ETERNALBLUE vs Internet Security Suites and nextgen protections

Due to the recent #wannacry ransomware events, we initiated a quick test in our lab.

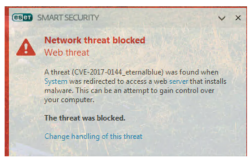
Most vendors claim to protect against the WannaDecrypt ransomware, and some even claims they protect against ETERNALBLUE exploit (MS17-010).

Unfortunately, our tests shows otherwise. Warning: We only tested the exploit and the backdoor, but not the payload (Wannacry)!

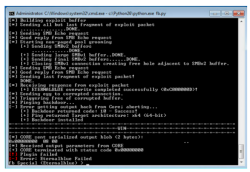
We don't want to disclose our test results until a fair amount of time is given to vendors to patch their product, but meanwhile we feel that we have to inform the public about the risks.

The following 3 products protected the system against the ETERNALBLUE exploit installing the DOUBLEPULSAR backdoor:

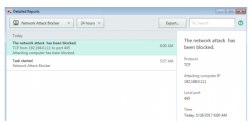
1. ESET Smart Security
2. F-Secure SAFE – but no log/alert on the console
3. Kaspersky Internet Security



ESET Smart Security Blocking ETERNALBLUE



FSecure SAFE blocking ETERNALBLUE

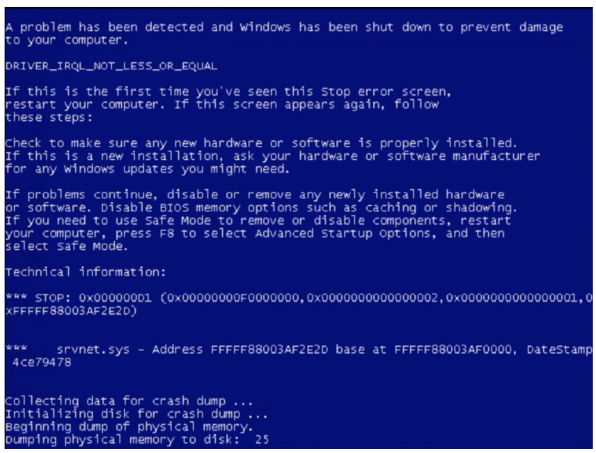


Kaspersky Internet Security protecting against ETERNALBLUE

Two product used network filtering to detect the exploit, and block it before kernel code level execution happens. We have not played with how these techniques can be bypassed (e.g. via obfuscating the exploit to bypass signatures), but that could be the content of another blog post.

The BSOD

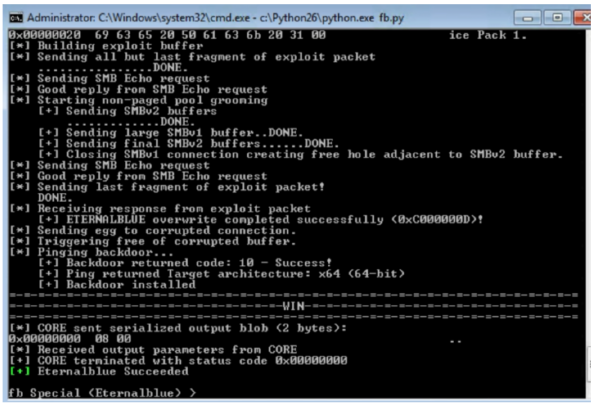
So far, we have one endpoint protection product where DOUBLEPULSAR installation failed due to Blue Screen of Death. Point 1 for integrity (hopefully) and -1 point for availability.



The FAILS

At the moment, we have tested **9 home Internet Security Suite products, 1 Next-gen endpoint protection and 1 EDR which can't protect (or alert) users** against ETERNALBLUE exploit installing

the DOUBLEPULSAR backdoor. All vendors claim to protect against #Wannacry and some claim to protect against ETERNALBLUE. But here is the thing, protecting against the payload does not mean users are fully protected against malicious code running in kernel mode.



Our focus of test were mostly home products (internet security suites), and whenever the default firewall policy was set to public, we changed the policy to home/work. All products were used with default settings. Some products for example have intrusion prevention turned off by default – and enabling it blocks ETERNALBLUE. But not many home users tweak default settings.

Conclusion

It is nice that all the AV vendors claim to protect against the ransomware payload, but in case there is a backdoor running on your machine in the kernel level, things are not that great.

Please note the ETERNALBLUE exploit was published basically 2 months before Wannacry and this blog post.

If anyone creates an in-memory ransomware which can work with the ETERNALBLUE exploit, the number of ransomwared systems would skyrocket. ETERNALBLUE can be linked with Meterpreter easily, and we have an in-memory Meterpreter ransomware extension. We are sure we are not the only ones having this capability ... If there will be an in-memory Meterpreter ransomware in-the-wild soon, we reserve the right to remove this section from the blogpost, and pretend we never wrote this 😉

We are in the middle of contacting all AV vendors about the issue. Although we guess they already know this, they only forgot to notify the marketing department to check their communication.