Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:29:14 UTC

Description(Malwarebytes) Emotet is a Trojan that is primarily spread through spam emails (malspam). The infection may arrive either via malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email. Emotet may try to persuade users to click the malicious files by using tempting language about “Your Invoice,” “Payment Details,” or possibly an upcoming shipment from well-known parcel companies.

Emotet has gone through a few iterations. Early versions arrived as a malicious JavaScript file. Later versions evolved to use macro-enabled documents to retrieve the virus payload from command and control (C&C) servers run by the attackers.

Emotet uses a number of tricks to try and prevent detection and analysis. Notably, Emotet knows if it’s running inside a virtual machine (VM) and will lay dormant if it detects a sandbox environment, which is a tool cybersecurity researchers use to observe malware within a safe, controlled space.

Emotet also uses C&C servers to receive updates. This works in the same way as the operating system updates on your PC and can happen seamlessly and without any outward signs. This allows the attackers to install updated versions of the software, install additional malware such as other banking Trojans, or to act as a dumping ground for stolen information such as financial credentials, usernames and passwords, and email addresses.
