

## Not so nice after all - afrodita ransomware

By f0wL

Published: 2020-01-09 · Archived: 2026-04-06 00:20:06 UTC

Thu 09 January 2020 in [Ransomware](#)

A new Ransomware strain spread by malicious Office documents targeted at Croatian systems - let's check it out



This strain was first discovered by Korben Dallas on Twitter on the 9th of January. As I already mentioned the Malware is delivered via a Malspam/Maldoc attack crafted for Users / Companies from Croatia. Researchers that were involved in the initial analysis: [@KorbenD\\_Intel](#), [@James\\_inthe\\_box](#), [@Malwageddon](#), [@pollo290987](#) and I ([@f0wLsec](#)). Thank you for your contributions!

***A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f\$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.***

Afrodita @ [AnyRun](#) | [VirusTotal](#) | [HybridAnalysis](#) --> sha256  
9b6681103545432cd1373492297a6a12528f327d14a7416c2b71cfdcbdafc90b

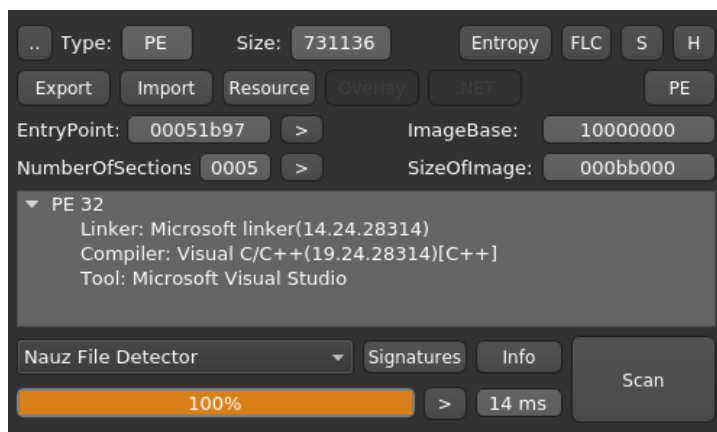
Here you can see three images extracted from the malicious Excel Docs. Funny how they didn't even bother to think of a fake company name for the second Logo :D



Afrodita uses a sleep routine for Sandbox evasion. In my Tests it took 30-60mins until the system was infected.



After unpacking the sample with UPX, *Detect it easy* returns the following:



It was likely build with a very new Version of Visual Studio (2019)

Below you can see a screenshot of PEBear from the Imports-Tab.

Offset	Name	Func. Count	Bound?	OriginalFirstT	TimeDateStar	Forwarder	NameRVA	FirstThunk
40000	KERNEL32...	110	FALSE	0	0	0	A5FD0	80010
40003	ADVAPI32.dll	3	FALSE	0	0	0	A600A	80000
40007	Rstrtmgr.DLL	4	FALSE	0	0	0	A5DB2	801CC
40009	SHELL32.dll	1	FALSE	0	0	0	A6008	801E0
40010	SHLWAPI.dll	1	FALSE	0	0	0	A5DB2	801E0
40011	USER32.dll	7	FALSE	0	0	0	A600E	801F4

Call via	Name	Ordinal	Original Thun	Thunk	Forwarder	Hint
40000	CryptReleaseContext	-	-	A6082	-	0
40003	CryptAcquireContextA	-	-	A600A	-	0
40009	CryptGenRandom	-	-	A6008	-	0

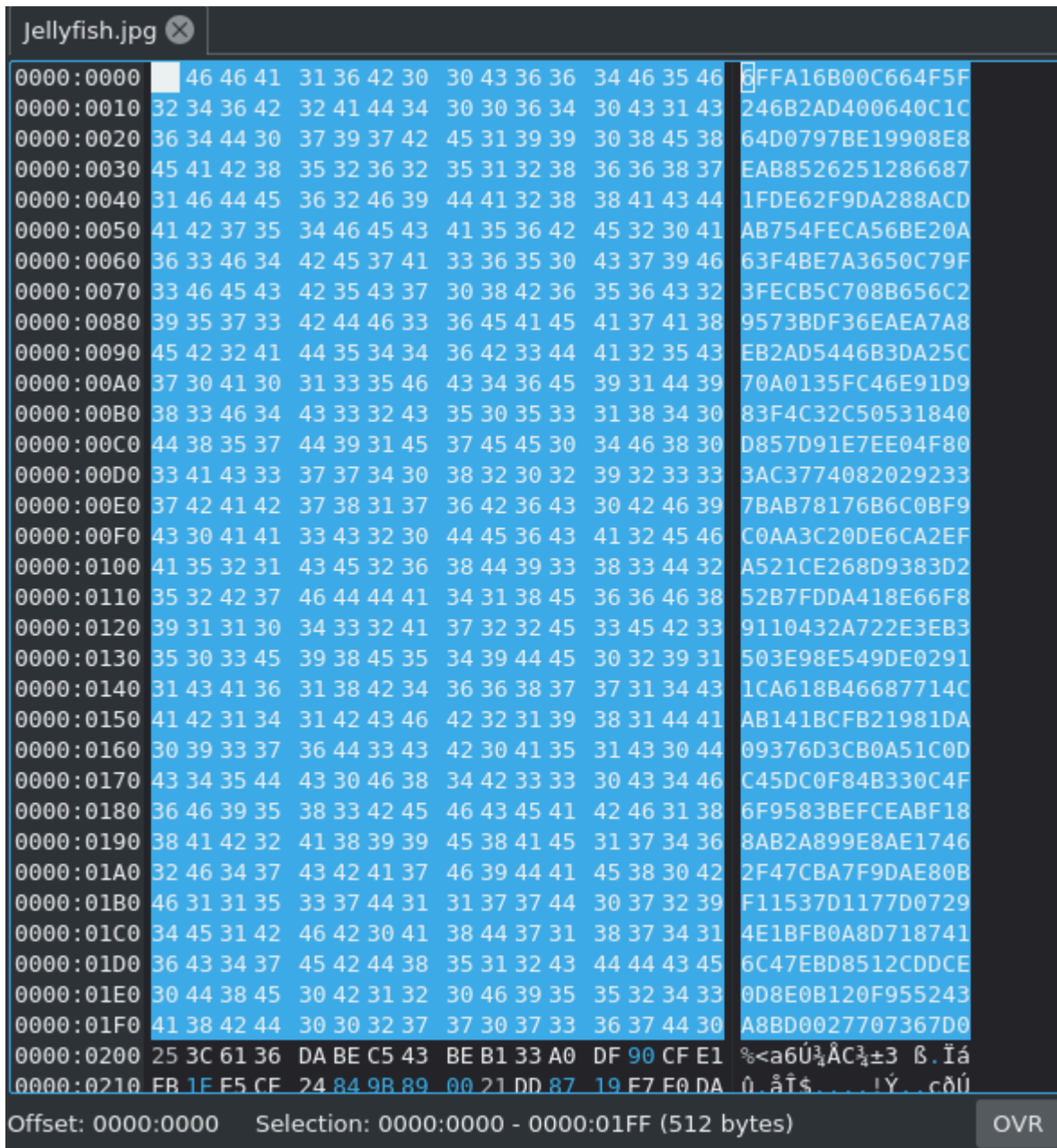
The extracted strings tell us quite a lot in this case. It looks like the internal name of the Project is *Afrodita* and it utilizes the CryptoPP Library. There are some references to .key files, but I haven't found a path or file on a infected machine yet. **README\_RECOVERY .txt** is will be the filename of the Ransomnote. It's contents are embeded in the binary's .data section with Base64 encoding. Lastly *Afrodita.dll* is the rewritten file that is downloaded as a payload (originally notice.jpg or verynice.jpg). It's executed via **rundll32.exe Afrodita.dll,Sura**.

```
F:\Work\x_Projects\Afrodita - VS2019\Afrodita\cryptopp\rijndael_simd.cpp
F:\Work\x_Projects\Afrodita - VS2019\Afrodita\cryptopp\sse_simd.cpp
F:\Work\x_Projects\Afrodita - VS2019\Afrodita\cryptopp\sha_simd.cpp
client-encrypted-private.key
client-encrypted-private.key
\ README_RECOVERY .txt
_uninsep.bat
client-public.key
client-public.key
client-public.key
client-public.key
Afrodita.dll
```

The following filetypes will be encrypted by Afrodita:

```
.TXT, .ZIP, .DAT, .JPE, .JPG, .PNG, .JPEG, .GIF, .BMP, .EXIF, .MP4, .RAR, .M4A, .WMA, .AVI, .WMV, .MI
```

The Ransomware encrypts the first 512 Bytes of the File Header which will render most filetypes useless. It does not leave any Signature in the data of the files and neither does it append a custom extension to the filename.



Another IOC: It creates the following Mutex: 835821AM3218SAZ

```
uint FUN_100151f0(void)
{
    DWORD DVar1;

    CreateMutexW((LPSECURITY_ATTRIBUTES)0x0,1,L"835821AM3218SAZ");
    DVar1 = GetLastError();
    return (uint)(DVar1 == 0xb7);
}
```

Update 10.01.2020:

The criminals obviously failed to properly display the key / victim ID in the Ransomnote. This was also a problem because the screwed encoding killed this Blogs Atom RSS Feed :D To resolve this issue I removed the malformed section from this page. If you want to have a look at the original note plus a couple of encrypted jpegs, download the [zip](#) file.

Also this Malware family isn't as new as I originally thought. According to Michael Gillespie the MalwareHunterTeam found the first Maldoc in Late November. A few days later Checkpoint research found it as well:

Today Michael also asked if anyone was able to parse the *main-public.key* because the format seems off. I extracted it from the binary:

```

000A:9D80 70 63 68 61 72 4E 6F 64 65 40 40 00 24 D3 08 10 pcharNode@@.$Ó..
000A:9D90 00 00 00 00 2E 3F 41 56 70 44 4E 61 6D 65 4E 6F .....?AVpDNameNo
000A:9DA0 64 65 40 40 00 00 00 00 24 D3 08 10 00 00 00 00 de@@....$Ó.....
000A:9DB0 2E 3F 41 56 44 4E 61 6D 65 53 74 61 74 75 73 4E .?AVDNameStatusN
000A:9DC0 6F 64 65 40 40 00 00 00 24 D3 08 10 00 00 00 00 ode@@...$Ó.....
000A:9DD0 2E 3F 41 56 70 61 69 72 4E 6F 64 65 40 40 00 00 .?AVpairNode@@..
000A:9DE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9DF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9E00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....
000A:9E10 58 00 00 80 18 00 00 80 00 00 00 00 00 00 00 00 X.....
000A:9E20 00 00 00 00 00 00 01 00 6B 00 00 00 30 00 00 80 .....k...0...
000A:9E30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
000A:9E40 00 20 00 00 48 00 00 00 70 10 0B 00 24 01 00 00 . .H...p...$...
000A:9E50 00 00 00 00 00 00 00 00 07 00 49 00 44 00 52 00 .....I.D.R.
000A:9E60 5F 00 52 00 53 00 41 00 00 00 00 00 00 00 00 00 .R.S.A.....
000A:9E70 30 82 01 20 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0. 0...*.H.+...
000A:9E80 01 05 00 03 82 01 0D 00 30 82 01 08 02 82 01 01 .....0.....
000A:9E90 00 C6 CD B1 91 E1 D1 CA 06 41 BA 91 5C DB E6 7F .ÆÍ±.áÑĒ.A².\Ûæ.
000A:9EA0 FD D2 E7 31 B5 91 FC D8 97 40 19 8F D7 44 3B 9D ýÏçlμ.üø.@...xD;.
000A:9EB0 B1 BF E6 36 83 72 29 3E 78 60 E1 DB 3C FA 5D 8A ±¿æ6.r)>x`áÛ<ú].
000A:9EC0 F6 52 BF AC 4B 5C 83 E3 FD 57 41 E2 19 FF 38 DC öR¿-K\..ăýWAá.ÿ8Û
000A:9ED0 8C 2E 37 1F 4F 74 9D 49 44 2D 3B 6A F4 40 FC 2E ..7.0t.ID-;jô@ü.
000A:9EE0 A7 AF 9E B3 9A 31 01 72 50 88 50 53 EA 65 63 97 §~.³.1.rP.PSêec.
000A:9EF0 89 77 A2 AE 5B 67 42 76 FF 27 D2 E0 43 03 30 50 .wç@[gBvÿ'òàC.0P
000A:9F00 46 7A 63 26 BD 00 9A 79 04 CD 11 83 E5 70 A8 62 Fzc&½...y.Í..âp`b
000A:9F10 DA D1 D3 AD 64 04 07 AB 5D 08 C1 C6 14 12 9E C3 ÚÑÓ.d...«].ÁÆ...Ă
000A:9F20 16 C4 4D 91 7B 17 2A DF CB 60 7F FB 33 5C F6 A8 .ĂM.{.*BĒ`.ú3\ö`
000A:9F30 48 3D 6F B1 29 88 C1 76 DC DE 74 E4 69 D6 0F 7E H=o±).ÁvÜptäiÖ.~
000A:9F40 32 EE E9 A5 96 62 68 A4 58 88 B7 CF E4 68 50 E9 2íé¥.bh=X.·ĪâhPé
000A:9F50 BB 3A 19 9A 3A EF 9A CC F0 8F 06 31 DC F7 77 01 »:..:î.İð...lÛ+w.
000A:9F60 2A C2 E7 C7 34 87 88 A4 45 37 87 1D D1 3B BE BA *ÂçÇ4...E7..Ñ;¾²
000A:9F70 F7 A1 1A 5D 7E BF 70 8A D1 98 FE 9E BE 4E 7D E3 +;.]~¿p.Ñ.p.¾N}ã
000A:9F80 63 30 66 10 8F CD 2D D3 E0 2A 9C 34 24 CF 07 40 c0f..İ-òà*.4$Ī.@
000A:9F90 FF 02 01 11 00 00 00 00 00 00 00 00 00 00 00 00 Ÿ.....
000A:9FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:A000 00 10 00 00 64 02 00 00 06 30 26 30 32 30 43 30 ....d....0&020C0
000A:A010 48 30 59 30 5E 30 6C 30 71 30 7F 30 84 30 92 30 H0Y0^0l0q0.0.0.0
000A:A020 97 30 A5 30 AA 30 B8 30 BD 30 CB 30 D0 30 DE 30 .0¥0²0,0½0Ē0Đ0P0
000A:A030 E3 30 F1 30 F6 30 04 31 09 31 17 31 1C 31 2A 31 ä0ñ0ö0.1.1.1.1*1

```

A quick look into the [CryptoPP Wiki](#) revealed that the key was in raw (uncooked) ASN.1 format (you can identify it by hex 30 82). Using an online ASN.1 decoder ([Link](#)) yields us the public key:

### ASN.1 JavaScript decoder

```

SEQUENCE (2 elem)
  SEQUENCE (1 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
  NULL
  BIT STRING (1 elem)
  SEQUENCE (2 elem)
    INTEGER (2048 bit) 25096615693731054222251480849593011269011075638654889785452933935645...
    INTEGER 17
MIIBIDANBgkqhkiG9w0BAQEFAAACQ0AMIIBCAKCAQEAxs2xkeHRygZBupFc2+Z//dLnMbWR/NiXQBmP
1007hbG/5jadkik+eGDh2zz6XYr2Ur+sS1yD4/1XQeIZ/zjcjC43H090nULELTtq9ED8LqevnrOaMQFy
UIhQU+pLY5eJd6KuW2dCdv8n0uBDAzBQRnpjJr0AmnkEzRGD5XCoYtrR061kBAerXQjBxhQSnsMWxE2R
excq38tgf/szXPaoSD1vsSmIwXbc3nTkadYPfjLu6aWWYmikWi3z+RoU0m70hmaOu+azPCPBjHc93cB
KsLnxzShiKRFN4cd0Tu+uvehG11+v3CK0Zj+nr50feNjMGYQj80t0+AqnDQkzwdA/wIBEQ==

```

with hex dump decode clear example

Browse... test key

```

-----BEGIN RSA PUBLIC KEY-----
MIIBIDANBgkqhkiG9w0BAQEFAAACQ0AMIIBCAKCAQEAxs2xkeHRygZBupFc2+Z//dLnMbWR/NiXQBmP
1007hbG/5jadkik+eGDh2zz6XYr2Ur+sS1yD4/1XQeIZ/zjcjC43H090nULELTtq9ED8LqevnrOaMQFy
UIhQU+pLY5eJd6KuW2dCdv8n0uBDAzBQRnpjJr0AmnkEzRGD5XCoYtrR061kBAerXQjBxhQSnsMWxE2R
excq38tgf/szXPaoSD1vsSmIwXbc3nTkadYPfjLu6aWWYmikWi3z+RoU0m70hmaOu+azPCPBjHc93cB
KsLnxzShiKRFN4cd0Tu+uvehG11+v3CK0Zj+nr50feNjMGYQj80t0+AqnDQkzwdA/wIBEQ==
-----END RSA PUBLIC KEY-----

```

### MITRE ATT&CK

- T1179 --> Hooking --> Persistence
- T1179 --> Hooking --> Privilege Escalation
- T1045 --> Software Packing --> Defense Evasion
- T1179 --> Hooking --> Credential Access
- T1114 --> Email Collection --> Collection

### IOCs

#### Afrodita

```

notnice.jpg --> SHA256: 9b6681103545432cd1373492297a6a12528f327d14a7416c2b71cfdcbdafc90b
SSDEEP: 6144:EXrm0zIiAhjC7Cqa5ZhiIJDQ13Xdksm1Cx2tJk:EbNqaCq6iIjcdksmJtJ

```

#### Payload Servers

```

hxxp://riskpartner[.]hr/wp-content/notnice.jpg
hxxp://content-delivery[.]in/verynice.jpg

```

#### E-Mail Addresses / Contact

```

afroditateam@tutanota.com
afroditasupport@mail2tor.com

```

hxtps://t[.]me/RecoverySupport

## Ransomnote

~~~ Greetings ~~~

[+] What has happened? [+]

Your files are encrypted, and currently unavailable. You are free to check.  
Every file is recoverable by following our instructions below.

Encryption algorithms used: AES256(CBC) + RSA2048 (military/government grade).

[+] Guarantees? [+]

This is our daily job. We are not here to lie to you - as you are 1 of 10000's.  
Our only interest is in us getting payed and you getting your files back.

If we were not able to decrypt the data, other people in same situation as you  
wouldn't trust us and that would be bad for our buissness --  
So it's not in our interest.

To prove our ability to decrypt your data you have 1 file free decryption.

If you don't want to pay the fee for bringing files back that's okey,  
but remeber that you will lose a lot of time - and time is money.

Don't waste your time and money trying to recover files using some file  
recovery "experts", we have your private key - only we can get the files back.

With our service you can go back to original state in less then 30 minutes.

[+] Service [+]

If you decided to use our service please follow instructions below.

Contact us:

Install Telegram(available for Windows,Android,iOS) and contact us on chat:  
Telegram contact: <https://t.me/RecoverySupport>

Also available at email [afroditateam@tutanota.com](mailto:afroditateam@tutanota.com) cc: [afroditasupport@mail2tor.com](mailto:afroditasupport@mail2tor.com)

Make sure you are talking with us and not impostor by requiring free 1 file decryption to make sure

[Removed victim ID because it breaks the RSS Feed :D]

Title Image by [Robert Drózd](#), modified

---

---

Source: <https://dissectingmalwa.re/not-so-nice-after-all-afrodita-ransomware.html>