



THE OTHER COVID-19 PANDEMIC

The Covid-19 pandemic has affected millions worldwide with countless deaths. It has devastated the economies of many countries, stopped children from attending school in person, and closed businesses. Then causing new surges as schools and businesses began to reopen.

I can hear you asking why is a cyber security Insight talking about Covid-19? Because Covid-19 has also brought about a cyber security pandemic.

As businesses and schools closed rapidly people began working and learning from home. And that rapid shift overwhelmed the cyber security teams and protections most companies had in place.

Company systems were designed to support a small percentage of employees working remotely. All of a sudden almost all employees were working remotely and using personal systems not equipped with the proper protections. Schools systems were designed for students in classes, not at home.

Cyber criminals are opportunists and jumped on the changes brought about by the pandemic both in terms of all the unsecured systems and people's thirst for information about the pandemic.

The results?

- At one point over 8000 sites per day were being created that lured people by claiming Covid-19 information. But the purpose of 90% of them was to infect systems and steal credentials and personal information.
- RDP, Remote Desktop Protocol, used to connect and manage computers remotely, was not properly secured on the 40% more machines using it on personal machines connecting from home.
- Studies found the number of attacks on RDP increased by 400% in a two-month period.
- As people craved information on Covid-19 emails with links to sites claiming to provide accurate information grew over 600% in one month.
- Despite all the training and warnings to not click on links in emails, the fear of Covid-19 caused many to lower their guard and click on the links. Three times more likely according to research.
- Zoom video conferencing became the go-to system for many companies and schools working remotely. But it also had some security gaps that were exploited allowing uninvited people to attend the meetings and steal information. At one point there were over 500,000 Zoom account credentials for sale on the Dark web.
- Ransomware has become the new scourge encrypting the data and files of the attacked entity. Attackers have no compunction about attacking companies, schools, government offices, hospitals, medical offices or anyone. And Covid-19 is the new lure to get people to click on the link that downloads the ransomware.

To learn more about cyber protection and education contact Aurora Information Management at info@AIMglb.com or call (888) 773-1920.