Trend Micro Survey Finds Nearly Half of Organizations Have Been Victims of BPC Attacks

Half of management teams lack awareness about BPC despite increased attacks

LONDON--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today revealed that 43 percent of surveyed organizations have been impacted by a Business Process Compromise (BPC). Despite a high incidence of these types of attacks, 50 percent of management teams still don't know what these attacks are or how their business would be impacted if they were victimized.

In a BPC attack, criminals look for loopholes in business processes, vulnerable systems and susceptible practices. Once a weakness has been identified, a part of the process is altered to benefit the attacker, without the enterprise or its client detecting the change. If victimized by this type of attack, 85 percent of businesses would be limited from offering at least one of their business lines.

"We're seeing more cybercriminals playing the long game for greater reward," said Rik Ferguson, vice president of security research for Trend Micro. "In a BPC attack, they could be lurking in a company's infrastructure for months or years, monitoring processes and building up a detailed picture of how it operates. From there they can insert themselves into critical processes, undetected and without human interaction. For example, they might re-route valuable goods to a new address, or change printer settings to steal confidential information – as was the case in the well-known Bangladeshi Bank heist."

Global security teams are not ignoring this risk, with 72 percent of respondents stating that BPC is a priority when developing and implementing their organization's cybersecurity strategy. However, the lack of management awareness around this problem creates a cybersecurity knowledge gap that could leave organizations vulnerable to attack as businesses strive to transform and automate core processes to increase efficiency and competitivenessi.

The most common way for cybercriminals to infiltrate corporate networks is through a Business Email Compromise (BEC). This is a type of scam that targets email accounts of high-level employees related to finance or involved with wire transfer payments, either spoofing or compromising them through keyloggers or phishing attacks.

In Trend Micro's survey, 61 percent of organizations said they could not afford to lose money from a BEC attack. However, according to the FBI, global losses due to BEC attacks continue to rise, reaching $12 billion earlier this year.

Ferguson continued: "To protect against all forms of BPC attacks, business and IT leaders must work together to put cybersecurity first and avoid potentially devastating losses. Companies need protection beyond perimeter controls, extending to detect unusual activity within processes if attackers breach the network. This includes locking down access to mission critical systems, file integrity monitoring, and intrusion prevention to stop lateral movement within a network."

For more information on BPC and BEC attacks, read this Trend Micro Researchreport.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

Research methodology

Research carried out by Opinium, commissioned by Trend Micro. Online survey among 1,125 IT decision-makers responsible for cybersecurity across the UK, US, Germany, Spain, Italy, Sweden, Finland, France, Netherlands, Poland, Belgium and Czech Republic.

i https://www.globenewswire.com/news-release/2018/05/30/1514183/0/en/Robotic-Process-Automation-Market-to-Grow-at-36-2-CAGR-till-2023-P-S-Market-Research.html

Contact:

Erin Johnson

media_relations@trendmicro.com
trendmicro@redconsultancy.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2018-12-06-Trend-Micro-Survey-Finds-Nearly-Half-of-Organizations-Have-Been-Victims-of-BPC-Attacks