#ShortAndMalicious: StrelaStealer aims for mail credentials

By DCSO CyTec Blog

Published: 2022-11-21 · Archived: 2026-04-05 20:13:29 UTC

Press enter or click to view image in full size

Strela surface-to-air missile launcher (Source: Wikipedia)

In our newest category **#ShortAndMalicious** *DCSO CyTec* aims to briefly highlight new and interesting samples we come across in our daily hunt for malware.

For the first entry in the series, we take a brief look at an undocumented custom malware we have been analysing under the moniker “StrelaStealer” (“Стрела” == arrow) which appears to be purpose-built to steal mail login data.

Press enter or click to view image in full size

```
'C:\Users\Serhii\Documents\Visual Studio 2008\Projects\'
'StrelaDLLCompile\Release\StrelaDLLCompile.pdb',0
```

PDB path contained in StrelaStealer samples

DCSO CyTec first discovered StrelaStealer early November 2022 distributed via ISO files with what appears to be Spanish targets based on used lure documents. It is unclear at this point in time if StrelaStealer is part of a targeted attack.

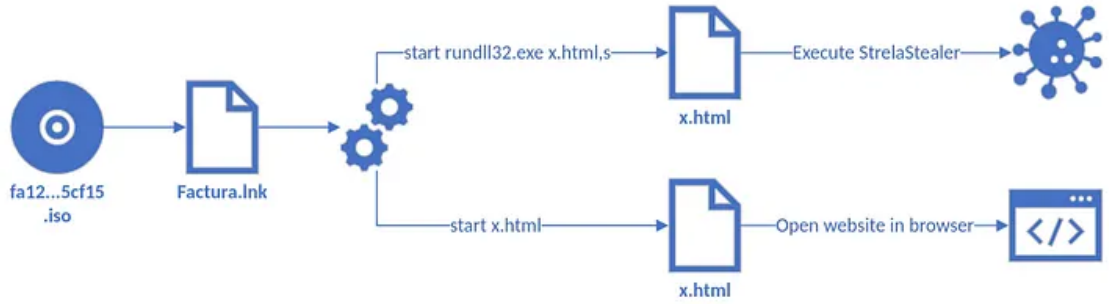
Blog authored by Johann Aydinbas and Axel Wauer.

Execution via polyglot

StrelaStealer samples are distributed in ISO files with varying content. In one instance, StrelaStealer uses a renamed msinfo32.exe to sideload StrelaStealer as slc.dll. Another, more interesting variant distributes StrelaStealer as a DLL/HTML polyglot.

Polyglots files are files that are valid as two or more different file formats. In this case, StrelaStealer uses a file that is both valid as a DLL as well as an HTML page.

Press enter or click to view image in full size



Execution of StrelaStealer via polyglot

The ISO file contains two files, one `Factura.lnk` and the polyglot `x.html` file. The LNK file then executes `x.html` twice, once as a DLL and a second time as an HTML file.

Press enter or click to view image in full size

```
DATA
   Relative path: ..\..\..\..\..\..\Windows\System32\cmd.exe
   Command line arguments: /c start rundll32.exe x.html,s & start x.html
   Icon location: %SystemRoot%\System32\SHELL32.dll
```

Parsed LNK file — command to execute the polyglot

Inspecting `x.html` then shows that it simply contains HTML code appended to the DLL file:

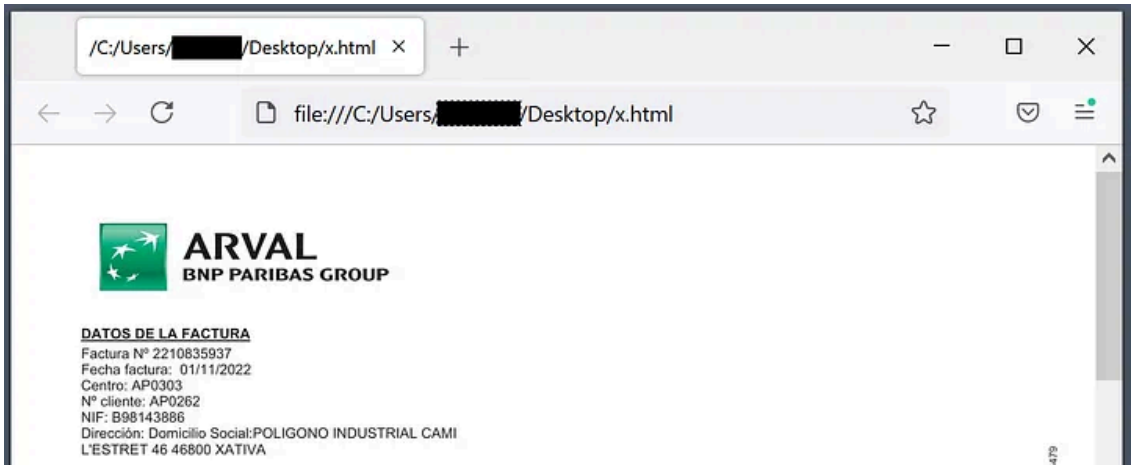
Press enter or click to view image in full size

```
B9D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
B9E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
B9F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
BA00h: 3C 73 63 72 69 70 74 3E 64 6F 63 75 6D 65 6E 74  <script>document
BA10h: 2E 67 65 74 45 6C 65 6D 65 6E 74 73 42 79 54 61  .getElementsByTa
BA20h: 67 4E 61 6D 65 28 22 68 74 6D 6C 22 29 5B 30 5D  gName("html")[0]
BA30h: 2E 69 6E 6E 65 72 48 54 4D 4C 20 3D 20 27 3C 69  .innerHTML = '<i
BA40h: 6D 67 20 73 72 63 3D 22 64 61 74 61 3A 69 6D 61  mg src="data:ima
BA50h: 67 65 2F 6A 70 65 67 3B 62 61 73 65 36 34 2C 2F  ge/jpeg;base64,/
```

Appended HTML code

Double-clicking it opens the browser and displays the lure document:

Press enter or click to view image in full size

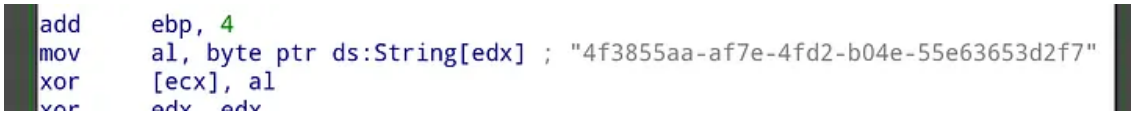


Lure document rendered by Firefox

Malware analysis

StrelaStealer samples are DLL files, with the main functionality triggered by calling its main export function named `Strela` or `s`. While its code is not obfuscated, strings are encrypted with a cyclic xor with a hardcoded key:

Press enter or click to view image in full size



Hardcoded xor key

Once executed, StrelaStealer attempts to locate and steal mail login data from Thunderbird and Outlook.

Get DCSO CyTec Blog's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

For Thunderbird, StrelaStealer searches for `logins.json` and `key4.db` in the `%APPDATA%\Thunderbird\Profiles\` directory and sends the file contents to its C2.

For Outlook, StrelaStealer enumerates the registry key `HKCU\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\` in order to find the values `IMAP User`, `IMAP Server` and `IMAP Password`. StrelaStealer then decrypts the `IMAP Password` using `CryptUnprotectData` before sending the triple to its C2.

Communication

Communication is done using plain HTTP POSTs, with the payload encrypted using the same xor key as for the strings. C2 server and resource name are hardcoded and so far all samples were configured for the same one:

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

The IP address is hosted on known Russian bulletproof hosting “Kanzas LLC” with the /24 likely being hosted in Moscow.

Stolen files from Thunderbird are sent home in the following format:

```
[prefix "FF"]
[DWORD size logins.json]
[contents of logins.json]
[contents of key4.db]
```

Outlook data uses the following format:

```
[prefix "OL"]
[Server1,User1,Password1]
[Server2,User2,Password2]
...
```

When sending home data, StrelaStealer checks for the last two bytes of the response to be `KH` which appears to signal a successful transfer and causes StrelaStealer to quit, otherwise it retries to send the data again after a 1 second sleep.

IoCs

As usual, you can find below the IoCs. We share a MISP event on our GitHub.

```
sha256
fa1295c746e268a3520485e94d1cecc77e98655a6f85d42879a3aeb401e5cf15
c8eb6efc2cd0bd10d9fdd4f644ebbebdebaff376ece9e48ff502f973fe837820
8b0d8651e035fcc91c39b3260c871342d1652c97b37c86f07a561828b652e907
879ddb21573c5941f60f43921451e420842f1b0ff5d8eccabe11d95c7b9b281e
b7e2e4df5cddcbf6c0cda0fb212be65dea2c442e06590461bf5a13821325e337
d8d28aa1df354c7e0798279ed3fecad8effef8c523c701faaf9b5472d22a5e28
ac040049e0ddbcb529fb2573b6eced3cfaa6cd6061ce2e7a442f0ad67265e800
bfc30cb876b45bc7c5e7686a41a155d791cd13309885cb6f9c05e001eca1d28a
6e8a3ffffd2f7a91f3f845b78dd90011feb80d30b4fe48cb174b629afa273403
c69bac4620dcf94acdee3b5e5bcd73b88142de285eea59500261536c1513ab86
be9f84b19f02f16b7d8a9148a68ad8728cc169668f2c59f918d019bce400d90e
1437a2815fdb82c7e590c1e6f4b490a7cdc7ec81a6cb014cd3ff712304e4c9a3Pdb path:
C:\Users\admin\source\repos\Dll1\Release\Dll1.pdb
"C:\Users\Serhii\Documents\Visual Studio 2008\Projects\StrelaDLLCompile\Release\StrelaDLLCompile.pdb
193.106.191[.]166
```

```
hxxp://193.106.191[.]166/server.phpITW URL:
hxxp://45.142.212[.]20/dll.dll
```

MITRE ATT&CK

```
T1003     - Credential Dumping
T1041     - Exfiltration Over C2 Channel
T1041     - Exfiltration Over Command and Control Channel
T1059.003 - Windows Command Shell
T1071     - Standard Application Layer Protocol
T1566.001 - Spearphishing Attachment
T1574.002 - DLL Side-Loading
```
