The 2020 Threat Landscape

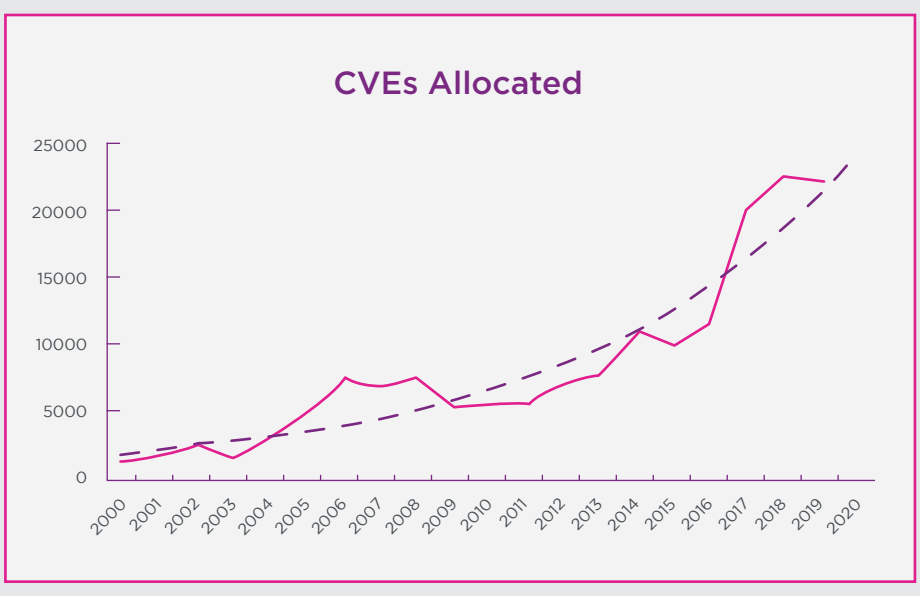
The mid-year update to the 2020 Vulnerability and Threat Trends Report analyzes the vulnerabilities, exploits and threats in play so far this year, revealing how COVID-19 has increased complexities.

Report at a Glance

20,000
New vulnerabilities expected in 2020 – shattering previous records

72%
Increase in new ransomware samples

50%
increase in mobile vulnerabilities

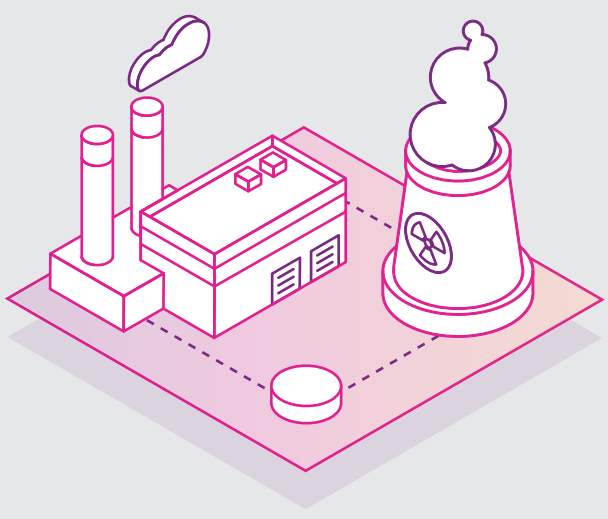


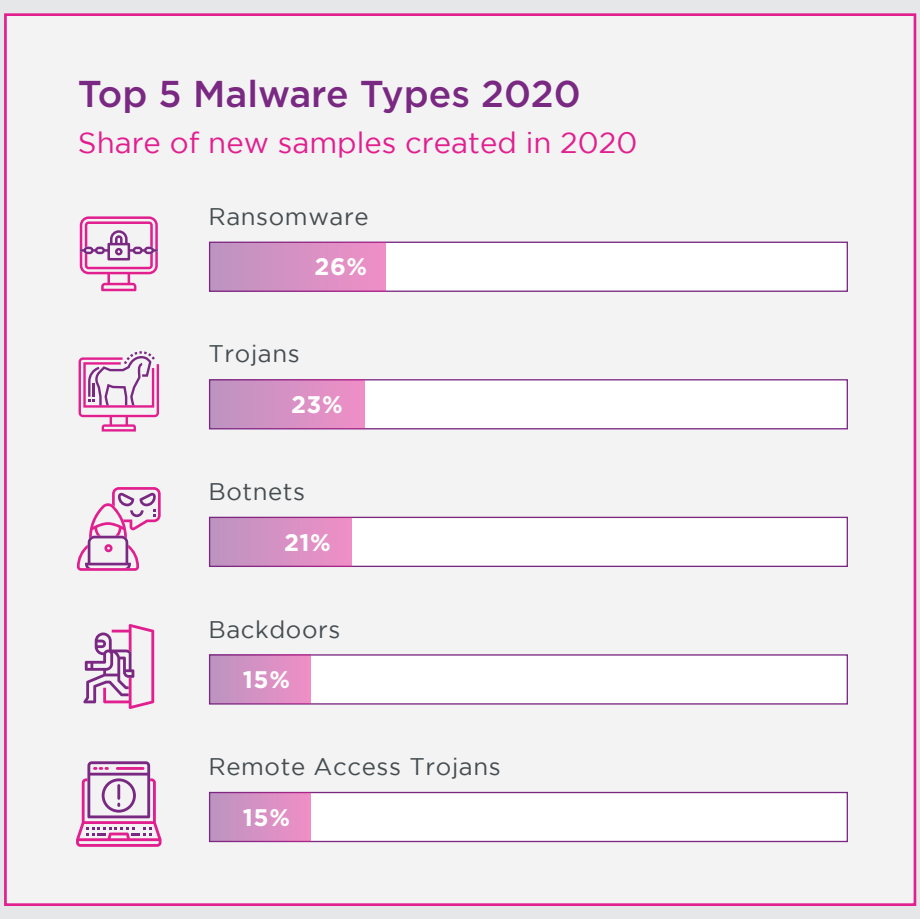
2020 will break new vulnerabilities record

With 20,000 new vulnerabilities expected this year, security leaders' workloads will increase at a time when they are focused on maintaining business continuity.

New OT advisories increase

Attacks on critical infrastructure have increased during the COVID-19 crisis: a **14% increase** in new OT flaws serves as a reminder of how exposed OT environments have become.





New ransomware and trojan samples soar

Criminals have seen opportunity in COVID-19 and have been using ransomware to target critical infrastructure, including research labs and healthcare companies.

110%

New Android vulnerabilities

A large increase in new Android flaws pushed total new mobile vulnerabilities up 50% – at a time when a mass remote workforce blurs the line between personal and corporate devices.

Newcomers to most vulnerable products list

Flaws in Edge Chromium and iPadOS – two products used in both personal and corporate environments – highlight how far the network perimeter has widened.

Chaos Needs Context

The report explains the current state of play for external threats. To understand internal threat context, you need to correlate vast and varied intelligence sources from within your infrastructure. It is only then that you will be able to navigate the challenges thrown up by the COVID-19 crisis while managing a record-breaking number of new vulnerabilities.

Resources:

Report: Mid-year Update to the Vulnerability and Threat Trends Report 2020
Whitepaper: Risk-Based Vulnerability Management

www.skyboxsecurity.com