EternalPetya (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:06:37 UTC

EternalPetya

aka: ExPetr, Pnyetya, Petna, NotPetya, Nyetya, NonPetya, nPetya, Diskcoder.C, BadRabbit

Actor(s): TeleBots, Sandworm

VTCollection

According to proofpoint, Bad Rabbit is a strain of ransomware that first appeared in 2017 and is a suspected variant of Petya. Like other strains of ransomware, Bad Rabbit virus infections lock up victims' computers, servers, or files preventing them from regaining access until a ransom—usually in Bitcoin—is paid.

References

2024-04-16 · Mandiant · Alden Wahlstrom, Anton Prokopenkov, Dan Black, Dan Perez, Gabby Roncone, John Wolfram, Lexie Aytes, Nick Simonian, Ryan Hall, Tyler McLellan
APT44: Unearthing Sandworm
VPNFilter BlackEnergy CaddyWiper EternalPetya HermeticWiper Industroyer INDUSTROYER2 Olympic Destroyer PartyTicket RoarBAT Sandworm

2023-01-29 · Acronis · Ilan Duhin
Petya/Not Petya Ransomware Analysis
EternalPetya

2022-11-18 · Atlantic Council · Justin Sherman
GRU 26165: The Russian cyber unit that hacks targets on-site
EternalPetya

2022-10-31 · The Record · Alexander Martin
Mondelez and Zurich reach settlement in NotPetya cyberattack insurance suit
EternalPetya

2022-10-24 · Youtube (Virus Bulletin) · Alexander Adamov
Russian wipers in the cyberwar against Ukraine

AcidRain CaddyWiper DesertBlade DoubleZero EternalPetya HermeticWiper HermeticWizard INDUSTROYER2 IsaacWiper KillDisk PartyTicket WhisperGate

2022-04-28 · Fortinet · Gergely Revay

An Overview of the Increasing Wiper Malware Threat

AcidRain CaddyWiper DistTrack DoubleZero EternalPetya HermeticWiper IsaacWiper Olympic Destroyer Ordinypt WhisperGate ZeroCleare

2022-04-20 · CISA · CISA

Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader Killnet

2022-04-20 · CISA · Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), CISA, FBI, Government Communications Security Bureau, National Crime Agency (NCA), NCSC UK, NSA

AA22-110A Joint CSA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader

2022-03-01 · Marco Ramilli's Blog · Marco Ramilli

DiskKill/HermeticWiper and NotPetya (Dis)similarities

EternalPetya HermeticWiper

2022-02-25 · CyberPeace Institute

UKRAINE: Timeline of Cyberattacks

VPNFilter EternalPetya HermeticWiper WhisperGate

2022-02-24 · Talos · Mitch Neff

Threat Advisory: Current executive guidance for ongoing cyberattacks in Ukraine

VPNFilter EternalPetya

2022-02-24 · Tesorion · TESORION

Report OSINT: Russia/ Ukraine Conflict Cyberaspect

Mirai VPNFilter BlackEnergy EternalPetya HermeticWiper Industroyer WhisperGate

2022-02-24 · nviso · Michel Coene

Threat Update – Ukraine & Russia conflict

EternalPetya GreyEnergy HermeticWiper Industroyer KillDisk WhisperGate

2022-02-23 · ISTARI · Manuel Hepfer

Re-cap: The Untold Story of NotPetya, The Most Devastating Cyberattack in History

EternalPetya

2021-09-09 · Recorded Future · Insikt Group

Dark Covenant: Connections Between the Russian State and Criminal Actors

BlackEnergy EternalPetya Gameover P2P Zeus

2021-05-31 · Wired · Andy Greenberg
Hacker Lexicon: What Is a Supply Chain Attack?
EternalPetya SUNBURST

2021-04-29 · The Institute for Security and Technology · The Institute for Security and Technology
Combating Ransomware A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force
Conti EternalPetya

2020-12-21 · IronNet · Adam Hlavek, Kimberly Ortiz
Russian cyber attack campaigns and actors
WellMail elf.wellmess Agent.BTZ BlackEnergy EternalPetya Havex RAT Industroyer Ryuk Triton WellMess

2020-11-04 · Stranded on Pylos Blog · Joe Slowik
The Enigmatic Energetic Bear
EternalPetya Havex RAT

2020-10-19 · UK Government · Dominic Raab, ForeignCommonwealth & Development Office
UK exposes series of Russian cyber attacks against Olympic and Paralympic Games
VPNFilter BlackEnergy EternalPetya Industroyer

2020-10-19 · Riskint Blog · Curtis
Revisited: Fancy Bear's New Faces...and Sandworms' too
BlackEnergy EternalPetya Industroyer Olympic Destroyer

2020-10-19 · CyberScoop · Tim Starks
US charges Russian GRU officers for NotPetya, other major hacks
EternalPetya

2020-10-19 · Wired · Andy Greenberg
US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit
EternalPetya Olympic Destroyer

2020-08-29 · Aguinet · Adrien Guinet
Emulating NotPetya bootloader with Miasm
EternalPetya

2020-07-29 · Kaspersky Labs · GReAT
APT trends report Q2 2020
PhantomLance Dacls Penquin Turla elf.wellmess AppleJeus Dacls AcidBox Cobalt Strike Dacls EternalPetya Godlike12 Olympic Destroyer PlugX shadowhammer ShadowPad Sinowal VHD Ransomware Volgmer WellMess X-Agent XTunnel

2020-07-29 · Atlantic Council · June Lee, Stewart Scott, Trey Herr, William Loomis
BREAKING TRUST: Shades of Crisis Across an Insecure Software Supply Chain
EternalPetya GoldenSpy Kwampirs Stuxnet

2020-06-21 · GVNSHTN · Gavin Ashton
Maersk, me & notPetya
EternalPetya

2020-06-09 · Kaspersky Labs · Costin Raiu
Looking at Big Threats Using Code Similarity. Part 1
Penquin Turla CCleaner Backdoor EternalPetya Regin WannaCryptor XTunnel

2020-03-05 · Microsoft · Microsoft Threat Protection Intelligence Team
Human-operated ransomware attacks: A preventable disaster
Dharma DoppelPaymer Dridex EternalPetya Gandcrab Hermes LockerGoga MegaCortex MimiKatz REvil RobinHood Ryuk SamSam TrickBot WannaCryptor PARINACOTA

2020-01-01 · Secureworks · SecureWorks
IRON VIKING
BlackEnergy EternalPetya GreyEnergy Industroyer KillDisk TeleBot TeleDoor

2019-08-01 · Kaspersky Labs · GReAT
APT trends report Q2 2019
ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy

2018-10-11 · ESET Research · Anton Cherepanov, Robert Lipovsky
New TeleBots backdoor: First evidence linking Industroyer to NotPetya
Exaramel EternalPetya Exaramel Industroyer

2018-08-22 · Wired · Andy Greenberg
The Untold Story of NotPetya, the Most Devastating Cyberattack in History
EternalPetya

2018-01-13 · The Washington Post · Ellen Nakashima
Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes
EternalPetya

2017-10-27 · F-Secure · F-Secure Global
The big difference with Bad Rabbit
EternalPetya

2017-10-26 · Reversing Labs · None
ReversingLabs' YARA rule detects BadRabbit encryption routine specifics
EternalPetya

2017-10-26 · FireEye · Barry Vengerik, Ben Read, Brian Mordosky, Christopher Glyer, Ian Ahl, Matt Williams, Michael Matonis, Nick Carr
BACKSWING - Pulling a BADRABBIT Out of a Hat
EternalPetya

2017-10-25 · RiskIQ · Yonathan Klijnsma
Down the Rabbit Hole: Tracking the BadRabbit Ransomware to a Long Ongoing Campaign of Target Selection
EternalPetya

2017-10-24 · Kaspersky Labs · Anton Ivanov, Fedor Sinitsyn, Orkhan Mamedov
Bad Rabbit ransomware
EternalPetya

2017-10-24 · Cisco Talos · Nick Biasini
Threat Spotlight: Follow the Bad Rabbit
EternalPetya

2017-10-24 · ESET Research · Editor
Kiev metro hit with a new variant of the infamous Diskcoder ransomware
EternalPetya

2017-10-24 · Wired · Andy Greenberg
New Ransomware Linked to NotPetya Sweeps Russia and Ukraine
EternalPetya

2017-10-24 · Intezer · Jay Rosenberg
NotPetya Returns as Bad Rabbit
EternalPetya

2017-10-24 · ESET Research · Marc-Etienne M.Léveillé
Bad Rabbit: Not-Petya is back with improved ransomware
EternalPetya

2017-09-19 · NCC Group · Ollie Whitehouse
EternalGlue part one: Rebuilding NotPetya to assess real-world resilience
EternalPetya

2017-08-24 · ESET Research · Marc-Etienne M.Léveillé
Bad Rabbit: Not-Petya is back with improved ransomware
EternalPetya Sandworm

2017-08-11 · Threatpost · Tom Spring
Ukrainian Man Arrested, Charged in NotPetya Distribution
EternalPetya

2017-07-14 · Malwarebytes · Malwarebytes Labs
Keeping up with the Petyas: Demystifying the malware family
EternalPetya GoldenEye PetrWrap Petya

2017-07-04 · Kaspersky · Anton Ivanov, Orkhan Mamedov
In ExPetr/Petya's shadow, FakeCry ransomware wave hits Ukraine

EternalPetya FakeCry

2017-07-03 · CrowdStrike · Karan Sood, Shaun Hurley

NotPetya Technical Analysis Part II: Further Findings and Potential for MBR Recovery

EternalPetya

2017-07-03 · G Data · G Data

Who is behind Petna?

EternalPetya

2017-07-03 · The Guardian · Alex Hern

'NotPetya' malware attacks could warrant retaliation, says Nato affiliated-researcher

EternalPetya

2017-06-30 · Kaspersky Labs · GReAT

From BlackEnergy to ExPetr

EternalPetya

2017-06-30 · Malwarebytes · Malwarebytes Labs

EternalPetya – yet another stolen piece in the package?

EternalPetya

2017-06-30 · ESET Research · Anton Cherepanov

TeleBots are back: Supply-chain attacks against Ukraine

EternalPetya

2017-06-29 · Bleeping Computer · Catalin Cimpanu

Ransomware Attacks Continue in Ukraine with Mysterious WannaCry Clone

EternalPetya

2017-06-29 · Malwarebytes · Malwarebytes Labs

EternalPetya and the lost Salsa20 key

EternalPetya

2017-06-29 · Microsoft · Microsoft Defender ATP Research Team

Windows 10 platform resilience against the Petya ransomware attack

EternalPetya

2017-06-29 · Robert Graham

NonPetya: no evidence it was a "smokescreen"

EternalPetya

2017-06-28 · CrowdStrike · Falcon Intelligence Team

CrowdStrike Protects Against NotPetya Attack

EternalPetya

2017-06-28 · hacks4pancakes
Why NotPetya Kept Me Awake (& You Should Worry Too)
EternalPetya

2017-06-28 · Kaspersky Labs · Anton Ivanov, Orkhan Mamedov
ExPetr/Petya/NotPetya is a Wiper, Not Ransomware
EternalPetya

2017-06-27 · Kaspersky Labs · GReAT
Schroedinger's Pet(ya)
EternalPetya

2017-06-27 · ESET Research · Editor
New WannaCryptor-like ransomware attack hits globally: All you need to know
EternalPetya Sandworm

2017-06-27 · Medium thegrugq · thegrugq
Pnyetya: Yet Another Ransomware Outbreak
EternalPetya

2017-06-27 · SANS · Brad Duncan
Checking out the new Petya variant
EternalPetya

2017-05-31 · MITRE · MITRE ATT&CK
Sandworm Team
CyclopsBlink Exaramel BlackEnergy EternalPetya Exaramel GreyEnergy KillDisk MimiKatz Olympic Destroyer Sandworm

Yara Rules

▶ [TLP:WHITE] win_eternal_petya_auto (20251219 | Detects win.eternal_petya.)	
▶ [TLP:WHITE] win_eternal_petya_w0 (20171222 | No description)	

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.eternal_petya