ARC VIEW

APRIL 19, 2018

Kaspersky Lab Moves Forward with Improved Cybersecurity Solutions

By Thomas Menze

Keywords

Kaspersky, Cybersecurity, Threat Management, Malware

Summary

Kaspersky Lab, a global cybersecurity company headquartered in Moscow, Russia is operated by a holding company in the United Kingdom. The company celebrated its 20th anniversary last year. Kaspersky Lab's solutions are designed to transform the company's threat intelligence and security expertise into cybersecurity solutions and services to help protect businesses, critical infrastructure, industry, governments, and consumers around the globe.

Kaspersky Lab continues to expand its portfolio, introducing and enhancing solutions such as endpoint detection and response to help prevent, detect, and respond to the most sophisticated cyber threats.

Moving Forward Despite DHS Ban

In Autumn 2017, the US Department of Homeland Security (DHS) ordered federal agencies and departments to remove software sold by the Russia-based Kaspersky Lab, citing concerns that the company's alleged ties to the Russian government could present potential vulnerability to intrusion by Russian intelligence.

The order directed the federal government's executive branch to identify all Kaspersky products then in use within 30 days and begin to phase these out entirely within 90 days.

The US government expressed concern about the possibility that Russian intelligence could access sensitive data and compromise systems using Kaspersky products, which are meant to guard against cyber intrusions. This prompted the company to beef up its Global Transparency Initiative and introduce a variety of new cybersecurity products and services, with more scheduled for release later in 2018.

Global Transparency Initiative

As part of its Global Transparency Initiative, which includes an independent review of the company's source code and establishing three Transparency Centers globally, Kaspersky Lab is extending its "bug bounty" program. This supplements the company's own extensive vulnerability detection and mitigation efforts. Rewards of up to $100,000 are now available for members of the HackerOne platform who help discover serious vulnerabilities in some of the company's flagship products. Kaspersky Lab has partnered with HackerOne for the Bug Bounty initiative. This 20-fold increase on existing rewards helps demonstrate the company's commitment to protect its customers by ensuring the complete integrity of its products.

Kaspersky Lab's "bug bounty" program supplements the company's own extensive vulnerability detection and mitigation efforts with rewards of up to $100,000.

Advanced Cybersecurity Platform

With IT-OT convergence and digital transformation melting previous protection perimeters, IT security teams in enterprises must recognize the fact that complex threats could already be present within their networks. Like many fatal diseases, targeted attacks can penetrate an organization's critical systems and stay unnoticed for years, causing irreparable damage in the process. Symptoms can be misleading and only an extensive examination can provide an accurate diagnosis.

According to the company, the next generation of the Kaspersky Anti Targeted Attack Platform, part of the company's Threat Management and Defense solution, uses a comprehensive set of technologies to help detect previously unknown threats and targeted attacks. To help organizations discover even the most complex attacks, it correlates different indicators of compromise in the network that are likely connected to a single operation.

Full visibility and accurate detection are only two parts of the equation. The very nature of targeted attacks means attackers will come back with new tools and techniques. If an emergency occurs, the cybersecurity team might need a trusted partner with the relevant skills and experience.

Kaspersky Cybersecurity Services includes several related services offerings. These include:

- Incident Response – for rapid incident recovery

- Targeted Attack Discovery – to proactively assess and rectify damage
- Kaspersky Managed Protection - a full, outsourced threat-hunting service

Kaspersky Industrial Cybersecurity

Malicious attacks on industrial systems – including industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) – have increased significantly in recent years. As previous attacks have shown, one infected USB drive or a single spear-phishing email is all it takes for attackers to bridge the air gap and penetrate an isolated network. Traditional security is no longer enough to protect industrial environments from cyber threats. As threats increasingly target critical infrastructure, it has never been more important for an industrial organization to choose the right advisor and technology partner to help secure its systems.

> As previous attacks have shown, one infected USB drive or a single spear-phishing email is all it takes for attackers to bridge the air gap and penetrate an isolated network.

Many industrial companies now use off-the-shelf networking technologies to improve the transparency and efficiency of enterprise management processes, as well as provide flexibility and fault tolerance for industrial automation. As a result, industrial networks are becoming increasingly like office IT networks – both in terms of use case scenarios and the technologies used. The unfortunate flip side of this is that internet threats, as well as other traditional IT threats, increasingly affect industrial networks.

Kaspersky Lab offers industrial end users three pillars with which to harden their automation systems:

- Awareness training - to cover the human factor
- Software - to identify abnormal network communication
- Security on-site service - to remove malware from the network

In 2018, Kaspersky Lab plans to launch the following security appliances to support industrial users:

- Asset management software
- Network identification flow map
- Machine learning (ML) for anomaly detection

Conclusion

Despite the recent headwinds the company has experienced, Kaspersky is still one of the top global IT security experts. Kaspersky Security Services for Office and Business applications are designed to deliver multi-layered security against known, unknown, and advanced threats. The unique combination of Big Data, threat intelligence, machine learning, and human expertise supports agile protection against any kind of threat — regardless of the platform and with minimal management overhead.

Despite the US Department of Homeland Security's order to remove Kaspersky software from government computers, the company has proceeded to develop its shift from classic cybersecurity to a total security approach. By predicting, detecting, and reacting to attacks, Kaspersky Lab's total approach is designed to help make organizations immune to most cyber threats.

According to Eugene Kaspersky, the company's founder and CEO, "We believe that everyone - from home computer users through to large cooperation's and governments - should be able to protect what matters most to them."

For further information or to provide feedback on this article, please contact your account manager or the author at tmenze@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.