Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator)

Abdul Razzaq Matthew Aditya*[1], Amelia Widya Octa Kuncoro Putri[2], Desta Lesmana Musthofa[3], Pujo Widodo[4]
[1,2,3,4] Program Studi Peperangan Asimetris, Universitas Pertahanan Republik Indonesia
Kawasan IPSC Sentul, Bogor, Indonesia

e-mail: ***[1]armatthewaditya1@gmail.com**, [2]ameliawidya007@gmail.com, [3]lesmanadesta@gmail.com, [4]pujowidodo78@gmail.com

Abstract

When we're talking about national defense, the meaning is currently expanding in line with the times. The advancement of technology today can be seen from the massive use of smartphones in the world. However, technological developments also followed by the potential for cybercrime which is also increasingly sophisticated, currently cybercrime is evolving from just password guessing to tools. One example of a tool is predatory spyware. Attacks with sophisticated equipment such as predatory hacking tools can threaten cyber security in the national defense system. Therefore, literature is needed to uncover and overcome cyber attacks and hacking threats to national defense. The method used in this article is descriptive qualitative research method. The results of this research are first, the cyber attack method consists of cyber espionage, vandalism, sabotage, and power grid attacks. Second, the operand mode of cybercrime consists of two ways, physically hacking and logically hacking. Third, predatory spyware is a hacking tool developed by the company Cytrox that can record the user's cellphone activity and has potential to threaten the country's cyber defense. Fourth, the biggest potential loss from predatory spyware is the dissemination of strategic information from the state to other parties that can threaten state security.

Keywords— *Cybercrimes, Cyber Threats, Hacking Tools, National Defense, Predator*

Abstrak

Ketika membicarakan pertahanan negara maknanya saat ini menjadi meluas selaras dengan perkembangan zaman. Majunya teknologi saat ini dapat dilihat dari masifnya penggunaan *smartphone* di dunia. Namun perkembangan teknologi diikuti juga dengan potensi dari kejahatan siber yang juga semakin canggih dimana saat ini kejahatan siber berevolusi dari hanya *password guessing* menjadi *tools.* Salah satu contoh dari *tools* adalah *spyware predator*. Serangan dengan peralatan canggih seperti *hacking tools predator* ini dapat mengancam keamanan siber pada sistem pertahanan negara. Oleh karenanya dibutuhkan literatur untuk mengungkap dan mengatasi serangan siber dan ancaman *hacking* terhadap pertahanan negara. Metode yang digunakan dalam artikel ini adalah menggunakan metode penelitian kualitatif deskriptif. Hasil dari dari penelitian ini adalah pertama, metode penyerangan siber terdiri atas spionase siber, vandalism, sabotase, dan serangan jaringan listrik. Kedua, modus oprandi pada kejahatan siber terdiri dari dua cara yakni *physically hacking* dan logically hacking. Ketiga, *spyware predator* adalah jenis tools hacking yang dikembangkan oleh perusahaan *cytrox* yang dapat merekam aktivitas ponsel pengguna dan hal ini tentu saja berpotensi mengancam pertahanan siber negara. Keempat, potensi kerugian terbesar dari *spyware predator* adalah tersebarnya informasi-informasi strategis negara terhadap pihak-pihak lain yang dapat mengancam keamanan negara.

Kata kunci— Ancaman Siber, Hacking Tools, Kejahatan siber, Pertahanan Negara, Predator

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

1. Pendahuluan

Seiring dengan perkembangan dalam berbagai bidang kehidupan manusia saat ini ketika membicarakan Pertahanan Negara artian dan konteks yang dihadapi tentu saja juga ikut berkembang. Seiring dengan semakin berkembangnya ilmu pengetahuan dan teknologi, hal ini tentu saja memiliki nilai positif bagi kemudahan kehidupan manusia, namun tentu saja hal ini juga membawa potensi yang dapat membahayakan manusia. Dalam konteks Negara dan Pertahanan perkembangan teknologi informasi diikuti oleh potensi ancaman dalam bidang keamanan siber pada negara. Data dari kominfo untuk jumlah pengguna internet di Indonesia pada tahun 2021 jumlahnya mencapai 202,6 juta pengguna, data ini meningkat cukup banyak dari tahun sebelumnya dimana pengguna internet Indonesia adalah 175,4 juta orang (Kominfo, 2021) . Hal ini dapat dikatakan bahwa di Indonesia mengalami penetrasi digital yang cukup tinggi, saat ini seluruh masyarakat di negara ini bergantung cukup tinggi pada teknologi. Kebergantungan ini tidak hanya dialami oleh masyarakat biasa namun pemerintahan dan urusan kenegaraan menjadi ikut bergantung pada teknologi. Oleh karenanya keamanan dalam penggunaan teknologi cukup penting karena potensi dari kejahatan secara siber yang semakin terbuka dengan tingginya masifnya penggunaan teknologi saat ini.

Pada tahun 2021 sendiri terdapat cukup banyak jumlah serangan siber secara general yang diterima oleh Indonesia. Dari berita yang dilansir dari (Liputan6.com, 2021) jumlah percobaan serangan siber yang ditujukan kepada Indonesia mencapai angka 1,3 miliar dalam kurun waktu Januari-November 2021. Sementara menurut Menteri Komunikasi dan Informatika (Kominfo) Johnny G. Plate menjelaskan bahwa di sepanjang tahun 2021 sejumlah 888.711.736 ancaman siber yang menghantam Indonesia atau sama dengan 42 ancaman siber di setiap detiknya. Selain itu, Suara.com (2021) melansir bahwa Johnny juga menjelaskan data dari Universitas Stanford pada tahun 2020, yang menemukan bahwa faktor kelalaian manusia atau yang biasa disebut sebagai *human error* menjadi faktor tertinggi atas adanya pelanggaran keamanan siber dengan persentase sebesar 88%. Selain dari Kominfo, BSSN atau Badan Siber dan Sandi Negara juga memberikan data bahwa saat ini sudah sebanyak 290 juta kasus serangan siber yang terjadi di Indonesia. Jumlah ini tentunya mengalami kenaikan dibanding tahun sebelumnya yaitu sebanyak 25%, dimana pada tahun sebelumnya kasus serangan siber telah memberikan kerugian yang cukup besar bagi Indonesia yaitu sebesar US$ 34,2 miliar.

Ancaman siber sendiri menurut (Putra, 2018: 107-108) memiliki artian setiap kondisi, situasi ataupun kemampuan yang dinilai dapat melakukan berbagai tindakan seperti gangguan dan serangan yang berpotensi merusak serta merugikan yang dapat menimbulkan berbagai ancaman, seperti ancaman kerahasiaan, ketersediaan, dan integritas dari sebuah sistem dan informasi. Dalam artian ini ancaman yang dimaksudkan adalah sesuatu yang belum terjadi namun memiliki potensial untuk dapat melakukan kerugian yang dalam konteks ini baik alat yang digunakan ataupun ancaman yang ditimbulkan bukan secara fisik namun secara siber. Pengertian dari ancaman secara siber dapat diartikan bahwa alat yang digunakan menggunakan teknologi informasi dan komputer serta kerugian

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

yang ditimbulkan juga lewat teknologi informasi.

Jika dilihat dari cakupannya ancaman siber *(cyber threat)* selain dapat dialami oleh individu dalam level mikro, cyber threat juga dapat menjadi masalah yang lebih kompleks dengan level yang lebih tinggi yakni level kenegaraan. Dunia maya saat ini telah menjadi medan perang baru tanpa batas di era modern sekarang ini dimana sumber ancaman tidak mudah ditebak apakah itu berasal dari individu, negara, atau individu yang ditunggangi oleh negara (Sutomo, 2022: 1260).Dalam hal ini konsep pertahanan nasional menjadi lebih luas cakupannya, karena potensi ancaman negara tidak hanya secara fisik namun juga secara siber. Dalam konteks politik kenegaraan setiap negara memiliki kewaspadaan yang cukup tinggi dalam berbagai ancaman baik berupa konflik besar seperti antar negara ataupun konflik dalam lingkup domestik. Adanya globalisasi juga mendorong perkembangan teknologi sehingga terdapat potensi ancaman konflik dengan menggunakan sarana dan prasarana yang lebih kompleks salah satunya teknologi informasi di dunia maya yang dapat mengarahkan pada peperangan siber *(cyber warfare)* (Subagyo, 2015 : 90-91). Peperangan siber sendiri menjadi salah satu ancaman terbesar yang dapat terjadi yang disebabkan oleh kejahatan siber.

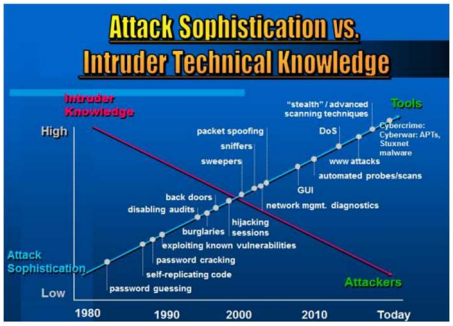
Ancaman oleh kejahatan siber saat ini adalah hal yang sangat relevan melihat perkembangan teknologi informasi, dan bukan hanya secara konseptual semata namun kejahatan siber memang nyata terjadi pada beberapa kasus. Kejahatan siber sendiri sudah berevolusi dan beragam jumlahnya, kejahatan siber dibagi menjadi beberapa diantaranya adalah: *hacking, cyber sabotage, cyber espionage, garding, cyber attack, vandalisme, spyware,* dan serangan jaringan listrik (Subagyo, 2015: 98-99). Perbedaan pada masing-masing kejahatan siber ini ada pada jenis teknologi yang digunakan, jenis kejahatan atau kerugian yang dilakukan dan tujuan dari tindakan cyber crime tersebut dilakukan. Dari berbagai banyak jenis kejahatan siber yang bisa terjadi hacking menjadi salah satu yang berbahaya.

Hacking atau peretasan merupakan kegiatan menerobos masuk secara ilegal ke program-program komputer milik pihak lain (Babys, 2021: 430). Dalam melakukan peretasan pada *device* atau komputer tentu saja memiliki konsekuensi yang cukup berbahaya. Beberapa hal yang dapat diretas berkaitan dengan informasi, harta seperti uang, dan berbagai kemungkinan informasi lain. Dalam konteks pertahanan negara peretasan sangat berpotensi terjadinya peretasan informasi yang bersifat kenegaraan yang dapat disalahgunakan oleh oknum yang tidak bertanggung jawab dan dapat merugikan negara. Dalam usaha peretasan ini tentu saja pihak peretas menggunakan apa yang disebut dengan *hacking tools* atau alat berupa sistem dalam komputer yang dapat meretas data dari komputer satu ke komputer lainnya.

Dalam perkembangannya, *cybercrime* sendiri mengalami evolusi mengikuti perkembangan penemuan sarana dan prasarana baru yang semakin canggih. Dari gambar 1 dapat dilihat perkembangan "*attack sophistication vs intruder technical knowledge"* dari mulai tahap awal pada tahun 1980an yang hanya *password guessing*, sampai perkembangan *cybercrime* dengan menggunakan tools saat ini. Berikut adalah gambar perkembangan *cybercrime* dari tahun ke-tahun:

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

Gambar 1. Attack Spohistication vs. Intruder Technical Knowledge



Source: Rabah (2018)

Karena perkembangan dari *cybercrimes* yang cukup pesat, hal ini selaras dengan teknologi yang juga berkembang pesat. Hal ini dapat dilihat dari perkembangan baik secara *hardware* maupun *software.* Perkembangan yang cukup perlihat adalah peralihan dari teknologi informasi yang dulu identik hanya dilakukan pada komputer saat ini ponsel juga memiliki kemampuan untuk bisa tersambung dengan jaringan internet. Penggunaan ponsel pintar atau *smartphone* saat inipun sudah semakin masif di dunia, pada juli 2021 terdapat 5,3 miliar orang menggunakan *smartphone* atau setara dengan 67 persen dari seluruh populasi penduduk dunia (Kompas, 2021). Namun hal ini tentu saja juga menjadi salah satu jenis potensi *cybercrimes* lain yang salah satunya adalah dengan menggunakan peralatan *tools* yang cukup berbahaya. Salah satu *tools* dalam kejahatan siber yang mengincar pengguna ponsel saat ini adalah *spyware predator.*

Predator sendiri merupakan salah satu jenis *spyware* dan juga dapat dikategorikan sebagai *hacking tools*. Dalam hal ini tentu saja predator dapat menjadi salah satu ancaman siber yang berbahaya. Baik secara data individual ataupun bahkan dapat menjadi ancaman yang cukup serius dalam hal politik. Ancaman utamanya adalah terletak pada informasi-informasi strategis kenegaraan yang dapat saja direkam dan disalah gunakan oleh pihak-pihak yang dapat membahayakan kondisi pertahanan negara. Pihak-pihak ini bisa saja pihak dari dalam negara sendiri maupun bahkan pihak luar.

Karena potensi yang sangat membahayakan inilah maka sangat diperlukan literatur yang mempelajari terkait hal ini. Literatur yang membahas mengenai kasus predator atau cyber threat/cybercrime secara general sangat lah jarang, apalagi literatur yang berkorelasi secara spesifik dengan konsep pertahanan negara. Oleh karenanya artikel ini bertujuan untuk melakukan kajian literatur yang dapat dikumpulkan dari berbagai sumber mengenai hacking tools terutama kasus predator serta *cyber threat/cybercrime* dan korelasinya dengan pertahanan negara.

1.2 Rumusan Masalah

Bagaimana serangan *hacking tools predator* dapat mengancam keamanan siber dan pertahanan negara?

2. Kajian Pustaka

2.1 Ancaman Siber (*Cyber Threat*)

Ancaman siber sendiri merupakan potensi kejahatan siber yang dapat terjadi. Ancaman siber sendiri secara garis besar tentu saja segala sesuatu ancaman kejahatan yang dapat dilakukan yang berhubungan dengan suatu teknologi informasi seperti komputer baik dalam perangkat keras ataupun perangkat ringannya. Ancaman siber sendiri memiliki tiga jenis menurut Mcdonnel dan Sayers dalam (Rahmawati, 2017: 55) diantaranya adalah:

a. Ancaman perangkat keras atau *hardware threat,* adalah ancaman

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

penyebab utamanya adalah instalasi suatu perangkat tertentu pada hardware yang bertujuan untuk melakukan kegiatan tertentu di dalam sistem komputer, hasil akhir dari pemasangan perangkat tersebut adalah dapat terjadi gangguan pada jaringan *software* dan *hardware* pada suatu komputer.

b. Ancaman perangkat lunak atau *software threat,* adalah suatu ancaman pada sebuah komputer yang penyebabnya adalah dikarenakan adanya *software tertentu* yang masuk dan bertujuan untuk melakukan hal-hal ilegal seperti mencuri, merusak dan memanipulasi informasi ada dalam komputer itu.
c. Ancaman pada data/informasi atau *data information threat*, merupakan salah satu jenis ancaman yang penyebabnya adalah karena adanya penyebaran beberapa data atau informasi untuk suatu tujuan tertentu.

2.2 Kejahatan Cyber (*Cyber Crime)*

Cyber Crime merupakan suatu jenis kejahatan dengan level transnasional yang sangat berbahaya karena dapat memicu terjadinya sebuah perang siber atau C*yber Warfare*. *Cybercrime* memiliki beberapa jenis atau macam-macam di dalamnya, menurut (Subagyo, 2018: 98-99) *cybercrime* terdiri atas enam jenis, diantaranya adalah sebagai berikut:

1. *Hacking* adalah suatu jenis kejahatan siber dimana terjadi penerobosan pada suatu program komputer yang dilakukan oleh pihak lain. Seseorang yang melakukan kegiatan hacking ini disebut dengan hacker. Hacker sendiri tentu saja orang dengan keahlian komputer tertentu yang membuat ia dapat melakukan peretasan terhadap komputer lain dan dapat mengakses informasi di dalam komputer lain tersebut.
2. *Cracking* adalah salah satu jenis dari hacking namun dengan tujuan yang buruk. Sedikit berbeda dengan hacking, pada cracking tujuan utamanya adalah pada hasil dari tindakan peretasan komputer. Jika hacker biasanya cukup puas pada level menerobos keamanan komputer, *cracker* atau sebutan untuk orang yang melakukan cracking melakukan ini untuk menikmati hasil dari peretasan tersebut dan biasanya hasil ini secara finansial seperti melakukan hacking pada kartu kredit dan kemudian melakukan pengambilan dan pencurian uang yang ada di dalamnya.
3. *Cyber Sabotage* merupakan jenis *cybercrime* dengan cara melakukan sabotase atau gangguan termasuk merusak dan juga menghancurkan baik data-data, sistem jaringan maupun program dalam suatu komputer yang mengakses internet.
4. *Cyber Attack* adalah jenis kejahatan siber yang menyerang dan mengganggu informasi yang ada dalam suatu komputer dengan sengaja. Tindakan ini biasanya memiliki tujuan untuk mengganggu baik secara fisik bahkan sistem dan perangkat lunak yang ada dalam suatu komputer.
5. *Carding* adalah kejahatan siber yang kegiatannya adalah dengan melakukan pembelian barang namun dengan menggunakan identitas dari orang lain. Data-data ini biasanya didapatkan dengan cara mencuri data identitas seseorang dari internet. Kejahatan ini biasa

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

disebut dengan *cyber fraud* atau penipuan pada dunia maya.

6. *Spyware* adalah program perangkat lunak yang menjadi alat bagi oknum untuk dapat mengakses kegiatan siber di komputer orang lain. *Spyware* dapat melakukan perekaman pada aktivitas siber dari user komputer tersebut seperti *cookies* dan juga *registry.* Kemudian informasi yang telah direkam dan diapatkan ini dapat diperjualbelikan kepada pihak ketiga seperti perusahaan yang dapat digunakan untuk tujuan tertentu seperti penyebaran virus atau mendapatkan informasi tertentu.

3. Metode Penelitian

Tulisan ini menggunakan metode penelitian kualitatif deskriptif dimana penelitian ini berusaha mendeskripsikan konsep dan pertanyaan utama pada tulisan ini. Penelitian kualitatif pada penelitian ini bersifat eksploratif dimana peneliti ingin memperdalam dan juga mengeksplorasi terkait topik penelitian yakni ancaman siber *hacking tools predator* dalam konteks pertahanan negara. Dalam artikel ini teknik pengumpulan data dilakukan dengan menggunakan studi-pustaka (studi literatur). Menurut (Kurniawan, 2013) penelitian kepustakaan dilakukan karena data-data yang diperlukan untuk tujuan penelitian adalah berasal dari sumber kepustakaan seperti buku, ensiklopedia, kamus, dokumen, jurnal, majalah dan lain sebagainya. Sementara menurut (Zed, 2008) Studi literatur merupakan kegiatan mengumpulkan data pustaka, membaca, mencatat, dan mengolah bahan penelitian untuk nantinya dapat dikaji ulang. Studi literatur memanfaatkan sumber perpustakaan untuk memperoleh data pada riset pustaka atau *library research.* Penelusuran pustaka tidak hanya terletak pada langkah awal penelitian atau kerangka penelitian semata, namun penelusuran kepustakaan juga memanfaatkan berapa sumber kepustakaan yang digunakan sebagai data dalam penelitian. Data yang ada pada artikel ini diambil dari buku, jurnal ilmiah, artikel berita serta dokumen terkait mengenai topik penelitian yaitu serangan hacking tools dan ancaman siber dalam sistem pertahanan negara studi kasus predator. Penggunaan studi kepustakaan bertujuan untuk mengeksplorasi informasi yang ada mengenai ancaman predator di Indonesia, mengingat studi terkait topik ini masih sangat jarang ditemukan. Oleh karenanya penelitian ini bermaksud mengetahui sejauh mana informasi yang dapat dikumpulkan mengenai topik ini di Indonesia.

4. Hasil dan Pembahasan

4.1 Metode Penyerangan Siber

Dalam melakukan aksinya, kejahatan siber dapat dibagi menjadi beberapa kategori berdasarkan metode penyerangan yang dilakukan. Menurut (Subagyo, 2015: 99-100) berikut ini adalah beberapa jenis metode penyerangan yang biasa dilakukan oleh para oknum yang melakukan kejahatan siber:

1. *Spionase cyber* adalah sebuat bentuk kejahatan siber yang secara topik paling erat kaitannya dengan dunia politik dan juga negara. Pada kejahatan siber ini biasa dilakukan dengan cara mengumpulkan

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

informasi rahasia ataupun sensitif milik individu, rival, ataupun kelompok musuh. Selain pada bidang politik *spionase cyber* ini juga sering terjadi pada bidang ekonomi maupun militer. Cara melakukan kegiatan spionase siber ini adalah biasanya dengan melakukan eksploitasi atau pengambilan informasi secara ilegal melalui jaringan internet atau *software* komputer dari negara lain. Informasi-informasi penting yang tidak ditangani dengan keamanan yang memadai dapat menjadi sasaran empuk untuk dicegat atau bahkan diubah informasinya.

2. *Vandalisme* adalah sebuah tindakan perusakan. Perusakan yang dimaksud adalah dengan merusak halaman atau web milik pihak orang lain yang tersambung dengan internet. Serangan atau perusakan yang sering terjadi adalah dalam bentuk propaganda tertentu. Selain itu vandalisme juga sering juga dilakukan melalui internet seperti email maupun pesan teks yang berisi dengan teks-teks propaganda tertentu.
3. Sabotase adalah kegiatan penyadapan akan suatu informasi atau dapat juga berupa gangguan pada peralatan untuk komunikasi. Alat yang digunakan untuk melakukan kegiatan sabotase ini biasanya adalah semacam *software* atau perangkat lunak khusus yang secara sengaja disembunyikan pada *hardware* komputer pihak lain yang menjadi incaran untuk dilakukan sabotase. Sabotase sendiri merupakan kegiatan sering dilakukan dalam dunia militer terutama berkaitan dengan komputer dan satelit untuk mengetahui koordinat yang menjadi lokasi penempatan peralatan pihak musuh.
4. Serangan Pada Jaringan Listrik merupakan metode penyerangan kejahatan siber yang terakhir, pada penyerangan ini biasanya dilakukan dengan melakukan pemadaman pada jaringan listrik. Hal ini dilakukan dengan tujuan untuk mengganggu atau mengalihkan perhatian. Serangan pada jaringan listrik ini biasa dilakukan dengan program sejenis *trojan horse* untuk mengendalikan infrastruktur listrik.

4.2 Modus Operandi Dalam Penggunaan *Hacking Tools*

Dalam melakukan aksi peretasan seorang hacker memiliki beberapa modus operandi tertentu atau jenis-jenis berdasarkan cara melakukan hacking pada komputer target. Berikut ini adalah beberapa modus operandi yang biasanya digunakan oleh para hacker menurut (Aslam, 2011: 35-36):

a. *Physically Hacking*

Physically Hacking atau peretasan secara fisik adalah metode peretasan yang menggunakan perangkat keras *(hardware)*. Metode peretasan ini memang sangat jarang dilakukan dan kurang familiar di kalangan masyarakat karena jarang terpublikasi secara umum melalui media massa. Metode peretasan ini bertujuan untuk pencarian sebuah informasi tertentu dengan memasukkan perangkat keras ke dalam unit yang digunakan yang ingin dijadikan sebagai korban. Selain itu kegiatan *physically hacking* ini juga biasa dilakukan oleh vendor tertentu yang ingin mengetahui sejumlah informasi yang dimiliki oleh pengguna perangkat yang mereka gunakan seperti lisensi produk, software yang digunakan oleh konsumennya.

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

b. *Logically Hacking*

Metode *logically hacking* menjadi salah satu metode yang paling sering digunakan dan digemari para hacker. Dikatakan sebagai *logically hacking* karena alat yang digunakan untuk meretas bersifat abstrak dan sebagian besar efek yang ditimbulkan memiliki sifat yang sama walaupun dapat berimbas ke dalam dunia nyata. Dalam melakukan serangan *logically hacking* seorang hacker biasanya melakukannya dalam beberapa tahapan (Aslam, 2011: 37-38). Tahapan penyerangan dengan metode ini terdiri dari lima tahap yakni sebagai berikut:

1. *Reconnaissance Reconnaissance* adalah tahap pengumpulan data, dalam tahap ini para hacker melakukan pengumpulan seluruh data yang dilakukan dengan sebanyak– banyaknya hingga mengenai target. Data yang dikumpulkan dapat berupa data – data personal atau pribadi atau dapat juga dikatakan sebagai data yang berguna untuk melakukan serangan.
2. *Scanning Scanning* atau titik awal dimulainya sebuah aktivias serangan hacker (pre-attack). Proses ini dijadikan sebagai salah satu media atau strategi untuk hacker dalam mencari berbagai kemungkinan yang dapat digunakan untuk mengambil alih komputer korban.
3. *Gaining access* Hasil dari proses pencarian informasi yang ditemukan dalam kedua proses sebelumnya mulai digunakan dalam tahapan ini. Tahapan inilah yang merupakan suatu peristiwa yang dikategorikan sebagai *cybercrime.* Hal ini dikarenakan dalam tahapan inilah penerobosan *(penetration)* terhadap kelemahan – kelemahan yang dimiliki oleh target.Yang patut diketahui bahwa dalam tahapan ini tidaklah perlu menggunakan teknologi yang canggih, seorang hacker bisa saja menggunakan metode social engineering yang memanfaatkan staf IT.
4. *Maintaining Access* Setelah mendapatkan akses penuh pada komputer target dalam tahap penerobosan, seorang hacker biasanya ingin mendapatkan kekuasaan penuh yang bersifat tetap. Dalam hal ini maintaining access sangat diperlukan. Para hacker biasanya melakukan penanaman berbagai aksesoris tambahan seperti backdoor, rootkit, Trojan untuk mempertahankan kekuasaannya terhadap jaringan target.
5. *Covering Tracks* Untuk melindungi diri hacker dari tuntutan pidana maka hacker harus menutupi jejak dalam sebuah penerobosan. Biasanya para hacker melakukan penghapusan *log file* ataukah melakukan pembuatan file atau directory yang diletakan secara tersembunyi di komputer korban.

4.3 Ancaman *Hacking Tools Predator*

Hacking tools predator sendiri merupakan salah satu jenis *spyware* yang merupakan sebuah jenis *software* yang dapat ditanamkan pada sistem *smartphone* yang fungsinya adalah untuk merekam serta menyimpan data-data dari aktivitas siber di ponsel tersebut. *Spyware predator* sendiri menurut laporan dari citizenlab adalah *software* yang diciptakan oleh perusahaan bernama *Cytrox* yang berbasis di israel (Citizenlab, 2021). Cytrox adalah perusahaan asal Makedonia Utara yang

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

diduga oleh Meta menjadi salah satu perusahaan spyware yang terkenal dan menyediakan jasa spyware seperti pegasus dan juga predator (hitechglitz, 2021). Terdapat beberapa perusahaan yang *concern* dan menjadi jasa sebagai tentara bayaran *cyber* yakni *Cobwebs Technologies, Cognyte, Black Cube,* dan *Bluehawk* CI yang berlokasi atau berbasis di Negara Israel. Tidak hanya itu, salah satu perusahaan di India termasuk dalam daftar perusahaan tentara *cyber,* perusahaan ini dikenal sebagai BellTroX, Cytrox salah satu individu yang berasal dari daerah Makedonia Utara, serta entitas "*unknown"* atau tidak dikenali beroperasi di luar Negara Tiongkok diyakini melakukan sebuah kampanye dalam hal pengawasan yang fokusnya terkhusus untuk para minoritas di daerah kawasan Asia-Pasifik (Prasetyo, 2022). Kasus predator oleh cytrox ini pada tahun 2021 cukup menjadi bahan perbincangan karena ilmuwan dari *citizenlab* menemukan bahwa ternyata terdapat dua politik asal mesir yang ternyata terdapat *spyware predator* pada ponsel *iphone* mereka (Citizenlab, 2021).

Namun ternyata *spyware predator* juga menyebar luas sampai ke pengguna Indonesia. Menurut berita yang dihimpun dari urbanjar.com. Terdapat banyak pengguna komputer dan ponsel yang dimata-matai dengan *spyware predator* termasuk pengguna dari Indonesia. Pengguna media sosial instagram dan facebook telah terdeteksi sebanyak 50 ribu pengguna. Tujuan dari oknum pemasangan *spyware* ini adalah untuk pengembangan dan pengeksploitasian sebuah data maupun informasi yang belum pernah dilihat, yang dilakukan dengan peretasan serta pencurian sebuah konten yang berada pada ponsel yang dimiliki oleh korban seperti log panggilan, perpesanan (teks pesan dan email), lokasi yang dilakukan dengan rahasia atau tersembunyi (Urbanjar, 2021). Laporan *Citizen Lab* menjelaskan bahwa banyak layanan Apple dapat diakses melalui Predator, termasuk browser Safari miliknya sendiri, App Store, Maps, dan bahkan layanan yang lebih sensitif seperti Kamera dan Mail. Lebih buruk lagi, beberapa kotak surat terenkripsi ujung-ke-ujung seperti Signal dan Telegram juga terpengaruh, sebuah tanda bahwa bahkan alternatif semacam itu tidak pernah 100% aman (Urbanbanjar, 2021).

4.4 Potensi Kerugian Ancaman *Hacking Tools Predator*

Meskipun belum ada data yang mengidentifikasi jumlah yang jelas berapa banyak masyarakat yang tengah dimata-matai oleh spyware predator namun hal ini tetap membahayakan. Belum ada informasi yang jelas pula mengenai identitas dari siapa saja yang teridentifikasi *spyware predator* di *smartphone* mereka. Namun potensi terburuk yang kemungkinan dapat terjadi adalah para individu yang teridentifikasi spyware predator di komputer atau ponsel mereka adalah para pejabat negara atau orang-orang dengan informasi strategis negara. Hal ini tentu saja sangat membahayakan mengingat kemampuan spyware yang dapat merekam informasi dari aktivitas siber yang dilakukan oleh komputer yang tengah dimata-matai

Informasi ini tentu saja dapat saja diperjualbelikan kepada pihak ketiga yang memiliki niat buruk dan mengancam kondisi keamanan negara. Potensi inilah yang kemudian haruslah menjadi perhatian khusus bagi pemerintah untuk bisa memperkuat pertahanan dari sektor siber. Melihat bagaimana performa *spyware predator* pada kasus politikus di mesir, hal ini tentu harus ada perhatian khusus dari Indonesia terhadap *hacking tools spyware predator* ini.

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

Hacking tools spyware predator dalam prakteknya melakukan penyitasan pada level mikro atau level individu. Oleh sebab itu kerugian pertama tentu saja ada pada level individu, namun jika hal ini dibiarkan bukan hal mustahil bahwa level dari peretasan ini bisa semakin membesar secara kuantitas, dan informasi-informasi yang diambil tanpa izin dari para pemilik smartphone ini dapat digunakan untuk tujuan-tujuan tertentu dan dapat merugikan publik secara luas. Selain itu dari sudut pandang pertahanan negara, informasi merupakan salah satu hal yang sangat krusial terutama yang berkaitan dengan informasi strategis dalam hal politik antar negara.

Meninjau bagaimana potensi bahaya dari *spyware predator* ini sayangnya di Indonesia sendiri masih belum ada kajian atau literatur yang menyoroti kasus ini. Hal ini akan menjadi semakin berbahaya mengingat untuk mempersiapkan diri dibutuhkan sumber-sumber yang credible dan cukup sebagai awalan untuk mempelajari isu ini sebelum memunculkan ide strategi pencegahan. Oleh karenanya dibutuhkan sinergi dari para peneliti dan juga para pemangku kepentingan dalam sektor pertahanan untuk bisa melakukan kajian mengenai hal ini.

5. Kesimpulan

Ancaman siber saat ini merupakan salah satu ancaman serius yang skalanya dapat menyebar dari level individu sampai negara. Metode penyerangan siber memiliki beberapa jenis, seperti spionase *cyber*, vandalisme, sabotase, dan serangan pada jaringan listrik. Terdapat dua jenis modus operandi yang digunakan para *hacker* untuk melakukan kejahatan siber yaitu *phisically hacking*, dan *logically hacking*. *Logicaly hacking* merupakan modus yang paling sering digunakan oleh para *hacker* dimana modus ini terdiri dari *reconnaissance*, *scanning*, *gaining access*, *maintaining access*, serta *covering tracks*.

Salah satu ancaman *hacking tools* yang saat ini mulai muncul adalah predator yang merupakan bagian dari *spyware* milik Israel. Predator biasanya ditanamkan pada *smartphone* dengan tujuan untuk merekam segala aktivitas yang ada dalam *smartphone* tersebut. Ancaman *spyware predator* mulai terkuak semenjak ditemukannya *software* ini di ponsel dua politikus asal Mesir. Sampai saat ini, ancaman *spyware predator* juga telah memasuki Indonesia.

Banyaknya potensi buruk dari adanya *spyware predator* ini harus menjadi perhatian khusus bagi pemerintah Indonesia. Mengingat kejadian yang menimpa dua politikus Mesir, tidak menutup kemungkinan bahwa pejabat-pejabat di Indonesia juga menjadi target dari pemasangan *spyware predator* ini. Potensi buruk yang bisa saja terjadi apabila terdapat *spyware predator* di ponsel pejabat Indonesia adalah diperjuakbelikannya data-data yang telah diambil oleh *hacker* kepada pihak ketiga, dimana hal ini tentu menimbulkan ketidakamanan nasional.

Daftar Pustaka

Acuan artikel dalam buku:

Zed, M. 2008. *Metode Penelitian* Kepustakaan Jakarta: Yayasan Pustaka Obor Indonesia

Acuan artikel dalam Jurnal:

Babys, S. A. 2021. "Ancaman Perang Siber di Era Digital dan Solusi Keamanan Nasional Indonesia" dalam Oratio Directa, Vol. 3 No. 1, pp 425-442

Putra, R. D., Supartono, S., & Deni, D. A. R. 2018. "Ancaman Siber Dalam Perspektif Pertahanan Negara

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

(Studi Kasus Sistem Pertahanan Semesta)" dalam Jurnal Peperangan Asimetris, Vol 4 No. 2, pp 99–120

Rabah, K. 2016. "Industry 4.0 and Cybersecurity: Where is the Universities?" dalam Mara International Journal of Scientific & Research Publications Vol. 2 No. 2 pp 15-33

Rahmawati, I. 2017. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense". Dalam Jurnal Pertahanan & Bela Negara, Vol. *7* No. 2 pp 51-66. DOI: http://dx.doi.org/10.33172/jpbh.v7i2.179

Subagyo, A. 2018. "Sinergi Dalam Menghadapi Ancaman Cyber Warfare." dalam Jurnal Pertahanan & Bela Negara Vol. *5* No. 1, pp 89-108. DOI: http://dx.doi.org/10.33172/jpbh.v5i1.350

Sutomo, A., Octavian, A., Widodo, P., & Reksoprodjo, Y. 2022. "Integration Strategy of Cyber Defense with National Cyber Security to Maintain State Sovereignty" dalam Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences, Vol 5 No. 1, pp 1260-1271. DOI:https://doi.org/10.33258/birci.v5i1.3727)

Acuan artikel dari website:

Anjani, 2021. "Perlindungan Keamanan Siber di Indonesia" dalam https://repository.cips-indonesia.org/uk/publications/341780/perlindungan-keamanan-siber-di-indonesia diakses 23 Februari 2022

Citizenlab. 2021. "Pegasus vs Predator Dissident Doubly Infected Iphone Reveals Cytrox Mercenary Spyware" dalam https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/ diakses 22 Februari 2022

Hitechglitz. 2021. "Pegasus Tidak Perlu Dikhawatirkan Kenali Predator Spyware Cytrox" dalam https://hitechglitz.com/indonesia/pegasus-tidak-perlu-dikhawatirkan-kenali-predator-spyware-cytrox/ diakses 23 Februari 2022

Kominfo. 2021. "Warganet Meningkat Indonesia Perlu Tingkatkan Nilai Budaya di Internet" dalam https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/ diakses 21 Februari 2022

Kurniawan, A. 2013." Metode Penelitian Pendidikan dan Pengajaran Matematika" dalam https://www.slideshare.net/mobile/saddamsvc/studi-kepustakaan-19891180 diakses 20 Februari 2022

Liputan6.com. 2021. "Indonesia Diberondong 13 Miliar Serangan Siber Sepanjang 2021" dalam https://www.liputan6.com/bisnis/read/4706493/indonesia-diberondong-13-miliar-serangan-siber-sepanjang-2021#:~:text=Indonesia%20Diberondong%201%2C3%20Miliar%20Serangan%20Siber%20Sepanjang%202021,-Liputan6.com&text=Liputan6.com%2C%20Jakarta%20%2D%20J

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

umlah,2021%20mencapai%201%2C3%20miliar. diakses 23 Februari 2022

Prasetyo. 2022. "Facebook Banned 7 Perusahaan 'Cyber Mercenary' karena Memata-matai 50.000 Pengguna" dalam https://idnsa.id/article/facebook-banned-7-perusahaan-cyber-mercenary-karena-memata-matai-50000-pengguna diakses 22 Februari 2022

Suara.com. 2021. "Kominfo: Ada 88 Jut Ancaman Siber Di Indonesia Sepanjang 2021" dalam https://www.suara.com/tekno/2021/10/13/140110/kominfo-ada-888-juta-ancaman-siber-di-indonesia-sepanjang-2021 diakses 23 Februari 2022

Teknokompas. 2021. "Jumlah Pengguna Ponsel di Dunia Tembus 5 Miliar" dalam https://tekno.kompas.com/read/2021/09/02/09144137/jumlah-pengguna-ponsel-di-dunia-tembus-5-miliar diakses 25 Februari 2022

Urbanbanjar. 2021. "Akun Mata-mata di FB dan Ig di Blokir Meta" dalam https://www.urbanjabar.com/featured/pr-922237482/akun-mata-mata-di-fb-dan-ig-diblokir-meta diakses 21 Februari 2022

Acuan dari tugas akhir, laporan penelitian, skripsi, tesis dan desertasi :

Aslam, M. A. A. 2011. "Modus Operandi dan Penanggulangan Kejahatan Cyber Crime yang Dilakukan oleh Hacker Tinjauan Hukum Kejahatan Internasional". Skripsi Hukum Internasional. Fakultas Hukum Universitas Hasanudin.