Hacking against corporations' surges as workers take computers home

April 17, 2020 - SAN FRANCISCO (Reuters) Hacking activity against corporations in the United States and other countries more than doubled by some measures last month as digital thieves took advantage of security weakness

Corporate security teams have a harder time protecting data when it is dispersed on home computers with widely varying setups and on company machines connecting remotely, experts said.

Even those remote workers using virtual private networks (VPNs), which establish secure tunnels for digital traffic, are adding to the problem, officials and researchers said.

Software and security company VMWare Carbon Black said this week that ransomware attacks it monitored jumped 148% in March from the previous month, as governments worldwide curbed movement to slow the novel coronavirus, which has killed more than 130,000.

"There is a digitally historic event occurring in the background of this pandemic, and that is there is a cybercrime pandemic that is occurring," said VMWare cybersecurity strategist Tom Kellerman.

"It's just easier, frankly, to hack a remote user than it is someone sitting inside their corporate environment. VPNs are not bullet-proof, they're not the be-all, end-all."

Using data from U.S.-based Team Cymru, which has sensors with access to millions of networks, researchers at Finland's Arctic Security found that the number of networks experiencing malicious activity was more than double in March in the United States and many European countries compared with January, soon after the virus was first reported in China.

The biggest jump in volume came as computers responded to scans when they should not have. Such scans often look for vulnerable software that would enable deeper attacks.

The researchers plan to release their country-by-country findings next week.

Rules for safe communication, such as barring connections to disreputable web addresses, tend to be enforced less when users take computers home, said analyst Lari Huttunen at Arctic.

That means previously safe networks can become exposed. In many cases, corporate firewalls and security policies had protected machines that had been infected by viruses or targeted malware, he said. Outside of the office, that protection can fall off sharply, allowing the infected machines to communicate again with the original hackers.

That has been exacerbated because the sharp increase in VPN volume led some stressed technology departments to permit less rigorous security policies.

"Everybody is trying to keep these connections up, and security controls or filtering are not keeping up at these levels," Huttunen said.

The U.S. Department of Homeland Security's (DHS) cybersecurity agency agreed this week that VPNs bring with them a host of new problems.

"As organizations use VPNs for telework, more vulnerabilities are being found and targeted by malicious cyber actors," wrote DHS' Cybersecurity and Infrastructure Security Agency.

The agency said it is harder to keep VPNs updated with security fixes because they are used at all hours, instead of on a schedule that allows for routine installations during daily boot-ups or shutdowns.

Even vigilant home users may have problems with VPNs. The DHS agency on Thursday said some hackers who broke into VPNs provided by San Jose-based Pulse Secure before patches were available a year ago had used other programs to maintain that access.

Other security experts said financially motivated hackers were using pandemic fears as bait and retooling existing malicious programs such as ransomware, which encrypts a target's data and demands payment for its release.

Reporting by Joseph Menn in San Franciso and Raphael Satter in Washington; Editing by Peter Henderson and Christopher Cushing