Opachki, from (and to) Russia with love - SANS ISC

By SANS Internet Storm Center

Archived: 2026-04-05 19:01:54 UTC

Opachki is a pretty interesting link hijacking trojan that has been spreading quite a bit in last couple of weeks. I started analyzing it couple of days ago and noticed that in the mean time Joe Stewart of SecureWorks posted his analysis as well (available here).

There are some very interesting things about Opachki so let me start at the beginning. The Trojan is distributed with a dropper which, when infecting the system, drops a DLL file. Both the dropper and the DLL file are packed with a packer called "Mystic Compressor". Besides this, the trojan never actually decrypts all strings in memory but calls a function to decrypt only what it needs and immediately deletes the data after it is not needed. Finally, the packer destroys PE header data from memory to make dumping more difficult.

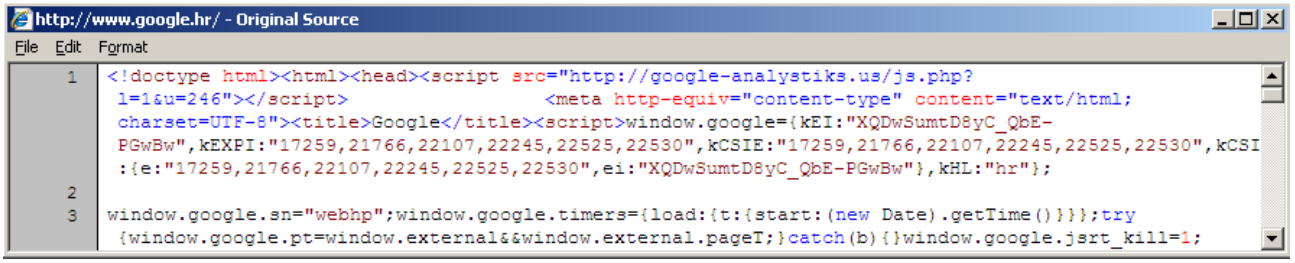
Besides dropping the DLL, the dropper also does one vary nasty action: it completely deletes the SafeBoot registry key by calling reg.exe, as shown below:

```
0012FCCC  00000000  hWnd = NULL
0012FCD0  00000000  Operation = NULL
0012FCD4  00833C18  FileName = "reg.exe"
0012FCD8  00833C58  Parameters = " delete HKLM\System\CurrentControlSet\Control\Safeboot /f"
0012FCDC  00000000  DefDir = NULL
0012FCE0  00000000  IsShown = 0
0012FCE4  00000000
0012FCE8  00833CD0  ASCII "rundll32.exe C:\DOCUME~1\Sasa\LOCALS~1\Temp\rundll32.dll,_IWMPEvents@0"
0012FCEC  00000000
```

This prevents the system from booting in Safe Mode – the attackers did this to make it more difficult to remove the trojan. This goes well with what I've been always saying – do not try to clean an infected machine, always reimage it.

As Opachki's main goal is to hijack links, it hooks the send and recv API calls in the following programs: FIREFOX.EXE, IEXPLORE.EXE, OPERA.EXE and QIP.EXE. While the first three are well known, I had to investigate the last one. It turned out that QIP.EXE is an ICQ client that is very popular in Russia, so the trojan has a component that directly attacks Russian users.

The trojan will monitor web traffic (requests and responses) that above mentioned applications make and will inject a malicious script tag into every response. The injected script tag can be actually seen in the browser (by selecting the view source option) and can be seen in the image below:



This will cause the browser to go to the shown site (google-analystisks.us), which is still live at the time of writing this diary. The site serves back a JavaScript file which modifies all links in the currently shown web page so they are redirected to a third site (http://thefeedwater.com/?do=rphp&sub=241&b= when I posted the diary). The PHP script at the google-analystisk.us web site is interesting as well – if you try to retrieve it directly you'll get an error back so you have to supply a referrer field. It also checks if you came from a search engine (i.e. Google) and returns back a different JavaScript file so it steals search queries as well.

Finally, Opachki performs another interesting action: it tries to see if the system is already infected with ZEUS and will remove ZEUS' files (rename them to C:ntldrs). It will check for all four ZEUS versions by verifying presence of the following files: C:WINDOWSsystem32ntos.exe, C:WINDOWSsystem32oembios.exe, C:WINDOWSsystem32twext.exe and C:WINDOWSsystem32sdra64.exe. I don't know why they do this, it could be that they are hijacking ZEUS or simply competing for same machines or using same attack vectors as the ZEUS crew.

The whole story about Opachki shows how that the bad guys are prepared to invest a lot of effort into building malware. Removing such a trojan is not simple and I would recommend reimaging the machine as the trojan puts a lot of effort into making removing difficult. As the Trojan is specifically attacking Russian users (among the others), it is probably safe to assume that it originates from Russia as well.

Finally, this shows that the bad guys are (probably) making good money by just hijacking links/clicking.

--

Bojan
INFIGO IS
