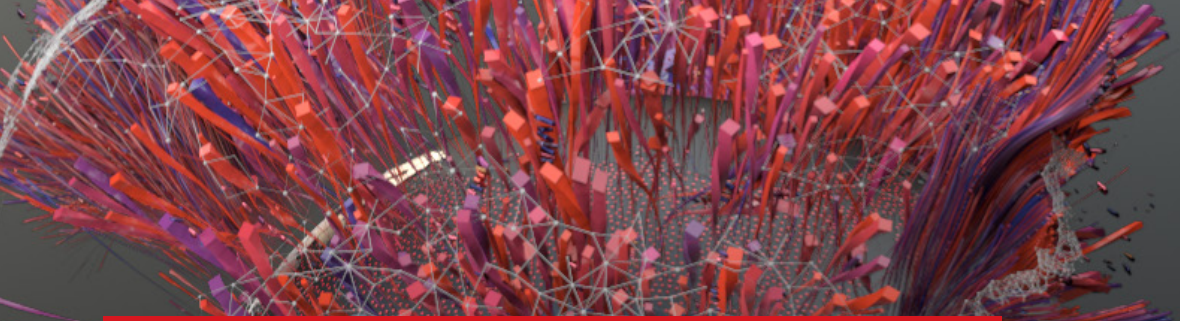

WHAT MIGHT PUSH YOU INTO THE RED?

In 2021 we blocked over 94 billion threats, with detections increasing 42% year on year, as malicious actors stepped up their attacks. As lucrative industry, online gaming and betting presents a cash and data rich lure for cyber criminal activity.

Attacks are typically DDOS and ransomware, phishing, trojans, spyware, viruses, worms, keyloggers, bots, cryptojacking and backdoor. The effects, and purpose of these attacks can vary, from operator losses, fines, lost business and ransoms, not to mention the loss of reputation and players drifting to competitors.

Customer Data and Identity Theft

Simple access to your customer records to gather account details and personal information for criminal use. These databases are valuable to criminals and can change hands very quickly to directly compromise your customers' security. This can lead to GDPR breaches, and to potentially expensive and reputation-damaging legal actions against your business.

Account Takeovers

Once cybercriminals have hacked your customers' accounts, they may not stop at capturing personal and banking data, but may take over the betting or gaming accounts themselves and make fraudulent bets, transactions and withdrawals while masquerading as your customers. Sometimes customers are not even aware this has happened.

Ransomware and DDOS

Ransomware that successfully infiltrates your systems can encrypt and exfiltrate your customers' account details, allowing malicious actors to either demand a ransom from you, or threaten your customers with misuse of their data (or both) along with offering additional avenues of approach.

Both Ransomware and DDOS will disrupt operations, compromise your platforms, limit or deny availability and can threaten the security of your customers, to the point where you have to respond by acceding to the wishes of the cybercriminals. You may have to pay large sums in order to continue your operation, and to limit reputational damage that could drive you out of business. Not all ransom payments will be covered by insurance policies, if it can be proven that your business was not adequately protected against this type of attack.

Game Integrity

Compromise the perceived integrity or stability of any game or betting platform and you will lose customers - fast. Hackers know this and can actually target the games themselves in order to damage your business - by changing odds, making impromptu payments and imposing new rules. Your reputation, and your profitability, is at stake if you are unable to deny access to these cybercriminals.

Money Laundering

The physical gaming and betting industry has always been a great place for criminals to hide illegal proceeds, and online platforms are no different. The UK gaming and betting industry is one of the most highly-regulated in the world. Organised criminals can leave you open to regulation breaches and large fines if you cannot clearly demonstrate due diligence and watertight security standards.

How can Trend Micro help keep you, and your customers, secure?