

# XORStringsNet

---

 [research.openanalysis.net/dotnet/xorstringsnet/agenttesla/2023/04/16/xorstringsnet.html](https://research.openanalysis.net/dotnet/xorstringsnet/agenttesla/2023/04/16/xorstringsnet.html)

OALABS Research

April 16, 2023

## Overview

---

Dr4k0nia published an open source .NET string encryption tool on her github XorStringsNET. This has been picked up and abused by malware developers to encrypt strings in their malware, including families like Redline and AgentTesla.

In response Dr4k0nia released a decryption method and a Yara rule.

| <https://twitter.com/dr4k0nia/status/1640049711431204872?s=20>

## References

---

- [XorStringsNET](#)
- [Encrypting strings in .NET](#)
- [Unpacking XorStringsNET](#)
- [Yara: msil\\_susp\\_obf\\_xorstringsnet](#)

## Samples

---

d56f2852762f7f9fcb07eaf018e143ab1e4ad46e1f2e943faf13618388ef21a2

## Analysis

---

There is a bug with the encryption which results in only one byte of the key being used to encrypt the strings. This means we can brute force the strings... or we could take a more measured approach.

### Step 1

---

First, locate the strings table in memory using the decryption routine, then locating the nested private struct and a field referencing that struct. In the example below the RVA: 0x0001BB7B for the field is the start of the strings table.

```
// Fields
// Token: 0x04000187 RID: 391 RVA: 0x0001BB7B File Offset: 0x00019D7B
.field private static valuetype A.u/A bL at I_0001bb7b // 19516 (0x4c3c) bytes
```

### Step 2

---

The strings table starts with a 4-byte global key that is used to decrypt the decryption function argument (the pointer to the encrypted string data). Following this key is a serialized stream of the encrypted strings using the following format.

```
4 bytes - length little endian
4 bytes - key (only 1st byte is used)
data

import struct

def xor_crypt(data, key_byte):
    out = []
    for c in data:
        out.append(c ^ key_byte)
    return bytes(out)

file_data = open('/tmp/nettest.bin', 'rb').read()

offset = 0x00019D7B
# skip the global enc key
offset += 4

ptr = offset

strings = []

while True:
    size = struct.unpack('<I', file_data[ptr:ptr+4])[0]
    if size == 0:
        break
    if size > 0x100:
        break
    ptr += 4
    key = file_data[ptr:ptr+1]
    ptr += 4
    data = file_data[ptr:ptr+size]
    ptr += size
    out = xor_crypt(data[::-1], ord(key))
    if not out.isascii():
        break
    strings.append(out)
```

```
from dnfile import dnPE
from dnfile.mdtable import MethodDefRow

import dnfile
from dnfile.enums import MetadataTables

from dncil.cil.body import CilMethodBody
from dncil.cil.error import MethodBodyFormatError
from dncil.clr.token import Token, StringToken, InvalidToken
from dncil.cil.body.reader import CilMethodBodyReaderBase

# key token indexes to dotnet meta tables
DOTNET_META_TABLES_BY_INDEX = {table.value: table.name for table in MetadataTables}
```

```

class_size_list = []

for row in pe.net.mdtables.ClassLayout.rows:
    type_row = pe.net.mdtables.TypeDef.rows[row.Parent.row_index - 1]
    if type_row.Flags.tdExplicitLayout:
        class_size_list.append(row.ClassSize)

# Assume the encryption table is the largest class
target_class_size = max(class_size_list)

target_rva = None

# Find the table based on the physical size
for i in range(0, len(pe.net.mdtables.FieldRva.rows) - 1, 2):
    curr_row = pe.net.mdtables.FieldRva.rows[i]
    next_row = pe.net.mdtables.FieldRva.rows[i + 1]
    if next_row.Rva - curr_row.Rva == target_class_size:
        target_rva = curr_row.Rva
        break

if target_rva is None:
    # It must be the last one
    target_rva = pe.net.mdtables.FieldRva.rows[-1].Rva

data = pe.get_data(target_rva, target_class_size)

def decrypt_table(data):
    strings = []
    ptr = 0
    # Jump past global key
    ptr += 4
    while ptr < len(data):
        size = struct.unpack('<I', data[ptr:ptr+4])[0]
        if size == 0:
            break
        if size > 0x100:
            break
        ptr += 4
        key = data[ptr:ptr+1]
        ptr += 4
        str_data = data[ptr:ptr+size]
        ptr += size
        out = xor_crypt(str_data[::-1], ord(key))
        if not out.isascii():
            break
        strings.append(out)
    return strings

decrypt_table(data)

```

```
[b'SC',
 b'/log.tmp',
 b'KL',
 b'KL',
 b'<br>[',
 b'yyyy-MM-dd HH:mm:ss',
 b']<br>',
 b'<br>',
 b'PW',
 b'Time: ',
 b'MM/dd/yyyy HH:mm:ss',
 b'<br>User Name: ',
 b'<br>Computer Name: ',
 b'<br>OSFullName: ',
 b'<br>CPU: ',
 b'<br>RAM: ',
 b'<br>',
 b'IP Address: ',
 b'<br>',
 b'<hr>',
 b'New ',
 b' Recovered!\n\nTime: ',
 b'MM/dd/yyyy HH:mm:ss',
 b'\nUser Name: ',
 b '/',
 b'\nOSFullName: ',
 b'\nCPU: ',
 b'\nRAM: ',
 b'\n',
 b'IP Address: ',
 b'\n',
 b'_',
 b '/',
 b '/',
 b'false',
 b'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0',
 b'false',
 b'false',
 b'false',
 b'false',
 b'false',
 b'false',
 b'false',
 b'20',
 b'20',
 b'1',
 b'false',
 b'587',
 b'false',
 b'mail.expertsconsultgh.co',
 b'oppong@expertsconsultgh.co',
 b'Oppong.2012',
 b'wisdombig57@gmail.com',
```

b'false',  
b'false',  
b'appdata',  
b'xFzxn',  
b'xFzxn.exe',  
b'xFzxn',  
b'Type',  
b': ',  
b': ',  
b'<br>',  
b'<hr>',  
b'<br>',  
b'<b>[ ',  
b']</b> ( ',  
b')<br>',  
b'{BACK}',  
b'{ALT+TAB}',  
b'{ALT+F4}',  
b'{TAB}',  
b'{ESC}',  
b'{Win}',  
b'{CAPSLOCK}',  
b'{KEYUP}',  
b'{KEYDOWN}',  
b'{KEYLEFT}',  
b'{KEYRIGHT}',  
b'{DEL}',  
b'{END}',  
b'{HOME}',  
b'{Insert}',  
b'{NumLock}',  
b'{PageDown}',  
b'{PageUp}',  
b'{ENTER}',  
b'{F1}',  
b'{F2}',  
b'{F3}',  
b'{F4}',  
b'{F5}',  
b'{F6}',  
b'{F7}',  
b'{F8}',  
b'{F9}',  
b'{F10}',  
b'{F11}',  
b'{F12}',  
b' ',  
b'control',  
b'{CTRL}',  
b'&',  
b'&#x26;',  
b'<',

b'&lt;',  
b'>',  
b'&gt;',  
b'''',  
b'&quot;',  
b'<br><hr>Copied Text: <br>',  
b'<hr>',  
b'logins',  
b'IE/Edge',  
b'2F1A6504-0641-44CF-8BB5-3612D865F2E5',  
b'Windows Secure Note',  
b'3CCD5499-87A8-4B10-A215-608888DD3B55',  
b'Windows Web Password Credential',  
b'154E23D0-C644-4E6F-8CE6-5069272F999F',  
b'Windows Credential Picker Protector',  
b'4BF4C442-9B8A-41A0-B380-DD4A704DDB28',  
b'Web Credentials',  
b'77BC582B-F0A6-4E15-4E80-61736B6F3B29',  
b'Windows Credentials',  
b'E69D7838-91B5-4FC9-89D5-230D4D4CC2BC',  
b'Windows Domain Certificate Credential',  
b'3E0E35BE-1B77-43E7-B873-AED901B6275B',  
b'Windows Domain Password Credential',  
b'3C886FF3-2669-4AA2-A8FB-3F6759A77548',  
b'Windows Extended Credential',  
b'00000000-0000-0000-0000-000000000000',  
b'SchemaId',  
b'pResourceElement',  
b'pIdentityElement',  
b'pPackageSid',  
b'pAuthenticatorElement',  
b'IE/Edge',  
b'UC Browser',  
b'UCBrowser\\',  
b'\*',  
b'Login Data',  
b'journal',  
b'wow\_logins',  
b'Safari for Windows',  
b'\\Common Files\\Apple\\Apple Application Support\\plutil.exe',  
b'\\Apple Computer\\Preferences\\keychain.plist',  
b'<array>',  
b'<dict>',  
b'<string>',  
b'</string>',  
b'<string>',  
b'</string>',  
b'<data>',  
b'</data>',  
b' -convert xml1 -s -o ''',  
b'\\fixed\_keychain.xml" ',  
b'''',

b''',  
b'\\Microsoft\\Credentials\\',  
b'\\Microsoft\\Credentials\\',  
b'\\Microsoft\\Credentials\\',  
b'\\Microsoft\\Credentials\\',  
b'\\Microsoft\\Protect\\',  
b'\\',  
b'credential',  
b'QQ Browser',  
b'Tencent\\QQBrowser\\User Data',  
b'\\Default\\EncryptedStorage',  
b'Profile',  
b'\\EncryptedStorage',  
b'entries',  
b'category',  
b'Password',  
b'str3',  
b'str2',  
b'blob0',  
b'password\_value',  
b'IncrediMail',  
b'PopPassword',  
b'SmtpPassword',  
b'Software\\IncrediMail\\Identities\\',  
b'\\Accounts\_New',  
b'PopPassword',  
b'SmtpPassword',  
b'SmtpServer',  
b'EmailAddress',  
b'Eudora',  
b'Software\\Qualcomm\\Eudora\\CommandLine\\',  
b'current',  
b'Settings',  
b'SavePasswordText',  
b'Settings',  
b'ReturnAddress',  
b'-',  
b'Falkon Browser',  
b'\\falkon\\profiles\\',  
b'profiles.ini',  
b'startProfile=([A-z0-9\\\/\\.\\"'+)'  
b'profiles.ini',  
b'\\browsedata.db',  
b'autofill',  
b'ClawsMail',  
b'\\Claws-mail',  
b'\\clawsrc',  
b'\\clawsrc',  
b'passkey0',  
b'master\_passphrase\_salt=(.+)',  
b'master\_passphrase\_pbkdf2\_rounds=(.+)',  
b'\\accountrc',



```
b'smtp_server',
b'address',
b'account',
b'[',
b' ',
b']',
b'\\passwordstorerc',
b'{(.*) (.*)}(.*)',
b'Flock Browser',
b'APPDATA',
b'\\Flock\\Browser\\',
b'signons3.txt',
b'---',
b'.',
b'---',
b'DynDns',
b'ALLUSERSPROFILE',
b'Dyn\\Updater\\config.dyndns',
b'username=',
b'password=',
b'https://account.dyn.com/',
b't6KzXhCh',
b'ALLUSERSPROFILE',
b'Dyn\\Updater\\daemon.cfg',
b'global',
b'accounts',
b'account.',
b'username',
b'account.',
b'password',
b'Psi/Psi+',
b'name',
b'jid',
b'password',
b'jid',
b'Psi/Psi+',
b'APPDATA',
b'\\Psi\\profiles',
b'APPDATA',
b'\\Psi+\\profiles',
b'\\accounts.xml',
b'\\accounts.xml',
b'OpenVPN',
b'Software\\OpenVPN-GUI\\configs',
b'Software\\OpenVPN-GUI\\configs',
b'Software\\OpenVPN-GUI\\configs\\',
b'username',
b'auth-data',
b'entropy',
b'USERPROFILE',
b'\\OpenVPN\\config\\',
b'remote ',
```

```
b'remote ',
b'NordVPN',
b'NordVPN',
b'NordVpn.exe*',
b'user.config',
b'//setting[@name='Username']/value",
b'//setting[@name='Password']/value",
b'NordVPN',
b'- ',
b'Private Internet Access',
b'%ProgramW6432%',
b'Private Internet Access\\data',
b'ProgramFiles(x86)',
b'\\Private Internet Access\\data',
b'\\account.json',
b'.*"username": "(.*?)"',
b'.*"password": "(.*?)"',
b'Private Internet Access',
b'privateinternetaccess.com',
b'FileZilla',
b'APPDATA',
b'\\FileZilla\\recentervers.xml',
b'APPDATA',
b'\\FileZilla\\recentervers.xml',
b'<Server>',
b'<Host>',
b'<Host>',
b'</Host>',
b': ',
b'<Port>',
b'</Port>',
b'<User>',
b'<User>',
b'</User>',
b'<Pass encoding="base64">',
b'<Pass encoding="base64">',
b'</Pass>',
b'<Pass>',
b'<Pass encoding="base64">',
b'</Pass>',
b'CoreFTP',
b'SOFTWARE\\FTPWare\\COREFTP\\Sites',
b'\\',
b'PW',
b'User',
b'Host',
b'Port',
b'hdfzpvsvpzimorhk',
b'WinSCP',
b'SOFTWARE\\Martin Prikryl\\WinSCP 2\\Sessions',
b'HostName',
b'UserName',
```

b'Password',  
b'PublicKeyFile',  
b':',  
b'PortNumber',  
b'22',  
b'[PRIVATE KEY LOCATION: "{0}"]',  
b'WinSCP',  
b'A',  
b'10',  
b'B',  
b'11',  
b'C',  
b'12',  
b'D',  
b'13',  
b'E',  
b'14',  
b'F',  
b'15',  
b'ABCDEF',  
b'Flash FXP',  
b'IP',  
b':',  
b'port',  
b'user',  
b'pass',  
b'quick.dat',  
b'Sites.dat',  
b'\\FlashFXP\\',  
b'\\FlashFXP\\',  
b'\\',  
b'\\',  
b'\\',  
b'\\',  
b'\\',  
b'yA36zA48dEhfrvghGRg57h5U1Dv3',  
b'FTP Navigator',  
b'SystemDrive',  
b'\\FTP Navigator\\Ftplist.txt',  
b'Server',  
b'Password',  
b'No Password',  
b'User',  
b'SmartFTP',  
b'APPDATA',  
b'SmartFTP\\Client 2.0\\Favorites\\Quick Connect',  
b'WS\_FTP',  
b'appdata',  
b'Ipswitch\\WS\_FTP\\Sites\\ws\_ftp.ini',  
b'HOST',  
b'UID',  
b'PWD',

b'PWD=',  
b'PWD=',  
b'FtpCommander',  
b'SystemDrive',  
b'\\Program Files (x86)\\FTP Commander Deluxe\\Ftplist.txt',  
b'SystemDrive',  
b'\\Program Files (x86)\\FTP Commander\\Ftplist.txt',  
b'SystemDrive',  
b'\\cftp\\Ftplist.txt',  
b'\\VirtualStore\\Program Files (x86)\\FTP Commander\\Ftplist.txt',  
b'\\VirtualStore\\Program Files (x86)\\FTP Commander Deluxe\\Ftplist.txt',  
b';Password=',  
b';User=',  
b';Server=',  
b';Port=',  
b';Port=',  
b';Password=',  
b';User=',  
b';Anonymous=',  
b':',  
b'FTPGetter',  
b'\\FTPGetter\\servers.xml',  
b'<server>',  
b'<server\_ip>',  
b'<server\_ip>',  
b'</server\_ip>',  
b':',  
b'<server\_port>',  
b'</server\_port>',  
b'<server\_user\_name>',  
b'<server\_user\_name>',  
b'</server\_user\_name>',  
b'<server\_user\_password>',  
b'<server\_user\_password>',  
b'</server\_user\_password>',  
b'FTPGetter',  
b'The Bat!',  
b'appdata',  
b'\\The Bat!',  
b'\\Account.CFN',  
b'\\Account.CFN',  
b'zzz',  
b'-----=',  
b'+-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz',  
b'Becky!',  
b'HKEY\_CURRENT\_USER\\Software\\RimArts\\B2\\Settings',  
b'DataDir',  
b'Folder.lst',  
b'\\Mailbox.ini',  
b'Account',  
b'Passwd',  
b'Account',

b'SMTPServer',  
b'Account',  
b'MailAddress',  
b'Becky!',  
b'Outlook',

b'Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676',

b'Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging  
Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676',  
b'Software\\Microsoft\\Windows Messaging  
Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676',

b'Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676',

b'Email',  
b'IMAP Password',  
b'POP3 Password',  
b'HTTP Password',  
b'SMTP Password',  
b'Email',  
b'Email',  
b'Email',  
b'IMAP Password',  
b'POP3 Password',  
b'HTTP Password',  
b'SMTP Password',  
b' Server',  
b'Windows Mail App',  
b'COMPlus\_legacyCorruptedStateExceptionsPolicy',  
b'1',  
b'Software\\Microsoft\\ActiveSync\\Partners',  
b'Email',  
b'Server',  
b'SchemaId',  
b'pResourceElement',  
b'pIdentityElement',  
b'pPackageSid',  
b'pAuthenticatorElement',  
b'syncpassword',  
b'mailoutgoing',  
b'FoxMail',  
b'HKEY\_CURRENT\_USER\\Software\\Aerofox\\FoxmailPreview',  
b'Executable',  
b'HKEY\_CURRENT\_USER\\Software\\Aerofox\\Foxmail\\V3.1',  
b'FoxmailPath',  
b'\\Storage\\',  
b'\\Storage\\',  
b'\\mail',  
b'\\mail',  
b'\\VirtualStore\\Program Files\\Foxmail\\mail',  
b'\\VirtualStore\\Program Files\\Foxmail\\mail',

```
b'\\VirtualStore\\Program Files (x86)\\Foxmail\\mail',
b'\\VirtualStore\\Program Files (x86)\\Foxmail\\mail',
b'\\Accounts\\Account.rec0',
b'\\Accounts\\Account.rec0',
b'\\Account.stg',
b'\\Account.stg',
b'POP3Host',
b'SMTPHost',
b'IncomingServer',
b'Account',
b'MailAddress',
b'Password',
b'POP3Password',
b'5A',
b'71',
b'Opera Mail',
b'\\Opera Mail\\Opera Mail\\wand.dat',
b'\\Opera Mail\\Opera Mail\\wand.dat',
b'opera:']
```