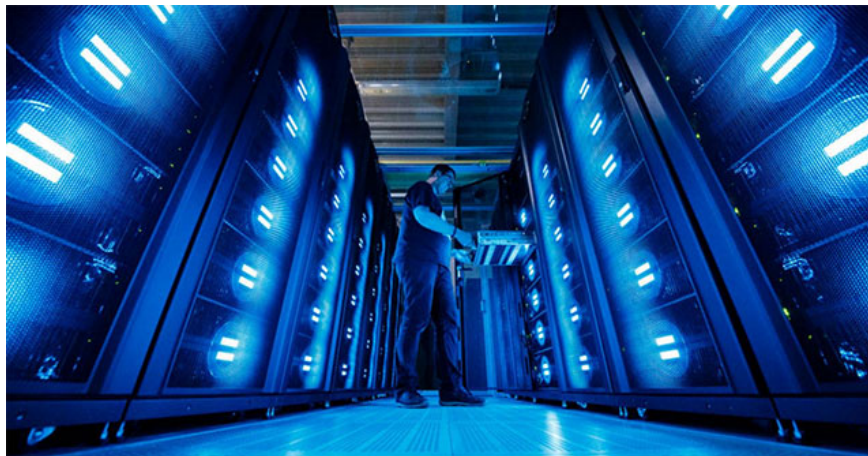


Supercomputers can completely detect cyber threats

As governments, businesses and individual users increasingly trust and use the internet for their daily activities, maintaining cybersecurity will still be an essential task for researchers, as well as security experts worldwide.

Identifying network security threats from raw internet data can be like 'digging a bottom needle'. Just by taking the example of the amount of internet traffic data generated during the 48-hour period, this number was too big for one or even the 100 most powerful laptops today in processing. data into something 'easy to digest' for our meat-based security analysts. That's why analysts have to rely on sampling to look for potential threats, then choose small data segments to look more intensively in the hope of finding worthwhile behavior. Surprise.

Although this type of sampling is applicable to some tasks, such as identifying common IP addresses, in general, in search of sophisticated threat trends, this method proved too limited.



1. Used since the 1990s, nearly 30-year-old 'supercomputers' are still running 'ferry ferries' and play an important role in many countries.

"If you are trying to detect an anomalous behavior, then by that definition, it is a very rare and unlikely behavior in practice, but it also applies a traditional sampling screening. The result is almost zero," said Vijay Gadepally, a senior employee at the supercomputing center of Lincoln Laboratory (LLSC).

Vijay Gadepally is one of Lincoln's leading research lab experts, who believes that supercomputers can provide a better way to screen and identify potential cyber threats. . It may be a way to allow analysts to access all the appropriate data at once to identify and analyze these highly discernible differences.

In a recently published article, Vijay Gadepally's team successfully localized and 'isolated' data stored about 96 hours of raw internet traffic into a data packet that could be readily accessed. problem. More specifically, they created this data packet by using 30,000 processing cores (equivalent to the power of about 1,000 laptops) at

LLSC Laboratories in Holyoke, Massachusetts, USA, and data Data was stored in MIT SuperCloud - anyone with an account can access it.

"[Our research] shows that we can fully utilize supercomputing resources to collect, analyze and pack huge amounts of data, and put it in a situation where a home Network security research may need to be used," explained Gadepally.



1. The most powerful supercomputer today, has 1 million processing cores, equal to 1% of human brain power

An example of the type of potential threatening activity requires analysts to exploit huge amounts of data to screen and identify those that are instructions from command and control servers (C&C). These servers often tell devices that are infected with malware to steal or manipulate data.

In addition, Vijay Gadepally also compared the pattern of command and control server behavior with those who call spam. Usually a normal caller can make and receive relatively equal number of calls, but spammers will make more calls than they receive. That's the same idea found on C&C servers, and this can only be found by looking at a huge amount of data over a long period of time.

The team is currently planning to spread more about the ability to compress such a large amount of data on supercomputers, and they hope analysts will take advantage of this resource to take the next step in Detects and suppresses cyber threats in a more efficient way. In addition, the team is working on ways to better understand what "normal" internet behavior looks like, to identify threats more easily.



1. What's special about supercomputers that survived 1 year on ISS International Space Station?

"The effectiveness of detecting threats on the network can be significantly enhanced by using an accurate aggregate model of normal network traffic based on supercomputer capabilities. And analysts can compare the internet traffic data they are studying with these models to find unusual behavior much easier," said Lincoln Laboratory member Jeremy Kepner. At LLSC, the person responsible for the new study said.

As governments, businesses and individual users increasingly trust and use the internet for their daily activities, maintaining cybersecurity will still be an essential task for researchers, as well as security experts worldwide. Meanwhile, supercomputers are a huge potential resource but have not been exploited yet.

You finished reading the article "**Supercomputers can completely detect cyber threats**" 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.