Nhat Le
CS479
Assignment 2
2/12/2024

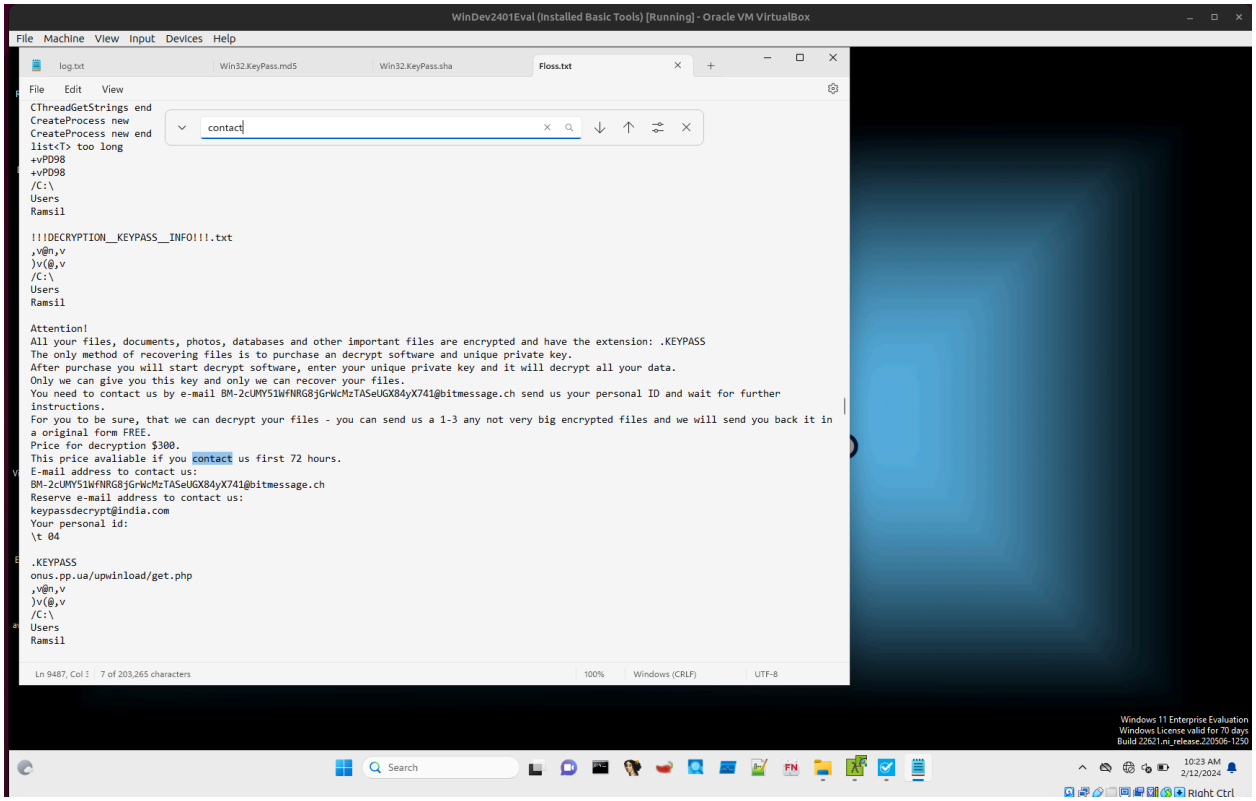
Basic Static Analysis Report

Type of Malware

File Type: PE executable, Target Intel 386, for Microsoft Windows

From What I see from VirusTotal, it has characteristics of worms since it looks for Network Share and characteristics of Virus since it affects other files on host.

From Floss.exe, I think this is a Ransom



From what I see from Floss.exe, I see multiple files like “delself.bat” looks like to delete itself And “http://kronus.pp.ua/upwinload/get.php” which looks like to get files or payload from another location. That makes me think this might be a Dropper but I am not sure.

From VirusTotal, this Host-based behavior

b067642173874bd2766da0d108401b4cf45d6e2a8b3971d95bf474be4f6282

From what I see, I think this is associated with a payload rather than a dropper or loader. The behaviors include actions such as manipulating processes, file systems, registry settings, services, and networking. These actions show that the malware performs malicious activities on the system.

Signatures

SHA256 hash: 35b067642173874bd2766da0d108401b4cf45d6e2a8b3971d95bf474be4f6282

MD5 hash: 6999c944d1c98b2739d015448c99a291

SHA1: d9beb50b51c30c02326ea761b5f1ab158c73b12c

Indicators of Compromise

I check Floss output and behaviors of the malware on VirusTotal and this is what I found

1. **Is there a file that gets created?**
    - Yes, several file-related actions are mentioned, such as "create file on Windows," "read file on Windows," "write file on Windows," "move file," "enumerate files on Windows," "enumerate files recursively," "check if file exists," "delete file," "get common file path," "copy file."
2. **Is a registry key changed?**
    - Yes, the behavior includes actions such as "query or enumerate registry value," "delete registry value," "set registry value," "delete registry key."
3. **Is there a particular IP address or hostname it will contact?**
    - I can't find any information that shows the malware will contact any IP or hostname.
4. **Will it open a port?**
    - The behavior does not explicitly mention opening ports. However, actions like "enumerate network shares" and potential interactions with services could involve port-related activities.
5. **Will it connect to a VPN or Wireguard?**
    - I can't find any information that shows the malware will connect to a VPN or Wireguard

In brief, it has variable operations which include file operations, registry modifications, and potentially the network-related actions. However, I can't find a sign of clear connection to specific IP addresses or hostnames, opened ports, or connecting to a VPN or Wireguard. However, these actions can also be part of the overall behavior of the malware but not be listed from basic static analysis.