Microsoft, the NSA, and GitHub

By *Roy Schestowitz*
Created *05/07/2018 - 7:23am*
Submitted by Roy Schestowitz on Thursday 5th of July 2018 07:23:07 AM Filed under Gentoo [1] Microsoft [2] Security [3]

- **Gentoo hacker's code changes unlikely to have worked [4]**

  Linux distribution Gentoo's maintainers say attempts by attackers last week to sabotage code stored on Github is unlikely to have worked.

  Gentoo's Github account was compromised in late June.

  The attacker was able to gain administrative privileges for Gentoo's Github account, after guessing the password for it.

  Gentoo's maintainers were alerted to the attack early thanks to the attacker removing all developers from the Github account, causing them to be emailed.

- **NSA Exploit "DoublePulsar" Patched to Work on Windows IoT Systems [5]**

  An infosec researcher who uses the online pseudonym of Capt. Meelo has modified an NSA hacking tool known as DoublePulsar to work on the Windows IoT operating system (formerly known as Windows Embedded).

The original DoublePulsar is a hacking tool that was developed by the US National Security Agency (NSA), and was stolen and then leaked online by a hacking group known as The Shadow Brokers.

At its core, DoublePulsar is a Ring-0 kernel mode payload that acts like a backdoor into compromised systems. DoublePulsar is not meant to be used on its own, but together with other NSA tools.

- **Predictable password blamed for Gentoo GitHub organisation takeover [6] [Ed: when Microsoft takes over the NSA gets all these passwords. (NSA PRISM)]**

  Gentoo has laid out the cause and impact of an attack that saw the Linux distribution locked out of its GitHub organisation.

  The attack took place on June 28, and saw Gentoo unable to use GitHub for approximately five days.

  Due a lack of two-factor authentication, once the attacker guessed an admin's password, the organisation was in trouble.

Gentoo Microsoft Security

Source URL: http://www.tuxmachines.org/node/113249

Links:
[1] http://www.tuxmachines.org/taxonomy/term/109
[2] http://www.tuxmachines.org/taxonomy/term/62
[3] http://www.tuxmachines.org/taxonomy/term/59
[4] https://www.itnews.com.au/news/gentoo-hackers-code-changes-unlikely-to-have-worked-496919
[5] https://www.bleepingcomputer.com/news/security/nsa-exploit-doublepulsar-patched-to-work-on-windows-iot-systems/
[6] https://www.zdnet.com/article/predictable-password-blamed-for-gentoo-github-organisation-takeover/