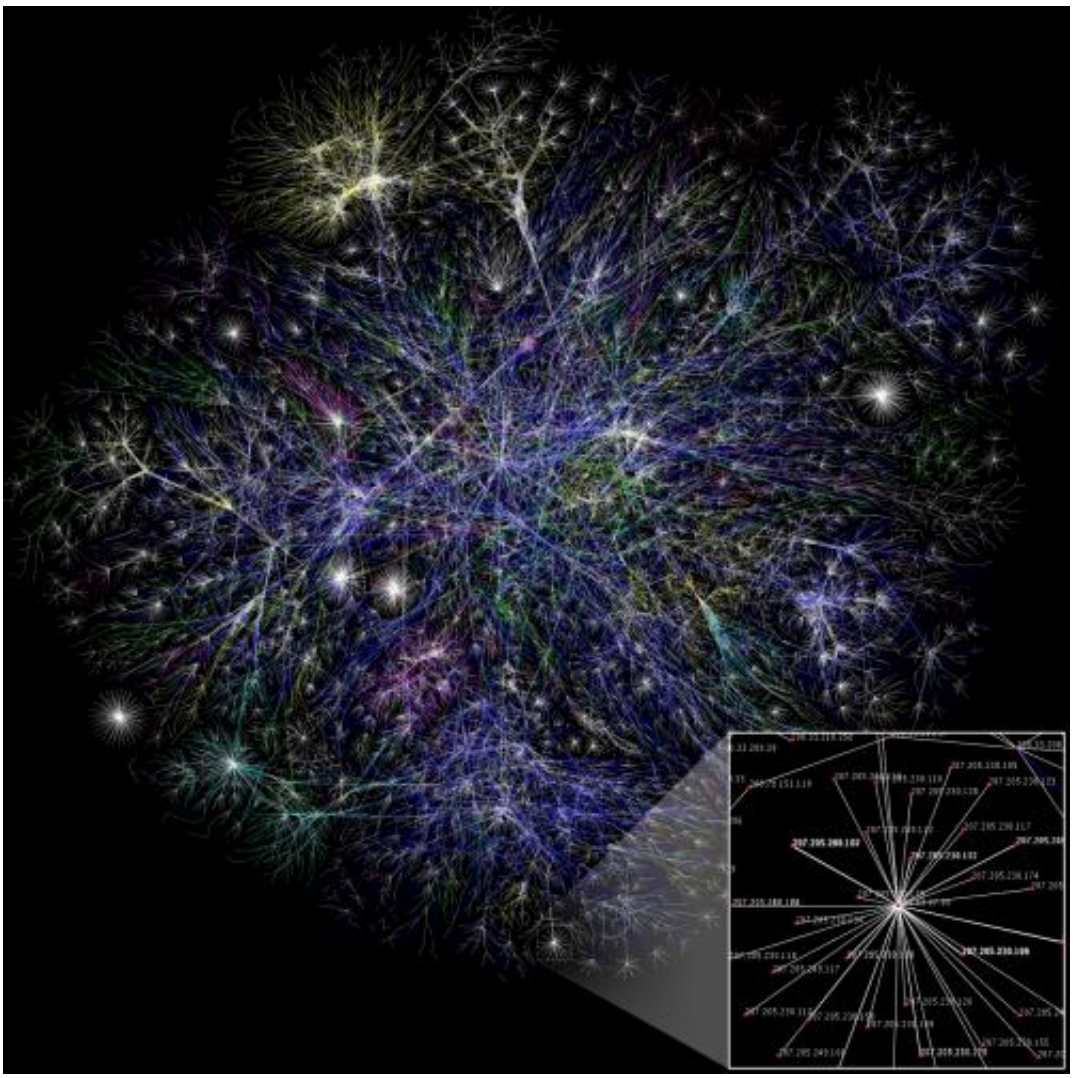
New method for monitoring internet traffic to detect cyber attacks

June 29 2016



Partial map of the Internet based on the January 15, 2005 data found on opte.org. Each line is drawn between two nodes, representing two IP addresses. Credit: Wikimedia Commons

The brute force and sheer scale of current Internet attacks put a heavy strain on classic methods of intrusion detection. Moreover, these methods aren't prepared for the rapidly growing number of connected devices: scalability is a major issue. PhD researcher Rick Hofstede, of the University of Twente's CTIT institute, proposes another way of monitoring internet traffic, thus tracing those attacks that actually have an effect and not all the others. The open source software he developed, is already being tested and used by several organizations in the world. Hofstede defends his PhD thesis on June 29.

Boldly trying a massive number of user name and password until you have that unique combination: that is an example of a 'brute force' Internet attack. Once having gained access to the user's computer, it can, in turn, be used for spreading illegal content or for performing a DDoS attack. Without knowing, users turn into attackers this way. This type of attacks take place via web applications that are relatively vulnerable, like WordPress or Joomla, but also using the Secure Shell (SSH) which enables remote login to a device. Check the contents of the data coming in, analyze network traffic and log files on every single computer: that's the classic approach.

Flow based

According to Rick Hofstede, this implies analyzing a vast amount of data that will never have effect. Within a network of a larger organizations, with probably tens of thousands of computers, smartphones and tablets connected, it will soon be impossible to check every device. Hofstede therefore chooses a 'flow based' approach: he looks at the data flow from a higher level and detects patterns. Just like you can recognize advertisement mailings without actually checking the content of the brochures. Major advantage is that this detection method can take place at a central spot, like a router taking care of traffic. Even if the number of devices connected to this router is growing rapidly – and that will

undoubtedly happen with the introduction of 5G and Internet of Things -, the detection can be scaled up easily. By zooming in on attacks that have effect, i.e. that lead to a 'compromise' and require action, Hofstede further narrows his analysis. Multiple attacks from the same sender can also be recognized in this way.

Hofstede did not just test his methodology inside the lab, he made his 'SSHCure' software available open source, for Computer Emergency Response Teams of several organisations. His method proves to be effective, and diminishes the number of incidents, with detection accuracies up to 100% - depending on the actual application and the type of network, for example. Future, more powerful routers will be able to perform the detection themselves, without the need of extra equipment, Hofstede expects.

Provided by University of Twente

Citation: New method for monitoring internet traffic to detect cyber attacks (2016, June 29) retrieved 4 May 2024 from https://phys.org/news/2016-06-method-internet-traffic-cyber.html