Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:05:36 UTC

Tool: BadRabbit

Names	BadRabbit
Category	Malware
Type	Ransomware
Description	(Talos) There have been several large scale ransomware campaigns over the last several months. This appears to have some similarities to NotPetya in that it is also based on Petya ransomware. Major portions of the code appear to have been rewritten. The distribution does not appear to have the sophistication of the supply chain attacks we have seen recently. Despite initial reports, we currently have no evidence that the EternalBlue exploit is being leveraged. However, we identified the usage of the EternalRomance exploit to propagate in the network. This exploit takes advantage of a vulnerability described in the Microsoft MS17-010 security bulletin. The vulnerability was also exploited during the Nyetya campaign.
Information	<https://blog.talosintelligence.com/2017/10/bad-rabbit.html> <https://www.riskiq.com/blog/labs/badrabbit/> <https://www.fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat.html> <https://www.reversinglabs.com/newsroom/news/reversinglabs-yara-rule-detects-badrabbit-encryption-routine-specifics.html> <https://securelist.com/bad-rabbit-ransomware/82851/> <https://labsblog.f-secure.com/2017/10/27/the-big-difference-with-bad-rabbit/> <https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/> <http://www.intezer.com/notpetya-returns-bad-rabbit/> <https://www.dropbox.com/s/tb8qmb98082p9e7/Whitepaper%20BadRabbit%20Ransomware.pdf?dl=0>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:badrabbit>

Last change to this tool card: 21 May 2020

Download this tool card in JSON format

All groups using tool BadRabbit

Changed	Name	Country	Observed	
APT groups				
	TeleBots		2015-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d8583406-a007-40a0-97a4-217300e1529f