Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:09:55 UTC

Tool: Defray777

Names	Defray777 Defray Defray 2018 Target777 Ransom X RansomExx Glushkov
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Palo Alto) Defray777 is an elusive family of ransomware also known as Ransom X and RansomExx. Although it has recently been covered in the news as a new family, it has been in use since at least 2018 and is responsible for a number of high-profile ransomware incidents -- as detailed in the articles we linked to. Defray777 runs entirely in memory, which is why there have been so few publicly discussed samples to date. In several recent incidents, Defray777 was loaded into memory and executed by Cobalt Strike, which was delivered by the Vatet loader.
Information	<https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3/> <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries> <https://www.csoonline.com/article/3604599/sprite-spider-emerging-as-one-of-the-most-destructive-ransomware-threat-actors.html> <https://blogs.vmware.com/networkvirtualization/2021/03/deconstructing-defray777.html/> <https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware> <https://blogs.blackberry.com/en/2017/09/cylance-vs-defray-ransomware> <https://securityintelligence.com/posts/ransomexx-upgrades-rust/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.defray>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:defray777>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Defray777

Changed	Name	Country	Observed	
APT groups				
	Sprite Spider, Gold Dupont	[Unknown]	2015-Nov 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ec6a3a6f-e491-4831-a92f-7fd13b93331f