Detecting REvil ransomware infections

You work for a Managed Security Provider (MSP). A user in your organization turns on their desktop one morning and is greeted by a message claiming that files on the system have been encrypted and payment must be made to get the files back. You find out that Kaseya VSA, remote monitoring management (RMM) software used by your organization and other MSPs, has been compromised by REvil ransomware and is being used to distribute ransomware to its on-premises customers. You hear that the infection is spreading even to other organizations that don’t use Kaseya.

As a security analyst, it is your goal to investigate the ransomware by attempting to reconstruct the events that led to the system being infected. You also want to understand the full scope of the security breach and prevent additional systems from becoming infected. You can use Splunk software to investigate programs or binaries that executed on the infected system, examine connections the infected machine had to other network devices, construct a timeline of events, and create traffic flow diagrams to help visualize what happened.

Required data

- Microsoft: Windows event logs
- Microsoft: Sysmon

How to use Splunk software for this use case

You can run many searches with Splunk software to identify signs of ransomware infections. Depending on your environment and requirements, you might find it useful to run some or all of the following:

- Microsoft Defender capabilities disabled
- Windows Defender status disabled or changed
- DLL loaded in a specific process
- Executable payload added through the command line

Next steps

If any results indicate the infection has been detected, then the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.

The content in this guide comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed.