
Malware Infecting Other Malware Can Complicate Antivirus Detection

(2010-11-22) - Contributed by Brian Prince

Malware infected with other malware can make life more complicated for antivirus programs.

Malware authors don't always get along - in fact, there have been a number of instances where attackers target each other. But sometimes, malware infecting malware can be a good thing for attackers.

According to Trend Micro Threat

Response Engineer Roland Dela Paz, there has been an uptick of this kind of activity, which he called "hybridized malware." Recently, Dela Paz wrote, Trend observed an IRC bot detected as WORM_LAMIN.AC that was also infected by a mother file infector PE_VIRUX.AA-O.

"It's not clear if these kinds of malware were intentionally created or if they are the result of a highly-infected user system," he blogged. "While some of these problems largely affect malware analysts (such as inaccurate detection names), the biggest issue for users is how it affects cleanup. An incomplete clean operation could lead to the creation of a damaged variant of the malware, which might allow them to evade detection by security software."

If this is deliberate, it could be a tactic that cyber-criminals can use to increase the effectiveness of their attacks, he argued. For example, because PE_VIRUX is polymorphic, WORM_LAMIN variants will also be harder to detect, he wrote.

"This is pure assumption mind you...but this trick of infecting a malware with a virus is being done by others as well to make life easier for their purposes, not to mention adding some layer of protection from AV (antivirus) scanners," Ivan Macalintal, manager of advanced threats research at Trend Micro, told eWEEK. "Why recreate something when there is already a working code for it?"

Dmitry Bestuzhev, senior malware researcher at Kaspersky Lab, said that this type of activity is nothing new.

"We saw it several times in the past...(with) Virut and Sality infecting any kind of malware, including Trojan.Banker," he said. "There is an interesting situation with the detection in this case. On the one hand we have a possible situation when an AV can detect Virut or any other file infector and clean and then deliver a clean copy of Banker for the customer and of course, the Banker will infect the machine and will (steal)money. On the other hand we can have situations when the initial malware, infected by another malware may be detected as an initial Trojan and a delete action could be taken to delete it."

"In practice I saw many cases (where) the infected malware is detected by many AVs, since many of them detected Virut, but...when the banker became clean of Virut it had a really low rate (of) detection," he added. "So, here we're talking about quality of signature and heuristics for detection. If the AV (has) a bad signature, naturally after the Virut disinfection it won't just detect the banker."

Typically, this does not affect the detection of individual threats however, Eric Chien, technical director of Symantec Security Response, told eWEEK. Once a detection engine detects the outer layer of a malicious file and cleans it, the underlying file is then exposed, and can be detected and removed, he said.

It's unlikely, Chien said, "that the main motivation behind malware affecting other malware is competitive in nature. (In) the underground economy, there are many non-technical people who are trying to make a quick buck. In some cases, these people who attempt to spread malware just don't realize that they themselves are infected and their malware has been infected by a file infector from their own machine."

In other cases, attackers are told to wrap their malware with a file infector to increase their returns, he said. Unknowingly, they start distributing infected Trojans.

"From their perspective they don't mind letting another piece of malware piggyback on their own; all they care about is how much money they can make," Chien said.