ABSTRAK

Pelacakan Pelaku Kejahatan Siber Pengguna *Virtual Private Network* (VPN) pada Jaringan *The Onion Router* (TOR) (Studi Kasus di Badan Siber dan Sandi Negara)

Muh. Abduh Dwi Putra

Teknologi VPN dan TOR dapat disalahgunakan oleh pelaku kejahatan siber untuk melakukan serangan siber, dengan maksud agar mereka sulit dilacak oleh pihak berwenang ketika mereka melakukan aksinya. Oleh sebab itulah penulis bermaksud ingin meneliti mengenai prosedur dan strategi yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), sebagai salah satu lembaga yang berwenang dalam *cyber security* di Indonesia, dalam melakukan pelacakan pelaku kejahatan siber di Indonesia yang menggunakan VPN pada jaringan TOR khususnya pada kasus ancaman teror melalui *Facebook*, *WhatsApp*, dan *e-mail*. Penelitian ini bersifat deskriptif dengan metode kualitatif. Teknik pengumpulan data adalah dengan observasi, wawancara disertai kuesioner dan dokumentasi. Teknik pengambilan sampel yaitu menggunakan *purposive sampling*. Penulis melakukan wawancara terhadap staf teknis dan berdiskusi mengenai prosedur penanganan serangan siber berupa dengan mengirimkan ancaman teror yang berisi pesan yang telah disematkan virus, yang dikirim kepada BSSN melalui *Facebook*, *WhatsApp messenger*, dan *e-mail* dengan minimal parameter adalah terlacaknya alamat IP pelaku. Penulis merekomendasikan *project profiling* pada akun media sosial yang digunakan pelaku. Ancaman teror tersebut terdeteksi oleh sistem *Honeynet* yang dimiliki BSSN. Berdasarkan hasil penelitian, alamat IP pengguna VPN dan TOR pelaku dapat terlacak oleh karena adanya kebocoran DNS dan WebRTC, perpindahan relai TOR yang terdeteksi, dan simpul keluar TOR yang tidak terenkripsi. *Project profiling* melalui akun media sosial dapat membantu proses pelacakan pelaku kejahatan siber pengguna VPN dan TOR di instansi BSSN dengan memanfaatkan informasi yang dapat digali dari profil akun tersebut.

Kata kunci : kejahatan siber, komputer forensik, pelacakan alamat IP, TOR, VPN

ABSTRACT

TRACKING CYBER CRIMINALS OF VIRTUAL PRIVATE NETWORK (VPN) USERS ON THE ONION ROUTER (TOR) NETWORK (CASE STUDY AT NATIONAL CYBER AND CRYPTO AGENCY)

Muh. Abduh Dwi Putra

VPN and TOR technology can be misused by cyber criminals to carry out cyber attacks, with the intention that they are difficult to track by the authorities when they carry out their actions. That is why the author intends to examine the procedures and strategies carried out by the Badan Siber dan Sandi Negara (BSSN), as one of the institutions authorized in cyber security in Indonesia, in tracking cyber crime perpetrators in Indonesia who use VPNs on the TOR network especially in cases of terror threats through Facebook, WhatsApp and e-mail. This research is descriptive with qualitative methods. Data collection techniques are by observation, interview accompanied by questionnaire and documentation. The sampling technique is using purposive sampling. The author conducted interviews with technical staff and discussed procedures for handling cyber attacks in the form of sending terror threats containing messages that have been pinned with viruses, sent to BSSN via Facebook, WhatsApp messenger, and e-mails with a minimum parameter is the tracing of the perpetrator's IP address. The author recommends project profiling on social media accounts that are used by actors. The terror threat was detected by the Honeynet system owned by BSSN. Based on the results of the study, the IP addresses of VPN users and TOR perpetrators can be traced by DNS and WebRTC leaks, detected TOR relay movements, and unencrypted exit TOR nodes. Project profiling through social media accounts can help the process of tracking cyber crime perpetrators VPN and TOR users in BSSN agencies by utilizing information that can be extracted from the account profile.

Key words : computer forensic, cybercrime, IP tracking, TOR, VPN