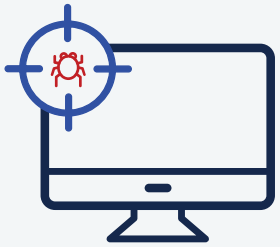
Malwarebytes LABS

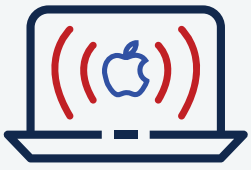
EXECUTIVE SUMMARY

State of Malware Report 2020



Global Windows malware detections increased by 13% on business endpoints

Rise in pre-installed malware and adware on Android devices



For the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint

It was the last year of the 2010s, and cybercriminals let the world know they meant business. From an increase in enterprise-focused threats to diversification of sophisticated hacking, evasion, and stealth techniques to aggressive adware aimed at Androids, the 2019 threat landscape was shaped by a cybercrime industry that was all grown up.

While Malwarebytes observed a relative plateau in the overall volume of threat detections in 2019, our telemetry showed a clear trend toward industrialization. Global Windows malware detections on business endpoints increased by 13 percent, and a bifurcation of attack techniques split threat categories neatly between those targeting consumers and those affecting organizations' networks. The Trojan-turned-botnets Emotet and TrickBot made a return in 2019 to terrorize organizations alongside new ransomware families, such as Ryuk, Sodinokibi, and Phobos. In addition, a flood of hack tools and registry key disablers made a splashy debut in our top detections, a reflection of the greater sophistication used by today's business-focused attackers.

Meanwhile, the 2019 mobile threat landscape fared no better. While Malwarebytes launched a massive drive to combat stalkerware—apps that enable users to monitor their partners' every digital move—which led to an increase in our detections, other nefarious threats lingered on the horizon, with increases in their detections not being helped along by our own research efforts. We observed a rise in pre-installed malware and adware on the devices of our Android customers, with the goal to either steal data or steal attention.

In fact, adware reigned supreme for consumers and businesses on Windows, Mac, and Android devices, pulling ever more aggressive techniques for serving up advertisements, hijacking browsers, redirecting web traffic, and proving stubbornly difficult to uninstall. And for the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint. Even exploits, malvertising, and web skimmers had a banner year. Outside of cryptominers and leftover WannaCry infections, it seemed there were few cybercrime tactics being outright abandoned or on the decline.

With an increase in impact and reach, then, came an increase in public awareness and scrutiny. And in no area was this more apparent than data privacy. On the heels of the Global Data Privacy Regulation (GDPR) in Europe and several public social media failures, a tsunami of data privacy legislation, proposals, fines, controversies, and public policies came forward in 2019. **After a decade marked by seemingly hundreds of high-profile data breaches, the fallout from all that personally identifiable information (PII) floating around on the dark web finally arrived.**