RansomExx ransomware also encrypts Linux systems

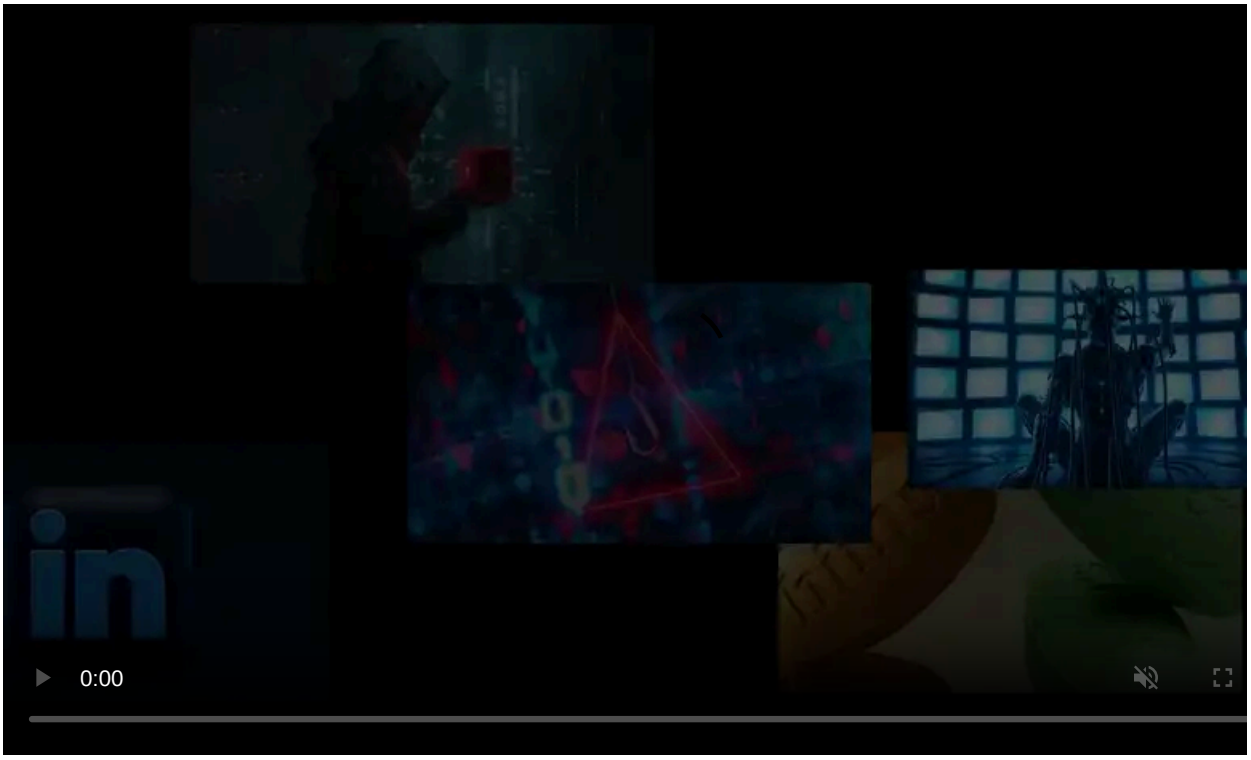
By Lawrence Abrams

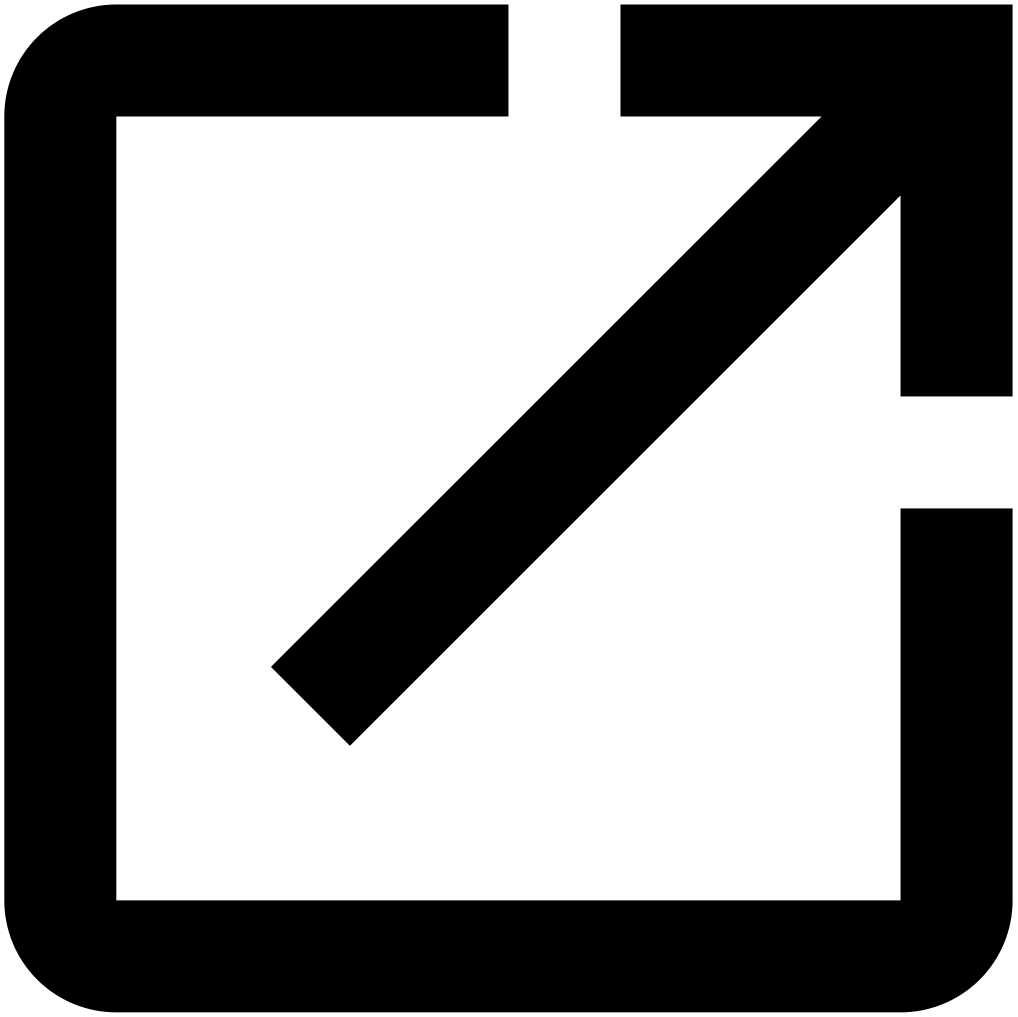
Published: 2020-11-06 · Archived: 2026-04-05 17:33:32 UTC

With companies commonly using a mixed environment of Windows and Linux servers, ransomware operations have increasingly started to create Linux versions of their malware to ensure they encrypt all critical data.

A new report today by Kaspersky takes a look at the Linux version of the RansomExx ransomware, also known as Defray777.

RansomExx has been getting a lot of attention this week due to their ongoing attacks against Brazil's government networks and previous attacks against the Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and Tyler Technologies.


0:00



Linux version of RansomExx

According to Kaspersky, when targeting Linux servers, the RansomExx operators will deploy an ELF executable named 'svc-new' used to encrypt a victim's server.

"After the initial analysis we noticed similarities in the code of the Trojan, the text of the ransom notes and the general approach to extortion, which suggested that we had in fact encountered a Linux build of the previously known ransomware family RansomEXX," Kaspersky researchers stated in their report.

Embedded in the Linux executable are a public RSA-4096 encryption key, the ransom note, and an extension named after the customer that will be appended to all encrypted files.

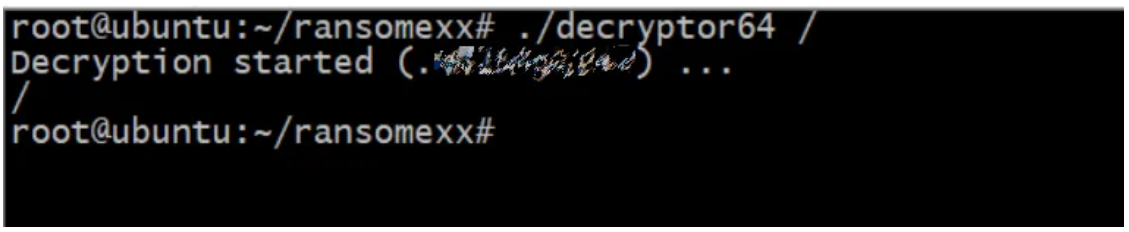
```
if ( a1 )
{
  v10 = strlen(s) + 277;
  v2 = alloca(16 * ((v10 + 23LL) / 0x10uLL));
  dest = (16 * ((&s + 7) >> 4));
  if ( dest )
  {
    strcpy(dest, s);
    strcat(dest, ".[redacted]");
    v3 = rand();
    sprintf(src, "-%08x", v3);
    strcat(dest, src);
    if ( fsize(dest) == -1 )
    {
      stream = fopen64(s, "r+");
      if ( stream )
      {
        v9 = fsize(s);
        if ( v9 )
        {
          if ( v9 > 15 )
          {
            mbedtls_aes_init(aes_ctx);
            pthread_mutex_lock(&csPreData);
            qmemcpy(ptr, &g_RansomHeader, 0x200uLL);
            mbedtls_aes_setkey_enc(aes_ctx, &g_KeyAES, 256LL);
            pthread_mutex_unlock(&csPreData);
            if ( !fseek(stream, 0LL, SEEK_END)
              && fwrite(ptr, 1uLL, 0x200uLL, stream)
              && !fseek(stream, -512 - v9, 1)
              && ProcessFileHandleWithLogic(stream, aes_ctx, a2, v9, CryptOneBlock) )
            {
              v13 = 1;
            }
```

Code to encrypt files in Linux version

Unlike the Windows version, Kaspersky states that the Linux version is a no-frills ransomware. It does not contain any code to terminate processes, including security software, does not wipe free space like the Windows version does, and does not communicate with a command and control server.

If a victim pays the ransom, they will receive both a Linux and Windows decryptor with the corresponding RSA-4096 private key and encrypted file extension embedded in the executable.

The Linux version is named 'decryptor64' and is a command-line driven decryptor, as shown below.



Fabian Wosar, the CTO of cybersecurity firm Emsisoft, told BleepingComputer that he first saw RansomExx utilizing a Linux version in attacks in July 2020, but may have been used earlier.

RansomExx is not the first ransomware to create Linux versions. In the past, Pysa (Menispoza), Snatch, and PureLocker have also distributed Linux variants.

Source: https://www.bleepingcomputer.com/news/security/ransomexx-ransomware-also-encrypts-linux-systems/