Issued 9/17/18

Microsoft Office is More Dangerous than you Think: Docs Deliver 45% of All Malware

Microsoft Office documents packed with malicious macros are the most common malware loader of the past month, accounting for 45% of all delivery mechanisms analyzed, according to a Thursday report from Cofense. Office Macros were followed in popularity by CVE-2017-11882, malicious batch scripts, malicious PowerShell scripts, and WSC downloaders, the report found. This demonstrates that threat actors tend to leverage tried-and-tested delivery mechanisms, the report noted. Macros may have a low barrier to entry, but they are not used only by immature or low-impact cybercriminals: Malware delivered via macros is among the worst in today's threat landscape, including Geodo, Chanitor, AZORult, and GandCrab, according to the report. Macros remain a popular email attachment method of delivering a malicious payload because they are typically enabled on a machine, or easily allowed with a single mouse click, the report noted—making it very easy to launch the first stage of an attack. When used this way, macros are embedded Visual Basic scripts that are often used to download or directly execute further payloads.