5/30/2017
05:20 PM

Cybercriminals Regularly Battle it Out on the Dark Web

Jai Vijayan
News

People operating criminal services on Tor and other darknets attack each other frequently, a study by Trend Micro shows.

Apparently, there's very little love lost between criminals in the cyber underworld.

A study of the Dark Web by Trend Micro shows that cybercriminals attack each other with almost the same ferocity as they reserve for their victims outside of it.

The security vendor recently set up four honeypots simulating a cybercrime operation on the Tor network. One of the honeypots simulated an invitation-only black market for stolen goods, another masqueraded as an underground forum for registered users, and one purported to be a private FTP file server for sensitive documents. The fourth honeypot purported to be a blog offering custom criminal services on the Dark Web.

The goal of the exercise was to find out if cyber criminals operating in the Dark Web tend to attack hidden services and servers used by other criminals on Tor.

The answer as it turned out was a resounding "yes." Over the six month period that the honeypots were up, Trend Micro counted numerous attacks against them from inside Tor and from the Internet as well. The attacks peaked in May, averaged around 170 per day.

"Gangs are actively targeting opponents to enlarge their domain in the Dark Web," says Marco Balduzzi, senior researcher at Trend Micro.

The Dark Web is a perfect platform for exchanging shady services such hacking services, 0-day flaws, other malware, and goods like illegal drugs, he says. "These 'shopping sites' are run by criminals who actively deface each other to redirect possible customers to their own shop."

In many cases, attackers looked for opportunities to compromise other criminal sites on the Dark Web so they could launch denial-of-service and targeted attacks with even more cover than if they were to launch them using their own infrastructure.

"Since the Dark Web — like Tor — enforces anonymity and confidentiality by protocol, a compromised machine in this network, gives the attacker the possibility to run anonymous attacks to third parties," Balduzzi says.

Among the attacks that Trend Micro saw were those that attempted to subvert traffic away from its honeypots to competitor websites. Also common were attempts to hijack and listen into the communications from and to the honeypot, as well as to steal data from their honeypot that was disguised as an FTP server.

Interestingly, Trend Micro's security researchers discovered that services hosted on Tor are not as private or inaccessible as some would assume. Tor proxies like Tor2web that allow Internet users to access the network, also makes hidden services on Tor accessible to search engines.

Trend Micro's honeypot on Tor was openly available to the public Internet and received a majority of the attacks in May, from there.

"Services hidden in the Dark Web are prone to attacks similarly to misconfigured and vulnerable services exposed to the Internet," Balduzzi says. Organizations that use Tor for legitimate purposes should not assume that a service or server us going to be hidden just because it is configured in the Dark Web as a hidden service, he warns.

Unlike attacks on the Internet, many of which are automated and of relatively low quality, attacks inside the Dark Web are manual and conducted by people with very specific goals in mind.

"On the Internet, websites are indexed by search engines like Google and attackers use Google Dorks to find vulnerable sites," he says.

This is a task that is usually conducted by bots and the attacks themselves tend to be generic: For example, an unpatched system might get attacked for secondary exploitation. On Tor, "attackers know what they are doing," Balduzzi says.

As a result, attacks are more sophisticated and running a specific goal like subverting an opponent business or stealing specific information.