StrelaStealer

Published: 2023-05-07 · Archived: 2026-04-05 21:21:02 UTC

Analysis

Sample - November 2022

`be9f84b19f02f16b7d8a9148a68ad8728cc169668f2c59f918d019bce400d90e`

`Wed Nov 2 08:50:41 2022 UTC`

String Decryption

The strings are encrypted with XOR using a hard coded key that resembles a GUID `4f3855aa-af7e-4fd2-b04e-55e63653d2f7`

IDA String Decrypt

The following can be used to highlight and decrypt strings in IDA.

```
key = b'4f3855aa-af7e-4fd2-b04e-55e63653d2f7'

def xor(data, key):
    out = []
    for i in range(len(data)):
        out.append(data[i] ^ key[i%len(key)])
    return bytes(out)


start = idc.read_selection_start()
end = idc.read_selection_end()
if idaapi.BADADDR in (start, end):
    ea = idc.here()
    start = idaapi.get_item_head(ea)
    end = idaapi.get_item_end(ea)
data = idc.get_bytes(start, end - start).encode('hex')

out = xor(data, key)
print(out)
```

Hot-key Bind.

```
import ida_expr import ida_kernwin
import idc
import ida_bytes
import ida_kernwin

ida_expr.compile_idc_text('static n_key() { RunPythonStatement("nopping()"); }')
ida_kernwin.add_idc_hotkey("Alt-N", "n_key")
```

C2 Comms

The harvested data is sent to the following hard coded C2 with a POST request.

`http[:]//193.106.191[.]166/server.php`

Decoy

The payload expects a `x.pdf` file to be present in the launch directory at runtime. This pdf is launched by the malware as a decoy to trick the user into thinking they have only opened a PDF not launched an executable. The PDF is not dropped by the payload, instead the payload relies on the previous stage to deploy the PDF. This directly ties the payload to delivery stage which is unusual for malware that is sold, and indicates that this malware is both developed and operated by the same actor.

```
cmd /c start msedge x.pdf
```

Sample - April 2023

`61118d0f778c2f9b3a2bb3e37176ba6a13ee266c49b89dab7e187129f5c00887`

`Sun Apr 2 22:42:15 2023 UTC`

Updates

- All strings are now plaintext
- The decoy has been simplified to launch an error message box rather than a PDF
- PE file not a DLL
- The C2 comms are still encrypted with a hard coded XOR string `7a7dd62b-c4ea-4bbb-9f3f-2e6d58aada40`

C2

`http[:]//91[.]215.85.209/server.php`

Decoy

The new "decoy" no longer requires a PDF instead a message box is launched that says...

```
El archivo está dañado y no se puede ejecutar
```

Translated from Spanish this reads `The file is damaged and cannot be executed`, an attempt to trick the user into thinking they can't open the lure. Based on the use of Spanish they are still targeting Spanish victims.

PDB Tracking

The following PDB paths have been found in versions of Strela.

```
 C:\Users\Serhii\Documents\Visual Studio 2008\Projects\StrelaDLLCompile\Release\StrelaDLLCompile.pdb
C:\Users\admin\source\repos\Dll1\Release\Dll1.pdb
C:\Users\Serhii\Documents\Visual Studio 2008\Projects\dll1\Release\dll1.pdb
C:\Users\Serhii\source\repos\WindowsProject1\x64\Release\WindowsProject1.pdb
```

Pivoting from these PDB paths and searching through public malware repositories related samples have been recovered indicating that the developer has been working on similar projects since at least `2022-01-23 21:58:42` (sample `d091cb30b4c19b24249af2648d8c43abd5390118d502b5041b5d89d2152a0d7a`).

Malware in Development

Some related samples are not malware but rather test code apparently used to test features in development. These include a sample `2F3A2B18252E39C5B95A199412D97916E6E2611F3A83EF7160E74AA959A41933` that appears to be some type of `putty.exe` launcher using the local path `C:\\Users\\Serhii\\Downloads\\putty.exe`.

C2 Tracking

Performing a revers lookup for the C2 IP `91.215.85[.]209` the following domains have been registered and point to this IP. It is unclear what their purpose is.

```
 posts-fi[.[com
carrefours-tw[.]com
directeredie[.]org
dkpostnord[.]com
fornying-skonto[.]com
redisimple[.]com
chunghwa-post[.]app
atuh-manor[.]com
post-chunghwa-tw[.]app
post-chunghwa-tw[.]com
tibouton[.]org
carrefour-tw[.]com
post-tw[.]app
```

Source: https://research.openanalysis.net/strelastealer/stealer/2023/05/07/streala.html