Check Point Research warns of a further increase in cyberattacks

Check Point Research (CPR) has warned of a further increase in cyberattacks and thinks it could be partly down to major powers leaking cyber superweapons.

Source: Pixabay

"We have long warned that organisations of all sizes are being bombarded by a global, fifth generation of cyber threats (Gen V). These are multi-vector cyber threats that can cause fatal damage and irreparable harm to the reputation of the compromised company. However, most companies are only secured against what we call third-generation threats (Gen III), which are threats that we've known about since the early 2000s and which seek to exploit vulnerabilities in applications," says Pankaj Bhula, regional spokesperson at Check Point Software.

"Cybercrime is evolving at such a breakneck pace that falling behind on protection for weeks or months can have serious consequences, let alone when security is years out of date. It's no wonder then that the pages of newspapers are filled with articles about victims of cyberattacks."

CPR said the problem is likely to be compounded by cyber superweapons being developed by major powers. The company explained that in the real world, it can take months or years to prepare for a military conflict.

"In the online world, a ‘war‘ can be unleashed in seconds. A cyber superweapon is a piece of malware used against a nation-state causing it significant harm. Perhaps the most high-profile example in recent years is the SolarWinds Sunburst attack."

Here's how hackers break into the business environment and how it can be avoided

Anna Collard 11 Jun 2021

It is unfortunate that even small hacker groups have access to very dangerous threats because sooner or later these strategic cyber weapons are leaked by the major powers. Moreover, threats and attacks are traded on the darknet, for example, so the number of potential cybercriminals is even larger. Customised data, threats and attacks can be purchased, so amateurs can cause devastating damage for a few tens of dollars.Stopping the cyberattack pandemic will require cooperation between governments, cybersecurity companies as well as individual organisations.

In May 2021, US organisations saw an average of 671 weekly attacks. This is a 25% increase from the beginning of the year where organizations faced 589 weekly attacks. In EMEA, the weekly average of attacks per organisation was 780 in May, compared to 643 at the start of the year, a 21% increase.

The comparison with May 2020 sounds even scarier. Year-over-year, there was a 70% increase in cyberattacks on US organisations, and a 97% increase in EMEA.

In the Americas, botnet attacks increased the most in May, up 26% compared to the beginning of this year. This was followed by infostealers (up 19%), banking Trojans (10%) and ransomware (9%). In EMEA, malware attacks on IoT devices (up 144%) and mobile attacks (up 41%) rocketed.