Zeus/Zbot

Zeus is the name for a family, or perhaps ecosystem of malware that is created and customised using a single toolkit. Not only does the toolkit generate the executable that infects systems, but it also produces server files that act as the command and control infrastructure for the operator's botnet. Primarily Zeus is used to steal banking details through the use of keystroke logging and screen captures that are sent from the infected system to the command and control sever. The infection targets only Windows systems and is typically installed on the target system through social engineering, spam and web browser exploits.

The creator of Zeus has claimed to have stopped developing the toolkit and sold it to the author of SpyEye, a competing toolkit. The source code for the toolkit has also leaked to the public and is widely available, which may result in the release of similar malware in the future.

Zeus botnets can be tracked at the network level using data available from https://zeustracker.abuse.ch/ [1]. Due to the large number of variants created by the toolkit detection and removal can be difficult. Seek advice from your anti-virus vendor for further information.

Information on how this malware operates can be found at http://www.fortiguard.com/analysis/zeusanalysis.html [2] and on the network traffic it creates at http://labs.snort.org/papers/zeus.html [3].

Links
[1] https://zeustracker.abuse.ch/
[2] http://www.fortiguard.com/analysis/zeusanalysis.html
[3] http://labs.snort.org/papers/zeus.html