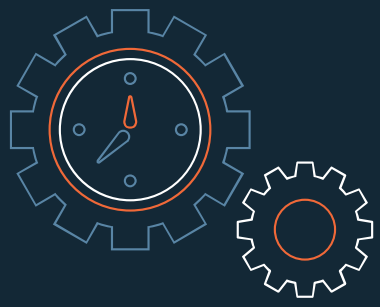
SecurityRisk ADVISORS

CyberSOC Threat Notification



Vendor: CISA

Published: October 6, 2020

Attribution Metrics

Threat Actor: Wizard Spider, Mummy Spider aka TA542

Origin: eCrime Syndicate

Malware Metrics

First Seen: June 2014

Malware Type: Banking Trojan

Tactic: Initial Access

Technique: Phishing

Emotet Malware

Executive Summary

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) released security advisory AA20-280A warning of an increase in Emotet attacks targeting state and local governments. Emotet resurged in July 2020 after a five-month period of inactivity.

Description

Emotet is a banking Trojan that is primarily spread through spearphishing emails containing malicious attachments. The malware can steal sensitive information including user credentials, financial information, and computer data and sends it to a remote command and control (C2) server. Emotet is commonly used to download other malware such as Qakbot and Trickbot. The Trojan has also been used to deploy ransomware payloads like Ryuk as seen in the recent UHS cyberattack. Once downloaded, the malware will establish persistence and attempt to propagate through the network. Additionally, modular Dynamic Link Libraries (DLL) are used to update the malware's capabilities and evade detection.

Safeguards/Recommendations

Organizations are encouraged to apply security best practices including blocking suspicious email attachments, maintaining antivirus software, and blocking suspicious IP addresses. The CISA and Multi-State Information Sharing & Analysis Center (MS-ISAC) released three Snort signatures which can be used to detect network activity associated with Emotet.

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io