SOCs to face greater challenges from cybercriminals targeting governments and media, despite staff shortages in 2023

Cairo, Egypt - 29 January 2023

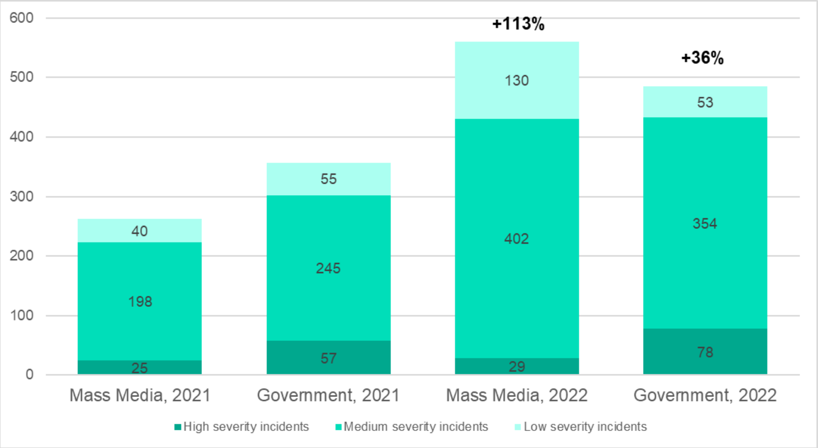
Kaspersky's experts share their predictions for challenges in Security Operation Centers (SOCs). In 2022, the number of incidents in government and mass media segments grew, and the trend will continue this year. SOCs from these – and other industries – are likely to face more reoccurring targeted attacks, as will supply chain attacks via telecommunication providers. Another threat awaiting SOCs is more initial compromises through public-facing applications. Organizations that are threatened by ransomware attacks might also encounter data destruction. From an internal point of view, SOC teams face personnel shortages and increasing demand for efficiencies.

As the role of cybersecurity in large businesses increases remarkably year-on-year, Security Operations Centers (SOCs) are of paramount importance as effectively organized teams can secure their business from rapidly evolving malware and attack methods. This year's Kaspersky Security Bulletin ends with tailored predictions for SOCs.

More reoccurring targeted attacks by state-sponsored actors

In 2022, Kaspersky's experts saw the average number of incidents in the mass media sector double, growing from 263 in 2021, to 561 in 2022. During the last year, a number of high-profile cases occurred, including when Iranian state TV broadcasting was interrupted by hackers during protests in the country. Media outlets were also subject to DDoS attacks, for example, such as those in the Czech Republic.

Alongside the government sector, where the average number of incidents increased by 36 percent in 2022, mass media became the prime target for cybercriminals among the 13 other analyzed segments including industrial, food, development, financial, and others.



The average number of incidents in mass media and government companies per 10K systems in 2021 and 2022, Managed Detection and Response worldwide statistics

The growth will continue in 2023, with reoccurring targeted attacks by state-sponsored actors likely to be often observed. While this is normally relevant for government organizations, the mass media segment has been increasingly targeted during international conflicts that are traditionally accompanied by information warfare where mass media inevitably play an important role.

"Large businesses and government agencies have always been targets of cybercriminals and state-sponsored actors, but geopolitical turbulence increased attackers' motivations and enlivened hacktivism, which cybersecurity specialists have not regularly encountered until 2022. The new wave of politically-motivated attacks is especially relevant for the government and mass media sectors. To effectively protect a company, it's necessary to implement a comprehensive threat detection and remediation provided through Managed Detection and Response services," said Sergey Soldatov, Head of Security Operation Center (SOC) at Kaspersky.

Supply chain attacks via telecommunication providers

In 2023, perpetrators may strike supply chains by attacking telecommunication companies more. This is a further attempt to hit customers, so the growing threat looms larger this year. In 2021, the telecom industry saw - for the first time - a prevalence of high severity incidents throughout the year. Although in 2022, the average share of high severity incidents was lower – 79 in 2021 per 10k systems monitored, versus roughly 12 in 2022 – these companies remain attractive targets for cybercriminals.

Ransomware destroyers; initial compromises via public-facing applications

Throughout 2022, Kaspersky observed a new ransomware trend that will continue in 2023 – ransomware actors will not only encrypt companies' data but also destroy it. This is relevant for organizations which are subject to politically-driven attacks.

Another threat awaiting SOCs is more initial compromises through public-facing applications. Penetration from the perimeter requires less preparation than phishing and old vulnerabilities are still exposed.

What SOCs will face internally? Processes and efficiency

In 2023, the value every team member (even not skilled ones) brings to SOC is increasing. Developing the skills of the team is the proven way to counter the increasing amount of threats. That means IR-related training and any form of SOC exercises, such as TTX, purple teaming, and advisory attack emulations, will be of vital importance.

The growing threat landscape leads to increasing budgets and demand for more efficiencies. Increasing numbers of incidents and threats transforms into a need to predict attacks and techniques, raising the value of threat intelligence and hunting.

To read the full report on SOC challenges in 2023, please visit Securelist.com. This report is a part of Kaspersky Security Bulletin (KSB) – an annual series of predictions and analytical reports on key shifts within the cybersecurity world. Click here to look at other KSB pieces.

To protect from the relevant threats, Kaspersky researchers recommend implementing the following measures:

- Always keep software updated on all the devices you use to prevent attackers from infiltrating your network by exploiting vulnerabilities. Install patches for new vulnerabilities as soon as possible. Once it is downloaded, threat actors can no longer abuse the vulnerability.

- Dedicated services can help combat high-profile attacks. The Kaspersky Managed Detection and Response service can help identify and stop intrusions in their early stages, before the perpetrators achieve their goals. If you encounter an incident, Kaspersky Incident Response service will help you respond and minimize the consequences, in particular - identify compromised nodes and protect the infrastructure from similar attacks in the future.

- Use the latest Threat Intelligence information to stay aware of actual TTPs used by threat actors.

- Choose a reliable endpoint security solution such as Kaspersky Endpoint Security for Business that is equipped with behavior-based detection and anomaly control capabilities for effective protection against known and unknown threats.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky’s deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company’s comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.