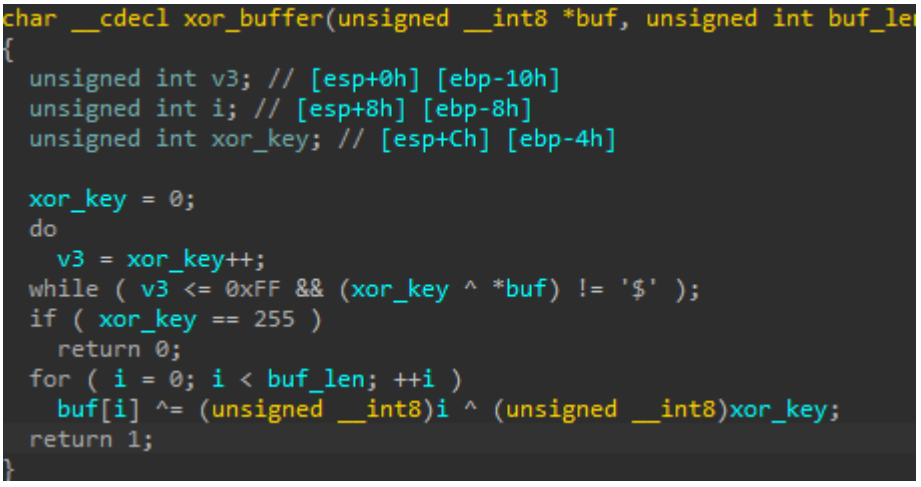
Lloyd Davies on X: "The Kaseya sideloaded DLL, a thread: * If launched as a service, sleeps for 1000ms indefinitely * If ServiceCrtMain is called, main malicious logic is unwrapped * Initial payload is unpacked, XOR'd using a calculated key and execution continues 1/? https://t.co/5M478lygaW" / X

Published: 2021-07-02 · Archived: 2026-04-05 15:41:27 UTC

Post

Conversation

The Kaseya sideloaded DLL, a thread: * If launched as a service, sleeps for 1000ms indefinitely * If ServiceCrtMain is called, main malicious logic is unwrapped * Initial payload is unpacked, XOR'd using a calculated key and execution continues 1/?



```
char __cdecl xor_buffer(unsigned __int8 *buf, unsigned int buf_le
{
  unsigned int v3; // [esp+0h] [ebp-10h]
  unsigned int i; // [esp+8h] [ebp-8h]
  unsigned int xor_key; // [esp+Ch] [ebp-4h]

  xor_key = 0;
  do
    v3 = xor_key++;
  while ( v3 <= 0xFF && (xor_key ^ *buf) != '$' );
  if ( xor_key == 255 )
    return 0;
  for ( i = 0; i < buf_len; ++i )
    buf[i] ^= (unsigned __int8)i ^ (unsigned __int8)xor_key;
  return 1;
}
```

New to X?

Trending now

What’s happening
