‘e Scan

Malware Detection Technique

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

eScan Anti-Virus – Malware Detection Technique

Malicious code, or malware, is one of the most pressing security problems on the Internet. Today, millions of compromised web sites launch drive-by download exploits against vulnerable hosts. As part of the exploit, the victim's machine is typically used to download and execute malware programs. These programs are often bots that join forces and turn into a botnet. Botnets are then used by cyber criminals to launch denial of service attacks, send spam mails, or host scam pages. Given the malware threat and its prevalence, it is not surprising that a significant amount of previous research has focused on developing techniques to collect, study, and mitigate malicious code. For example, there have been studies that measure the size of botnets, the prevalence of malicious web sites, and the infestation of executables with spyware. Moreover the implementation of honeypots helps further studies on malware in the wild.

What exactly is a honeypot?

Unlike firewalls or Intrusion Detection Systems, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that can do everything from detecting encrypted attacks in networks to capturing the latest in on-line credit card fraud. It is this flexibility that gives honeypots their true power. It is also this flexibility that can make them challenging to define and understand.

At eScan we classify them into four different categories. This not only helps us identify and segregate malware according to its nature but also makes it easier to classify.

What we have here are 4 main categories of honeypots working on an individual level. We have the **Malware URL Collection Honeypot** which relies on web crawlers to analyze each webpage for malware. This is achieved by breaking traffic into two sets – HTTP Requests and HTTP Response. In the case of the former, each request is further broken up into their – Landing URL, Redirect URL, Exploit and Malware URL (if any). On the other hand HTTP Response breaks each set of data into their individual components which sums up to HTML, JavaScript, PDF and Flash. Each of these individual sections are further decoded and scanned for malicious links or exploits.

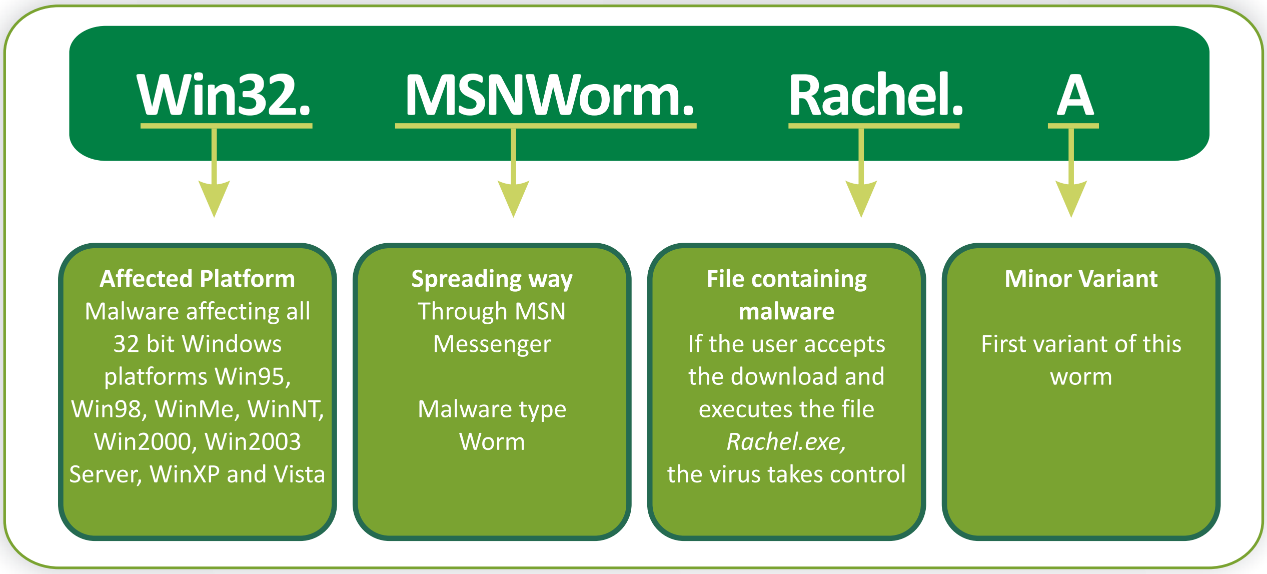
Now, to be able to capture a malware in the wild, we have something known as the **Malware Collection Honeypot**. At eScan we make use of three sets of tools to help identify and collect malware – namely known as the Watcher, Fetcher and Hunter. The Watcher basically runs silently on the Honeypot and adopts a real-time file system monitoring to help detect and collect any system changes which could translate to a potential malware. The Fetcher on the other hand is executed at random intervals and uses a comparing technique to extract new or modified files. The Hunter on the other hand is used at network level and is designed to identify and extract executables from the network stream. With that said, all collected samples are sent for further analysis.

Now to identify spammers it is necessary to encourage them to use honeypot services also known as our **Spam Collection Honeypot**, to their advantage. We achieve this by deploying fake servers which hosts a number of open proxies and open relays. To ensure each of their action is traceable a log is maintained for all deployed services. The **Phishing Collection Honeypot** that we use to analyze fake or spoofed web pages also relies on web crawlers to analyze the webpage content. The crawlers are designed to send back links to our server where they are further analyzed. To further speed up the process and keep false positives at a bare minimum all links are analyzed against predefined set of definitions. All collected information is also checked against

external sources as this prevents genuine sites from getting blacklisted.
All potentially infected or newly detected samples are further inspected by a knowledgeable team of virus analysts in a secure and virtualized environment. It is in this virtualized and secure environment that our team of experts segregate them into Malware, Spam, Malicious URL & Phishing sites. However, Spam, Malicious URL and Phishing are mostly automated as their numbers are way too high to be tested individually.

Our Malware database on the other hand is generated after analyzing various set samples collected from various deployed honeypots. This also includes samples from our partners and customers. All potential threats are further analyzed in our labs in a virtual environment using various tools like systracer, sandboxie etc and a behavioral pattern of the malware is generated after analyzing the reports provided by these tools, since behaviors are the building blocks of our analysis. The analysis provides us with various data about the malware like the dropped files, registry value addition/modification and the configuration changes performed by the malware in order to execute itself either on system boot up or on executing a specific application. This has the benefit that our analysis runs in complete isolation from the samples that are examined, making it much harder for malware to detect the presence of our system. A specific set of malware programs have a similar mode of infecting a system. So even if a new variant of a malware is created, the behavior with respect to its entry points into a system, locations of the infected files saved on the system and sometimes even the names of the malware program files are similar. Taking all this into consideration, a rough set of malware database is generated which is then tested under various environments to check for possible false positives. This is important because at times malware writers use genuine files or a registry value. At times it is also possible that the same registry value which is used by the malware program may also be used by legitimate software.

Once this database has been checked thoroughly, the same is then added to our eScan update servers. This file is then available for download along with the automatic virus signature updates for the eScan clients. This is a continuous



Win32. MSNWorm. Rachel. A

Affected Platform
Malware affecting all 32 bit Windows platforms Win95, Win98, WinMe, WinNT, Win2000, Win2003 Server, WinXP and Vista

Spreading way
Through MSN Messenger

Malware type
Worm

File containing malware
If the user accepts the download and executes the file *Rachel.exe,* the virus takes control

Minor Variant

First variant of this worm

process, so a new database is generated and uploaded as and when the detection and behavioral pattern is available for the new set of Malware.

The other aspect that needs to be kept in mind is the naming convention of the newly discovered malware. However, in order to avoid adding to the glory of the malware authors the malware will need to be renamed. The problem in naming such malware doesn't end there. The main issue is that the malware discovered is not only researched by one research body. There are number of other security labs which simultaneously conduct tests on the same malware string. Here the first to publicly announce the discovery gets to give it a name. All in all, the naming methodology should contain information the industry can recognize: [affected platform] [malware type/spreading method] [virus name] [variant].

Having said that, the standard turnaround time for creating a virus signature is close to 2 hours. The time taken to build the virus definition files is not limited to just one or two viruses but thousands are worked upon in the span of 2 hours. Once the virus definitions are created they are then uploaded to the server, following which they get downloaded at regular intervals of 2 hours by all eScan products installed across the globe. However the time taken to create definition files totally depends on the complexity of the malware which can be anything from 2 hours to a 24 hour time period.

Of all the tests carried out to study the behavior of malicious programs, one important security threat that affects many Internet users today is 'Spyware'. A spyware can roughly be defined as malicious software that obtains information from a user's computer without their knowledge or consent. Having said that, a Spyware can also act as a backdoor agent which can further download malicious programs such as a Keylogger or even a Rootkit. Such malicious software is different from other types of malware, such as viruses and worms, which generally aim to propagate to other systems and cause damage. A spyware attempts to silently monitor the behavior of users, record their web surfing habits, or steal sensitive data such as passwords and user information. The collected information is then sent back to the spyware distributor, where it is used for targeted advertisement or marketing studies. Additionally such spyware programs cause unexpected problems such as performance degradation and frequent crashes of the victim's system. eScan provides its users with a multiple set of options to rid the computer from such spyware infection problems. The first level of protection is provided by the signature based real-time eScan monitor. eScan's real-time monitor will identify known instances of spyware by comparing the binary image of the files to its database of signatures and thus prevents it from being executed on a users system. In order to elude detection, malicious program like a 'Fake Anti-virus' will first try to disable the local Anti-virus software installed on the user's system. With eScan's self protection feature for its files and folders, such kind of activity will not be allowed, thus preventing malware to get total access of the user's system.

Additionally, eScan also provides a Malware URL blocking feature. A separate database of infected URL is maintained by eScan other than the virus signature database to block such infected URLs and hence prevents the user from downloading a malware file unknowingly. This is particularly helpful as a preventive measure since BHOs (Browser Helper Objects) are used by a large fraction of spyware programs. Browser Helper Objects are Windows dynamic linked libraries that are automatically loaded by Internet Explorer when it is launched. These components run in the same address space as the browser and have full control over the browser's functionality. This is the main reason why it is one of the most frequently used techniques employed by spyware program writers because they allow easy programmatic access to the information that flows through a user's browser.

A crucial aspect that needs to be kept in mind is the speed at which malware gets created. Therefore ensuring a timely response to each new variant or strain is far from easy. The real problem is the gap between the time a new threat gets released into the wild to the time an end-users computer receives the required signature. Having said that, this small gap basically represents an open window during which the system remains vulnerable.

So how do we put a lock on such threats?

To shutdown this vulnerable window of opportunity for hackers, eScan comes with Heuristics or proactive detection method which doesn't totally rely on traditional signatures to detect malware. (Note: By default the proactive scan is disabled). So rather than being a simple fingerprint or signature based scanner, the implementation of Heuristics allows the eScan engine to study the behavioral pattern of all running or executed application. This works because malicious programs inevitably attempt to perform actions that legitimate applications do not. Examples of suspicious behavior would include attempting to drop files, disguise processes, replication or execution of code in another process's memory space. Because heuristic scanners look for behavioral characteristics rather than relying on simple pattern-matching, they are able to detect and block new and emerging threats for which a signature or fingerprint has yet to be released.

Here is a brief example of how the eScan Engine works in the background:

- Each time a file is accessed, copied or downloaded via the Web, e-mail or Instant Messenger, the file is intercepted by eScan's real-time monitor and sent for scanning.
- The file is then checked against pre-defined signatures that are continually updated every 2 hours. If the file contents match one of the signatures, the product automatically tries to disinfect the virus. If this action fails, the file is moved to the quarantine folder. If no signature is matched, the file is passed to Heuristics to be checked.
- The file is then checked by executing it in a virtual environment within the eScan Engine. If the file exhibits suspicious, malware-like activity, Heuristics reports the file as malicious. If not, the file is declared clean and the relevant process is allowed to run.
- The eScan Heuristics Engine (when enabled) monitors the actions of the processes (specific processes) as they are executed on the computer. It analyses the behavioral pattern and gives a certain score for each action that gets performed. When the overall score for a process reaches a given threshold, the process is reported as harmful.