**Types of Malware:**

**Ramnit:**

Virus:W32/Ramnit.N is distributed in infected EXE, DLL and HTML files; it can also be distributed via removable drives. Once active, the virus infects EXE, DLL and HTML files found on the computer. It will also drop a malicious file that attempts to connect to and download other files from a remote server. Before proceeding to infect other files on the machine, the malware first determines whether a previous instance of its process is already running by checking for its unique mutex . If the mutex is not present, the virus will spawn a new process (a copy of itself) . The dropped process will then spawn other hidden processes (either the default web browser process or svchost.exe). The infection routine is injected into these new processes via a hook on Windows Native System Services. Ramnit.N modifies EXE, DLL and HTML files by appending its own malicious code to the end of the file. When the infected file is run, it drops another malicious file to the same directory where it was executed. The dropped file will be named using the format, "[*original\_filename*]mgr.exe". The dropped file might connect to and download other malicious files from a remote server.

**Kelihos:**

Kelihos malware is often dropped and installed as the payload of other malware, such as trojan-downloaders. Some variants are also distributed via links to malicious websites that are circulated through the Facebook social network. Once the malware has been installed on a system, it typically tries to contact a remote server and download its other components, including a [backdoor](https://www.f-secure.com/v-descs/www.f-secure.com/v-descs/backdoor.shtml) that gives remote attackers further control over the affected system.

The backdoor also connects the system to a botnet under the attacker's control. The botnet (referred to as the Kelihos or Hlux botnet) is built on a peer-to-peer or P2P infrastructure, so commands are relayed through other similarly infected machines from the attacker's command and control server (a structure that makes this kind of botnet much harder to detect and shut down). Once included in the botnet, the affected system may be instructed to download other malware, or be used to send spam email messages to other victims. It may also be directed to perform other malicious actions, such as stealing Bitcoins. When present on the system, the Kelihos malware is able to function as an information stealer.

**Vundo:**

The adware is normally downloaded by users from the websites; these malicious sites are normally promoted by spam emails. The Vundo family is often distributed as DLL files. It is known to be bundled with adware and/or spyware programs.

For representative examples of Vundo variants and associated programs:

* [Trojan:W32/Vundo.HD](https://www.f-secure.com/v-descs/trojan_w32_vundo_hd.shtml)
* [Trojan:W32/Monderd.gen](https://www.f-secure.com/v-descs/trojan_w32_monderd_gen.shtml)
* [Adware:W32/Virtumonde](https://www.f-secure.com/sw-desc/adware_w32_virtumonde.shtml)

Malware in the Vundo family are installed without the user's consent as a Browser Helper Objects (BHOs). During installation, the DLL file is dropped in Windows system directory. The file name is randomly generated using 8 alphabetic characters. Upon execution, the DLL is injected into 2 running processes:

* Explorer.exe
* Winlogon.exe

### Activity

Once installed, the trojan modifies Microsoft Internet Explorer's security setting to trust cookie content created by the trojan. Some variants may also attempt to download and execute arbitrary files from remote websites. The program runs hidden from the user.

**Lollipop:**

The *Lollipop.exe* file is a software component of *Lollipop* by *Lollipop Network, S.L*.  
"Lollipop.exe", identified in Microsoft's Threat Encyclopedia as ["Adware:Win32/Lollipop"](https://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=Adware:Win32/Lollipop) and by Symantec as "Trojan.Gen.2", is [adware](https://en.wikipedia.org/wiki/Adware) by Lollipop Network, S.L., in Barcelona, Spain, a "primary distributor" of unwanted software, advertised as a "performance based contextual advertising network" aimed at Europe and Latin America. It is typically bundled with the PlayerPlus application on video streaming websites and installs without user consent under the profile folder as "C:\Users\\AppData\Local\Lollipop\Lollipop.exe". It has three different ways of setting itself to start at Windows boot depending on the OS and antivirus in use. It transmits data to a remote server identifying the computer's geographical location and security software. The ads it presents vary based on location and browsed keywords and may be pornographic. It can be removed via the Control Panel; removing all entries containing "Lollipop" is advised.

**Simda:**

Backdoor:W32/Simda was first seen in 2009, and has since rapidly expanded into a large family of malware with a wide range of capabilities. Early variants focused primarily on stealing passwords and other data from infected machines. In 2013, Simda was reportedly found being used as a banking trojan (primarily targeting banks in Russia and Europe).

Simda variants are typically distributed via compromised sites that redirect users to websites hosting [exploit kits](https://www.f-secure.com/v-descs/exploit.shtml), which deliver the malware onto systems containing vulnerabilities the kits are able to exploit. When executed on a machine, Backdoor:W32/Simda will install a copy of itself, then delete the original file. During installation, some Simda variants include routines to check for the presence of virtual machines, sandboxes, debugging programs or network traffic analysis tools (essentially, programs that are often used by security researchers); if found, the malware will delete itself. This check allows the malware to evade systems that could potentially spot the infection in progress.

### Information harvesting

If successfully installed, Simda will hook into various APIs in order to capture various types of data, depending on the specific variant involved. Data captured may include network and machine information, online banking and shopping details, email credentials, browser history details, screenshots and so on.

**Tracur:**

When the Trojan is executed, it copies itself as the following file:  
%System%\[NAME OF AN EXISTING DLL]32.exe  
It then drops the following files:

* %System%\[NAME OF AN EXISTING DLL]32.exe ([W32.Mozipowp](http://www.symantec.com/security_response/writeup.jsp?docid=2010-030406-0305-99))
* %System%\[NAME OF AN EXISTING DLL]32.dll
* %UserProfile%\Application Data\SysWin\lsass.exe ([W32.Mozipowp](http://www.symantec.com/security_response/writeup.jsp?docid=2010-030406-0305-99))

If Firefox/chrome is installed on the computer, the threat installs itself as a Firefox/chrome extension by replacing the following files:

* %UserProfile%\Application Data\Mozilla\Firefox\Profiles\install.rdf
* %UserProfile%\Application Data\Mozilla\Firefox\Profiles\chrome\xulcache.jar
* %UserProfile%\Application Data\Mozilla\Firefox\Profiles\chrome\chrome.manifest
* %UserProfile%\Application Data\Google\Chrome\User Data\Default\[RANDOM LETTERS]\contentscript.js

It will also record the information when the user visits websites that URL contain any of the following strings:

* search.aol.com
* search.yahoo.com
* search.netscape.com
* bing.com
* search.lycos.com
* altavista.com
* gigablast.com
* youtube.com/results

The Trojan then opens a back door on the compromised computer by attempting to connect to a server and then waits for commands. The remote attacker can perform the following actions on the compromised computer:

* Download and execute remote files
* Control the web browser redirection parameters
* Steal information  
  It then creates the registry entries to register itself as a system service:

**Gatak:**

It may arrive as one of the following files:

* %UserProfile%\Application Data\Google Talk\googletalk.exe
* %UserProfile%\Application Data\Skype\Phone\Skype.exe

When the Trojan is executed, it may create several configuration files at the following location: %UserProfile%\Application Data\Microsoft\[RANDOM FOLDER NAME]\[RANDOM FILE NAME]   
Next, the Trojan may create one of the following registry entries so that it is executed every time Windows starts:

* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\"googletalk" = "%UserProfile%\Application Data\Google Talk\googletalk.exe /autostart"
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Skype" = "%UserProfile%\Application Data\Skype\Phone\Skype.exe\" /nosplash /minimized""

It then injects itself into the following process:   
explorer.exe . The Trojan then opens a back door on TCP port 80 and connects to the remote locations: