Agent.btz, Software S0092 | MITRE ATT&CK®

Archived: 2026-04-05 15:53:43 UTC

Domain	ID		Name	Use
Enterprise	T1560	.003	Archive Collected Data: Archive via Custom Method	Agent.btz saves system information into an XML file that is then XOR-encoded.[2]
Enterprise	T1052	.001	Exfiltration Over Physical Medium: Exfiltration over USB	Agent.btz creates a file named thumb.dd on all USB flash drives connected to the victim. This file contains information about the infected system and activity logs.[1]
Enterprise	T1105		Ingress Tool Transfer	Agent.btz attempts to download an encrypted binary from a specified domain.[2]
Enterprise	T1091		Replication Through Removable Media	Agent.btz drops itself onto removable media devices and creates an autorun.inf file with an instruction to run that file. When the device is inserted into another system, it opens autorun.inf and loads the malware.[2]
Enterprise	T1016		System Network Configuration Discovery	Agent.btz collects the network adapter's IP and MAC address as well as IP addresses of the network adapter's default gateway, primary/secondary WINS, DHCP, and DNS servers, and saves them into a log file.[2]
Enterprise	T1033		System Owner/User Discovery	Agent.btz obtains the victim username and saves it to a file.[2]

Source: https://attack.mitre.org/software/S0092/