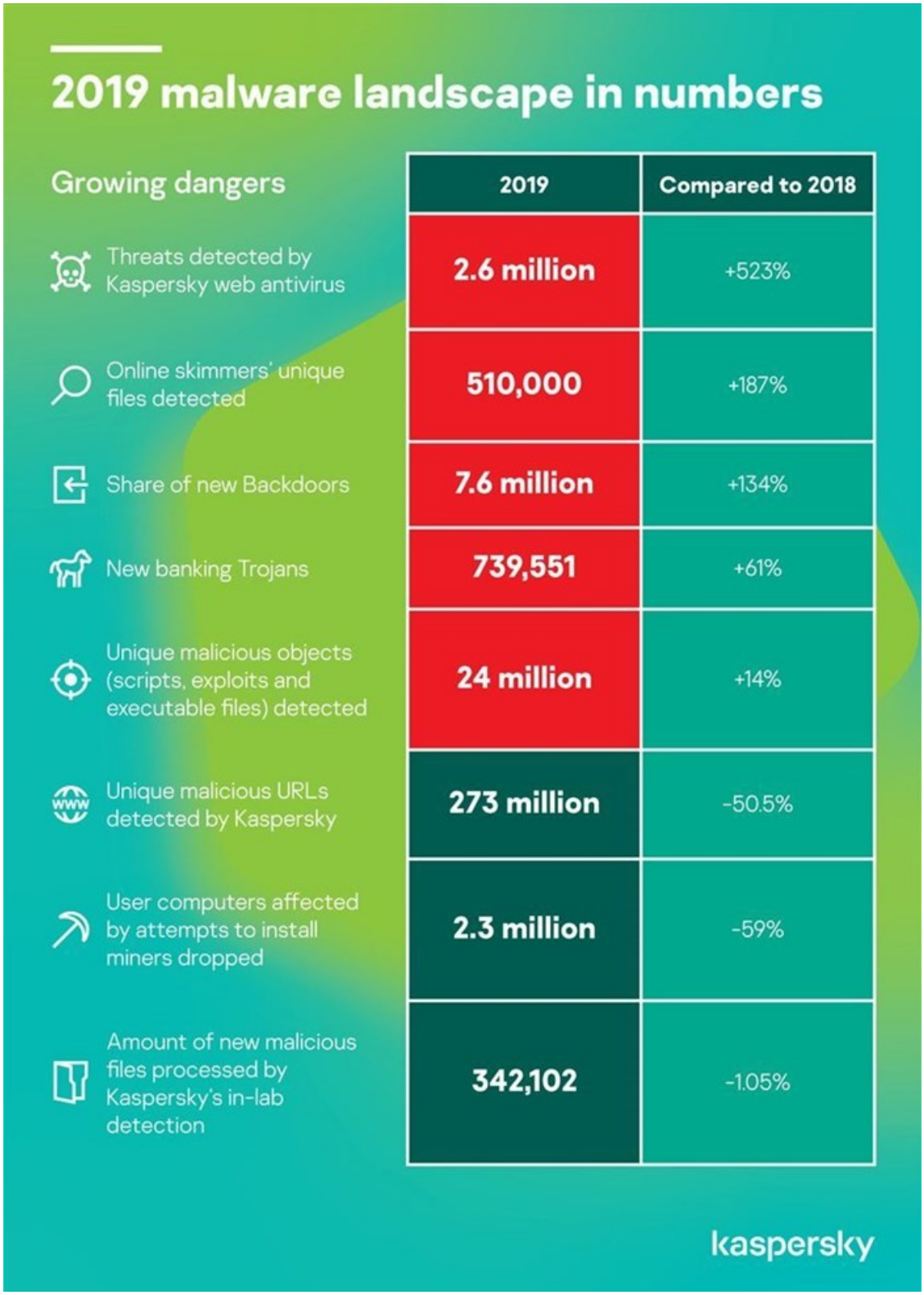
# Malware variety grew by 13.7% in 2019

In 2019, the number of unique malicious objects detected by Kaspersky's web antivirus solution rose by an eighth, compared to the previous year - reaching 24,610,126.




This growth was mainly influenced by a 187% rise in web skimmer files. Other threats, such as backdoors and banking Trojans detected in-lab, also grew, while the presence of miners dropped by more than a half.

These trends have demonstrated a shift in the type of threats used by attackers on the web who search for more effective

ways to target users, according to the Kaspersky Security Bulletin: Statistics of the Year report.

In 2018, unique malicious objects (including scripts, exploits and executable files) detected by Kaspersky's web antivirus solution totalled 21,643,946, rising to 24,610,126 this year. The growth accounts for an increase in the number and variety of HTML pages and scripts with hidden data loading – usually used by unscrupulous advertisers.

Yet, most notably, the growth was also partially caused by online skimmers (sometimes referred to as sniffers) – where scripts are embedded by attackers in online stores and used to steal users' credit card data from websites.

The growth of online skimmers' unique files (scripts and HTML) detected by Kaspersky web antivirus equalled 187%, reaching 510,000. At the same time, the number of threats detected by web antivirus has risen five-fold (by 523%), totalling 2,660,000 in 2019.

Web skimmers also entered the top 20 malicious objects detected online, taking 10th place in the overall ranking. The share of new Backdoors and banking Trojan files, among all types of threats detected in-lab, also grew by 134% and 61% to reach 7,644,402 and 739,551 respectively.

Nevertheless, the number of unique malicious URLs detected by Kaspersky web antivirus halved in comparison to 2018 (50.5%) – from 554,159,621 to 273,782,113. This shift was largely caused by significant decrease of hidden web miners, even though several detections related to them (including Trojan.Script.Miner.gen, Trojan.BAT.Miner.gen, Trojan.JS.Miner.m), can still be seen in the top 20 web malware threats.

The presence of programs that secretly generate cryptocurrency on users' computers (called 'local' miners) has also been steadily declining over the year: the number of users' computers affected by attempts to install miners dropped by 59%, from 5,638,828 to 2,259,038.

85% of web threats were detected as malicious URL – this detection name is used to identify links from Kaspersky's blacklist. It includes links to web pages containing redirects to exploits, sites with exploits and other malicious programs, botnet command and control centres, extortion websites, and others.

"The volume of online attacks has been growing for years, but in 2019 we saw a clear shift from certain types of attacks that are becoming ineffective, to the ones focused on gaining clear profit from users. This is partly due to users becoming more aware of the threats and how to avoid them, and organisations steadily becoming more responsible. A good example is miners, which have lost their popularity due to lower profitability and cryptocurrencies' fight against covert mining. This year we also witnessed growth in zero-day exploits, showing products remain vulnerable and are used by attackers for sophisticated attacks, and this trend is likely to continue in the future," says Vyacheslav Zakorzhevsky, Head of Anti-Malware Research at Kaspersky.

The number of new malicious files processed by Kaspersky's in-lab detection technologies amounted to 342,102 - which is 1.05% less than the previous year.

## Stay protected

In order to stay protected, Kaspersky recommends the following:

- Pay close attention to and don’t open any suspicious files or attachments received from unknown sources
- Do not download and install applications from untrusted sources
- Do not click on any links received from unknown sources and suspicious online advertisements
- Create strong passwords and don’t forget to change them regularly
- Always install updates. Some of them may contain critical security issues fixes
- Ignore messages asking to disable security systems for office software or antivirus software
- Use a robust security solution appropriate to your system type and devices

For more, visit: https://www.bizcommunity.com