

Global Ransomware and Cyberattacks on Healthcare Spike during Pandemic

B labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/



Liviu ARSENE

May 13, 2020

One product to protect all your devices, without slowing them down.

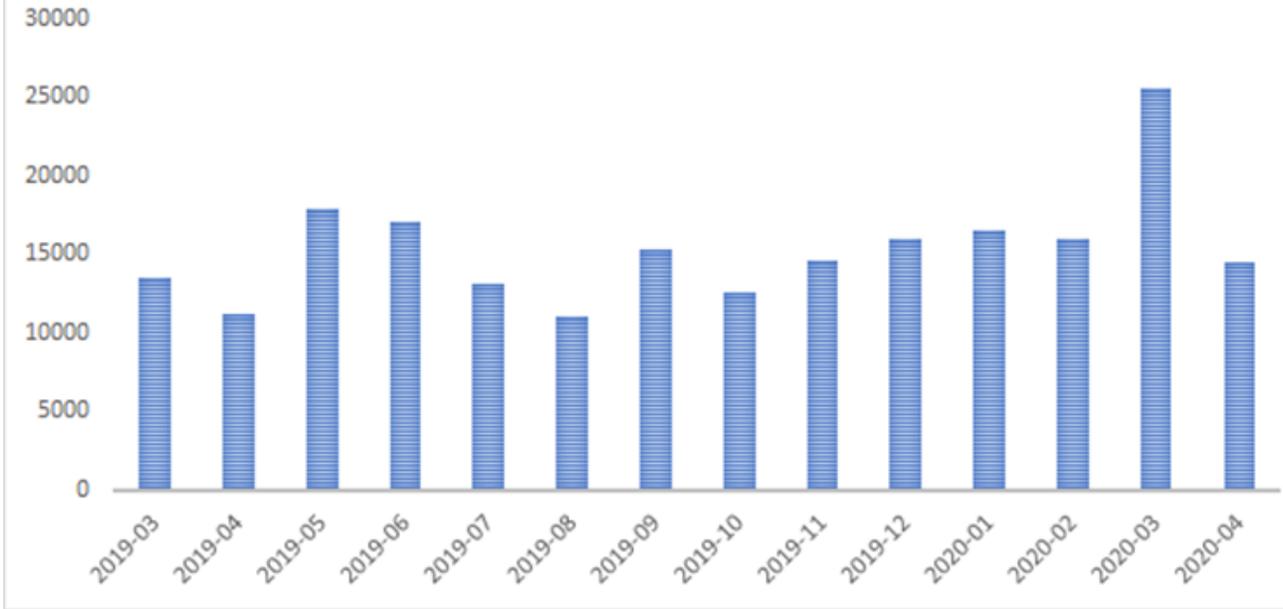
[Free 90-day trial](#)



With healthcare systems under constant strain amid the SARS-CoV-2 global pandemic, hospitals and healthcare facilities around the world have also been hit by a wave of cyberattacks, including ransomware attacks. While officials have already issued warnings that hospitals, governments and universities may be more conscious about losing data and access to critical systems, Bitdefender telemetry reveals that the number of cyberattacks and ransomware incidents directly targeting healthcare significantly increased over the past couple of months.

The number of cyberattacks detected at hospitals in March increased by almost 60 percent from February, according to Bitdefender telemetry. This is the highest spike in our global evolution of cyberattacks detected at hospitals reported over the past 12 months, showing that cybercriminals have clearly leveraged the pandemic to launch these campaigns.

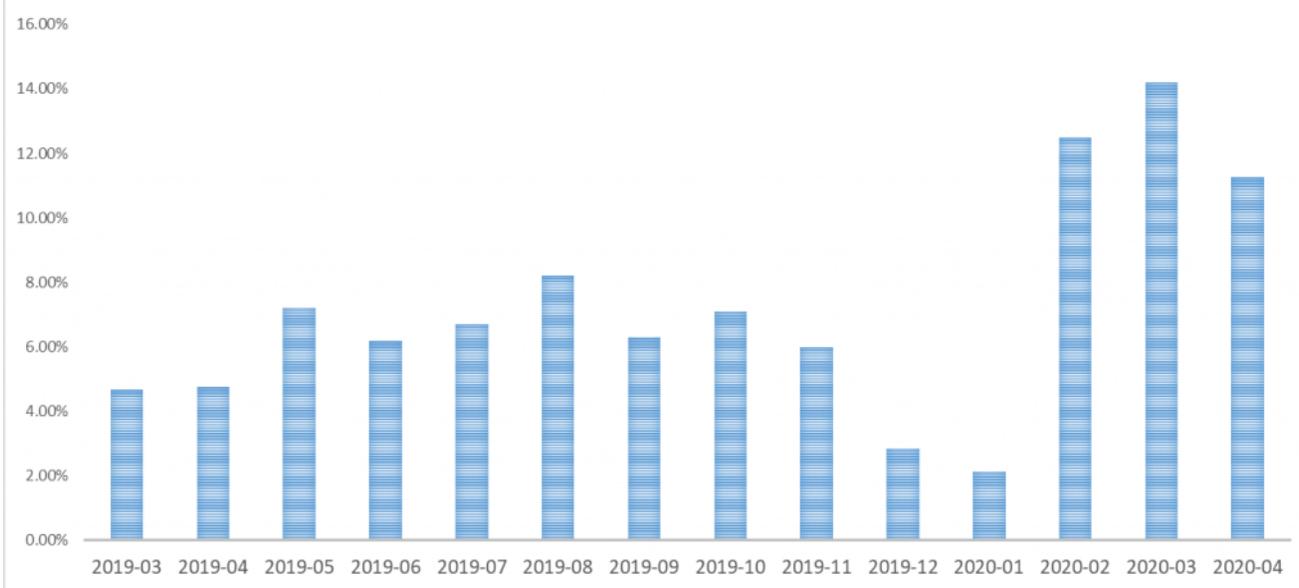
GLOBAL EVOLUTION OF CYBER-ATTACKS DETECTED AT HOSPITALS



Hospitals face a wide array of generic threats (spray and prey or smash and grab) but ransomware causes the most damages and disruption to their operations. Because everything is digital and ransomware blocks access to computers and databases, hospital activity can be paralyzed, with no admissions, no discharges, and no access to patient data.

The number of successfully blocked ransomware attacks at hospitals, as shown by Bitdefender telemetry, jumped significantly in February, March and April. If during 2019 the highest spike in blocked ransomware attacks detected at hospitals was registered in August, during March 2020 the number of blocked ransomware reports rose almost 73 percent.

NUMBER OF BLOCKED RANSOMWARE ATTACKS AT HOSPITALS



It's likely that, since hospitals have been facing new procedures and measures, and new documentation regarding the pandemic on a daily basis, especially during the past couple of months, attackers have been impersonating public institutions and global healthcare organizations to trick medical staff into clicking on malicious URLs or opening infected attachments.

While Coronavirus-themed threats have become the norm during the past couple of months, it's not just the healthcare industry that has been assaulted by a wave of attacks. From retail to hospitality and leisure, education and government, all verticals have registered an increase in malware related to the new Coronavirus.

As these attacks are mostly opportunistic by nature, exploiting popular media topics, the global evolution of Coronavirus-themed malware reports seems linked to how the actual SARS-CoV-2 virus spreads around the world. Previous telemetry from Bitdefender showed that, while the real-world virus hit Europe hardest during the first weeks of March, attackers also focused on Europe when distributing threats. Just weeks later, as the SARS-CoV-2 virus spread to the United States, malware telemetry started to spike there as well.

As March seems to have been the peak of both the global pandemic and of Coronavirus-themed cyberattacks, Bitdefender has been offering free access to its enterprise-grade security at zero-cost (<http://www.bitdefender.com/freehealthcaresecurity>) to healthcare organizations of all sizes around the world, from small dental and ophthalmic practices to large hospitals.

Bitdefender's offer is open to all global healthcare organizations, and our goal is to help them work at full capacity without worrying about cyberattack leveraging the pandemic.

Note: This article is based on technical information provided courtesy of Bitdefender Labs teams.

TAGS

[anti-malware research](#) [miscellaneous](#)

AUTHOR

Liviu ARSENE



ding energy. That's
vs editor for the past
