Cyber GRX

CyberGRX Ransomware Threat Profile and Ecosystem View

Ransomware continues to dominate headlines with no sign of slowing down. And why would it? Ransomware is an extremely lucrative business for cyber criminals, estimated to have cost businesses globally $20 billion in 2020, up from $11.5 billion in 2019 according to the 2021 Checkpoint Software Security Report. While the average ransom paid by mid-sized organizations in 2020 was $170,404, the cost to recover from an attack was closer to $1.85 million when accounting for downtime, resources, hardware, and network costs as reported in Sophos' The State of Ransomware 2021 report. And effects can be long-lasting after a ransom is paid. On average, organizations that paid the ransom recovered just 65% of the encrypted files, leaving over one-third of their data inaccessible. (Sophos 2021)

In order to fight ransomware, companies need a methodology that combines a wide range of security safeguards with a modern approach to third-party cyber risk management, including threat intelligence and comprehensive data analytic capabilities. CyberGRX has several tools available to help combat ransomware, available to our enterprise and third-party members.

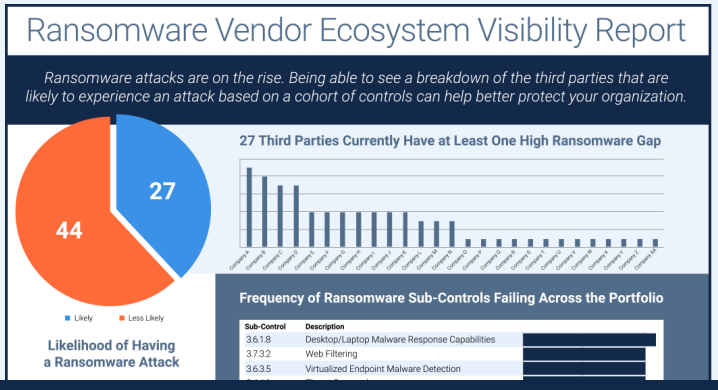
Ransomware Threat Profiles

The Ransomware Threat Profile, available in the Framework Mapper tool, allows a company to pull a report for individual third parties to view their coverage of 124 controls that have specifically been identified as critical to ransomware protection by MITRE®. CyberGRX examined tactics and techniques from over 160 use cases, including 49 ransomware attacks, in order to identify primary controls needed to detect, prevent, and mitigate the threat of ransomware.

In additional to the Ransomware Threat Profile, CyberGRX also offers threat profiles aligned with specific ransomware campaigns and other recent cyberattacks including REvil Ransomware – Kaseya Supply Chain Attack, SolarGate, CodeCov, and Accellion. These profiles provide a view of how the third party rates against each identified control known to be exploited in these attacks. Companies can filter by those controls that are missing/absent and follow up with the third party to request remediation.

Ransomware Ecosystem View

In addition to Threat Profiles, the CyberGRX Ransomware Ecosystem View is an additional report available to CyberGRX members that provides an overview of the ransomware risk within their entire third-party ecosystem. Based on the same identified controls as the Ransomware Threat Profile, this report provides a holistic view of which third parties currently have at least one ransomware gap as well as the which controls are least covered across their portfolio. With this information, they are also provided a breakdown of which third parties are most likely to experience a ransomware attack.



Talk to a Third-Party Risk Consultant today about how we can arm you with real-time intelligence to defend yourself differently.

www.CyberGRX.com

Cyber GRX