Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:53:51 UTC

Tool: Buran

Names	Buran VegaLocker Vega
Category	Malware
Type	Ransomware
Description	(ESET) The component that first attracted our attention is the previously unseen Win32/Filecoder.Buran. It is a Delphi binary that sometimes comes packed. It was mainly distributed during February and March of 2019. It implements the expected behavior of ransomware, discovering local drives and network shares and encrypting files found on these devices. It doesn't require an internet connection to encrypt its victims' files, since it doesn't communicate with a server to send the encryption keys. Instead, it appends a "token" at the end of the ransom message and demands that the victims communicate with the operators via email or Bitmessage. To encrypt as many important resources as possible, Filecoder.Buran starts a thread dedicated to killing key software that might have open handles on files containing valuable data, thus preventing them being encrypted. The targeted processes are mainly database management systems (DBMS). Furthermore, Filecoder.Buran removes log files and backups, to make it as difficult as possible for victims without any offline backups to recover their files.
Information	<https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.vegalocker>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Buran

Changed	Name	Country	Observed	
APT groups				
	TA2101, Maze Team	[Unknown]	2019-Feb 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a9995f6b-30ae-4e92-8fbf-60375500b7db