Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:30:25 UTC

Tool: CryptoWall

Names	CryptoWall
Category	Malware
Type	Ransomware
Description	(SecureWorks) After the emergence of the infamous CryptoLocker ransomware in September 2013, CTU researchers observed an increasing number of ransomware families that destroyed data in addition to demanding payment from victims. While similar threats have existed for years, this tactic did not become widespread until CryptoLocker's considerable success. Traditionally, ransomware disabled victims' access to their computers through non-destructive means until the victims paid for the computers' release. Early CryptoWall variants closely mimicked both the behavior and appearance of the genuine CryptoLocker. The exact infection vector of these early infections is not known as of this publication, but anecdotal reports from victims suggest the malware arrived as an email attachment or drive-by download. Evidence collected by CTU researchers in the first several days of the February 2014 campaign showed at least several thousand global infections.
Information	<https://www.secureworks.com/research/cryptowall-ransomware>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowall>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool CryptoWall

Changed	Name	Country	Observed	
APT groups				
	TA530	[Unknown]	2016-Nov 2016	

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