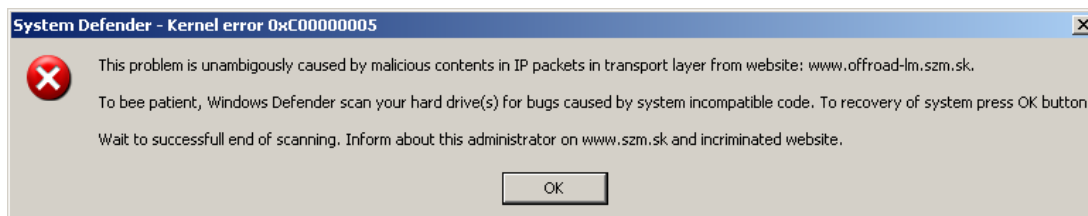




Na pohodu nov MBR črv Win32/Zimuse

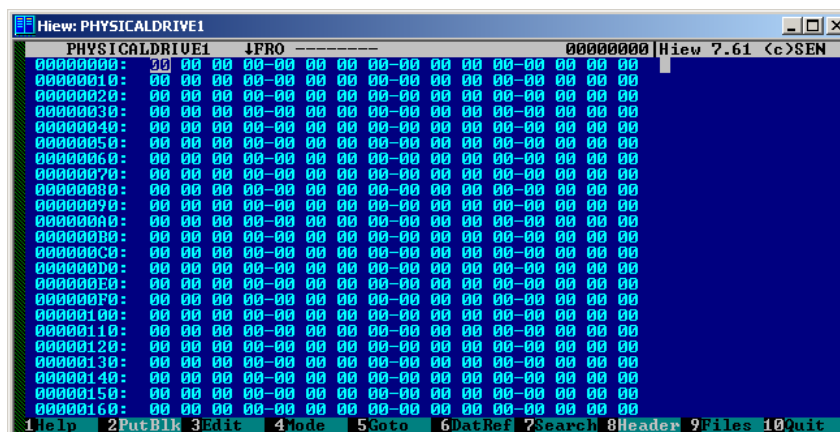
Nova Master Boot Record (MBR ali osnovni zagonski odsek) grožnja Win32/Zimuse izhaja iz centralne Slovaške. Na začetku je bila usmerjena na točno določen slovaški motociklistični off-road klub, danes pa poznamo že dve različici črva (Win32/Zimuse.a in Win32/Zimuse.B), ki sta se razširili tudi globalno. Grožnja na vseh pogonih računalnika prepíše osnovni zagonski odsek (MBR) s svojimi podatki in tako povzroči, da so podatki na računalniku nedostopni. Obnovitev teh podatkov je zahtevna in brez posebne programske opreme praktično nemogoča.

Ob izbruhu je bila grožnja večinoma prisotna le na Slovaškem, nekaj dni po tem pa je črv zelo dejaven tudi v ZDA, na Tajskem, v Španiji, Italiji, na Češkem in ostalih evropskih državah.



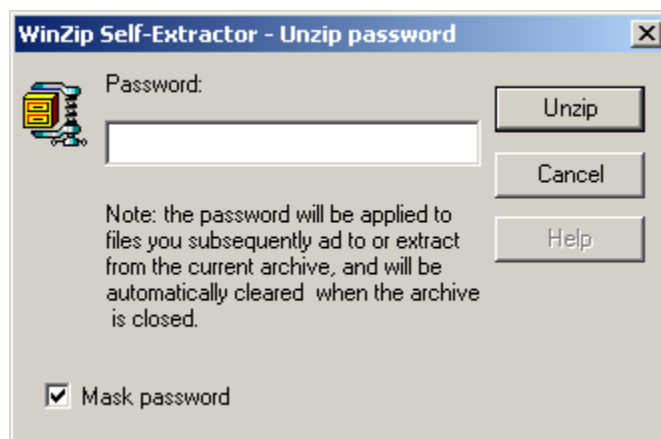
Črv za širjenje uporablja dve metodi - lahko je na spletne strani pripet kot samoraztezni ZIP arhiv ali kot program za testiranje IQ koeficienta, širi pa se tudi preko izmenljivih USB medijev kot so recimo USB ključki.

Črv Win32/Zimuse prvih 50Kb trdega diska prepíše z ničlami:



Omenjeni različici črva - Win32/Zimuse.a in Win32/Zimuse.B se razlikujeta po metodi širjenja in času, ki ga potrebujeta za izvršitev. Različica črva A za širjenje preko USB naprav potrebuje 10 dni, različica B pa le 7. Tudi čas, ko se škodljiva koda izvrši je v različici B skrajšan iz 40 na 20 dni.

Zanimivo je tudi dejstvo, da v kolikor za odstranjevanje grožnje ne uporabite prave metode, črv na računalniku svoje izvrševanje prične takoj. Podobno kot, če pri deaktiviranju bombe prerežete napačno žico.



Zelo verjetno je, da je bil črv ustvarjen z namenom, da bi ga poslali članom motociklističnega kluba v slovaški pokrajini Liptov, dejstvo pa je, da se je, potem, ko je okužil tudi nekatera omrežja podjetij, razširil tudi globalno. Črv močno na spominja na drugega MBR črva, ki je tudi izhajal iz Slovaške – OneHalf.

Črv nima naprednih sposobnosti, da bi podatke na trdih diskih tudi zakodiral, ustvarjen je bil le z namenom, da prepíše MBR na vseh trdih diskih. Grožnje iz preteklosti posnema tudi v tem, da potrebuje čas, da se sproži oz. izvrši – v tem primeru 20 ali 40 dni.

Uporabniki rešitev ESET Smart Security in ESET NOD32 Antivirus ste pred to grožnjo varni, ESET je za črva Win32/Zimuse pripravil tudi posebno odstranjevalno orodje.

ESET

Podjetje je bilo ustanovljeno leta 1992 in je že od samega nastanka usmerjeno v razvoj varnostnih rešitev. ESETovi produkti so že od vsega začetka ocenjeni kot eni od najboljših protivirusnih rešitev na trgu. Zaradi svoje tehnološke dovršenosti so bili že večkrat nagrajeni kot najučinkovitejši, najnatančnejši in najhitrejši protivirusni programi. Podjetje ima sedež v Bratislavi, svoje pisarne pa imajo še v Bristolu, Buenos Airesu, Pragi, San Diegu, s svojimi partnerji pa so prisotni v več kot 100 državah po celem svetu.

www.eset.si

SI SPLET

SI SPLET d.o.o. je podjetje, ki se ukvarja s trženjem varnostnih in drugih rešitev na področju informacijskih tehnologij. V letu 2002 si je podjetje pridobilo ekskluzivno partnerstvo s podjetjem ESET za distribucijo varnostnih rešitev ESET v Sloveniji.

www.sisplet.com