WIKIPEDIA

WANK (computer worm)

The **WANK Worm** was a computer worm that attacked DEC VMS computers in 1989 over the DECnet. It was written in DIGITAL Command Language.[1]
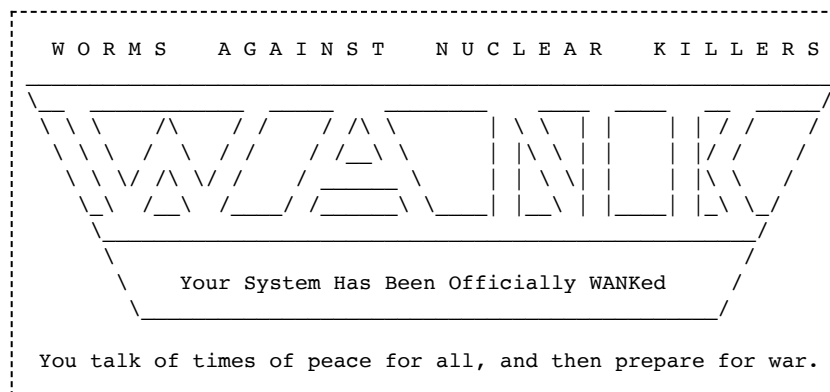
Contents

Origin

The worm is believed to have been created by Melbourne-based hackers, the first to be created by an Australian or Australians. The federal police of Melbourne thought the worm was created by two hackers who used the names Electron and Phoenix.[2] Julian Assange was believed to be involved, but he does not acknowledge this.[3][4]

Political message

The WANK worm had a distinct political message attached, and it was the first major worm to have a political message.[2] WANK in this context stands for Worms Against Nuclear Killers. The following message appeared on infected computer's screen:

```
 W O R M S    A G A I N S T    N U C L E A R    K I L L E R S
 _____
 \__  _____  _____    _____    ____  ____   __  _____/
  \ \ \    /\    / /    / /\ \       |    \ \  | |    | | / /    /
   \ \ \  /  \  / /    / /__\ \      |     \ \ | |    | |/ /    /
    \ \ \/ /\ \/ /    /_____\ \     |      \ \| |    |   <    /
     \_\  /__\  /____/        \ \____|       \ | |____| |\ \__/
      \                                                        /
       \            Your System Has Been Officially WANKed    /
        _____/

 You talk of times of peace for all, and then prepare for war.
```

The worm coincidentally appeared on a DECnet computer network shared between NASA and the US Department of Energy (DOE) days before the launch of a NASA space shuttle carrying the Galileo spacecraft. At the time, there were protests outside the Kennedy Space Center in Florida by anti-nuclear groups regarding the use of the plutonium-based

power modules in Galileo. The protesters contended that if this shuttle blew up "like Challenger did", the plutonium spilled would cause widespread death to residents of Florida.

The worm propagated through the network pseudo-randomly from one system to the other by using an algorithm which converted the victim machine's system time into a candidate target node address (composed of a DECnet Area and Node number) and subsequently attempted to exploit weakly secured accounts such as SYSTEM and DECNET that had password identical to the usernames. The worm did not attack computers within DECnet area 48, which was New Zealand. A comment inside the worm source code at the point of this branch logic indicated that New Zealand was a nuclear-free zone. New Zealand had recently forbidden U.S. nuclear-powered vessels from docking at its harbours, thus further fueling the speculation inside NASA that the worm attack was related to the anti-nuclear protest.[5] The line "You talk of times of peace for all, and then prepare for war" is drawn from the lyrics of the Midnight Oil song "Blossom and Blood". Midnight Oil are an Australian rock band known for their political activism and opposition to both nuclear power and nuclear weapons. The process name of the second version of the worm to be detected was "oilz", an Australian shorthand term for the band.[6]

Playful nature

The DECnet network affected was jointly operated between the NASA Space Physics Analysis Network (SPAN) and the Department of Energy's High Energy Physics Network (HEPnet). The only separation between the networks was a prearranged division of network addresses (DECnet "Areas"). Thus, the worm, by picking a random target address, could affect both networks equally. The worm code included 100 common VAX usernames that were hard-coded into its source code. In addition to its political message, the worm contained several features of an apparently playful nature. The words "wank" and "wanked" are slang terms used in many countries to refer to masturbation. In addition, the worm contained "over sixty" randomizable messages that it would display to users, including "Vote anarchist" and "The FBI is watching YOU". The worm was also programmed to trick users into believing that files were being deleted by displaying a file deletion dialogue that could not be aborted, though no files were actually erased by the worm.

anti-WANK and WANK_SHOT

R. Kevin Oberman (from DOE) and John McMahon (from NASA) wrote separate versions of an anti-WANK procedure and deployed them into their respective networks. It exploited the fact that before infecting a system, WANK would check for `NETW_(random number)`, that is a copy of its own, in the process table. If one was found, the worm would destroy itself. When anti-WANK was run on a non-infected system, it would create a process named `NETW_(random number)` and just sit there. anti-WANK only worked against the earlier version of the worm, though, because the process name of the worm in a later version was changed to `OILZ`.

Bernard Perrot of the Institut de Physique Nucléaire in Orsay wrote a second program. The worm was trained to go after the RIGHTSLIST database, the list of all the people who have accounts on the computer. By renaming the database and putting a dummy database in its place, the worm would, in theory, go after the dummy, which could be designed with a hidden bomb. Ron Tencati, the SPAN Security Manager, obtained a copy of the French manager's worm-killing program and gave it to McMahon, who tested it. It was then distributed to system administrators of both networks to be installed onto their computers. It still took weeks for the worm to be completely erased from the network.

See also

- Father Christmas (computer worm)

References

1. JULIAN ASSANGE 2006 "The Anti-Nuclear WANK Worm" http://www.counterpunch.org/2006/11/25/the-curious-origins-of-political-hacktivism/

2. Dreyfus, Suelette. "Introduction" (http://www.xs4all.nl/~suelette/underground/justin/introduction.html), *Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier*, Mandarin Australia, 1997.

3. Bernard Lagan, "International man of mystery," (http://www.smh.com.au/technology/technology-news/international-man-of-mystery-20100409-ryvf.html) *The Sydney Morning Herald*, 10 April 2010. Retrieved 17 March 2014.

4. David Leigh and Luke Harding, *WikiLeaks: Inside Julian Assange's War on Secrecy* (2011) p. 42.

5. Dreyfus 1997, Chapter 1 (http://www.xs4all.nl/~suelette/underground/justin/chapter_1.html).

6. Dreyfus, Suelette. "Computer Hackers: juvenile delinquents or international saboteurs?" (http://www.aic.gov.au/events/aic%20upcoming%20events/1998/~/media/conferences/internet/dreyfus.ashx), presented at the conference: Internet Crime held in Melbourne, 16–17 February 1998, by the Australian Institute of Criminology

External links

- CERT advisory (http://www.cert.org/advisories/CA-1989-04.html)
- Advisory from Virus Test Center, University of Hamburg, Germany (http://agn-www.informatik.uni-hamburg.de/catalog/vms/html/wank_wor.htm)
- Dreyfus, Suelette; Assange, Julian (June 1997). *Underground* (http://www.underground-book.net/). Random House Australia. ISBN 1863305955.
- Norman, James (2003-05-25). "Hack to the future" (http://www.theage.com.au/articles/2003/05/24/1053585748340.html). *The Age*.
- "Juvenile Delinquents or International Saboteurs?" (http://www.aic.gov.au/events/aic%20upcoming%20events/1998/~/media/conferences/internet/dreyfus.ashx) presented by Suelette Dreyfus at the Internet Crime conference held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology
- Darby, Tom; Schmidt, Charles. "The history of worm like programs" (http://snowplow.org/tom/worm/history.html). *The Morris Internet Worm*.
- "Hacktivism and Politically Motivated Computer Crime" (https://web.archive.org/web/20080227132540/http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf) - Written by one of the Digital Equipment Corporation investigators; disputes the WANK worm had any political motivation but was rather a play on the British meaning of the word "wank"