KMSpico Windows Activator

KMSPico offers the functionality to activate Windows 8 (all editions). It also claims to support all versions of Windows Desktop and Server and MS Office (fig 1).

The OS	The MS Office	The Server
Win Vista Business/N	Office 2010 All	Server 2008 Standard/Datacenter/Enterprise
Win Vista Enterprise/N	Office 2013 All	Server 2008 (R2) Standard/Datacenter/Enterprise
Win 7 Professional/N	Office 365 All	Server 2012 Standard/Datacenter/Enterprise
Win 7 Enterprise/N	Office 2016 All	Server 2012 (R2) Standard/Datacenter/Enterprise
Windows 8 All		Server All
Windows 8.1 All		
Windows 10 All		

Note: Both 32-bit & 64-bit versions are supported.

Fig 1

When executed, it drops the following files "%Program Files%\KMSPico 10.0.6" folder:

- installkms.bat

- kmsact.exe

- KMSPico10.0.9__<random name>.exe

• **installkms.bat**

It starts with the installation; first, it executes KMSPico10.0.9__<random name>.exe and then kmsact.exe. It later kills running instances of Chrome, Firefox or Internet Explorer web browsers.

```
echo Running KMSPico...
"KMSPico10.0.9__8174_i[redacted].exe"
echo.
echo Installing KMSPico 10.0.6... [47%%]
echo.
@echo off
taskkill /f /IM chrome.exe
taskkill /f /IM firefox.exe
taskkill /f /IM iexplore.exe
cls
echo Running KMSPico...
echo.
echo Installing KMSPico 10.0.6... [47%%]
echo.
echo Applying Registry Patch... [78%%]
echo.
echo Installing Genuine Validation Driver.... [97%%]
echo.
@echo off
echo New KMSPico 11.0.1 Found! ** UPDATE IN PROGRESS... **
echo.
"kmsact.exe"
echo.
```

Fig 2. Installkms batch file content

• **kmsact.exe**

Kmsact is short for KMS activator. It obtains the current user's session details and tries to connect windows7activators.com domain which was inactive during our analysis.

• **KMSPico10.0.9__<random name>.exe**

It is a PUA detected as SoftwareBundler.Mizenota. It connects to the below malicious domains and downloads other malicious components

- www.smaltinecdcf.site/index.php

- cdn1.downloadcrest.com/V38/amipb.js

- cdn2.downloadcrest.com/9ee1efd2-b9b2-403f-8f9a-5fc856fa00a3/main.css

Installation of PUA

KMSPico installer collects the below system information and sends it to a pre-configured site.

- Operating System version
- MAC ID
- Default language
- Default browser
- installed .NET Framework versions
- timedatestamp

In response, it receives a Javascript file that checks for the presence of PUAs from the list of 20 and installs if any of them is not found on the user's machine (fig 3).

```
test: function()
{
  this.bCompExist =
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\yessearchesSoftware\\yessearcheshp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\trotuxSoftware\\trotuxhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\youndooSoftware\\youndoohp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\hohosearchSoftware\\hohosearchhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\istartsurfSoftware\\istartsurfhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\websearchesSoftware\\websearcheshp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\sweet-pageSoftware\\sweet-pagehp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\omiga-plusSoftware\\omiga-plushp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\mystartsearchSoftware\\mystartsearchhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\vi-viewSoftware\\vi-viewhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\key-findSoftware\\key-findhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\omniboxesSoftware\\omniboxeshp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\yoursearchingSoftware\\yoursearchinghp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\oursurfingSoftware\\oursurfinghp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\istartpageingSoftware\\istartpageinghp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\walasearchSoftware\\walasearchhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\yessearchesSoftware\\yessearcheshp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\hohosearchSoftware\\hohosearchhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\walasearchSoftware\\walasearchhp') != 0) ||
    (g_ami.CheckRegKey(g_hklm | g_hk64, 'SOFTWARE\\mysites123Software\\mysites123hp') != 0);


  if (!g_test && g_preinstall && g_comps[0].sn == this.sn)
        return -1;

  return (this.bCompExist) ? 0 : 1;

},
```

Fig 3. Javascript containing PUA list

In its installation window, it shows an uncommon trait of disabled options of "Custom Install" and “Close” button (fig 4).

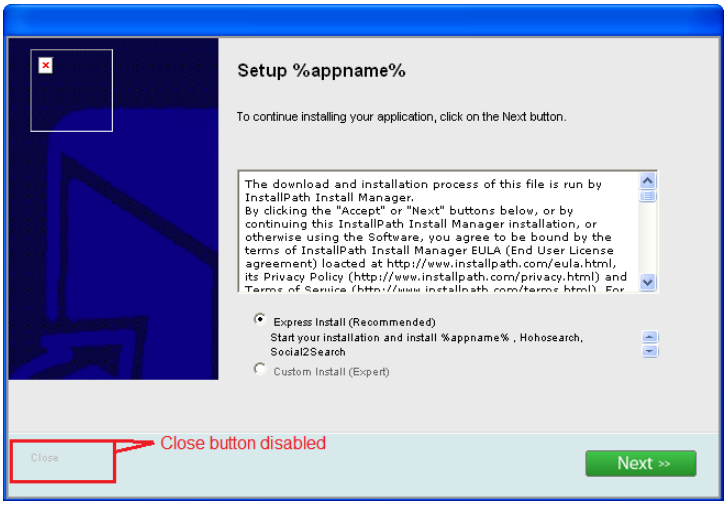
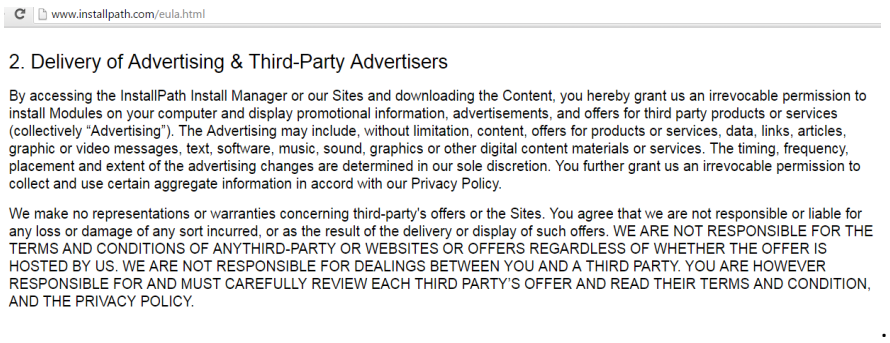


Fig 4. Installation Window

With only one option left to proceed (‘Next’), with the installation, its EULA grants irrevocable permission to InstallPath to show advertisements without accepting any responsibility for loss or damage (fig 5).


www.installpath.com/eula.html

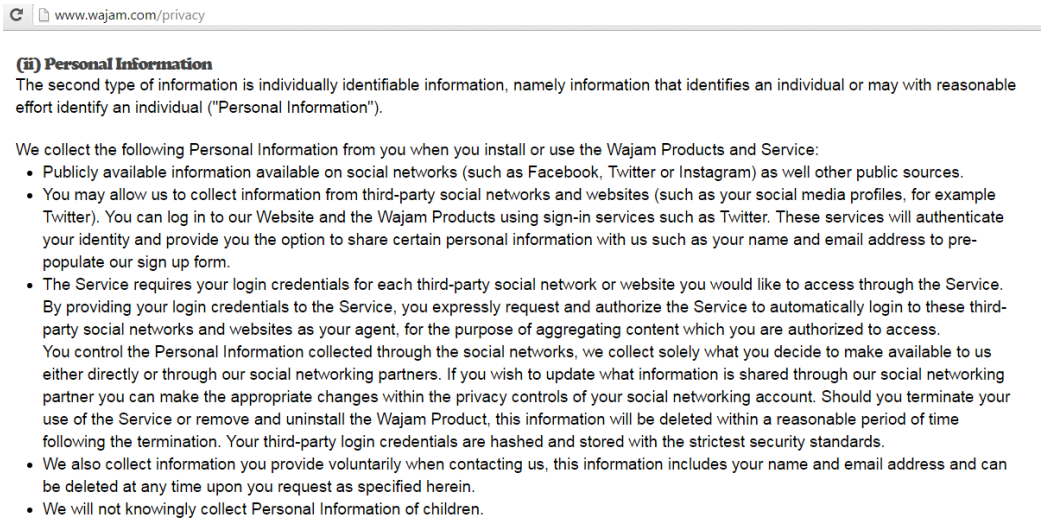
2. Delivery of Advertising & Third-Party Advertisers

By accessing the InstallPath Install Manager or our Sites and downloading the Content, you hereby grant us an irrevocable permission to install Modules on your computer and display promotional information, advertisements, and offers for third party products or services (collectively "Advertising"). The Advertising may include, without limitation, content, offers for products or services, data, links, articles, graphic or video messages, text, software, music, sound, graphics or other digital content materials or services. The timing, frequency, placement and extent of the advertising changes are determined in our sole discretion. You further grant us an irrevocable permission to collect and use certain aggregate information in accord with our Privacy Policy.

We make no representations or warranties concerning third-party's offers or the Sites. You agree that we are not responsible or liable for any loss or damage of any sort incurred, or as the result of the delivery or display of such offers. WE ARE NOT RESPONSIBLE FOR THE TERMS AND CONDITIONS OF ANYTHIRD-PARTY OR WEBSITES OR OFFERS REGARDLESS OF WHETHER THE OFFER IS HOSTED BY US. WE ARE NOT RESPONSIBLE FOR DEALINGS BETWEEN YOU AND A THIRD PARTY. YOU ARE HOWEVER RESPONSIBLE FOR AND MUST CAREFULLY REVIEW EACH THIRD PARTY'S OFFER AND READ THEIR TERMS AND CONDITION, AND THE PRIVACY POLICY.

Fig 5. EULA grants permissions for installPath

It also checks for the presence of Wajam - a social search engine that shows results based on your friends. The privacy policy for Wajam states the storage and usage of login credentials of social networking sites (fig 6).


www.wajam.com/privacy

(ii) Personal Information

The second type of information is individually identifiable information, namely information that identifies an individual or may with reasonable effort identify an individual ("Personal Information").

We collect the following Personal Information from you when you install or use the Wajam Products and Service:

- Publicly available information available on social networks (such as Facebook, Twitter or Instagram) as well other public sources.
- You may allow us to collect information from third-party social networks and websites (such as your social media profiles, for example Twitter). You can log in to our Website and the Wajam Products using sign-in services such as Twitter. These services will authenticate your identity and provide you the option to share certain personal information with us such as your name and email address to pre-populate our sign up form.
- The Service requires your login credentials for each third-party social network or website you would like to access through the Service. By providing your login credentials to the Service, you expressly request and authorize the Service to automatically login to these third-party social networks and websites as your agent, for the purpose of aggregating content which you are authorized to access.
  You control the Personal Information collected through the social networks, we collect solely what you decide to make available to us either directly or through our social networking partners. If you wish to update what information is shared through our social networking partner you can make the appropriate changes within the privacy controls of your social networking account. Should you terminate your use of the Service or remove and uninstall the Wajam Product, this information will be deleted within a reasonable period of time following the termination. Your third-party login credentials are hashed and stored with the strictest security standards.
- We also collect information you provide voluntarily when contacting us, this information includes your name and email address and can be deleted at any time upon you request as specified herein.
- We will not knowingly collect Personal Information of children.

Fig 6

The existence of Wajam can be seen on a large scale. The graph below represents the statistics for the last six months for Wajam (fig 7).

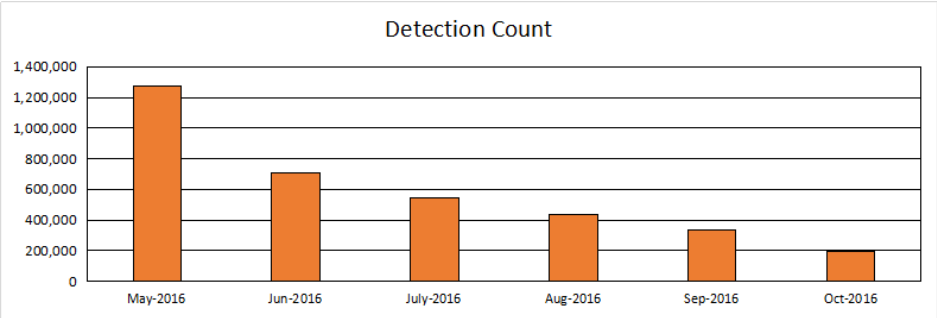


Fig7. Wajam detection statistics from May 2016 to Oct 2016

Kaymundler detection statistics

Kaymundler is active in the market. Fig 8 represents the Kaymundler detection statistics for the last six months (May 2016 to Oct 2016).

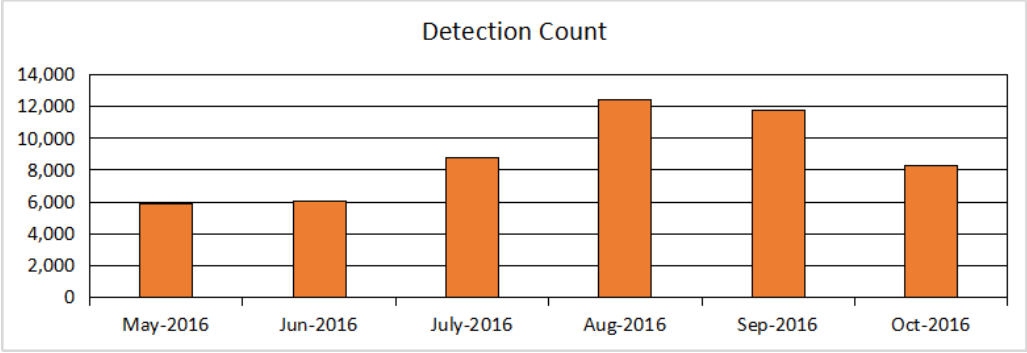


Fig 8. Kaymundler detection statistics (May 2016 to Oct 2016)