Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:47:46 UTC

Tool: Erebus

Names	Erebus
Category	Exploits
Type	Ransomware
Description	(Trend Micro) Erebus ransomware (RANSOM_EREBUS.A) first emerged last September 2016 being distributed by malvertisements (malicious advertisements). The malicious ads diverted victims to the Rig exploit kit, which infects the victim's systems with the ransomware. This Erebus variant targets 423 file types, scrambles files with RSA-2048 encryption algorithm, and appends the affected files with the .ecrypt extension. This version of Erebus was observed using compromised websites in South Korea as its command and control (C&C) servers.
Information	<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures> <https://blog.trendmicro.com/trendlabs-security-intelligence/erebus-resurfaces-as-linux-ransomware/> <https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.erebus> <https://malpedia.caad.fkie.fraunhofer.de/details/win.erebus>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:erebus>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Erebus

Changed	Name	Country	Observed

APT groups

	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2436d99d-14a6-427a-839b-856c5f3d902c