

Not so nice after all - Afrodita Ransomware

dissectingmalware.com/not-so-nice-after-all-afrodita-ransomware.html

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!

[@James_inthe_box](#) [@malwrhunterteam](#) [@Malwageddon](#)
69450923d812f3696e8280508b636955 XLS 12/60 VT scan detections. Not nice..
upped to Malshare: <https://t.co/jXxXrJxcB9> pic.twitter.com/TPfP0BCZOB

— Korben Dallas ([@KorbenD_Intel](#)) [January 9, 2020](#)

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

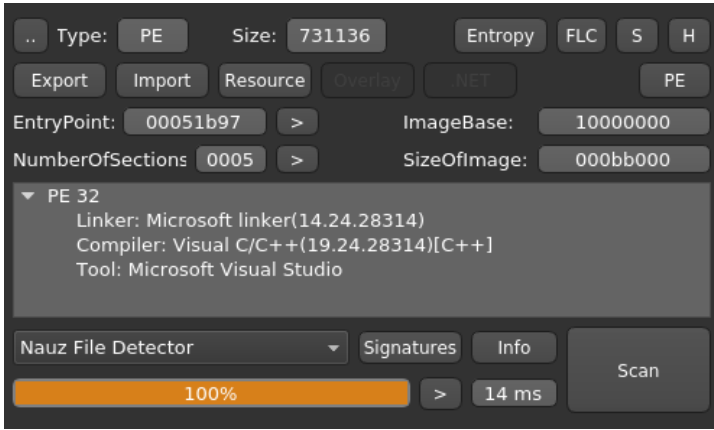


Za ispravno prikazivanje dokumenta pritisnite Enable Content.
Pritiskom na Enable Content provjeriti će se primatelj dokumenta te će se prikazati polja s oznakom GDPR_ZASTITA.

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
00000000	KERNEL32.dll	110	FALSE	0	0	0	43700	80110
00000003	ADVAPI32.dll	3	FALSE	0	0	0	43705	80105
00000004	Rstrtmgr.DLL	4	FALSE	0	0	0	43D82	801CC
00000005	SHELL32.dll	1	FALSE	0	0	0	44008	80180
0000000A	SHLWAPI.dll	1	FALSE	0	0	0	45D82	801E8
0000000E	USER32.dll	7	FALSE	0	0	0	4600C	80170

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
00000000	CryptReleaseContext	-	-	44082	-	0
00000004	CryptAcquireContextA	-	-	44008	-	0
00000008	CryptGenRandom	-	-	44008	-	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 notnice.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, .MKV, .CSV, .M3U, .FLV, .WALLET, .JAVA, .CLASS, .HTML, .HTM, .CSS, .LUA, .ASP, .PHP, .INCPAS, .ASM, .HPP, .CPP, .SLN, .ACCD, .MDB, .PPTM, .PPTX, .PPT, .XLK, .XLSB, .XLSM, .XLSX, .XLS, .WPS, .DOCM, .DOCX, .DOC, .ODB, .ODC, .ODM, .ODP, .ODS, .ACCD, .ACCDT, .ACUDE, .D3DBSP, .SIE, .SQL, .BACKUPDB, .BACKUP, .BAK, .SUM, .IBANK, .T13, .T12, .QDF, .GDB, .TAX, .PKPASS, .SLDM, .SLDX, .PPSM, .PPSX, .PPAM, .POTM, .POTX, .PPS, .POT, .XLW, .XLL, .XLAM, .XLA, .XLTM, .XLTX, .XLM, .XLT, .DOTM, .DOTX, .DOT, .BC6, .BC7, .BKP, .QIC, .BKF, .SIDN, .SIDD, .MDDATA, .ITL, .ITDB, .ICXS, .HVPL, .HPLG, .HKDB, .MDBACKUP, .SYNCDB, .GHO, .CAS, .SVG, .MAP, .WMO, .ITM, .FOS, .MOV, .VDF, .ZTMP, .SIS, .SID, .NCF, .MENU, .LAYOUT, .DMP, .BLOB, .ESM, .VCF, .VTF, .DAZIP, .FPK, .MLX, .IWD, .VPK, .TOR, .PSK, .RIM, .W3X, .FSH, .NTL, .ARCH00, .LVL, .SNX, .CFR, .VPP_PC, .LRF, .MCMETA, .VFS0, .MPQGE, .KDB, .DB0, .DBA, .ROFL, .HKX, .BAR, .UPK, .DAS, .IWI, .LITEMOD, .ASSET, .FORGE, .LTX, .BSA, .APK, .RE4, .SAV, .LBF, .SLM, .BIK, .EPK, .RGSS3A, .PAK, .BIG, .WOTREPLAY, .XXX, .DESC, .P7C, .P7B, .P12, .PFX, .PEM, .CRT, .CER, .DER, .X3F, .SRW, .PEF, .PTX, .R3D, .RW2, .RWL, .RAW, .RAF, .ORF, .NRW, .MRWREF, .MEF, .ERF, .KDC, .DCR, .CR2, .CRW, .BAY, .SR2, .SRF, .ARW, .3FR, .DNG, .CDR, .INDD, .EPS, .PDF, .PDD, .PSD, .DBF, .MDF, .WB2, .RTF, .WPD, .DXG, .DWG, .PST, .ODT, .DXF, .MP3, .MRW, .NEF, .JFIF, .DRF, .BLEND, .APJ, .3DS, .SDA, .PAT, .FXG, .FHD, .DXB, .DRW, .DESIGN, .DDRW, .DDOC, .DCS, .CSL, .CSH, .CPI, .CGM, .CDX, .CDRW, .CDR6, .CDR5, .CDR4, .CDR3, .AWG, .AIT, .AGD1, .YCBCRA, .STX, .ST8, .ST7, .ST6, .ST5, .ST4, .SD1, .SD0, .RWZ, .RA2, .PCD, .NWB, .NOP, .NDD, .MOS, .MFW, .MDC, .KC2, .IIQ, .GRY, .GREY, .GRAY, .FPX, .FFF, .EXF, .DC2, .CRAW, .CMT, .CIB, .CE2, .CE1, .3PR, .MPG, .SQLITEDB, .SQLITE3, .SQLITE, .SDF, .SAS7BDAT, .S3DB, .RDB, .PSAFE3, .NYF, .NX2, .NX1, .NSH, .NSG, .NSF, .NSD, .NS4, .NS3, .NS2, .MYD, .KPDX, .KDBX, .IDX, .IBZ, .IBD, .FDB, .ERBSQL, .DB3, .DB-JOURNAL, .CLS, .BDB, .ADB, .MONEYWELL, .MMW, .HBK, .FFD, .DGC, .DDD, .DAC, .CFP, .CDF, .BPW, .BGT, .ACR, .AC2, .AB4, .DJVU, .SXM, .ODF, .MSG, .STD, .SXD, .OTG, .STI, .SXI, .OTP, .ODG, .STC, .SXC, .OTS, .SXG, .STW, .SXW, .OTH, .OTT

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.

```

Jellyfish.jpg x
0000:0000 46 46 41 31 36 42 30 30 43 36 36 34 46 35 46 6FFFA16B00C664F5F
0000:0010 32 34 36 42 32 41 44 34 30 30 36 34 30 43 31 43 246B2AD400640C1C
0000:0020 36 34 44 30 37 39 37 42 45 31 39 39 30 38 45 38 64D0797BE19908E8
0000:0030 45 41 42 38 35 32 36 32 35 31 32 38 36 36 38 37 EAB8526251286687
0000:0040 31 46 44 45 36 32 46 39 44 41 32 38 38 41 43 44 1FDE62F9DA288ACD
0000:0050 41 42 37 35 34 46 45 43 41 35 36 42 45 32 30 41 AB754FECA56BE20A
0000:0060 36 33 46 34 42 45 37 41 33 36 35 30 43 37 39 46 63F4BE7A3650C79F
0000:0070 33 46 45 43 42 35 43 37 30 38 42 36 35 36 43 32 3FECB5C708B656C2
0000:0080 39 35 37 33 42 44 46 33 36 45 41 45 41 37 41 38 9573BDF36EAEA7A8
0000:0090 45 42 32 41 44 35 34 34 36 42 33 44 41 32 35 43 EB2AD5446B3DA25C
0000:00A0 37 30 41 30 31 33 35 46 43 34 36 45 39 31 44 39 70A0135FC46E91D9
0000:00B0 38 33 46 34 43 33 32 43 35 30 35 33 31 38 34 30 83F4C32C50531840
0000:00C0 44 38 35 37 44 39 31 45 37 45 45 30 34 46 38 30 D857D91E7EE04F80
0000:00D0 33 41 43 33 37 37 34 30 38 32 30 32 39 32 33 33 3AC3774082029233
0000:00E0 37 42 41 42 37 38 31 37 36 42 36 43 30 42 46 39 7BAB78176B6C0BF9
0000:00F0 43 30 41 41 33 43 32 30 44 45 36 43 41 32 45 46 C0AA3C20DE6CA2EF
0000:0100 41 35 32 31 43 45 32 36 38 44 39 33 38 33 44 32 A521CE268D9383D2
0000:0110 35 32 42 37 46 44 44 41 34 31 38 45 36 36 46 38 52B7FD4A18E66F8
0000:0120 39 31 31 30 34 33 32 41 37 32 32 45 33 45 42 33 9110432A722E3EB3
0000:0130 35 30 33 45 39 38 45 35 34 39 44 45 30 32 39 31 503E98E549DE0291
0000:0140 31 43 41 36 31 38 42 34 36 36 38 37 37 31 34 43 1CA618B46687714C
0000:0150 41 42 31 34 31 42 43 46 42 32 31 39 38 31 44 41 AB141BCFB21981DA
0000:0160 30 39 33 37 36 44 33 43 42 30 41 35 31 43 30 44 09376D3CB0A51C0D
0000:0170 43 34 35 44 43 30 46 38 34 42 33 33 30 43 34 46 C45DC0F84B330C4F
0000:0180 36 46 39 35 38 33 42 45 46 43 45 41 42 46 31 38 6F9583BEFCEABF18
0000:0190 38 41 42 32 41 38 39 39 45 38 41 45 31 37 34 36 8AB2A899E8AE1746
0000:01A0 32 46 34 37 43 42 41 37 46 39 44 41 45 38 30 42 2F47CBA7F9DAE80B
0000:01B0 46 31 31 35 33 37 44 31 31 37 37 44 30 37 32 39 F11537D1177D0729
0000:01C0 34 45 31 42 46 42 30 41 38 44 37 31 38 37 34 31 4E1BFB0A8D718741
0000:01D0 36 43 34 37 45 42 44 38 35 31 32 43 44 44 43 45 6C47EBD8512CDDCE
0000:01E0 30 44 38 45 30 42 31 32 30 46 39 35 35 32 34 33 0D8E0B120F955243
0000:01F0 41 38 42 44 30 30 32 37 37 30 37 33 36 37 44 30 A8BD0027707367D0
0000:0200 25 3C 61 36 DA BE C5 43 BE B1 33 A0 DF 90 CF E1 %<a6Ú¼ÃC¼±3 ß. Ĩá
0000:0210 FB 1F F5 CF 24 84 9B 89 00 21 DD 87 19 F7 F0 DA ú. ãİ$. . . . İÝ. cđÚ
Offset: 0000:0000 Selection: 0000:0000 - 0000:01FF (512 bytes) OVR

```

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:

#Afrodita Ransomware, appears to be a new strain.
Targeting businesses in Croatia via legitimate looking Excel spreadsheets.

Subject: "Poziv na placanje"

DZ: [http://content-delivery\[.\]in/verynice.jpg](http://content-delivery[.]in/verynice.jpg)

XLSM: 597ec6887f3bc5077939bdf1fb69f1

DLL: eba**cb**ff99234887d9f27719e48baf**e**59 pic.twitter.com/IM0h4fHUdT

— Check Point Research (@CPR**Research**) [December 3, 2019](#)

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@@.$0..
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@@....$0.....
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@@...$0.....
000A:9DD0 2E 3F 41 56 70 61 69 72 4E 6F 64 65 40 40 00 00 .?AVpairNode@@..
000A:9DE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9DF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000A:9E00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....
000A:9E10 58 00 00 80 18 00 00 80 00 00 00 00 00 00 00 00 X.....
000A:9E20 00 00 00 00 00 00 01 00 6B 00 00 00 30 00 00 80 .....k...0...
000A:9E30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
000A:9E40 00 20 00 00 48 00 00 00 70 10 0B 00 24 01 00 00 . .H...p...$...
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±.áÑĚ.Aª.\Ûæ.
000A:9EA0 FD D2 E7 31 B5 91 FC D8 97 40 19 8F D7 44 3B 9D ýòçlμ.ũö.@...xD; .
000A:9EB0 B1 BF E6 36 83 72 29 3E 78 60 E1 DB 3C FA 5D 8A ±¿æ6.r)>x`áú<ú].
000A:9EC0 F6 52 BF AC 4B 5C 83 E3 FD 57 41 E2 19 FF 38 DC öR¿-K\ .äýWAâ.ÿ8Û
000A:9ED0 8C 2E 37 1F 4F 74 9D 49 44 2D 3B 6A F4 40 FC 2E ..7.Ot.ID-;jô@ũ.
000A:9EE0 A7 AF 9E B3 9A 31 01 72 50 88 50 53 EA 65 63 97 §¯.³.l.rP.PSêec.
000A:9EF0 89 77 A2 AE 5B 67 42 76 FF 27 D2 E0 43 03 30 50 .w†@[gBvÿ'ôàC.OP
000A:9F00 46 7A 63 26 BD 00 9A 79 04 CD 11 83 E5 70 A8 62 Fzc&½..y.Î..âp"b
000A:9F10 DA D1 D3 AD 64 04 07 AB 5D 08 C1 C6 14 12 9E C3 ÚŃÓ.d.«].ÁÆ...Ă
000A:9F20 16 C4 4D 91 7B 17 2A DF CB 60 7F FB 33 5C F6 A8 .ĂM.{.*βĚ`.03\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 2ié¥.bh=X.ÎähPé
000A:9F50 BB 3A 19 9A 3A EF 9A CC F0 8F 06 31 DC F7 77 01 »:..:î.İð..1Û+w.
000A:9F60 2A C2 E7 C7 34 87 88 A4 45 37 87 1D D1 3B BE BA *ĂçÇ4...=E7..Ń;¼ª
000A:9F70 F7 A1 1A 5D 7E BF 70 8A D1 98 FE 9E BE 4E 7D E3 ÷j.]~¿p.Ń.þ.¼N}ă
000A:9F80 63 30 66 10 8F CD 2D D3 E0 2A 9C 34 24 CF 07 40 c0f..Î-ôà*.4$İ.@
000A:9F90 FF 02 01 11 00 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¥0ª0_0½0Ě0Đ0P0
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)
OBJECT IDENTIFIER (2 elem)
  1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
OIL
BIT STRING (1 elem)
SEQUENCE (2 elem)
  INTEGER (2048 bit) 25096615693731054222251480849593011269011075638654889785452933935645...
INTEGER 37

MIIBIDANBgkqhkiG9w0BAQEFAAOCAQAMIBCAKCAQEAs2+keHRYgZBupFc2+Z//dLnMbWR/NiXQBmP
10Q7nbG/5jaDcik+eGDh2zz6XYr2Ur+sS1yD4/1XQeIZ/zjcjC43H090nU1ELTtq9ED8LqevnrOaMQFy
UIhQU+p1Y5eJd6KuW2dCdv8n0uBDAzBQRnpjJr0AmnKzRGD5XCoYtrR061kBAerXQjBxhQSnsMwxE2R
excq38tgf/szXPaoSD1vsSmIwXbc3nTkadYPfjLu6aWwYmikWii3z+RoUOm70hma0u+azPCPBjHc93cB
KsLnzSHiKRFN4cd0Tu+uvehG11+v3CK0Zj+nr50feNjMGYQj80t0+AqnDQkzwdA/wIBEQ==

with hex dump  decode  clear  example
Browse...  test.key
```

-----BEGIN RSA PUBLIC KEY-----

```
MIIBIDANBgkqhkiG9w0BAQEFAAOCAQAMIBCAKCAQEAs2+keHRYgZBupFc2+Z//dLnMbWR/NiXQBmP
10Q7nbG/5jaDcik+eGDh2zz6XYr2Ur+sS1yD4/1XQeIZ/zjcjC43H090nU1ELTtq9ED8LqevnrOaMQFy
UIhQU+p1Y5eJd6KuW2dCdv8n0uBDAzBQRnpjJr0AmnKzRGD5XCoYtrR061kBAerXQjBxhQSnsMwxE2R
excq38tgf/szXPaoSD1vsSmIwXbc3nTkadYPfjLu6aWwYmikWii3z+RoUOm70hma0u+azPCPBjHc93cB
KsLnzSHiKRFN4cd0Tu+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
hxxps://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 we CAN decrypt!!

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

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

---