FORENSIK KOMPUTER HUMAN INTERFACE DEVICE BADUSB BERBASIS MICROCONTROLLER ATMEGA32U4 ARDUINO LEONARDO PADA REGISTRY SISTEM OPERASI MICROSOFT WINDOWS 7

Nugroho Budhisantosa
Fakultas Ilmu Komputer, Universitas Esa Unggul, Jakarta
Jalan Arjuna Utara No 9 Kebon Jeruk Jakarta 11510
nugroho.budhisantosa@esaunggul.ac.id

Abstract

One attack mode on information security is to use a BadUSB device that is connected to the target computer, using this technique various information such as memory dump activities to get the password and embed the reverse shell can be done in a matter of seconds on Microsoft Windows 7 operating system. This paper is an introduction to how computer forensic investigations can be carried out on computers to bring cyber criminals to court. Although the computer forensic technique discussed in this paper looks simple, but in fact this activity requires the precision and patience of the investigator.

***Keywords** : Human Interface Device, BadUSB, ATMEGA32U4, and Registry.*

Abstrak

Salah satu modus serangan pada keamaman informasi adalah dengan menggunakan perangkat BadUSB yang dihubungkan dengan komputer target, menggunakan teknik ini bermacam informasi seperti aktivitas memory dump untuk mendapatkan password dan menanamkan reverse shell dapat dilakukan dalam waktu hitungan detik saja pada sistem operasi Microsoft Windows 7. Tulisan ini merupakan pengantar tentang bagaimana investigasi forensik komputer dapat dilakukan pada komputer untuk membawa pelaku kejahatan siber ke meja hijau. Meskipun teknik forensik komputer yang dibahas di dalam tulisan ini terlihat sederhana tetapi sesungguhnya aktivitas ini memerlukan ketelitian dan kesabaran dari investigator.

Kata kunci : *Human Interface Device, BadUSB, ATMEGA32U4,* dan *Registry*.

Pendahuluan

Pesatnya kemajuan teknologi juga diikuti oleh pesatnya jumlah jenis perangkat teknologi informasi yang dirancang untuk mempermudah kehidupan manusia. Namun seperti halnya pisau bermata dua, perangkat teknologi informasi yang sama ternyata juga dimanfaatkan oleh sebagian orang dalam kelompok hacker untuk mempermudah mereka dalam melakukan tindakan melawan hukum. Perangkat dengan mikro kontroler Arduino misalnya, perangkat ini sejatinya dikembangkan untuk memudahkan pemanfaatan peralatan elektronik dalam berbagai bidang pada mesin-mesin penggerak, namun ditangan mereka, perangkat keras berplatform hardware terbuka ini ternyata mereka manfaatkan dengan merekayasanya sebagai perangkat antarmuka manusia atau *Human Interface Defice* (HID) untuk keperluan menginjeksikan perintah-perintah jahat pada komputer.

BadUSB adalah perangkat USB yang dimanipulasi oleh hackers agar lebih dikenali oleh komputer target bukan dalam wujud aselinya sebagai *USB Flash Disk* melainkan dengan sedikit teknik rekayasa sederhana, perangkat ini kemudian akan dikenali sebagai perangkat antar muka seperti halnya keyboard komputer. Teknik rekayasa ini dilakukan dengan cara manupulasi protokol HID yang digunakan. Melalui keyboard palsu inilah *script* jahat atau *payload* yang tersimpan di dalam memori USB diinjeksikan ke dalam sistem komputer selayaknya pengguna komputer mengetikkan perintah-perintah menggunakan *keyboard* komputer. Penggunaan teknik reverse shell juga merupakan hal yang umum di dalam penggunaan BadUSB, menggunakan teknik ini, script akan memerintahkan komputer untuk membuat koneksi ke komputer hacker. Dengan metode ini hacker tidak lagi akan direpotkan dengan sistem keamanan firewall yang dibuat untuk memblok paket-paket dari luar.

Bentuk baru dari ancaman serangan siber terhadap keamanan informasi ini bukanlah bentuk serangan yang sempurna yang tidak dapat ditemukan bukti kejahatannya di persidangan pelaku kejahatan komputer karena sistem operasi modern seperti sistem operasi Microsoft Windows 7 secara *default* akan mencatat semua perangkat HID yang dihubungkan ke dalam database sistem registernya. Dari titik inilah aktivitas forensik komputer dapat dilakukan. Rumusan masalah yang akan dibahas pada tulisan ini adalah:

1. Bagaimanakah teknik indikasi awal digunakan untuk mengetahui bahwa BadUSB telah digunakan dalam melakukan penyerangan pada suatu komputer
2. Apakah identitas Mikrochip ATMEGA32U4 secara khusus akan tercatat di dalam register sistem operasi Microsoft Windows 7.
3. Bagaimana teknik mendapatkan penanda waktu pada barang bukti digital pada modus serangan BadUSB berbasis mikrochip ATMEGA32U4

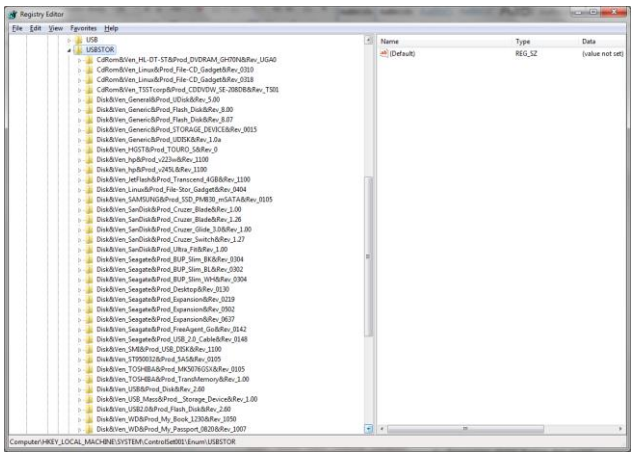
Tulisan ini hanya akan membahas analisa forensik komputer pada *Root key* HKLM\SYSTEM\ControlSet001\ENUM\USBSTOR dari register sistem operasi Micrtosoft Windows 7 dan penanda waktu dari barang bukti register yang didapatkan. Mempelajari cara kerja dari register sistem operasi Microsoft Windows terhadap serangan BadUSB berbasis chip ATMEGA32U4. Memberikan referensi pada pihak-pihak yang tertarik untuk mendalami investigasi forensik komputer

Tinjauan Teori

Forensik Komputer adalah kata serapan dari bahasa Inggris yaitu *Computer Forensics* dimana kata *Forensics* sendiri berasal dari kata *Forensis* yang di dalam Bahasa latin berarti *belonging to the forum* yang di dalam istilah hukum dapat diartikan sebagai *pertaining to the courts* yang berarti membawa ke pengadilan. Secara terminologi istilah Forensik Komputer sendiri lebih diartikan sebagai membawa barang bukti digital ke pengadilan guna keperluan peneggakan hukum, bukan sekedar membawa komputer secara fisik ke persidangan.

Sistem register atau *registry* dari sistem operasi Microsoft Windows adalah suatu basis data yang disusun secara hierarkis yang mengandung informasi mengenai konfigurasi sebuah sistem, mulai dari konfigurasi perangkat keras, perangkat lunak, asosiasi ekstensi berkas dengan aplikasinya hingga preferensi pengguna.

Pada sistem operasi Microsoft Windows 7, sistem register akan mencatat semua perangkat USB yang terhubung pada sistemnya di dalam *Root keys* :
HKLM\SYSTEM\ControlSet001\ENUM\USBSTOR



Gambar 1
Isi Root keys

Dengan memperhatikan sistem pencatatan dari register sistem operasi Microsoft Windows 7 inilah maka *Root keys* di atas adalah lokasi tempat mendapatkan barang bukti serangan *BadUSB* berbasis chip ATMEGA32U4. Barang bukti digital adalah informasi jejak elektronik yang tersimpan di dalam media penyimpanan perangkat elektronik di dalam bentuk berkas-berkas digital yang digunakan untuk keperluan melakukan suatu kejahatan siber serta barang-barang yang didapatkan dari sebuah tindak kejahatan. Secara fisik, barang bukti digital tersimpan di dalam media penyimpanan dalam bit-bit informasi yang tidak terlihat oleh mata telanjang sehingga diperlukan proses pengolahan secara khusus mengikuti prosedur ketat yang ada agar dapat menjadi informasi yang terlihat oleh mata.

Barang bukti digital dianggap sah dan dapat diajukan ke persidangan jika informasi yang tercantum di dalamnya dapat diakses, dijamin keutuhannya, dan dapat dipertanggungjawabkan. Untuk keperluan ini diperlukan prosedur forensik komputer berupa pengumpulan, akuisisi, pemulihan, penyimpanan/pemeliharaan, dan pemeriksaan barang bukti digital dengan cara yang dapat dipertanggung jawabkan.

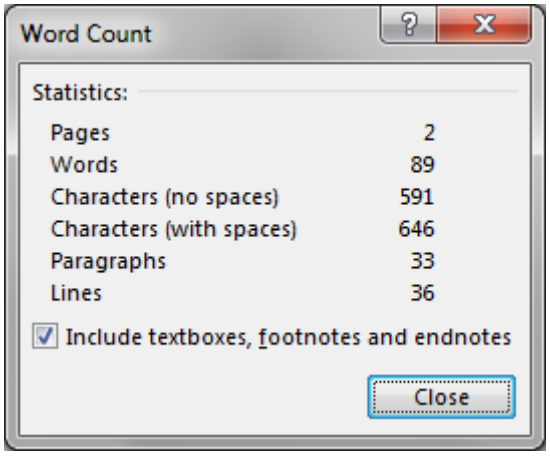
Timestamp atau penanda waktu adalah salah satu bagian yang tidak terpisahkan di dalam investigasi barang bukti digital. Sedemikian pentingnya peran penanda waktu ini sehingga pada prosedur pemeliharaan barang bukti digital, perlu juga diperhatikan agar tidak terjadi perubahan pada penanda waktu ini. Penanda waktu di dalam sistem berkas komputer adalah waktu saat suatu even dicatat oleh komputer. Di dalam investigasi forensik komputer, penanda waktu digunakan untuk mengetahui waktu dari barang bukti berkas digital dibuat, dimodifikasi, dan terakhir kalinya mengalami pengaksesan. Penanda waktu ini harus dipelihara keasliannya dengan hati-hati dan dicatat di dalam riwayat barang bukti atau *chain of custody*.

Human Interface Device (HID) dalam ujud aslinya adalah adalah perangkat yang digunakan oleh manusia untuk berinteraksi dengan komputer dimana pengguna komputer dan komputer menggunakan perangkat ini untuk berkomunikasi melalui serangkaian *input* dan *output* dari manusia ke komputer dan sebaliknya. Melalui protokol yang digunakan, sistem operasi modern seperti Microsoft Windows, Linux, MacOS jika dahulu memerlukan *propertiary* driver untuk mengenali perangkat keras yang dihubungkan, sekarang secara cerdas dapat langsung mengenali keberadaan perangkat keras yang terhubung melalui port USB, seperti keyboard dan mouse tanpa memerlukan driver khusus. Protokol HID membuat implementasi penggunaan perangkat input-output komputer menjadi sangat sederhana. Protokol menentukan cara pertukaran data dan kemudian menyajikan "*deskriptor* HID" ke host.

Arduino Leonardo adalah mikrokontroler berbasis *Microchip* ATMEGA32U4 yang merupakan chip RISC 8-bit *self-programming flash program memory* yang memiliki memori penyimpanan SRAM berukuran 2.5KB.

Gambar 2
Microchip ATMEGA32U4

Microchip ATMEGA32U4 menjadi salah satu chip pilihan pelaku kejahatan siber untuk melakukan aksinya karena chip ini menggunakan 8-bit ASCII code untuk berkomunikasi, sama halnya dengan cara berkomunikasi keyboard komputer, pada umumnya dan memiliki memori penyimpanan sebesar 2.5KB. *Microchip* ATMEGA32U4 memiliki ukuran memori hanya sebesar 2.5KB. Ukuran ini memang sepintas terlihat sangat kecil jika dibandingkan dengan memori penyimpanan berkas yang saat ini yang telah berukuran Giga Byte, namun bagi para pelaku kejahatan siber ukuran memori penyimpanan sebesar 2.5KB ini adalah ruang penyimpan yang cukup besar untuk menyimpan payload hingga berjumlah 20.000 karakter pengetikan oleh keyboard. Sebagai ilustrasi, jumlah karakter yang dipakai didalam jurnal ini adalah 12.770 karakter sedangkan *payload script* untuk melakukan *dump hashing password* dari dalam memori komputer dapat dituliskan menggunakan tidak lebih dari 646 karakter.



Gambar 3
Jumlah karakter script hashing dump

Banyak perangkat USB sekarang ini memiliki kemampuan *multiple USB interfaces*, contohnya perangkat *keyboard-mouse* nirkable yang terhubung ke komputer melalui *USB dongle*, perangkat ini dikelompokkan di dalam kelompok *composite devices* atau perangkat komposit. Untuk ini Microsoft membuat driver independen *USB generic parent driver* (Usbccgp.sys) dimana degnan menggunakan driver ini para vendor dapat memilih dukungan driver untuk beberapa interfaces.

Gambar 4
BadUSB dengan chip ATMEGA32U4

Supaya dapat digunakan sesuai tujuannya, BadUSB setidaknya akan memerlukan 2 interface yaitu keyboard dan USB Flash Disk untuk menyimpan script payloadnya, sehingga keberadaan usbccgp didalam register sistem operasi Windows 7 dapat digunakan sebagai titik masuk untuk melakukan aktivitas forensik komputer.

Metode Penelitian

Analisis forensik serangan HID BadUSB berbasis chip ATMEGA32U4 pada tulisan ini dilakukan melalui tahapan:

1. Pencatatan waktu penelitian

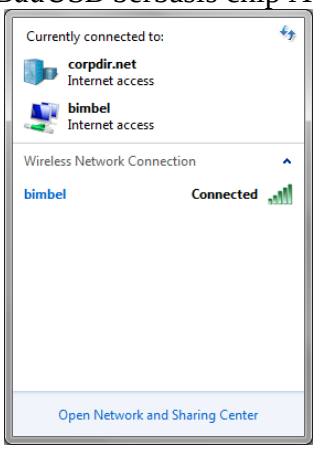
2. Menghubungkan BadUSB berbasis chip ATMEGA32U4 pada salah satu port USB komputer
3. Mengamati perilaku dan payload BadUSB berbasis chip ATMEGA32U4.
4. Melakukan analisa pada pada Root keys **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB**
5. Melakukan ekstraksi penanda waktu menggunakan teknik ekspor *key*

Pembahasan

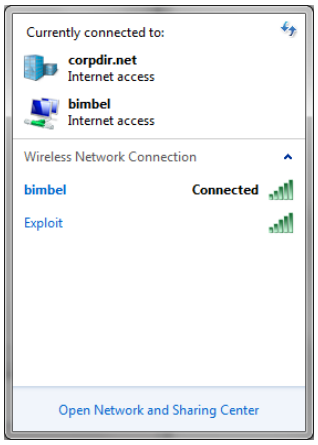
1. Penelitian dilakukan pada tanggal 22 - 23 Agustus 2018
2. Menghubungkan *BadUSB* berbasis chip ATMEGA32U4 pada salah satu port USB komputer

Gambar 5
Menghubungkan BadUSB ke komputer

3. Mengamati perilaku dan payload *BadUSB* berbasis chip ATMEGA32U4.

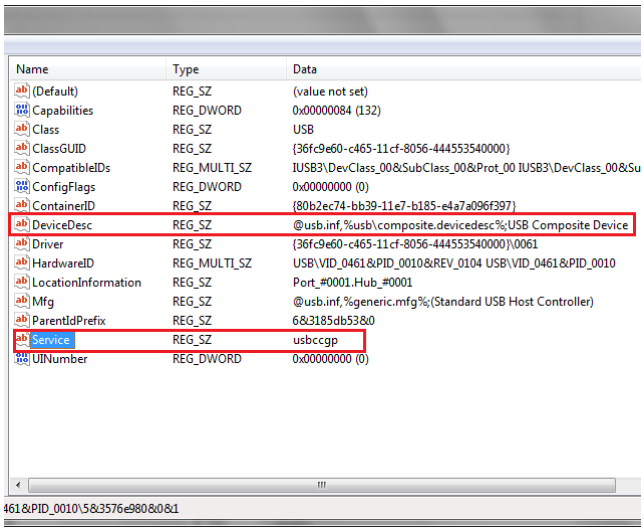


Gambar 6
Eksisting WiFi sebelum BadUSB dihubungkan



Gambar 7
Access Point Exploit yang dibuat oleh *BadUSB*

4. Melakukan analisa pada pada Root keys **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB**



Gambar 8
Key usbcccgp dan USB Composite Device

Analisa pada Root keys *HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB* mendapatkan *key usbccgp* dan *USB Composite Device* ditemukan pada *key*. Hal ini merupakan indikasikan awal bahwa perangkat BadUSB pernah dihubungkan dan informasi dari Location information key menunjukkan BadUSB dihubungkan ke ke port 1 USB

Kesimpulan

Forensik komputer pada kasus kejahatan siber menggunakan perangkat HID BadUSB di sistem operasi Microsoft Windows 7 tidaklah mudah untuk dilakukan karena akan berurusan dengan penelusuran pada banyak key register. Hal ini disabkan karena perangkat BadUSB tidak memberikan informasi kepada komputer mengenai chip set dan firmware yang digunakannya.
Prosedur berikutnya dari aktivitas forensik komputer di atas adalah untuk mendapatkan informasi penanda waktu atau timestamps yang dapat digunakan untuk mengetahui payload yang digunakan untuk melakukan penyerangan.

Daftar Pustaka

https://www.youtube.com/watch?v=EfkC7kmIMt8
https://www.youtube.com/watch?v=OEG9tW0m0Xw
https://www.youtube.com/watch?v=y9pg5vO5KYY
Universal Serial Bus (USB), Device Class Definition for Human Interface Devices (HID), Firmware Specification—6/27/01, Version 1.11
https://www.youtube.com/watch?v=F7NlCaaL3yU&t=7s
https://github.com/whid-injector/WHID
https://helgeklein.com/blog/2010/06/registry-tricks/