Circus Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:02:24 UTC

NamesCircus Spider *(CrowdStrike)* Country[Unknown] MotivationFinancial gain First seen2019 Description(Carbon Black) MailTo is a ransomware variant that has recently been reported to have been part of a targeted attack against Toll Group, an Australian freight and logistics company. This ransomware makes no attempt to remain stealthy, and quickly encrypts the user's data as soon as the ransomware is launched. Once the encryption phase completes, the encrypted files are renamed to contain the word "mailto", which is where the name originated from. ObservedSectors: Education, Energy, Government, Healthcare, Manufacturing, Shipping and Logistics, Transportation.
Countries: Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, China, Colombia, France, Germany, Guatemala, Hungary, India, Iran, Ireland, Italy, Luxembourg, Malaysia, Netherlands, New Zealand, Nicaragua, Nigeria, Norway, Pakistan, Poland, Russia, Saudi Arabia, South Africa, Spain, Sweden, Thailand, Ukraine, USA, Vietnam. Tools usedNetWalker. Operations performedFeb 2020Ransomware Attack Hinders Toll Group Operations
<https://threatpost.com/ransomware-attack-hinders-toll-group-operations/152552/> Mar 2020Netwalker Ransomware Infecting Users via Coronavirus Phishing
<https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/> Mar 2020Spanish hospitals targeted with coronavirus-themed phishing lures in Netwalker ransomware attacks
<https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware> May 2020Michigan State University hit by ransomware gang
<https://www.zdnet.com/article/michigan-state-university-hit-by-ransomware-gang/> May 2020Ransomware recruits affiliates with huge payouts, automated leaks
<https://www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/> Jun 2020Netwalker ransomware continues assault on US colleges, hits UCSF
<https://www.bleepingcomputer.com/news/security/netwalker-ransomware-continues-assault-on-us-colleges-hits-ucsf/> Jun 2020Philadelphia-area health system says it 'isolated' a malware attack
<https://www.cyberscoop.com/crozer-keystone-cyber-attack-netwalker-ransomware/> Jul 2020Netwalker Ransomware Stole Data After Targeting Lorien Health Services
<https://latesthackingnews.com/2020/07/23/netwalker-ransomware-stole-data-after-targeting-lorien-health-services/> Sep 2020Netwalker ransomware hits Pakistan's largest private power utility
<https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/> Sep 2020Netwalker ransomware hits Argentinian government, demands $4 million
<https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/> Sep 2020Cyber threat startup Cygilant hit by ransomware
<https://techcrunch.com/2020/09/03/cygilant-ransomware/> Sep 2020Equinix data center giant hit by Netwalker Ransomware, $4.5M ransom
<https://www.bleepingcomputer.com/news/security/equinix-data-center-giant-hit-by-netwalker-ransomware-45m-ransom/> Oct 2020Enel Group hit by ransomware again, Netwalker demands $14 million

<https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/> Counter operationsJan 2021Department of Justice Launches Global Action Against NetWalker Ransomware <https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware> Feb 2022NetWalker ransomware affiliate sentenced to seven years in prison <https://therecord.media/netwalker-ransomware-affiliate-sentenced-to-seven-years-in-prison/> Dec 2024Romanian Netwalker ransomware affiliate sentenced to 20 years in prison <https://www.bleepingcomputer.com/news/security/romanian-netwalker-ransomware-affiliate-sentenced-to-20-years-in-prison/> Information<https://www.carbonblack.com/blog/threat-analysis-unit-tau-threat-intelligence-notification-mailto-netwalker-ransomware/> <https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest>
