Mallard Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:06:51 UTC

APT group: Mallard Spider

Names	Mallard Spider *(CrowdStrike)* Gold Lagoon *(SecureWorks)*	
Country	[Unknown]	
Motivation	Financial crime, Financial gain	
First seen	2008	
Description	(The Hacker News) First documented in 2008, Qbot (aka QuakBot, QakBot, or Pinkslipbot) has evolved over the years from an information stealer to a 'Swiss Army knife' adept in delivering other kinds of malware, including Prolock ransomware, and even remotely connect to a target's Windows system to carry out banking transactions from the victim's IP address. Attackers usually infect victims using phishing techniques to lure victims to websites that use exploits to inject Qbot via a dropper. QakBot has been observed to be distributed by Emotet (operated by Mummy Spider, TA542).	
Observed		
Tools used	Egregor, Mimikatz, ProLock, QakBot.	
Operations performed	Mar 2020	PwndLocker Fixes Crypto Bug, Rebrands as ProLock Ransomware <https://www.bleepingcomputer.com/news/security/pwndlocker-fixes-crypto-bug-rebrands-as-prolock-ransomware/>
	Mar 2020	Ransomware Attack Renders LaSalle County Government Computers Unusable <https://chicago.cbslocal.com/2020/03/04/ransomware-attack-renders-lasalle-county-government-computers-unusable/>

	Apr 2020	QBot malware is back replacing IcedID in malspam campaigns <https://www.bleepingcomputer.com/news/security/qbot-malware-is-back-replacing-icedid-in-malspam-campaigns/>
	May 2020	FBI warns of ProLock ransomware decryptor not working properly <https://www.bleepingcomputer.com/news/security/fbi-warns-of-prolock-ransomware-decryptor-not-working-properly/>
	May 2020	Ransomware Hit ATM Giant Diebold Nixdorf <https://krebsonsecurity.com/2020/05/ransomware-hit-atm-giant-diebold-nixdorf/>
	May 2020	ProLock Ransomware teams up with QakBot trojan for network access <https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/>
	Aug 2020	Qbot steals your email threads again to infect other victims <https://www.bleepingcomputer.com/news/security/qbot-steals-your-email-threads-again-to-infect-other-victims/>
	Sep 2020	FBI issues second alert about ProLock ransomware stealing data <https://www.bleepingcomputer.com/news/security/fbi-issues-second-alert-about-prolock-ransomware-stealing-data/>
	Sep 2020	ProLock ransomware increases payment demand and victim count <https://www.bleepingcomputer.com/news/security/prolock-ransomware-increases-payment-demand-and-victim-count/>
	Oct 2020	QBot uses Windows Defender Antivirus phishing bait to infect PCs <https://www.bleepingcomputer.com/news/security/qbot-uses-windows-defender-antivirus-phishing-bait-to-infect-pcs/>
	Nov 2020	QBot phishing lures victims using US election interference emails <https://www.bleepingcomputer.com/news/security/qbot-phishing-lures-victims-using-us-election-interference-emails/>
	Nov 2020	QBot partners with Egregor ransomware in bot-fueled attacks <https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/>
	Dec 2020	Qbot malware switched to stealthy new Windows autostart method <https://www.bleepingcomputer.com/news/security/qbot-malware-switched-to-stealthy-new-windows-autostart-method/>
Information	<https://thehackernews.com/2020/08/qakbot-banking-trojan.html>	

Last change to this card: 10 August 2021

Download this actor card in PDF or JSON format
