Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:14:10 UTC

Tool: Agent.BTZ

Names	Agent.BTZ Minit Chinch Sun rootkit
Category	Malware
Type	Backdoor, Rootkit
Description	(Kaspersky) The story of Agent.btz began back in 2007 and was extensively covered by the mass media in late 2008 when it was used to infect US military networks. Here is what Wikipedia has to say about it: “The 2008 cyberattack on the United States was the ‘worst breach of U.S. military computers in history’. The defense against the attack was named ‘Operation Buckshot Yankee’. It led to the creation of the United States Cyber Command. It started when a USB flash drive infected by a foreign intelligence agency was left in the parking lot of a Department of Defense facility at a base in the Middle East. It contained malicious code and was put into a USB port from a laptop computer that was attached to United States Central Command.
Information	<https://securelist.com/agent-btz-a-source-of-inspiration/58551/> <http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html> <http://www.intezer.com/new-variants-of-agent-btz-comrat-found/> <http://www.intezer.com/new-variants-of-agent-btz-comrat-found-part-2/> <https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/> <https://en.wikipedia.org/wiki/Agent.BTZ>
MITRE ATT&CK	<https://attack.mitre.org/software/S0092/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_btz>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:agent.btz>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Agent.BTZ

Changed	Name	Country	Observed	
APT groups				
	Turla, Waterbug, Venomous Bear		1996-2024	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d20d0064-ff8e-44e3-a55f-e4b54d53a357