

Forum:[Hack Forums](#)

Thread: [RELIABLE WORM FOR YOUR TASKS|ONLY PROVEND SOFTWARE|FULL VERSION](#)

HofmanoID11 - May 21, 2024, 9:12 am

[Download Link](#)

This worm is easy to use
Easy to encrypt
Easy to disguise
Easy to use
Flexible soft

Reviewed by staff : crypto miner

Bastille - May 22, 2024, 1:40 am

OP shared the following .zip file : Black_Worm_Generator.zip

MD5 : a0f144fe8f7aa2a9604e3cbaf87b7b73

SHA-1 : b0042438ddea82bbbfef3085d35c5dc9a524667d

[VT](#) Report

Composed of the following :

Appartheid :

Spoiler ([Click to View](#))

This has few similarities with a "Black Worm" [repo on Github](#) which was modified last time 6 years ago :

The .dll file is the same and is flagged as malicious (size / hash)

MD5 : 851ec9d84343fbd089520d420348a902

SHA-1 : f8e2a80130058e4db3cf569cf4297d07d05c93e0

[VirusTotal](#)

[Wikipedia](#) :

Blackworm is an Internet worm discovered on January 20, 2006 that infects several versions of Microsoft Windows. It is also known as Grew.a, Grew.b, Blackmal.e, Nyxem.e, Nyxem.d, Mywife.d, Tearec.a, CME-24, and Kama Sutra.

The old Github repo is probably a fake of the original BlackWorm that was discovered in 2006, this also has a "Decryptor" that is flagged as a stealer

and seems to "work" no matter what password you type :

Let's go back to our little naughty boy :

Black Worm Generator v3.5.exe was flagged as a crypto miner (monero) :

This malware runs so many things flagged as suspicious that I won't spend time describing each of them.

Here is the VirusTotal report, if you want to discuss about it because you're interested in malware analysis feel free to message

<https://www.virustotal.com/gui/file/6e785b074434cc4962019d4c2435199a72ec2f8c17f6b1375fcacbc4d7ce22fd/detection>

Here is the TRIA.GE report as well : <https://tria.ge/240521-tvvagsbe92/behavioral1>

TLDR; BlackWorm was a famous malware back in the 00's, it seems that many people try to release "new" versions of it that are fake, I've seen versions from 3.0 up to 6.0 on the Internet, people claiming that version 4.1 is the newest in 2022 while you can read on other forums that version 6.0 has been released in 2019 and is the latest, of course they were all fake.