An Overview of Google Rapid Response

Jeff Malavasi
Dept. of Computing Security
Rochester Institute of Technology
Email: jm3378@rit.edu

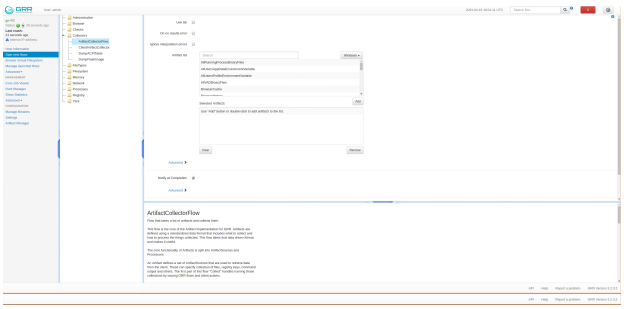
I. Introduction

Google Rapid Response is agent-based solution that can be quickly deployed in order to conduct a forensic investigation against an environment [1]. Once a client is configured with the agent, customized flows are used to gather artifacts from the host and send them back to a centralized server. These artifacts vary depending on the host operating system but can include metrics such as running processes, services, antivirus detections, registry keys, and more. A set of flows can be combined into a hunt, which can be run against the population on a scheduled interval. Hunts are often customized based on the organizational unit or function of the asset. The tool should be used when an organization needs to determine whether or not it has been attacked, as well as to proactively hunt for indicators of compromise (IOCs). In this report, GRR was first used to establish a baseline against a clean Windows 7 virtual machine, before infecting it with malware. GRR is then used in order to detect IOCs.

II. Methods

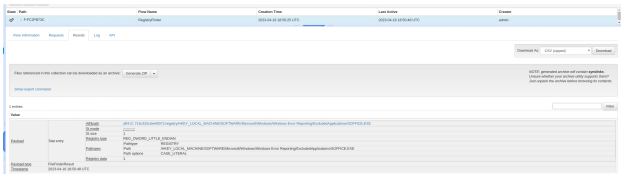
A. Installation & Setup

Google Rapid Response (GRR) is installed by first setting up the centralized server. This host will be used to remotely connect to clients in order to gather artifacts, which will be later stored in a database. Next, each machine that will be investigated needs to be setup with the GRR monitor agent. The agent support many operated systems and can be deployed at scale using group policy or mobile device management. In order to collect information, a flow must be configured and launched. Below is an example of the artifact collection flow that can be used to quickly scan a host.

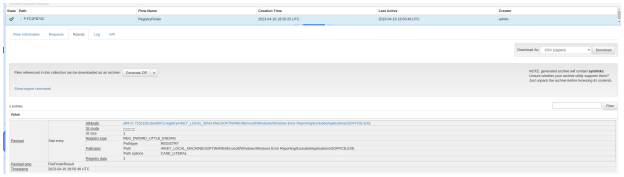


B. Registry Finder

The first flow that was investigated was registry finder. This flow is part of the default configuration and can be used to enumerate any part of the Windows registry. This is useful in order to look for binaries that have registered themselves to start automatically, modified system settings, or attempts to evade detection. For example, malware may exclude itself from Windows error reporting in order to prevent Microsoft from receiving copies of the code. In order to detect this, the registry finder flow can be used in order to list the contents of ExcludedApplications key in the Windows Error Reporting Hive.

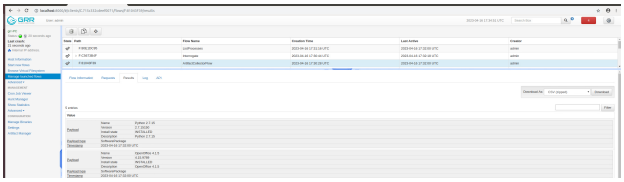


The malware creates a record for the soffice.exe binary that prevents it from being reported to Microsoft.



C. Artifact: WMIInstalledSoftware

The next collection that was investigated was the WMI-InstalledSoftware artifact. On Windows systems, WMI is a built in database that stores information about the systems hardware, software and configuration. This artifact gathers all of the installed applications on the system. This can be used to monitor for new applications, which can be fed into a sandbox to be safely evaluated. Additionally, organizations can use this to detect unsanctioned software within the environment. After infection, this flow was used to detect the installation of OpenOffice.



D. Artifact: WindowsPersistentMechanismFiles

The final artifact that was collected was the WindowsPersis-tentMechanismFiles artifact. When creating malware, authors often write backdoors that enable them to have persistent access to a host after infection. This allows them to continue

to maintain a foothold in an environment even if the initial source of infection is removed. This artifact looks for files on the host system that are likely to be used to maintain persistent access. In the tested malicious file, a binary called scalc.exe is created as a backdoor.

III. Conclusion

GRR can be used to conduct an investigation across a large enterprise in both proactive and reactive scenarios. In this example, GRR was used in order to detect indicators of compromise of a known malicious binary. The relevant flows could be later combined into a hunt in order to determine how much exposure the malware has across the organization. As more and more organization shift to a remote and mobile workforce, hunting for indicators of compromise on employee endpoints will become extremely important.

References

[1] G. Team, "Read the docs: Google rapid response," https://grr-doc.readthedocs.io/en/latest/, 2021.