Malware distribution trough software piracy: a case study

Trust no one or you will be assimilated! This is the current scenario inside the software cracking and piracy community. This paper focuses on the study of the usage of pirate software to infect systems and their abuse by miscreants. Statistics from collected malware related to software piracy will be presented.

The author believes software piracy will always exist, here included operational systems, applications and games. The problem is directly related to the customer's compulsory behavior for new features and releases leading the user to consume any product; even in beta version (sometimes faked versions) and piracy products.

To deal with this demand, some specialized piracy groups had, for long time, supplied this market with diverse products, among others, we emphasize keygens, which are applications that can generate a registration key to allow software installation and cracks, which are modifications in files from the target software that allows their execution or removes existing protections.

With the advance of software protection techniques, new forms to circumvent these protections and to make this content available are being offered, such as installation packages, cracked versions ready to run and CD emulators. The piracy community is always developing new ways to take care of the demand and to circumvent the protections that are implemented.

The universe of software piracy possess multiple mechanisms of distribution: sites specialized in cracks, keygens and emulators (cd-roms), ftp servers, CDs being sold in streets or offered in sites and mainly P2P applications.

The process of malware distribution uses any of these mechanisms, with only small differences. We must understand that miscreants are very creative and their main goal is to infect as many systems as possible. Files that are accessible through web pages are hosted in sites that explore vulnerabilities in navigators. Why wait for user to download and execute if the system can be infected and controlled through browser vulnerabilities?

Even the malware files, available as keygens and cracks, possess different forms of infection; the great majority of analyzed specimens will infect a system in a second stage, after the installation and decompression. This technique is used only to make more difficult the file identification as malware. The main functionality of this type of malware also varies from simple downloaders and adware to botnets. From the miscreant's point of view this is the perfect scenario, the end user is downloading and executing malicious code with their consent and without any restrictions.

In 2006 one of the main sources of malware propagation through software piracy was the creation of dozens of crackers for the Windows Genuine Advantage. The constant updates of the WGA tool had made users of counterfeit versions of Windows to often search for new versions of crackers and, when they did not succeed, they simply started to install all available crackers. From the WGA cracking files collected, almost 70% were classified as downloaders and bots with elevated degree of sophistication and difficult removal process.

The same issue occurred in the end of the 2006 with the launching of the new version of the Internet Explorer, whose installation only successes through the authentication of the operational system as being legit.

This kind of exploitation and propagation is not restricted to Microsoft products; any popular software with some installation restriction is being used as an attack vector.

The consumer of piracy software is at this moment being heavily targeted by the piracy community which only aims to infect and to control their system for illicit purposes and to feed the piracy industry, normally by stealing all serial numbers of installed software from the users system and later distribution on web sites, without forgetting the traditional use of the systems as part of botnets.

The message here is simples, there is no crack or keygen or another tool related to software piracy that can be considered safe to use, even to download. Users must be discouraged to consume any kind of software piracy in order to avoid their personal information and systems being used my miscreants.