2022
BrightCloud® Threat Report
Executive Summary

In the last year, we witnessed many shifts across the threat landscape. From faster time to deployment of ransomware to an uptick in social engineering tactics, malicious actors made leaps and bounds. Knowing how these shifts impact your business and your data is important.

The threat intelligence data presented in our upcoming 2022 BrightCloud® Threat Report is backed by our BrightCloud® Threat Intelligence platform. Our platform gathers continuous data through machine learning-based architecture from millions of real-world endpoints. Our experienced threat research experts analyze this data using sixth generation machine learning and artificial intelligence, providing us with wide-reaching insights and expectations for what lies ahead.

Our full threat report will break down a broad range of threat activities and take a deeper look into what we've seen evolve over the course of the previous year.

Below are several noteworthy trends and activities:

Multiple factors resulted in a 58% year-over-year drop in malware at the endpoint. These factors include:

- Disruption of Emotet, DarkSide and REvil cybercrime operations
- Increase in evasive tactics by leveraging living off the land binaries
- Improvements to upstream detections by BrightCloud technology

Ransomware continues to be the biggest threat small to medium-sized (SMBs) face.

- For SMBs, remote desktop protocol (RDP) remains the primary vector for infection, followed by email phishing
- Smaller businesses witnessed an increase in RDP compromises, whereas larger businesses saw an increase in phishing as the prime vector for ransomware infections
- Median ransomware payments plateaued in 2021, averaging **$70,000**
- Small businesses are becoming the main target of ransomware actors

34.1% of businesses with 21-100 protected endpoints encountered an infection in 2021.

- For businesses with 1-20 protected endpoints, the rate was **8.3%**
- For businesses with 101-500 protected endpoints, the rate rose to **65.1%**
- And for businesses with over 500 employees, the rate was **89.7%**

As the threat landscape continues to evolve, the best approach to combat and recover from cyber threats is to establish cyber resilience. Cyber resilience works by developing a layered defense in depth strategy that zeros in on training your personnel, blocking threats, protecting your devices, backing up your data and recovering from data loss quickly.

Be the first to know. Get the full analysis of the latest threat trends, insights, predictions and more with our 2022 BrightCloud® Threat Report. Our report serves as a guide to help you **enhance your defense** and **strategize recovery**.