Issued 10/10/17

This Cheap and Nasty Malware Wants to Steal Your Data

Hackers have launched a string of campaigns against defense, aerospace and manufacturing contractors in the US and South Korea in an effort to install data-stealing malware.

The campaigns have used a data stealing software package being sold online at relatively low-cost -- prices range from $29 a week to a $299 full-package 'pro' deal. The FormBook malware provides users with a range of espionage capabilities, including key logging, taking screenshots, clipboard monitoring grabbing passwords from web pages and emails. In an underground advertisement which makes it look more like legitimate software than a criminal tool, its authors describe FormBook as 'advance[d] internet activity logging software' which is designed 'to give you extensive and powerful internet monitoring experience'.

Several FormBook campaigns have been uncovered by researchers at FireEye - while each campaign users email as the primary attack vector, the malicious attachment can come in the form of PDFs, Office Documents, ZIP, RAR, ACE or ICO attachments, as well as shortened URLs. Each campaign uses slightly different distribution methods, with aerospace, defense and manufacturing the industries most targeted - although attacks also targeted education, energy, government, financial services and more. Attacks weren't specially targeted in any way, with generic messages covering common subjects distributed to potential victims.