Not so nice after all - Afrodita Ransomware

dissectingmalwa.re/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

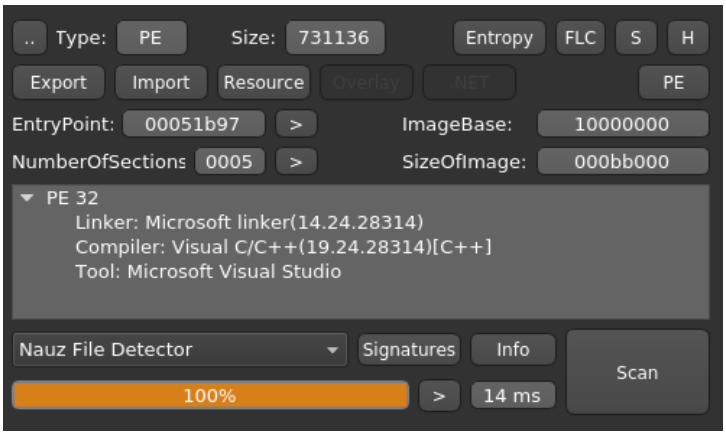
A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

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

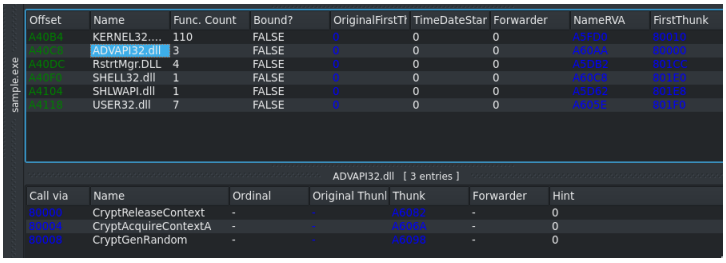
Afrodita uses a sleep routine for Sandbox evasion. In my Tests it took 30-60mins until the system was infected.

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.



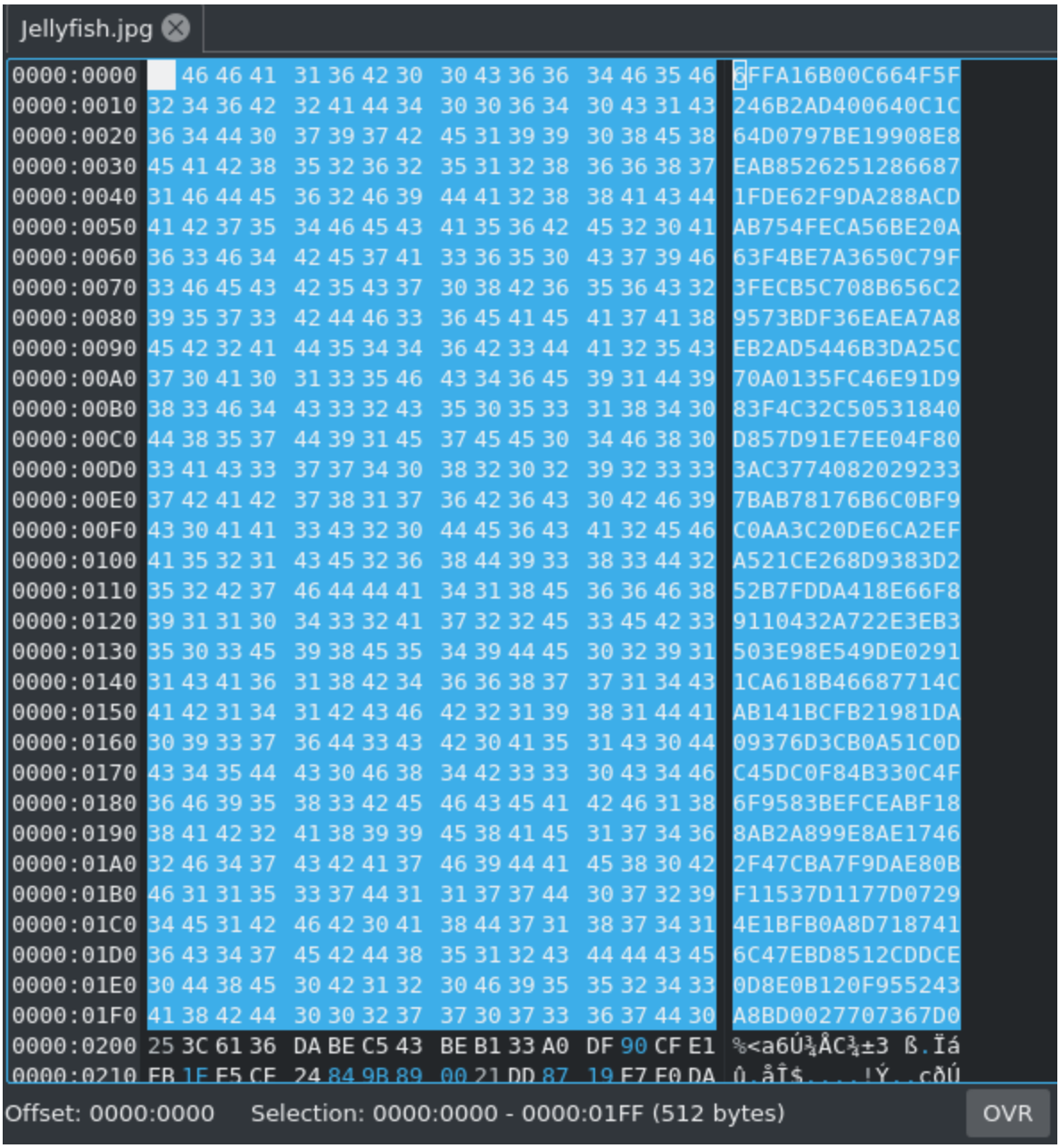
The extracted strings tell us quite a lot in this case. It looks like the internal name of the Project is *Afrodita* and it utilizes the CryptoPP Library. There are some references to .key files, but I haven't found a path or file on a infected machine yet. **README_RECOVERY .txt** is will be the filename 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, .ACCDB, .MDB, .PPTM, .PPTX, .PPT, .XLK,
.XLSB, .XLSM, .XLSX, .XLS, .WPS, .DOCM, .DOCX, .DOC, .ODB, .ODC, .ODM, .ODP, .ODS,
.ACCDR, .ACCDT, .ACCDE, .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.



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);
}
```

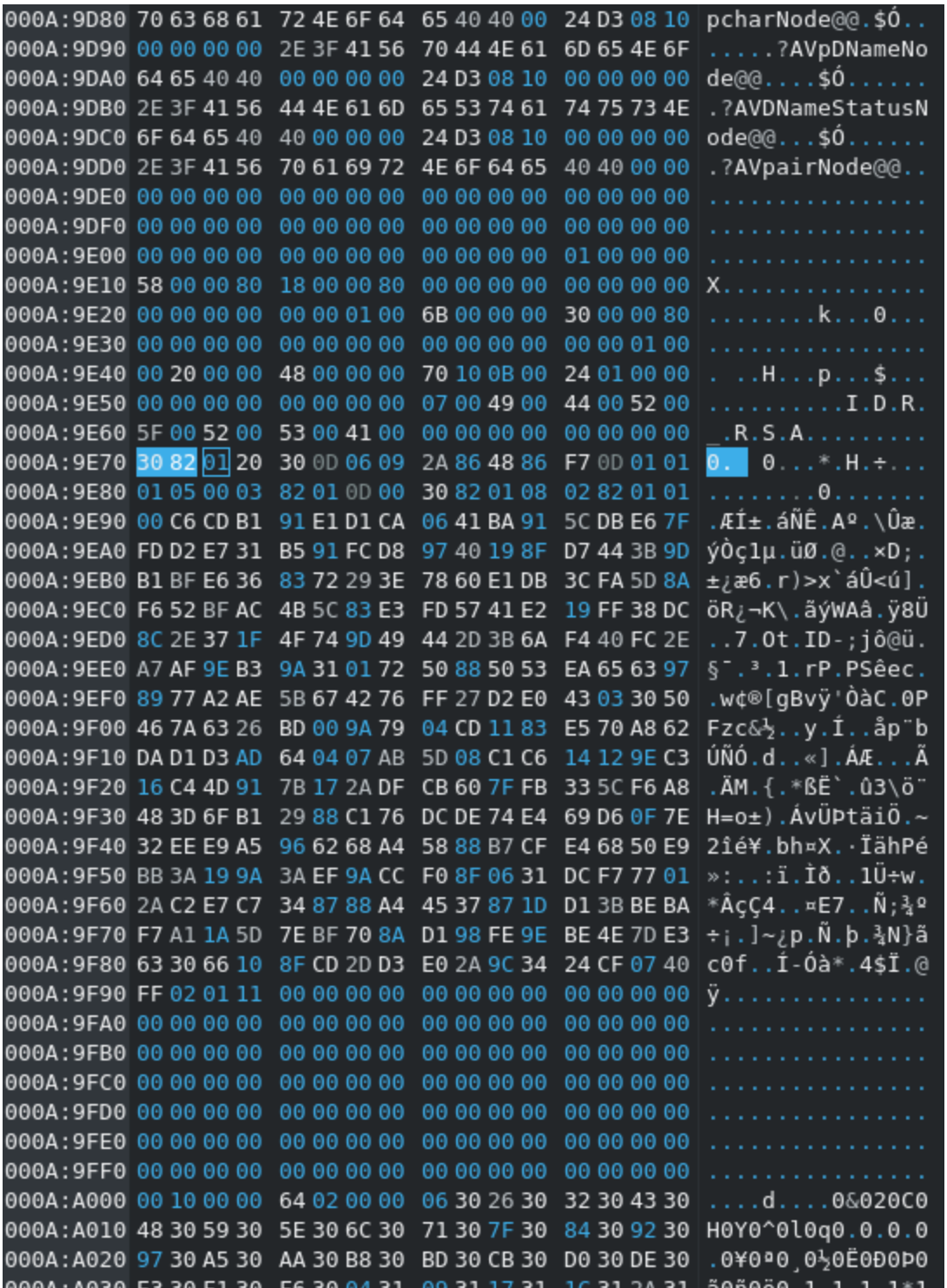
Update 10.01.2020:

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
> XLSM: 597ec6887f3bcdc5077939bdf1fb69f1
> DLL: ebacbff99234887d9f27719e48bafe59 pic.twitter.com/lM0h4fHUDT
>
> — Check Point Research (@*CPResearch*) 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@@.$Ó..
000A:9D90 00 00 00 00  2E 3F 41 56  70 44 4E 61  6D 65 4E 6F  .....?AVpDNameNo
000A:9DA0 64 65 40 40  00 00 00 00  24 D3 08 10  00 00 00 00  de@@....$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±.áÑÊ.Aº.\Ûæ.
000A:9EA0 FD D2 E7 31  B5 91 FC D8  97 40 19 8F  D7 44 3B 9D  ýÒç1µ.üØ.@..×D;.
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\.ãýWAâ.ÿ8Ü
000A:9ED0 8C 2E 37 1F  4F 74 9D 49  44 2D 3B 6A  F4 40 FC 2E  ..7.Ot.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  .w¢®[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..åp¨b
000A:9F10 DA D1 D3 AD  64 04 07 AB  5D 08 C1 C6  14 12 9E C3  ÚÑÓ.d..«].ÁÆ...Ã
000A:9F20 16 C4 4D 91  7B 17 2A DF  CB 60 7F FB  33 5C F6 A8  .ÄM.{.*ßË`.û3\ö¨
000A:9F30 48 3D 6F B1  29 88 C1 76  DC DE 74 E4  69 D6 0F 7E  H=o±).ÁvÜÞtäiÖ.~
000A:9F40 32 EE E9 A5  96 62 68 A4  58 88 B7 CF  E4 68 50 E9  2îé¥.bh¤X.·ÏähPé
000A:9F50 BB 3A 19 9A  3A EF 9A CC  F0 8F 06 31  DC F7 77 01  »:..:ï.Ìð..1Ü÷w.
000A:9F60 2A C2 E7 C7  34 87 88 A4  45 37 87 1D  D1 3B BE BA  *ÂçÇ4..¤E7..Ñ;¾º
000A:9F70 F7 A1 1A 5D  7E BF 70 8A  D1 98 FE 9E  BE 4E 7D E3  ÷¡.]~¿p.Ñ.þ.¾N}ã
000A:9F80 63 30 66 10  8F CD 2D D3  E0 2A 9C 34  24 CF 07 40  c0f..Í-Óà*.4$Ï.@
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¥0ª0¸0½0Ë0Ð0Þ0
000A:A030 E3 30 F1 30  F6 30 04 31  09 31 17 31  1C 31 2A 31  ã0ñ0ö0.1.1.1.1*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:


```
-----BEGIN RSA PUBLIC KEY-----
MIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEAxs2xkeHRygZBupFc2+Z//dLnMbWR/NiXQBmP
10Q7nbG/5jaDcik+eGDh2zz6XYr2Ur+sS1yD4/1XQeIZ/zjcjC43H090nUlELTtq9ED8LqevnrOaMQFy
UIhQU+plY5eJd6KuW2dCdv8n0uBDAzBQRnpjJr0AmnkEzRGD5XCoYtrR061kBAerXQjBxhQSnsMWxE2R
excq38tgf/szXPaoSD1vsSmIwXbc3nTkadYPfjLu6aWWYmikWIi3z+RoUOm7OhmaOu+azPCPBjHc93cB
KsLnxzSHiKRFN4cd0Tu+uvehGl1+v3CK0Zj+nr5OfeNjMGYQj80t0+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 cc: 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