Evasive Malware’s Gone Mainstream
By Christopher Kruegel, Chief Scientist, Lastline Labs

This year at the RSA Conference in San Francisco, I presented “Evasive Malware: Exposed and Deconstructed.” During that presentation, I led a discussion around the dramatic growth of evasive malware, the increasingly sophisticated behaviors observed in the past year, and what that means for enterprise security professionals and the processes, tools and techniques that they use to protect their organizations.

To support that presentation, Lastline Labs conducted analysis on hundreds of thousands of samples collected in 2014. We found that evasive malware that was once uncommon and seemingly reserved for advanced, targeted attacks by powerful threat actors has gone mainstream. This new Lastline Labs report contains fresh insights into evasive malware along with an update to our “AV Can’t Keep Up” report from 2013-14.

Evasive Malware Aimed at Bypassing Sandboxes Doubles January vs. December 2014

Increasingly, malware that is used by APT (Advanced Persistent Threat) groups leverages sophisticated evasive maneuvers to hide its true malicious nature from traditional sandboxes until it reaches a specific target machine. In fact, in our dataset, we saw the percentage of malware samples that were evasive more than double from January 2014 to December 2014.

Evasive malware is shifting from a seldom-used, sophisticated weapon in the hands of a few to a widely proliferated, popular tool used by many attackers in many ways. The barriers to entry for building and disseminating evasive malware are apparently now more easily surmounted.

Multi-Evasive Malware Runs Rampant

In addition, individual malware samples are including more evasive behaviors, often using a combination of the more of the 500+ evasive behaviors that we track. So, while a year ago, only a small fraction of malware showed any signs of sandbox evasion, today, a sizeable portion is evasive. And while evasive malware a year ago tended to leverage at most two or three evasive tricks, much of today’s evasive malware is tailored to bypass detection using as many as 10 or more different techniques.
Lately, malware authors are throwing in everything but the kitchen sink when it comes to evasive maneuvers—which can actually work in our favor in detecting evasive malware if we know to look for these behaviors. The four most common types of evasive behavior observed by Lastline Labs over the past year were 1) environmental awareness, 2) confusing automated tools, 3) timing-based evasion and 4) obfuscating internal data. Many samples in our study exhibited all four categories of evasive behavior.

**AV Still Can’t Keep Up**

At the same time, signature-based AV scanners are falling farther behind. Last year, we reported that AV can’t keep up with new malware -- with not one scanner having a perfect day catching every new sample, and some new malware going undetected by 10% of the AV scanners for an entire year. In today’s report, we show that from April 2014 to March 2015, no single AV scanner had a perfect day either.

But what’s worse is that the most difficult-to-detect malware became even more elusive. After a full year, 64% of the AV engines failed to detect the 1% of least detected malware. This is a significant increase compared to last year, when this number was only 10%.

![Probability of Malware Detection for Antivirus Solutions](image)

On the brighter side, AV scanners are catching average malware faster than last year — reaching 80% coverage sooner, although never getting to 100%. But the sharp decline in the detection rate of the 1% least detected malware is much more pronounced than this slight improvement in average malware detection rates. As noted last year, the configuration of the various antivirus scanners used by VirusTotal is not necessarily optimal, and it is always possible that a better detection rate could be achieved by relying on external signals or using more “aggressive” configurations.

Ultimately, the more evasive behaviors malware employs the more likely it will succeed in bypassing both signature-based and behavior-based detections. While much of the average malware can still be detected using signature-based tools and standard sandboxing (those built on OS emulation or virtualization with limited visibility into malware execution), evasive malware is bypassing both. Malware authors are always cramming more tricks into their code, and the only way for security professionals to weed them out is to continuously adapt. If we build tools tailor-made to detect evasive malware, integrate across security systems and share threat intelligence, it is possible to get ahead of advanced threats.