Monty Spider - Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: Monty Spider

Names	Monty Spider *(CrowdStrike)* Gold Riverview *(SecureWorks)*	
Country	Russia	
Motivation	Financial gain	
First seen	2012	
Description	(IBM) Necurs emerged in 2012 as an infector and rootkit, and quickly partnered with elite cybercrime gangs to become part of the top spamming and infection forces in the malware realm. Unlike most botnets, Necurs stands out due to its technical complexity, partnership diversity and continued evolution in an era when even the most complex malicious infrastructures can no longer withstand disruption. In the past year alone, we have seen Necurs take on various roles. Linked with the spam distribution of the Dridex gang, it is used to spread one of the world's most nefarious banking Trojans. It also moved to mass distributing Locky, Dridex's ransomware child, then added distributed denial-of-service (DDoS) attacks. Most recently, Necurs moved to pump-and-dump stock scam distribution before returning to spreading millions of Dridex-laden spam emails a day. Necurs has been observed to distribute Dridex (Indrik Spider) Locky (Dungeon Spider), TrickBot (Wizard Spider, Gold Blackburn) and much of the malware from TA505, Graceful Spider, Gold Evergreen.	
Observed	Countries: Worldwide.	
Tools used	Necurs.	
Operations performed	Feb 2016	Necurs.P2P – A New Hybrid Peer-to-Peer Botnet <https://www.malwaretech.com/2016/02/necursp2p-hybrid-peer-to-peer-necurs.html>

Jan 2017	From the start, it became apparent that Locky's growth was powered by Necurs, a huge botnet of infected devices used to send email spam. <https://www.bleepingcomputer.com/news/security/numbers-show-locky-ransomware-is-slowly-fading-away/>
Mar 2017	Spam Sent by Necurs Botnet Is Trying & Succeeding in Altering Stock Market Prices <https://www.bleepingcomputer.com/news/security/spam-sent-by-necurs-botnet-is-trying-andamp-succeeding-in-altering-stock-market-prices/>
Oct 2017	Necurs Malware Will Now Take a Screenshot of Your Screen, Report Runtime Errors <https://www.bleepingcomputer.com/news/security/necurs-malware-will-now-take-a-screenshot-of-your-screen-report-runtime-errors/>
Nov 2017	During the month of November, the Necurs botnet has returned to Check Point’s Global Threat Index’s top ten most prevalent malware. <https://blog.checkpoint.com/2017/12/11/novembers-wanted-malware-return-necurs-botnet-brings-new-ransomware-threat/>
Jan 2018	World's Largest Spam Botnet Is Pumping and Dumping an Obscure Cryptocurrency <https://www.bleepingcomputer.com/news/cryptocurrency/worlds-largest-spam-botnet-is-pumping-and-dumping-an-obscure-cryptocurrency/>
Apr 2018	World's Largest Spam Botnet Finds a New Way to Avoid Detection... For Now <https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/>
Jun 2018	Necurs Poses a New Challenge Using Internet Query File <https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-poses-a-new-challenge-using-internet-query-file/>
Aug 2018	Necurs Targeting Banks with PUB File that Drops FlawedAmmyy <https://cofense.com/necurs-targeting-banks-pub-file-drops-flawedammyy/>
Jun 2019	Necurs Spam uses DNS TXT Records for Redirection <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/necurs-spam-uses-dns-txt-records-for-redirection/>
Jan 2020	Has Necurs Fallen From (Cybercrime) Grace? Elite Malware Botnet Now Distributes Clunky Scams

		<https://securityintelligence.com/posts/has-necurs-fallen-from-cybercrime-grace-elite-malware-botnet-now-distributes-clunky-scams/>
Counter operations	Mar 2020	Today, Microsoft and partners across 35 countries took coordinated legal and technical steps to disrupt one of the world's most prolific botnets, called Necurs, which has infected more than nine million computers globally. <https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/>
Information	<https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/> <https://www.netformation.com/our-pov/casting-light-on-the-necurs-shadow/> <https://blog.talosintelligence.com/2018/01/the-many-tentacles-of-necurs-botnet.html> <https://www.cert.pl/en/news/single/necurs-hybrid-spam-botnet/>	

Last change to this card: 10 August 2021

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=bc90e2ed-dafb-40e4-9a38-36c245625c7e