Grasshopper

7 April, 2017

Today, April 7th 2017, WikiLeaks releases Vault 7 "Grasshopper" -- 27 documents from the CIA's Grasshopper framework, a platform used to build customized malware payloads for Microsoft Windows operating systems.

Grasshopper is provided with a variety of modules that can be used by a CIA operator as blocks to construct a customized implant that will behave differently, for example maintaining persistence on the computer differently, depending on what particular features or capabilities are selected in the process of building the bundle. Additionally, Grasshopper provides a very flexible language to define rules that are used to "perform a pre-installation survey of the target device, assuring that the payload will only [be] installed if the target has the right configuration". Through this grammar CIA operators are able to build from very simple to very complex logic used to determine, for example, if the target device is running a specific version of Microsoft Windows, or if a particular Antivirus product is running or not.

Grasshopper allows tools to be installed using a variety of persistence mechanisms and modified using a variety of extensions (like encryption). The requirement list of the *Automated Implant Branch* (AIB) for Grasshopper puts special attention on PSP avoidance, so that any *Personal Security Products* like 'MS Security Essentials', 'Rising', 'Symantec Endpoint' or 'Kaspersky IS' on target machines do not detect Grasshopper elements.

One of the persistence mechanisms used by the CIA here is 'Stolen Goods' - whose "components were taken from malware known as Carberp, a suspected Russian organized crime rootkit." confirming the recycling of malware found on the Internet by the CIA. "The source of Carberp was published online, and has allowed AED/RDB to easily steal components as needed from the malware.". While the CIA claims that "[most] of Carberp was not used in Stolen Goods" they do acknowledge that "[the] persistence method, and parts of the installer, were taken and modified to fit our needs", providing a further example of reuse of portions of publicly available malware by the CIA, as observed in their analysis of leaked material from the italian company "HackingTeam".

The documents WikiLeaks publishes today provide an insights into the process of building modern espionage tools and insights into how the CIA maintains persistence over infected Microsoft Windows computers, providing directions for those seeking to defend their systems to identify any existing compromise.