31 MAY 2017 NEWS

Dark Web Hackers Are Attacking Each Other Relentlessly

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

Cybercriminals operating inside the Dark Web continuously launch attacks and surveillance attempts designed to disrupt their fellow black hats, new Trend Micro research has revealed.

The security vendor set up several honeypots in Tor, consisting of: a closed black market; a blog advertising services; a closed underground forum; and a private file server.

The installations exposed one or more flaws which could allow an attacker to take control, according to senior threat researcher, Marco Balduzzi.

Trend Micro recorded as many as 170 attacks daily on one of its honeypots in May 2016, although the volume can partly be explained by Tor proxies like Tor2web, which effectively exposed its hidden services to the public internet without requiring any additional configuration.

After filtering out Tor2web, however, the attacks continued – hitting around 44 per day in July.

These included disruptive defacements; attempts to hijack communications going to and from the honeypot; and data theft from the FTP file server; Monitoring of IRC conversations via logins to the simulated chat platform; and manual attacks against the custom app running the forum.

Interestingly, while attacks from the public internet tended to use automated tools, those emanating from the Dark Web were usually manual in nature and more cautious, Balduzzi explained.

“For example, once they gained access to a system via a web shell, they would gather information about the server first by listing directories, checking the contents of databases, and retrieving configuration/system files,” he revealed.

“These manual attackers often deleted any files they placed into our honeypot; some even went ahead and left messages for us … indicating that they had identified our honeypot. Interestingly, attackers seem to be aware that compromised hidden services in the Dark Web are gold mines as all originating attacks like DDoS or SPAM will be automatically anatomized by Tor.”

Indexing and searching is more difficult on the Dark Web, highlighting the determination of the black hats to spy on and disable the operations of their competitors, Balduzzi concluded.