May 30, 2017

Dark web services getting attacked too, as Tor sites become less hidden

Despite their anonymity, sites and services hidden on the dark web are not immune to cyberattacks, as recently demonstrated by a group of researchers who coaxed cybercriminals into attacking fake Tor sites in order to study their behavior.

Cybercriminals will need to search out ever deeper recesses of the dark web, as Tor sites are increasingly exposed and potentially hacked, said Marco Balduzzi, Trend Micro senior research scientist.

Over a seven-month period between February and September 2016, researchers from Trend Micro and French communications school Eurecom monitored honeypots that they created, as they were repeatedly subjected to both automated and manual attacks. The honeypots were designed to look just like typical underground services, including an invitation-only drug marketplace, a blog site promoting solutions for hosting in the Tor network; and a custom private forum that required registration and a referral to join.

The automated attacks would often attempt to upload web shells, phishing kits and mailers, or try to deface sites, according to paper authored by the researchers. Many of these attacks took place via Tor proxies such as Tor2web, which allow ordinary browsers to access dark web content while still keeping the materials anonymous, but as a byproduct also expose hidden URLs to malicious campaigns.

"Internet crawlers automatically index information logs [that are] made unexpectedly available online by these proxies. As a consequence, attackers can benefit from Google Dorks to look for vulnerable services like known buggy web applications in both the surface and the hidden web," explained Marco Balduzzi, report co-author and Trend Micro senior research scientist, in an interview with SC Media. (Google Dorking is a means of acquiring ordinarily hard-to-find web information by leveraging Google's advanced search techniques.)

Other automated attacks used security scanning tools to locate potential targets, then executed path traversal exploits on the honeypots in an attempt to access private keys. In total, the researchers collected 157 unique variations of web shells, six phishing kits and 22 mailers, and observed 33 page defacements, more than 1,500 path traversal attempts, and over 400 attempts to steal the private key.

While some of the automated attacks appeared accidental as web scripts unintentionally meandered into dark web territory, the manual attacks seemed quite purposeful in nature, with cybercriminals apparently going out of their way to actively seek out and investigate services operated by potentially rival organizations.

These manual attacks were generally more careful and covert, as the hackers who perpetrated them would usually delete traces of their activity, the report explains. In a few cases, however, attackers left messages after realizing during reconnaissance that they had come across a honeypot. The researchers also found evidence of 71 FTP file downloads perpetrated by the manual intruders.

"Given that indexing and searching is more difficult within the dark web, this shows the amount of effort motivated criminals are putting into finding and disabling sites controlled by their competitors," wrote Balduzzi in a May 30, 2017 blog post summarizing the research.

Balduzzi co-wrote the original report along with Onur Catakoglu, Eurecom researcher, and Davide Balzarotti, associate professor at Eurecom. Entitled "Attacks Landscape in the Dark Side of the Web," the paper was originally published in April 2017 and was subsequently presented at a pair of industry conferences.

To encourage attacks on their honeypots, Trend Micro promoted its fake Tor services by posting their URLs on various forums, sites and search engines (regular and dark web), as well as by visiting their apps using Tor2web, which shares URL details with the Tor search engine Ahmia.

With their sites becoming less private and more prone to attack due to Tor proxies and yellow-page services, criminals may have to penetrate even deeper into the dark web's recesses to conduct their business, Balduzzi told SC Media. "More and more criminals are actively looking for new, unmonitored grounds to communicate and act in a more hidden fashion," said Balduzzi.