Sony Rootkit Malware

Debbie Ogidan

AGENDA

- Who Sony is?
- Background
- Attack: Detailed description
- After the attack
- Questions

SONY

- Sony BMG was an American record company owned 50-50 by Sony Corporation of America and Bertelsmann.

- Sony is a big manufacturer of audio, video, game, communications and tech products(sony music,pictures).

SONY

Background

Copy protection implemented on about 22 million CDs.

When inserted into a computer,the CDs installed one of two pieces software that provided a form of DRM by modifying the OS to interfere with CD copying: 2 million contained XCP installed on Windows and other 20 had MediaMax CD-3 installed on Mac OS X . However, Mac OS X asked user for more information when the software tried to modify the OS.

One of the programs would install a phone home which gives reports on the user even if the user refuses the EULA while the other program was not mentioned at all.

Programs contained code from several pieces of copylefted free software

Both programs configured the OS to hide the software's existence(rootkits).

XCP Rootkit

- Scandal erupted on October 2005 when Winternals researcher named Mark posted the tech analysis of F4I's XCP on his blog
- He ascertained the fact about a software being installed on his computer by a sony BMG music CD.
- He compared it to a rootkit and noted the fact that the EULA does not mention the software.
- He asserted that the software is illegitimate and that DRM had "gone too far".

Problems with XCP

- Creates security holes that can be exploited by malicious software(worms/viruses). People even used it to cheat in online games.
- Constantly runs in the background consuming sys resources with or without CD in it
- Employs safe procedure to start and stop: can lead to system crashes.
- No uninstaller and attempt to can cause OS to not recognize existing drives.

After

- Sony released software to remove rootkit component of XCP from Windows computer.
- Russinovich analyzed it again and saw that it created more security problems about privacy.
- Removal program only unmasked the files installed by rootkit but did not remove it.
- In November, Sony provided a “new and improved” removal tool to remove rootkit from windows computer.
- With MediaMax CD-3, and XCP, sony instructed all retailers to remove unsold music discs from their shelves.
- Estimated impact by security experts was determined to be about 500,000 networks.
- Reuters reported that Sony BMG would exchange affected CDs for new unprotected disks as well as unprotected MP3 files.
- Despite the recall, CDs were still for sale in New York city music retail outlets and Boston.

After

- As of May 2006, the Sony BMG's website offered consumers a link to "Class action settlement" regarding XCP and MediaMax with a deadline to submit a claim.
- Texas was the first state to bring legal action against Sony BMG group($75,000)
- New York and California class action suits against Sony($7.50 per purchase of a CD)
- Other actions: Italy, Federal Trade Commission

References

Sony BMG copy protection rootkit scandal. (2005, November 16). Wikipedia, the free encyclopedia. Retrieved November 18, 2021, from https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

Brown, B. (n.d.). *Sony BMG Rootkit scandal: 10 years later*. CSO Online. https://www.csoonline.com/article/2998952/sony-bmg-rootkit-scandal-10-years-later.html

Questions?

Thank You