Mummy Spider, TA542 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:58:42 UTC

Other threat group: Mummy Spider, TA542

Names	Mummy Spider *(CrowdStrike)* TA542 *(Proofpoint)* ATK 104 *(Thales)* Mealybug *(Symantec)* Gold Crestwood *(SecureWorks)*
Country	[Unknown]
Motivation	Financial crime
First seen	2014

Description	(Crowdstrike) Mummy Spider is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo. First observed in mid-2014, this malware shared code with the Bugat (aka Feodo) banking Trojan. However, Mummy Spider swiftly developed the malware's capabilities to include an RSA key exchange for command and control (C2) communication and a modular architecture. Mummy Spider does not follow typical criminal behavioral patterns. In particular, Mummy Spider usually conducts attacks for a few months before ceasing operations for a period of between three and 12 months, before returning with a new variant or version. After a 10 month hiatus, Mummy Spider returned Emotet to operation in December 2016 but the latest variant is not deploying a banking Trojan module with web injects, it is currently acting as a 'loader' delivering other malware packages. The primary modules perform reconnaissance on victim machines, drop freeware tools for credential collection from web browsers and mail clients and a spam plugin for self-propagation. The malware is also issuing commands to download and execute other malware families such as the banking Trojans Dridex and Qakbot. Mummy Spider advertised Emotet on underground forums until 2015, at which time it became private. Therefore, it is highly likely that Emotet is operated solely for use by Mummy Spider or with a small trusted group of customers. Emotet has been observed to distribute BokBot (Lunar Spider), Dridex (Indrik Spider), DoppelPaymer (Doppel Spider), Zeus Panda (Bamboo Spider, TA544) and Trickbot (Wizard Spider, Gold Blackburn), as well as QakBot (Mallard Spider).	
Observed	Sectors: Defense, Energy, Financial, Government, Healthcare, Manufacturing, Retail, Shipping and Logistics, Utilities, Technology. Countries: Worldwide.	
Tools used	Emotet.	
Operations performed	Aug 2017	While the earlier variants of EMOTET primarily targeted the banking sector, our Smart Protection Network (SPN) data reveals that this time, the malware isn't being picky about the industries it chooses to attack. The affected companies come from different industries, including manufacturing, food and beverage, and healthcare. Again, it is possible that due to the nature of its distribution, EMOTET now has a wider scope. <https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/>
	Oct 2018	Emotet Awakens With New Campaign of Mass Email Exfiltration <https://www.kryptoslogic.com/blog/2018/10/emotet-awakens-with-new-campaign-of-mass-email-exfiltration/>
	Nov 2018	According to our telemetry, the latest Emotet activity was launched on November 5, 2018, following a period of low activity. Figure 1 shows a spike in the Emotet detection rate in the beginning of November 2018, as seen in our telemetry data.

	<https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/> <https://www.welivesecurity.com/2018/12/28/analysis-latest-emotet-propagation-campaign/>
Nov 2018	Secret Service Investigates Breach at U.S. Govt IT Contractor <https://krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/>
Jan 2019	Between January 1, 2019, to May 1, 2019, threat actors conducted thousands of malicious email campaigns, hundreds of which were sent to Canadian organizations. While discussions of threats in this region often focus on “North America” generally or just the United States, nearly 100 campaigns during this period were either specifically targeted at Canadian organizations or were customized for Canadian audiences. <https://www.proofpoint.com/us/threat-insight/post/beyond-north-america-threat-actors-target-canada-specifically>
Apr 2019	Beginning the morning of April 9th, the Emotet gang began utilizing what appears to be the stolen emails of their victims. It was noted back in October of 2018 that a new module was added that could steal the email content on a victim’s machine. <https://cofense.com/emotet-gang-switches-highly-customized-templates-utilizing-stolen-email-content-victims/>
Sep 2019	Emotet is back after a summer break <https://blog.talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html> <https://threatpost.com/emotet-resurgence-continues-with-new-tactics-techniques-and-procedures/149914/>
Dec 2019	The city of Frankfurt, Germany, became the latest victim of Emotet after an infection forced it to close its IT network. But the financial center wasn’t the only area that was targeted by Emotet, as there were also incidents that occurred in Gießen and Bad Homburg, a town and a city north of Frankfurt, respectively, as well as in Freiburg, a city in southwest Germany. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-attack-causes-shutdown-of-frankfurt-s-it-network>
Jan 2020	Threat actor group TA542, the group that’s behind Emotet, is back from their Christmas holiday. Based on past activity and what we’re seeing in just three days, one of the world’s most disruptive threats is back to work and everyone around the world should take note and implement steps to protect themselves. <https://www.proofpoint.com/us/corporate-blog/post/emotet-returns-after-holiday-break-major-campaigns> <https://blog.talosintelligence.com/2020/01/stolen-emails-reflect-emotets-organic.html>

Jan 2020	Pretending to be the Permanent Mission of Norway, the Emotet operators performed a targeted phishing attack against email addresses associated with users at the United Nations. <https://www.bleepingcomputer.com/news/security/united-nations-targeted-with-emotet-malware-phishing-attack/>
Jan 2020	EMOTET Uses Corona Virus Outbreak in New Spam Campaign <https://www.trendmicro.com/vinfo/th/threat-encyclopedia/spam/3682/emotet-uses-corona-virus-outbreak-in-new-spam-campaign>
Feb 2020	Emotet Evolves With new Wi-Fi Spreader <https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/>
Feb 2020	Emotet SMiShing Uses Fake Bank Domains in Targeted Attacks, Payloads Hint at TrickBot Connection <https://securityintelligence.com/posts/emotet-smishing-uses-fake-bank-domains-in-targeted-attacks-payloads-hint-at-trickbot-connection/>
Mar 2020	Emotet Wi-Fi Spreader Upgraded <https://www.binarydefense.com/emotet-wi-fi-spreader-upgraded/>
Jun 2020	Emotet malware now steals your email attachments to attack contacts <https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-your-email-attachments-to-attack-contacts/>
Jul 2020	It was never a question of “if” but “when”. After five months of absence, the dreaded Emotet has returned. Following several false alarms over the last few weeks, a spam campaign was first spotted on July 13 showing signs of a likely comeback. <https://blog.malwarebytes.com/trojans/2020/07/long-dreaded-emotet-has-returned/>
Jul 2020	Researchers tracking Emotet botnet noticed that the malware started to push QakBot banking trojan at an unusually high rate, replacing the longtime TrickBot payload. <https://www.bleepingcomputer.com/news/security/emotet-botnet-is-now-heavily-spreading-qakbot-malware/>
Aug 2020	Emotet malware strikes U.S. businesses with COVID-19 spam <https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/>
Aug 2020	Emotet strikes Quebec’s Department of Justice <https://www.welivesecurity.com/2020/09/16/emotet-quebec-department-justice-eset/>
Aug 2020	Since August, CISA and MS-ISAC have seen a significant increase in malicious cyber actors targeting state and local governments with Emotet phishing emails. <https://us-cert.cisa.gov/ncas/alerts/aa20-280a>

Oct 2020	On October 1, 2020, we observed thousands of Emotet email messages with the subject “Team Blue Take Action” sent to hundreds of organizations in the US. The message body is taken directly from a page on the Democratic National Committee's website, with the addition of a line requesting that the recipient open the attached document. <https://www.proofpoint.com/us/blog/threat-insight/emotet-makes-timely-adoption-political-and-elections-lures>
Oct 2020	New Emotet attacks use fake Windows Update lures <https://www.zdnet.com/article/new-emotet-attacks-use-fake-windows-update-lures/>
Dec 2020	Emotet malware hits Lithuania's National Public Health Center <https://www.bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/>
Nov 2021	Emotet malware is back and rebuilding its botnet via TrickBot <https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/>
Dec 2021	Emotet now drops Cobalt Strike, fast forwards ransomware attacks <https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/>
Jan 2022	Emotet Spam Abuses Unconventional IP Address Formats to Spread Malware <https://www.trendmicro.com/en_us/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html>
Feb 2022	New Emotet Infection Method <https://unit42.paloaltonetworks.com/new-emotet-infection-method/>
Mar 2022	Emotet Targeting Japanese Organizations <https://www.cybereason.com/blog/research/threat-alert-emotet-targeting-japanese-organizations>
Mar 2022	Emotet Spoofs IRS in Tax Season-Themed Phishing Email Campaign <https://cofense.com/blog/emotet-spoofs-irs-in-tax-season/>
Apr 2022	Emotet modules and recent attacks <https://securelist.com/emotet-modules-and-recent-attacks/106290/>
Apr 2022	Emotet botnet switches to 64-bit modules, increases activity <https://www.bleepingcomputer.com/news/security/emotet-botnet-switches-to-64-bit-modules-increases-activity/>
Apr 2022	Emotet malware infects users again after fixing broken installer <https://www.bleepingcomputer.com/news/security/emotet-malware-infects-users-again-after-fixing-broken-installer/>

	Apr 2022	Emotet Tests New Delivery Techniques <https://www.proofpoint.com/us/blog/threat-insight/emotet-tests-new-delivery-techniques>
	Apr 2022	Emotet malware now installs via PowerShell in Windows shortcut files <https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/>
	Jun 2022	Emotet malware now steals credit cards from Google Chrome users <https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-credit-cards-from-google-chrome-users/>
	Jun 2022	Back From the Dead, Emotet Returns in 2022 <https://www.deepinstinct.com/blog/emotet-malware-returns-in-2022>
	Nov 2022	Emotet botnet starts blasting malware again after 4 month break <https://www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/> <https://blog.talosintelligence.com/emotet-coming-in-hot/>
Counter operations	Jul 2020	A vigilante is sabotaging the Emotet botnet by replacing malware payloads with GIFs <https://www.zdnet.com/article/a-vigilante-is-sabotaging-the-emotet-botnet-by-replacing-malware-payloads-with-gifs/>
	Jan 2021	World’s most dangerous malware EMOTET disrupted through global action <https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>
	Jun 2024	Authorities Ramp Up Efforts to Capture the Mastermind Behind Emotet <https://thehackernews.com/2024/06/authorities-ramp-up-efforts-to-capture.html>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/> <https://documents.trendmicro.com/assets/white_papers/ExploringEmotetsActivities_Final.pdf> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/> <https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service> <https://www.malwarebytes.com/emotet/> <https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor> <https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/>	

Last change to this card: 19 June 2024

Download this actor card in PDF or JSON format
