Issued 3/20/18

Cyber-Crooks Find a New Way to Share Malware

Yet another cybercrime-as-a-service offering is making it easier for even wannabe crooks to carry out large-scale malware campaigns. Known as BlackTDS, the service further lowers the bar for prospective cybercriminals. It allows individuals without technical know-how to instruct the service owners to carry out highly scalable, potentially massive spam and malvertising campaigns on their behalf. The service includes hosting and configuration of the components of a sophisticated drive-by attack, as well as support for social engineering and the flexibility to either distribute malware directly, or simply redirect victims to exploit kit landing pages. "The low cost, ease of access, and relatively anonymity of BlackTDS reduce the barriers to entry to web-based malware distribution," said researchers at security company Proofpoint, who detailed the campaign. Those behind BlackTDS have been advertising their services on underground markets since December 2017, offering their services for the purposes of handling social engineering and the redirection to exploit kits, while also claiming to prevent detection by cybersecurity researchers and sandbox tools. The adverts describe BlackTDS as offering 'dark web traffic ready-made solutions' capable of being able to use code injection on hacked websites, as well as stating that the user doesn't need to have their own server to receive traffic, meaning the service is open to even low-level criminals. "BlackTDS handles not only the filtering and redirection but also hosts social engineering templates -- like fake Flash updates -- that can be used to trick users into clicking, downloading, and installing malware," Kevin Epstein, VP, Threat Operations Center at Proofpoint, told ZDNet. In many cases, the malicious code is delivered to victims through fake software updates purporting to be Java, Flash, font packs,

and more, as well as other social engineering schemes where the users are encouraged to download fake updates which then compromise the system.