

## **El Gobierno de los EE.UU. (y aliados) Utilizan Microsoft Windows Para Atacar a Otras Naciones**

Por el Dr. Roy Schestowitz

Co-autor con G. Forbes

El software propietario es una guerra tecnológica

Resumen: Una débil admisión de Stuxnet ayuda a mostrar que el uso de Windows no garantiza el respeto a la seguridad nacional de otras naciones que los Estados Unidos.

"Veterano Oficial Superior de Defensa atrapado en cobertura de la participación los EE.UU. en Stuxnet" es el tipo de informe que estamos siempre esperando. Además, de exponer no sólo la penosa participación del gobierno en lo que respecta a la tecnología sino que también refuerza el peligro muy real de Windows y por relación todo el software propietario de Microsoft. [Wired ha cubierto este informe especial](#):

*En "CodeWars: La Amenaza Cyber de los Estados Unidos", la corresponsal de Melissa Lee pide a Lynn directa: "¿Los EE.UU. participan en modo alguno en el desarrollo de Stuxnet?"*

*La respuesta de Lynn es lo suficiente larga para que un espectador no atento puede ser que note que no responde a la pregunta.*

*"Los desafíos de Stuxnet, como ya lo he dicho, demuestra la dificultad de atribuir cualquier, cualquier atribución y es algo que todavía estamos viendo, es difícil entrar en cualquier tipo de comentario al respecto hasta que hayamos terminado nuestro examen, "Lynn responde.*

*"Pero señor, yo no le he preguntando si usted piensa que otro país estaba involucrado", presional Lee. "Le estoy preguntando si los EE.UU. estuvo involucrado. Si el Departamento de Defensa estaba involucrado. "*

*"Y esto no es algo que vamos a ser capaces de responder en este momento", dice Lynn finalmente.*

Para mayores antecedentes, véase también:

- [\*\*1. Langner Ralph dice malware de Windows Posiblemente Diseñado para descarrilar programa nuclear de Irán\*\*](#)
- [\*\*2. Los virus de Windows pueden tener una motivación política a veces\*\*](#)
- [\*\*3. ¿Quién necesita Windows Puertas traseras cuando es tan inseguro?\*\*](#)
- [\*\*4. La inseguridad de Windows se convierte en una cuestión política\*\*](#)
- [\*\*5. Windows, Stuxnet y lapidación pública\*\*](#)
- [\*\*6. Stuxnet crece más allá de las infecciones Siemens-Windows\*\*](#)
- [\*\*7. BP ha abandonado ya Windows?\*\*](#)
- [\*\*8. Informes: Apple para la carga de \(Seguridad\) Actualizaciones\*\*](#)
- [\*\*9. Los virus de Windows pueden tener una motivación política a veces\*\*](#)
- [\*\*10. Nueva falla en Windows Facilita Más ataques DDoS\*\*](#)
- [\*\*11. Siemens es malo para la industria, debido en parte a Microsoft\*\*](#)

- [12. Problemas de seguridad de Microsoft en la prensa británica Vista, 7 y Vista no es una panacea](#)
- [13. Negligencia de Microsoft en parches \(las peores Entre todas las empresas\) es la culpable de Stuxnet](#)
- [14. Software de Microsoft: una prueba de Darwin para la incompetencia](#)
- [15. Septiembre malo para la seguridad de Microsoft, Symantec rumores de Compra](#)
- [16. Según Microsoft, Crédito por falta de seguridad](#)
- [17. Muchos Servidores Windows son Abandonados; Minnesota va en la dirección opuesta por Dar Microsoft Sus datos](#)
- [18. Usuarios de Windows Aún bajo el ataque de Stuxnet, Halo, y Zeus](#)
- [19. La propaganda de seguridad de Microsoft: villanos se convierten en héroes](#)
- [20. Problemas de seguridad en IOS y Windows](#)
- [21. Ojo de Seguridad: La propaganda de la BBC, rootkits, y Stuxnet en las instalaciones nucleares de Irán](#)
- [22. Ojo de Seguridad: ClamAV dice que Windows es un virus, Microsoft Compromisos Mac OS X, y Stuxnet se vuelve loco](#)
- [23. Vulnerabilidad del Windows Nucleo en el núcleo de Acción de Gracias, la inseguridad usados para la vigilancia de nuevo](#)
- [24. Cablegate revela el acceso del gobierno requirente de datos de Microsoft, Kill Switches](#)
- [25. El uso de Microsoft Windows Asesina](#)
- [26. Irán muestra el lado negativo de usar software propietario](#)
- [27. Blanqueo defectos inherentes Windows](#)
- [28. Por motivos políticos Software Privativo](#)
- [29. Cuando Windows Mata](#)

Recuerde que la **NSA (Agencia de Seguridad Nacional)**, que también proporcionó estadísticas Web favorables a **Microsoft** hace unos meses, recomendando Vista 7 [[1](#), [2](#), [3](#)], en secreto, porque las puertas traseras son "libres", como en forma gratuita, con todas las ediciones. Los vendidos de **la NSA probablemente le recomendarán Vista 8**, así. Por desgracia para **Microsoft** y la **NSA, Windows** está perdiendo su punto de apoyo. [Cringely escribe sobre como cae su uso](#) en "La Pesadilla de Steve Ballmer":

*Ballmer confirmó en enero que la próxima versión de Windows tiene una versión para ser usada con procesadores ARM, que están instalados principalmente en los teléfonos inteligentes y computadoras de tableta. Se refuerza esta idea, más recientemente, por decirlo explícitamente Windows 8 es ejecutado en todas las plataformas de hardware de Microsoft es compatible actualmente con los teléfonos, llamando a la próxima versión de "Microsoft Windows la más riesgoso todavía."*

*Ballmer está en lo correcto: Windows 8 la hacer o rompe para Microsoft.*

Imagine un mundo donde todo el mundo utilice programas con código fuente que pueda ser auditados. Sin duda, haría que **Microsoft** y algunos de los engaños de la **NSA** imposible de ser mencionados por no decir mucho.

En las noticias de hoy nos encontramos con que "[Corea del Norte \[va\] a tener su propio ordenador portátil](#)" y "sus ordenadores portátiles podrían estar ejecutando "Estrella Roja", un sistema operativo basado en Linux desarrollado por los Nor-Coreanos.