# 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

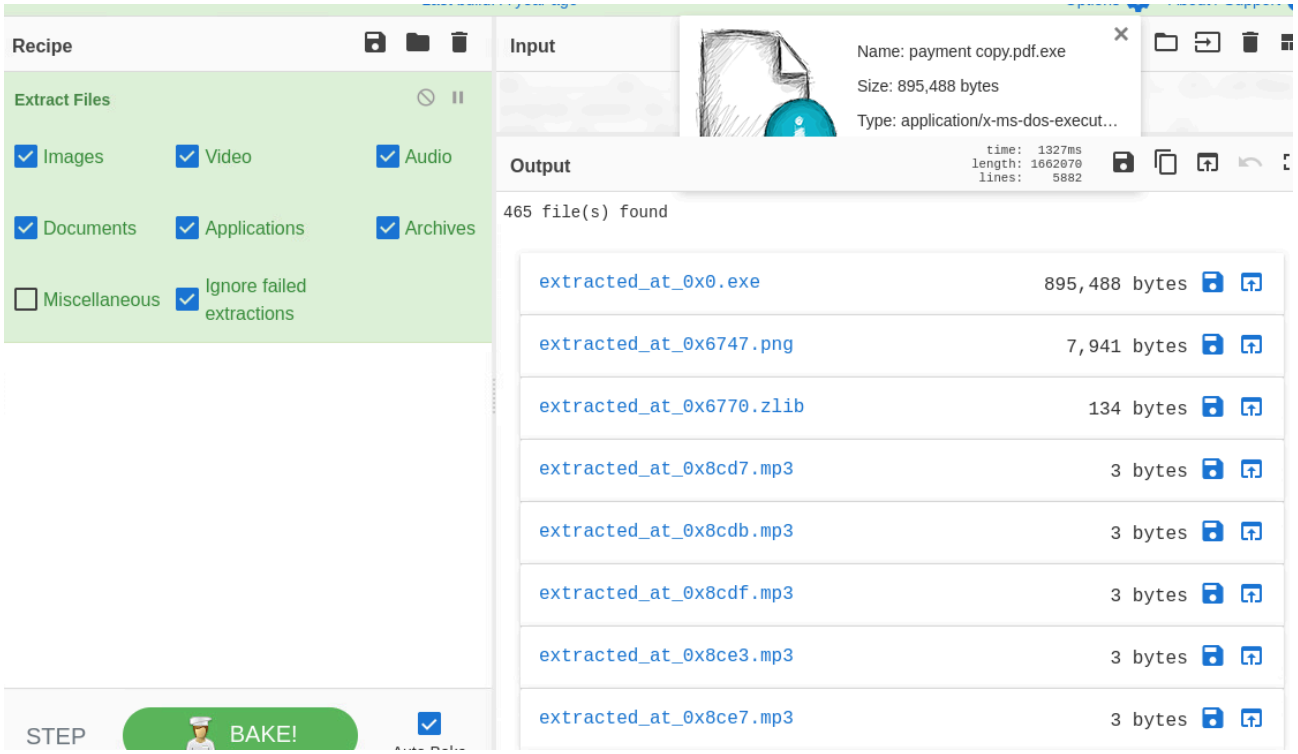
Customer Service Manager

Tel: +352 40 46 46 1
HSBC

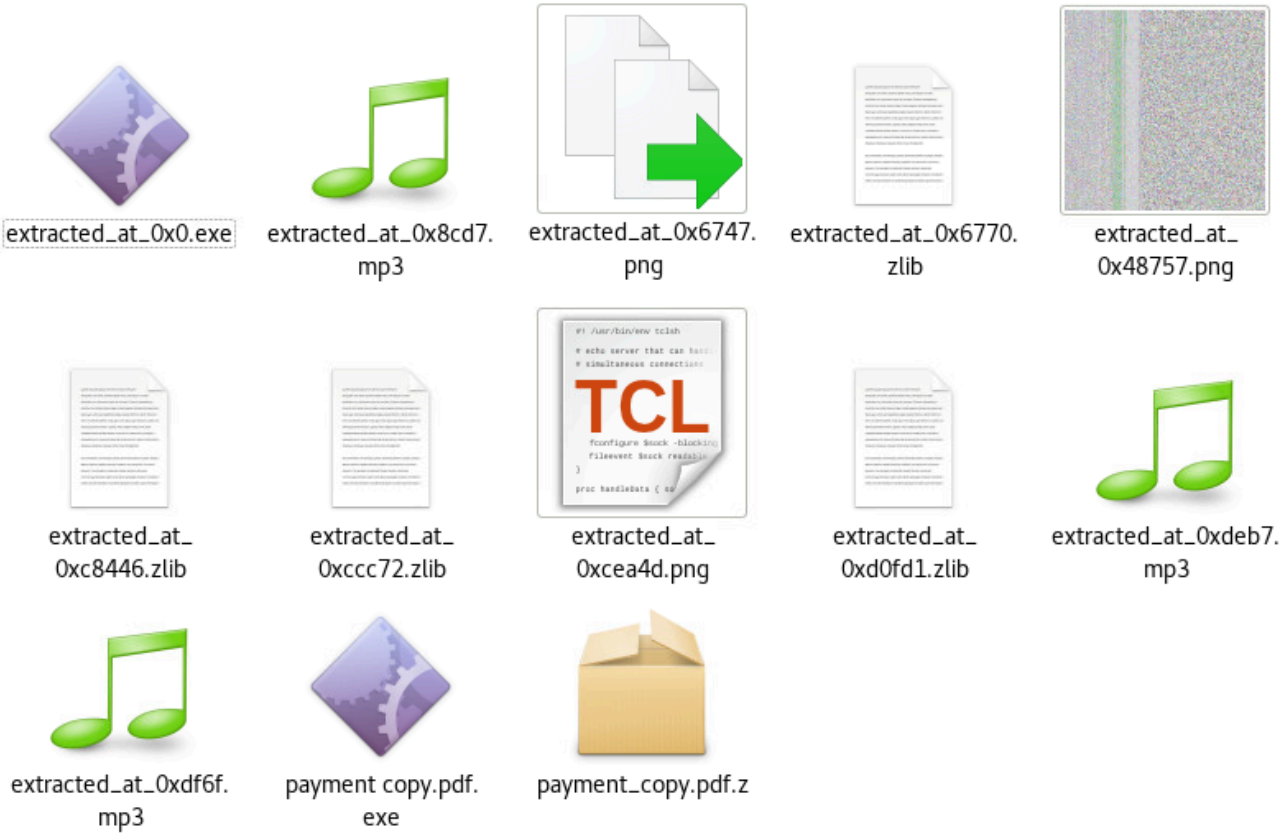
HSBC



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.




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+6SOQ77lPQaFpbeS

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

---