Article Side

Malware Evolution by Eccuni

Article published on December 20th 2011 | Computer

Malware threats today are far more serious than they were before. Why you may ask? It is because malware threats today has the ability to infect millions of nodes and coordinate all of them to perform a single purpose - create havoc on the internet superhighway. Aside from that fact, modern malware can be undetected when they pass through tough security boundaries, they are adaptable and it has more application compared to other worms and viruses. Because of the threat of modern malware, there are many ways to deter the threats of malware.

Malware's History

Four decades ago, a bright individual in BBN named Bob Thomas made an experiment about mobile application, thus came the Creeper program. Creeper program during those times was very astonishing because it was the first program to transfer from one computer to another, through ARPANET. Thus, the very first computer virus, and with this experiment it has exposed the very principle of malware - the ability to spread in a network.

The appearance of Morris Worm back in 1988 showed the power of these simple programs in certain uses and applications. Many years later until the early years of the 21st century malware has continued to evolve; gaining more functions and increasingly more infectious. But even the advances in malware technology, there were still limitations in the code of the malware itself.

Malware Synthesis

By the year 2007, malware has finally changed and made a sudden evolution. During this time, botnets finally appeared and it has changed what many of us believe about malware. Unlike their predecessors, botnets are centrally controlled by a cyber criminal; botnets in different infected computers would cooperate together as one massive application. Aside from this, malware have become more intelligent and are not limited to some capabilities and applications.

This malware evolution has changed the world of malware and cyber criminals have found new ways to develop different kinds of codes for their malware. Instead of the common capabilities of malware such as sending spam, malware can perform dangerous attacks. The command, control and the stealth capabilities of malware have greatly improved far from before. Attackers who use malware program can update it to suits his needs; one day it could send spam mails, the next day it would steal personal information. That is why companies and other organization must have incident response teams.

Our Modern Malware

Because of the evolution of malware and its complex structure nowadays; it is best to know more and understand malware. For us to better understand malware, we need to understand its lifecycle.

Malware begins with infection. The way how they were delivered whether, in a file, from an infected web page or how malware communicates with their author. Persistence of a malware should also be understood because there are malware that can disable antivirus, install backdoors, use rootkit and others. This area should be understood especially by many companies so that they can handle these problems by conducting incident handling training.

Once the malware has taken resident in a victim's computer or system, it will look for ways to communicate with the author without triggering the security system. A malware that can communicate means that they are dangerously, powerful malware; if malware cannot communicate, then they would appear like regular viruses or worms. Powerful malware can communicate via non-standard ports, proxies, encrypting traffic and tunnel within some applications.

Malware will be updated by their authors, they will receive new commands and controls that would make them accomplished the programmed tasks. It can be updated from exchanging of messages from different network or file configuration. Sometimes, malware are programmed to look for ways to connect with their author, when the connection has been severed.

Finally, malware have different functions and behavior. Some malware will target certain information or details in a certain company while some would vary from time to time - depending on the needs of the author.

If we understand these important factors that would define the modern malware, then it is possible to control the possibilities of malware attacks on companies. Companies can then employ the use of tools and better security programs to deter malware; they can also hire a person or a group of people to handle these problems but they must have completed incident response training and other cyber security trainings so that they can perform their tasks much better.

Article Source:
http://www.articleside.com/computer-articles/malware-evolution.htm - Article Side

Eccuni - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in incident response.

More information about EC-Council is available at www.eccouncil.org, a incident response, a incident handling training, a incident response training

Article Keywords:
Malware Evolution, incident response, incident handling training, incident response training, viruses, modern malware, BBN, mobile application, Creeper program, Creeper program, ARPANET, Malware Synthesis, botnets, antivirus, victim, powerful malware, pro