Changes in REvil ransomware version 2.2

intel471.com/blog/changes-in-revil-ransomware-version-2-2

```
call    rc4_decrypt_string ; L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
xor     eax, eax
mov     [ebp+var_1E], ax
lea     eax, [ebp+var_1C]
push    eax             ; out_buffer
push    14h             ; buffer_length
push    5               ; rc4_key_length
push    0BBFh           ; rc4_key_offset
push    edi             ; rc4_array
call    rc4_decrypt_string ; L"mjOObKp0yy"
xor     eax, eax
mov     [ebp+var_8], ax
mov     eax, [ebp+var_4]
lea     eax, ds:2[eax*2]
push    eax             ; cbData
push    esi             ; lpData
push    REG_SZ          ; dwType
lea     eax, [ebp+var_1C]
push    eax             ; lpValueName
```

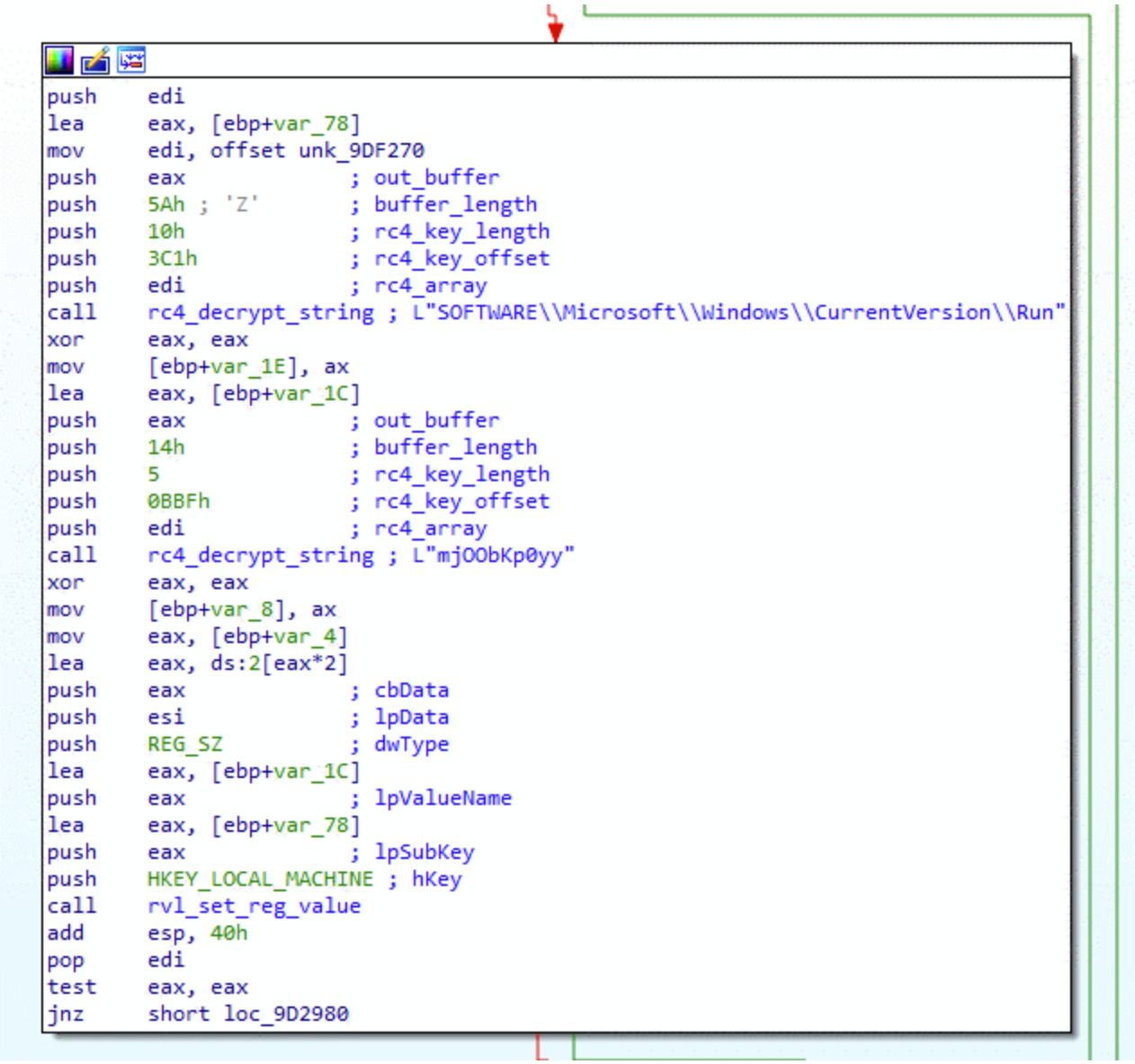
By the Intel 471 Malware Intelligence team.

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**.



```
push    edi
lea     eax, [ebp+var_78]
mov     edi, offset unk_9DF270
push    eax             ; out_buffer
push    5Ah ; 'Z'       ; buffer_length
push    10h             ; rc4_key_length
push    3C1h            ; rc4_key_offset
push    edi             ; rc4_array
call    rc4_decrypt_string ; L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
xor     eax, eax
mov     [ebp+var_1E], ax
lea     eax, [ebp+var_1C]
push    eax             ; out_buffer
push    14h             ; buffer_length
push    5               ; rc4_key_length
push    0BBFh           ; rc4_key_offset
push    edi             ; rc4_array
call    rc4_decrypt_string ; L"mjOObKp0yy"
xor     eax, eax
mov     [ebp+var_8], ax
mov     eax, [ebp+var_4]
lea     eax, ds:2[eax*2]
push    eax             ; cbData
push    esi             ; lpData
push    REG_SZ          ; dwType
lea     eax, [ebp+var_1C]
push    eax             ; lpValueName
lea     eax, [ebp+var_78]
push    eax             ; lpSubKey
push    HKEY_LOCAL_MACHINE ; hKey
call    rvl_set_reg_value
add     esp, 40h
pop     edi
test    eax, eax
jnz     short loc_9D2980
```

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.

```
75    else if ( LastError == ERROR_SHARING_VIOLATION )
76    {
77      rvl_restart_manager(filename, FALSE);
78      rvl_sleep(1000);
79    }
80  }
81  rvl_salsa20_init(filedata_struct);
82  return filedata_struct;
83}
```

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.

```
.text:009D1A73                push    eax             ; out_buffer
.text:009D1A74                push    0Ah             ; buffer_length
.text:009D1A76                push    0Eh             ; rc4_key_length
.text:009D1A78                push    0D7h ; 'x'      ; rc4_key_offset
.text:009D1A7D                push    ebx             ; rc4_array
.text:009D1A7E                call    rc4_decrypt_string ; L"-path"
.text:009D1A83                add     esp, 50h
.text:009D1A86                xor     eax, eax
.text:009D1A88                mov     [ebp+var_12A], ax
.text:009D1A8F                lea     eax, [ebp+s_silent_arg]
.text:009D1A95                push    eax             ; out_buffer
.text:009D1A96                push    0Eh             ; buffer_length
.text:009D1A98                push    10h             ; rc4_key_length
.text:009D1A9A                push    0A84h           ; rc4_key_offset
.text:009D1A9F                push    ebx             ; rc4_array
.text:009D1AA0                call    rc4_decrypt_string ; L"-silent"
.text:009D1AA5                xor     eax, eax
.text:009D1AA7                mov     [ebp+var_176], ax
.text:009D1AAE                lea     eax, [ebp+s_nolan_arg]
.text:009D1AB4                push    eax             ; arg_name
.text:009D1AB5                call    rvl_is_arg_present_in_cmdline
```

Indicators of compromise

Context	Indicator
REvil v2.2 sample	ffe7fe45327645a48ca83b7dd4586de22618206001b7a7354d9d285e0308f195
REvil v2.2 sample	774354fe16764fa513052ff714048858cb315691599a08d13ba56be1c796a16d