Issued 7/17/17

$7 Malware Allows Anyone to Become a Hacker Overnight

Security company Proofpoint has discovered a new form of malware that can be purchased for just $7 and which has the potential of going undetected by antivirus software. In an in-depth analysis of the malware, Proofpoint explains that Ovidiy Stealer is priced at $7-13 USD and the archive includes one build that comes as a precompiled executable. The company says the file is encrypted to "thwart analysis and detection," and while the infection can be detected by some antivirus solutions, it's flagged with a generic description that says little about its purpose.

Ovidiy Stealer typically spreads with the help of executable email attachments, compressed executable attachments, and links to keygen websites or hosting pages. In all cases, the included file is an executable that's infected with the malware, so this is the first thing to look for if you want to remain protected. The malware targets a number of popular software solutions, including Google Chrome, Opera browser, Filezilla, and Torch browser. "We have observed versions 1.0.1 through 1.0.5 distributed in the wild. Ovidiy Stealer is written in .NET and most samples are packed with either .NET Reactor or Confuser. Upon execution the malware will remain in the directory in which it was installed, and where it will carry out tasks. Somewhat surprisingly, there is no persistence mechanism built into this malware, so on reboot it will cease to run, but the file will remain on the victim machine," Proofpoint says.

Once it infects a machine, the malware uses SSL/TLS for communication with a command and control server, and looks for passwords in the applications mentioned above to transmit them to the hackers. It sends information such as processor ID, website with saved credentials, targeted applications, username and password, and registered Ovidiy Stealer username. Several updated samples of the password stealer have already been spotted online, so updating security software and always checking twice before downloading files coming from untrusted sources are the two best ways to remain protected.