Guru Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:25:12 UTC

Other threat group: Guru Spider

Names	Guru Spider *(CrowdStrike)*	
Country	Russia	
Motivation	Financial gain	
First seen	2014	
Description	(Forcepoint) Quant is not new or a very novel piece of malware: we covered the basics of it last year when it was first advertised by its creator, MrRaiX, and began to emerge in the wild. However, analysis of the newly obtained samples quickly revealed some differences to the previously documented Quant-based Locky and Pony campaigns. Further, these newest samples all appeared to attempt to download the same payload files from the C2 server after their initial connection.	
Observed	Countries: Worldwide.	
Tools used	Madness PRO DDoS, MBS BTC Stealer, MKL Pro Keylogger, Quant Loader, Z*Stealer.	
Operations performed	Sep 2016	On September 1, 2016 a new trojan downloader became available to purchase on various Russian underground forums. Named 'Quant Loader' by its creator, the downloader has already been used to distribute the Locky Zepto crypto-ransomware, and Pony (aka Fareit) malware families. <https://www.forcepoint.com/blog/x-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground>
	Mar 2018	QuantLoader is a Trojan downloader that has been available for sale on underground forums for quite some time now. It has been used in campaigns serving a range of malware, including ransomware, Banking Trojans, and RATs. The campaign that we are going to analyze is serving a BackDoor. <https://blog.malwarebytes.com/threat-analysis/2018/03/an-in-depth-malware-analysis-of-quantloader/>
	Mar 2018	Barracuda Threat Spotlight: New URL File Outbreak Could be a Ransomware Attempt

		<https://blog.barracuda.com/2018/04/10/barracuda-threat-spotlight-new-url-file-outbreak-could-be-a-ransomware-attempt/>
Information	<https://www.forcepoint.com/blog/x-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground> <https://www.forcepoint.com/zh-hant/blog/security-labs/quantize-or-capitalize>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
