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!

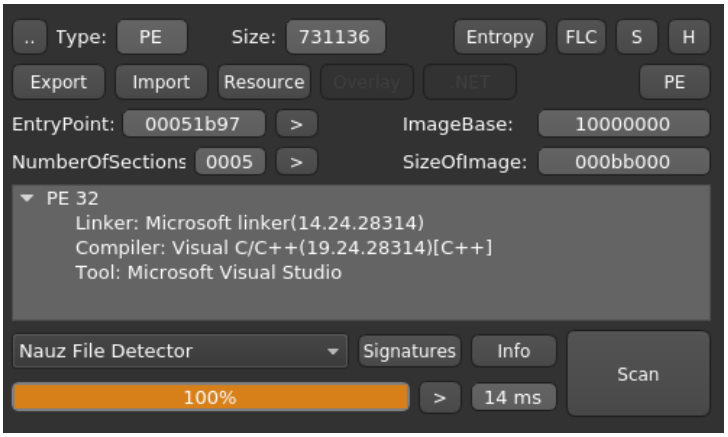
A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

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

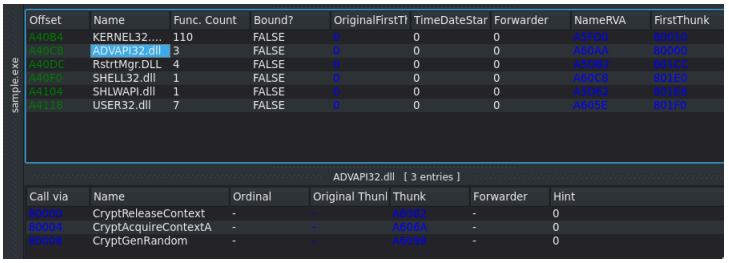
Afrodita uses a sleep routine for Sandbox evasion. In my Tests it took 30-60mins until the system was infected.

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.



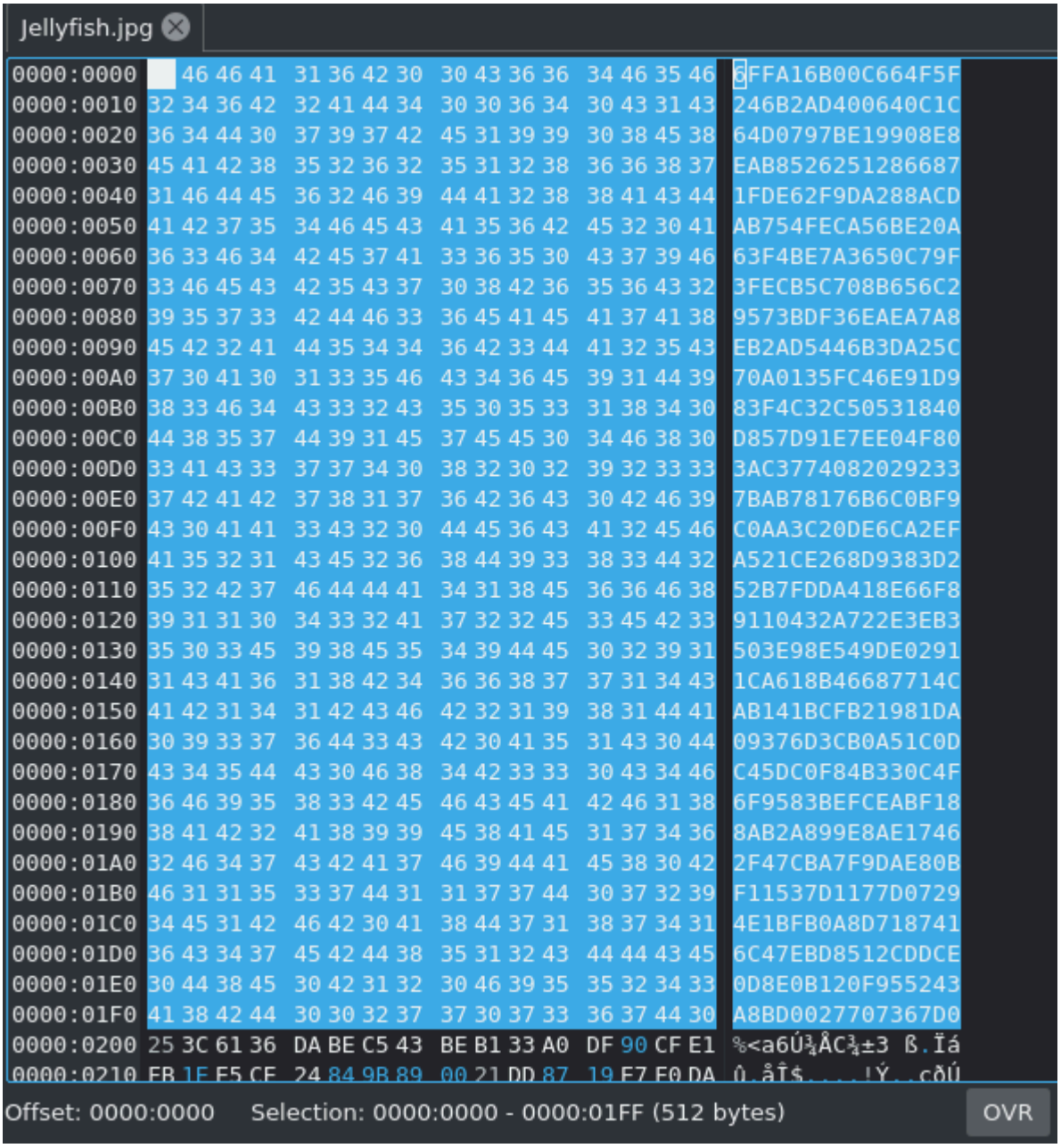
The extracted strings tell us quite a lot in this case. It looks like the internal name of the Project is *Afrodita* and it utilizes the CryptoPP Library. There are some references to .key files, but I haven't found a path or file on a infected machine yet. **README_RECOVERY .txt** is will be the filename 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, .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*

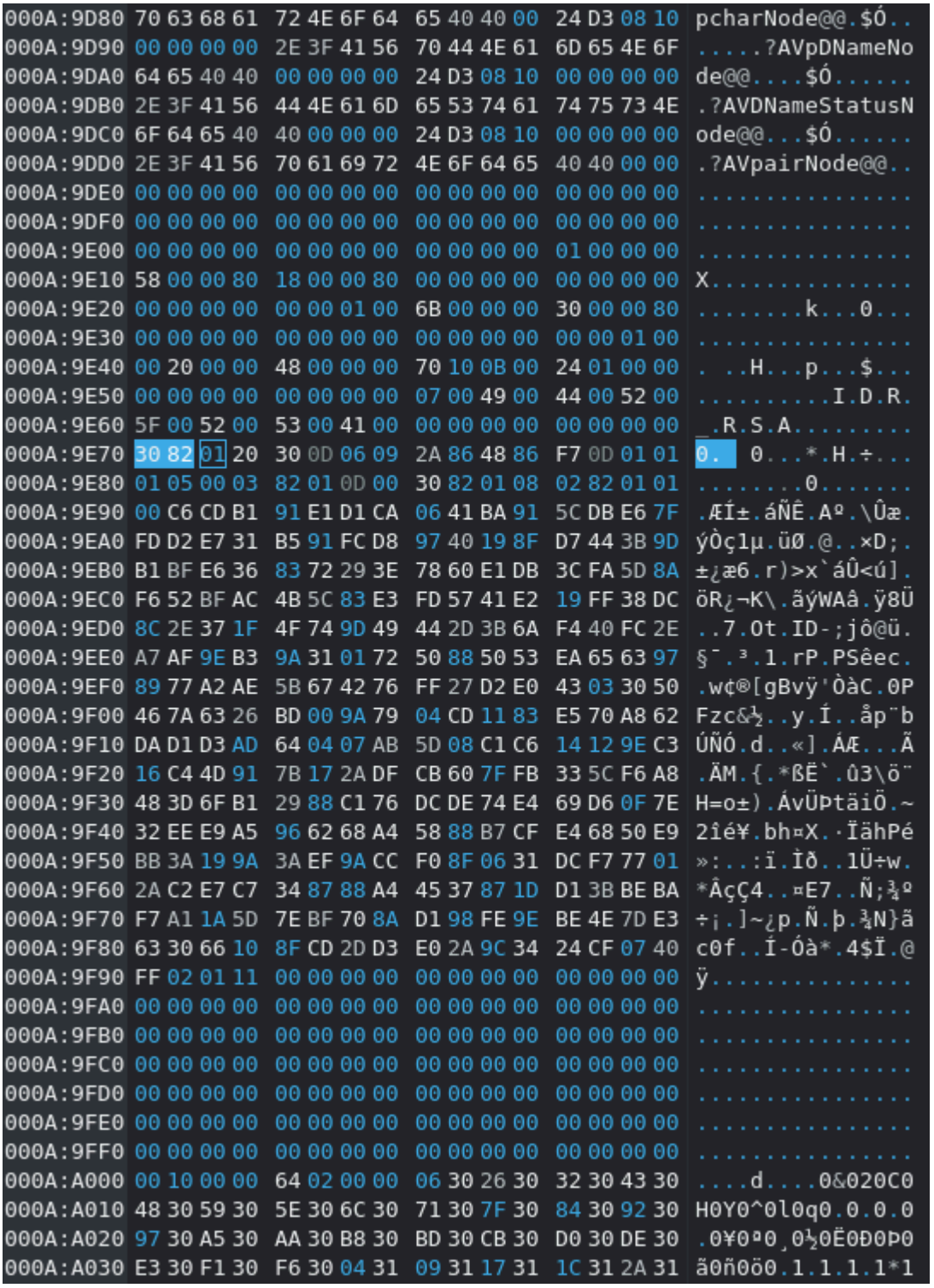
```
uint FUN_100151f0(void)

{
  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:



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
```

```
[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