Cybersecurity study of the dark web exposes vulnerability to machine identities

March 8 2019

Credit: CC0 Public Domain

A thriving marketplace for SSL and TLS certificates—small data files used to facilitate confidential communication between organizations' servers and their clients' computers—exists on a hidden part of the Internet, according to new research by Georgia State University's Evidence-Based Cybersecurity Research Group (EBCS) and the University of Surrey.

Networked machines use keys and SSL/TLS certificates to identify and authenticate themselves when connecting to each other, much like humans employ user names and passwords to go online, according to Venafi, a privately held provider of machine identity protection and sponsor of the research.

When these certificates are sold on the darknet, they are packaged with a wide range of crimeware that delivers machine identities to cybercriminals who use them to spoof websites, eavesdrop on encrypted traffic, perform attacks and steal sensitive data, among other activities.

Uncovering the widespread availability of these certificates on the darknet was a surprise, according to lead author David Maimon, an associate professor in Georgia State's Andrew Young School of Policy Studies and director of the EBCS. A search of five marketplaces in the darknet for this research uncovered 2,943 mentions for "SSL" and 75 for "TLS." In comparison, there were just 531 mentions for "ransomware."

"One very interesting aspect of this research was seeing TLS certificates packaged with wrap-around services—such as Web design services—to give attackers immediate access to high levels of online credibility and trust," he said. "It was surprising to discover how easy and inexpensive it is to acquire extended validation certificates, along with all the documentation needed to create very credible shell companies without any verification information."

"This study found clear evidence of the rampant sale of TLS certificates on the darknet," said Kevin Bocek, vice president of security and threat intelligence for Venafi. "TLS certificates that act as trusted machine identities are clearly a key part of cybercriminal toolkits, just like bots, ransomware and spyware. Every organization should be concerned that the certificates used to establish and maintain trust and privacy on the Internet are being weaponized and sold as commodities to cybercriminals."

More information: Download a free copy of the report at ebcs.gsu.edu/download/ssl-tls- … nce-on-the-dark-web/.

Provided by Georgia State University

Citation: Cybersecurity study of the dark web exposes vulnerability to machine identities (2019, March 8) retrieved 5 May 2024 from https://techxplore.com/news/2019-03-cybersecurity-dark-web-exposes-vulnerability.html