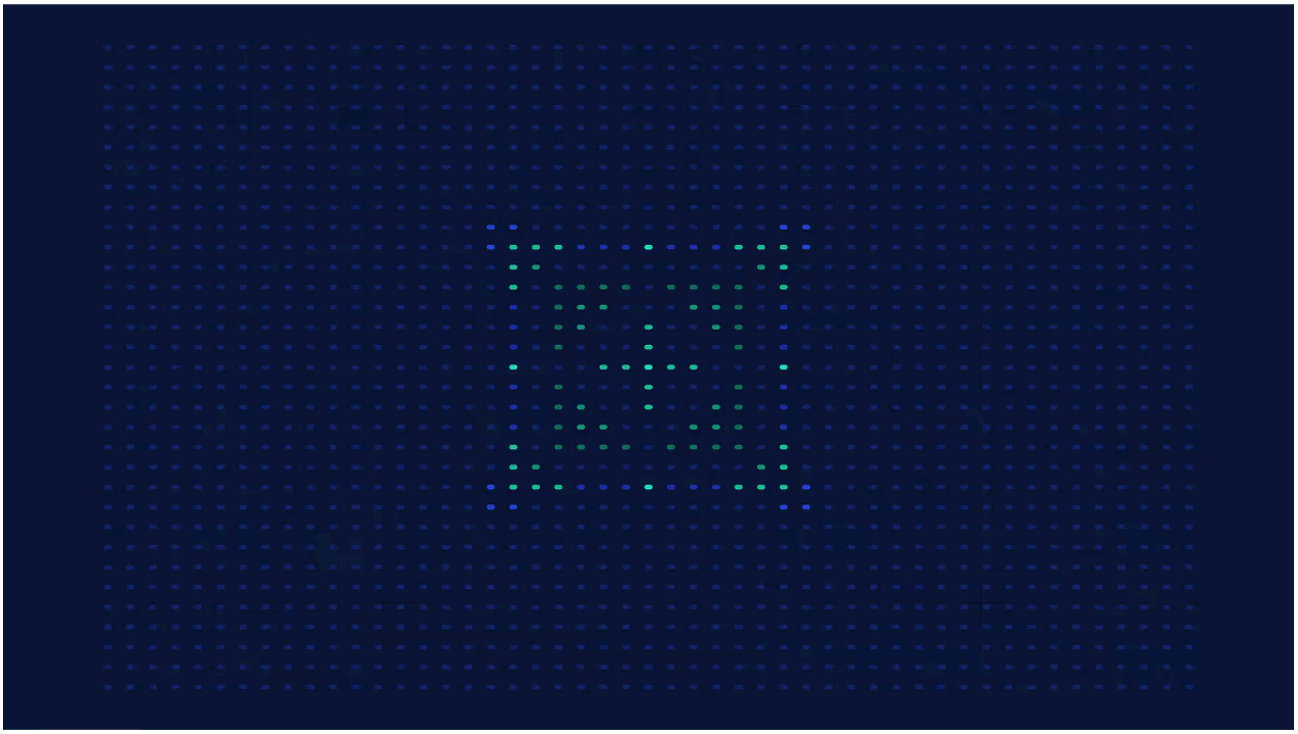
Mummy Spider's Emotet Malware is Back After a Year Hiatus; Wizard Spider's TrickBot Observed in Its Return

By Anomali Threat Research

Published: 2025-12-18 · Archived: 2026-04-05 13:07:58 UTC

Mummy Spider’s Emotet Malware is Back After a Year Hiatus,; Wizard Spider’s TrickBot Observed in Its Return

- Endnotes



Mummy Spider (TA542, Emotet) recently resumed their malicious activity with the notorious information-stealing malware, Emotet, after a year-long hiatus.[1] As part of this return, the Emotet malware has been observed delivered via the TrickBot malware, which is organized by the Wizard Spider (TrickBot, UNC1878) group.[2]

Emotet and Trickbot are dangerous families that have undergone numerous changes and upgrades over years, with Emotet being first discovered in 2014 and TrickBot in 2016.[3] The longevity of these malware families, even with international law enforcement taking down Emotet infrastructure as of January 2021, showcases the relentless nature of the threat actors behind them.

To assist in helping the community, especially with the online shopping season upon us, Anomali Threat Research has made available two threat actor focused dashboards: Mummy Spider and Wizard Spider, for Anomali ThreatStream customers. The Dashboards are preconfigured to provide immediate access and visibility into all known Mummy Spider and Wizard Spider indicators of compromise (IOCs) made available through commercial and open-source threat feeds that users manage on ThreatStream.

Customers using ThreatStream, Anomali Match, and Anomali Lens are able to immediately detect any IOCs present in their environments and quickly consume threat bulletins containing machine-readable IOCs. This enables analysts to quickly operationalize threat intelligence across their security infrastructures, as well as communicate to all stakeholders if/how they have been impacted.

Anomali recently added thematic dashboards that respond to significant global events as part of ongoing product enhancements that further automate and speed essential tasks performed by threat intelligence and security operations analysts. In addition to Mummy Spider and Wizard Spider, ThreatStream customers currently have access to multiple dashboards announced as part of our November quarterly product release.

Customers can integrate the Mummy Spider and Wizard Spider dashboard, among others, in the “+ Add Dashboard” tab in the ThreatStream console:

Endnotes

[1] “#Emotet has almost doubled its botnet C2 infrastructure in the past 24 hours from 8 active C2s yesterday to 14 active C2s today…,” abuse.ch, accessed November 22, 2021, published November 16, 2021, https://twitter.com/abuse_ch/status/1460649241454563341; “Another Update on #Emotet E4 distro - We are now seeing URL based lures for the document downloads…,” Cryptolaemus, accessed November 22, 2021, published November 17, 2021, https://twitter.com/Cryptolaemus1/status/1460870766518484993.

[2] Luca Ebach, “Guess who’s back,” cyber.wtf, accessed November 22, 2021, published November 15, 2021, https://cyber.wtf/2021/11/15/guess-whos-back/; “Emotet is back. Here’s what we know.,” Intel471 Blog, accessed November 22, published November 16, 2021, https://intel471.com/blog/emotet-is-back-2021.

[3] Alina Georgiana Petcu, “Emotet Malware Over the Years: The History of an Infamous Cyber-Threat,” Heimdal Security Blog, accessed November 22, 2021, published April 29, 2021, https://heimdalsecurity.com/blog/emotet-malware-history/; Hugh Aver, “New tricks of the Trickbot Trojan, Kaspersky Blog, accessed November 22, 2021, published October 19, 2021, https://www.kaspersky.com/blog/trickbot-new-tricks/42622/#:~:text=Exactly%20five%20years%20ago%2C%20in,credentials%20for%20online%20banking%20services.
