



INVESTIGATING COMMERCIAL PAY-PER-INSTALL

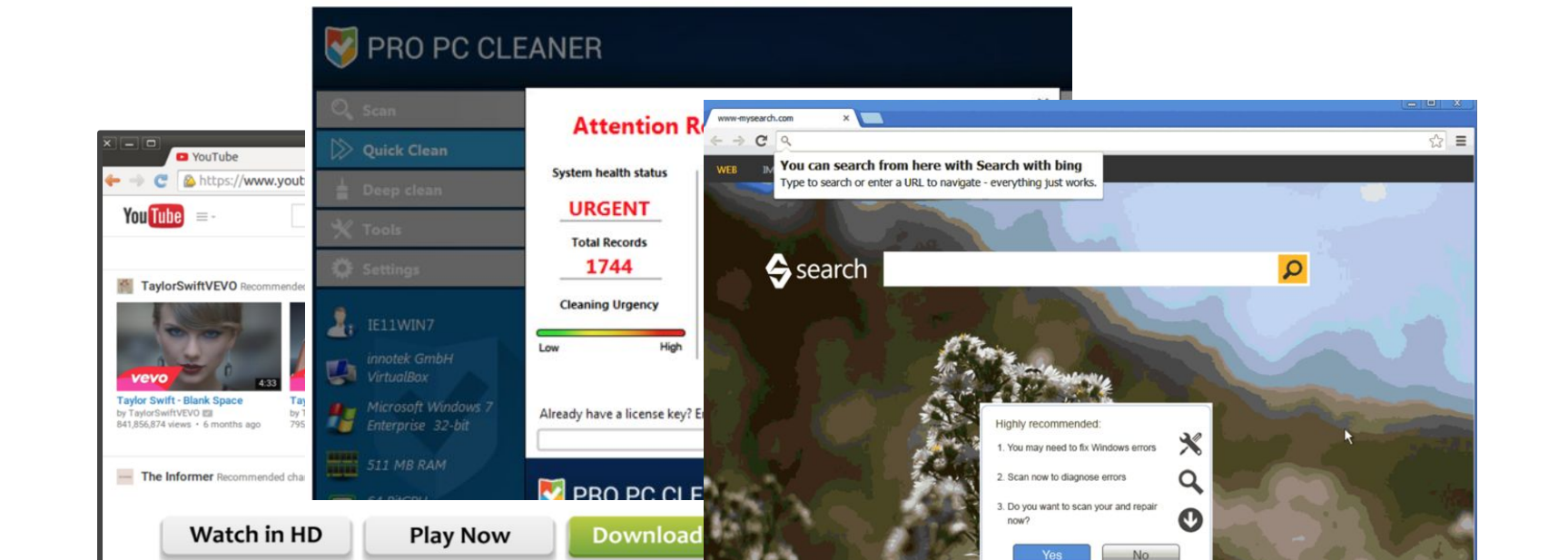
Kurt Thomas, Juan A. Elices Crespo, Ryan Rasti, Jean-Michel Picod, Cait Phillips, Marc-André Decoste, Chris Sharp, Fabio Tirelo, Ali Tofigh, Marc-Antoine Courteau, Lucas Ballard, Robert Shield, Nav Jagpal, Moheeb Abu Rajab, Panos Mavrommatis, Niels Provos, Elie Bursztein, Damon McCoy

Google

NYU

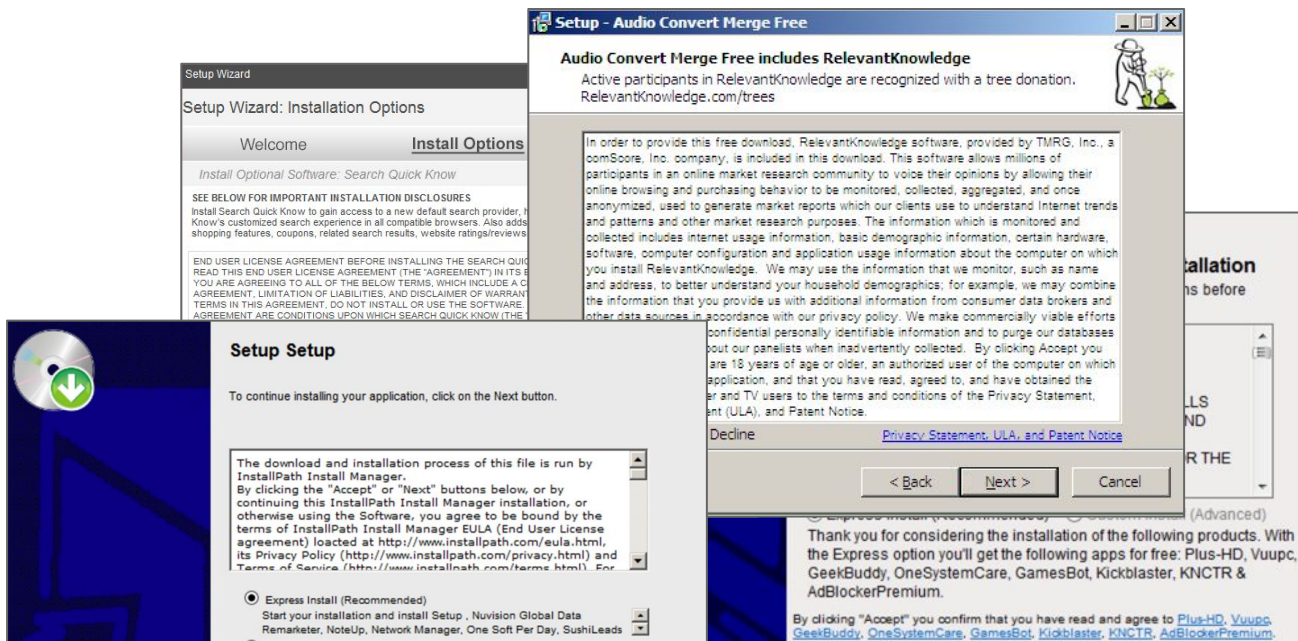
INTERNATIONAL
COMPUTER SCIENCE
INSTITUTE

Unwanted software



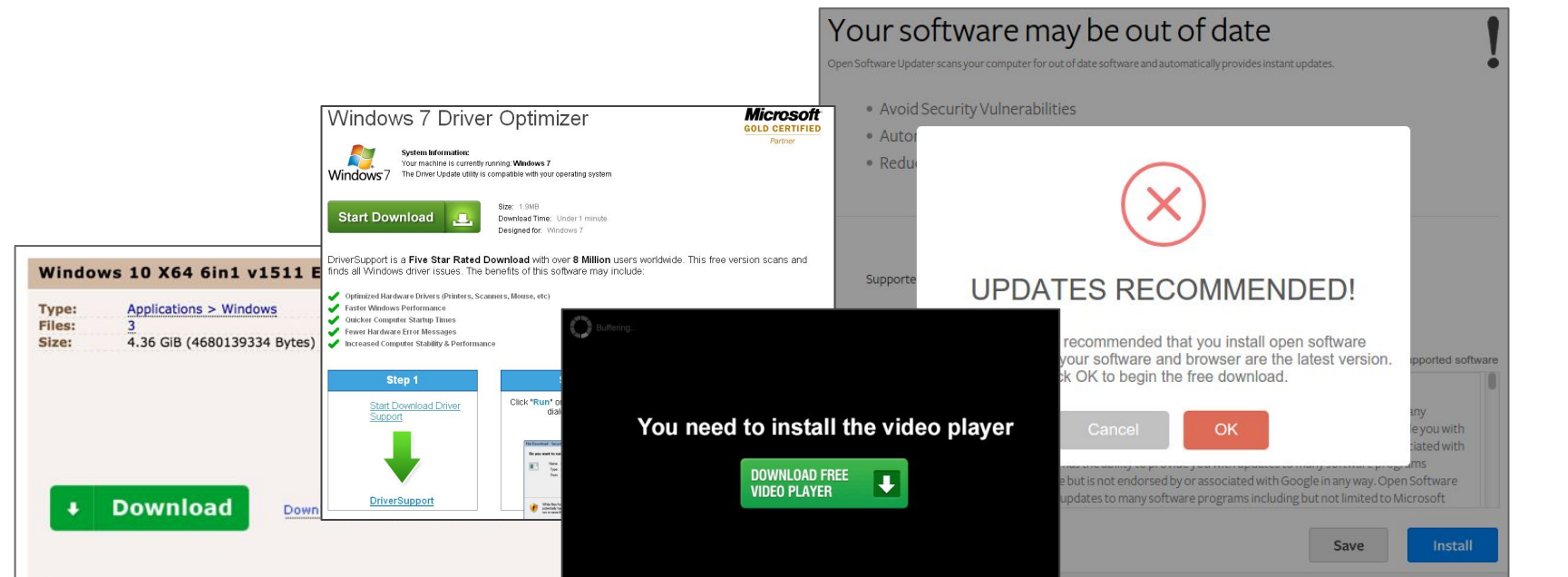
Millions of users with symptoms of unwanted software. How was it installed?

Commercial pay-per-install



Practice of bundling several additional applications.

Deceptive promotions



Users deceived into unintentionally installing unrelated software.

Our work

Year-long investigation into businesses profiting from bundling:

Relationships with unwanted software

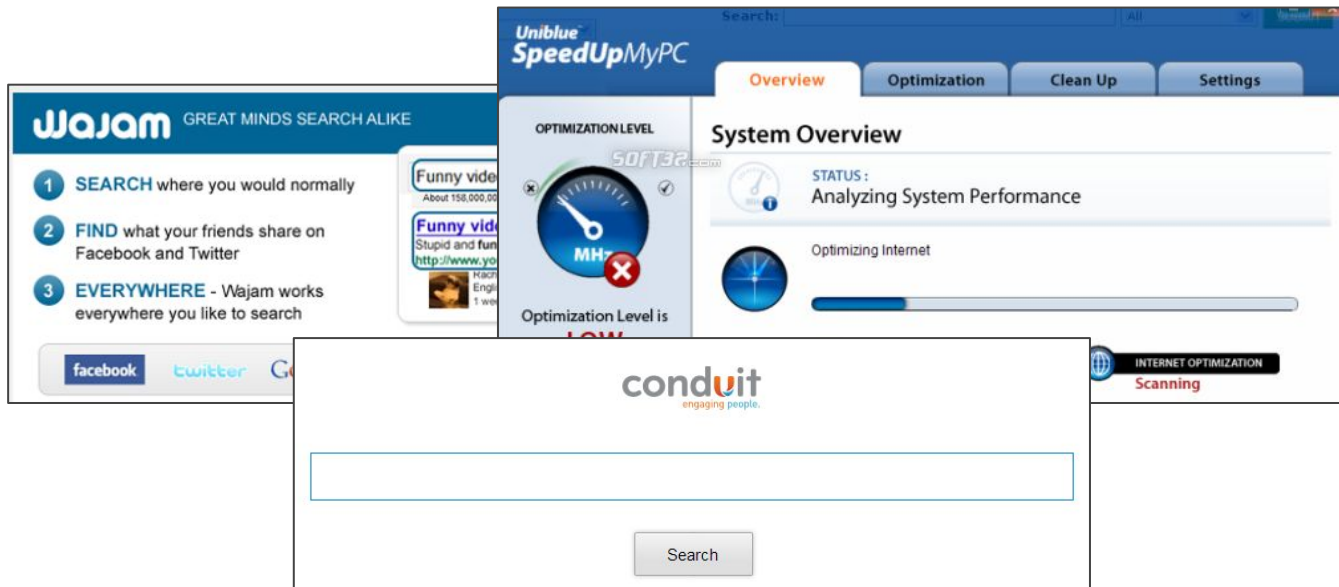
Deceptive promotional tools

Negative impact on users

Get the community on board to tackle unwanted software

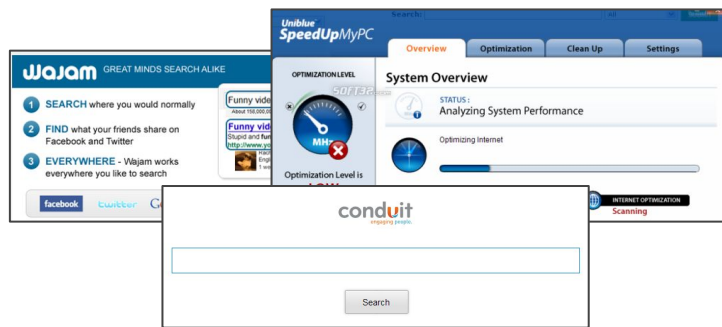
1 BEHIND THE SCENES

Pay-per-install affiliate model

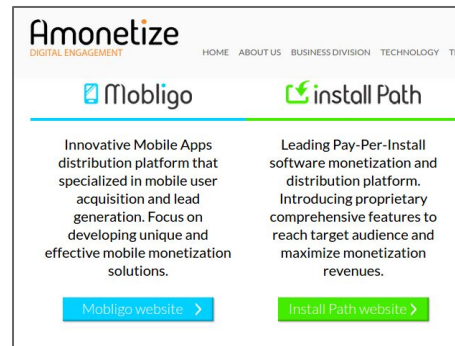


Advertisers: software developers willing to buy installs.

Pay-per-install affiliate model



Advertisers



PPI Network

PPI affiliate network: middle-man that create download manager.

Pay-per-install affiliate model



Advertisers



Amonetize
DIGITAL ENGAGEMENT

HOME ABOUT US BUSINESS DIVISION TECHNOLOGY TEAM

Mobligo

Innovative Mobile Apps distribution platform that specialized in mobile user acquisition and lead generation. Focus on developing unique and effective mobile monetization solutions.

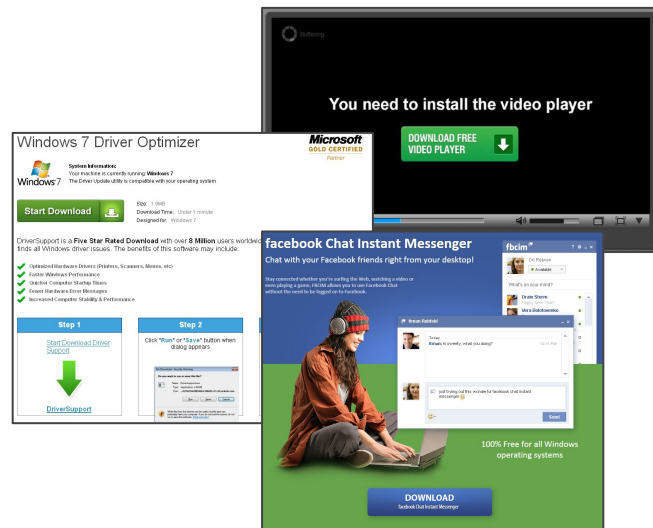
[Mobligo website >](#)

Install Path

Leading Pay-Per-Install software monetization and distribution platform. Introducing proprietary comprehensive features to reach target audience and maximize monetization revenues.

[Install Path website >](#)

PPI Network



Publishers

Publishers: popular software developers or websites that distribute bundles for a fee.

PPI bundle generator

Step 1 - Select a Campaign

Product Name

Campaign

Movies and Video orier

Step 2 - Configure Your Download Manager

File Name Prefix

Name

EXE File URL

Link

Image File URL

Link

Command Line


Parameter

"Thank You" Page URL

URL

Step 3 - Add to Your Site & Start Marketing

Get Your Download Manager



Create a New Co-bundle

Name this Co-bundle:

Name your co-bundle

?

☒

Show a Thank You after my install so I can earn more

Number of offers to show:

☒ Show 5 offerscreens

?

☐ Show 4 offerscreens

?

☐ Show 3 offerscreens

?

☐ Show 2 offerscreens


?

☐ Show 1 offerscreens

Advertisers:

☒ Automatically select the Best Advertisers for me

★ We highly suggest using our Automatic system to select advertisers!!
Our advanced EEPI (Effective Earnings Per Install) algorithm analyzes your traffic, user install patterns, user country Location, pc specs and other metrics to suggest the most effective advertiser.
Using EEPI(Effective Earnings Per Install), you can earn the highest possible earning per install!
Note: We show 5 advertiser screen to a consumer when they install your software.



Click here to see earnings per country

Pay-per-install affiliate model



Advertisers



Amonetize
DIGITAL ENGAGEMENT

HOME ABOUT US BUSINESS DIVISION TECHNOLOGY TEAM

Mobligo

Innovative Mobile Apps distribution platform that specialized in mobile user acquisition and lead generation. Focus on developing unique and effective mobile monetization solutions.

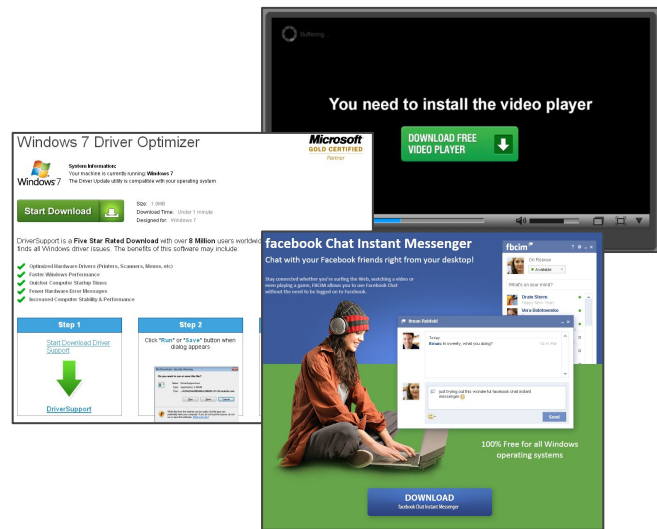
[Mobligo website >](#)

Install Path

Leading Pay-Per-Install software monetization and distribution platform. Introducing proprietary comprehensive features to reach target audience and maximize monetization revenues.

[Install Path website >](#)

PPI Network



Publishers

Decentralized distribution can lend itself to abuse.

2 MONITORING PPI NETWORKS

Over 50 PPI programs in operation

The screenshot shows a forum post from user 'umeriutt00' in a section titled 'MAKE MONEY ONLINE TIPS'. The post is titled 'Top 10 Pay Per Install Networks' and includes a list of networks: CashMyLinks, Amonetize, MediaKings, RevenYou, SkyMonetizer, Optimum Installer, Somoto, Optimum Installer, Installerex, Solimba, Install Monetizer, PayPerInstall, Pay Per Install B, One Installer, Conduit, and OpenCandy. Below the list, there is a definition of a Pay Per Install network: 'A Pay per install network basically pays you to get users to install a piece of software. Software developers will reach out to the PPI network and sign up, and then the affiliate's job is to get people to install the software or opt in for the software installation.' The post also features social sharing buttons for Facebook, Twitter, and Google+.

umeriutt00
Jr. VIP
Premium Member

MAKE MONEY ONLINE TIPS

Top 10 Pay Per Install Networks

Here is a list of Pay Per Install Networks:

- CashMyLinks - [http://www.cashmylinks.com](#)
- Amonetize - [http://www.amonetize.com](#)
- MediaKings - [http://www.media kings.com](#)
- RevenYou - [www.revenyou.com](#)
- SkyMonetizer - [http://www.skymonetizer.com](#)
- Optimum Installer - [http://www.optimuminstaller.com](#)
- Somoto - [www.somoto.com](#)
- Optimum Installer - [http://www.optimuminstaller.com](#)
- Installerex - [www.installerex.com](#)
- Solimba - [www.solimba.com](#)
- Install Monetizer - [http://www.installmonetizer.com](#)
- PayPerInstall - [http://www.payperinstall.com](#)
- Pay Per Install B - [http://www.payperinstallb.com](#)
- One Installer - [http://www.oneinstaller.com](#)
- Conduit - [www.conduit.com](#)
- OpenCandy - [http://www.opencandy.com](#)

What is a Pay Per Install Network?

A Pay per install network basically pays you to get users to install a piece of software. Software developers will reach out to the PPI network and sign up, and then the affiliate's job is to get people to install the software or opt in for the software installation.

Home » Cash Money » Make Money » Affiliate Programs

Amonetize - PPI Network | Best Conversion

Discussion in 'Affiliate Programs' started by Sentinel, Apr 18, 2014.

Thread Status: Not open for further replies.



Outbrowse
Open Candy
Amonetize
Install Monetizer

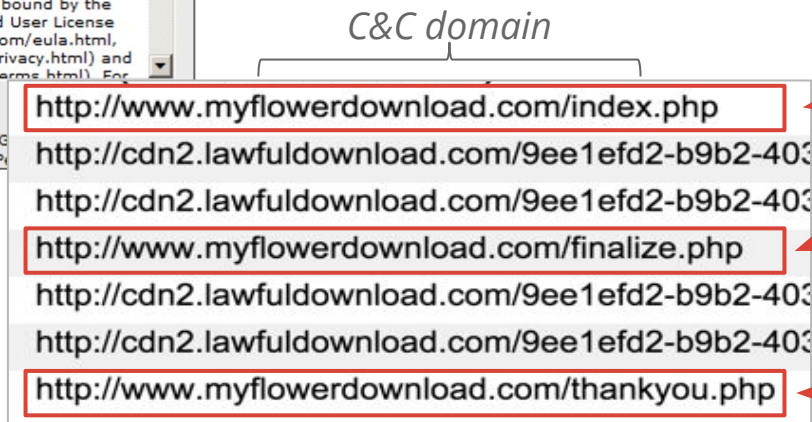
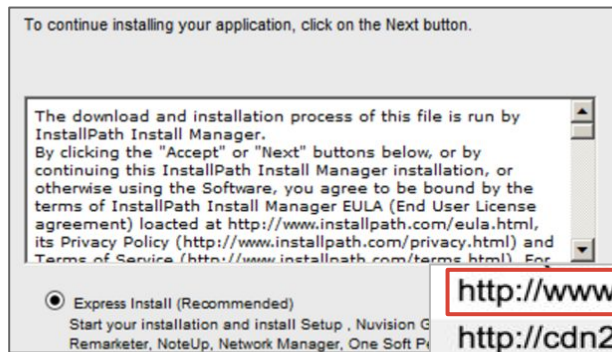
Crawl pricing data

Country Earn up to	
<p>★ Below is the highest payout our advertiser will pay you for an install in the below countries. Note: payout per individual advertiser varies for each country.</p> <p>Select the Automatic option and our EEPI technology will select the most effective advertiser for a country, thus earning you the highest possible income per install.</p>	
United States	\$0.91
United Kingdom	\$0.41
Australia	\$0.27
Germany	\$0.21
France	\$0.21
Canada	\$0.18
Japan	\$0.15

Top 100 countries		
Country	Max Rate	Average Rate
US	\$2.08	\$0.68
AU	\$1.08	\$0.40
GB	\$1.07	\$0.33
CA	\$0.87	\$0.29

Country	Payout Rate
United States	\$0.70
United Kingdom	\$0.40
Canada	\$0.40
Australia	\$0.40

Upon launching a PPI bundle...



*Fingerprint system
& request offers*

*Report successful
installs*

*Optional splash
screen post-install*

Device fingerprinting

Collect system details for targeting and fraud detection:

IP

Browser

OS

Is Admin?

MAC Addr

Machine ID

Example:

```
Net1.1=&Net2=3.5.30729.5420SP1&Net4=4.5.50709&OSversion=NT6.1SP1&Slv=5.1.30514.0&Sysid=CEAEEB  
CAA03CB3EC62DC488C72EBF446&X64=N&admin=Y&browser=ChromeHTML&cavp=&chver=47.0.2526.80&cmd1=OYU  
N0152part1rar__11652_i1815985212_il1207335.exe&dprod=CC83E1275C52718800E7B151A55F92&dprod4=8D  
CC9AFDA6C9A3D6202D6D292AA245&exe=OYUN0152part1rar__11652_i1815985212_il1207335&ffver=&lang_Df  
ltUser=0409&mac=MDAyMzQ1Njc4OTAyMDAwMAA%3D&machg=YzExMTBlZGQtZmQxZS00ZTIwLTg0NzctMmJjMjg2YmQ1  
ODNiAA%3D%3D&name=Sk9ITi1lQWwA%3D&netfs=0&ts=1452339517&ver=1.1.5.26
```


Building milkers

<http://www.myflowerdownload.com/index.php>



```
001. SvNlmsAxc2 * JqaEv`5)Bkmnjf`grQsoa & quot;  
002. 8 + $Fmkcsez_oajgRvjdo & quot;  
003. 8) + & amp;  
004. /2&#39;21&quot;*J`Ibs!6&quot;FF=TXARLQANRZMN&gt;PMnbtu\j`UZJcbnoqj`oUZTcm`o  
005. & #39;No_DteP`kperQ_qi&quot;8(% MldAxcM)nnjqP`huc2) )Oksr@p`KcpokpTcme3 -+P  
006. pkbphsRepnaigZYomenoYgeZYMd] racHmhrb] sx z@F & gt;  
007. W\FN ? AJZE & lt; & lt;  
008. FFHDSMALR : PBV[Oe_m[cIplnd_tztAIBS ^ ? UPM = IM] RMDN Qj ^ op_o_[XSc\j ^ aN  
009. K[M ? & gt;@DGCMBNTU & lt; J@UZP`_ncfKjjmc`n { | CC@R]@OQNELOWPLCORKfrrY  
010. qlta + dfnm_if ^ pik`Wm ^ tbls9f_gk` + @b`jncgWd];  
011. /,l-mmabbll:qr ([\kpf_q[ib8;O,10-4.9$Hdc_qQRJ2argj9+/qmn)]ka[s]scmn`k,`il+/ma  
012. xjakd[J_dblr_rc`f: hdc_qed; - * .noicqcrd\8 + 2. - 6 & quot; dgnld];  
013. /2/27$g]\ n : , 6 / 03![jnlqlxed; - .0qvmaet;.*!] d_71 & quot;  
014. h`8 % , gp[fc = /ln`kqfim96,,*l`vq_qja]8(% O[sa&quot;8()&#39;?a`hpmiYg=_q[!  
015. !Afd` [obtb9) 1 * HmhklnhknP\l`8 * ++Dgn[m ^ n ^ hbuR_o]3 + . & amp;  
016. !Olc`h & lt;  
017. _rblHjsr\dg8 /*/,0*Ndkrr[kKfd`j&gt;hkj[m`Lgi]3lrfk(&quot;A`fMnl&gt;mBdeafZjq  
018. , 0 * ld]] brs9l. + % L`earSMD3 ensl: - * kmo,  
019. agc] t_n] moco(bkm - * ga_com.@yl\ed\Mc`dnSam)`g = l`earg_5 / -3#jqkds ^ ld]  
020. ./ - 0$_anmga714042g ^ _aj & lt;.71 + -l\mrhsnyg_5 - /3#mxobgo5.+$a`a92$cZ8  
021. 1 & amp;, +$brsarld8)]Q] tc2( * * ; c`irdgizJA[s] & quot; 8 & #39;?knhrippk  
022. mjg`jdJdf`8kokh, & gt;  
023. YiKsk;  
024. r ? hc ^ c] hv4snuc & #39;MnlFh@cgp`knbtbCmot_gd`k 70, MmiBlO_fql_mAilr`fkar  
025. ghimk mpTwk]3 / )LkngoauZrfimPyn`k3., !( & quot; P`_F ^ w4!DKCTW & gt; NPO ?  
026. SCDTPI PK&#39;Xfiam; m] WUQa]n&#39;f&#39;d #Mk&#39;h&#39;e( = Y ^ damUQ&#39;f&#39;h&#39;Q xfa = p&#39;v&#39;e&#39;f
```

Build milkers to simulate request from Chrome, IE; Windows 7 system.

Building milkers

<http://www.myflowerdownload.com/index.php>

```
001. SvNlmsAxc2 * JqaEv`5)Bkmnjf`grQsoa & quot;  
002. 8 + $Fmkcsez_oajgRvjd0 & quot;  
003. 8) + & amp;  
004. /2&#39;21&quot;*J`Ibs`1&quot;FF=TXARLQANRZMN&gt;PMnbtu\j`UZJcbnoqj`oUZTcm`o  
005. & #39;No_DteP`kperQ_qi&quot;8(% MldAxcM)nnjqP`huc2) )Oksr@p`KcpokpTcme3 ->P  
006. pkbbsRepnaigZYOmenqoYgeZYMd) racHmhrb) sx z@F & gt;  
007. W\FN ? AJZE & lt; & lt;  
008. FFHDSMALR : PBV[Oe_m[cIplnd_tztAIBS ^ ? UPM = IM] RMDN Qj ^ op_o_[XSc\j ^ aN  
009. K[M ? & gt;@DGCMBNTU & lt; J@UZP`ncfKjjmc`n { | CC@R]@OQNELOWPLCORKfrrY  
010. qlta + dfnm_if ^ pik`Wm ^ tble9f_gk` + @b`jncgWd);  
011. /,1-mmabbbl:qr ([\kpf_q[ib8;0,10-4.9$Hdc_qQRJ2arqj9+/qmn)]ka[s]scmn`k,`il+/ma  
012. xjakd[J_dblr_rc`f: hdc ged  
013. /2/27$g]\) n : , 6 / 03![]  
014. h`8 % , gp[fc = /in`kqfim9  
015. !Afd` [obtb9) 1 * Hmhklnhk  
016. !Olc`h & lt;  
017. _rblHjsr\dg8 /*/,0*Ndkrr[k  
018. , 0 * ld]] brs9l. + % L`e  
019. agc] t_n] moco(bkm - * ga_  
020. ./ - 0$_anmga714042g ^ _a  
021. 1 & amp; , +$brsarld8))Q]  
022. mjg`jdJdf`8kokh, & gt;  
023. YiKsk;  
024. r ? hc ^ c] hv4snuc & #39;  
025. ghimk mpTwk]3 / )LkngoauZr  
026. SOLDTI PK&#39;Bian m; W
```

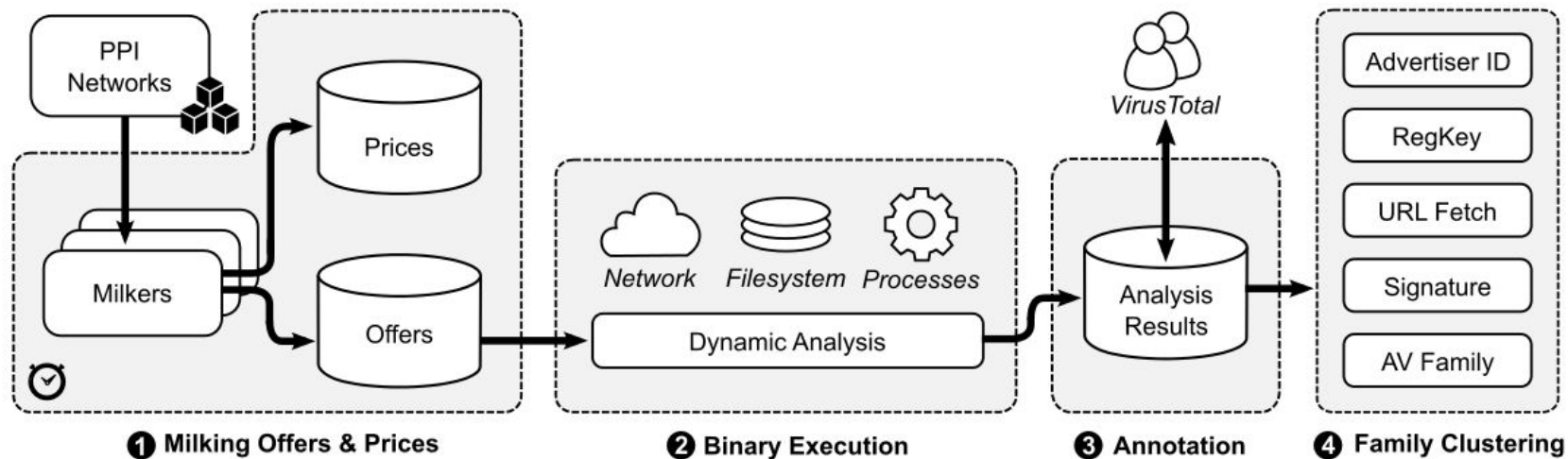
```
1 {  
2 "SleepAfterInstall": 1800000,  
3 "ExeURL": "http://x.superhavenfolks.com/file7/190109817"  
4 "RegKey": "[  
5 {"RegKey32": "...\\C1856559-BA5C-41B7-961C-677E...}]  
6 "PostRegKey": ...,  
7 "ProductID": 10001,  
8 "CommandLine": "-defaultsearch=true",  
9 "RunInAggressiveInstaller": "1",  
10 }
```

Executable URL

Do-not-install
criteria

Build milkers to simulate request from Chrome, IE; Windows 7 system.

Analysis pipeline

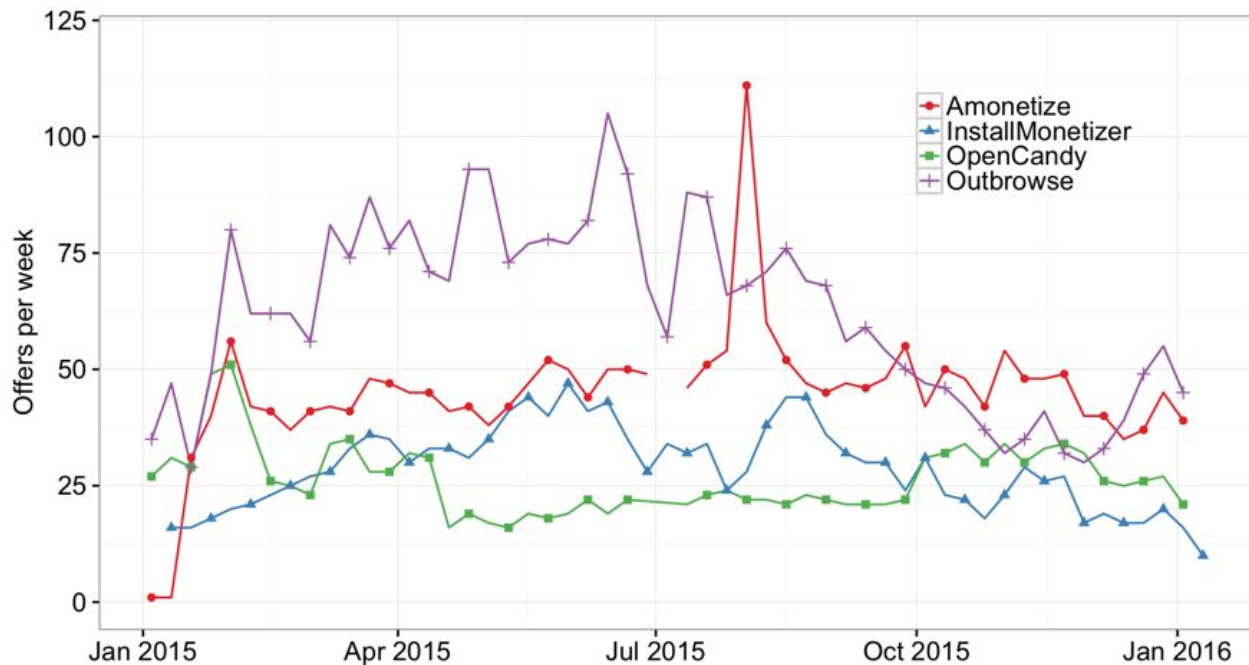


Dataset

PPI Network	Milking Period	Offers	Unique
Outbrowse	Jan 8, 2015 -- Jan, 7, 2016	107,595	584
Amonetize	Jan 8, 2015 -- Jan, 7, 2016	231,327	356
InstallMonetizer	Jan 11, 2015 -- Jan, 7, 2016	30,349	137
OpenCandy	Jan 9, 2015 -- Jan, 7, 2016	77,581	134
Total	Jan 8, 2015 -- Jan, 7, 2016	446,852	1,211

3 ANALYSIS

Distinct advertisers per week



160 software families each week

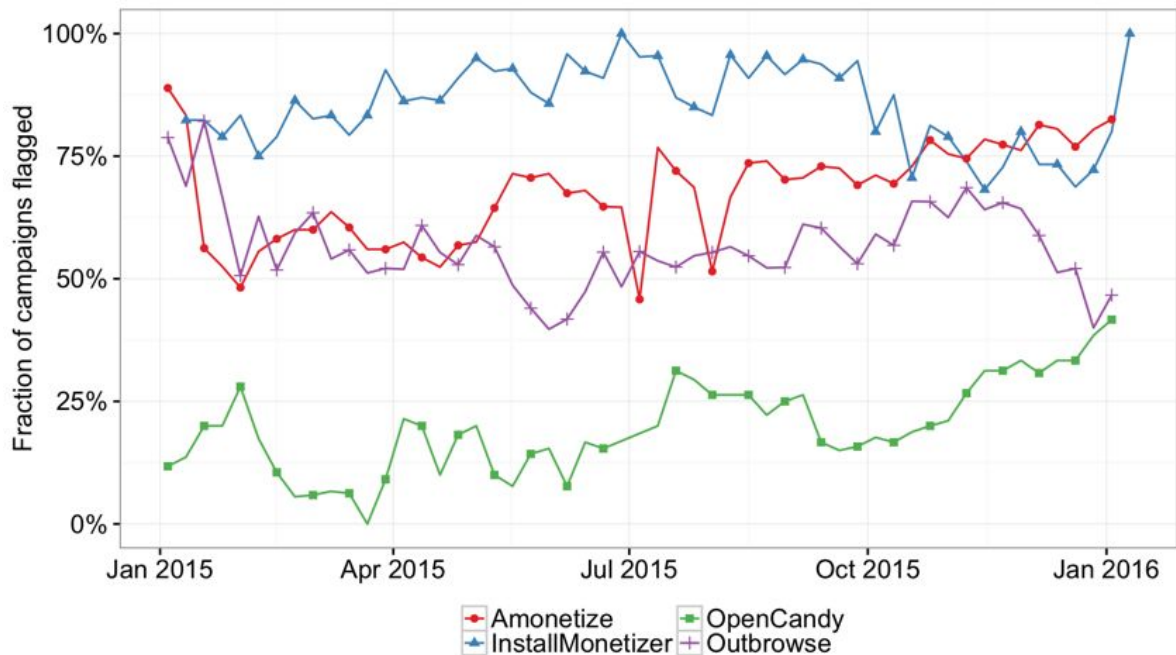
Most frequent advertisers

	Brand	PPI Networks	Days Active
Ad Injectors	<i>Wajam</i>	4	365
	<i>Vopackage</i>	3	365
	<i>Youtube Dwnldr</i>	3	365
	<i>Eorezo</i>	2	365
Browser Settings Hijackers	<i>Browsefox</i>	4	363
	<i>Conduit</i>	3	327
	<i>CouponMarvel</i>	1	300
	<i>Smartbar</i>	3	294
Cleanup Utilities	<i>Speedchecker</i>	2	365
	<i>Uniblue</i>	4	327
	<i>OptimizerPro</i>	4	302
	<i>Systweak</i>	3	249

Other advertisers

	Brand	PPI Networks	Days Active
Anti-virus	<i>AVG Toolbar</i>	2	333
	<i>LavaSoft</i>	1	305
	<i>Comodo</i>	4	153
	<i>Qihoo 360</i>	2	144
Brandname Software	<i>Opera</i>	4	340
	<i>Skype</i>	2	176
	<i>Yahoo Toolbar</i>	1	27
	<i>AOL Toolbar</i>	1	25

VirusTotal labels



59% of weekly offers flagged by at least 1 AV

Anti-virus detection

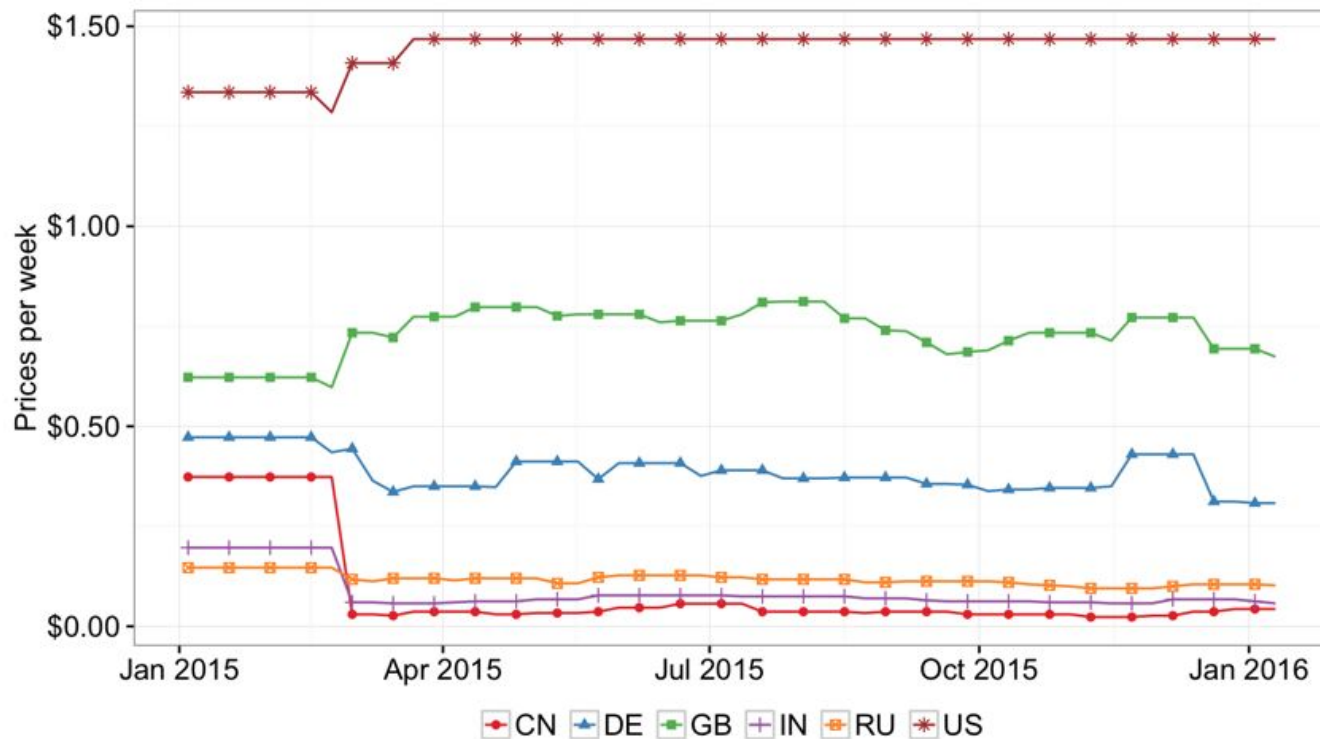
Advertiser-specified installation criteria avoids hostile AV:

```
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hkcu, 'SOFTWARE\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'Software\\\\\\AVAST Software')!=0)
(g_ami.CheckRegKey(g_hkcu, 'Software\\\\\\AVAST Software')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Avira')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Classes\\\\\\avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\ESET')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'AppEvents\\\\\\Schemes\\\\\\Apps\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SYSTEM\\\\\\CurrentControlSet\\\\\\Services\\\\\\avast! Antivirus ')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Microsoft\\\\\\Windows\\\\\\CurrentVersion\\\\\\Uninstall\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\{C1856559-BA5C-41B7-961C-677E89A2C490}')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\{0D40F91C-41DE-4E06-8B14-ABCCF7A51495}')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\{8B261394-6C7D-4CFC-A767-E02F34A60D8B}')!=0)
```

```
HKEY_LOCAL_MACHINE SOFTWARE\\\\\\OpenVPN
HKEY_LOCAL_MACHINE SOFTWARE\\\\\\VMware,*Inc.
HKEY_LOCAL_MACHINE SOFTWARE\\\\\\Oracle\\\\\\VirtualBox|
```

20% of advertisers use some AV/VM detection

Price per install



Price ranges
\$0.10-\$1.50

4 USER IMPACT

Unwanted software warnings



The site ahead contains harmful programs

Attackers on [this website](#) might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

☐ Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

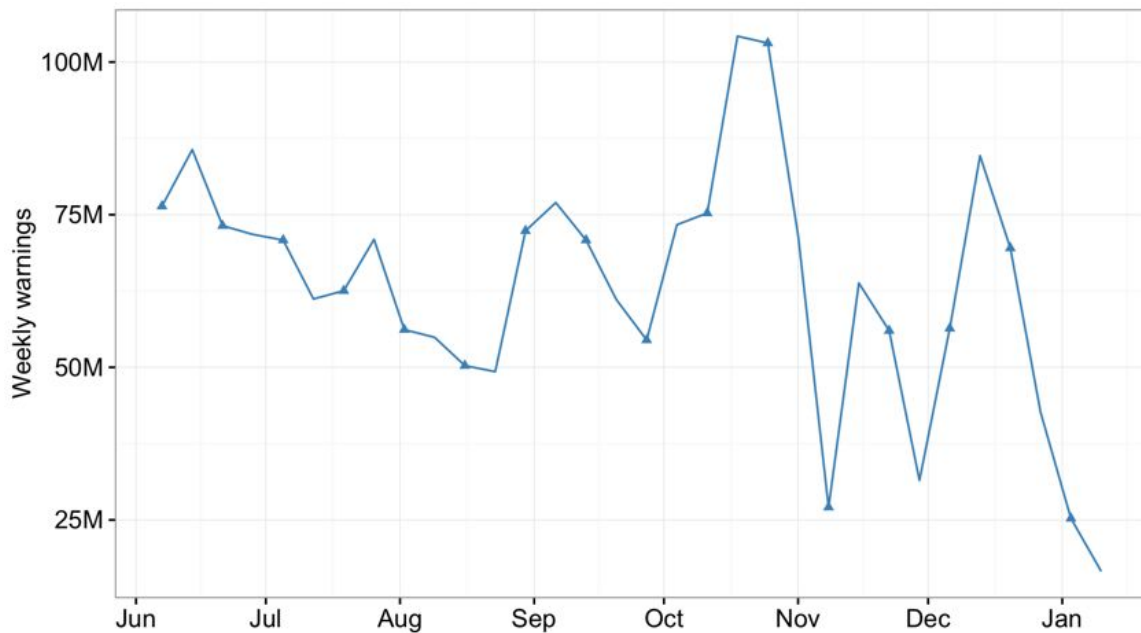


pua.exe may harm your browsing experience, so Chrome has blocked it.

Dismiss

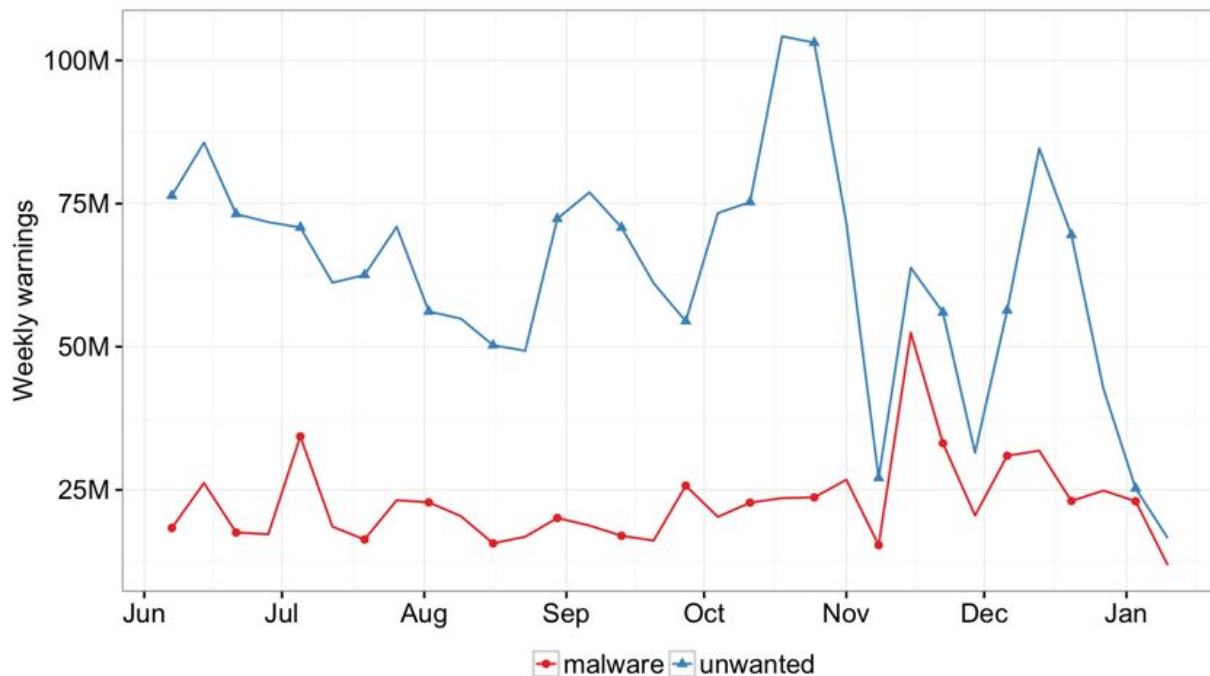


Weekly user warnings



*60M warnings
every week*

Compared to other threats...



3x more warnings
than malware

Existing installs

Chrome Cleanup Tool

This application will scan and remove software that may cause problems with Chrome, such as crashes, unusual startup pages or toolbars, unexpected ads you can't get rid of, or otherwise changing your browsing experience.

For Windows

[Download now](#)



Tens of millions of detected unwanted installs

Existing installs



Of the tens of millions of installs:




Top families	Fraction of installs	PPI advertiser?
Conduit	20.9%	Y
Elex	13.4%	Y
Multiplug	5.1%	Y
Crossrider	4.6%	Y
Browsefox	3.8%	Y
My PC Backup	2.8%	Y
Systweak	2.8%	Y
Mobogenie	2.4%	Y
Smartbar	2.2%	Y
Wajam	1.8%	Y

*Top 10 programs
detected on user
machines*

5 DECEPTIVE DISTRIBUTION

Promotional tools

PERINSTALLCASH
Home / Promo tools
Promo tools
Promo tools
Attention! Never save any exe-files to your server! Outdated
[Show All](#) [Movie traffic](#) [Download traffic](#) [Youtube traf](#)
**DIRECT LINK**
Software
NEW! Basic direct download link for common cases. Place it on your site and see how profit grows.
[» How to setup](#)
**LINK LOCKER**
Software
Lock any URL with get paid when used to access the link
[» How to setup](#)

[NEWS](#) [STATISTICS](#) [MANAGE](#) **[PROMOTOOLS](#)** [PAYMENTS](#) [HELP](#) [LOG OUT](#)
uTorrent Download #2 (add parameters fn=File_to_download.zip size=sizeinMB)
Copy this link and use on your website:
 [preview](#)
[View banners \(4\)](#)

Java Update Download (add parametr auto=1 for auto download exe)
Copy this link and use on your website:
 [preview](#)

Java Update Error (add parametr auto=1 for auto download exe)
Copy this link and use on your website:
 [preview](#)


Domain cycling

07 New domains New

IMPORTANT!!!

Jan

We replaced some blocked promo domains with new ones. Please change it at your side as soon as possible, using of old domains can lead to profit loss.

Old domain => New domain:

letshareus.com => letshare.club

downloadsoundcloud.net => downloadsoundcloud.xyz

fbmessenger.net => fbchat.xyz

mp3gino.com => ginoplayer.xyz (also dynamic banners are now on blocks.ginoplayer.xyz)

loadvids.net => loadvids.xyz

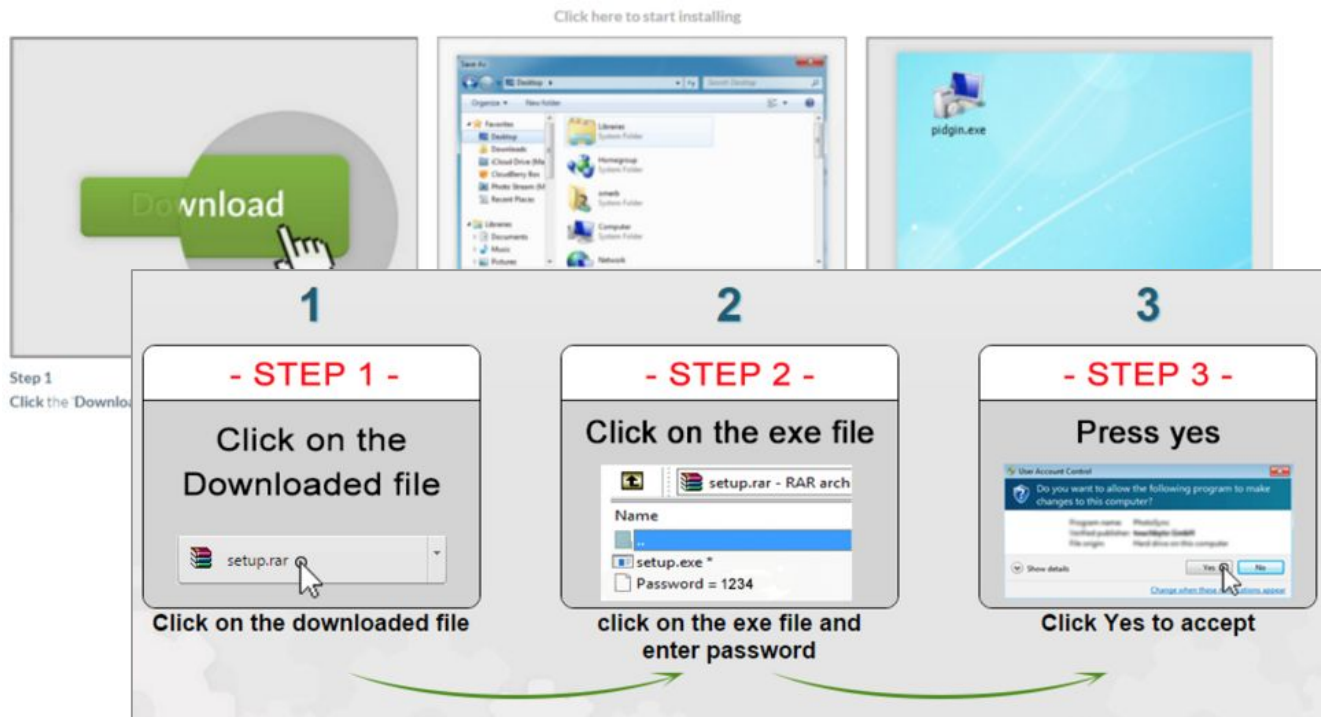
saveclip.net => saveclip.xyz

wallpapermanager.net => wallpaperman.xyz

Also, note that our main direct download domain now is download5-cdn.com, so if you still use download4-cdn.com or download3-cdn.com - replace it as soon as possible.

*Distribution sites
cycle every 1-7
hours*

Safe Browsing evasion



Takeaways

Unwanted software massive commercial ecosystem:

Tens of millions of users affected

Pay-per-install primary distribution vector

Misaligned incentives for advertisers, publishers

THANKS!

kurtthomas@google.com

Top regions impacted

Country	Fraction of warnings
India	8.2%
Brazil	7.2%
Vietnam	6.4%
United States	6.2%
Turkey	5.1%
Thailand	3.3%
Pakistan	3.2%
Mexico	2.6%
Indonesia	2.5%
Philippines	2.5%