Dec 2012 Batchwiper Samples

contagiodump.blogspot.com/2012/12/batchwiper-samples.html

Update: Jan 18, 2013 - Here is a nice analysis BatchWiper Analysis by Emanuele De Lucia
The next time the virus will wake up is Jan 21, 2013. Time to grab it, read and play.

Several people asked for Batchwiper, so here are the samples.

From Maher - Iranian CERT:

Latest investigation have been done by Maher center in cyber space identified a new targeted data wiping malware. Primitive analysis revealed that this malware wipes files on different drives in various predefined times. Despite its simplicity in design, the malware is efficient and can wipe disk partitions and user profile directories without being recognized by anti-virus software. However, it is not considered to be widely distributed. This targeted attack is simple in design and it is not any similarity to the other sophisticated targeted attacks. The identified components of this threat are listed in the following table:

Name	MD5
GrooveMonitor.exe [dropper]	f3dd76477e16e26571f8c64a7fd4a97b
juboot.exe	fa0b300e671f73b3b0f7f415ccbe9d41
jucheck.exe	c4cd216112cbc5b8c046934843c579f6
SLEEP.EXE	ea7ed6b50a9f7b31caeea372a327bd37
WmiPrv.exe	b7117b5d8281acd56648c9d08fadf630

File

Download. Email me if you need the password