



Forum: Sécurité

Topic: Bat To Exe Converter bien vérolé !

Subject: Bat To Exe Converter bien vérolé !

Publié par: Tof81

Contribution le : 10/07/2018 19:00:48

Je voudrais attirer l'attention sur la toute dernière version 3.0.10 portable 64 bits de ce soft : elle génère des .exe avec un max de cochonneries !!!

Merci Malwarebytes

A noter que Bat_To_Exe_Converter_(x64).exe donne 0/67 chez VirusTotal mais que Bat_To_Exe_Converter.exe donne 4/67 (probablement des faux positifs ?)

Je ne sais pour les versions antérieures car je ne viens de l'utiliser qu'il y a peu de temps.

Je vous joins un exemple. Vous verrez que le fichier batch ne contient que des commandes simples et de base DOS ...

Ne pas lancer le fichier .exe !!!

Mêmes résultats avec la version 32 bits.

PS : vu les virus je n'ai pas installé la version install pour faire des test ... !!!

Fichier(s) attaché(s):

HC.jpg (323.23 KB)



26 engines detected this file

SHA-256 e6679bcb88bbd3be1c0a11e9e18125c06bef4886f4d76dde879dbf8529a480a
 File name Logoff-64.exe
 File size 88.5 KB
 Last analysis 2018-07-10 16:46:50 UTC



26 / 67

Detection	Details	Community
Ad-Aware	Application.CoinMiner.AT	Arcabit Application.CoinMiner.AT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender Application.CoinMiner.AT
Bkav	W32.eHeur.Malware14	CrowdStrike Falcon malicious_confidence_60% (D)
Cybereason	malicious.db524d	Cylance Unsafe
Cyren	W32/Trojan.HHSX-2525	DrWeb Trojan.MulDrop8.23006
Emsisoft	Application.CoinMiner.AT (B)	Endgame malicious (high confidence)
eScan	Application.CoinMiner.AT	F-Prot W32/Trojan3.ALME
F-Secure	Application.CoinMiner.AT	GData Application.CoinMiner.AT
Jiangmin	Trojan.VB.aadq	Malwarebytes Trojan.Injector
MAX	malware (ai score=76)	McAfee-GW-Edition BehavesLike.Win32.Generic.mh
Rising	Malware.Heuristic!ET#100% (RDM+cmRtazrkDZKi4wGVw/AeSpNa...	Sophos ML heuristic
Symantec	ML.Attribute.HighConfidence	TACHYON Trojan-Dropper/W32.Scrop.90624
VBA32	Trojan.MulDrop	Zillya Tool.BadJoke.Win32.3497
AegisLab	Clean	AhnLab-V3 Clean

[test.zip](#) Taille: 48.04 KB; Hits: 452