BumbleBee hunting with a Velociraptor

sec-consult.com/blog/detail/bumblebee-hunting-with-a-velociraptor/

During his research, he used several tools and techniques to define ways to detect the presence of BumbleBee on a compromised infrastructure.

The various detection opportunities described in the report can be useful for organizations to detect an infection in its first stages and, therefore, prevent further malicious activity starting from BumbleBee. The detection opportunities rely on open-source tools (e.g., Velociraptor) and rules (e.g., Yara, Sigma) so they can be used by any company or the wider community.

SEC Defence offers Threat Hunting and Incident Response services to support clients in promptly detecting and responding to cyber threats such as BumbleBee. To request immediate support in case of a potential incident or breach, get in touch with SEC Defence.

Introduction

Ransomware attacks, combined with **data exfiltration**, are one of the **most relevant cyber threats** for companies worldwide, as reported by the Enisa Threat Landscape 2022. According to the NIST's Incident Handling guide, the prevention and detection phases of those types of attacks can be crucial to minimize the potential incident's impacts (e.g., operational, legal, etc.).

To gain initial access into a victim's infrastructure, ransomware operators abuse mostly the following techniques:

- **Phishing campaigns**, also conducted by initial access brokers[1], that deliver malware which acts as a loader for subsequent post-exploitation frameworks like Cobalt Strike or Meterpreter.
- **Exposed vulnerable services** that can be exploited to execute arbitrary commands remotely.
- **Compromised accounts** that allow the threat actor to login into services like VPN.

One of the newest malware families, first discovered by the Google Threat Analysis Group in 2021, and delivered by initial access brokers is called BumbleBee and it has been used by the well-known Russian group *Wizard Spider* which has been linked to ransomware like Conti, Quantum, Royal, etc.

In this article, SEC Defence shows the analysis that has been performed of a BumbleBee sample and provides some threat hunting methods to detect BumbleBee techniques.

BumbleBee

BumbleBee is commonly distributed via malicious ISO images. and abuses thread-hijacking emails to induce the victims to download the ISO file and subsequently open it. When executed, BumbleBee performs mainly the following actions:

- Verifies if it is running in an analysis or sandboxing environment by performing various checks like enumerating the registry keys and drivers related to VMware or VirtualBox.
- Gathers information about the compromised system through WMI queries.
- Connects to the command and control (C2) servers embedded into the malware configuration that is RC4 encrypted.

Furthermore, BumbleBee can also receive specific commands from the threat actors that can be useful for further malicious actions like achieving persistence and downloading other malware (e.g., Cobalt Strike).