Universidad Nacional Autónoma de México
Facultad de Ciencias
# Análisis de Software Malicioso

Hernández Chávez Jorge Argenis

Agosto 2019

# 1. Documentacion tecnica

**NOTA**
Los comentarios de la logica de la implementacion estan en el codigo para un mejor detalle.
A continuacion se muestran las pruebas apartir de imagenes tomadas.

# 2. Fuentes


https://www.dreamincode.net/forums/topic/34743-winexec/
https://www.geeksforgeeks.org/system-call-in-c/
https://sites.google.com/site/sencillamentec/home/entrada-de-datos/sscanf
https://www.includehelp.com/c/working-with-hexadecimal-values-in-c-programming-language.aspx
https://stackoverflow.com/questions/1382051/what-is-the-c-equivalent-for-reinterpret-cast
https://www.tutorialspoint.com/c_standard_library/c_function_memcpy.htm
https://stackoverflow.com/questions/10210981/unsuccessfully-using-sscanf-to-read-in-hexadecimal
https://www.geeksforgeeks.org/strtoul-function-in-c-c/
https://foro.elhacker.net/programacion_cc/programa_para_convertir_decimal_binario_hexadecimal_o
https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-gettemppatha
https://www.sanfoundry.com/c-program-convert-hex-binary/


# 3. Conclusion

**¿Qué importancia tiene este proyecto respecto a seguridad informática?**
Este proyecto me resulto muy útil ya que encontre muchas cosas que desconocia encuanto al lenguaje estructurado(C) ya que todas esas funciones me hicieron ver más cosas que suceden sin que mucha gente se percarte de los problemas como filtracion de la informacion y de progrmas mal intencionados con diferente propocitos y como con cierto tiempo que nos llevo a nosotros como aprendices a desarrollar estas aplicaciones, ahora una persona que se dedica de lleno a esto y que aparte tienen los años de esperiencias es de mayor facilidad tener todo al alcance de sus manos sin que nosotros nos percatemos.

**¿Qué aprendieron?**
nuevas funciones y un mayor entendimiento del tema visto. Al igual que hay que pensar en que mucha gente usa este tipo de herramientas par al daño de la integridad de una persona.
es por eso que en este proyecto al ver las vulnerabilidades del equipo en cuestion ver que no pase lo mismo de nuevo. Ya que estaremos protegiendo de manera eficaz. **¿Qué les gustó?**
La verdad todo ya que se aprendieron cosas nuevas se reafirmo conocimiento al igual que, se me hizo divertida, desafiante tanto que me llevo mucho tiempo resolverla. **¿ Cómo se enfrentarían a este tipo de amenazas?**
Primeramente hacer lo necesario para que al momento que entro la amenaza saber como entro y hace bloquear esa via de entrada, ver los sistemas que se estan corriendo para que podamos seguir la vida del programa maliciosa y asi evitar que se vuelva a propagar, al igual que nos ayudaria a pensar de donde se encuentra el progrmam malicioso.

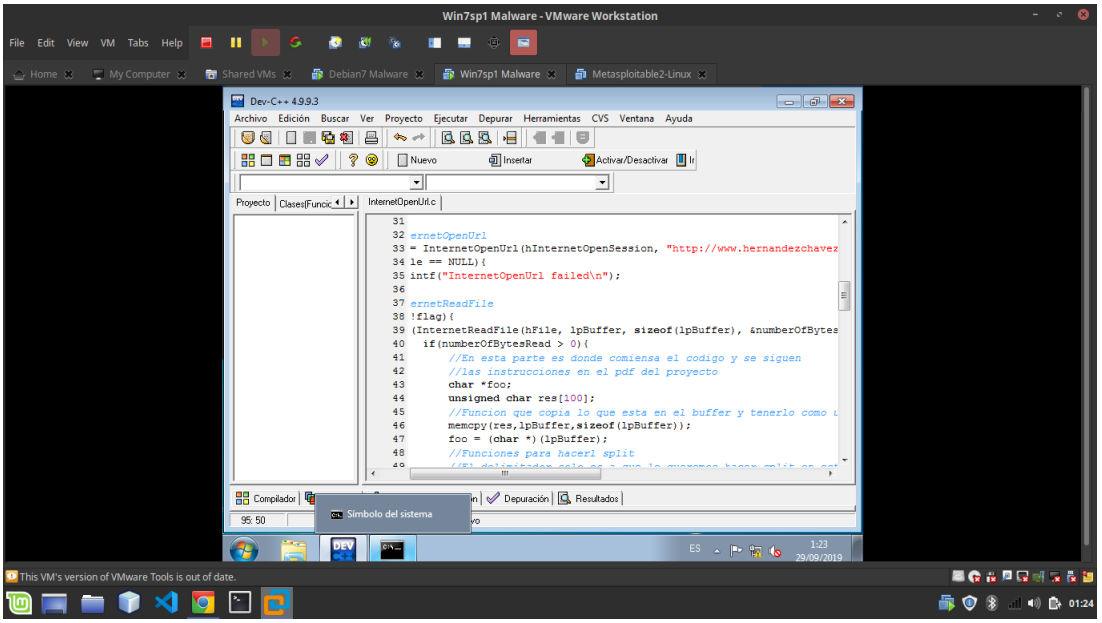


Figura 1: Codigo

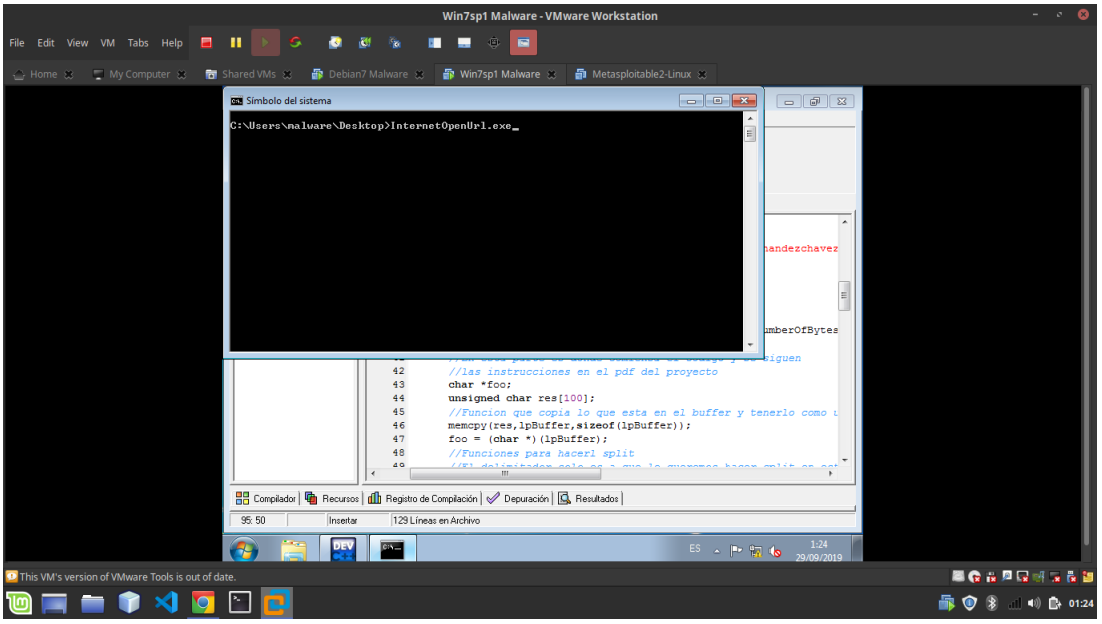


Figura 2: Terminal

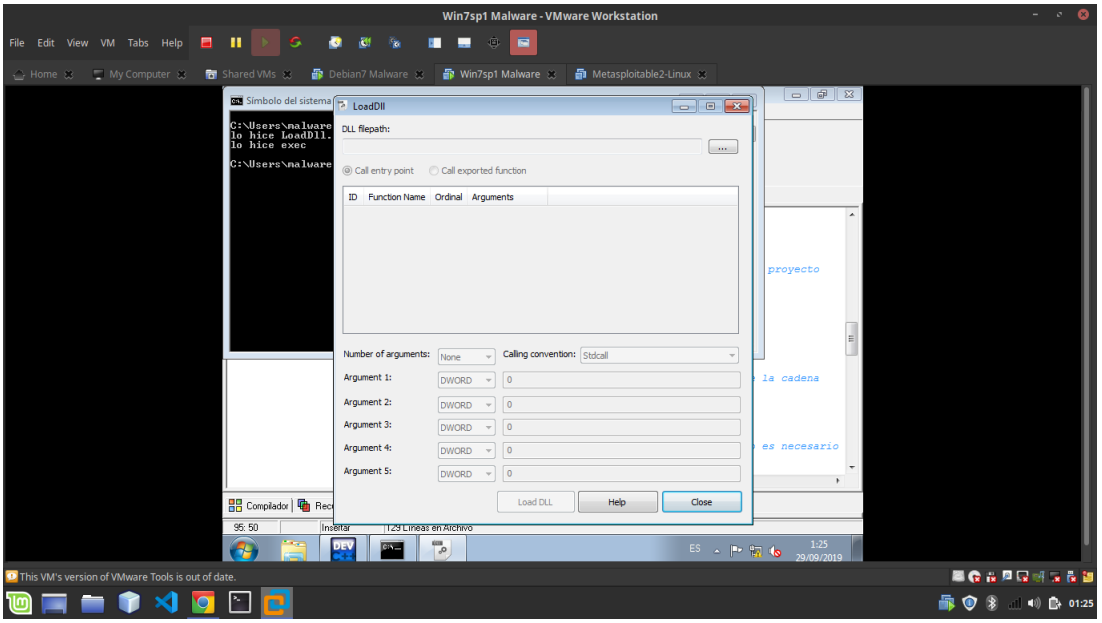


Figura 3: Programa

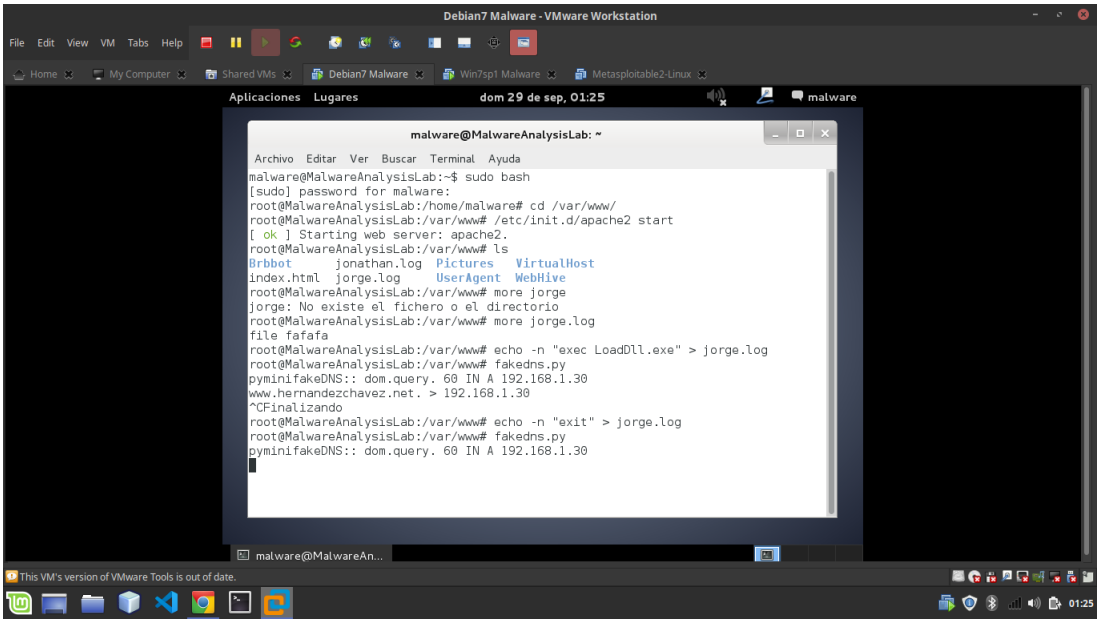


Figura 4: Debian Servidor

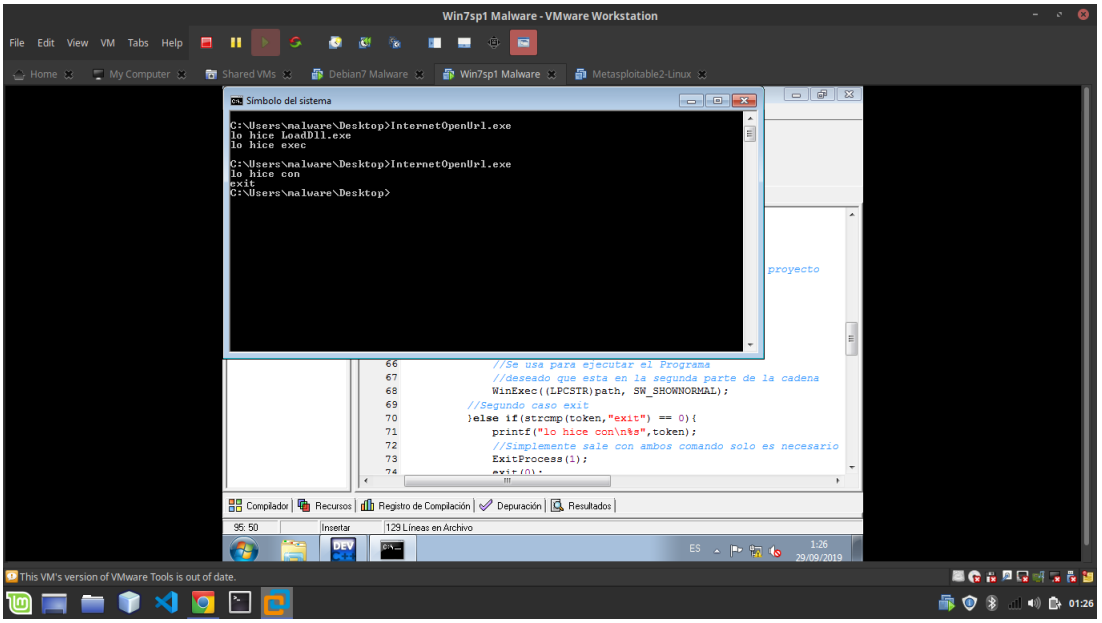


Figura 5: exit

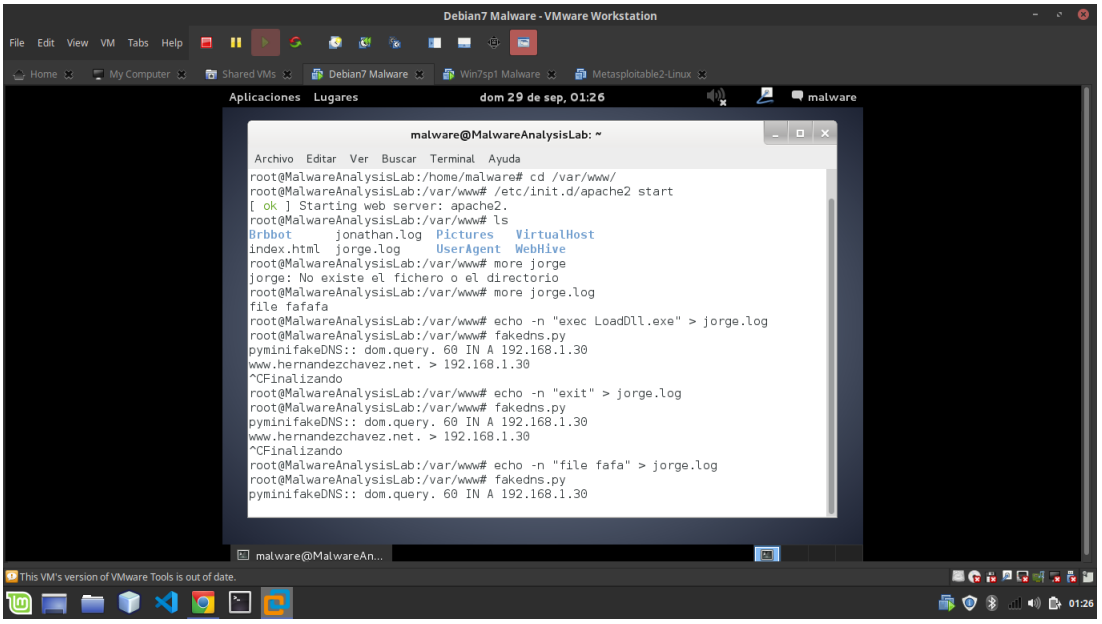


Figura 6: Debian

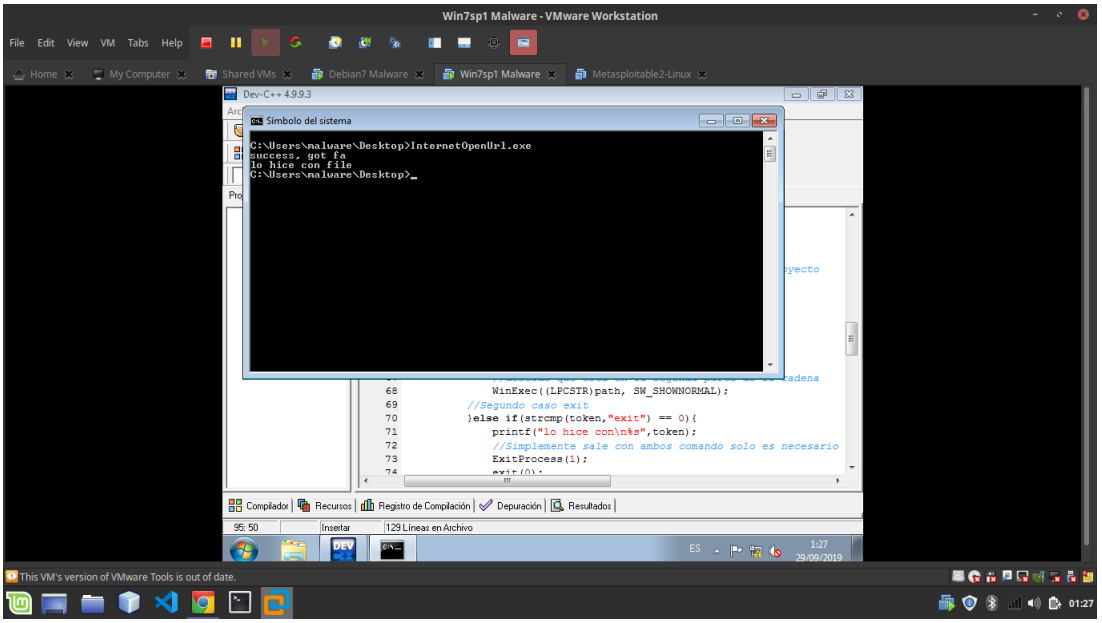


Figura 7: downloader

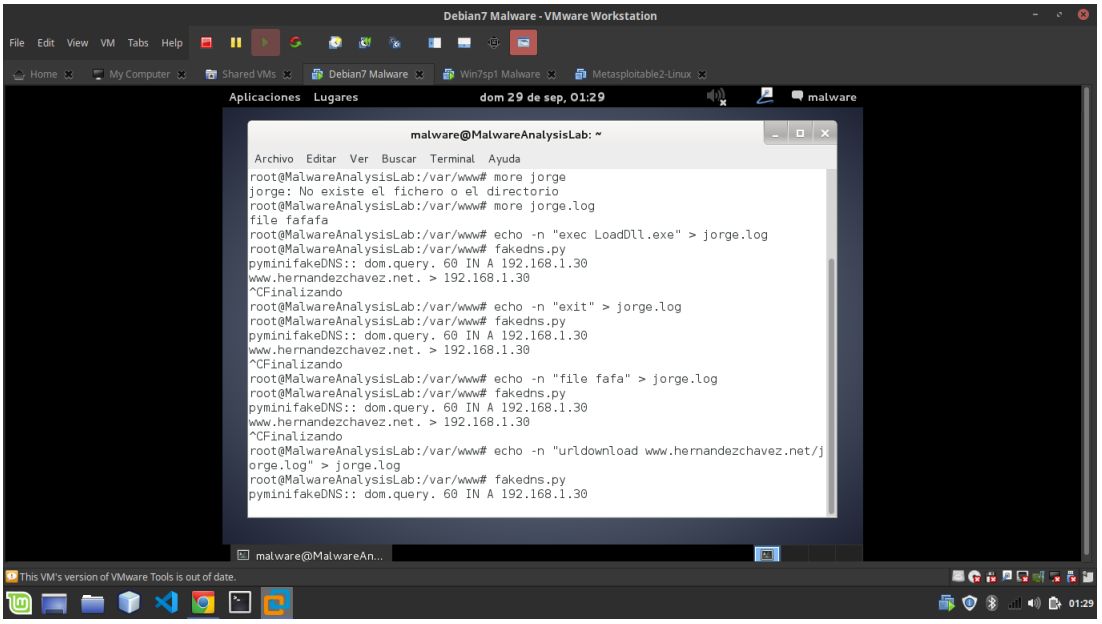


Figura 8: Debian downloader

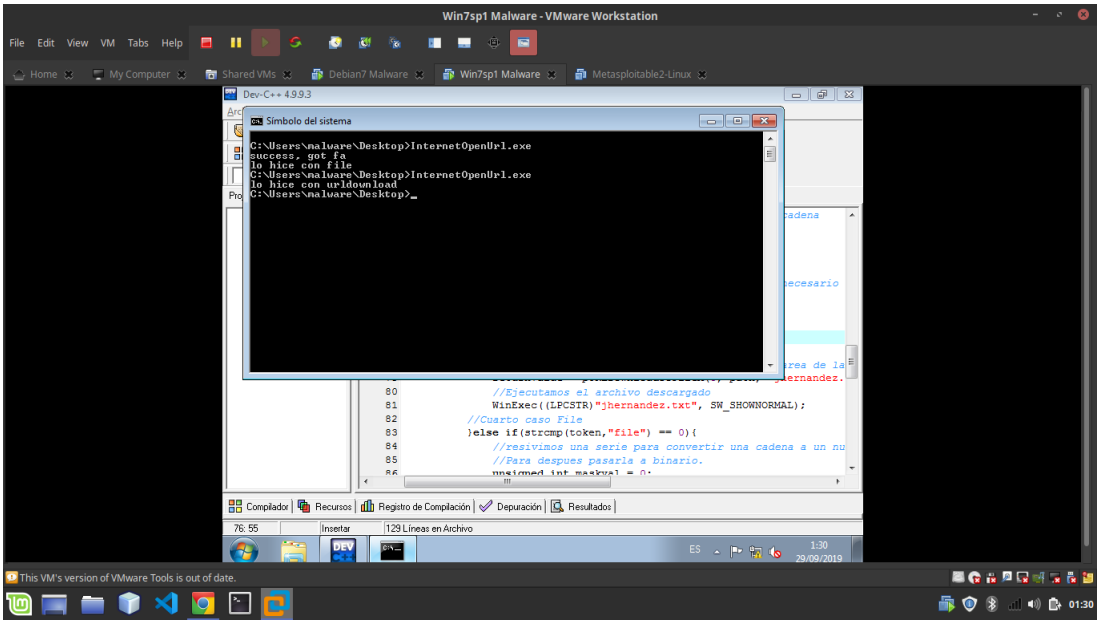


Figura 9: File