Issued 11/9/17

Two Banking Trojans That Can Plunder Your Accounts Are On the Rise

The use of two notorious strains of banking Trojan that are able to silently infect computers, steal login details and empty accounts has spiked in recent months, Microsoft warns. The malware variants – dubbed Qakbot and Emotet – are known as "information stealers" and, while technically separate, they share a number of key behavioral similarities.

Some of the new strains in use by hackers have worm-like capabilities that let them quickly spread across infected computer networks. The worm functionality, adopted after the WannaCry ransomware outbreak in May, was also noted by SophosLabs in August. Essentially, they have both evolved into effective tools for financial cybercrime. New analysis, from January to August this year, suggested both Trojans were getting better at hitting targets. At the start of 2017, Emotet infections were minimal – well under 5,000 detections. Yet in August, Microsoft encountered the malicious software on machines more than 15,000 times.

Experts found that – like WannaCry – it could take advantage of a Windows OS protocol known as Server Message Block (SMB) to "drop copies" of the malware onto linked computers.