Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:37:13 UTC

DescriptionCurrently, we identify this malware family as “Ghambar,” due to the word being used in some function names and variables inside the same malware’s code; also subsequent samples expose potentially personally identifiable information and alternative names. While Ghambar does not seem to share any significant codebase with past tools, we believe that Ghambar might be the successor of TinyZBot, which is one of the artifacts described by Cylance in the Operation Cleaver report. Similar to TinyZBot, Ghambar is also developed in C# and it employs the same SOAPbased command and control protocol. While it is provided with fewer features, Ghambar appears better designed and with a cleaner code style.

Interestingly, Ghambar is designed to leave as little footprint on the system as possible. When collecting screenshots, clipboard data, and intercepted keystrokes, it attempts to directly send the data to the C&C without writing on disk.

While executing a parallel keylogger, Ghambar is also able to receive instructions from the C&C on additional tasks to execute. These tasks can be additional plugins to be downloaded and executed, generic tasks on the file system, or a number of predefined commands.

Ghambar is provided with a fullfeatured plugins system. If instructed to do so by the C&C, the malware is able to download, store, and execute any given plugin.

Other than generally creating, deleting and fetching files, Ghambar is also able to executed a number of predefined commands if instructed to do so by the C&C. The commands, identified by a commandtype identifier, include the following:
• Selfdestruct;
• Execute a command through 'cmd.exe' and return output;
• Take a screenshot;
• Shutdown the computer;
• Restart the computer;
• Logoff the user;
• Lock the computer;
• Turn on and off the monitor;
• Set and copy clipboard data;
• Enable or disable mouse/keyboard (although these procedures are not yet implemented);
• “Enable or disable desktop” (not implemented);
• Trigger a BSOD (also, not implemented).

While the sample we obtained might be an earlier stage still under development, Ghambar is alreadyprovided with enough features to make it a fullyfunctional backdoor.
