Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:27:20 UTC

Tool: Ramnit

Names	Ramnit Nimnul
Category	Malware
Type	Banking trojan, Credential stealer, Info stealer, Exfiltration
Description	(Cybereason) The Ramnit Trojan is a type of malware able to exfiltrate sensitive data. This kind of data can include anything ranging from banking credentials, FTP passwords, session cookies, and personal data. Leaking this information can easily destroy user trust in a business, and in the process lose customers and ruin reputations. Luckily, our onboarding was timely, and was able to detect the trojan just as it was beginning to exfiltrate information. Our customer used our remediation tool immediately to stop the exfiltration in its tracks.
Information	<https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan> <https://malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/> <http://www.nao-sec.org/2018/01/analyzing-ramnit-used-in-seamless.html> <http://contagiodump.blogspot.com/2012/01/blackhole-ramnit-samples-and-analysis.html> <https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/> <https://research.checkpoint.com/ramnits-network-proxy-servers/> <http://www.vkremez.com/2018/02/deeper-dive-into-ramnit-banker-vnc-ifsb.html> <https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/w32-ramnit-analysis-15-en.pdf> <https://securityintelligence.com/posts/ramnit-banking-trojan-stealing-card-data/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ramnit>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Ramnit>

Last change to this tool card: 03 February 2022

Download this tool card in JSON format

All groups using tool Ramnit

Changed	Name	Country	Observed	
Other groups				
	TA554	[Unknown]	2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=662b809d-91d0-4190-b58d-b9080d2f70c3