Schadprogramm IceRat hat es auf Nutzerpasswörter und illegales Coin-Mining abgesehen - Dabei wird auf außergewöhnliche Strategien gesetzt, um nicht entdeckt zu werden

Die Schadsoftware IceRat spioniert die Zugangsdaten von Nutzern für verschiedene Online-Dienste aus und kann bei einer Infektion ungewollt die Stromrechnung von Anwendern in die Höhe treiben - durch verdecktes illegales Coin-Mining. Technisch haben sich die Entwickler einiges ausgedacht, um eine Erkennung des Schadcodes durch Sicherheitslösungen zu verhindern.
G DATA-Virusanalyst Karsten Hahn hat IceRat genauer unter die Lupe genommen. Gelangt das gefährliche Schadprogramm auf den Computer, späht es die Zugangsdaten für verschiedene Online-Dienste, zum Beispiel Facebook oder Amazon aus. Diese Informationen alleine reichen den Kriminellen allerdings nicht aus: Sie installieren zusätzlich einen Coin-Miner, der illegal digitale Währungen schürft. So verdienen die Täter zusätzlich Geld und die Opfer haben es mit einer erhöhten Stromrechnung zu tun.

Cyberkriminelle setzen auf eine Doppelstrategie, um Virenschutzlösungen auszutricksen

Bei IceRat haben die Angreifer die Schadfunktionen nicht in eine Datei geschrieben, sondern diese auf mehrere Komponenten verteilt, die zu der Malware zusammengesetzt wurden. Bei den meisten dieser Bestandteile ist der Analyst auf eine Programmiersprache gestoßen, die für Schadcode sehr ungewöhnlich ist: JPHP. Dabei handelt es sich um eine PHP-Implementierung, die in der virtuellen Maschine von Java läuft.

Durch dieses Vorgehen versuchen die Cyberkriminellen Sicherheitslösungen auszutricksen, um eine Erkennung zu verhindern. Wenn einzelnen Dateien des Schadprogramms der Gesamtkontext fehlt, ist es schwer, diese als bösartig zu identifizieren. Die Nutzung von JPHP ist ebenfalls so ungewöhnlich, dass viele Sicherheitslösungen nicht Alarm schlagen.

"IceRat ist sehr gefährlich und schädigt Nutzer gleich in zweierlei Hinsicht. Eine Infektion führt dazu, dass nicht nur Passwörter in fremde Hände geraten und lukrativ in speziellen Untergrundmärkten verkauft werden können. Gleichzeitig wird der Computer auch noch für illegales Coin-Mining missbraucht. Damit verdienen die Angreifer doppelt auf Kosten ihrer Opfer", sagt Karsten Hahn, Virusanalyst bei G DATA CyberDefense.