PRODAFT BLINDSPOT

POTENTIAL APPLICATION ANALYSIS:

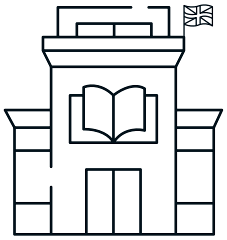
RANSOMWARE ATTACK ON ONE OF THE LARGEST LIBRARIES IN THE WORLD

Industry: Public Information Service

Region: Western Europe

Challenge: Targeted compromise by a high-end ransomware group in a serial campaign affecting multiple public, educational and governmental institutions across the globe

WHO IS THE ENTITY?



British Library is the national library of the UK and simultaneously one of the biggest libraries in the world. Their collection boasts over 170 million items including various books, maps, recordings, stamps, prints, drawings and newspapers. The library complex has been open since 1998 and still serves as an important place to study, gather and research, as well as a hosting place for numerous events.

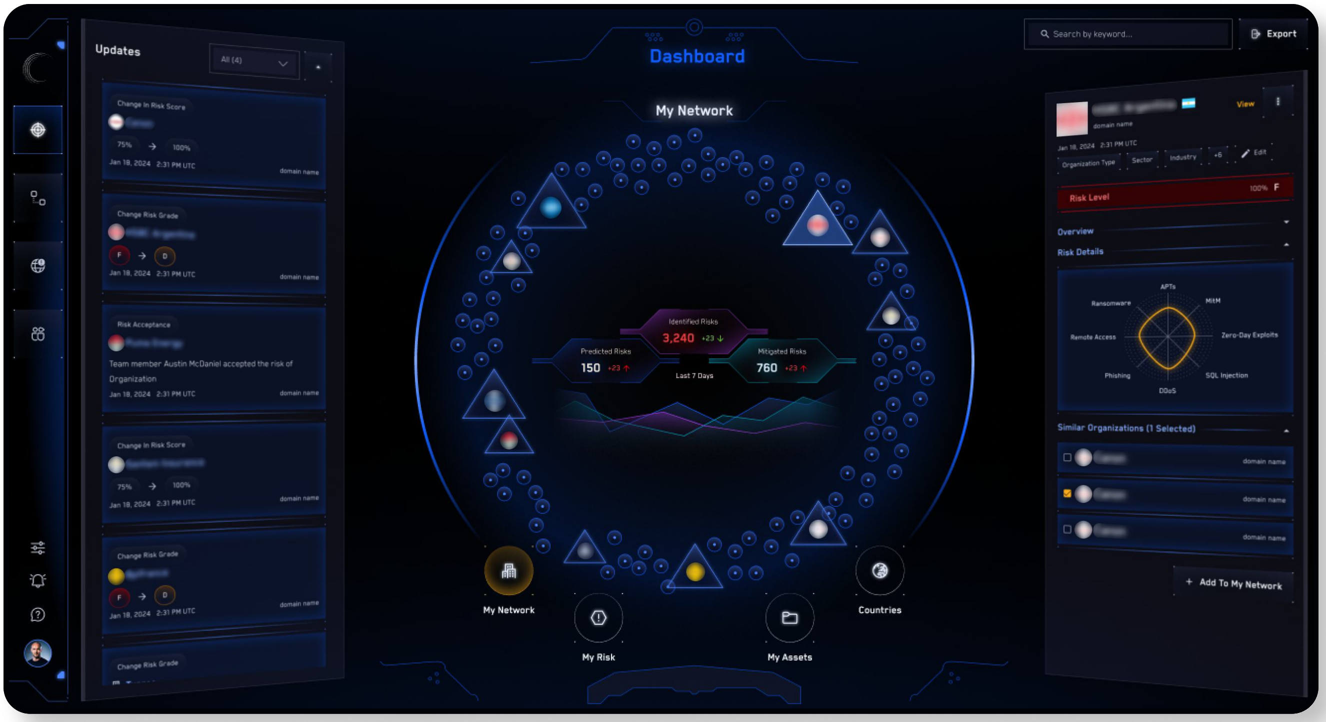
WHAT WAS THE PROBLEM?

In November 2023, the news became public: The library was targeted in a complex cyberattack that resulted in a **complete fall of the computing infrastructure** for the entire institution. The cybercriminals published some of the stolen data on the dark web, including personal user information.

The Library itself became aware of the attack on October 28, 2023, when the Library network turned out to be impossible to access. The attack, claimed by the **Rhysida ransomware group**, crippled the institution by **exfiltrating, encrypting and destroying** substantial data. Over 600GB of data has been put up for auction and illegally shared on the dark web. Months later, the Library has been continuing its process to rebuild the infrastructure, noting that the majority of its former systems and services cannot be used as they were.

WHAT DID BLINDSPOT DETECT?

Our risk intelligence platform, BLINDSPOT, detected an infection incident at the end of October 2023 that was already attributed to the threat actor known as **Vice Society/ Rhysida**. The ransomware group infected the institution with **SystemBC** malware. Additionally, on October 31st by 6:41 am **QBot** (commonly used as a delivery mechanism for ransomware payloads) compromised the library's account. With the first alert, BLINDSPOT was already displaying **a possibility of other related infections** upon this incident due to the nature of malware used in this attack



Team member Austin McDaniel accepted the risk of Organization

It's important to note that BLINDSPOT has already detected a few infection incidents dating back to July and September of the same year, which were conducted by the threat actor **Wazawaka**. Although these incidents don't seem to be intertwined in this specific case, prior infection incidents and the complex nature of cybercrime gang affiliations often serve as **precursor events** to a more serious cyberattack in the later stages.

In the end, a BLINDSPOT's early notification that the threat actor might deploy a ransomware strain to the victim's infrastructure proved to be correct when the attack turned into a full-blown ransomware case.

HOW COULD IT HAVE PLAYED OUT?

Had the Library been aware of the first infection incidents leading to the encryption and exfiltration of their data, it **could have prevented a ransomware incident** of such a scale. With the actionable time and mitigation recommendations offered by the platform, the Library could have had a major advantage in **predicting and intercepting the next moves** of the Rhysida/Vice Society ransomware group.

In line with the Library's official list of lessons learned from the incident, collaborating with sector peers to stay informed about common threats is highly advised. However, being able to know their adversaries and **implement adequate risk intelligence solutions** is a must.

Incorporating proactive risk intelligence systems to prevent similar scenarios becomes a key recommendation in protecting the institution and the whole supply chain.

Since 2012, PRODAFT has been redefining the approach to proactive threat intelligence. We developed BLINDSPOT, a risk management platform that supplies organizations with intelligence based on facts and real-time incidents, to help them fight against the global surge of supply chain cyberattacks. BLINDSPOT gives companies an overview of their adversaries and never-seen-before observables right from the infrastructures of cybercriminals, actively allowing them to stay one step ahead.

Organizations can save millions of dollars by proactively safeguarding their digital assets and supply chain. An early warning system provides them with an actionable time to mitigate the risks before they can turn into a full-scale cyberattack. Our use cases show that this time can range from weeks to months of extra time, depending on the current stage of cyberattacks and how fast the cybercriminals are moving.