TINJAUAN HUKUM MENGENAI TINDAK PIDANA *CRACKING* MENGGUNAKAN *BOTNET* (ROBOT NETWORK) TERHADAP SISTEM KOMPUTER DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

ABSTRAK

TEDI PRATAMA

Seiring perkembangan teknologi informasi, *cybercrime* muncul sebagai dampak negatif dari perkembangan tersebut. Tindak pidana *cracking* menjadi salah satu contoh. Namun tindak pidana *cracking* ini semakin berkembang dengan berbagai teknik yang sangat tinggi dan modus yang berbeda dan juga mempunyai dampak yang sangat besar. *Botnet* merupakan tindak pidana *cracking* yang dianggap sangat berbahaya pada saat ini. Ini karena akibat yang ditimbulkanya sangat besar. Dalam tindak pidana *cracking* menggunakan *botnet* tersangka dengan sengaja menanamkan *payload* yang ditanam dan diinstruksikan untuk penyebaran virus/*worm*, *spam*, *phising*, *spyware* juga teknik XSS untuk pencurian data, dan bahkan secara serentak menyerang dan merusak DoS (*Denial of Service*) melalui *search bot* dan mengumpulkan data, membuat data *base*-nya dan melakukan *hacking online*. Akibat dari penggunaan teknik tinggi ini, penegak hukum akan kesulitan dalam menentukan ketentuan hukum mana yang akan diterapkan pada tersangka dan bagaimana upaya pembuktian yang akan dilakukan penegak hukum. Oleh karena itu, penulis menitik beratkan Penelitian ini pada masalah ketentuan hukum dan upaya pembuktian tindak pidana *cracking* menggunakan *botnet* berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal ini dikarenakan tidak sedikit para tersangka lolos dari jeratan hukum sebagai akibat dari kesulitan dalam menerapkan ketentuan hukum mana yang tepat bagi tersangka dan upaya pembuktian yang tepat. Permasalahan yang muncul antara lain tentang pengaturan tindak pidana *cracking* menggunakan *botnet* terhadap sistem komputer dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta upaya pembuktian atas tindak pidana *cracking* menggunakan *botnet*.

Penelitian ini, dilakukan secara deskriptif analistis dengan menggunakan metode pendekatan yuridis normatif, data yang diperoleh dianalisis secara yuridis kualitatif.

Berdasarkan anilisis terhadap data yang diperoleh disimpulkan bahwa, perbuatan yang dilakukan tersangka dengan cara memasukkan *software* ke dalam ratusan komputer dan merusak kinerja sistem komputer dan melakukan *hacking online* dengan cara memasukkan *worm* yang berisi perintah-perintah ke dalam jutaan komputer termasuk instansi-instansi penting untuk mengendalikan sistem pengoperasian secara masal (tindak pidana *botnet*) merupakan suatu perbuatan melawan hukum yang dapat menimbulkan akibat hukum sebagaimana diatur dalam Pasal 32 ayat 1 juncto Pasal 33 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan telah memenuhi unsur-unsur dalam ketentuan tersebut. Upaya pembuktian yang dapat dilakukan adalah melalui proses persidangan dengan hukum pembuktian sesuai dengan Pasal 1 angka (4), Pasal 5 angka (1), dan Pasal 5 angka (2) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan tetap memperhatikan Pasal 183 dan Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

LEGAL VIEW ABOUT CRACKING USING CRIMINAL OFFENSE BOTNETS (ROBOT NETWORK) TO COMPUTER SYSTEM ASSOCIATED WITH UNDANG-UNDANG NUMBER 11 YEAR 2008 ABOUT THE INFORMATION AND ELECTRONIC TRANSACTIONS

ABSTRACT

TEDI PRATAMA

As developments in information technology, cybercrime emerged as the negative impact of these developments. Cracking crime be one example. But crime is increasingly cracking developed with various techniques that are very high and different modes and also had a huge impact. Cracking botnet is a crime which is considered very dangerous at this time. This is because due to the extremely large ditimbulkanya. In cracking using a botnet crime suspects deliberately planted embed payload and instructed to spread viruses / worms, spam, phishing, spyware is also XSS techniques for data theft, and even simultaneously attacking and damaging DoS (Denial of Service) through a search bot and collect data, make it a data base and conduct online hacking. Resulting from the use of this high technique, law enforcement will be difficulty in determining the legal provisions which would apply to suspect and how efforts to proving that law enforcement will be carried out. Therefore, the authors of this research focuses on the problem of legal provisions and efforts to proving the crime cracking using botnets based on Undang-Undang Number 11 Year 2008 concerning Electronic Transactions and Information. This is because not a few of the suspects escaped from the shackles of law as a result of the difficulty in applying the legal provisions which are appropriate for the suspect and the proper evidentiary efforts. The problems that arise are about the settings using botnets cracking crime against computer systems in Law Number 11 Year 2008 concerning Electronic Transactions and Information and verification efforts on cracking crime using botnets.

This study, conducted by descriptive analytical method normative juridical approach, the data obtained was analyzed by juridical qualitative.

Based on data obtained anilisis concluded that the defendant performed acts by entering into hundreds of computer software and damage the performance of computer systems and hacking online by entering a worm that contains the commands into the millions of computers, including important government agencies to control operating system en masse (botnet crime) is an unlawful act that could lead to legal consequences as set forth in Article 32 paragraph 1 in conjunction with Article 33 of Undang-Undang Number 11 Year 2008 concerning Electronic Transactions and Information and has met the elements in the regulation . Efforts of proof that can be done is through a trial process with the rules of evidence in accordance with Article 1 (4), Article 5 digits (1), and Article 5 figures (2) of Undang-Undang Number 11 of 2008 on Electronic Information and Transactions with due regard to Article 183 and Article 184 of Act Book of Criminal Procedure (Criminal Procedure Code).