Bitdefender® Global Leader In Cybersecurity

The Gig Economy Behind RANSOMWARE

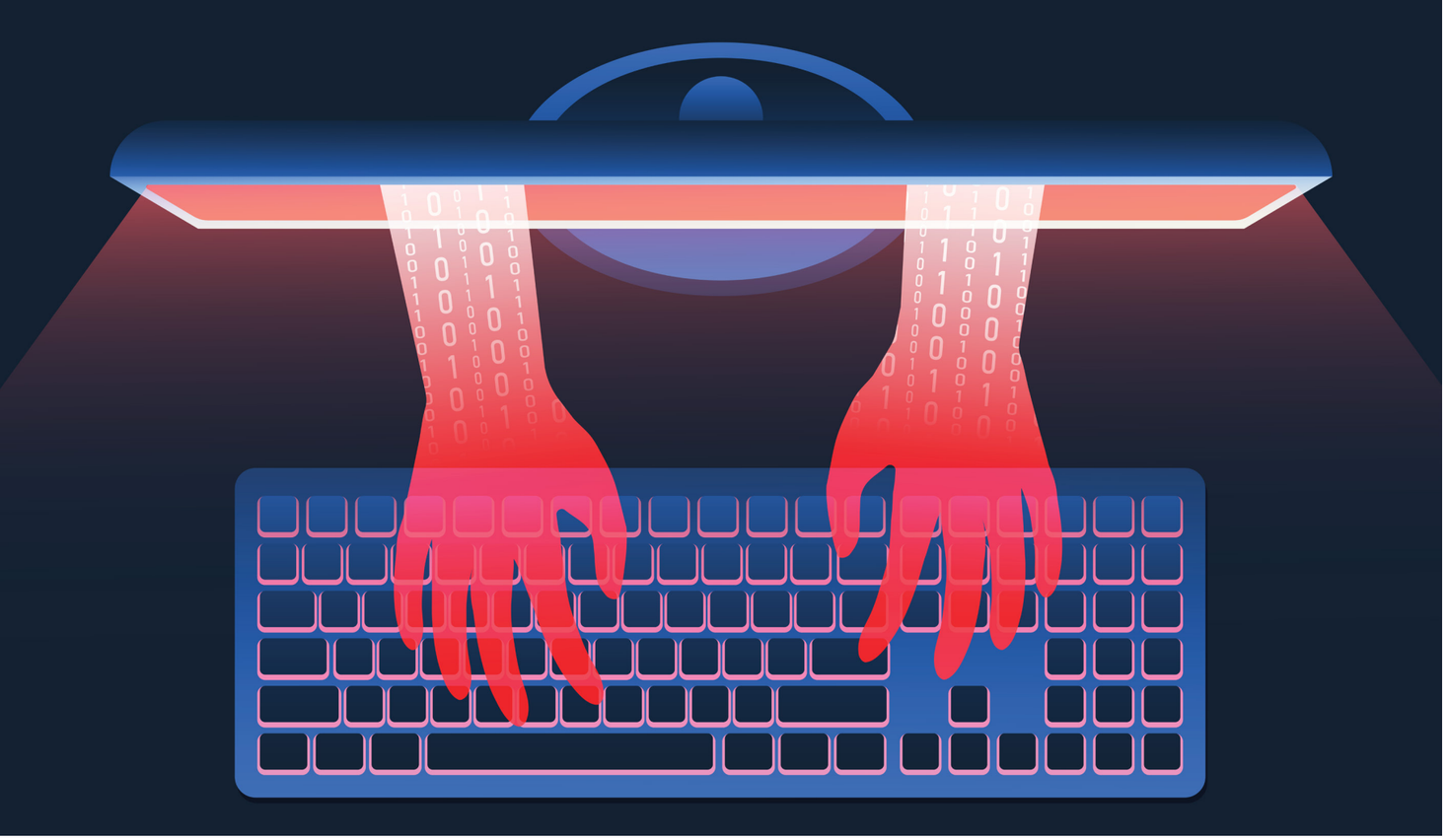
Table of contents

Bitdefender Global Leader In Cybersecurity

Introduction

Cybercrime, much like a business, continues to evolve and refine its operations to be more efficient and profitable. Ransomware-as-a-Service (RaaS) is one of the biggest evolutions of late, democratizing access to ransomware. Much like Uber revolutionized transportation by allowing anyone with a car to become a driver, RaaS democratization enables individuals, regardless of their technical prowess, to launch sophisticated ransomware attacks, effectively turning illicit cyber activities into a gig economy.

RaaS has increased the frequency and sophistication of ransomware attacks, making them one of the top security threats organizations worldwide face, increasing alerts across numerous tools and leading to inefficiencies in the management of cybersecurity operations. These attacks target critical infrastructure, healthcare systems, educational institutions, and private corporations—no sector is immune. These attacks can cause colossal economic and operational damages, often running into millions of dollars due to downtime, data loss, and reputational damage.



Once onboard, affiliates are given access to custom ransomware tools suited for their operations. The relationship's foundation is a profit-sharing model where affiliates receive a significant portion of the ransoms, driving them to maximize attack impact. For businesses, this motivation drives more attacks targeting those with weaker security posture or maturity, driving the need for better resource allocation to prevent being attacked despite budget constraints.

While the profit-sharing model draws many cybercriminals, it also involves substantial risks. Legal repercussions for caught individuals can be severe, adding a layer of danger to their activities. Trust remains a delicate issue; with high stakes involved, the potential for betrayal can leave affiliates vulnerable, either by losing out on profits or facing legal actions if operators choose to sever ties or disclose information to authorities.

Operators and Affiliates

Operators and affiliates engage in a symbiotic relationship crucial for the operation's success. Acting as architects, operators develop and maintain the ransomware, ensuring it remains undetectable, and manage the infrastructure required for these attacks, from server maintenance to ransom collection platforms. Affiliates, the ground operatives, deploy this ransomware, select targets, and execute attacks, culminating in ransom negotiations. This partnership begins with a rigorous selection process on dark web forums and encrypted channels where operators vet potential affiliates for their skills and history of evading detection.

Specialized Roles and Responsibilities Within the RaaS Model

Efficiency in RaaS drives specialization, expanding beyond operators and affiliates. By specializing, each individual brings expertise and experience, increasing the likelihood of a successful attack.

- Operators are pivotal in managing ransomware development and overseeing its deployment and ransom collection infrastructure. They handle complex financial processes and provide technical support and software updates to sustain the operation's backbone.

- Software developers focus on building and maintaining the technical tools required for the operation, ensuring that the ransomware and its deployment mechanisms are constantly updated and more likely to bypass advanced security protocols.

- Initial access brokers are penetration experts who specialize in finding vulnerabilities and securing access points to penetrate target systems, setting the stage for the attack.

- Affiliates execute the attacks by leveraging access to deploy ransomware, navigate through network defenses, and manage the spread across the victim's infrastructure.

- Professional negotiators drive ransom negotiations, especially in high-value cases, to optimize the outcome by leveraging control over the victim's data.

Each specialist focuses on refining their skills in their respective domains, enabling the creation of more advanced and covert methods of infiltration and attack execution. Each role fills a unique niche in the ransomware attack cycle, helping ensure that each attack not only breaches security but also aligns strategically with the overarching objectives of their illicit enterprise.

Collaboration Among Cybercriminals

The collaboration on the dark web and encrypted communications channels intensifies attacks, bringing a wealth of tools, techniques, and critical information about potential vulnerabilities and successful strategies. Criminals foster a community of learning and development, driving innovation in creating more evasive malware and more targeted phishing campaigns.

These efforts accelerate the evolution of ransomware tactics, making it increasingly challenging for cybersecurity professionals to keep pace. The collaborative nature of these groups exacerbates security gaps and increases the need for advanced risk mitigation strategies. Defenders must constantly adapt and evolve their strategies and technologies, driving law enforcement and cybersecurity agencies to develop sophisticated, integrated approaches that can match the coordination and specialization of the criminals.

Bitdefender Global Leader In Cybersecurity

The collaborative nature of these groups exacerbates security gaps and increases the need for advanced risk mitigation strategies.

Economic Forces Driving **Cybercrime**

Cybercrime operates under the same economic principles that drive legitimate markets—supply and demand, market entry barriers, and competition, yet it has unique dynamics. The demand for illegal access, data, and software exploits drives the supply of increasingly sophisticated cyber attack methodologies. With the rise of tools like RaaS, barriers to entry are lower than ever, creating a highly-competitive environment that compels cybercriminals to continually innovate to maintain their edge.

Financial motivations predominantly drive cybercrime, offering high-profit margins and lower risks than traditional crimes. Cybercriminals benefit from the ability to operate virtually anywhere, significantly reducing the likelihood of apprehension. This has led to the transformation of cybercrime into highly organized, economically driven operations that mirror traditional businesses in structure but focus on maximizing profit and minimizing risk.

The economic impact of cybercrime is profound, draining billions from the global economy and influencing international cybersecurity policies and regulations, which necessitate substantial investments in defensive technologies to stay compliant. This international aspect of cybercrime also presents complex challenges for legal systems as international cooperation is required to respond to these evolving digital threats.

Comparison With Regular Markets

Cybercrime markets mirror legitimate business structures. They operate with distinct hierarchies and specializations but under the cloak of anonymity and without formal regulation. These digital underworlds function with roles akin to traditional businesses: operators as CEOs, affiliates as sales forces or field agents, and coders and testers as R&D departments. Unlike conventional markets driven by transparency and regulatory oversight, cybercrime exploits secrecy, facilitated by technologies such as Tor and encrypted communication channels, to maintain anonymity.

In these covert markets, trust and anonymity are crucial. Cybercriminals utilize Tor networks and cryptocurrencies to conduct transactions without revealing their identities. To establish and maintain trust within these anonymous settings, they employ mechanisms similar to e-commerce, including vendor ratings, buyer feedback, and escrow services that hold funds until transactions are completed. Despite the lack of formal oversight, this pseudo-regulatory environment enables transactions to proceed with a semblance of reliability.

However, this anonymity poses significant challenges for law enforcement and cybersecurity professionals, complicating efforts to trace illegal activities and disrupt criminal operations. Addressing these challenges requires a deep understanding of the market dynamics and specialized tools designed to penetrate the anonymity that protects these criminal networks.

With the rise of tools like RaaS, barriers to entry are lower than ever, creating a highly-competitive environment that compels cybercriminals to continually innovate to maintain their edge.

Profit-sharing Models and the Gig Economy Analogy

RaaS employs a profit-sharing model similar to the gig economy's commission-based earnings, where operators and affiliates share the proceeds from each successful attack. This arrangement incentivizes affiliates to carry out as many attacks as possible, enhancing their earnings and benefiting operators who receive a portion of each ransom. This model mirrors the flexibility and scalability of the gig economy, allowing cybercriminal networks to rapidly adjust strategies and expand their operations without significant upfront investments or fixed infrastructures.

Adopting this gig economy framework within cybercrime has fundamentally changed the composition of the cyber workforce. It has lowered entry barriers, enabling individuals with minimal initial investment to participate in cybercriminal activities. These new entrants can gradually undertake more complex roles, starting with simple tasks as they build experience and trust within the network. This model not only diversifies the pool of talent in these illicit enterprises but also offers the flexibility to work remotely, attracting a broader range of participants and expanding the reach and capability of cybercrime networks worldwide.

Challenges and **Threats**

Security professionals have a tough job adapting to combating increasingly sophisticated attacks. Technological advancements like artificial intelligence (AI) and machine learning create an ongoing arms race between cybercriminals, who leverage these technologies for malicious purposes, and cybersecurity defenders, who use them to enhance protective measures.

Legal and geopolitical complexities hinder international cooperation against cybercrime, exacerbated by jurisdictional discrepancies that allow cybercriminals to exploit safe havens. Resource disparity further complicates this, making smaller organizations particularly vulnerable to ransomware attacks, as they often lack the necessary defenses.

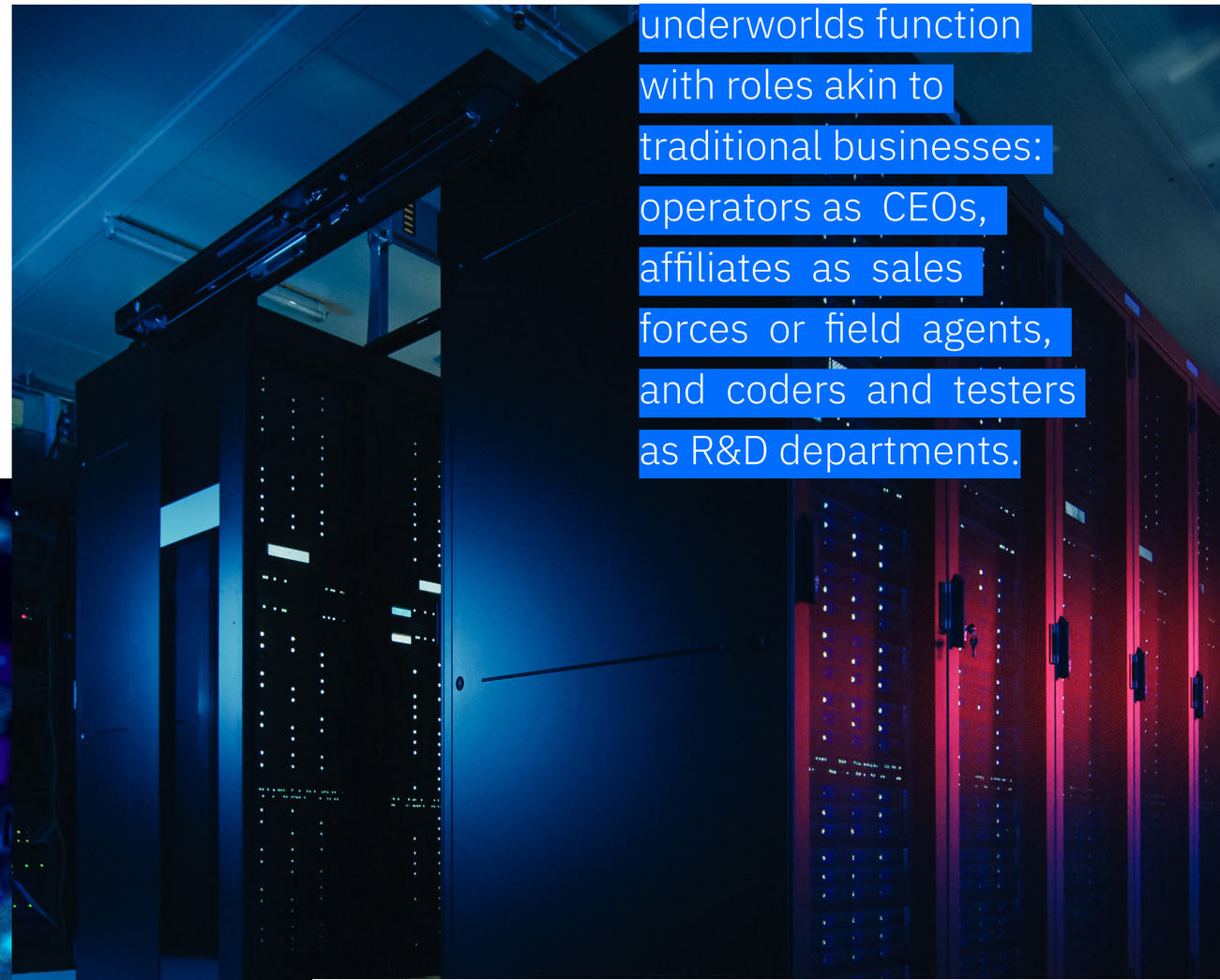
Increasing Sophistication and Scalability of Attacks

The sophistication and scalability of ransomware attacks have dramatically evolved, challenging cybersecurity defenses. These attacks typically unfold in multiple stages, starting with an initial network infiltration through phishing or exploiting vulnerabilities, followed by lateral movements to explore and exploit further system weaknesses. This progression often culminates in data lockdown or exfiltration, with each phase meticulously crafted to maximize impact and evade detection.

Automating ransomware deployment using sophisticated scripts allows cybercriminals to target multiple organizations simultaneously, greatly expanding the threat landscape and diminishing the effectiveness of traditional security measures. Their scalability further complicates challenges for smaller businesses trying to maintain a strong security posture despite limited resources and ongoing skills shortages. These operations make it all the worse when integrated with other cybercrimes like data theft and distributed denial-of-service (DDoS) attacks, further complicating defensive strategies and amplifying the potential damage, driving the need for advanced detection and response capabilities.

Trust Dynamics Within the Cybercriminal Network

Trust is the most significant hurdle for criminals due to the illegal nature of activities. Cybercriminals have co-opted trust mechanisms from legitimate business practices to foster a sense of reliability within their networks. Reputation plays a crucial role in building this trust. Like feedback systems on legitimate e-commerce platforms, darknet markets and forums use reputation scores and reviews to vet members and ensure accountability, reducing fraud risks. Additionally, escrow services are employed in transactions to mediate trust issues between unknown parties, holding funds or digital goods securely until all transaction terms are met.

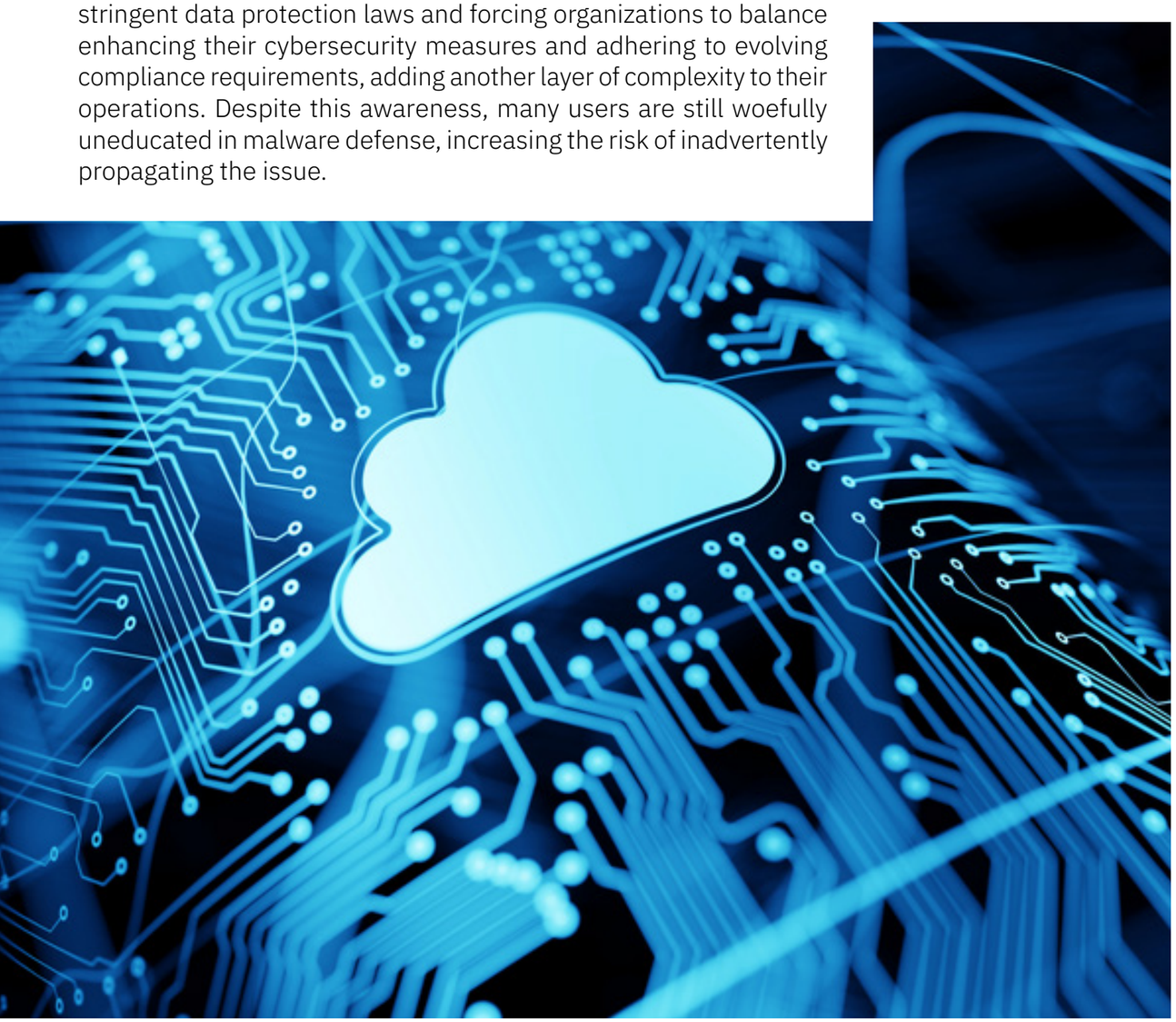


These digital underworlds function with roles akin to traditional businesses: operators as CEOs, affiliates as sales forces or field agents, and coders and testers as R&D departments.

Despite these systems, relationships within cybercriminal networks remain inherently unstable due to the high stakes and illegal context. Over time, cybercriminals may form alliances that stabilize operations and foster loyalty, which is essential for coordinating complex operations involving multiple specialists. However, the potential for betrayal is high, with internal conflicts, double-crossing, and the risk of exposure to law enforcement threatening the integrity of these partnerships. Such betrayals disrupt operations and can lead to the arrest and prosecution of involved parties.

Key **Ransomware** Trends

As ransomware continues to change, several trends have emerged. Attacks continue to evolve, exploiting new technologies and platforms to find and leverage vulnerabilities. This has pushed ransomware into the public view, driving stringent data protection laws and forcing organizations to balance enhancing their cybersecurity measures and adhering to evolving compliance requirements, adding another layer of complexity to their operations. Despite this awareness, many users are still woefully uneducated in malware defense, increasing the risk of inadvertently propagating the issue.



Data Exfiltration

Cybercriminals increasingly employ data exfiltration techniques to copy and transfer sensitive data before encryption, greatly enhancing their leverage over victims and complicating their decision-making processes. This approach forms the basis of the double extortion tactic, where attackers demand a ransom for data decryption and threaten to publicly release stolen data if their demands are not met. This tactic particularly affects sectors like healthcare and financial services, which face severe legal and reputational risks if personal and financial data are compromised.

Organizations are implementing comprehensive defensive measures to counter these threats, including advanced detection systems to monitor unusual data movements, enhanced data segmentation, and robust employee training programs to identify and mitigate threats. Quick-response incident plans are crucial to ensure rapid recovery and minimal damage from such attacks.

The collaborative nature of these cybercriminal groups exacerbates security gaps and increases the need for advanced risk mitigation strategies.

Manual Hacking Operations

The increased adoption of manual hacking techniques heightens the effectiveness of these cyber assaults and helps them bypass automated defenses. These sophisticated techniques enable attackers to navigate complex network environments, carefully choosing entry points and pathways that minimize detection and maximize impact. These operations require high skill and adaptability, positioning human operators at the forefront of orchestrating these attacks while allowing them to evade defense measures and exploit new vulnerabilities as they are discovered within the network.

The manual aspect of these operations often mimics legitimate network activity, making them particularly challenging to detect. Traditional automated security systems may fail to recognize these activities as malicious due to their subtle and discreet nature, blending seamlessly with routine tasks performed by legitimate users. Without specialized IT staff, these attacks will go unnoticed until too late. Proactive incident response plans that can be readily deployed increase resilience but only mitigate damage.

Vulnerabilities in Edge Network Devices

Edge network devices, particularly those operating in demilitarized zones (DMZs) such as VPN appliances, remote access software, and file transfer services, significantly expand the attack surface for cybercriminals. These devices, crucial for facilitating external access to corporate networks, pose substantial security challenges. Newly discovered vulnerabilities in these devices are quickly weaponized, allowing them to be targeted as initial access points for ransomware attacks due to their exposure to the internet and the critical access they provide.

While Internet of Things (IoT) devices, including routers, security cameras, and smart sensors, are being integrated into corporate networks to enhance efficiency and data collection capabilities, they are less commonly used as direct vectors for ransomware attacks.

Supply Chain Expansion

The complexity of global supply chains significantly broadens the attack surface for cybercriminals, with each layer of suppliers, manufacturers, and service providers offering potential entry points for attacks. While high-impact upstream software supply chain attacks, like the SolarWinds incident, are rare, they show the severe consequences of such breaches, disrupting operations and undermining trust in widely used tools.

However, a more frequent and often overlooked threat within supply chains is Business Email Compromise (BEC) and similar attacks, where cybercriminals impersonate executives or trusted partners to send malicious links or fraudulent requests. These attacks happen daily and can impact companies of all sizes, leading to significant financial losses and compromised business operations.

In response to these diverse threats, organizations are intensifying their focus on supply chain security, employing comprehensive third-party risk assessments and secure communication protocols to verify and secure each component. Training employees to recognize and respond to signs of BEC and other email-based fraud helps mitigate the broader risks associated with supply chain attacks.

At Bitdefender, we believe strongly in understanding attacker behavior to build the most effective defenses.

Ransomware is a complex problem with many stages and approaches. Unfortunately, there is no single solution.

The only effective defense against modern ransomware attacks is to implement a multi-layered defense-in-depth strategy, with effective security controls for prevention, protection, detection, and response. Bitdefender provides a range of products and services to address the problem of ransomware for companies of all sizes.

Uncover the Secrets of Stopping Ransomware

Explore our in-depth, continuously updated white paper on the ransomware ecosystem. Discover how our cutting-edge cybersecurity solutions can protect your organization from sophisticated ransomware threats. We always update this document to reflect the prevailing tactics and techniques, mapping our security controls to different stages of the kill chain.

Stay informed and ahead of cybercriminals by accessing this comprehensive live document on TechZone.

Learn More

Bitdefender® Global Leader In Cybersecurity

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Trusted. Always.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.