LV Ransomware

secureworks.com/research/lv-ransomware

Counter Threat Unit Research Team

Tuesday, June 22, 2021 *By: Counter Threat Unit Research Team*

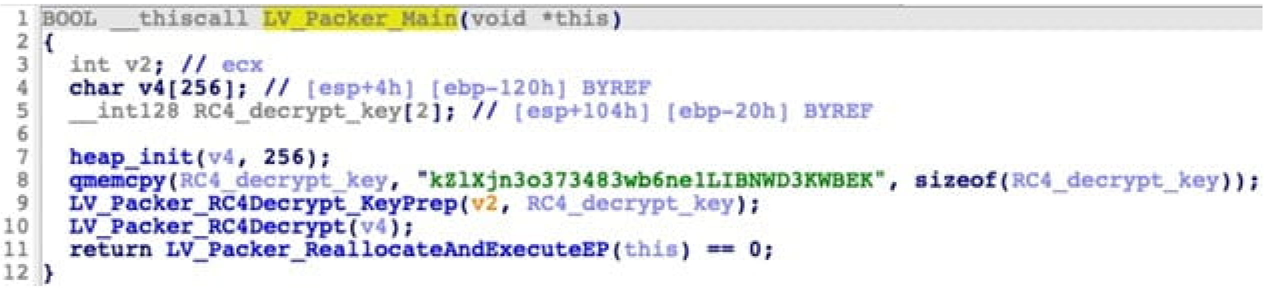
Summary

Secureworks® Counter Threat Unit™ (CTU) researchers investigated reports that the LV ransomware had the same code structure as REvil. This overlap could indicate that the GOLD SOUTHFIELD cybercriminal threat group that operates REvil sold the source code, that the source code was stolen, or that GOLD SOUTHFIELD shared the code with another threat group as part of a partnership. CTU™ analysis confirmed that the GOLD NORTHFIELD threat group, which operates LV, replaced the configuration of a REvil v2.03 beta version to repurpose the REvil binary for the LV ransomware.

CTU researchers have not observed LV ransomware advertisements on underground forums as of this publication. However, variations in partner and campaign IDs across LV configurations and the practice of naming and shaming victims could indicate that GOLD NORTHFIELD is launching a ransomware-as-a-service (RaaS) offering.

LV packer

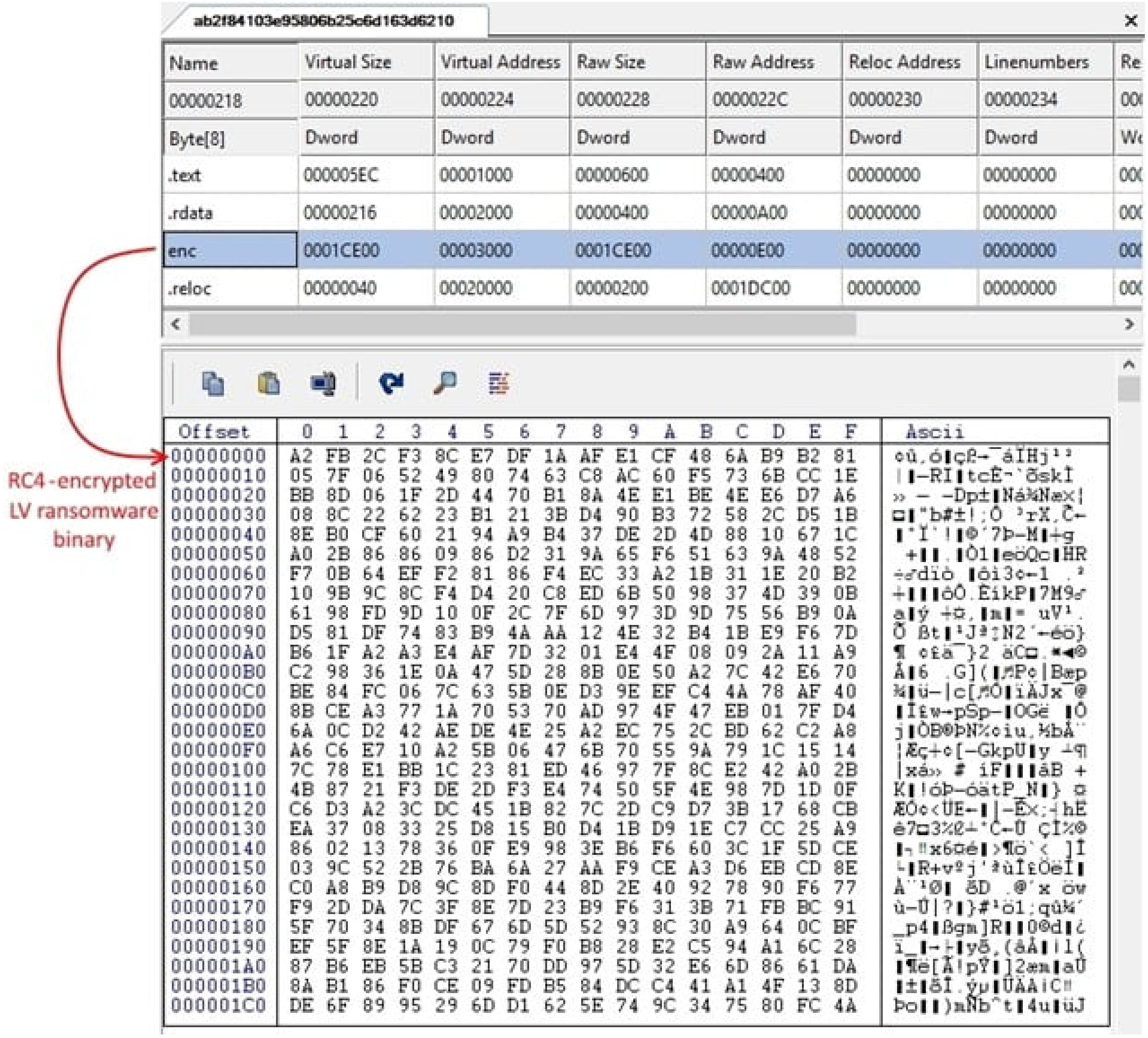
The packed LV ransomware samples identified by CTU researchers appear to use the same basic crypter. Figure 1 shows the entire contents of the packed executable's main function, which contains five of the executable's nine functions.



```
BOOL __thiscall LV_Packer_Main(void *this)
{
  int v2; // ecx
  char v4[256]; // [esp+4h] [ebp-120h] BYREF
  __int128 RC4_decrypt_key[2]; // [esp+104h] [ebp-20h] BYREF

  heap_init(v4, 256);
  qmemcpy(RC4_decrypt_key, "kZlXjn3o373483wb6nelLIBNWD3KWBEK", sizeof(RC4_decrypt_key));
  LV_Packer_RC4Decrypt_KeyPrep(v2, RC4_decrypt_key);
  LV_Packer_RC4Decrypt(v4);
  return LV_Packer_ReallocateAndExecuteEP(this) == 0;
}
```

Figure 1. Main function for the packer used to unpack and execute LV ransomware. (Source: Secureworks)

The packed executable stores the LV ransomware binary as RC4-encrypted data within a section named 'enc' (see Figure 2).



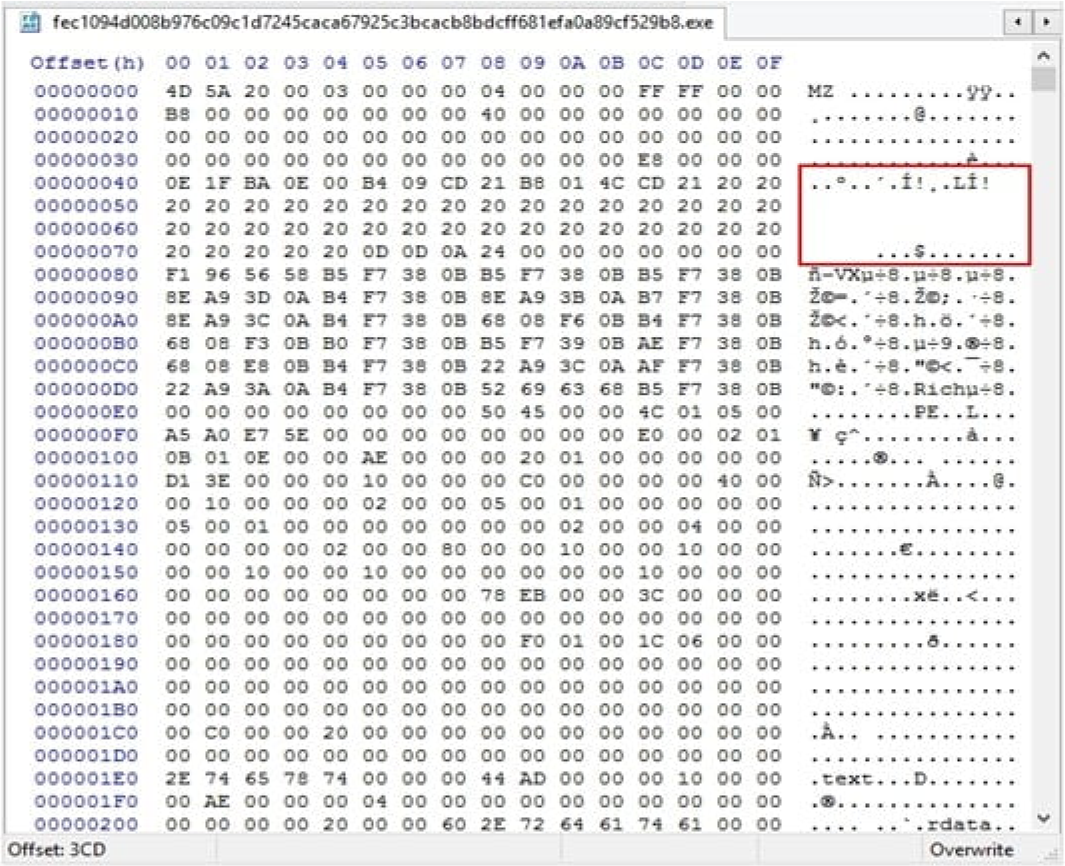
ab2f84103e95806b25c6d163d6210

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Re
00000218	00000220	00000224	00000228	0000022C	00000230	00000234	00
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	W
.text	000005EC	00001000	00000600	00000400	00000000	00000000	00
.rdata	00000216	00002000	00000400	00000A00	00000000	00000000	00
enc	0001CE00	00003000	0001CE00	00000E00	00000000	00000000	00
.reloc	00000040	00020000	00000200	0001DC00	00000000	00000000	00

```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000000  A2 FB 2C F3 8C E7 DF 1A AF E1 CF 48 6A B9 B2 81
00000010  05 7F 06 52 49 80 74 63 C8 AC 60 F5 73 6B CC 1E
00000020  BB 8D 06 1F 2D 44 70 B1 8A 4E E1 BE 4E E6 D7 A6
00000030  08 8C 22 62 23 B1 21 3B D4 90 B3 72 58 2C D5 1B
00000040  8E B0 CF 60 21 94 A9 B4 37 DE 2D 4D 88 10 67 1C
00000050  A0 2B 86 86 09 86 D2 31 9A 65 F6 51 63 9A 48 52
00000060  F7 0B 64 EF F2 81 86 F4 EC 33 A2 1B 31 1E 20 B2
00000070  10 9B 9C 8C F4 D4 20 C8 ED 6B 50 98 37 4D 39 0B
00000080  61 98 FD 9D 10 0F 2C 7F 6D 97 3D 9D 75 56 B9 0A
00000090  D5 81 DF 74 83 B9 4A AA 12 4E 32 B4 1B E9 F6 7D
000000A0  B6 1F A2 A3 E4 AF 7D 32 01 E4 4F 08 09 2A 11 A9
000000B0  C2 98 36 1E 0A 47 5D 28 8B 0E 50 A2 7C 42 E6 70
000000C0  BE 84 FC 06 7C 63 5B 0E D3 9E EF C4 4A 78 AF 40
000000D0  8B CE A3 77 1A 70 53 70 AD 97 4F 47 EB 01 7F D4
000000E0  6A 0C D2 42 AE DE 4E 25 A2 EC 75 2C BD 62 C2 A8
000000F0  A6 C6 E7 10 A2 5B 06 47 6B 70 55 9A 79 1C 15 14
00000100  7C 78 E1 BB 1C 23 81 ED 46 97 7F 8C E2 42 A0 2B
00000110  4B 87 21 F3 DE 2D F3 E4 74 50 5F 4E 98 7D 1D 0F
00000120  C6 D3 A2 3C DC 45 1B 82 7C 2D C9 D7 3B 17 68 CB
00000130  EA 37 08 33 25 D8 15 B0 D4 1B D9 1E C7 CC 25 A9
00000140  86 02 13 78 36 0F E9 98 3E B6 F6 60 3C 1F 5D CE
00000150  03 9C 52 2B 76 BA 6A 27 AA F9 CE A3 D6 EB CD 8E
00000160  C0 A8 B9 D8 9C 8D F0 44 8D 2E 40 92 78 90 F6 77
00000170  F9 2D DA 7C 3F 8E 7D 23 B9 F6 31 3B 71 FB BC 91
00000180  5F 70 34 8B DF 67 6D 5D 52 93 8C 30 A9 64 0C BF
00000190  EF 5F 8E 1A 19 0C 79 F0 B8 28 E2 C5 94 A1 6C 28
000001A0  87 B6 EB 5B C3 21 70 DD 97 5D 32 E6 6D 86 61 DA
000001B0  8A B1 86 F0 CE 09 FD B5 84 DC C4 41 A1 4F 13 8D
000001C0  DE 6F 89 95 29 6D D1 62 5E 74 9C 34 75 80 FC 4A
```

Figure 2. Encrypted LV ransomware binary stored in the enc section of the packer executable. (Source: Secureworks)

The packed samples analyzed by CTU researchers use the hard-coded "kZlXjn3o373483wb6ne1LIBNWD3KWBEK" key to decrypt the contents of the enc section. The "This program cannot be run in DOS mode" string is removed from decrypted binaries' PE headers (see Figure 3).



fec1094d008b976c09c1d7245caca67925c3bcacb8bdcff681efa0a89cf529b8.exe

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   4D 5A 20 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ .........ÿÿ..
00000010   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ,.......@.......
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00   ............è...
00000040   0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 20 20   ..º..´.Í!¸.LÍ!
00000050   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000060   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000070   20 20 20 20 20 0D 0D 0A 24 00 00 00 00 00 00 00        ...$.......
00000080   F1 96 56 58 B5 F7 38 0B B5 F7 38 0B B5 F7 38 0B   ñ–VXµ÷8.µ÷8.µ÷8.
00000090   8E A9 3D 0A B4 F7 38 0B 8E A9 3B 0A B7 F7 38 0B   Ž©=.´÷8.Ž©;.·÷8.
000000A0   8E A9 3C 0A B4 F7 38 0B 68 08 F6 0B B4 F7 38 0B   Ž©<.´÷8.h.ö.´÷8.
000000B0   68 08 F3 0B B0 F7 38 0B B5 F7 39 0B AE F7 38 0B   h.ó.°÷8.µ÷9.®÷8.
000000C0   68 08 E8 0B B4 F7 38 0B 22 A9 3C 0A AF F7 38 0B   h.è.´÷8."©<.¯÷8.
000000D0   22 A9 3A 0A B4 F7 38 0B 52 69 63 68 B5 F7 38 0B   "©:.´÷8.Richµ÷8.
000000E0   00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00   ........PE..L...
000000F0   A5 A0 E7 5E 00 00 00 00 00 00 00 00 E0 00 02 01   ¥ ç^........à...
00000100   0B 01 0E 00 00 AE 00 00 00 20 01 00 00 00 00 00   .....®... ......
00000110   D1 3E 00 00 00 10 00 00 00 C0 00 00 00 00 40 00   Ñ>.......À....@.
00000120   00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00   ................
00000130   05 00 01 00 00 00 00 00 00 00 02 00 00 04 00 00   ................
00000140   00 00 00 00 02 00 00 80 00 00 10 00 00 10 00 00   .......€........
00000150   00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00   ................
00000160   00 00 00 00 00 00 00 00 78 EB 00 00 3C 00 00 00   ........xë..<...
00000170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000180   00 00 00 00 00 00 00 00 00 F0 01 00 1C 06 00 00   .........ð......
00000190   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001C0   00 C0 00 00 20 00 00 00 00 00 00 00 00 00 00 00   .À.. ...........
000001D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001E0   2E 74 65 78 74 00 00 00 44 AD 00 00 00 10 00 00   .text...D.......
000001F0   00 AE 00 00 00 04 00 00 00 00 00 00 00 00 00 00   .®..............
00000200   00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00   .... ..`.rdata..
```

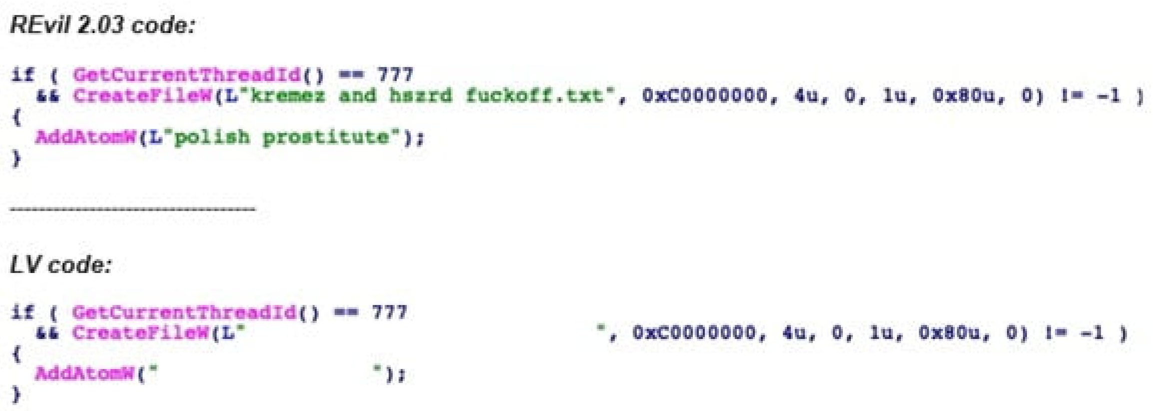
Offset: 3CD   Overwrite

Figure 3. Strings removed from header of decrypted LV binary. (Source: Secureworks)

Once decrypted, the ransomware binary is copied into a new memory allocation created with Read/Write/Execute (RWE) access rights. The packer then executes the unpacked ransomware binary by jumping to the entry point defined in the PE header.

Origin and configuration

The code structure and functionality of the LV ransomware sample analyzed by CTU researchers are identical to REvil. The version value in the LV binary is 2.02, its compile timestamp is 2020-06-15 16:24:05, and its configuration is stored in a section named '.7tdlvx'. These characteristics align with REvil 2.02 samples first identified in the wild on June 17, 2020. The LV sample also contains a code segment that is unique to REvil 2.03. The only purpose of this code segment in REvil binary is to taunt prominent security researchers. LV replaces the insults with the space character (see Figure 4).



REvil 2.03 code:

```
if ( GetCurrentThreadId() == 777
  && CreateFileW(L"kremez and hszrd fuckoff.txt", 0xC0000000, 4u, 0, 1u, 0x80u, 0) != -1 )
{
  AddAtomW(L"polish prostitute");
}
```

LV code:

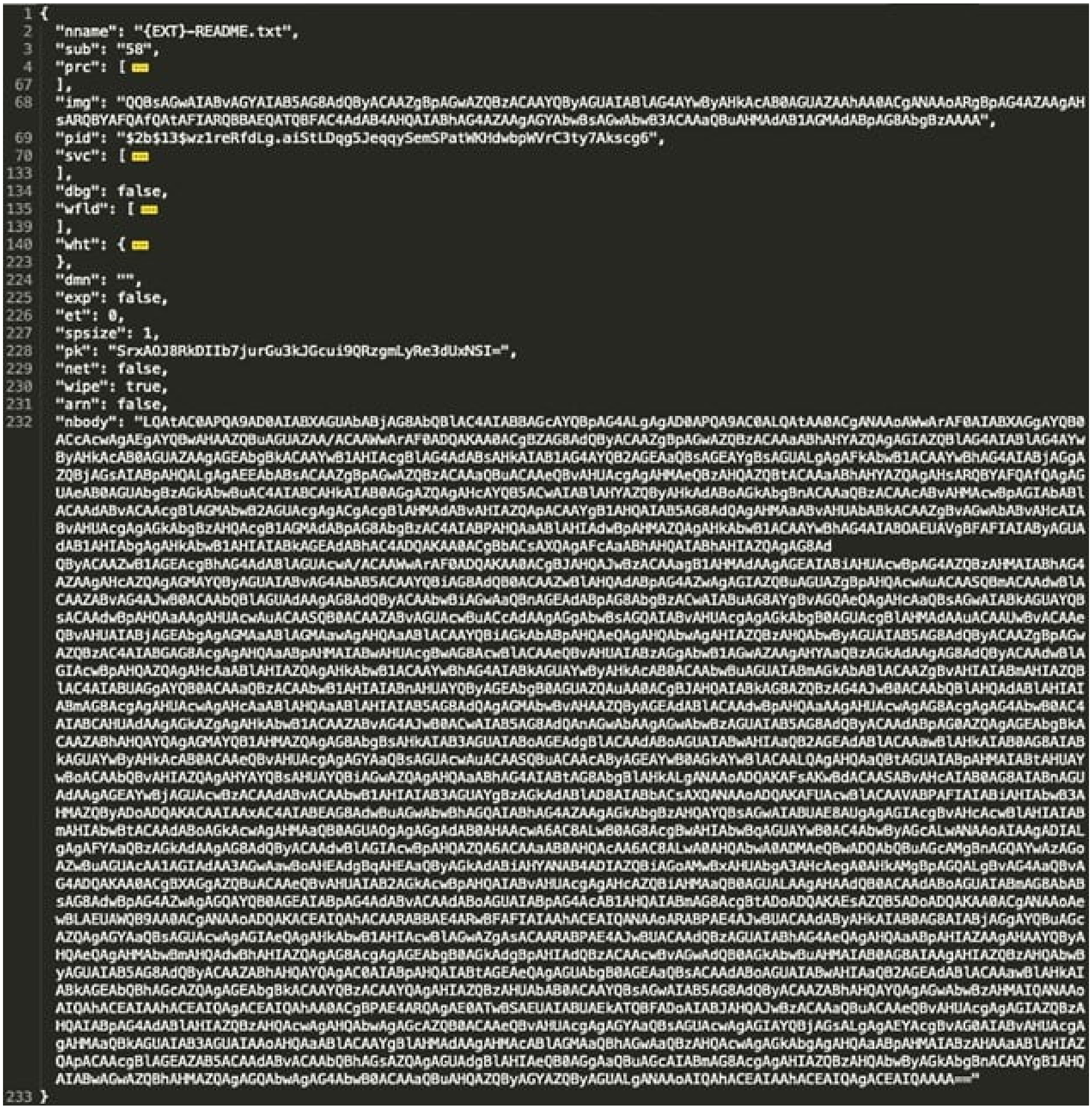
```
if ( GetCurrentThreadId() == 777
  && CreateFileW(L"                              ", 0xC0000000, 4u, 0, 1u, 0x80u, 0) != -1 )
{
  AddAtomW("                 ");
}
```

Figure 4. LV code segment duplicating REvil 2.03 code but replacing strings with spaces. (Source: Secureworks)

This type of code modification suggests that GOLD NORTHFIELD does not have access to REvil's source code. The threat actors likely used a hex editor to remove potentially identifying characteristics from the binary to conceal that LV is a repurposed version of REvil. The hard-coded 2.02 version value and the unique REvil 2.03 code suggests that GOLD NORTHFIELD used a beta version of REvil 2.03 as the basis for LV ransomware.

REvil binary repurposing

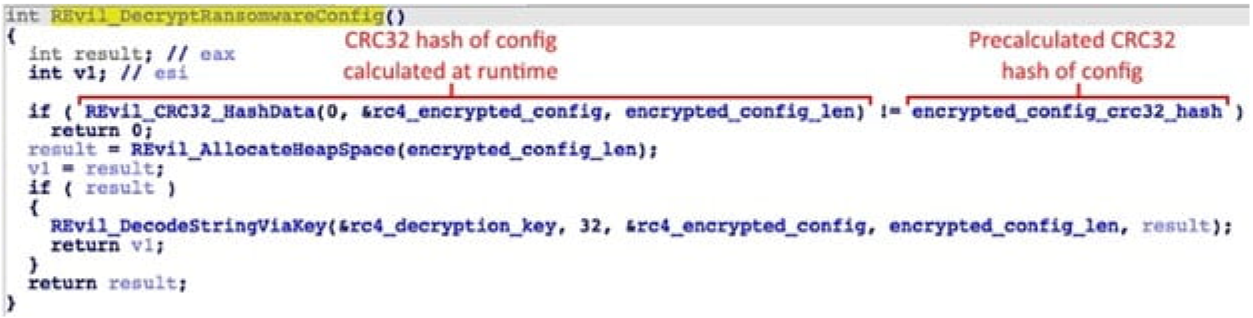
The GOLD NORTHFIELD threat actors replaced the REvil configuration stored within the binary's '.7tdlvx' section with their own configuration. Successful replacement required the format of the REvil and LV configurations to be identical. Figure 5 shows the LV configuration extracted from the REvil binary. It is a JSON-formatted string containing key elements utilized by REvil (e.g., sub, net, dmn, pk).



```
{
  "nname": "{EXT}-README.txt",
  "sub": "58",
  "prc": [ …
  ],
  "img": "QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwByAHkAcAB0AGUAZAAhAA0ACgANAAoARgBpAG4AZAAgAH
  sARQBYAFQAfQAtAFIARQBBAEQATQBFAC4AdAB4AHQAIABhAG4AZAAgAGYAbwBsAGwAbwB3ACAAaQBuAHMAdAB1AGMAdABpAG8AbgBzAAAA",
  "pid": "$2b$13$wz1reRfdLg.aiStLDqg5JeqqySemSPatWKHdwbpWVrC3ty7Akscg6",
  "svc": [ …
  ],
  "dbg": false,
  "wfld": [ …
  ],
  "wht": { …
  },
  "dmn": "",
  "exp": false,
  "et": 0,
  "spsize": 1,
  "pk": "SrxAOJ8RkDIIb7jurGu3kJGcui9QRzgmLyRe3dUxNSI=",
  "net": false,
  "wipe": true,
  "arn": false,
  "nbody": "LQAtAC0APQA9AD0AIABXAGUAbABjAG8AbQBlAC4AIABBAGcAYQBpAG4ALgAgAD0APQA9AC0ALQAtAA0ACgANAAoAWwArAF0AIABXAGgAYQB0
  ACcAcwAgAEgAYQBwAHAAZQBuAGUAZAA/ACAAWwArAF0ADQAKAA0ACgBZAG8AdQByACAAZgBpAGwAZQBzACAAaABhAHYAZQAgAGIAZQBlAG4AIABlAG4AYw
  ByAHkAcAB0AGUAZAAgAGEAbgBkACAAYwB1AHIAcgBlAG4AdABsAHkAIAB1AG4AYQB2AGEAaQBsAGEAYgBsAGUALgAgAFkAbwB1ACAAYwBhAG4AIABjAGgA
  ZQBjAGsAIABpAHQALgAgAEEAbABsACAAZgBpAGwAZQBzACAAaQBuACAAeQBvAHUAcgAgAHMAeQBzAHQAZQBtACAAaABhAHYAZQAgAHsARQBYAFQAfQAgAG
  UAeAB0AGUAbgBzAGkAbwBuAC4AIABCAHkAIAB0AGgAZQAgAHcAYQB5ACwAIABlAHYAZQByAHkAdABoAGkAbgBnACAAaQBzACAAcABvAHMAcwBpAGIAbABl
  ACAAdABvACAAcgBlAGMAbwB2AGUAcgAgACgAcgBlAHMAdABvAHIAZQApACAAYgB1AHQAIAB5AG8AdQAgAHMAaABvAHUAbABkACAAZgBvAGwAbABvAHcAIA
  BvAHUAcgAgAGkAbgBzAHQAcgB1AGMAdABpAG8AbgBzAC4AIABPAHQAaABlAHIAdwBpAHMAZQAgAHkAbwB1ACAAYwBhAG4AIAB0AEUAVgBFAFIAIABlAGUA
  dAB1AHIAbgAgAHkAbwB1AHIAIABkAGEAdABhAC4ADQAKAA0ACgBbACsAXQAgAFcAaABhAHQAIABhAHIAZQAgAG8Ad
  QByACAAZwB1AGEAcgBhAG4AdABlAGUAcwA/ACAAWwArAF0ADQAKAA0ACgBJAHQAJwBzACAAagB1AHMAdAAgAGEAIABiAHUAcwBpAG4AZQBzAHMAIABhAG4
  AZAAgAHcAZQAgAGMAYQByAGUAIABvAG4AbAB5ACAAYQBiAG8AdQB0ACAAZwBlAHQAdABpAG4AZwAgAGIAZQBuAGUAZgBpAHQAcwAuACAASQBmACAAdwBlA
  CAAZABvAG4AJwB0ACAAbQBlAGUAdAAgAG8AdQByACAAbwBiAGwAaQBnAGEAdABpAG8AbgBzACwAIABuAG8AYgBvAGQAeQAgAHcAaQBsAGwAIABkAGUAYQB
  sACAAdwBpAHQAaAAgAHUAcwAuACAASQB0ACAAZABvAGUAcwBuACcAdAAgAGgAbwBsAGQAIABvAHUAcgAgAGkAbgB0AGUAcgBlAHMAdAAuACAAUwBvACAAe
  QBvAHUAIABjAGEAbgAgAGMAaABlAGMAawAgAHQAaABlACAAYQBiAGkAbABpAHQAeQAgAHQAbwAgAHIAZQBzAHQAbwByAGUAIAB5AG8AdQByACAAZgBpAGw
  AZQBzAC4AIABGAG8AcgAgAHQAaABpAHMAIABwAHUAcgBwAG8AcwBlACAAeQBvAHUAIABzAGgAbwB1AGwAZAAgAHYAaQBzAGkAdAAgAG8AdQByACAAdwBlA
  GIAcwBpAHQAZQAgAHcAaABlAHIAZQAgAHkAbwB1ACAAYwBhAG4AIABkAGUAYwByAHkAcAB0ACAAbwBuAGUAIABmAGkAbABlACAAZgBvAHIAIABmAHIAZQB
  lAC4AIABUAGgAYQB0ACAAaQBzACAAbwB1AHIAIABnAHUAYQByAGEAbgB0AGUAZQAuAA0ACgBJAHQAIABkAG8AZQBzAG4AJwB0ACAAbQBlAHQAdABlAHIAI
  ABmAG8AcgAgAHUAcwAgAHcAaABlAHQAaABlAHIAIAB5AG8AdQAgAGMAbwBvAHAAZQByAGEAdABlACAAdwBpAHQAaAAgAHUAcwAgAG8AcgAgAG4AbwB0AC4
  AIABCAHUAdAAgAGkAZgAgAHkAbwB1ACAAZABvAG4AJwB0ACwAIAB5AG8AdQAnAGwAbAAgAGwAbwBzAGUAIAB5AG8AdQByACAAdABpAG0AZQAgAGEAbgBkA
  CAAZABhAHQAYQAgAGMAYQB1AHMAZQAgAG8AbgBsAHkAIAB3AGUAIABoAGEAdgBlACAAdABoAGUAIABwAHIAaQB2AGEAdABlACAAawBlAHkAIAB0AG8AIAB
  kAGUAYwByAHkAcAB0ACAAeQBvAHUAcgAgAGYAaQBsAGUAcwAuACAASQBuACAAcAByAGEAYwB0AGkAYwBlACAALQAgAHQAaQBtAGUAIABpAHMAIABtAHUAY
  wBoACAAbQBvAHIAZQAgAHYAYQBsAHUAYQBiAGwAZQAgAHQAaABhAG4AIABtAG8AbgBlAHkALgANAAoADQAKAFsAKwBdACAASABvAHcAIAB0AG8AIABnAGU
  AdAAgAGEAYwBjAGUAcwBzACAAdABvACAAbwB1AHIAIAB3AGUAYgBzAGkAdABlAD8AIABbACsAXQANAAoADQAKAFUAcwBlACAAVABPAFIAIABiAHIAbwB3A
  HMAZQByADoADQAKACAAIAAxAC4AIABEAG8AdwBuAGwAbwBhAGQAIABhAG4AZAAgAGkAbgBzAHQAYQBsAGwAIABUAE8AUgAgAGIAcgBvAHcAcwBlAHIAIAB
  mAHIAbwBtACAAdABoAGkAcwAgAHMAaQB0AGUAOgAgAGgAdAB0AHAAcwA6AC8ALwB0AG8AcgBwAHIAbwBqAGUAYwB0AC4AbwByAGcALwANAAoAIAAgADIAL
  gAgAFYAaQBzAGkAdAAgAG8AdQByACAAdwBlAGIAcwBpAHQAZQA6ACAAaAB0AHQAcAA6AC8ALwA0AHQAbwA0ADMAeQBwADQAbQBuAGcAMgBnAGQAYwAzAGo
  AZwBuAGUAcAA1AGIAdAA3AGwAawBoAHEAdgBqAHEAaQByAGkAdAB1AHYANAB4ADIAZQB1AGoAMwBxAHUAbgA3AHcAegA0AHkAMgBpAGQALgBvAG4AaQBvA
  G4ADQAKAA0ACgBXAGgAZQBuACAAeQBvAHUAIAB2AGkAcwBpAHQAIABvAHUAcgAgAHcAZQBiAHMAaQB0AGUALAAgAHAAdQB0ACAAdABoAGUAIABmAG8AbAB
  sAG8AdwBpAG4AZwAgAGQAYQB0AGEAIABpAG4AdABvACAAdABoAGUAIABpAG4AcAB1AHQAIABmAG8AcgBtADoADQAKAEsAZQB5ADoADQAKAA0ACgANAAoAe
  wBLAEUAWQB9AA0ACgANAAoADQAKACEAIQAhACAARABBAE4ARwBFAFIAIAAhACEAIQANAAoARABPAE4AJwBUACAAdAByAHkAIAB0AG8AIABjAGgAYQBuAGc
  AZQAgAGYAaQBsAGUAcwAgAGIAeQAgAHkAbwB1AHIAcwBlAGwAZgAsACAARABPAE4AJwBUACAAdQBzAGUAIABhAG4AeQAgAHQAaABpAHIAZAAgAHAAYQByA
  HQAeQAgAHMAbwBmAHQAdwBhAHIAZQAgAG8AcgAgAGEAbgB0AGkAdgBpAHIAdQBzACAAcwBvAGwAdQB0AGkAbwBuAHMAIAB0AG8AIAAgAHIAZQBzAHQAbwB
  yAGUAIAB5AG8AdQByACAAZABhAHQAYQAgAC0AIABpAHQAIABtAGEAeQAgAGUAbgB0AGEAaQBsACAAdABoAGUAIABwAHIAaQB2AGEAdABlACAAawBlAHkAI
  ABkAGEAbQBhAGcAZQAgAGEAbgBkACAAYQBzACAAYQAgAHIAZQBzAHUAbAB0ACAAYQBsAGwAIAB5AG8AdQByACAAZABhAHQAYQAgAGwAbwBzAHMAIQANAAo
  AIQAhACEAIAAhACEAIQAgACEAIQAhAA0ACgBPAE4ARQAgAE0ATwBSAEUAIABUAEkATQBFADoAIABJAHQAJwBzACAAaQBuACAAeQBvAHUAcgAgAGIAZQBzA
  HQAIABpAG4AdABlAHIAZQBzAHQAcwAgAHQAbwAgAGcAZQB0ACAAeQBvAHUAcgAgAGYAaQBsAGUAcwAgAGIAYQBjAGsALgAgAEYAcgBvAG0AIABvAHUAcgA
  gAHMAaQBkAGUAIAB3AGUAIAAoAHQAaABlACAAYgBlAHMAdAAgAHMAcABlAGMAaQBhAGwAaQBzAHQAcwAgAGkAbgAgAHQAaABpAHMAIABzAHAAaABlAHIAZ
  QApACAAcgBlAGEAZAB5ACAAdABvACAAbQBhAGsAZQAgAGUAdgBlAHIAeQB0AGgAaQBuAGcAIABmAG8AcgAgAHIAZQBzAHQAbwByAGkAbgBnACAAYgB1AHQ
  AIABwAGwAZQBhAHMAZQAgAGQAbwAgAG4AbwB0ACAAaQBuAHQAZQByAGYAZQByAGUALgANAAoAIQAhACEAIAAhACEAIQAgACEAIQAhAA=="
}
```

Figure 5. LV configuration. (Source: Secureworks)

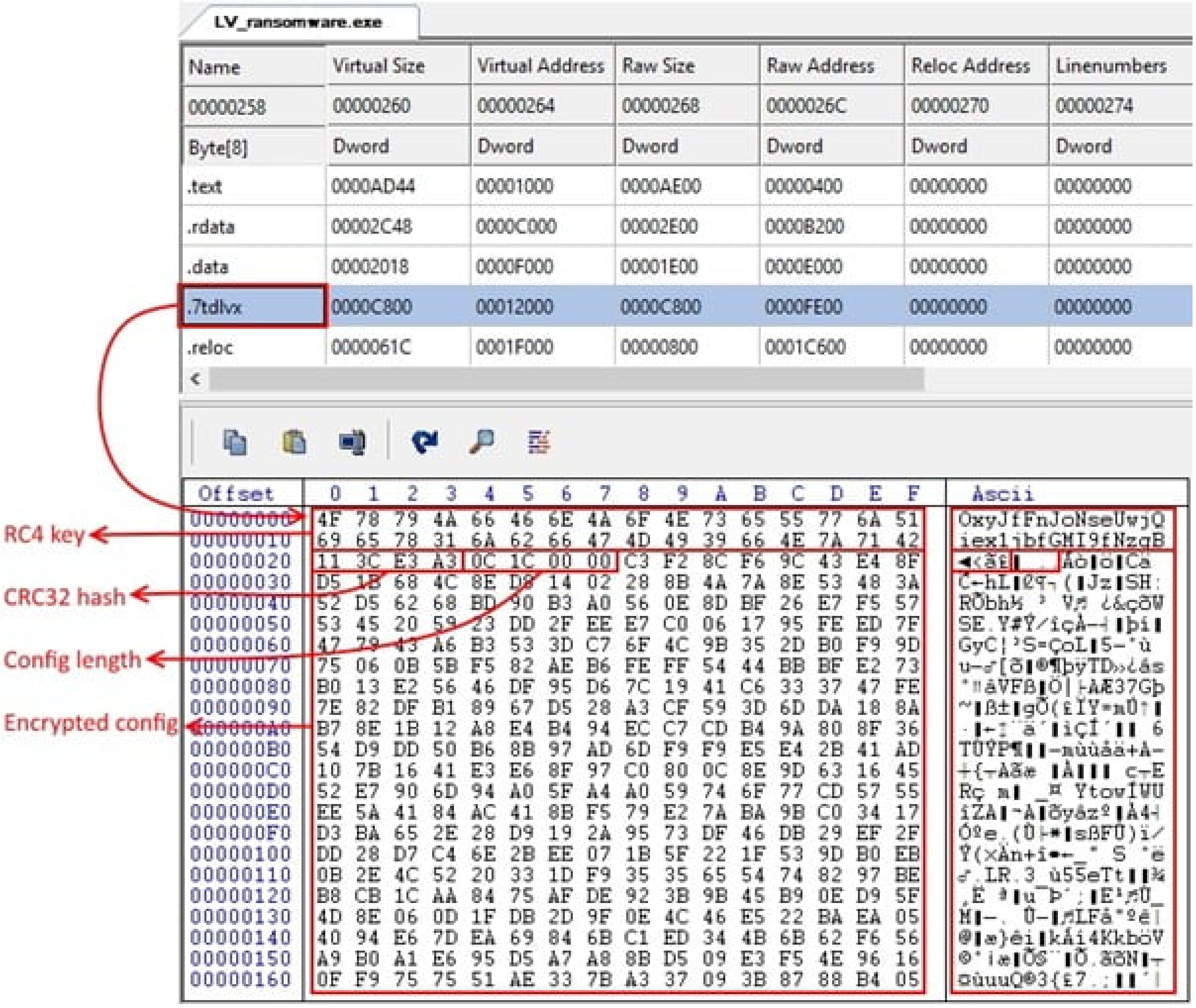
GOLD NORTHFIELD then had to RC4-encrypt the LV configuration with a 32-byte key. To bypass REvil's anti-tamper control that ensures the integrity of the configuration (see Figure 6), GOLD NORTHFIELD also had to generate a CRC32 hash of the updated encrypted configuration and then replace the hard-coded precalculated CRC32 hash stored in the binary with the updated configuration's CRC32 hash. These changes are necessary because the REvil code calculates the configuration's CRC32 hash value at runtime and terminates if the calculated and hard-coded hashes do not match.



```
int REvil_DecryptRansomwareConfig()
{
  int result; // eax
  int v1; // esi

  if ( REvil_CRC32_HashData(0, &rc4_encrypted_config, encrypted_config_len) != encrypted_config_crc32_hash )
    return 0;
  result = REvil_AllocateHeapSpace(encrypted_config_len);
  v1 = result;
  if ( result )
  {
    REvil_DecodeStringViaKey(&rc4_decryption_key, 32, &rc4_encrypted_config, encrypted_config_len, result);
    return v1;
  }
  return result;
}
```

Figure 6. Configuration anti-tamper control implemented in the REvil binary. (Source: Secureworks)

Finally, GOLD NORTHFIELD could add the RC4 key used to encrypt the configuration, the CRC32 hash of the encrypted configuration, the length of the encrypted configuration, and the encrypted configuration itself to the REvil binary via the identified configuration section (.7tdlvx) in the defined order (see Figure 7).



LV_ransomware.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers
00000258	00000260	00000264	00000268	0000026C	00000270	00000274
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	0000AD44	00001000	0000AE00	00000400	00000000	00000000
.rdata	00002C48	0000C000	00002E00	0000B200	00000000	00000000
.data	00002018	0000F000	00001E00	0000E000	00000000	00000000
.7tdlvx	0000C800	00012000	0000C800	0000FE00	00000000	00000000
.reloc	0000061C	0001F000	00000800	0001C600	00000000	00000000

```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000000 4F 78 79 4A 66 46 6E 4A 6F 4E 73 65 55 77 6A 51  OxyJfFnJoNseUwjQ
00000010 69 65 78 31 6A 62 66 47 4D 49 39 66 4E 7A 71 42  iex1jbfGMI9fNzqB
00000020 11 3C E3 A3 0C 1C 00 00 C3 F2 8C F6 9C 43 E4 8F  ◄<ã£      Ãò ö Cä
00000030 D5 1B 68 4C 8E D9 14 02 28 8B 4A 7A 8E 53 48 3A  Õ hL Ù¶ ( Jz SH:
00000040 52 D5 62 68 BD 90 B3 A0 56 0E 8D BF 26 E7 F5 57  RÕbh½ ³ V♫ ¿&çõW
00000050 53 45 20 59 23 DD 2F EE E7 C0 06 17 95 FE ED 7F  SE Y#Ý/îçÀ♠↨ þí
00000060 47 79 43 A6 B3 53 3D C7 6F 4C 9B 35 2D B0 F9 9D  GyC¦³S=ÇoL 5-°ù
00000070 75 06 0B 5B F5 82 AE B6 FE FF 54 44 BB BF E2 73  u♠♂[õ ®¶þÿTD»¿âs
00000080 B0 13 E2 56 46 DF 95 D6 7C 19 41 C6 33 37 47 FE  °‼âVFß Ö| AÆ37Gþ
00000090 7E 82 DF B1 89 67 D5 28 A3 CF 59 3D 6D DA 18 8A  ~ ß± gÕ(£ÏY=mÚ↑
000000A0 B7 8E 1B 12 A8 E4 B4 94 EC C7 CD B4 9A 80 8F 36  · ←↕¨ä´ ìÇÍ´   6
000000B0 54 D9 DD 50 B6 8B 97 AD 6D F9 F9 E5 E4 2B 41 AD  TÙÝP¶  -mùùåä+A-
000000C0 10 7B 16 41 E3 E6 8F 97 C0 80 0C 8E 9D 63 16 45  ►{▬Aãæ  À   c▬E
000000D0 52 E7 90 6D 94 A0 5F A4 A0 59 74 6F 77 CD 57 55  Rç m  _¤ YtowÍWU
000000E0 EE 5A 41 84 AC 41 8B F5 79 E2 7A BA 9B C0 34 17  îZA ¬A õyâzº À4↨
000000F0 D3 BA 65 2E 28 D9 19 2A 95 73 DF 46 DB 29 EF 2F  Óºe.(Ù *•sßFÛ)ï/
00000100 DD 28 D7 C4 6E 2B EE 07 1B 5F 22 1F 53 9D B0 EB  Ý(×Än+î•←_" S °ë
00000110 0B 2E 4C 52 20 33 1D F9 35 35 65 54 74 82 97 BE  ♂.LR 3 ù55eTt  ¾
00000120 B8 CB 1C AA 84 75 AF DE 92 3B 9B 45 B9 0E D9 5F  ¸Ë ª u¯Þ ; E¹♫Ù_
00000130 4D 8E 06 0D 1F DB 2D 9F 0E 4C 46 E5 22 BA EA 05  M ♠.  Û- ♫LFå"ºê
00000140 40 94 E6 7D EA 69 84 6B C1 ED 34 4B 6B 62 F6 56  @ æ}êi kÁí4KkböV
00000150 A9 B0 A1 E6 95 D5 A7 A8 8B D5 09 E3 F5 4E 96 16  ©°¡æ Õ§¨ Õ.ãõN ▬
00000160 0F F9 75 75 51 AE 33 7B A3 37 09 3B 87 88 B4 05  ¤ùuuQ®3{£7.; ´
```

Figure 7. REvil configuration structure when stored in the binary. (Source: Secureworks)

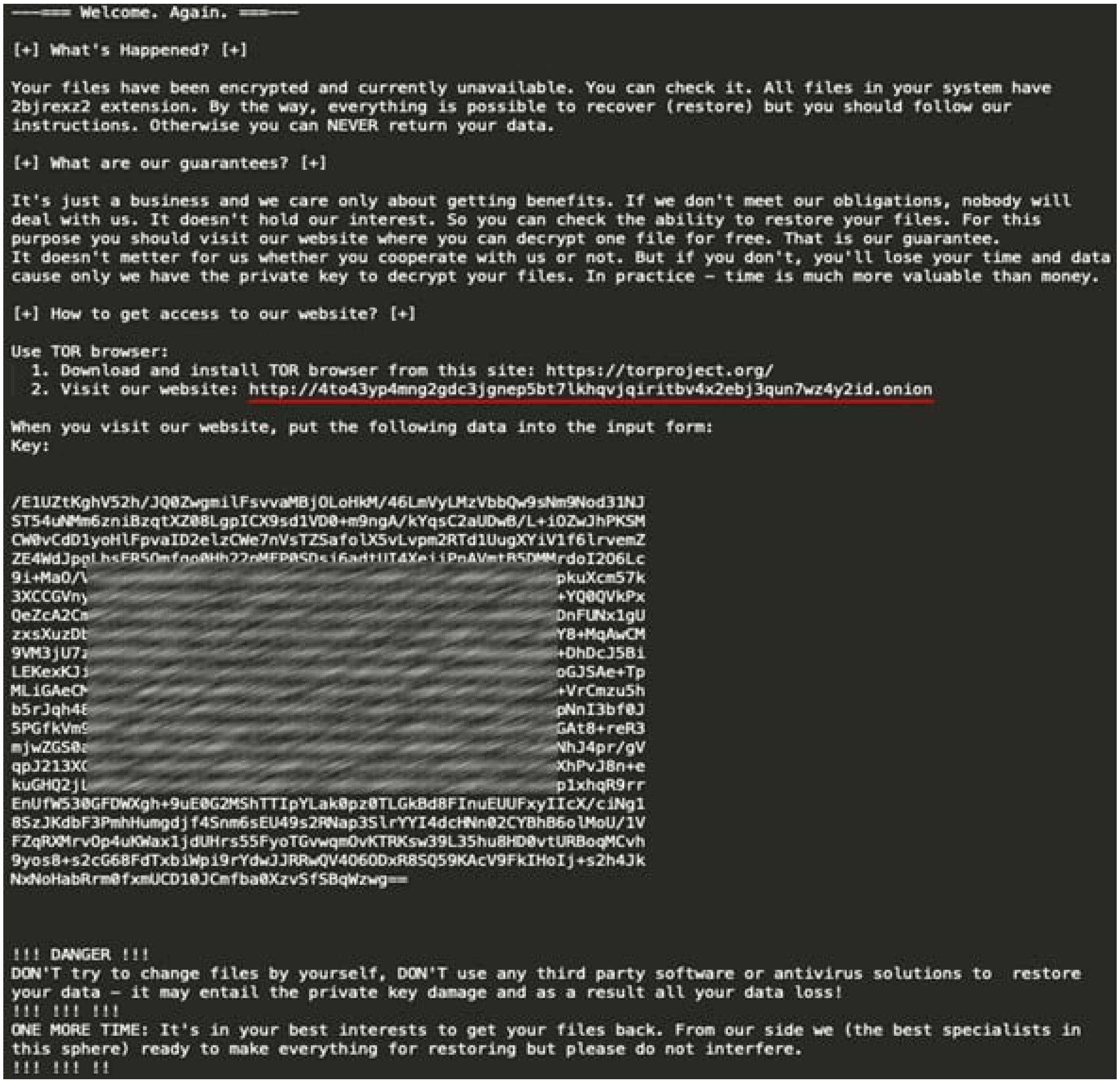
If done correctly, the binary will successfully execute using LV's updated configuration. Files on the victim's system will be encrypted with session keys that are protected by LV's public key, and victims will be directed to LV's ransom payment site via the updated ransom note.

Configuration comparisons

CTU analysis of numerous LV configurations led to several insights:

- The dmn configuration element was consistently assigned an empty string (e.g., "dmn": ""). In a standard REvil configuration, this value contains over 1,200 command and control (C2) domains that the malware uses to communicate infection information to the threat actor. This information can include the ransomware version, session keys used for file encryption, public key used to encrypt the session keys, and victims' details such as username, hostname, and region. Although the net configuration key is set to False in the LV samples, removal of all domains from the dmn configuration key ensures that LV ransomware victims' data is not sent to REvil C2 servers. Removing these domains rather than replacing them with C2 domains operated by GOLD NORTHFIELD suggests that the group may not be capable of maintaining C2 infrastructure or developing the backend automation required to process and track victims' data.
- The partner ID (pid) varied in some of the configurations. This variation suggests that GOLD NORTHFIELD could leverage this element to track individual RaaS partners, which is how GOLD SOUTHFIELD uses this element. However, LV configurations had matching bcrypted partner IDs across different configurations. Although the pid is hashed, a partner could be tracked using the bcrypted hash value. REvil generates a new bcrypted hash for each configuration, making partner tracking impossible.
- The campaign ID (sub) varied in some of the configurations. GOLD NORTHFIELD might have adopted GOLD SOUTHFIELD's approach of using this element to track individual campaigns or configuration builds.
- The attacker's public key (pk) was different in each configuration. GOLD NORTHFIELD needs a master encryption key pair to decrypt files encrypted by LV ransomware. The pk rotation across configurations suggests the creation of a unique key pair for each victim, which prevents file decryption across multiple victims if the attacker's private key is obtained.

- The only ransom note (nbody) change from the standard REvil format was replacing REvil's ransom payment Tor domain with LV's domain (see Figure 8).

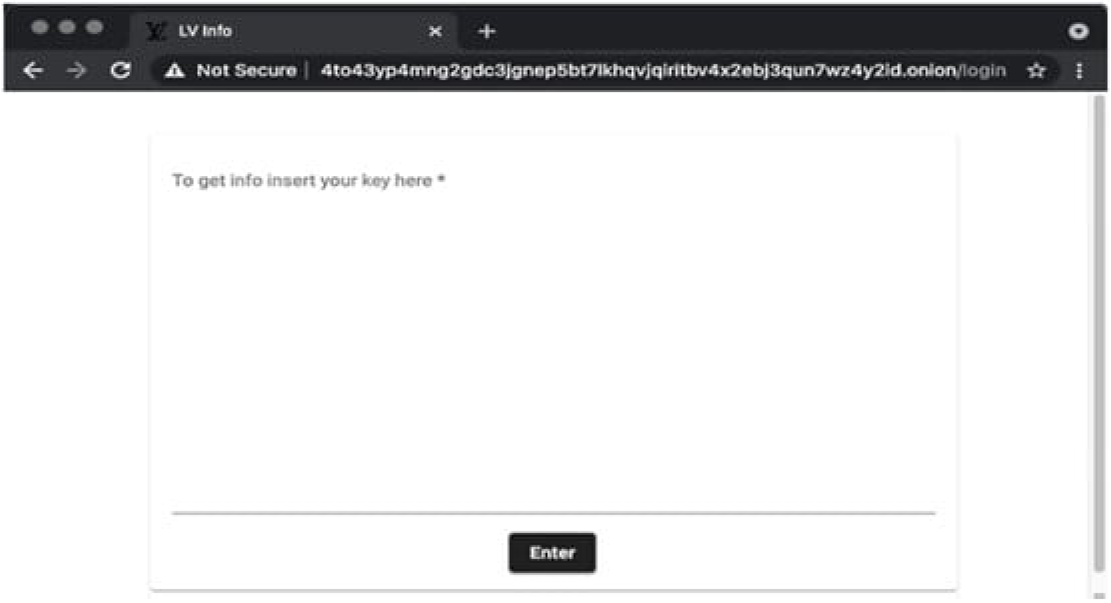


```
---=== Welcome. Again. ===---

[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have
2bjrexz2 extension. By the way, everything is possible to recover (restore) but you should follow our
instructions. Otherwise you can NEVER return your data.

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will
deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this
purpose you should visit our website where you can decrypt one file for free. That is our guarantee.
It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data
cause only we have the private key to decrypt your files. In practice - time is much more valuable than money.

[+] How to get access to our website? [+]

Use TOR browser:
  1. Download and install TOR browser from this site: https://torproject.org/
  2. Visit our website: http://4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion

When you visit our website, put the following data into the input form:
Key:


/E1UZtKghV52h/JQ0ZwgmilFsvvaMBjOLoHkM/46LmVyLMzVbbQw9sNm9Nod31NJ
ST54uNMm6zniBzqtXZ08LgpICX9sd1VD0+m9ngA/kYqsC2aUDwB/L+1OZwJhPKSM
CW0vCdD1yoHlFpvaID2elzCWe7nVsTZSafolX5vLvpm2RTd1UugXYiV1f6lrvemZ
ZE4WdJpgLhsFR5Omfgo0Hh22nMFP0SDsj6adtUT4XejjPnAVmtR5DMMrdoI2O6Lc
9i+MaO/\ [redacted] pkuXcm57k
3XCCGVny                                              +YQ0QVkPx
QeZcA2Cm                                              DnFUNx1gU
zxsXuzDt                                              Y8+MqAwCM
9VM3jU7z                                              +DhDcJ5Bi
LEKexKJi                                              oGJSAe+Tp
MLiGAeCM                                              +VrCmzu5h
b5rJqh4E                                              pNnI3bf0J
5PGfkVm9                                              GAt8+reR3
mjwZGS0z                                              NhJ4pr/gV
qpJ213XC                                              XhPvJ8n+e
kuGHQ2jL                                              p1xhqR9rr
EnUfW530GFDWXgh+9uE0G2MShTTIpYLak0pz0TLGk8d8FInuEUUFxyIIcX/ciNg1
8SzJKdbF3PmhHumgdjf4Snm6sEU49s2RNap3SlrYYI4dcHNn02CYBhB6olMoU/1V
FZqRXMrvOp4uKWax1jdUHrs55FyoTGvwqmOvKTRKsw39L35hu8HD0vtURBoqMCvh
9yos8+s2cG68FdTxbiWpi9rYdwJJRRwQV4O6ODxR8SQ59KAcV9FkIHoIj+s2h4Jk
NxNoHabRrm0fxmUCD10JCmfba0XzvSfSBqWzwg==



!!! DANGER !!!
DON'T try to change files by yourself, DON'T use any third party software or antivirus solutions to  restore
your data - it may entail the private key damage and as a result all your data loss!
!!! !!! !!!
ONE MORE TIME: It's in your best interests to get your files back. From our side we (the best specialists in
this sphere) ready to make everything for restoring but please do not interfere.
!!! !!! !!
```

Figure 8. LV ransom note. (Source: Secureworks)

Ransom payment site

After accessing the ransom payment site, victims are presented with a basic form that requests the key from the ransom note (see Figure 9).



4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion/login

To get info insert your key here *

Figure 9. LV ransom payment site key submission form. (Source: Secureworks)

Previous CTU analysis of the REvil ransom note determined that this key represents information about the ransomware infection that has been encrypted and then Base64-encoded:

- Compromised host details:
  - CPU architecture (32-bit or 64-bit)
  - Fixed-drive information (drive letter, drive type, total size, and free space)
  - Workgroup/domain
  - Configured locale, and whether it aligns with one of the specified countries where the malware cannot be used
  - Hostname
  - Operating system
- Ransomware details:
  - Configured partner ID
  - Threat actor's configured public key
  - Encrypted session private key
  - Configured campaign ID
  - Unique ID based on host's volume serial number and CPUID
  - Victim's username
  - Ransomware version

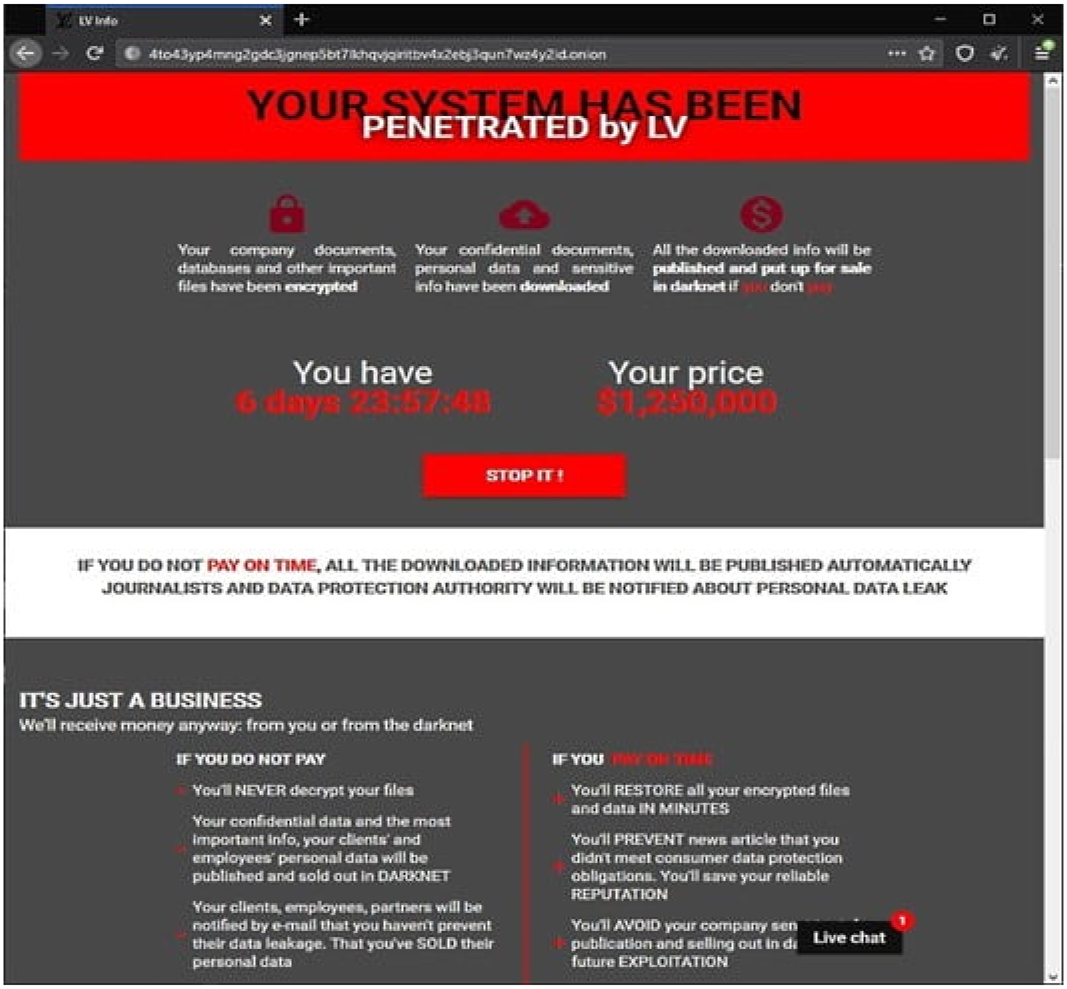
As of this publication, CTU researchers have identified three ransom payment Tor domains specified in LV ransom notes. Each of the domains successfully loads the landing page, but CTU researchers' attempts to submit the key from the ransom note returned HTTP errors (see Table 1).

Ransom payment domain	HTTP error
4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id . onion	502 - Bad Gateway
l55ysq5qjpin2vq23ul3gc3h62vp4wvenl7ov6fcn65vir7kc7gb5fyd . onion	403 - Forbidden
36yvrbzhbzyuzia7qxahsaw2yizcr3heljw2jtde3smyuhkokjnb2sid . onion	403 - Forbidden

Table 1. LV ransom payment domains and HTTP errors.

The HTTP errors may be caused by anti-analysis controls implemented by GOLD NORTHFIELD to inspect characteristics of the submitted key for suspicious or undesirable activity. They may also indicate that the threat group is struggling to maintain resilient infrastructure due to lack of skill or insufficient resources.

When key submission is successful, the site displays a page showing the ransom amount in U.S. dollars and how much time the victim has to pay the ransom before sensitive data is disclosed (see Figure 10). The page also includes a live chat function for the victim to interact with the threat actors.


LV Info
4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion
STOP IT !
Live chat
1

YOUR SYSTEM HAS BEEN PENETRATED by LV

Your company documents, databases and other important files have been **encrypted**

Your confidential documents, personal data and sensitive info have been **downloaded**

All the downloaded info will be **published and put up for sale in darknet** if you don't pay

You have
6 days 23:57:48

Your price
$1,250,000

IF YOU DO NOT PAY ON TIME, ALL THE DOWNLOADED INFORMATION WILL BE PUBLISHED AUTOMATICALLY
JOURNALISTS AND DATA PROTECTION AUTHORITY WILL BE NOTIFIED ABOUT PERSONAL DATA LEAK

IT'S JUST A BUSINESS
We'll receive money anyway: from you or from the darknet

IF YOU DO NOT PAY

- You'll NEVER decrypt your files
- Your confidential data and the most important info, your clients' and employees' personal data will be published and sold out in DARKNET
- Your clients, employees, partners will be notified by e-mail that you haven't prevent their data leakage. That you've SOLD their personal data

IF YOU PAY ON TIME

- You'll RESTORE all your encrypted files and data IN MINUTES
- You'll PREVENT news article that you didn't meet consumer data protection obligations. You'll save your reliable REPUTATION
- You'll AVOID your company sen[illegible] publication and selling out in da[illegible] future EXPLOITATION

Figure 10. LV ransom payment site. (Source: ID Ransomware blog)

Leak sites

CTU researchers identified two LV ransomware leak sites that have an identical structure but appear to be operated independently. The sites listed victims during the same timeframe, but only one victim was listed on both sites (see Figure 11). It is unclear why GOLD NORTHFIELD would operate two leak sites.

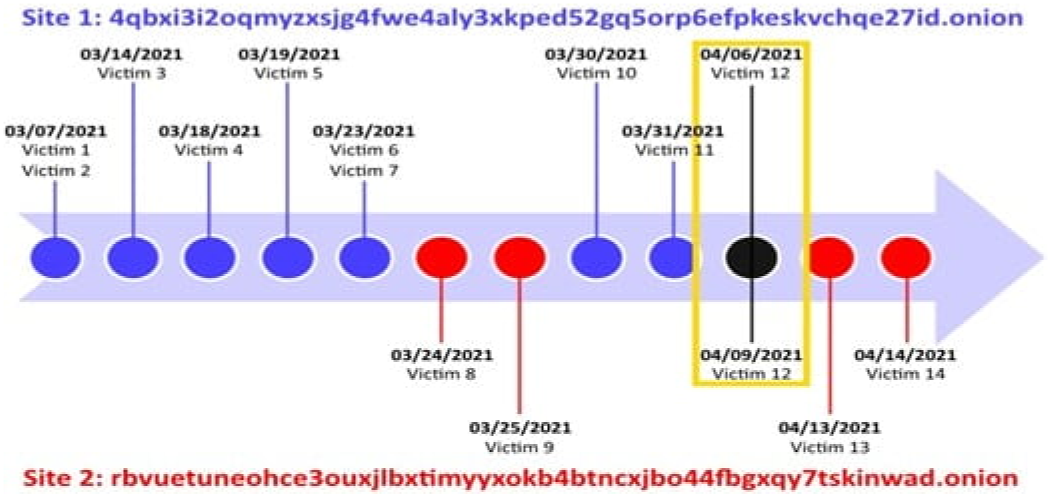
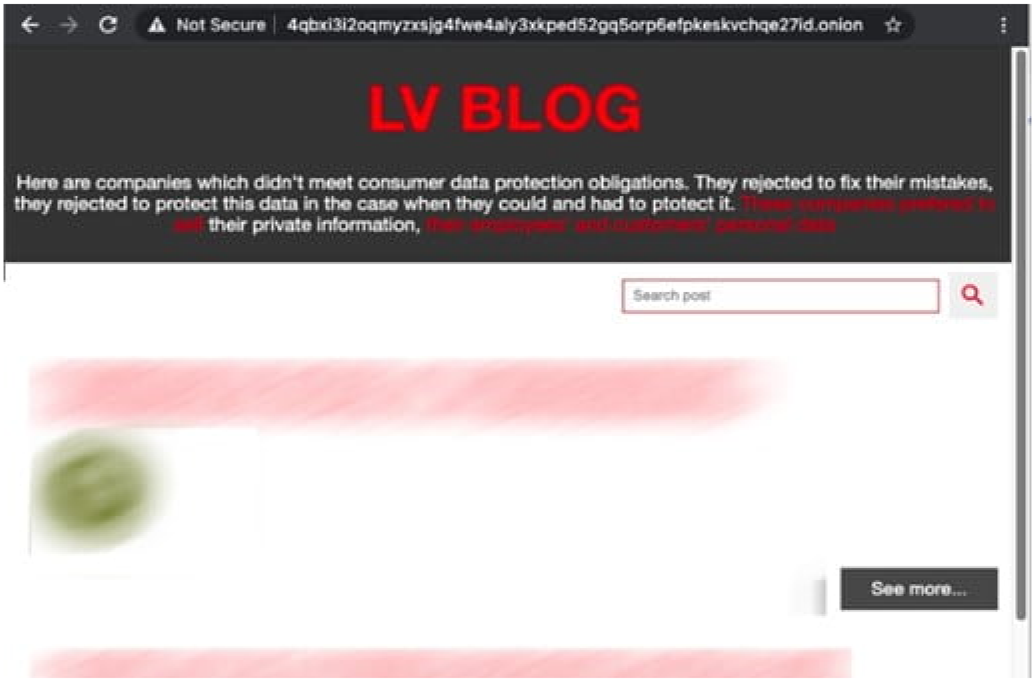


Figure 11. Victims added to LV leak sites between March 7 and April 14, 2021. Only one victim (highlighted in yellow) was listed on both sites. (Source: Secureworks)

The leak sites name and shame victims. The threat actors coerce the victims into paying the ransom by threatening to publish their sensitive information (see Figure 12).


Not Secure | 4qbxi3i2oqmyzxsjg4fwe4aly3xkped52gq5orp6efpkeskvchqe27id.onion
Search post
See more...

LV BLOG

Here are companies which didn't meet consumer data protection obligations. They rejected to fix their mistakes, they rejected to protect this data in the case when they could and had to ptotect it. These companies preferred to sell their private information, their employees' and customers' personal data

Figure 12. LV leak site. (Source: Secureworks)

GOLD NORTHFIELD typically threatens to publicly release sensitive information if victims do not initiate contact within 72 hours. The threat actors post screenshots of the victim's sensitive files on the leak sites to support their claims. However, it appears that none of the victims' data has been released as of this publication. It is unclear if victims paid the ransom and the threat actors just keep the full list of victims on the leak site as evidence of their conquests.

Conclusion

CTU analysis revealed that the LV ransomware is not a distinct ransomware family; it is repurposed REvil ransomware. By modifying the binary of a prolific ransomware family, the GOLD NORTHFIELD threat actors significantly expedited their maturity within the ransomware ecosystem. Without expending resources on ransomware development, the group can operate more efficiently than its competitors while still offering a best-in-class ransomware offering, ultimately resulting in a more profitable business model. GOLD NORTHFIELD's unauthorized manipulation of REvil will likely prompt GOLD SOUTHFIELD to implement additional anti-tamper controls and modify configuration storage and processing to impede future attempts to overwrite the REvil configuration.

It is too early in GOLD NORTHFIELD's evolution to evaluate the threat it poses. The ability to repurpose the REvil binary suggests that the threat actors have technical capabilities. Additionally, the complexity required for this repurposing and the configuration variations across LV samples suggest that GOLD NORTHFIELD may have automated the process. Although a RaaS for the LV ransomware could provide direct competition for GOLD SOUTHFIELD's RaaS offering, the lack of a reliable and organized infrastructure needed to operate a successful RaaS offering suggests that GOLD NORTHFIELD has to expand its capabilities and resources to compete with other ransomware operations.

Threat indicators

The threat indicators in Table 2 can be used to detect activity related to LV ransomware. The domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
6f0b92488eae3ccefc0db7a6b0d652ee	MD5 hash	Packed LV ransomware
45adc4224d2ae9fd75b19417ca6913515c5222ee	SHA1 hash	Packed LV ransomware
457936c28938616495836c472b3389a0870574bee6a5dc026d5bd14979c6202c	SHA256 hash	Packed LV ransomware
58682ca2a49ed4bfb8d5aaf76cf0fade	MD5 hash	Packed LV ransomware
b00d58e9ffd784db86e77a6a31c76e1bd58ba79b	SHA1 hash	Packed LV ransomware
ab2f84103e95806b25c6d163d6210a21fb3283cd29dddee917d33e654d733425	SHA256 hash	Packed LV ransomware
7b1cf5fc0bfb1021fe0e14e518c32026	MD5 hash	Packed LV ransomware

Indicator	Type	Context
380cd990a9e5aec85233ef1d2635dc04d5a96e6b	SHA1 hash	Packed LV ransomware
d4fc76bf8baae39feec23990857c52199e80265a34faeece0d830eb77645c944	SHA256 hash	Packed LV ransomware
a4331ff805b0a8f2a2892777c224b65e	MD5 hash	Packed LV ransomware
2c5521077dd1a6f5f3558351370880aee9ab7c71	SHA1 hash	Packed LV ransomware
329983dc2a23bd951b24780947cb9a6ae3fb80d5ef546e8538dfd9459b176483	SHA256 hash	Packed LV ransomware
fa8117afd2dbd20513522f2f8e991262	MD5 hash	Packed LV ransomware
f7b876edb8fc0c83fd8b665d3c5a1050d4396302	SHA1 hash	Packed LV ransomware
78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff	SHA256 hash	Packed LV ransomware
d1c9c12e08c8e2111da989e2318b1c42	MD5 hash	Unpacked LV ransomware
d0c7f3c8de28d0fccec9d4925afeb5fa9dd62b5d	SHA1 hash	Unpacked LV ransomware
e25eaaac03aa958688cbe950275156169eb4955e145bc9627fcbfb36cd832a84	SHA256 hash	Unpacked LV ransomware
4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion	Domain name	LV ransomware payment site
l55ysq5qjpin2vq23ul3gc3h62vp4wvenl7ov6fcn65vir7kc7gb5fyd.onion	Domain name	LV ransomware payment site
36yvrbzhbzyuzia7qxahsaw2yizcr3heljw2jtde3smyuhkokjnb2sid.onion	Domain name	LV ransomware payment site
rbvuetuneohce3ouxjlbxtimyyxokb4btncxjbo44fbgxqy7tskinwad.onion	Domain name	LV ransomware leak site
4qbxi3i2oqmyzxsjg4fwe4aly3xkped52gq5orp6efpkeskvchqe27id.onion	Domain name	LV ransomware leak site

Table 2. Indicators for this threat.

References

Gillespie, Michael (@demonslay335). "Sodinokibi." Twitter, November 13, 2020, 5:24 pm. https://twitter.com/demonslay335/status/1327376936935493635

Ivanov, Andrew. "LV Ransomware." ID Ransomware blog. November 13, 2020. Original (in Russian): https://id-ransomware.blogspot.com/2020/10/lv-ransomware.html. English translation: https://translate.google.com/translate?hl=en&sl=ru&u=https://id-ransomware.blogspot.com/2020/10/lv-ransomware.html&prev=search&pto=aue

Secureworks. "GOLD NORTHFIELD." Accessed June 1, 2021. https://www.secureworks.com/research/threat-profiles/gold-northfield

Secureworks. "GOLD SOUTHFIELD." Accessed April 22, 2021. https://www.secureworks.com/research/threat-profiles/gold-southfield

Secureworks. "REvil/Sodinokibi Ransomware." September 24, 2019. https://www.secureworks.com/research/revil-sodinokibi-ransomware

xiaopao (@Kangxiaopao). "LV ransomware." Twitter, October 23, 2020, 5:43 am. https://twitter.com/Kangxiaopao/status/1319575086995652609