

Forum: [Hack Forums](#)

Thread: [Analyze the file](#)

m4dh4ck3r - November 28, 2016, 3:08 am

Found this in my startup.

<https://a.pomf.cat/sqotep.exe>

Help me find out what malware it is :\

VirusTotal

<https://virustotal.com/en/file/2da63827ad1449ca5f2888adfa9645f1eaf8b39d26ec214441ee80f3a56e6e72/analysis/1480329595/>

Malwr :

<https://malwr.com/analysis/ZTMyYWNmMTVkJBkNGMwNTkwZGIzOTg2NjU0MTZINzE/>

GruntStyl - November 28, 2016, 7:21 am

It looks to be a false positive. Seems to be a Bing service by Microsoft. I'll throw it in a VM and see what I can find. But you seem to be in the clear.

EDIT: Yes you are 100% safe. It is just a bing service file. Tested in VM/Sandbox. No malicious behavior was taking place. More then likely was using it as an update service.

JoshuTee - November 28, 2016, 2:14 pm

It's a Bing process file, nothing harmful. But why is it in your startup? Did you install any programs lately?

Shaggy - November 29, 2016, 12:01 pm

Website is currently blacklisted by McAfee Siteadvisor!
others are clear

Aura - November 29, 2016, 6:01 pm

(Nov 29, 2016 01:01 PM)czzyllle Wrote: [\[CITE\]](#) Website is currently blacklisted by McAfee Siteadvisor!

others are clear

This is because there's a shitload of malicious downloads hosted on pomf.cat.

LogoiLab - December 1, 2016, 6:36 am

The file is signed by Microsoft.