Gamescom 2017: It's all fun and games until black hats step in

welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

August 22, 2017

ESET researchers have discovered a new sneaky malware threat named Joao, targeting gamers worldwide.

Tomáš Gardoň

22 Aug 2017 - 10:56AM

ESET researchers have discovered a new sneaky malware threat named Joao, targeting gamers worldwide.

ESET researchers have discovered a new sneaky malware threat named Joao, targeting gamers worldwide. Spread via hacked Aeria games offered on unofficial websites, the modular malware can download and install virtually any other malicious code on the victim's computer.

To spread their malware, the attackers behind Joao have misused massively-multiplayer online role-playing games (MMORPGs) originally published by Aeria Games. At the time of writing this article, the Joao downloader was being distributed via the anime-themed MMORPG Grand Fantasia offered on gf.ignitgames[.]to.

Our research has shown that several other Aeria games have been misused in the same way in the past, however, their corresponding unofficial websites have either gone inactive or had the malicious downloads removed in the meantime.

ESET blocks the website serving Joao malware and has informed Aeria Games about the matter.

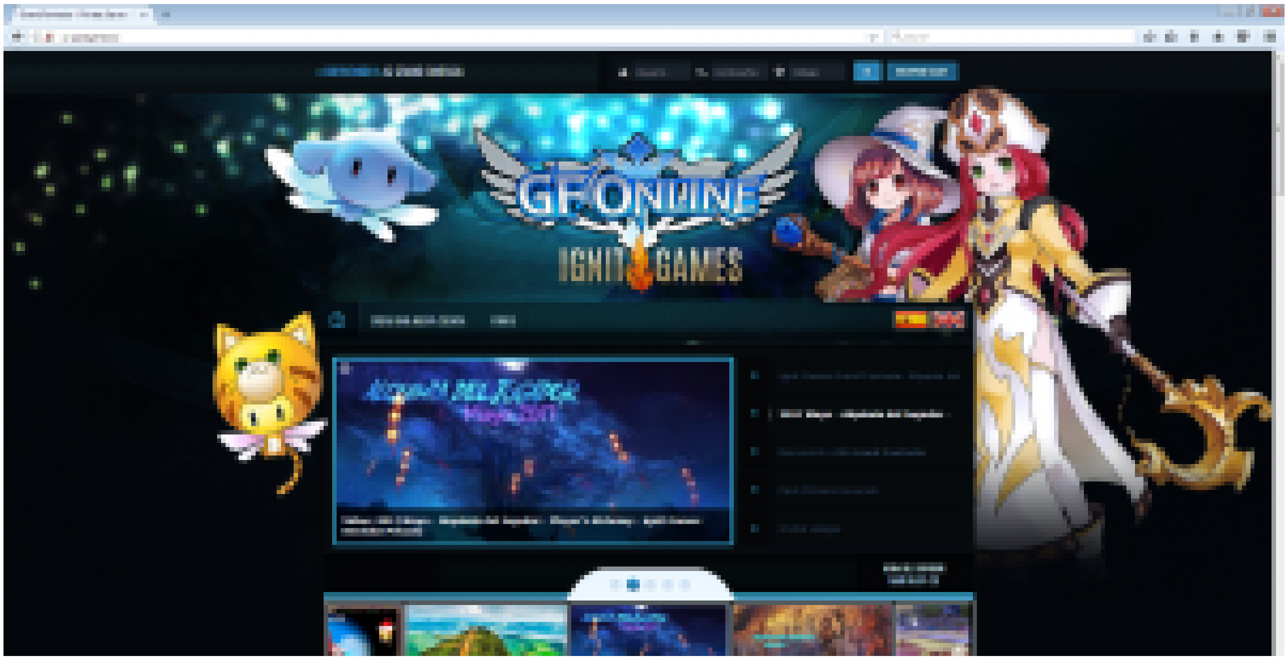

Figure 1: Infected version of Grand Fantasia as distributed via gf.ignitgames[.]to

How does it work?

The affected games have been modified to run Joao's main component – a malicious library mskdbe.dll, detected by ESET's systems as Win32/Joao.A. When users run the game launcher, Joao is launched along with it.

Upon launching, the Joao downloader first sends basic information about the infected computer – device name, OS version and information on user privileges – to the attacker's server because the malware keeps its operations "silent" and since the game works as expected, there's nothing suspicious about the whole infection process from the user's point of view.

Compared to downloading and launching a legitimate Aeria game, the only visible difference is an extra .dll file in the game's installation folder.

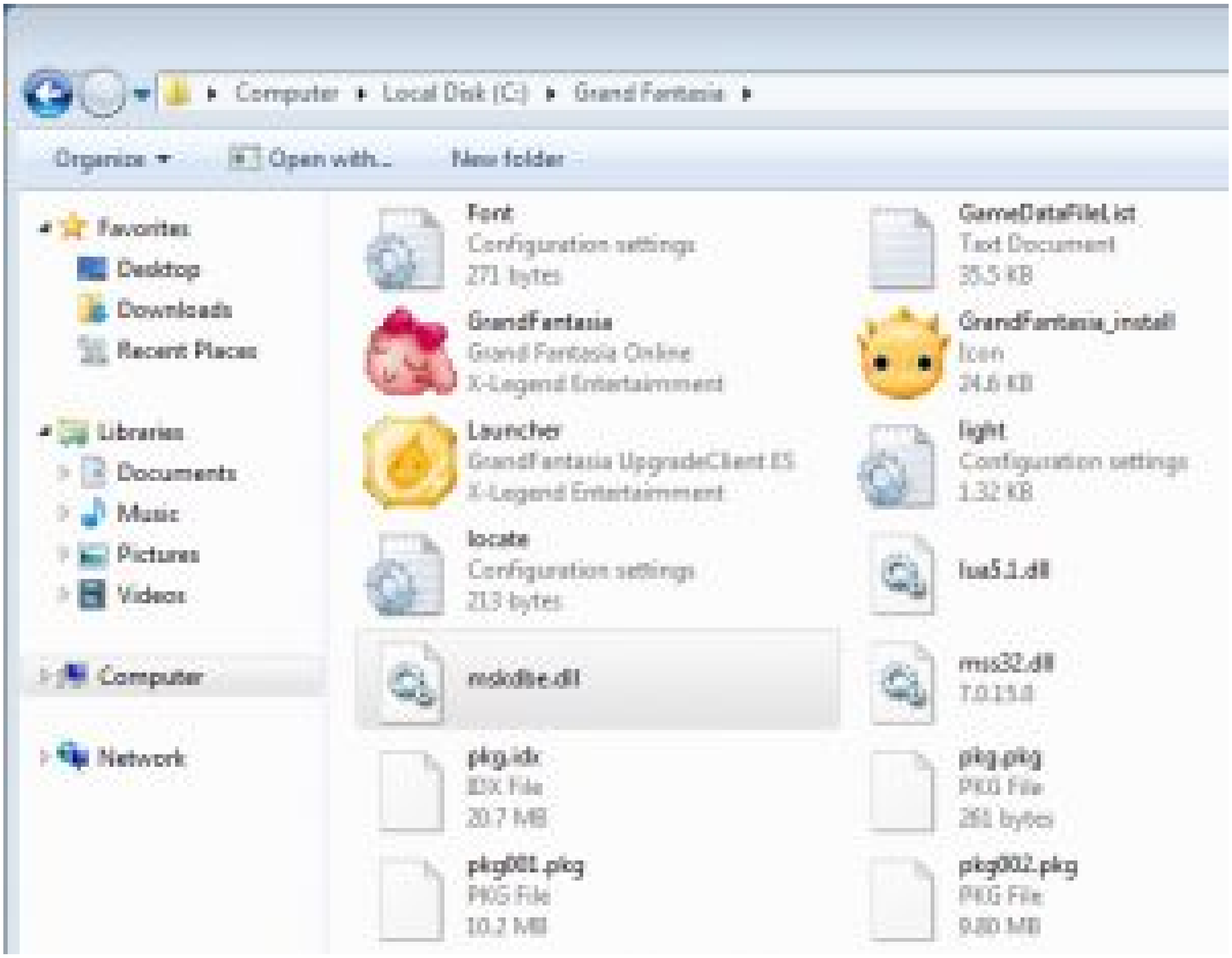

Figure 2: Joao downloader in the game's installation folder

After the communication with the server has been established, server-side logic decides whether and which components will be sent to the victim's computer. The Joao components we discovered during our research had backdoor, spying, and DDoS capabilities.

Has my computer been infected? How do I clean it?

Downloading lots of games from different sources and unsure if any of this applies to you? For a quick check of Joao's presence on your computer, you can try running a search for "mskdbe.dll" – if the search returns a result, your computer has most likely been infected with the Joao malware. If no such file is found, it doesn't automatically mean you haven't crossed paths with the malware – the crooks can rename the file at any moment.

Therefore, it's best to use a reliable security solution to detect the threat and remove it for you – you can also use ESET's Free Online Scanner.

How to stay safe?

With the gamescom fair underway, let's take a look at how you can enjoy gaming without being faced with threats.

- **Favor official sources whenever possible.** The MMORPGs targeted by these particular attackers are just a fraction of what might be lurking under download links on thousands of other unofficial websites and forums distributing games.
- **Keep your games updated.** Games, too, have vulnerabilities that can be exploited by malicious actors. Make sure you have all available patches applied.
- **Use a reliable security solution and keep it turned on while gaming.** At any point of your gaming experience, things might take a wrong turn – and you want to be prepared for that. Many security solutions today have a gamer mode option that lets you enjoy your games without interruptions while also keeping your computer protected.
- **Keep in mind that there are other threats targeting gamers**. Check out ESET's further security tips for gamers.

Additional information

ESET's systems have detected Joao all around the world. The following map shows which countries have been most affected:

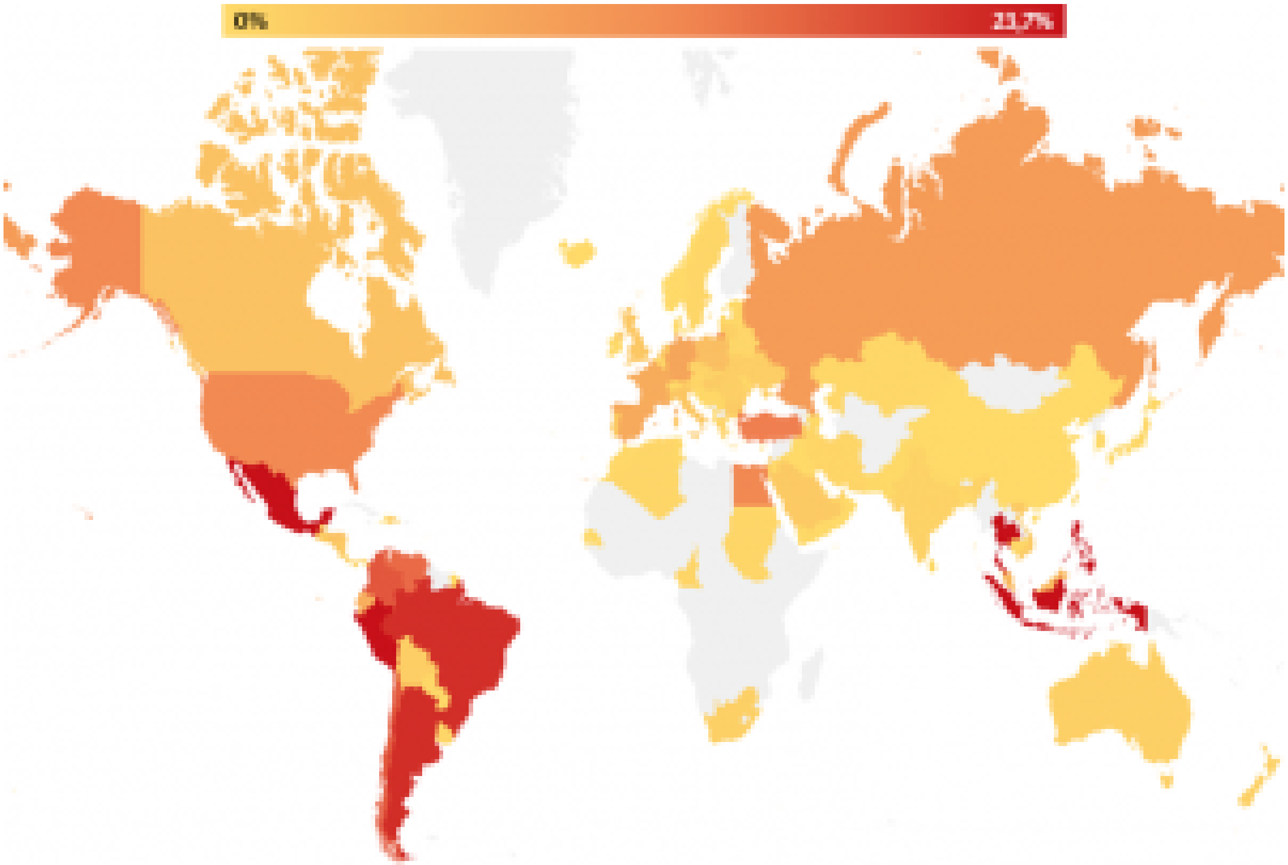

Figure 3: Joao detections distribution based on ESET's detection systems

IoCs

Joao downloader : mskdbe.dll – Win32/Joao.A

Hashes:

49505723d250cde39087fd85273f7d6a96b3c50d

d9fb94ac24295a2d439daa1f0bf4479420b32e34

4ede2c99cc174fc8b36a0e8fe6724b03cc7cb663

e44dbadcd7d8b768836c16a40fae7d712bfb60e2

b37f7a01c5a7e366bd2f4f0e7112bbb94e5ff589

fdbb398839c7b6692c1d72ac3fcd8ae837c52b47

5ab0b5403569b17d8006ef6819acc010ab36b2db

c3abd23d775c85f08662a00d945110bb46897c7c

00a0677e7f26c325265e9ec8d3e4c5038c3d461d

IoCs
c1b4c2696294df414cfc234ab50b2e209c724390
844f20d543d213352d533eb8042bd5d2aff4b7d4
2ce51e5e75d8ecc560e9c024cd74b7ec8233ff78
12a772e2092e974da5a1b6e008c570563e9acfe9
287c610e40aff6c6f37f1ad4d4e477cb728f7b1d
5303a6f8318c2c79c2188377edddbe163cd02572
6f17c3ab48f857669d99065904e85b198f2b83f5
51dfe50e675eea427192dcc7a900b00d10bb257a
ec976800cd25109771f09bbba24fca428b51563e
13e05e44d1311c5c15c32a4d21aa8eadf2106e96
0914913286c80428b2c6dec7aff4e0a9b51acf50
1e9c0a2a75db5b74a96dbfd61bcdda47335aaf8b
392b54c5a318b64f4fd3e9313b1a17eac36320e1
ba40012bdee8fc8f4ec06921e99bc4d566bba336
6d130e6301f4971069513266a1510a4729062f6d
beea9351853984e7426107c37bc0c7f40c5360e0
a34d6a462b7f176827257991ef9807b31679e781
ac86700c85a857c6d8c72cb0d34ebd9552351366
af079da9243eb7113f30146c258992b2b5ceb651
1e6125b9c4337b501c699f481debdfefea070583
a158f01199c6fd931f064b948c923118466c7384
350fc8286efdf8bcf4c92dc077088dd928439de9
2da8a51359bf3be8d17c19405c930848fe41bb04
Components:
JoaoShepherd.dll – Win32/Joao.B

IoCs
joaoDLL.dll – Win32/Joao.C
joaoInstaller.exe – Win32/Joao.D
JoaoShepherd.dll (x64) – Win64/Joao.B
joaoInstaller.exe (x64) – Win64/Joao.D
Hashes:
0d0eb06aab3452247650585f5d70fa8a7d81d968
f96b42fd652275d74f30c718cbcd009947aa681a
6154484d4acf83c21479e7f4d19aa33ae6cb716c
d338babd7173fa9bb9b1db9c9710308ece7da56e
ef2a21b204b357ca068fe2f663df958428636194
6b0e03e12070598825ac97767f9a7711aa6a7b91
28ca2d945731be2ff1db1f4c68c39f48b8e5ca98
d08120dd3fa82a5f117d91e324b2baf4cbbcaea5
f95aef3ca0c4bd2338ce851016dd05e2ee639c30
9b2d59a1aa7733c1a820cc94a8d5a6a5b4a5b586
ceb15c9fd15c844b65d280432491189cc50e7331
3331ac2aecfd434c591b83f3959fa8880141ab05
2ff2aadc9276592cbe2f2a07cf800da1b7c68581
3bceb54eb9dd2994b1232b596ee0b117d460af09
86617e92fc6b8625e8dec2a006f2194a35572d20
18a74078037b788f8be84d6e63ef5917cbafe418
4b0c1fcd43feab17ca8f856afebac63dedd3cd19
6bfa98f347b61d149bb2f8a2c9fd48829be697b6
7336e5255043841907e635b07e1e976d2ffb92b5
745396fedd66a807b55deee691c3fe70c5bc955d

IoCs
574f81b004cb9c6f14bf912e389eabd781fe8c90
d7751fc27efbc5a28d348851ce74f987d59b2d91
19bf7b5ad77c62c740267ea01928c729ca6d0762
ecc0ade237fa46a5b8f92ccc97316901a1eaba47
7075ffa5c8635fb4afeb7eea69a910e2f74080b3
47f68b6352243d1e03617d5e50948648f090dc32
7a4f05fc0906e3e1c5f2407daae2a73b638b73d9
b6d7da761084d4732e85fd33fb670d2e330687a2
ab69fb7c47e937620ab4af6aa7c36cf75f262e39
0e9e2dcf39dfe2436b220f13a18fdbce1270365d

22 Aug 2017 - 10:56AM

Newsletter

Discussion