Nitol botnet

By Contributors to Wikimedia projects

Published: 2012-12-27 · Archived: 2026-04-02 11:25:52 UTC

From Wikipedia, the free encyclopedia

The **Nitol botnet** mostly involved in spreading malware and distributed denial-of-service attacks.

The Nitol Botnet was first discovered around December 2012, with analysis of the botnet indicating that the botnet is mostly prevalent in China where an estimate 85% of the infections are detected. In China the botnet was found to be present on systems that came brand-new from the factory, indicating the trojan was installed somewhere during the assembly and manufacturing process. According to Microsoft the systems at risk also contained a counterfeit installation of Microsoft Windows.

On 10 September 2012 Microsoft took action against the Nitol Botnet by obtaining a court order and subsequently sinkholing the 3322.org domain.[1] The 3322.org domain is a Dynamic DNS which was used by the botnet creators as a command and control infrastructure for controlling their botnet. Microsoft later settled with 3322.org operator Pen Yong, which allowed the latter to continue operating the domain on the condition that any subdomains linked to malware remain sinkholed.[2]

- Internet crime
- Internet security

1. ^ *Leyden, John (13 September 2012). "Microsoft seizes Chinese dot-org to kill Nitol bot army". The Register. Retrieved 27 December 2012.*
2. ^ *Leyden, John (4 October 2012). "Chinese Nitol botnet host back up after Microsoft settles lawsuit". The Register. Retrieved 27 December 2012.*

- Analysis of the Nitol Botnet, created by Microsoft as part of Operation b70
