SOPHOS

EMOTET ECOSYSTEM

Breaking in...

Massive spam email campaigns deliver EMOTET to most victims, by means of malicious office documents. Some of the payloads may be attached to the message, while others may be linked in the spam. The malicious macro code runs a PowerShell script that, in turn, downloads the malware binary to the %temp% folder.

Download and Launch Binary {>_}

Partners in Crime

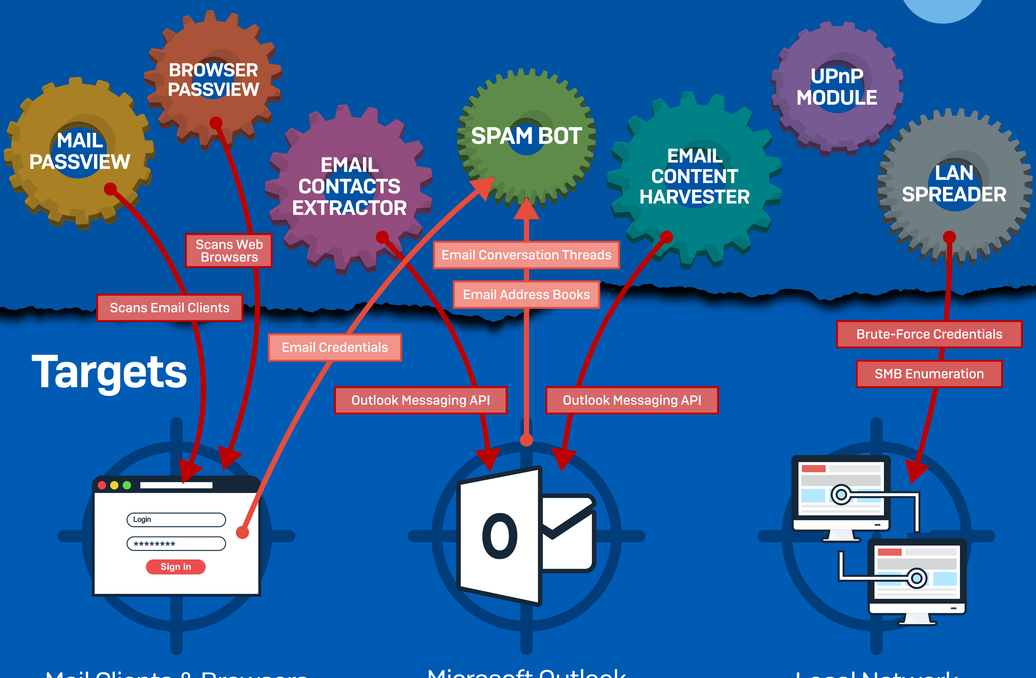
The main EMOTET executable establishes persistence, then collects user and hardware information from the infected machine. It communicates with a C2 server that decides which of the several available payload modules it will deliver based on the victim's profile.

Components

To Friends, Colleagues and Family

Arsenal

EMOTET modules run as a child process from the main executable, or can be injected into a new instance of it. It saves the results to a temporary data file then sends it to the C2. The modules may be third party utilities, or bespoke tools that carry out specific tasks.



Targets

Mail Clients & Browsers

Microsoft Outlook

Local Network

Find out more at
www.sophos.com/en-us/labs

SOPHOS labs