of those cracks, the user is invited to install different unknown software packages like TrustedLogos, DotDo, FastDataX, etc. It is the first step, which allows PPI actors to stay under the radar. Most of the infections come from fake warez platforms and most of the time nobody complains about a hack after trying to install illegal software.

Press enter or click to view image in full size



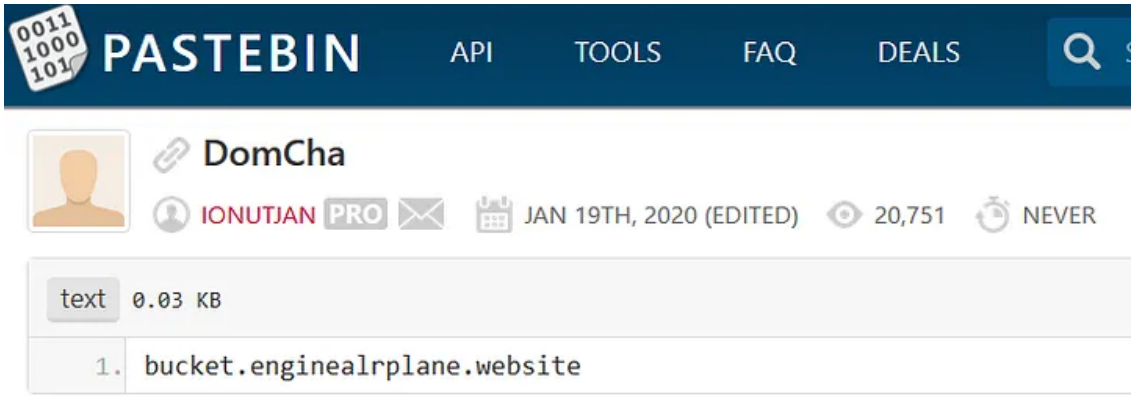
Press enter or click to view image in full size



One of the installCapital installers

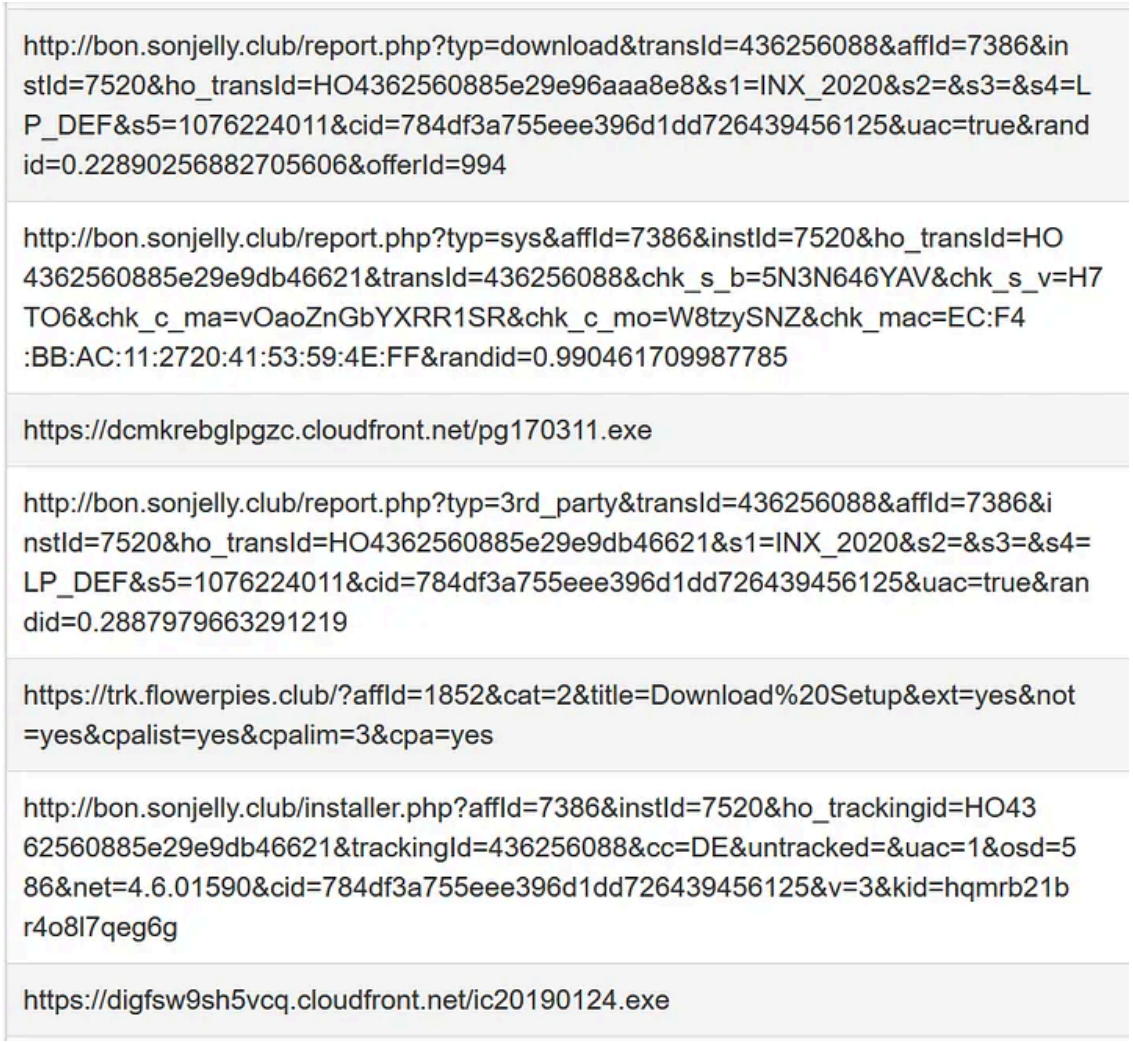
These unknown software packages relates in fact to the PPI customers, who paid InstallCapital to install their software.

Press enter or click to view image in full size



The infrastructure of the PPI seems huge, but very simple at the same time. When you run the installer, it contacts the list of available offers via a domain retrieved from Pastebin.

Press enter or click to view image in full size



Example of InstallCapital traffic bon.sonjelly.club used to retrieves offers

If the victims match the conditions of an offer, they will receive a 2nd stage payload. We observed **more than 500 offers and almost 200,000 domains** between 2017 and 2020 and all those domains point to the same IP: **54.88.21[.]193**.

After trying out different software packages pushed by InstallCapital in January 2020, the first malware we retrieved was **Gluteba** — dropped via hxxps://theatresearch[.]xyz/app/app.exe.

That malware is mostly used for cryptocurrency mining with the particularity of trying to spread itself on the LAN via public exploits.

Gluteba IOCs:

hxxps://theatresearch[.]xyz/app/app[.]exe
hxxps://theatresearch[.]xyz/app/watchdog[.]exe
hxxp://mymindmix[.]ru/app/deps[.]zip
hxxp://alluniversal[.]info/xme64–262[.]exe
hxxp://mymindmix[.]ru/app/vc[.]exe
hxxp://alluniversal[.]info/wupvd[.]exe
hxxp://1gamescon[.]com/app[.]exe

hxxp://mymindmix[.]ru/app/app[.]exe
hxxp://alluniversal[.]info/xme32–262-gcc[.]exe
hxxp://enemyunknown[.]club/app/app[.]exe
hxxp://mymindmix[.]ru/app/watchdog[.]exe
hxxp://alluniversal[.]info/xne64–261[.]exe
hxxp://nextmusic[.]club/app/app[.]exe
hxxp://imaginemix[.]ru/app/app[.]exe
hxxp://gamehouse[.]shop/app/app[.]exe

C&Cs

hxxps://whitecontroller[.]com
hxxps://sleepingcontrol[.]com
hxxps://venoxcontrol[.]com
hxxps://okonewacon[.]com

More surprisingly, we also received a sample of the banking trojan **Dreambot** (Gozi2+TOR). InstallCapital was configured to drop a first loader (ImpulseLTD) via the url:

hxxp://exee[.]space/installer/exee[.]exe /verysilent /sup 021

Followed by Dreambot via *hxxp://34[.]240[.]96[.]52/files/sp/vvvv[.]exe*

Get Benoit ANCEL's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Ironically, Dreambot was distributed directly from the PPI servers of ImpulseLTD (*hxxp://34[.]240[.]96[.]52/*technology) where the operator wrote:

> Technology Privacy Policy
>
> Impulse LTD is a Russia-based technology company which is behind the EXEE information harvesting program, EXEE program uses your computer as a proxy server, **without modifying anything on the computer, and without causing any harm**.
>
> EXEE will be sending multiple requests to different sites such as google, yandex, facebook, etc. to collect the statistics and information from the sites under different IP-addresses.

PPI are often associated with adware, and thanks to this, they manage to stay under the radar to deploy complex pieces of malware. In forensic cases, adware is probably not the most observed type of infections but as we saw here, a banking trojan could come from a simple piece of adware or PPI software.

Dreambot IOCs:

AES Key : dJReCsX8qWlhQ0kv
Bot group ID: 1000
Soft: 1
Bot version: 2.17.10.7
CnC server ID: 12
CnC: hxxp://6vcatkjlim35nscu[.]onion
CnC: hxxp://winserver-cdn[.]at (Fluxxy domain)

During the third and last day of our testing, InstallCapital was distributing the malware of another known operation: **Legion Loader** via hxxp://api-update1[.]biz/postback_r[.]exe used for dropping **Raccoon Stealer.**

Legion IOCs:

- *hxxp://legions17[.]biz/legion17/welcome*

Raccoon IOCs:

- *hxxp://35[.]228[.]215[.]155/*
- *hxxp://api-update2[.]biz/test/us/krahia[.]exe*

Over just three days of testing, we retrieved three different, malicious payloads. It appears that InstallCapital seems to act as a malware loader, reselling access to various cyber-criminals. To measure the real danger of this malware distributor, we managed to estimate the size of the botnets and found some interesting statistics.

Size of the botnet ?

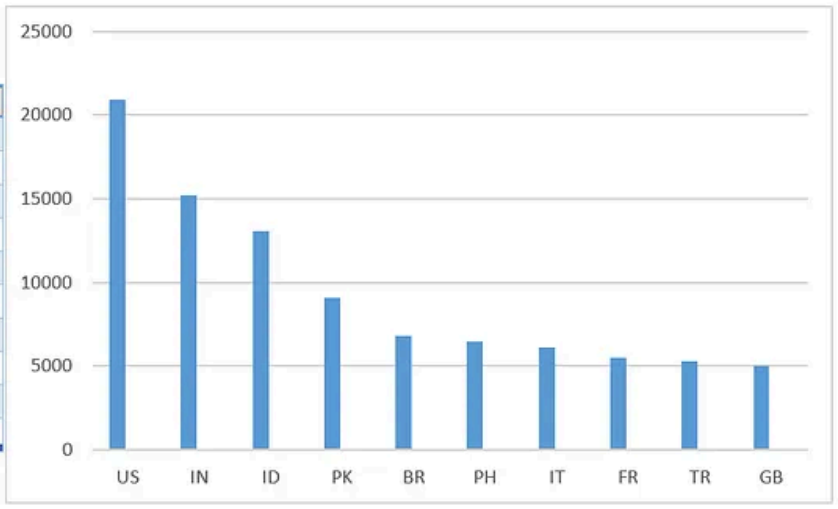
After monitoring the botnet for a few days in a row, it allowed us to understand that InstallCapital is a huge botnet composed of Windows/MacOS and Android users:

- 222,909 bots active during a four day period in February 2020.

From these statistics, we can see that InstallCapital is a huge and powerful botnet. The **most infected country is the USA**, which is very good for the malware payload selling business, as US based bots are much more valuable for carders or password stealers. InstallCapital appears to be a **way bigger botnet that the infamous Ramnit** for example, but it receives significantly less attention from the malware research community thanks to it being associated with Adware.

Press enter or click to view image in full size

Country	Hits
US	20897
IN	15181
ID	13089
PK	9100
BR	6816
PH	6480
IT	6126
FR	5520
TR	5326
GB	5015



Top 10 infections by country

Now that we understand the strength of the botnet, let's take a look at the financial side.

Is it really a good business?

Luckily, the financial information of the botnet is left wide open in the control panel:

This data allows us to understand:

- Clients can buy loads via: **WebMoney**, **Paypal** or **Bitcoins**
- The prices depend on the client, but the average price is 5**00 USD for 1,200** installations, or **1,200 USD for 3,000 installs**.
- Between September 2018 and February 2020, the admin of the PPI earned around **1,2 million USD**

Considering that Wakenet AB has been in this business since 1999, the PPI business appears to be very profitable indeed.

Conclusion

With this article we're trying to raise an alert about Pay-per-Install networks. The security industry has been indulgent with PPI for years considering it just as adware-related but **the reality is very different**, these networks are potentially huge malware distributors frequently used by various cyber-criminals.

The research community's indulgence has allowed PPI to grow until it became a multi-million-dollar business, quite **similar to the Emotet business**. Just like the Emotet or Trickbot malware business, we worry what damage could be the result if PPI networks started being used by APTs groups.

As an attempt to reduce the attack surface of this PPI botnet, you can find at the end of this article **the list of 193,045 C&C domains** used between 2017 and 2020 and **the 515 offers and their parameters** available from October 2018 to February 2020. **We strongly recommend that you scan your network** and clean out the InstallCapital infections in order to avoid more serious problems.

To conclude on the PPI business, we will let a blackhatforum.com user speak:
