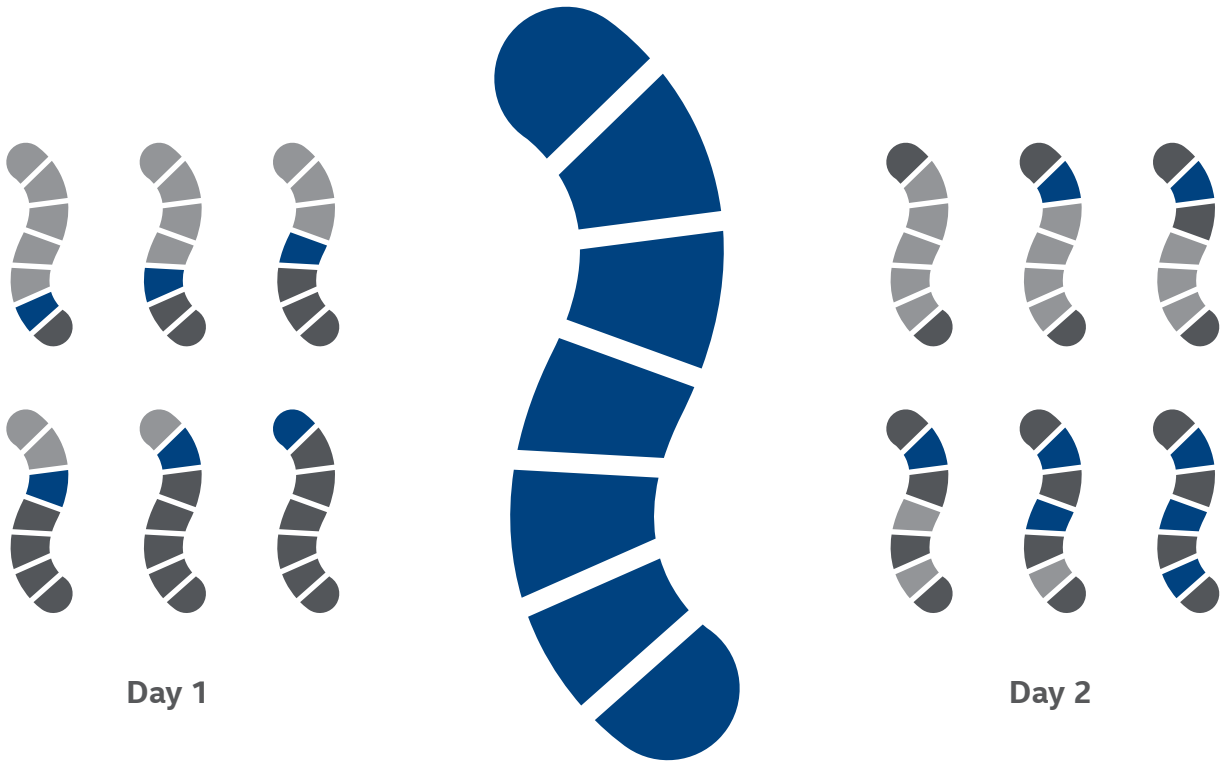
April 2015

# Catch Me If You Can: Antics of a Polymorphic Botnet

**McAfee Labs**

**W32/Worm-AAEH is a polymorphic downloader worm that changes its form with every infection and morphs its identity up to six times per day to evade detection.**




**W32/Worm-AAEH behaviors:**

**Executes**
at system startup.

**Copies**
itself on all removable drives.

**Disables**
Windows Task Manager's ability to terminate applications.

**Detects and evades**
virtual machines and antivirus software.

**Injects malware**
- Password stealers
- Ransomware
- Rootkits
- And more

The McAfee Labs zoo contains more than five million unique W32/Worm-AAEH samples. It infected over 23,000 systems in 2014. In April 2015, a global law enforcement action took down the control servers for this botnet.

Catch Me If You Can: Antics of a Polymorphic Botnet

Visit **www.mcafee.com/PolymorphicBotnet** for the full report.



McAfee is now part of Intel Security.