Malwarebytes

2021

State of Malware Report

EXECUTIVE SUMMARY

The story of 2020 is of the devastating COVID-19 pandemic, and of how the world adapted. The story of malware in 2020 then, is a story of how the tools and tactics of cybercrime and cybersecurity changed against a backdrop of enormous changes to ordinary life.

The novel coronavirus outbreak that began in the city of Wuhan in China was declared a global pandemic on March 12, 2020. Any thoughts that cybercriminals might be above exploiting the catastrophe were quickly disabused. Instead, they adapted and doubled down. As the world watched in alarm at the outbreak spreading, criminals preyed upon people's fears mercilessly, with an avalanche of coronavirus phishing emails and scams.

Around the world, governments tried to stop their hospitals from being overwhelmed by ordering lockdowns, stay-in-place orders, and school closures. By April 2020, half the world's population had been asked or ordered to stay at home. As entire businesses switched to remote working, IT teams found themselves trying to fit months-long projects into days, with security an unfortunate but understandable casualty. Faced with a new landscape, cybercriminals ditched some old tactics and placed a new emphasis on gathering intelligence. And as people adapted to their "new normal," scammers exploited their isolation with a resurgence in tech support scams. New adversaries crawled out of the woodwork, too. April's global shutdown was accompanied by a staggering rise in the use of stalkerware, a short-hand term for the type of mobile monitoring and Spyware apps that are sometimes deployed by abusive partners.

The pandemic also created new challenges to online privacy. As countries turned to digital contact tracing to contain outbreaks, a stark dichotomy emerged: It is possible for people to have personal privacy or effective contact tracing, but probably not both. Around the world, the progress of privacy-preserving legislation slowed to a crawl.

As entire businesses switched to remote working, IT teams found themselves trying to fit months-long projects into days, with security an unfortunate but understandable casualty.

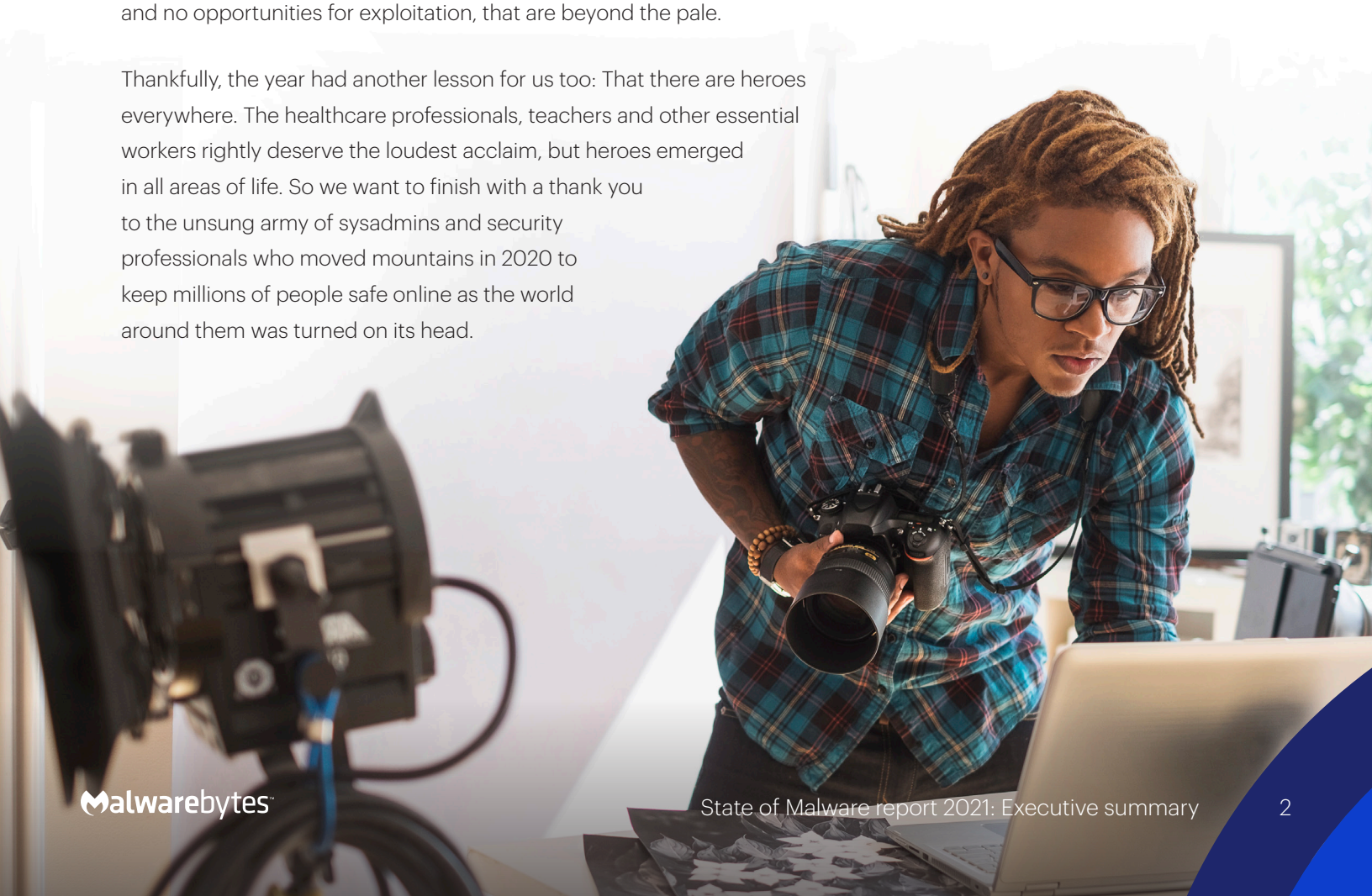
And what began as a global health crisis soon became a global economic crisis too, with almost no business left unscathed. The fate of different industry sectors was mirrored in the number of cyberattacks they suffered. As the manufacturing and automotive sectors contracted, attackers simply turned their faces to agriculture and other essential industries instead. Ransomware gangs reneged on early promises to stay away from hospitals and hit new lows instead, attacking hospitals and medical facilities in organized campaigns.

What began as a global health crisis soon became a global economic crisis too, with almost no business left unscathed.

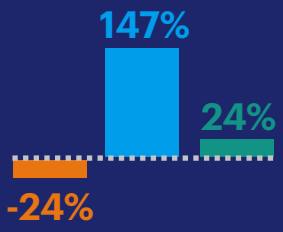
Through it all, there is one form of business that seems to have thrived in 2020 though—the creation and operation of malicious software. The pace of innovation picked up in 2020 as many entirely new malware families emerged. Ransomware gangs continued to learn from each other too, with successful tactics spreading quickly between them. Perhaps the most important new tactic that emerged was "double extortion," which saw cybercriminal groups extorting more money with threats to leak sensitive data than from decrypting compromised computers.

If 2020 taught us anything, it's that cybercrime stops for nothing. There are no targets, and no opportunities for exploitation, that are beyond the pale.

Thankfully, the year had another lesson for us too: That there are heroes everywhere. The healthcare professionals, teachers and other essential workers rightly deserve the loudest acclaim, but heroes emerged in all areas of life. So we want to finish with a thank you to the unsung army of sysadmins and security professionals who moved mountains in 2020 to keep millions of people safe online as the world around them was turned on its head.



Here are key takeaways of what we learned in 2020

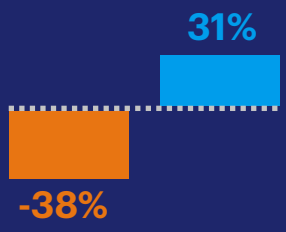


Malware detections on Windows business computers decreased by **24%** overall, but detections for HackTools and Spyware on Windows increased dramatically—by **147%** and **24%**, respectively

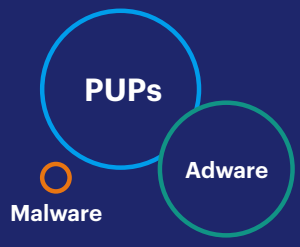
Among the top five threats for both businesses and consumers were the Microsoft Office software cracker KMS, the banking malware Dridex, and BitCoinMiners; business detections for KMS and Dridex rose by **2,251%** and **973%**, respectively

Detections for the most notorious business threats Emotet and Trickbot fell this year by **89%** and **68%** respectively, although the operators behind these threats still pulled off several big attacks in 2020

A new ransomware called **Egregor** came onto the scene in late 2020, deployed in attacks against Ubisoft, K-Mart, Crytek, and Barnes & Noble

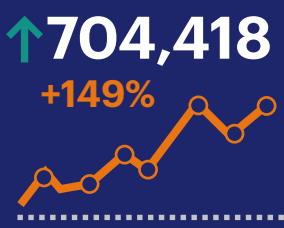


Overall Mac detections decreased by **38%**, though Mac detections for businesses increased **31%**



Malware accounted for just **1.5%** of all Mac detections in 2020—the rest can be attributed to Potentially Unwanted Programs (PUPs) and Adware

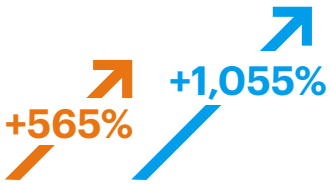
ThiefQuest tricked many researchers into believing it was the first example of ransomware on macOS since 2017, but the malware was hiding its real activity of massive data exfiltration. It accounted for more than **20,000 detections** in 2020



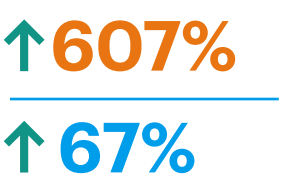
On Android, HiddenAds—which aggressively pushes ads to users—racked up **704,418 detections**, an increase of nearly **149%**

We **twice** uncovered pre-installed malware on phones provided by Assurance Wireless through the US government-funded Lifeline Assistance program

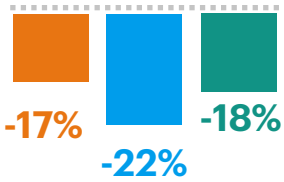
Here are key takeaways of what we learned in 2020 (cont.)



Stalkerware-type app detections—which include detections for Monitor apps and Spyware apps on Android—surged in conjunction with shelter-in-place orders that governments began implementing in February and March: Monitor app detections rose from January to December by **565%**; Spyware app detections rose across the same time period by **1,055%**



The agriculture industry suffered through a **607%** increase in malware detections, while detections in the food and beverage industry increased by **67%**



More traditional targets, such as manufacturing, healthcare and medical, and automotive all experienced drops in detections by varying degrees—education fell **17%**, healthcare dropped **22%**, and the automotive industry decreased by **18%**

GET THE FULL REPORT

Read the complete **2021 State of Malware report** for the latest information on global malware trends and attacks.

malwarebytes.com/business

LABS | blog.malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.