Agent	The Trojan.Agent infections may often install themselves by copying their executable to the Windows or Windows system folders, and then modifying the registry to run this file at each system start. Agent variants may also change the configuration settings for Windows Explorer and/or for the Windows interface.
AutoRun	Autorun worms are a type of malware that spread by taking advantage of the Windows autorun feature. Autorun allows executable files on a drive to be run automatically when that drive is accessed. The feature works via a file named autorun.inf. When a drive is accessed, Windows checks for the presence of autorun.inf and, if found, follows the instructions contained within that file.
FraudLoad	Trojan-Downloader.Win32.FraudLoad.has is a computer threat that can secretly run in the background of a system. Trojan-Downloader.Win32.FraudLoad.has spreads via malicious websites and drive-by downloads. This type of trojan secretly downloads malicious files from a remote server, then installs and executes the files.
FraudPack	Trojan.FraudPack.Gen has two main components: one that is associated with rogue security applications, and one that is associated with adware. The first component is designed to change the Internet Explorer homepage and security settings. It also displays fake error messages that claim that the computer has been infected. Trojan.FraudPack.Gen will attempt to convince you to download a specific rogue security program, such as the Security Scanner fake anti-virus. Rogue security programs are fake computer security applications that are used as part of a scam to steal a victim's money. Instead of fixing problems on the infected computer, they cause the computer to behave erratically and crash frequently. They also spam the victim with constant fake security alerts. This is all done to convince the victim to pay for a "full version" of the fake security application in order to fix these problems – the very problems Trojan.FraudPack.Gen is causing itself. Trojan.FraudPack.Gen is also associated with a number of different registry entries and adware components. ESG security researchers strongly advise removing these immediately. These belong to several different, unrelated malware programs and can cause a whole series of different problems on the infected computer. Trojan.FraudPack.Gen may also include components designed to monitor your online activity, track your keystrokes and send your personal information to a remote party. It is because of this that ESG security researchers consider that removal of Trojan.FraudPack.Gen should be a top priority.
Hupigon	The HUPIGON malware family consists of backdoors. These are usually dropped by other malware onto a system or are downloaded unknowingly by users when visiting malicious sites. HUPIGON

	variants may drop several files or copies of themselves. HUPIGON variants open ports or connect to servers to allow remote users to connect to the affected system. Once a successful connection is established, the remote user executes commands on the system, such as to delete files and folders, download and execute files, and terminate processes. Variants may also gather information about the affected system. They can also steal information such as logged keystrokes, passwords, and other user credentials.
Krap	A trojan, or trojan horse, is a seemingly legitimate program which secretly performs other, usually malicious, functions. It is usually user-initiated and does not replicate. Mal/Krap-D is the actual backdoor component of this malware attack. Mal/Krap-D in particular targets computers with the Windows operating system. Its two variants, OSX/Dloadr-DPG and Linux/Dldr-GV, target computers with the Mac OSX operating system and different Linux distributions respectively. Mal/Krap-D is installed a result of a malicious JavaScript applet that is located on hacked websites. This malicious applet was detected recently on the website for a Colombian transport business. Due to the fact that this malware attack targets different operating systems, it is strongly recommended that Linux and Mac OSX computer users use a reliable anti-malware program to secure their computers. They are especially vulnerable due to the fact that Windows users are more accustomed to the need for anti-virus protection.
Lipler	Trojan Downloader.Win32.Lipler.iml is a rouge program and is one of the latest addition to the group of fake antivirus programs. It is designed in such a way that it looks like a genuine antivirus product but in reality it is just a useless program. This fake software usually gets into your computer when you try to watch online movies from unknown websites. When you visit these websites, you are usually prompted to download a video codec to watch the movie. This is a trick done by the hackers to infect your computer with malware. The video codec actually contains the fake antivirus software installation files. Once the download is complete, Trojan Downloader.Win32.Lipler.iml will get automatically installed to your computer.
Magania	Win32/Magania is a password stealing trojan that injects code into the "*explorer.exe*" process. The injected code varies according to the sample. This type of trojan steals passwords and other sensitive

	information. It may also secretly install other malicious programs.
Poison	Here is how a typical Poison Ivy attack works: The attacker sets up a custom PIVY server, tailoring details such as how Poison Ivy will install itself on the target computer, what features are enabled, the encryption password, and so on. The attacker sends the PIVY server installation file to the targeted computer. Typically, the attacker takes advantage of a zero-day flaw. The target executes the file by opening an infected email attachment, for example, or visiting a compromised website. The server installation file begins executing on the target machine. To avoid detection by anti-virus software, it downloads additional code as needed through an encrypted communication channel.Once the PIVY server is up and running on the target machine, the attacker uses a Windows GUI client to control the target computer. Poison Ivy is so widely used that security professionals have a harder time tracing attacks that use the RAT to any particular attacker.
Swizzor	http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=136491 This trojan was originally detected as Adware-Lop. Due to stealthing and obfuscation mechanisms it uses and the very large number of new variants released in recent weeks, the classification has been changed. This application generates extra pop-up ads while using Internet Explorer. Many versions of this application exist and this description may not cover all.
Tdss	http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tdss TDSS, also known as *Tidserv*, *TDSServ*, and *Alureon*, first appeared in the middle of 2008. TDSS malware are known for their rootkit capabilities and the ability to bypass anti-malware protection. These capabilities make TDSS difficult to detect and consequently, difficult to remove from an affected system. TDSS is often used to distribute other malware like FAKEAV and DNS changers. It is also utilized for click fraud, search engine

	optimization, and advertisements.
VB	http://waleedassar.blogspot.com/2012/03/visual-basic-malware-part-1.html
Virut	http://en.wikipedia.org/wiki/Virut Virut is a malware botnet that is known to be used for cybercrime activities such as DDoS attacks, spam (in collaboration with the Waledac botnet[1]), fraud, data theft, and pay-per-install activities.[2][3][4] It spreads through executable file infection (through infected USB sticks and other media), and more recently, through compromised HTML files (thus infecting vulnerable browsers visiting compromised websites).[2][5] It has infected computers associated with at least 890,000 IP addresses in Poland.[2
Zbot	http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99 The Trojan.Zbot files that are used to compromise computers are generated using a toolkit that is available in marketplaces for online criminals. The toolkit allows an attacker a high degree of control over the functionality of the final executable that is distributed to targeted computers. The Trojan itself is primarily distributed through spam campaigns and drive-by downloads, though given its versatility, other vectors may also be utilized. The user may receive an email message purporting to be from organizations such as the FDIC, IRS, MySpace, Facebook, or Microsoft. The message body warns the user of a problem with their financial information, online account, or software and suggests they visit a link provided in the email. The computer is compromised if the user visits the link, if it is not protected.