CHECK POINT™

YOU DESERVE THE BEST SECURITY

CHECK POINT SOFTWARE'S 2022 SECURITY REPORT:
Global Cyber Pandemic's Magnitude Revealed

Highlights of the Check Point 2022 Cyber Security Report Include:

50% ▶ Cyberattacks against corporate networks increased by **50%** in 2021 compared to 2020

1,605 ▶ Education and Research was the most targeted sector, with organizations facing an average of **1,605** weekly attacks

146% ▶ Software Vendors saw **146%** Increase in Cyber Attacks in 2021, marking Largest Year-on-Year Growth

The 2022 Security Report reveals the key attack vectors and techniques witnessed by Check Point researchers during the past year. A year that started with the SolarWinds attack, presenting a whole new level of sophistication and spread, and ending to one of the most severe attacks the internet have seen — the Log4j vulnerability exploitation.

We shall deep dive into some of the emerging trends that will undoubtedly shape the year to come.

We'll discuss cloud services, developments in the mobile landscape and IoT, cracks in the ransomware ecosystem, the return of Emotet, and, of course, the Log4J zero-day vulnerability that punctuated an already busy year.

Main Trends during the year:

- **Supply chain attacks:** the infamous SolarWinds attack laid the foundations for a supply chain attack frenzy. 2021 saw numerous sophisticated attacks such as Codecov in April and Kaseya in July, concluding with the Log4j vulnerability that was exposed in December. The striking impact achieved by this one vulnerability in an open-source library demonstrates the immense inherent risk in software supply chains.
- **Cyber-attacks disrupting everyday life:** 2021 saw an increase in attacks targeting critical infrastructure which led to huge disruption to individuals' day-to-day lives, and in some cases even threatened their sense of physical security.
- **Cloud services under attack:** Cloud provider vulnerabilities became much more alarming in 2021 than they were previously. The vulnerabilities exposed throughout the year have allowed attackers, for varying timeframes, to execute arbitrary code, escalate to root privileges, access mass amounts of private content and even cross between different environments.
- **Developments in the mobile landscape:** Throughout the year, threat actors have increasingly used smishing (SMS phishing) for malware distribution and have invested substantial efforts in hacking social media accounts to obtain access to mobile devices.

DOWNLOAD
CHECK POINT
SECURITY REPORT 2022

The continued digitization of the banking sector in 2021 led to the introduction of various apps designed to limit face-to-face interactions, and those in turn have led to the distribution of new threats.

- **Cracks in the ransomware ecosystem:** Governments and law enforcement agencies changed their stance on organized ransomware groups in 2021, turning from preemptive and reactive measures to proactive offensive operations against the ransomware operators, their funds and supporting infrastructure. The major shift happened following the Colonial Pipeline incident in May which made the Biden administration realize they had to step up efforts to combat this threat.
- **Return of Emotet:** One of the most dangerous and infamous botnets in history, is back. Since Emotet's November return, CPR found the malware's activity to be at least 50% of the level seen in January 2021, shortly before its initial takedown. This rising trend continued throughout December with several end-of-year campaigns, and is expected to continue well into 2022, at least until the next takedown attempt.

The 2022 Cyber Security Report gives a detailed overview of the cyber-threat landscape and recommendations on how to prevent the next cyber pandemic.

These findings are based on data drawn from Check Point Software's ThreatCloud Intelligence between January and December 2021, highlighting the key tactics cyber-criminals are using to attack businesses.

Check Point Research provides leading cyber threat intelligence to Check Point Software's customers and the greater intelligence community.

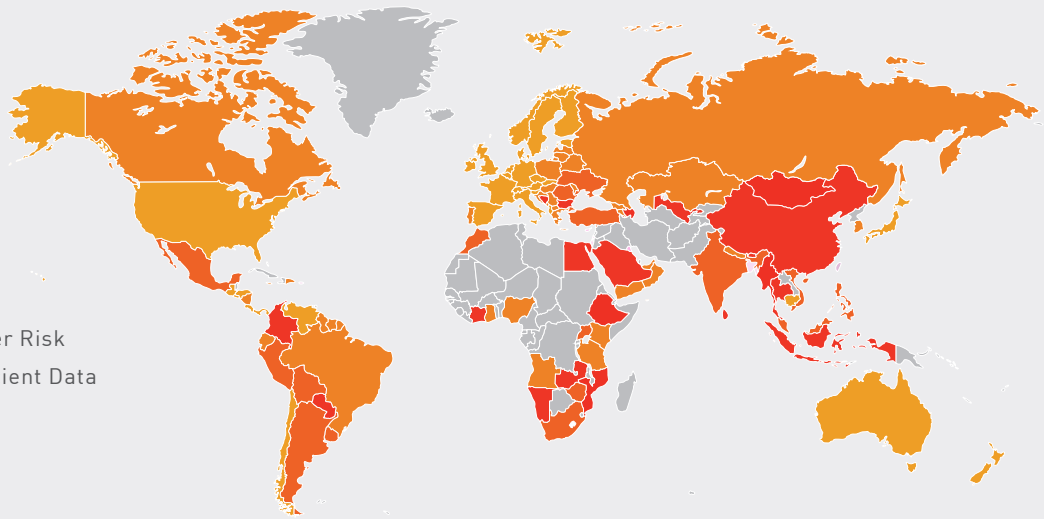
The research & Intelligence teams collect and analyzes global cyber-attacks data stored on ThreatCloud, to keep hackers at bay, while ensuring all Check Point products are updated with the latest protections.

From the moment a breach is initiated, ThreatCloud begins sharing data across the entire network, providing researchers with the intelligence they need to deeply analyze and report on attacks.

Check Point Research publications and intelligence sharing fuel the discovery of new cyber threats and the development of the international threat intelligence community to keep you secure.

GLOBAL THREAT INDEX MAP

The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.*



* Darker = Higher Risk
* Grey = Insufficient Data

DOWNLOAD
CHECK POINT
SECURITY REPORT 2022

cp<r>
CHECK POINT RESEARCH

research.checkpoint.com