



Server-Side Polymorphism: Crime-Ware as a Service Model (CaaS)

By Ryan Sherstobitoff

As the malware threat landscape continues to evolve, hackers are constantly adapting techniques to counteract detection technologies. By utilizing sophisticated methods to evade current antivirus technologies, hackers are relentless in their pursuit of damaging IT systems and stealing personal information.

Several years ago, hackers used polymorphism and metamorphism as tactics to generate new variants in which the virus would morph itself into different variations and successfully bypass signature-based technologies. The antivirus industry eventually responded to polymorphism by creating emulation technologies which mimicked the properties of the morphed virus so it could be detected. This emulation approach depended on the researcher's access to the polymorphic engine; however, the logic needed to be decoded before protection for specific mutations could be developed.

Subsequently, proactive technologies were developed (behavioral, heuristic) when worms began to self-replicate across networks and exploit zero-day vulnerabilities faster than a signature could be created. The idea was to provide protection without depending solely on reactive technologies, which were slow and clunky. Instead, innovative methods were developed that attempt to predict dangerous characteristics. Heuristics really was the first stride towards being proactive by using a statistical probability model to calculate a file's potential of being bad.

The malware landscape has evolved: hackers are shifting their interests from

fame and notoriety to profit and crime and are continually developing new ways to slip below the radar for financial gain. Some of these methods are very innovative and certainly thinking-out-of-the-box when it comes to crime, such as custom HTML injection into financial sites to obtain additional sensitive, personal information.

As we begin to map out the evolution there are common themes when it comes to stealth and camouflage techniques including the following:

- Custom run-time packers
- Server-side polymorphism

In the lab we have discovered that approximately 90 percent of all malware use some form of packers, and the trend indicates they are becoming more customized by the day. Packers compress the code which prevents AV analysts from easily decoding the sample, thus, increasing reaction time dramatically. AV investigators are continually evolving generic unpacking routines (techniques which decompress the file and reveal the malware) in order to combat the rise of packers.

Finally, we have found the emergence of server-side polymorphism or "Crime-Ware as a Service" (CaaS) in which the polymorphic engine does not reside within the virus code itself, rather remotely on a server. There are two forms of server-side polymorphism that we know of today. One type distributes mutated variations of malware in volume into the wild. With the other computers that are part of a botnet and the specific bot variant can mutate remotely via a command over HTTP. This is called *crime-ware as a service* because the actual viral code does not reside on the host but in the cloud similar to a software-

as-a-service platform. In other words CaaS provides malware on demand to the infected host.

This methodology has proven to be quite effective and difficult to counteract when it comes down to the traditional antimalware model. Server-side polymorphism is so hard to detect because the transformation functions (the routines used to change the signature of the code) are not visible to the virus analyst. The actual algorithms or techniques can not be studied to the degree necessary to create an effective vaccination. Botnet communication is often encrypted as a defense mechanism to thwart discovery of the command and control server dishing out the mutated malware.

The best bet for stopping server-side polymorphism is through the use of host-based intrusion prevention technologies (HIPS) which deal with malware at each individual workstation. They are widely regarded by security experts as a more effective safeguard against malware. However, HIPS solutions are only effective to the degree that they implement multiple layers of inspection ranging from the network stack to the application layer using proactive technologies (heuristics, behavioral analysis, behavioral blocking, etc) to provide a holistic view of the threat at hand.

About the Author

Ryan Sherstobitoff is the Chief Corporate Evangelist at Panda Security USA (www.pandasecurity.com). He is widely recognized as a security expert throughout the country and lectures audiences across the U.S. on cybercrime trends as well as corporate risk assessments. He can be reached at ryans@us.pandasecurity.com or through his blog at <http://pandasecurity.wordpress.com/>.