

## Infostealer Malware with Double Extension - SANS ISC

By SANS Internet Storm Center

Archived: 2026-04-05 16:50:17 UTC

Got this file attachment this week pretending to be from HSBC Global Payments and Cash Management. The attachment payment\_copy.pdf.z is a rar archive, kind of unusual with this type of file archive but when extracted, it comes out as a double extension with pdf.exe. The file is a trojan infostealer and detected by multiple scanning engines.

---

Good morning,

The attached payment advice is issued at the request of our customer. The advice is for your reference, kindly confirm in return.

Yours faithfully,

Global Payments and Cash Management

Customer Service Manager

Tel: +352 40 46 46 1  
HSBC



August 2016HSBC Premier Account Opening Application Form© Copyright. HSBC Bank Middle East Limited 2016 ALL RIGHTS RESERVED.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of HSBC Bank Middle East Limited. Issued

by HSBC Bank Middle East Limited U.A.E Branch, P.O. Box 66, Dubai, U.A.E, regulated by the Central Bank of the U.A.E and lead regulated by the Dubai Financial Services Authority. V160512

Using [CyberChef](#) Forensics -> Extract Files, you can view a list of files part of the executable from the .exe, .zlib and various mp3 and png.

**Recipe**

**Extract Files**

- Images
- Video
- Audio
- Documents
- Applications
- Archives
- Miscellaneous
- Ignore failed extractions

**Input**

Name: payment copy.pdf.exe  
Size: 895,488 bytes  
Type: application/x-ms-dos-execut...

**Output**

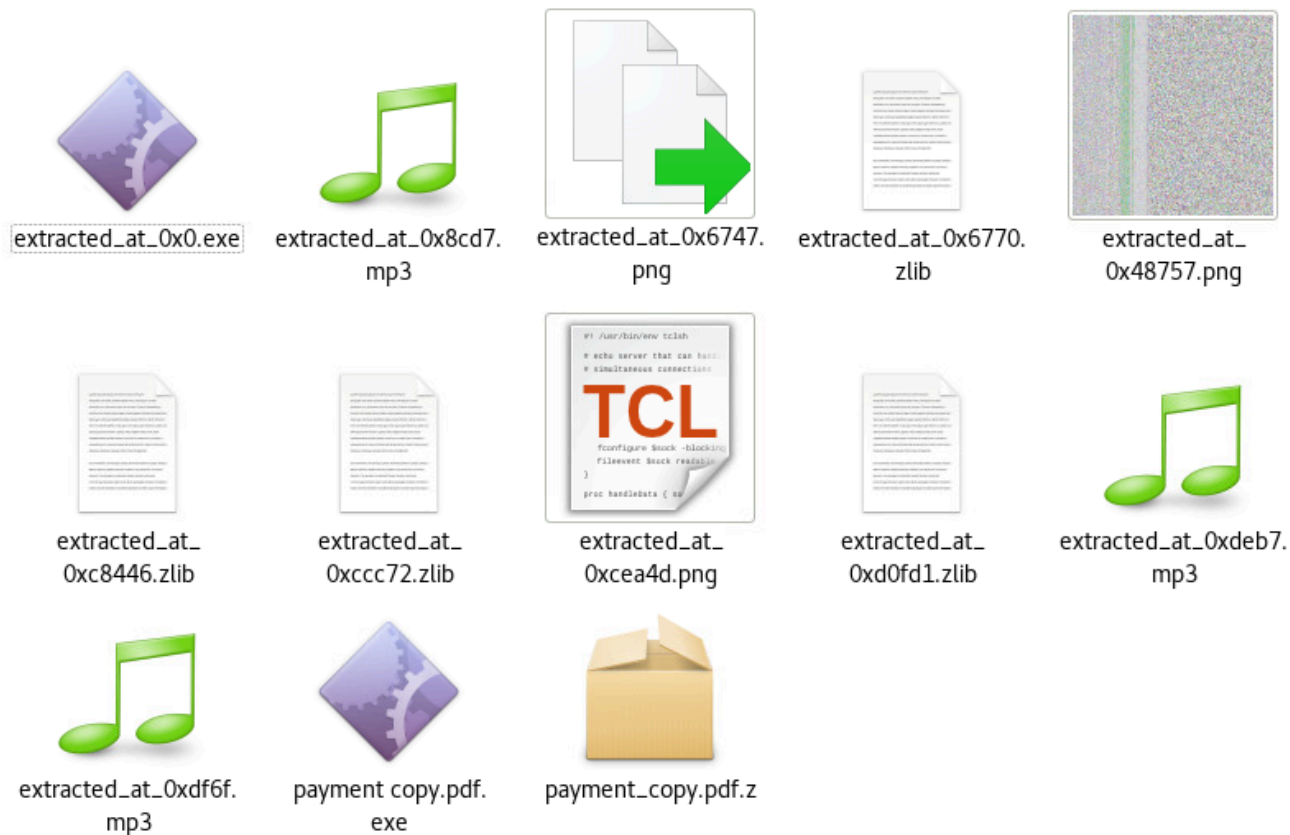
time: 1327ms  
length: 1662070  
lines: 5882

465 file(s) found

extracted_at_0x0.exe	895,488 bytes
extracted_at_0x6747.png	7,941 bytes
extracted_at_0x6770.zlib	134 bytes
extracted_at_0x8cd7.mp3	3 bytes
extracted_at_0x8cdb.mp3	3 bytes
extracted_at_0x8cdf.mp3	3 bytes
extracted_at_0x8ce3.mp3	3 bytes
extracted_at_0x8ce7.mp3	3 bytes

STEP **BAKE!**

Saving some of the files to review and analyze them:



### Indicators of Compromise

Filename: payment\_copy.pdf.z -> RAR archive data

[SHA256](#): 37da8f89540f4dae114f1f55cfd4d89be9582fbd480ac6ed6c34ac04ec8d576b

SSDEEP:

12288:jiE0YCjBwMh6ny+h+n6SN/PAQDnNNTtcvCEYLPQE5FiER3RiSbhXwS:eE3K0Mh6nyU+6SOQ77IPQaFpbeS

Filename: payment\_copy.pdf.exe

IPs: 3.232.242[.]170, 52.20.78[.]240, 54.91.59[.]199, 65.108.213[.]43, 209.197.3[.]8

Domains: api.ipify[.]org, api.ipify.org.herokudns[.]com, mail.reousaomilia[.]gr, reousaomilia[.]gr,

www.inkscape[.]org

[SHA256](#): 3ccaf74f465a79ec320fdb7e44ae09551f4348efd3bf8bf7b3638cc0c1cd8492

[1] <https://www.virustotal.com/gui/file/37da8f89540f4dae114f1f55cfd4d89be9582fbd480ac6ed6c34ac04ec8d576b>

[2] <https://www.virustotal.com/gui/file/3ccaf74f465a79ec320fdb7e44ae09551f4348efd3bf8bf7b3638cc0c1cd8492>

[3] <https://gchq.github.io/CyberChef/>

-----

Guy Bruneau [IPSS Inc.](#)

[My Handler Page](#)

Twitter: [GuyBruneau](#)

gbruneau at isc dot sans dot edu

---

Source: <https://isc.sans.edu/diary/Infostealer+Malware+with+Double+Extension/29354>