IMPLEMENTASI DAN ANALISIS SERANGAN USB *PASSWORD STEALER* TERHADAP PENGAMBILAN *LOGIN DATA* PADA GOOGLE CHROME DAN MOZILLA FIREFOX MENGGUNAKAN POWERSHELL

IMPLEMENTATION AND ANALYSIS OF USB PASSWORD STEALER ATTACK ON TAKING DATA LOGIN FROM GOOGLE CHROME AND MOZILLA FIREFOX USING POWERSHELL

Abdul Azies Muslim[1], Avon Budiono[2], Ahmad Almaarif[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]**abdulaziesmuslim@telkomuniversity.ac.id**, [2]**avonbudi@telkomuniveristy.ac.id**,
[3]**ahmadalmaarif@telkomuniversity.ac.id**

Abstrak

Seiring dengan berkembangnya sistem operasi Windows, aplikasi *browser* untuk menjelajah internet juga berkembang pesat. *Browser* yang paling banyak digunakan di dunia saat ini antara lain adalah Google Chrome dan Mozilla Firefox. Kedua *browser* ini memiliki fitur penyimpanan *username* dan *password* sehingga memudahkan pengguna saat melakukan *login* pada *website* tertentu yang diinginkan, namun pada kenyataannya menyimpan *username* dan *password* pada *browser* cukup berbahaya karena data-data yang tersimpan dapat diretas menggunakan serangan *brute force* ataupun dibaca melalui suatu program. Salah satu cara untuk mendapatkan *username* dan *password* pada *browser* adalah dengan menggunakan program yang dapat membaca *login data* Google Chrome dan Mozilla Firefox dari penyimpanan internal komputer lalu menampilkan *username* dan *password* yang tersimpan pada kedua *browser* tersebut. Pada penelitian ini akan dilakukan penyerangan dengan mengimplementasikan *Rubber Ducky* menggunakan BadUSB untuk menjalankan program ChromePass dan PasswordFox serta Powershell *script* menggunakan perangkat Arduino *Pro Micro* Leonardo sebagai USB *Password Stealer*. Hasil yang didapatkan dari penelitian ini adalah *username* dan *password* pada Google Chrome dan Mozilla Firefox berhasil didapatkan saat USB dihubungkan ke perangkat target, adapun rata-rata waktu berjalannya penyerangan ini adalah 14 detik sebelum kemudian dikirimkan ke *email* penulis.

Kata kunci : *Rubber Ducky*, Arduino *Pro Micro* Leonardo, Powershell, ChromePass, PasswordFox.

Abstract

Along with the development of the Windows operating system, browser applications to surf the internet are also growing rapidly. The most widely used browsers in the today is Google Chrome and Mozilla Firefox. Both browsers have a username and password management feature that makes users log in to a website easily, but in fact saving usernames and passwords in the browser is quite dangerous because the stored data can be hacked using brute force attacks or read through a program. One way to get a username and password in the browser is to use a program that can read Google Chrome and Mozilla Firefox login data from the computer's internal storage and then show those data. In this study an attack will be carried out by implementing Rubber Ducky using BadUSB to run the ChromePass and PasswordFox program and the Powershell script using the Arduino Pro Micro Leonardo device as an USB Password Stealer. The results obtained from this study are the username and password on Google Chrome and Mozilla Firefox successfully obtained when the USB is connected to the target device, the average time of the attack is 14 seconds then sending it to the author's email.

Keywords: Rubber Ducky, Arduino Pro Micro Leonardo, Powershell, ChromePass, PasswordFox.

1. Pendahuluan

Pada saat ini, penggunaan *personal computer* (PC) maupun laptop dalam kegiatan sehari-hari masih banyak ditemukan baik untuk belajar, bekerja, atau sekedar mencari hiburan. Sejak PC pertama kali diluncurkan, terjadi perkembangan yang pesat baik dari sisi perangkat keras maupun perangkat lunak hingga hari ini. Salah satu komponen terpenting pada sebuah PC adalah Sistem operasi sebagai perangkat lunak untuk dapat menjalankan mengeksekusi perintah dari pengguna. Sistem operasi Windows milik Microsoft menempati posisi pertama dari

sisi penjualan yaitu sebanyak 87.36% sampai pada Oktober 2019 [1].

Seiring dengan perkembangan sistem operasi Windows, aplikasi *bowser* juga berkembang pesat. Berbagai aplikasi *browser* bersaing untuk mendapatkan pengguna sebanyak-banyaknya melaui sistem-sistem operasi yang ada. Aplikasi *browser* yang paling banyak digunakan di dunia saat ini adalah Google Chrome dengan pangsa pasar sebesar 59.2%. Posisi Google Chrome saat ini sangatlah kuat dan hampir tidak bisa disaingi karena posisi kedua yang diduduki oleh Safari memiliki pangsa pasar sebesar 14,6% [2]. Salah satu fitur yang dimiliki oleh *browser* adalah menyimpan password pada *website* tertentu sehingga pengguna tidak perlu melakukan login setiap kali membuka *website* tersebut, fitur ini sangat bermanfaat digunakan pada *website* seperti media sosial ataupun *website* yang membutuhkan akun pengguna untuk menjalankannya. Pada kenyataannya fitur menyimpan password pada *browser* cukup berbahaya karena data-data yang tersimpan tidak terenkripsi dan peretas bisa mendapatkannya dengan serangan *brute force*, selain itu *password* yang tersimpan juga mudah dibaca melalui *malware* [3].

Saat ini komputer mendukung penyimpanan berkas eksternal yang salah satunya bernama *flashdisk*, perangkat ini terhubung dengan komputer melalui Universal Serial Bus (USB) sehingga *flashdisk* dapat dibaca dan diakses pada komputer yang telah terhubung. USB *interface* sebenarnya merupakan celah yang cukup berbahaya untuk terjadinya penyerangan, bahkan di beberapa organisasi penggunaan USB *flash drive* dilarang dikarenakan sangat berpotensial untuk digunakan sebagai alat *hacking* dalam bentuk USB-*based attack* dengan sebutan BadUSB [4].

BadUSB merupakan perangkat USB yang dimanipulasi oleh penyerang, agar saat terdeteksi oleh komputer target perangkat ini akan dikenali sebagai perangkat antar muka USB biasa, seperti keyboard komputer. Bentuk serangan dari BadUSB semakin beragam pada saat ini yang meliputi USBdriveby, Evilduino, USBee, USB Killer, dan lain sebagainya.

Penelitian ini menyajikan penyerangan berupa pengambilan data *browser* Google Chrome dan Mozilla Firefox dari komputer dengan sistem operasi Windows menggunakan perangkat Arduino *Pro Micro* Leonardo sebagai USB *Password Stealer*. Mekanisme ini memungkinkan penyerang untuk terhubung dengan komputer target menggunakan USB *Human Interface Device* (HID) berupa *keyboard* kemudian mengambil *username* dan *password* yang disimpan pada *browser* dari komputer target menggunakan program ChromePass dan PasswordFox melalui *Command Prompt* (CMD) dan Powershell. Data yang telah diambil dari *browser* kemudian dikirimkan melalui *email*. Disini penulis memanfaatkan beberapa alat dan teknologi seperti Arduino *Pro Micro* Leonardo, Arduino *Integrated Development Environment* (IDE), ChromePass, dan PasswordFox. Pada akhir penelitian penulis juga memberikan rekomendasi pencegahan terkait penyerangan ini.

2. Dasar Teori /Material dan Metodologi/perancangan

2.1 *Microcontroller*

Microcontroller (pengendali mikro) adalah sistem komputer dalam sebuah chip, perangkat ini dikenal juga dengan sebutan komputer chip tunggal. Disebut mikro karena ukurannya yang kecil dan *controller* karena kemampuannya untuk mengatur objek dan proses. Pengendali mikro bersifat *dedicated* untuk melakukan tugas yang ditentukan dan menjalankan aplikasi tunggal. Produk yang dikontrol secara otomatis seperti, *remote control*, perkakas listrik, mainan, serta perangkat perkantoran seperti mesin fotokopi, printer, dan mesin faks diprogram menggunakan pengendali mikro [5].

2.2 Arduino

Arduino adalah pengendali mikro *open source* yang dapat dengan mudah diprogram, dihapus dan diprogram ulang kapan saja. Pertama kali diperkenalkan pada tahun 2005, platform Arduino dirancang untuk memberikan kemudahan bagi siapapun untuk membuat perangkat yang berinteraksi dengan lingkungannya menggunakan sensor dan aktuator (alat kontrol mekanis). Arduino merupakan platform komputasi yang digunakan untuk membangun program perangkat elektronik dengan bertindak sebagai komputer mini seperti mikrokontroler lainnya dengan mengubah *input* menjadi *output* untuk berbagai perangkat elektronik [6].

2.3 Nirsoft.net

Nirsoft.net merupakan sebuah website yang menyediakan *tools* gratis yang berkaitan dengan IT, didirikan oleh seorang *developer* yang memiliki pengetahuan mendalam pada C++, framework .NET, windows API, dan *reverse engineering* bernama Nir Sofer pada tahun 2001. Website ini memberikan kemudahan dalam dunia IT dengan *tools* yang disediakan seperti, *password recovery*, jaringan, alamat IP, Windows *registry*, dan lain sebagainya [7].

Pada penelitian ini penulis menggunakan dua buah *tools* yang disediakan oleh nirsoft.net untuk mengambil password yang disimpan pada *browser* Google Chrome dan Mozilla Firefox, yaitu ChromePass.exe dan PasswordFox.exe. kedua *tools* ini akan dijalankan pada komputer target menggunakan USB yang telah diprogram sebelumnya sehingga dapat mengambil data password untuk kemudian dikirimkan kepada penulis melalui *email*.

2.4 Microsoft Powershell

Microsoft Powershell adalah *command-line shells* dan bahasa skrip yang secara *default* terinstall pada system operasi Windows. Berdasarkan Microsoft .NET *framework*, termasuk didalam powershell adalah antarmuka yang

memungkinkan *programmer* untuk mengakses layanan sistem operasi. Powershell dapat dikonfigurasi oleh *administrator* untuk membatasi akses dan mengurangi kerentanan pada sistem operasi [8].

2.5 Sistem Operasi

Sistem operasi merupakan perangkat lunak yang mengelola perangkat keras komputer, sistem ini menyediakan basis untuk program aplikasi dan sebagai penengah antara pengguna komputer dan perangkat keras komputer. Sistem operasi dapat mengatur waktu kerja, pengecekan kesalahan, mengelola input dan output, penyimpanan, komplikasi serta pengolahan data. Secara umum, dapat disimpulkan bahwa sistem operasi merupakan perangkat lunak lapisan pertama pada memori komputer pada saat komputer dinyalakan atau *booting* yang bertugas mengelola sumber daya perangkat keras komputer dan menyediakan layanan untuk aplikasi lainnya [9].

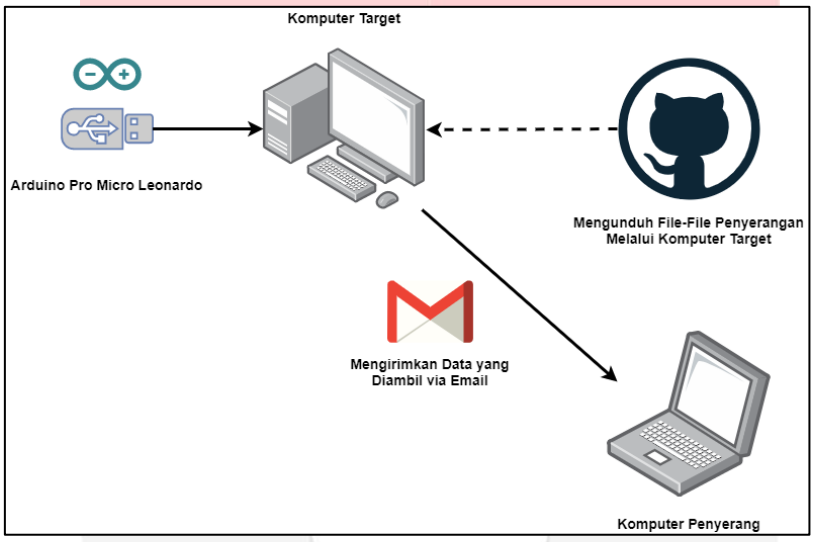
2.6 *Universal Serial Bus* (USB)

Merupakan antarmuka *plug and play* yang memungkinkan komputer untuk berkomunikasi dengan perangkat periferal dan lainnya. Dengan koneksi ini, komputer dapat mengirim atau mengambil data dari perangkat. Saat ini USB menjadi standar industri yang dikembangkan untuk koneksi periferal elektronik seperti keyboard, modem, dan lainnya [10]. Standar ini dikembangkan untuk mengganti koneksi yang berukuran lebih besar dan lebih lambat seperti port serial dan paralel. Tujuan dikembangkan standar ini adalah untuk mengembangkan antarmuka tunggal yang dapat digunakan di beberapa perangkat dan menghilangkan konektor yang berbeda beda saat ini.

3. Pembahasan

3.1. Perancangan Sistem

Dalam melakukan penyerangan, dibutuhkan hardware dan software yang mendukung. Maka dari itu dilakukan identifikasi arsitektur yang terdiri dari *hardware* dan *software* untuk melakukan penyerangan.



Gambar 1. Ilustrasi Penyerangan

Pada Gambar 1 ditampilkan ilustrasi penyerangan yang dilakukan untuk melakukan pengambilan data pada komputer target. Penyerangan diawali dengan menghubungkan perangkat USB *Password Stealer* ke komputer target melalui port USB. Setelah itu USB *Password Stealer* akan menjalankan baris kode yang disematkan oleh penyerang ke dalam perangkat Arduino. Proses yang berlangsung saat perangkat dihubungkan ke komputer target yaitu pembuatan folder, mengunduh program ChromePass, PasswordFox, dan Powershell *script* dari Github penulis, menjalankan program untuk mendapatkan data *browser*, mengirimkan *email* berisi *username* dan *password* dari komputer target, serta menghapus folder untuk menghilangkan jejak penyerangan.

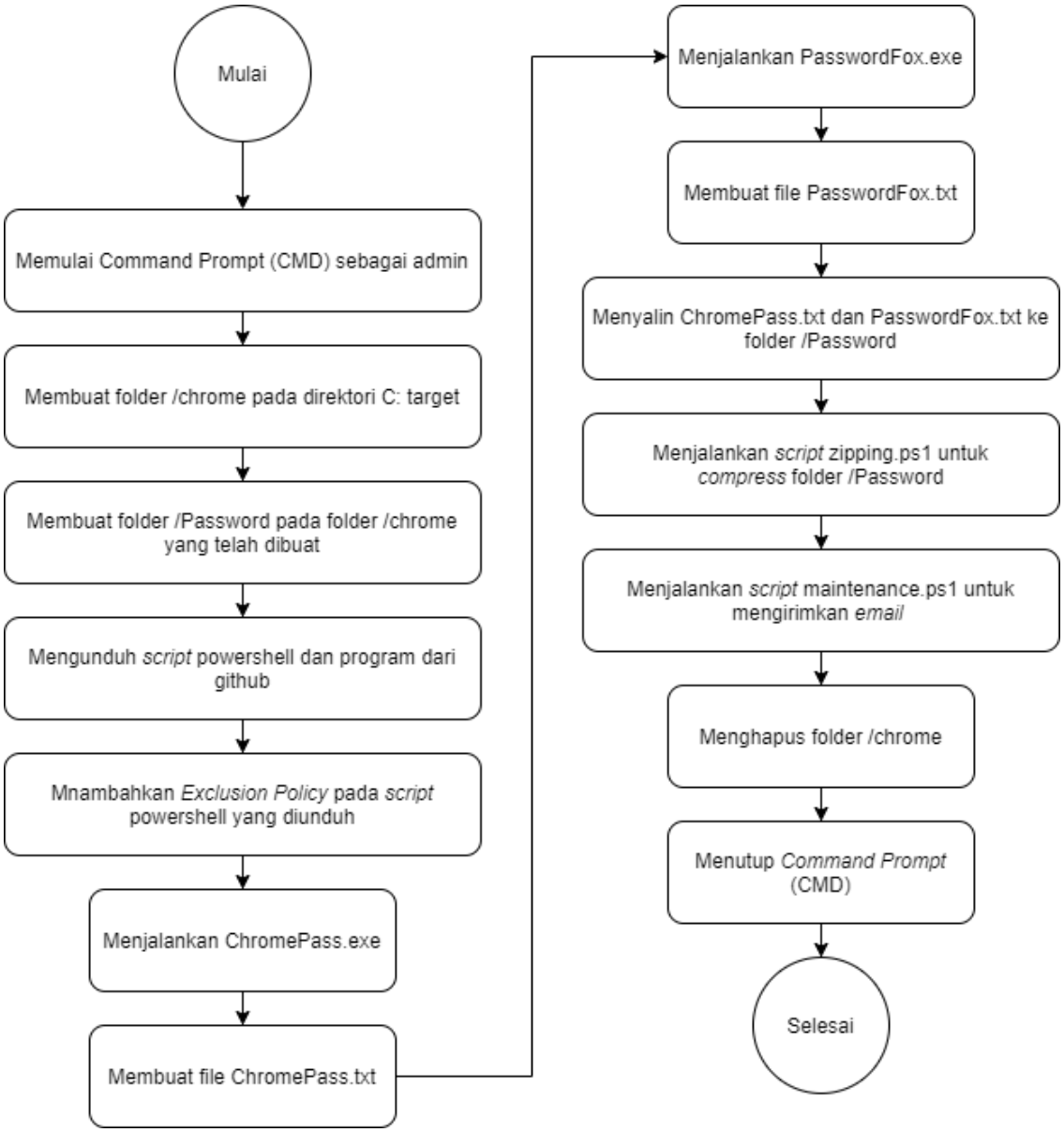
3.2. Skenario Penyerangan

1. Menghubungan USB *Password Stealer*
   Penyerang menguhubungkan USB *Password Stealer* pada komputer target yang terhubung dengan jaringan internet.
2. Menjalankan Arduino *script*
   Menjalankan Arduino *script* yang sudah dikonfigurasi untuk mengontrol *keyboard* dan membuat folder pada komputer target serta menjalankan Powershell script.
3. Menjalankan Powershell *script*
   Menjalankan Powershell *script* untuk mengunduh *file* penyerangan seperti ChromePass dan PasswordFox serta Powershell *script* lainnya.
4. Menjalankan ChromePass dan PasswordFox
   ChromePass dan PasswordFox yang telah diunduh dijalankan pada komputer target. Data yang diambil tersimpan dalam format .txt.

5. Mengirim Data Melalui *Email*
   Data yang telah didapatkan dari komputer target dikirimkan kepada penyerang melalui email yang telah ditentukan Powershell *script* kemudian menghapus folder yang telah dibuat untuk menghilangkan jejak penyerangan.
6. Melepas USB *Password Stealer*
   Penyerang melepaskan USB *Password Stealer* dari komputer target untuk mengakhiri proses pengambilan *username* dan *password*.

4. Pengembangan Sistem

Pada bagian ini dijelaskan tentang mekanisme dari penyerangan yang dilakukan. Gambar 2 berikut menunjukkan mekanisme penyerangan yang dilakukan pada penelitian ini.



Gambar 2. Alur Penyerangan

Berdasarkan gambar diatas, sistem penyerangan diawali dengan USB *Password Stealer* dihubungkan ke perangkat target, membuat folder, mengunduh dan menjalankan program ChromePass, PasswordFox, menjalankan Powershell *script* untuk melakukan *compress* file, mengirimkan *email* berisi *username* dan *password* dari komputer target, hingga menghapus folder dan menutup *command prompt*.

4.1. Menjalankan Arduino *Script*

Gambar 3 berikut adalah baris perintah Arduino *Script* untuk memberikan *input* pada *keyboard* komputer target yang akan berjalan secara otomatis untuk menjalankan penyerangan.

```
#include "Keyboard.h"
void typeKey(int key) {
  Keyboard.press(key);
  delay(100);
  Keyboard.release(key);
}
void setup() {
  // Begining the Keyboard stream
  Keyboard.begin();
  // Wait 500ms
  delay(600);
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(100);
  Keyboard.print("powershell Start-Process cmd -Verb runAs");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.press(KEY_LEFT_ARROW);
  delay(100);
  typeKey(KEY_RETURN);
  delay(1000);
  Keyboard.print("cd / & mkdir chrome & cd chrome");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("mkdir Password");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("echo (wget
'https://raw.githubusercontent.com/abdulaziesmuslim/TA/master/ChromeUpdateDo
wnload.ps1' -OutFile ChromeUpdateDownload.ps1) > b.ps1");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("powershell -ExecutionPolicy ByPass -File b.ps1");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("powershell -ExecutionPolicy ByPass -File
ChromeUpdateDownload.ps1");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("ChromePass.exe /stext ChromePass.txt");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("PasswordFox.exe /stext PasswordFox.txt");
  typeKey(KEY_RETURN);
  delay(8000);
  Keyboard.print("for %I in (ChromePass.txt PasswordFox.txt) do copy %I
c:\\chrome\\Password");
  typeKey(KEY_RETURN);
  delay(1000);
  Keyboard.print("powershell ./zipping.ps1");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("powershell ./maintenance.ps1");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("cd C:/");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("rmdir /s /q chrome");
  typeKey(KEY_RETURN);
  delay(100);
  Keyboard.print("exit");
  typeKey(KEY_RETURN);

  // Ending streampdateDownload.pps1
  Keyboard.end();
}
```

Gambar 3. Baris Perintah Arduino *Script*

4.2. Menjalankan PowerShell *Script*

Dalam penyerangan ini terdapat beberapa *script* powershell yang dijalankan, antara lain ChromeUpdateDownload.ps1, zipping.ps1, dan maintenance.ps1. Masing-masing *script* powershell memiliki fungsi yang berbeda selama berlangsungnya penyerangan.

4.3. Menjalankan ChromePass dan PasswordFox

Kedua *tools* yang digunakan memiliki kegunaan dan yang sama yaitu mengambil *username* dan *password* pada Google Chrome dan Mozilla Firefox berdasarkan *login data* masing-masing *browser* yang tersimpan pada penyimpanan lokal komputer. Google Chrome menyimpan *login data* yang disimpan pengguna pada direktori C:\Users\HP-PC\AppData\Local\Google\Chrome\User Data\Default sedangkan Mozilla Firefox menyimpan *login data* pengguna pada direktori C:\Users\HP-PC\AppData\Roaming\Mozilla\Firefox\Profiles.

4.4. Mengirim Data Melalui *Email*

Pengiriman *email* dilakukan dengan cara menjalankan *script* maintenance.ps1, pada *script* ini data email penyerang dimasukkan sebagai pengirim juga penerima. Selain itu *script* ini akan menggunakan *port* SMTP 587 agar dapat mengirimkan *email* dari komputer target.

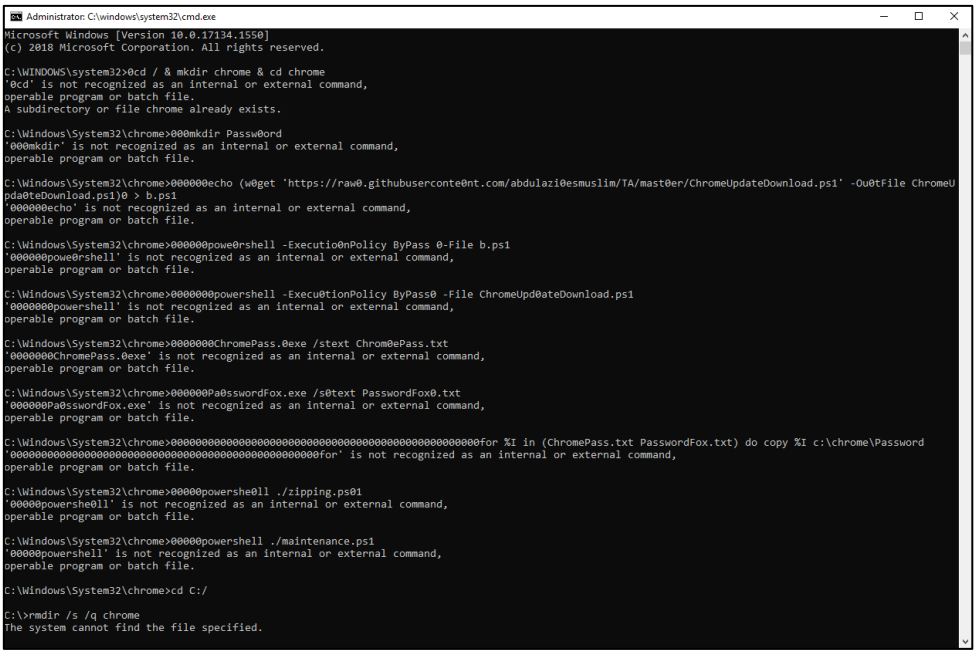
5. Analisis

5.1. Analisis Arduino *Script*

Pada pengujian ini, penulis menggunakan perangkat Laptop dan USB HID Arduino. Arduino *script* yang digunakan oleh penulis memiliki total *delay* 8 detik dengan *delay* tercepat selama 0.1 detik dan *delay* terpanjang 5 detik seperti pada Gambar IV-3. Namun pada proses pengujian normal yang dilakukan, lamanya proses penyerangan melebihi *delay* yang diatur pada Arduino *script* karena membutuhkan waktu proses saat melakukan *execution policy bypass* ketika menjalankan *script* powershell dan mengirimkan *email*. Selain itu juga dari pengujian yang dilakukan terjadi kegagalan saat menyalin *file* .txt kedalam folder sehingga *email* yang dikirimkan kosong. Setelah dilakukan pengujian, dapat diambil rata-rata proses penyerangan berjalan selama 14 detik, adapun kesimpulan yang diambil adalah Arduino *script* memiliki sistem *delay* yang harus diatur manual dan dapat menyebabkan gangguan saat proses penyerangan tergantung pada kondisi komputer target.

5.2. Analisis Interupsi

Berdasarkan pengujian yang dilakukan pada komputer target, adanya interupsi saat proses penyerangan sedang berlangsung akan menyebabkan kegagalan program meskipun proses penyerangan terus berlanjut hingga *input* keyboard yang sudah di program berjalan semua. Gambar 3 berikut menampilkan program yang berjalan namun terjadi interupsi tombol 0 pada *keyboard* komputer.



Gambar 4. Interupsi Keyboard saat Program Berjalan

5.3. Analisis Pengambilan Data

Pengambilan data ini dilakukan pada *browser* Google Chrome dan Mozilla Firefox. Kedua *browser* ini menyimpan *login data* penggunanya yang berisikan *username* dan *password* pada direktori C: komputer seperti yang telah dijelaskan sebelumnya. Pada penyerangan ini pula penulis menggunakan *tools* yang disediakan oleh Nirsoft.net bernama ChromePass dan PasswordFox untuk mengambil *login data* pengguna kedua *browser*

tersebut. Baik ChromePass mauun PasswordFox bekerja dengan cara mengambil *login data* kedua *browser* pada penyimpanan lokal komputer lalu melakukan dekripsi terhadap *login data* tadi agar dapat dibaca oleh penyerang.

Pada pengujian ini dilakukan beberapa skenario dengan parameter yang berbeda sehingga dapat disesuaikan dengan kondisi komputer target yang beragam seperti yang dicantumkan pada Tabel 1.

Tabel 1. Analisis Skenario Penyerangan

Skenario	Penjelasan	Hasil
Satu	Pengambilan data dengan kedua *browser* terpasang pada komputer target	Berhasil
Dua	Pengambilan data dengan salah satu *browser* terpasang pada komputer target	Berhasil mengambil data dari *browser* yang terpasang saja
Tiga	Pengambilan data dengan kedua *browser* tidak terpasang pada komputer target	Hanya berhasil megirimkan *email* kosong
Empat	Pengambilan data *username* dan *password* menggunakan kombinasi karakter kapital, angka, serta simbol	Berhasil
Lima	Pengambilan data *username* dan *password* menggunakan panjang hingga 50 karakter	Berhasil
Enam	Pengambilan data dengan kondisi komputer target tidak terhubung dengan internet	Gagal, karena *script* powershell dan *tools* pengambilan data diunduh terlebih dahulu

5.4. Rekomendasi Untuk Mencegah Penyerangan

Berdasarkan hasil penelitian pengambilan data *browser* Google Chrome dan Mozilla Firefox pada komputer target menggunakan ChromePass.exe dan PasswordFox.exe, penulis mendapatkan hasil bawha penyerang dapat menggunakan *tools* tersebut dengan mudah untuk mengambil *login data* pada *browser* komputer target.

Rekomendasi yang dapat penulis berikan untuk mencegah terjadinya serangan seperti ini terbagi dalam dua aspek, yaitu:

1. Pengguna
    - Memperhatikan komputer agar tidak dihubungkan dengan perangkat USB yang mencurigakan karena bentuk BadUSB yang digunakan penyerang seringkali sulit dibedakan dengan USB *mass storage* biasa.
    - Mematikan atau mengunci komputer saat ditinggalkan karena pengambilan *username* dan *password* menggunakan USB hanya memakan waktu yang singkat serta tidak meninggalkan jejak sehingga pemilik komputer tidak akan menyadari bahwa telah terjadi penyerangan terhadap perangkatnya.
    - Tidak menyimpan *username* dan *password* pada *browser* apapun untuk menghindari segala bentuk pengambilan data baik menggunakan BadUSB ataupun metode lainnya.
    - Menggunakan fitur 2-*step verification* pada akun pribadi baik tersimpan maupun tidak pada *browser* agar jika terjadi pengambilan data pada *browser*, data tersebut tidak berguna bagi penyerang atau sulit untuk gunakan karena menggunakan pengamanan berlapis.
2. Sistem
    - Selalu melakukan pembaruan pada *browser* Google Chrome dan Mozilla Firefox saat tersedia untuk meningkatkan keamanan *login data* sehingga memungkinkan ChromePass dan PasswordFox yang digunakan penyerang tidak dapat membaca *username* dan *password* yang tersimpan pada *browser* dengan *patch* terbaru.
    - Menggunakan aplikasi pihak ketiga untuk menyimpan *login data* browser sehingga ChromePass dan PasswordFox tidak bisa membaca *username* dan *password* yang disimpan. Hal ini dikarenakan baik ChromePass dan PasswordFox hanya dapat membaca *login data* yang disimpan pada Google Chrome dan Mozilla Firefox sehingga penggunaan *Browser Pasword Manager* selain bawaan kedua *browser* tersebut dapat mencegah penyerangan ini.
    - Mematikan *port* USB melalui Windows *Registry* pada perangkat komputer dapat mencegah perangkat USB yang terhubung dibaca oleh komputer sehingga terhindar dari segala bentuk penyerangan menggunakan BadUSB.
    - Melakukan *disable port* SMTP agar jika terjadi penyerangan yang membutuhkan pengiriman *email* melalui komputer target tidak dapat dilakukan.

6. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagaimana berikut:

1. Perangkat Arduino *Pro Micro* Leonardo dapat diprogram menjadi USB *password stealer* menggunakan Arduino IDE dan *tools* dari Nirsoft.net. Ketika USB *password stealer* dihubungkan dengan komputer target, program akan berjalan untuk mengambil data *username* dan *password* yang tersimpan pada *browser* menggunakan ChromePass dan PasswordFox. *Output* dari penelitian ini adalah didapatkannya *login data* yang dikirimkan kepada penyerang melalui *email*.
2. Pengambilan data dari Google Chrome dan Mozilla Firefox dapat dilakukan dengan menggunakan ChromePass dan PasswordFox sehingga tingkat keamanan dari menyimpan *username* dan *password* pada *browser* cukup rentan. Berdasarkan proses pengambilan data yang dilakukan menggunakan USB *password stealer*, versi *browser* yang digunakan adalah Google Chrome versi 83.0.4103.116 dan Mozilla Firefox versi 77.0.1. Penyerangan ini dapat dilakukan pada seluruh versi kedua *browser* dibawahnya namun belum tentu dapat digunakan pada versi terbaru nantinya dikarenakan mungkin akan ada peningkatan keamanan dari masing-masing *browser*.
3. Rekomendasi untuk meminimalisir terjadinya penyerangan seperti ini berdasarkan aspek pengguna adalah memperhatikan komputer agar tidak dihubungkan dengan perangkat USB yang mencurigakan, mematikan atau mengunci komputer saat sedang ditinggalkan, tidak menyimpan *username* dan *password* pada *browser* apapun, dan menggunakan fitur 2-step verification pada akun pribadi baik tersimpan maupun tidak pada *browser*. Adapun dari sisi keamanan sistem dapat dilakukan pembaruan pada *browser* Google Chrome dan Mozilla Firefox, menggunakan aplikasi BPM pihak ketiga, mematikan *port* USB pada perangkat komputer dan melakukan *disable port* SMTP.

7. Saran

Untuk penelitian lebih lanjut, terdapat saran-saran yang dapat membantu untuk mengembangkan penelitian dimasa yang akan datang, yaitu:

1. Melanjutkan pengujian USB *Attack* dengan target pengambilan data *browser* yang lebih luas seperti *history*, *bookmark*, dan *cache*.
2. Memperhatikan versi *tools* penyerangan yang disediakan Nirsoft.com, selalu usahakan untuk menggunakan versi terbaru untuk setiap program yang digunakan.
3. Melakukan penelitian menggunakan *antivirus* selain Windows *Defender* untuk mencegah berjalannya program yang mencurigakan pada komputer.

Daftar Pustaka:

[1] Net MarketShare, "Operating System Market Share," October 2019. [Online]. Available: https://netmarketshare.com/.

[2] W3Counter, "Browser & Platform Market Share," 4 November 2019. [Online]. Available: https://www.w3counter.com/globalstats.php?year=2019&month=11. [Accessed 4 November 2019].

[3] Mateso, "The Danger of Storing Passwords via Browser," 25 March 2019. [Online]. Available: https://blog.passwordsafe.de/en/2019/03/25/how-dangerous-is-it-to-store-your-passwords-in-the-browser/. [Accessed 5 December 2019].

[4] B. Cannols and A. Ghafarian, "Hacking Experiment by Using USB Rubber Ducky Scripting," *SYSTEMICS, CYBERNETICS AND INFORMATICS*, pp. 66-71, 2017.

[5] A. Hussain, A. Hammad, K. Hafeez and T. Zainab, "Programming a Microcontroller," *International Journal of Computer Applications*, vol. 155, no. 5, pp. 21-26, 2016.

[6] L. Louis, "Working Principle of Arduino and Using It As a Tool for Study and Research," *International Journal of Control, Automation, Communication and Systems (IJCACS)*, pp. 21-29, 2016.

[7] N. Sofer, "About," May 2008. [Online]. Available: https://www.nirsoft.net/about_nirsoft_freeware.html. [Accessed 14 Juni 2020].

[8] D. Hendler, S. Kels and A. Rubin, "Detecting Malicious PowerShell Commands using Deep Neural Networks," *Asia Conference on Computer and Communications Security*, pp. 187-197, 2018.

[9] A. Silberschatz, G. Gagne and P. B. Galvin, Operating System Concepts, Hoboken, New Jersey: John Wiley & Sons, 2018.

[10] Computer Hope, "USB," 16 11 2019. [Online]. Available: https://www.computerhope.com/jargon/u/usb.htm.