Agent.BTZ

By Contributors to Wikimedia projects

Published: 2014-03-03 · Archived: 2026-04-05 22:41:06 UTC

From Wikipedia, the free encyclopedia

This article is about the worm. For the Trojan infecting Windows, Android, and other operating systems, see Agent.AWF.

Agent.BTZ	
Malware details	
Technical name	• W32/Autorun.worm.dw (McAfee) • Worm:W32/Agent.BTZ(F-Secure)
Type	Worm
Origin	Russia
Technical details	
Written in	x86 ASM

Agent.BTZ, also named **Autorun**,[1][2] is a computer worm that infects USB flash drives with spyware. A variant of the **SillyFDC** worm,[3] it was used in the massive 2008 cyberattack on the US military, infecting 300,000 computers.

Technical description

[edit]

The Agent.BTZ worm is a DLL file, written in x86-32 assembly language.[4] It spreads by creating an AUTORUN.INF file to the root of each drive with the DLL file.[5] It has the ability "to scan computers for data, open backdoors, and send through those backdoors to a remote command and control server."[3]

In 2008, at a US military base in the Middle East, a USB flash drive infected with Agent.BTZ was inserted into a laptop attached to United States Central Command. From there it spread undetected to other systems, both classified and unclassified.[6] In order to try to stop the spread of the worm, the Pentagon banned USB drives and removable media devices. They also disabled the Windows autorun feature on their computers.[3] The Pentagon spent nearly 14 months cleaning the worm from military networks.[3]

Chinese hackers were thought to be behind the attack because they had used the same code that made up Agent.BTZ in previous attacks.[7] According to an article in *The Economist*, "it is not clear that agent.btz was designed specifically to target military networks, or indeed that it comes from either Russia or China."[8] An article in the *Los Angeles Times* reported that US defense officials described the malicious software as "apparently designed specifically to target military networks." It's "thought to be from inside Russia", although it was not clear "whether the destructive program was created by an individual hacker or whether the Russian government may have had some involvement."[9]

In 2010, American journalist Noah Shachtman wrote an article to investigate the theory that the worm was written by a single hacker.[3] Later analyses by Kaspersky Lab found relations to other spyware, including Red October, Turla, and Flame.[10]

In December 2016, the United States FBI and DHS issued a Joint Analysis Report which included attribution of Agent.BTZ to one or more "Russian civilian and military intelligence Services (RIS)."[11]

1. ^ *Shevchenko, Sergei (30 November 2008). "Agent.btz - A Threat That Hit Pentagon". ThreatExpert Blog. Retrieved 14 December 2016.*
2. ^ *"W32/Autorun.worm.dw - Malware". McAfee Labs Threat Center. 21 November 2008. Retrieved 14 December 2016.*
3. ^ Jump up to: ***a b c d e*** *Shachtman, Noah (25 August 2010). "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack". Wired. Retrieved 14 December 2016.*
4. ^ *"Agent.BTZ - Virus Information". Panda Security. Retrieved 14 December 2016.*
5. ^ *"Worm:W32/Agent.BTZ Description". F-Secure Labs. Retrieved 14 December 2016.*
6. ^ *William J. Lynn III. "Defending a New Domain". Foreign Affairs. Retrieved 2010-08-25.*
7. ^ *Leyden, John (20 November 2008). "US Army bans USB devices to contain worm". The Register. Retrieved 14 December 2016.*
8. ^ *"The worm turns". The Economist. 4 December 2008. Retrieved 14 December 2016.*
9. ^ *Barnes, Julian E. (28 November 2008). "Pentagon computer networks attacked". Los Angeles Times. Retrieved 14 December 2016.*
10. ^ *Gostev, Alexander (12 March 2014). "Agent.btz: a Source of Inspiration?". Securelist. Retrieved 19 May 2020.*
11. ^ *"GRIZZLY STEPPE – Russian Malicious Cyber Activity" (PDF). US CERT. Retrieved 2 March 2017.*

Source: https://en.wikipedia.org/wiki/Agent.BTZ