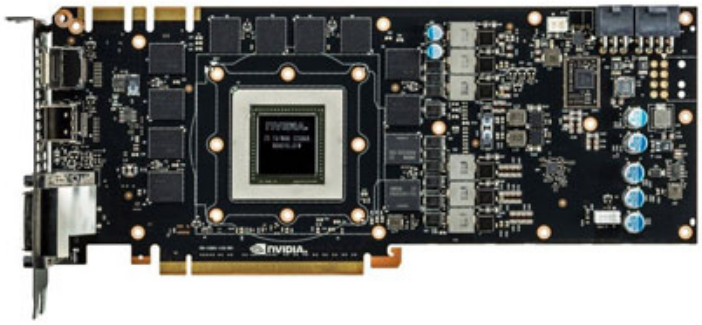
Appeared super risk of computer underground GPU exploitation

Graphics processing chips (GPUs) are known to have much higher computing power than the main processor chips (CPUs). If used for good purposes, the GPU will be very beneficial. But if bad guys take advantage of GPU, the consequences will be very unpredictable.

Graphics processing chips (GPUs) are known to have much higher computing power than the main processor chips (CPUs). If used for good purposes, the GPU will be very beneficial. But if bad guys take advantage of GPU, the consequences will be very unpredictable.

Rombertik malware appears to attack hard drive and delete MBR

Like many other programs (*applications*), the virus is essentially a software and its " *destructive* " capability is also dependent on the power of computer hardware, which has relied on CPU for many years. But with technology development, CPUs are no longer the most powerful chip a machine can own. If your computer is equipped with a GPU (*or graphics card*), it is likely that its computing power (*measured by FLOPS*) will be higher than the current CPU.



A NVIDIA graphics card

In fact, taking advantage of GPU for " *non-transparent* " purposes has existed for a long time. For example, unlock the phone, break the login password, break the Wi-Fi password . mainly based on the GPU. However, the above programs run on hacker / cracker computers, not users and are basically not dangerous by viruses. But a recently published tool shows the threat of viruses running on GPUs completely.

A group of application developers called Jellyfish has released a set of rootkits (*a software that runs in the background*) and a keylogger (*keyboard monitoring software*) that runs on Linux, with a remote access tool (RAT) available. for Windows. These programs are in common, based on the OpenCL programming interface,

an interface that allows applications to exploit both the power of CPU and GPU. The generation of chips released in recent years by AMD, Intel and NVIDIA mostly supports OpenCL.

The danger is that ANTIVIRUS has not detected malicious code running on the GPU

But the most dangerous thing about these malware (malware) is that antivirus (antivirus) programs are currently unable to identify them if they are running on the GPU. Most antivirus only recognize malicious code when they run on the CPU. Therefore, although the programs that Jellyfish wrote are only for the purpose of raising people's vigilance. But it is possible that there have been many viruses based on GPUs that have been launched and are " *launching themselves* " on users' computers even though they have built-in antivirus.

Not long ago, ?Torrent users had trouble installing the EpicScale application to plow " *virtual money* " Bitcoin. The case was discovered and quickly resolved. But if this happened once, we are not sure whether it will happen until Monday or Tuesday. Because the number of new viruses is still constantly born and because there are always bad people who want to take advantage of your computer or smartphone.

You finished reading the article "**Appeared super risk of computer underground GPU exploitation**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.