XORStringsNet

Published: 2023-04-16 · Archived: 2026-04-05 19:18:06 UTC

```
[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'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'&amp;',
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\\recentservers.xml',
b'APPDATA',
b'\\FileZilla\\recentservers.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'hdfzpysvpzimorhk',
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'yA36zA48dEhfrvghGRg57h5UlDv3',
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\\
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:']
```

Source: https://research.openanalysis.net/dotnet/xorstringsnet/agenttesla/2023/04/16/xorstringsnet.html