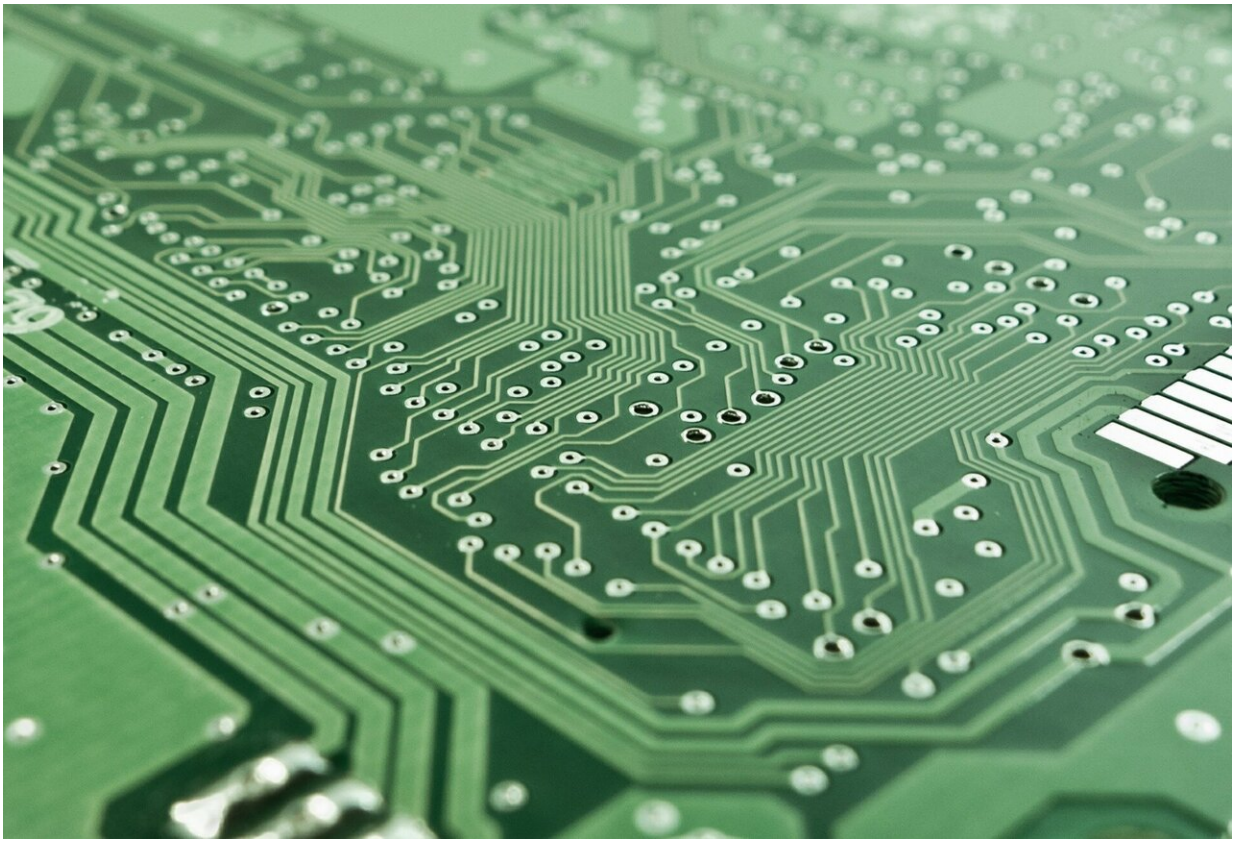
Trickbot trojan found to now have the ability to modify a computer's UEFI

December 4 2020, by Bob Yirka



Credit: CC0 Public Domain

A combined team of security experts from Advanced Intelligence and Eclypsium has announced that the Trickbot trojan malware now has the ability to modify a computer's Unified Extensible Firmware

Interface—the interface between the firmware on a computer motherboard and the computer's operating system—in this case, Microsoft Windows.

Trickbot has been in the news of late due to its advanced capabilities. It has a modular design and is notable for its ability to gain administrative capabilities on infected computers. The entities behind the creation of the trojan are believed to be criminals in Russia and North Korea, and they have used it to target telecoms, health care firms, education institutions and even infrastructure operators (quite often in the form of ransomware).

The trojan and its designers have also achieved a degree of fame over the past year as they managed to overcome a takedown by a combined team of experts from Microsoft and a variety of security firms. Now, it appears the trojan has become even more sophisticated, able to embed itself in the computer's firmware. This new development is considered to be a serious threat because of what it can do once installed.

When a computer boots up, the UEFI and firmware work together to bring up the operating system—if nefarious code has been embedded in the firmware, it can load its own software modules or even modify the operating system as it loads. Such modules would then go undetected by conventional antivirus software and would not be overcome, even if the hard drive were wiped clean or replaced altogether.

The team at Eclypsium has dubbed the new feature "Trickboot," and suggests it allows its makers to take control over both individual computers and whole networks of them. And as a bonus, because it is modular, it can be sold by the developers to users with criminal intent—all the buyers need do is add code to be executed by one of the existing modules. Such functionality could give groups with limited resources the power to create havoc in the user community.

More information: eclypsium.com/2020/12/03/trick … ersist-brick-profit/