CYLANCE

CASE STUDY FINANCIAL SERVICES

HBOR Takes on Cybersecurity

INDUSTRY
Financial Services

ENVIRONMENT
- 500 endpoints

CHALLENGES
- Incumbent antivirus solution not effective

SOLUTION
- Deploy CylancePROTECT® to detect and prevent malware, including ransomware, from executing in real time
- Retain ThreatZERO™ Services to optimize and operationalize CylancePROTECT

HBOR

The Company

The Croatian Bank of Reconstruction and Development (HBOR) is a development and export bank, owned by the Republic of Croatia. The institution primarily finances projects that bolster the Croatian economy. Through its operations, HBOR supports systematic, sustainable, and balanced economic and social development. When developing finance programs and special loan terms and conditions, as well as when establishing target groups, HBOR takes into account balanced and sustainable social development and environmental protection. HBOR is aware of multiple influences they have on their clients, partners, and wider community as a financial institution, and is aware of expectations that stakeholders have concerning HBOR. HBOR was founded in 1992 and employs around 350 people across three locations in Zagreb and five regional offices.

The Situation

By March of 2017, Croatia had become the second largest target in the world for ransomware attacks.

Ivan Kovač, Data Protection Officer and CISO at HBOR said, "I knew our existing endpoint protection wasn't keeping up with the detection rate required. . . Our testing confirmed that our endpoint security solution could not prevent attacks. We knew a single endpoint detection failure could be disastrous."

"We are at 100% threat and device protection now, and generally forget about it, which is good! It should be like that!" **— Ivan Kovač, Data Protection Officer and CISO**

HBOR uses Infrastructure as a Service (IaaS), which eliminates the need for on-site hardware except for endpoint devices. Employees access their email and applications on bank-issued devices from anywhere. The device-heavy nature of HBOR's operations motivated the bank to place special emphasis on endpoint security.

The Process

Ivan and his team attended an Infosecurity Europe Conference, seeking the best endpoint security solution. The HBOR attendees met with Cylance® and discussed using artificial intelligence to detect unknown malware. "When we understood the logic of how Cylance works and that it could stop ransomware, we realized it was something we needed at HBOR," Ivan said.

HBOR requires that every potential product go through a proof of concept (POC) evaluation. "I was not happy with the third-party antivirus product tests I found online. I wanted to test for myself and see how the solutions would perform on our machines," Ivan said. The bank defined their critical security requirements then put five competitors to the test.

Ivan gathered 600 samples of zero-day malware for the test environment. The testbed also incorporated 10 ransomware samples, including Petya. CylancePROTECT was one of only two solutions capable of stopping Petya during the POC process. Ivan said, "Based on the solution's performance and the partner relationship, we selected Cylance and are very happy with our decision."

The Results

After selecting CylancePROTECT, HBOR saw other banks and institutions fall victim to an outbreak of WannaCry ransomware. Thanks to the forward-thinking nature of Ivan and his security team, the bank was fully protected. According to Ivan, "Cylance gives us the confidence we need to let our executives know our endpoints are protected from ransomware and other zero-day threats."

HBOR is running CylancePROTECT in Auto Quarantine mode. According to Ivan, "The quarantine was full of great stuff we did not know existed. The solution found a lot of junk on the network, which helped us conduct a big clean up mission."

HBOR also benefits from the product's easy administration. According to Ivan, "We don't have a large security team, so it's a big plus that we can set it and forget it."

The greatest compliment HBOR can give their security solution lies in the numbers – the bank has suffered zero ransomware attacks since installing CylancePROTECT.

The Update — One Year Later

Cylance reached out to Ivan for an update on his experience with CylancePROTECT one year after its implementation at HBOR. He replied with a list of ways Cylance has improved their operations:

- Cylance and Microsoft System Center Endpoint Protection (SCEP) are running together seamlessly. Cylance's automated handling of threat alerts has allowed HBOR to fully automate the response process. Employees once dedicated to investigating SCEP alerts are now working on other projects.
- Cylance is included in the company's Windows 10 image and has deployed without issue.
- Infection rates on portable devices has dropped to zero. This produced considerable cost savings as employee time is no longer lost to evaluating, cleaning, or re-imaging infected machines.
- Simplified device control management allows admins to spend less time configuring user accounts and has led to a more secure environment.
- All devices have achieved 100% protected status, allowing HBOR security technicians to focus on other areas.

Ivan summed up his experience with Cylance by stating, "Cylance is exactly what we needed – silent powerful protection working reliably below radar and without usual user alert or administrative fuss. It is not only the cost in money terms, but less time and better peace of mind amongst us security staff and our superiors. We are confident we do the best we can in endpoint protection now."

HBOR has shown its confidence in Cylance by renewing its contract with an increase in the number of licenses to cover all new employee endpoints.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

20181011-1804