



File Transfer Services Under Siege: A Growing Threat Landscape

The escalating wave of cyberattacks on file transfer services (FTSs), marked by a substantial 48% increase in 2023 as reported by Sophos, underscores a mounting concern in the cybersecurity landscape. These attacks pose significant risks, manifesting in financial losses, reputational damage, and privacy breaches that impact both businesses and individuals alike. FTSs, functioning as conduits for sensitive data, emerge as prime targets for malicious actors, evident in prominent incidents like the 2023 Clop ransomware attack, the 2021 Accellion MFT attack, and the 2020 Emotet malware campaign.

In the 2023 Clop ransomware attack, malevolent actors exploited vulnerabilities in FTSs, exemplifying the potential consequences of compromised file transfer services. Similarly, the 2021 Accellion MFT attack showcased the severe fallout, including data breaches, operational disruptions, and multimillion-dollar ransom demands. The 2020 Emotet malware campaign further demonstrated the global impact of FTS-related cyber threats, causing disruptions and stealing sensitive data on an unprecedented scale.

The attractiveness of FTSs to threat actors lies in their widespread use across various industries, coupled with a concerning lack of awareness within organizations regarding the associated security risks. Leveraging these vulnerabilities, cyber adversaries strategically exploit FTSs to infiltrate networks, emphasizing the urgent need for heightened vigilance.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the

highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.