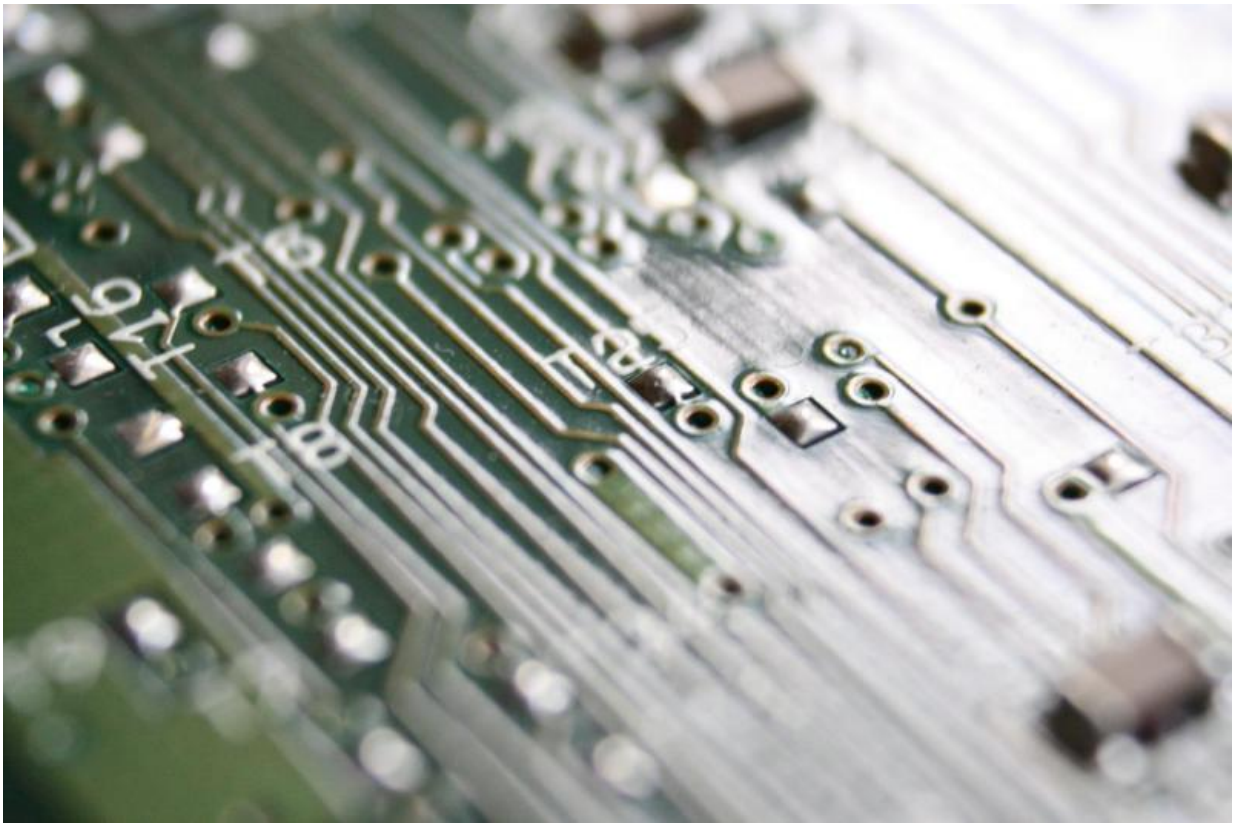
Ransomware ported to web languages poses serious threat

January 6 2016, by Bob Yirka



Credit: Public Domain

Security experts around the world have been reporting that there is a new type of ransomware threat on the Internet—one that has been written using HTML, CSS and Javascript—the programming languages of web

pages. The threat is perceived by many in the field as an ominous sign of things to come because the code has been placed on dark web sites that are accessible to anyone willing to share the proceeds of an attack with the developers.

In their initial form, ransomware attacks took the form of pop-up windows that refused to go away (making the computer unusable) until the person being attacked paid money to the developer. Users soon found out that they could get out of paying by simply rebooting their computer and then running it in safe mode when it came back up, allowing for running software that got rid of the viral code. Newer versions also use a pop-up screen to notify users that they have been attacked, but only after user data has been scrambled. A message on the pop-up window demands payment for the key to unscramble the data. Users can comply with such demands by making payments through untraceable Bitcoin transactions, though there is no guarantee they will ever regain access to their data.

Now it appears things have grown worse, as developers have created similar code that runs with web languages and have made it available to anyone who wants it, allowing non-traditional hacker types to serve co-accomplices. It is called Ransom32 and those who choose to participate can do so by agreeing to give 25 percent of any ransom received to the developers—which can be enforced because the developers possess the encryption keys to unlock the user data.

This new type of ransomwear poses a significant threat because it moves the domain of computer crime into the mainstream. Ostensibly, users get such infections by accessing an infected email, which means they can avoid an attack by not opening suspect email—but it appears conceivable that some people might target someone else's computer intentionally by physical means—they could send an infected email to their own cloud account, gain physical access to a target computer, open their own email

account and then access the infected message thereby launching the attack. People who know little to nothing about coding viruses could conceivably extort money anonymously from employers, colleagues, or even "friends" with such software.

Experts suggest users be ever more diligent in backing up their data to a device not physically connected to their computer to prevent becoming victims of such attacks.

Citation: Ransomware ported to web languages poses serious threat (2016, January 6) retrieved 3 May 2024 from https://techxplore.com/news/2016-01-ransomware-ported-web-languages-poses.html