BTB
SECURITY

BTB'S INDUSTRY REPORT SCORECARD

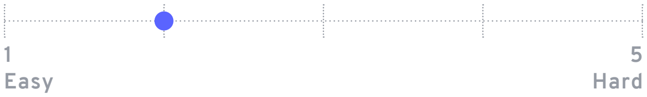
CHECK POINT RESEARCH
2020 CYBER SECURITY REPORT

ANALYZED BY:
MATT WILSON
(CISSP, GPEN, GSEC)

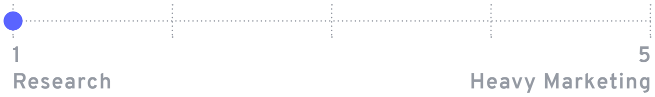
Every year it seems that more and more security vendors are publishing reports on the state of security or on cybersecurity trends. While some of these reports are informative and provide actionable information, too many are thinly disguised marketing pieces or are so dense that getting through them is more challenging than finishing "War and Peace".

With our scorecards we provide a quick review of these reports and call out what you need to know to improve your organization's security posture.

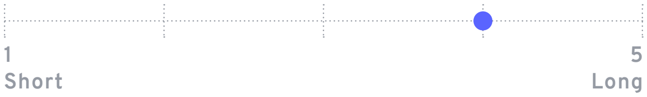
EASE OF READ



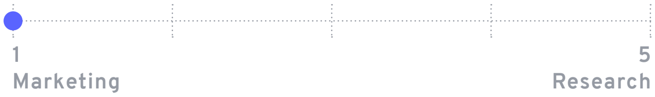
FOCUS



LENGTH: 80 PAGES



MARKETING VS. RESEARCH: 0 CREDITED AUTHORS



OVERALL TRENDS IDENTIFIED

- As the public cloud industry experiences rapid growth, attacks directly targeting public cloud providers are on the rise.
- Misconfiguration or mismanagement of cloud environments was at fault in the majority of successful attacks involving cloud resources.
- While email remains the most common vector for phishing attacks, cybercriminals are increasingly employing SMS messages as well as direct messaging on social media and gaming platforms.
- The mobile threat landscape has matured, with more vulnerabilities in mobile devices, apps and operating systems being exploited more frequently.
- The more things change, the more they stay the same. The majority of malicious file types, whether delivered via email or the web, are still these common ones: .exe, .doc, .pdf, .rtf and .xls.

BEST OF THE REPORT

- If you're in search of a detailed summary of the major cybersecurity happenings in 2019, you've come to the right place. Well researched and based on numerous sources, this report could provide ample evidence to a CISO looking to justify investments this year.
- The report contains detailed comparative insights on malware goals and families as well as target geographies and verticals – information that defenders will find useful.
- While the report's authors make predictions for 2020, they also examine their prior predictions to see how well they held up in 2019. Some of these, however, were broadly worded and are "confirmed" only by anecdotal evidence.

> *Attacks on mobile and cloud platforms… evolved this year, with more vulnerabilities exposed and potential exploits released in the wild. These advanced attacks on public cloud services enabled the massive data breaches we witnessed this year."*
>
> **- VIA CHECK POINT RESEARCH
> 2020 CYBER SECURITY REPORT**

REPORT HIGHLIGHTS

$1.5 TRILLION
STOLEN BY CYBERCRIMINALS ANNUALLY

MORE THAN 90%
OF ENTERPRISES USE CLOUD SERVICES

67% OF SECURITY TEAMS
LACK VISIBILITY INTO THEIR CLOUD INFRASTRUCTURE

66% OF SECURITY TEAMS
BELIEVE TRADITIONAL SECURITY SOLUTIONS OFFER LIMITED OR NO FUNCTIONALITY IN CLOUD ENVIRONMENTS

ATTACK METHODS AND VECTORS

27%
of all organizations globally were impacted by cyberattacks involving a mobile device

68%
of malicious files were distributed via email

32%
of malicious files were distributed via the web

84%
of malware is from one of the six most prevalent malware families

BTB'S TAKEAWAY

At BTB, we review multiple cybersecurity industry studies and research reports on an ongoing basis to compare findings and validate trends.

Check Point's recommendation that organizations enforce Zero Trust-based principles of network segmentation and "least privileged" access controls is useful for security programs with the maturity and resources to be able to do so. Advice like "keep security patches up-to-date," "conduct routine audits and penetration tests," and "monitor incident logs and alerts" is sound. However, we disagree with the authors' assertion that prevention is more important than detection, response and remediation in cybersecurity. Though preventing breaches is always preferable, it's critical to balance proactive controls with robust detection, response and remediation capabilities as well.

SECURITY IN THE CLOUD REQUIRES ADHERENCE TO FAMILIAR BEST PRACTICES

Maintaining a strong security posture in today's cloud-based and hybrid computing environments demands strong internal access controls, MFA, ongoing monitoring and robust patch and asset management. The basic principles – visibility and awareness – haven't changed.

Through all of our reviews, and our own experiences, we recommend focusing on the following:

- Correct IT Hygiene issues (patching, hardening, backup).
- Measure and improve your security posture. Assessments lead to less expensive and more effective outcomes by prioritizing by risk.
- Train your users, especially executives and board members (**execs and the board are allies,** it's your responsibility to make them believe).
- Deploy effective monitoring. Make sure whatever solution you've deployed is functional, not just by ticking feature-set boxes, but by having the People and Process to support the solution.

BTB SECURITY

LOOK FOR OTHER BTB REPORT SCORECARDS TO CUT THROUGH THE FLUFF AND FIND OUT WHAT YOU NEED TO KNOW TO KEEP YOUR BUSINESS SECURE.