Changes in REvil ransomware version 2.2

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 14:18:00 UTC

By the Intel 471 Malware Intelligence team.

Summary

The REvil ransomware-as-a-service (RaaS) operation continues to impact businesses worldwide. The threat actors responsible for developing and maintaining the malware have released an updated ransomware, namely version 2.2. In this short blog post, we will cover the significant changes from the previous version, which we covered in detail in an earlier blog post (see: https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/).

Persistence mechanism

REvil ransomware persists on a machine if the **arn** configuration field is set to **true**. It writes its path to the registry key **SOFTWARE\Microsoft\Windows\CurrentVersion\Run**. An example of the value name of the registry key entry is **mjOObKp0yy**.


revil

In version 2.1, first collected by our systems March 15, 2020, this persistence mechanism was removed. It seems this little experiment didn’t go as planned, because the new version 2.2 brings the same persistence mechanism back!

Restart Manager to terminate processes

One of the more interesting new features of REvil version 2.2 is the use of the Windows Restart Manager to terminate processes and services that can lock files targeted for encryption. If a process has an open file handle for a specific file, then writes to that file by another process (in this case, a ransomware) it will be prevented by the Windows operating system (OS). To circumvent this, the REvil developers have implemented a technique using the Windows Restart Manager also used by other ransomware such as SamSam and LockerGoga (see: https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/).

REvil ransomware opens files for encryption with no sharing (dwShareMode equals 0). As a result, the Restart Manager is invoked whenever a sharing violation occurs when opening an already opened file.


pasted image 0 6

The function prototype for **rvl_restart_manager** is:

VOID rvl_restart_manager(LPCWSTR Filename, BOOL DoEndSession)

The following explains how REvil employs this technique:

- Call **OpenSCManagerW** to open the “ServicesActive” database.
- Start a new Restart Manager session by calling **RmStartSession** and save the returned handle in a global variable for future calls.
- Invoke **RmRegisterResources** with the target file name to register it to the Restart Manager session.
- Retrieve the list of all applications currently using the file by calling **RmGetList**. This application programming interface (API) returns an array of **RM_PROCESS_INFO** structures.
- If a normal process is using the file, it is terminated by a call to **TerminateProcess**.
- If a service is encountered, **ControlService** is invoked with the **SERVICE_CONTROL_STOP** control code to stop the service followed by a call to **DeleteService**.
- If a critical process is encountered, its critical status is removed by calling **ZwSetInformationProcess** with the information class **ProcessBreakOnTermination** before terminating it. This may lead to undefined behavior on the victim system.

New ‘-silent’ flag

A new command-line option -silent was added that skips termination of blacklisted processes, services and shadow copy deletion. However, this flag does not impact the new Restart Manager functionality.

 pasted image 0 7

Indicators of compromise

 Screen Shot 2020 09 03 at 11.48.30 am

---