What are “WannaMine” attacks, and how do I avoid them?

nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/

By Paul Ducklin 31 Jan 2018

There’s a hot security news topic right now that combines the ETERNALBLUE exploit and cryptomining.

ETERNALBLUE is infamous for having been used in the WannaCry worm, so the combination of this method of breaking in, followed by a cryptomining payload, has been dubbed **WannaMine**.

WannaMine attacks aren’t new, but our Support team has recently had a surge in the number of enquiries from people asking for advice about the issue.

Support therefore asked us if we’d make a Facebook Live video about it…and here it is.

(We’ve also included a Questions and Answers section below, based on the video.)

(Can’t see the video directly above this line, or getting an error such as “no longer available”? Watch on Facebook instead.)

Note. With most browsers, you don’t need a Facebook account to watch the video, and if you do have an account you don’t need to be logged in. If you can’t hear the sound, try clicking on the speaker icon in the bottom right corner of the video player to unmute.

QUESTIONS AND ANSWERS FROM THE VIDEO

Q. Is WannaMine like WannaCry? Is it ransomware that scrambles my disk?

A. The name “WannaMine” is a portmanteau word that refers to a malware family that uses the network spreading capabilities of *Wanna*Cry to deliver crypto*mining* malware rather than ransomware.

Q. What is cryptomining malware? Is it as dangerous as ransomware?

A. Cryptomining is when crooks secretly get your computer to do the calculations needed to generate cryptocurrency, such as Bitcoin, Monero or Ethereum; the crooks keep any cryptocoin proceeds for themselves.

To make money with cryptomining, you need a lot of electricity to deliver a lot processing power on a lot of computers.

By illegally installing cryptominers inside your network, the crooks therefore steal your resources to do their work.

Q. Can cryptomining damage my computer?

A. We’ve seen stories of mobile phone batteries bulging due to overheating when the device was deliberately forced to do mining calculations for hours on end.

However, WannaMine doesn’t run on mobile phones – it attacks Windows computers.

Nevertheless, even if no permanent damage is done, you’ll probably find your laptop batteries draining much faster than usual, your fans running flat out, and your laptop being noticeably hotter than usual.

Also, if malware like WannaMine can penetrate your network, you are at serious risk of other malware at the same time, including ransomware.

We frequently see evidence of cryptomining left behind on computers that were zapped by ransomware, so don’t ignore WannaMine infections if they show up – where one crooks goes, others will surely follow.

Q. If I don’t own any cryptocoins and I’m not part of the cryptocurrency scene, am I still at risk?

A. Yes.

WannaMine malware attacks aren’t trying to locate your digital cryptocurrency stash and steal it.

They want free use of your computer for cryptomining calculations of their own, whether you’re interested in cryptocurrency or not.

Q. Can security software prevent WannaMine attacks?

A. Yes.

Exploit prevention software (e.g. **Sophos Intercept X**) can block the ETERNALBLUE attack to prevent malware like this from entering your network in the first place.

Anti-virus and host intrusion prevention software (e.g. **Sophos Endpoint Protection**) can stop the malicious processes that allow the WannaMine attack to proceed, even if the exploit triggers at te start.

Network security software (e.g. **Sophos XG Firewall**) can block the network activity required for malware like WannaMine to work.

Q. What else can I do?

A. Patch promptly, and pick proper passwords.

WannaMine malware typically includes the same ETERNALBLUE exploit that was abused by WannaCry and allowed it to spread.

This exploit was patched last year in Microsoft update MS17-010, so a properly patched network wouldn't be open to the exploit in the first place.

If the ETERNALBLUE hole is already closed, WannaMine can try to spread using password cracking tools to find weak passwords on your network.

It only takes one user with poor password hygiene to put your whole network at risk.