Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:49:57 UTC

(FireEye) FormBook is a data stealer, but not a full-fledged banker (banking malware). It does not currently have any extensions or plug-ins. Its capabilities include:

• Key logging
• Clipboard monitoring
• Grabbing HTTP/HTTPS/SPDY/HTTP2 forms and network requests
• Grabbing passwords from browsers and email clients
• Screenshots

FormBook can receive the following remote commands from the C2 server:

• Update bot on host system
• Download and execute file
• Remove bot from host system
• Launch a command via ShellExecute
• Clear browser cookies
• Reboot system
• Shutdown system
• Collect passwords and create a screenshot
• Download and unpack ZIP archive
