Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:49:10 UTC

Tool: NotPetya

Names	NotPetya EternalPetya ExPetr Pnyetya Petna Nyetya NonPetya nPetya Petrwrap Diskcoder.C GoldenEye
Category	Malware
Type	Ransomware, Wiper, Worm, Remote command
Description	(US-CERT) On June 27, 2017, NCCIC was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list. Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods. NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below: • PsExec - a legitimate Windows administration tool • WMI - Windows Management Instrumentation, a legitimate Windows component • EternalBlue - the same Windows SMBv1 exploit used by WannaCry • EternalRomance - another Windows SMBv1 exploit
Information	<https://www.us-cert.gov/ncas/alerts/TA17-181A> <https://securelist.com/from-blackenergy-to-expetr/78937/> <https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-

b85626af34ef_story.html>
<https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/>
<https://labsblog.f-secure.com/2017/06/30/eternal-petya-from-a-developers-perspective/>
<https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>
<https://threatpost.com/ukrainian-man-arrested-charged-in-notpetya-distribution/127391/>
<http://blog.erratasec.com/2017/06/nonpetya-no-evidence-it-was-smokescreen.html>
<https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/>
<https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/september/eternalglue-part-one-rebuilding-notpetya-to-assess-real-world-resilience/>
<https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-yet-another-stolen-piece-package/>
<https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/>
<https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik>
<https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/>
<https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/>
<https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b>
<http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>
<https://securelist.com/schroedingers-petya/78870/>
<https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/>
<https://www.bleepingcomputer.com/news/security/ransomware-attacks-continue-in-ukraine-with-mysterious-wannacry-clone/>
<https://www.gdatasoftware.com/blog/2017/07/29859-who-is-behind-petna>
<https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4>
<https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/>
<https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/>
<https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/>
<https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/>
<https://tisiphone.net/2017/06/28/why-notpetya-kept-me-awake-you-should-worry-too/>
<https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/>
<https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out/>

	<https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/> <https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/> <https://www.dropbox.com/s/hksfa7zzc17jgrq/Whitepaper%20Petya%20Ransomware.pdf?dl=0>
MITRE ATT&CK	<https://attack.mitre.org/software/S0368/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.eternal_petya> <https://malpedia.caad.fkie.fraunhofer.de/details/win.petya>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:notpetya>

Last change to this tool card: 21 May 2020

Download this tool card in JSON format

All groups using tool NotPetya

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=f1c756d0-c922-45d9-94d5-fb355f523add