Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:34:16 UTC

Tool: WastedLocker

Names	WastedLocker
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Fox-IT) The new WastedLocker ransomware appeared in May 2020 (a technical description is included below). The ransomware name is derived from the filename it creates which includes an abbreviation of the victim's name and the string 'wasted'. The abbreviation of the victim's name was also seen in BitPaymer, although a larger portion of the organisation name was used in BitPaymer and individual letters were sometimes replaced by similar looking numbers. Technically, WastedLocker does not have much in common with BitPaymer, apart from the fact that it appears that victim specific elements are added using a specific builder rather than at compile time, which is similar to BitPaymer. Some similarities were also noted in the ransom note generated by the two pieces of malware. The first WastedLocker example we found contained the victim name as in BitPaymer ransom notes and also included both a protonmail.com and tutanota.com email address. Later versions also contained other Protonmail and Tutanota email domains, as well as Eclipso and Airmail email addresses. Interestingly the user parts of the email addresses listed in the ransom messages are numeric (usually 5 digit numbers) which is similar to the 6 to 12 digit numbers seen used by BitPaymer in 2018.
Information	<https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us> <https://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html> <https://labs.sentinelone.com/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/> <https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/> <https://unit42.paloaltonetworks.com/wastedlocker/>

	<https://securelist.com/wastedlocker-technical-analysis/97944/> <https://news.sophos.com/en-us/2020/08/04/wastedlocker-techniques-point-to-a-familiar-heritage/> <https://www.csoonline.com/article/3574907/wastedlocker-explained-how-this-targeted-ransomware-extorts-millions-from-victims.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0612/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.wastedlocker>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=wastedlocker-ransomware>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool WastedLocker

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d718aaef-4608-46fd-8245-a6036ebf54f2