PRUEBA EXPERIMENTAL EN LAS VULNERABILIDADES DE SEGURIDAD HACIENDO USO DE BAD USB

Mtro. Flores Montaño Luis Alberto
Email: luisfloresmontano@hotmail.com
M. en C. Esther Viridiana Vázquez Carmona
Email: evazquezc1801@alumno.ipn.mx
M. en C. Rodrigo Vázquez López
Email: rvazquezl1800@alumno.ipn.mx
Dr. Juan Carlos Herrera Lozada
jlozada@ipn.mx
Dr. Jacobo Sandoval Gutiérrez
Email: j.sandoval@correo.ler.uam.mx

Instituto Politécnico Nacional
Centro de Innovación y Desarrollo Tecnológico en Cómputo
Universidad Autónoma Metropolitana

Resumen

La ingeniería social y el uso de memorias USB han demostrado ser muy efectivos a lo largo de los años para un ataque cibernético. Como es habitual la educación en ciberseguridad es escasa, ya que diversas personas suelen conectar dispositivos USB de dudosa procedencia. No obstante, pese a contar con un sistema de protección ante ataques USB, las computadoras necesitan usar de dispositivos periféricos a menudo, por lo que la mayoría de las ocasiones se les imposibilita detectar un dispositivo de ataque. Debido a esto es factible explotar un sistema utilizando un Bad USB, "disfrazado" de un dispositivo de interfaz humana como puede ser un teclado (en inglés HID). Las herramientas que utilizan un esquema como es el caso de Kautilya o Rubber Ducky; sin embargo, en esta investigación se implementa el uso de Bash Bunny, desarrollada por la empresa Hak5, que implementa cargas útiles (en inglés "Payloads"), las cuales contienen una serie de comandos capaces de realizar diversas tareas sin el consentimiento de la víctima.
Bash Bunny, al igual que su homogéneo Rubber Ducky, se disfraza como un dispositivo USB, y toma en ocasiones menos de 5 segundos realizar un ataque físico, dejando a una computadora vulnerable ante robo de credenciales o deshabilitación de diversos protocolos de seguridad, permitiendo así realizar otros tipos de ciberataques, ya sea de forma remota como puede ser el caso de un Phising o un backdoor. En esta investigación se detalla el proceso para realizar dicho ataque haciendo uso de Bash Bunny(Bad USB).

Palabras Clave: Ciberataque, Ciberseguridad, Bad USB, Bash Bunny, HID.

Summary

Social engineering and the use of USB sticks for an attack have proven to be very effective over the years. As usual, cybersecurity education is scarce, since various people often connect USB devices of dubious origin. However, despite having a protection system against USB attacks, computers often need to use peripheral devices, so most of the time they are unable to detect an attack device. Due to this, it is feasible to exploit a system using a Bad USB, "disguised" as a human interface device such as a keyboard (HID). Tools that use a scheme such as Kautilya or Rubber Ducky; however, in this investigation the use of Bash Bunny is implemented, developed by the company

Hak5, which implements payloads (in English “Payloads”), which contain a series of commands capable of performing various tasks without the consent of the victim. . Bash Bunny, like its homogeneous Rubber Ducky, disguises itself as a USB device, sometimes taking less than 5 seconds to perform a physical attack, leaving a computer vulnerable to credential theft or disabling various security protocols, thus allowing carry out other types of cyberattacks, either remotely, such as a Phishing or a backdoor. This investigation details the process to carry out said attack using Bash Bunny (Bad USB).

Keywords: Cyberattack, Cybersecurity, Bad USB, Bash Bunny, HID.

I. Introducción

Acorde con el artículo del sitio web de Microsoft TechNet “Definición de una vulnerabilidad de seguridad “(Wibjorn, 2022), hay tres elementos principales en la ciberseguridad: confidencialidad, integridad y disponibilidad. Tomando en cuenta la clasificación de estos tres elementos, el atacante podría encontrar un elemento para hacer al sistema vulnerable (Vouteva et. al, 2015).

Tomando en cuenta lo anterior el atacante puede intentar extraer información confidencial del sistema y utilizarlos sin autorización alguna. Esto con el propósito de espiar a un competidor comercial, o en su defecto para el comienzo de un proceso de reconocimiento que expone más vulnerabilidades del sistema. Un ejemplo de esto es la modificación de la información del sistema, alteración en datos y privilegios del sistema, así como agregar las puertas traseras (en inglés Backdoors) para posteriormente acceder por esos puntos vulnerables (Vouteva et. al, 2015).

Adicionalmente, el pirata informático también podría intentar que el sistema no esté disponible provocando un bloqueo, DoS, etc., y posteriormente limitando a los usuarios el acceso a las funciones del sistema objetivo, tal es el caso de un sistema como un proveedor de internet, de servicios en específicos o incluso de un banco, lo que ocasionaría un retraso en diversas operaciones, así como desconfianza en usuarios clientes de diversas compañías (Vouteva et. al, 2015).

Actualmente existen diversos métodos para penetrar en una red ya sea como pirata informático (hacker) o “pentester”. Uno de estos métodos muy conocidos es la ingeniería social, la cual es parte de los diversos caminos posibles para que un atacante pudiera ingresar a un sistema. La intención de este método mencionado es utilizar la manipulación humana o la previsibilidad del comportamiento humano, con el fin de extraer información confidencial de ciertas víctima o dispositivo objetivo. No obstante, este método mencionado puede utilizarse en combinación con otro método conocido como ataque físico, los cuales pueden lograr obtener un acceso a una computadora conectada a la red objetivo y usarla como un punto de entrada para el atacante. Dicho de otra manera, un ataque físico, consiste en conectar una memoria USB a la máquina o dispositivos objetivo (Vouteva et. al, 2015). Este ataque se puede hacer mediante el uso de un dispositivo USB detectado por la computadora de la víctima como un dispositivo de interfaz humana (en inglés HID), este en lugar de ser reconocido como un dispositivo de almacenamiento masivo, se reconoce como un tipo de teclado, por el que ejecuta un código sin el conocimiento o consentimiento del usuario; este puede ser conectado mientras que la víctima se distrae, o se retira momentáneamente de su equipo. Este tipo de USB se le conoce como USB defectuoso o Bad USB. Cabe mencionar, que es común escuchar acerca de los peligros que pueden presentar las memorias USB normales; sin embargo; una Bad USB a menudo son subestimados sus ataques, bajo el esquema de que estos requieren un conocimiento más técnico (Vouteva et. al, 2015).

Los ataques basados en USB presentan un desafío nuevo y únicos para los investigadores dedicados a la ciberseguridad forense. Estos tipos de ataques permiten realizar un ataque discreto, donde posteriormente ponen en compromiso a la ciberseguridad física. Este tipo de ataques pueden realizarse únicamente conectado el dispositivo a la máquina víctima (Thomas et. al, 2021).

Por otro lado, los dispositivos están diseñados para limitar la cantidad de información que queda operando en el disco, debido a esto se presenta un desafío al análisis forense de la memoria, ya que no presenta evidencia del ataque ejecutado, presentado de esta manera limitaciones en el análisis realizado. Adicionalmente, estos dispositivos están diseñados específicamente para realizar este tipo de ataques y que además es bastante sencillo obtenerlos en el mercado. Siendo así realizar este tipo de ataques puede ser llevados a la práctica, incluso por atacantes poco experimentados. Cabe mencionar que este tipo de dispositivos (Bad USB) son artefactos basados en la memoria que pueden seguir

siendo extraíbles durante un período prolongado de tiempo incluso después de que el ataque haya terminado, y hasta después de ser desenchufado (Thomas et. al, 2021).

II Investigaciones relevantes en el área de vulnerabilidad en protocolos de ciberseguridad usando Bad USB

Actualmente existen diversas investigaciones acerca de pruebas de ataques realizados por los dispositivos Bad USB; tal es el caso de los siguientes investigadores: en la conferencia de BlackHat, E.E.U.U 2014, los investigadores Karsten Nohl y Jakob Lell presentan diversos escenarios de ataques USB utilizando un Bad USB (SrLabs,2022). Estos ataques mostraron que es posible usar un USB para redirigir las consultas del DNS del usuario a el servidor DNS de un atacante.

Posteriormente el investigador Samy Kamkar demuestra un microcontrolador Teensy USB, configurado para instalar una puerta trasera (Backdoor), y cambiar la configuración de DNS de una máquina desbloqueada (Kamkar,2022). Por su parte el investigador Nikhil "SamratAshok" Mittal desarrolló otra forma de usar un USB defectuoso en una herramienta, llamada Kautilia (Samratashok, 2022); este último incluye funciones de recopilación de información y la ejecución de scripts.

III. Funcionamiento de los dispositivos Bad USB

En la figura 1, se muestra como interactúa una plataforma de ataque basado en el ataque Bad USB con una máquina objetivo.

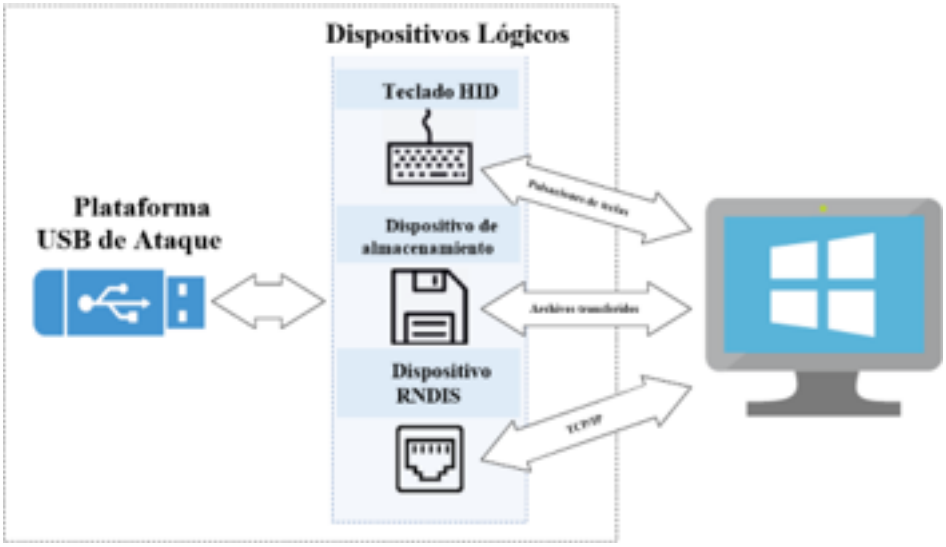

Figura 1. Plataforma de ataque basado en Bad USB (Elaboración propia).

Primeramente, la seguridad física de la máquina objetivo se ve comprometida de tal manera que un USB al ser insertado no puede ser reconocido por el sistema operativo. Una vez que el dispositivo ha sido conectado al sistema, esté ampliará su funcionalidad a la falsificación de uno o más tipos de dispositivos conocidos o de confianza, haciendo se pasar como un teclado o dispositivo de interfaz humana (HID). Con esto el dispositivo Bad USB, utiliza los medios virtuales falsificados para realizar la actividad maliciosa en la máquina o red de la víctima. Algunos de los ejemplos objetivos más comunes es la exfiltración de datos y ejecución de carga útil. Posteriormente al realizar la actividad maliciosa, el dispositivo es desconectado de la maquina víctima, permitiendo al atacante salir del área. El ataque se completa con una interacción mínima con la máquina destino (Vouteva et. al, 2015).

IV. Funcionamiento y desempeño de Bash Bunny

La herramienta de ataque Bash Bunny desarrollada por Hak5, es probablemente el dispositivo más avanzado hasta la fecha, este es capaz de realizar diversos ataques informáticos. Como se ha mencionado anteriormente es un dispositivo que se hace pasar por un dispositivo de interfaz humana

(HID), así como una USB de confianza, tarjetas de red, memorias flash entre otros; adicionalmente tiene la apariencia de una memoria USB, por lo que es capaz de robar cualquier tipo de información en el sistema; cabe mencionar que los sistemas operativos donde se puede utilizar, abarcan diversos sistemas operativos, como Windows, Linux, OS X y sistemas basados en Unix y Android (RedBird,2022).

Algunas de las tareas maliciosas que es capaz de realizar este dispositivo son el control de archivos, recibir contraseñas de los usuarios, instalar software malicioso, todo esto como si se tratara de un dispositivo de confianza. Es importante mencionar que los creadores (Hak5) de este dispositivo cuentan con un repositorio que abarca diversas cargas útiles (payloads) para atacar cualquier sistema informático, adicionalmente permite al usuario crear diversas cargas útiles, utilizando un simple editor de textos, sin necesidad de APIs o SDKs (Zion3R,1970).

Este dispositivo en su interior tiene un microcomputador Linux con un procesador ARM Cortex A7 de cuatro núcleos, caché de 32 K L1/512 K L2, memoria DDR3 de 512 MB, disco SLC NAND de 8 GB y el cual es capaz de interpretar diversos lenguajes de programación convencionales como es el caso de Ruby, Pyhton, Perl, entre otros. Cabe mencionar que el tiempo de arranque de este dispositivo es de 7 segundos y además puede funcionar de tres formas distintas; teniendo en cuenta que Bash Bunny contiene un interruptor el llamado modo armado el cual es un modo para la configuración del dispositivo y las otras dos posiciones se utilizan para seleccionar entre dos ataques diferentes preparados de antemano, a su vez cuenta con un led multicolor, el cual notifica el tipo de interruptor en el que se encuentra Bash Bunny(Antal,2022). En la figura 2 se muestra un ejemplo de esta funcionalidad.

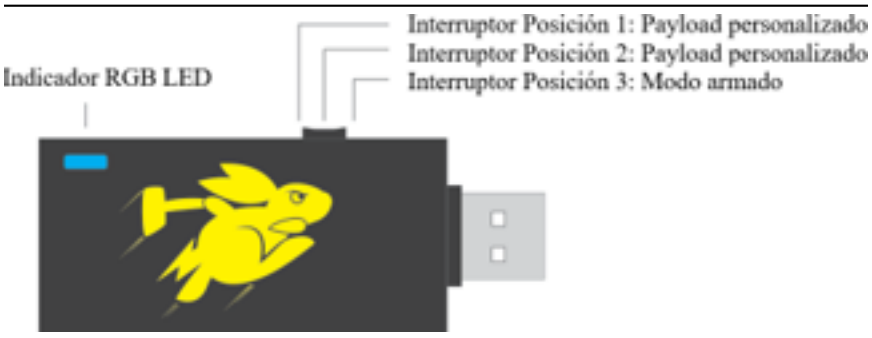

Figura 2. - Funcionalidad de Bash Bunny (Elaboración propia).

A grandes rasgos este dispositivo funcionar de la siguiente manera: Primero se carga el payload de ataque en el dispositivo, seguidamente se desliza el interruptor del dispositivo a “modo armado”, se conecta a la máquina víctima, en este caso al puerto USB, en automático se abren los archivos de carga útil y se ejecutan y finalmente se retira la dispositivo Bash Bunny (RedBird,2022).

Antes de realizar la ejecución del Bash Bunny es necesario desarrollar los scripts o también conocidas como cargas útiles, estas pueden ser escritas en cualquier editor de textos estándar, como es el caso del bloc de notas, vi, nano, entre otros. Dichas cargas útiles deben tener por nombre “payload.txt”. Cuando Bash Bunny arranca con su interruptor en la posición 1 o 2, “payload.txt” s ejecuta el archivo de la carpeta correspondiente del interruptor.

Estas scripts se pueden intercambiar únicamente copiando y pegando en el Bash Bunny cuando se encuentra en su modo Armado (posición 3 del interruptor, la más cercana al enchufe USB), a través de almacenamiento masivo. Cabe mencionar que este dispositivo interpreta directamente el lenguaje Ducky Script que se ha convertido en sinónimo de malos ataques USB. Con su modo de ataque HID, Bash Bunny se convierte en un teclado y Ducky Script se procesa con un comando “QUACK” rápido y fácil. Cabe mencionar que se pueden descargar diversos scripts o cargas útiles dentro del repositorio Github en la página https://github.com/hak5/bashbunny-payloads.

El siguiente código de carga útil, permite que Bash Bunny convierta en un teclado como en una unidad flash. Luego, inyecta pulsaciones de teclas que le indican al objetivo de Windows que ejecute un script de PowerShell guardado en dicha unidad flash.

```
GET SWITCH_POSITION
LED ATTACK
ATTACKMODE HID STORAGE
RUN WIN powershell "(gwmi win32_volume
'label=''BashBunny''').Name+'payloads\\$SWITCH_POSITION\d.cmd')"
LED FINISH
```

Los ataques avanzados se habilitan mediante la combinación de ataques HID con el dispositivo USB adicional compatible con Bash Bunny, como Gigabit Ethernet, serie y almacenamiento. Junto con un lenguaje de secuencias de comandos que admite condiciones y lógica mediante BASH, es posible una nueva era de ataques de inyección de pulsaciones de teclas.

VI. Conclusiones

Bash Bunny es una herramienta para realizar ataques de tipo físico. Con esta herramienta las posibilidades de realizar cargas útiles o scripts son muy diversas y único límite es la imaginación de cada creador. Adicionalmente, es una herramienta para cualquier "pentester", pirata informático y profesional de seguridad, a un precio de aproximadamente dos mil pesos mexicanos. Sin embargo, también existe la opción de crear una Bad USB propia, alternativa a Bash Bunny.

Un USB defectuoso en el caso de computadoras desbloqueadas y ataques que pueden ser 'escritos' por un teclado explotaciones simples, como obtener acceso remoto a la computadora con los privilegios de usuario actuales, puede provocar fugas de información confidencial. Las computadoras portátiles personales a menudo no requieren una escalada de privilegios, ya que el usuario cuenta de la víctima contiene toda la información de esa computadora portátil.

Existen formas limitadas en las que se pueden prevenir estos ataques como es el caso de la aplicación de políticas locales o de grupo incluyendo hardware o ejecutables en la lista blanca, el cual podría ser una opción. Sin embargo, no se aplican con frecuencia, especialmente en dispositivos personales.

Referencias

1. Antal, L. (**n.d.**). *Bash Bunny – Guide. Hacking Lab.* Retrieved November 3, 2022, from https://hackinglab.cz/en/blog/bash-bunny-guide/

2. Bash Bunny by Hak5. (**n.d.**). *Bash Bunny by Hak5 - Bash Bunny.* Retrieved November 3, 2022, from https://docs.hak5.org/bash-bunny/

3. Jesús. (**2021, March 9**). *Pasos Para Configurar Bash Bunny en Español: Operating systems, scripting, PowerShell and security. Operating systems, scripting, PowerShell and security.* Retrieved November 3, 2022, from https://www.jesusninoc.com/03/09/pasos-para-configurar-bash-bunny-en-espanol/

4. RedBird. (**n.d.**). *Bash Bunny: Dispositivo de ataque USB multifuncional. RedBird Seguridad Ofensiva.* Retrieved November 3, 2022, from https://r3dbird.blogspot.com/2019/04/bash-bunny-dispositivo-de-ataque-usb.html

5. Samratashok. (**n.d.**). *Samratashok/Kautilya: Kautilya - tool for easy use of human interface devices for offensive security and penetration testing. GitHub.*Retrieved November 4, 2022, from https://github.com/samratashok/Kautilya

6. Security Research Labs. (**n.d.**). Retrieved November 4, 2022, from https://www.srlabs.de/

7. Thomas, T., Piscitelli, M., Nahar, B. A., & Baggili, I. (**2021**). *Duck Hunt: Memory forensics of USB attack platforms. Forensic Science International: Digital Investigation,* 37, 301190.

8. Usbdriveby. Samy Kamkar (**n.d.**). *USBdriveby: exploiting USB in style.* Retrieved November 4, 2022, from http://samy.pl/usbdriveby/

9. Vouteva, S., Verbij, R., & Roos, J. (**2015**). *Feasibility and Deployment of Bad USB.* University of Amsterdam, System and Network Engineering Master Research Project.

10. Wibjorn. (**n.d.**). *Microsoft learn: Build skills that open doors in your career. Microsoft Learn: Build skills that open doors in your career.*Retrieved November 4, 2022, from https://technet.microsoft.com/

11. Zion3R. (**1970, January 1**). *Bash Bunny, UN USB hacking para atacar sistemas informáticos. Hacking Land - Hack, Crack and Pentest.*Retrieved November 3, 2022, from https://www.hacking.land/2017/03/bash-bunny-un-usb-hacking-para-atacar.html?amp=1&m=1

Cómo citar este artículo en APA

Flores, A., Vázquez, E., Vázquez, R., Herrera, J. & Sandoval J. (**1 de enero de 2023**). Prueba experimental en las vulnerabilidades de seguridad haciendo uso de Bad USB *Boletín UPIITA.* (94). https://www.poner la liga del articulo

Regresar al índice