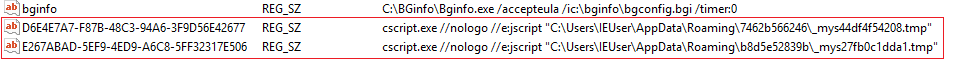
# "Filler" malware IOCs

"Filler" is malware met als doel een computer te vullen met "garbage" bestanden. Door enorm veel bestanden aan te maken raakt het filesystem zo vervuild dat normale gebruik van de computer ernstig wordt beperkt.

## Werking

Bij lancering van Filler wordt de malware gekopieerd naar tenminste 25 verschillende locaties. Deze locaties zijn willekeurig gekozen, maar de bestandsnaam van de kopie begint altijd met de karakters "\_mys" en hebben de extensie ".tmp".

Voor elk van deze nieuwe locaties wordt een Run-key aangemaakt in het Register (in *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*). Dit heeft tot doel dat elke keer dat de computer wordt herstart, het script opnieuw gedraaid wordt. De key van de key/value pair in het Register is een willekeurige string, maar de value heeft altijd de volgende structuur:  
**cscript.exe //nologo //e:jscript "<bestandspad>"**

****

Figuur - Register key/value-pair

Ook schrijft Filler een waarde weg in het Register op locatie *HKLM\Software\LegitCorp\Version.* Het is niet duidelijk waar deze waarde toe dient, daar deze altijd **0x19** lijkt te zijn.

Nadat Filler zichzelf heeft gekopieerd naar diverse locaties, worden deze locaties ook aangeroepen om te draaien. Op deze manier zorgt Filler ervoor veel verschillende taken te verdelen over de verschillende processen. Filler lijkt 4 verschillende taken te kunnen uitvoeren:

* Aanmaken van veel bestanden op verschillende locaties
* Aanmaken van snelkoppelingen naar bestanden op verschillende locaties
* Scannen op lokaal netwerk naar online machines
* Scannen op internet naar voorgedefinieerde IP adressen

Het is niet duidelijk of Filler iets doet met de opgedane kennis bij het scannen naar andere machines.

# IOCs Filler

SHA256-hash: ec1dc949b0f37429343ad40b1a09607e5e45fe7376fea9373c29b65894a36d77

Registry:

* Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
* Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\LegitCorp\Version

Bestandsnamen:

* Filler.js (orgineel)
* \_mys<willekeurige karakters>.tmp (kopieën)