Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:39:02 UTC

Tool: BitPaymer

Names	BitPaymer FriedEx IEncrypt wp_encrypt
Category	Malware
Type	Ransomware, Credential stealer, Big Game Hunting
Description	(IBM) The submitted file is a custom packed BitPaymer ransomware loader that is designed to run on Windows 7 or above or any version of Windows server. The loader uses Alternate Data Streams to hide its tracks and service hijacking to maintain persistence. The loader uses RC4 to decrypt its configuration data. The BitPaymer ransomware is used to encrypt files based on the settings from the configuration data. It has the ability to encrypt local and remote disks and can whitelist various file types that are not to be encrypted. The ransom note follows the same general outline as that of other ransomware families; however, BitPaymer is customized to the company or victim being attacked and contains their names in the configuration data itself.
Information	<https://exchange.xforce.ibmcloud.com/malware-analysis/guid:14521d85c16836ad5e8cd7176a9f5003> <https://nakedsecurity.sophos.com/2017/09/21/how-bitpaymer-ransomware-covers-its-tracks/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/> <https://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework> <https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec/> <https://cyware.com/news/bitpaymer-ransomware-an-insight-into-the-ransomwares-attack-campaigns-ced9027b> <https://lifars.com/2019/11/analysis-of-dridex-bitpaymer-and-doppelpaymer-campaign/> <https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-

	dridex-authors/> <https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0570/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.friedex>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Bitpaymer>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool BitPaymer

Changed	Name	Country	Observed	
APT groups				
	Indrik Spider		2007-Oct 2024	

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

↑