Log4J - https://jfrog.com/blog/log4shell-0-day-vulnerability-all-you-need-to-know/

The Log4J vulnerability was an exploit against the Log4J Log4Shell logging feature that is specifically from the 2.x branch. This logging feature allows string substitution to be dynamically generated at time of logging via a lookup method. This lookup method fetches a specified Java class from a remote source which is then deserialized for execution of the string generation. The implication of a remote attacker being able to control a logged string, is that the attacker gains remote code execution on the application that the logs were sent from.

This exploit after initial finding, motivated attackers worldwide to attempt to launch attacks on every application that uses Log4J. This exploitation sent the cyber security teams of applications into a fervor ensuring that the logging exploit was removed and/or patched before any further transmissions from their servers, these delays and code changes easily translate to billions of dollars in lost time due to the massive scope of applications using Log4J. The attackers created a simple script hosted on Github that any novice could use to fish for a vulnerable domain by sending requests to random HTTP servers.

FIN7 Malware-ladened USBs - https://gizmodo.com/hackers-have-been-sending-malware-filled-usb-sticks-to-1848323578

Malware itself, while very technically complicated, often relies on low-tech social engineering to place itself on the desired system to enact itself. In the case of FIN7's exploit, they sent malware-filled USB sticks via mail to companies disguised as Christmas presents. Some unsuspecting employees will attempt to view their Christmas present on the USB sticks. Once connected to a company computer, the malware/ransomware can be deployed. This attack was effective in many cases and while the gullible employees are certainly at fault, the vulnerability can easily be prevented with a corporate security policy in place. The attacks can be avoided with a rule that either blocks USBs (a bit extreme) or makes USBs read only with no possible execution.

This attack was mostly enacted with planting ransomware onto computers via the USB drives. The nature of ransomware allowed the hackers to extract over a billion dollars of money from companies to remove the locks/malware on their data and systems. Not all of this billion was from this specific holiday season, but over several years. This exploit is not particularly complex from a technical standpoint, the hardest part is finding the weak link in a company that will fall for the ruse.