COLORTOKENS

Online Deal Company Selects ColorTokens to Combat Ransomware and Achieve Cyber Resilience

Industry

Online Advertising and Marketing

Location

The Netherlands

Key Challenges

- A cybercriminal placed ransomware on multiple servers, targeting 30 GB of sensitive data
- Lack of visibility into IT networks led to difficulty in investigating and containing the breach
- Multiple open ports and servers were vulnerable to cyberattacks
- Weak firewall rules created security vulnerabilities

“ColorTokens helped us contain and eradicate ransomware effectively. The IT team deployed the solution in minutes and we immediately got visibility into our entire IT network. Our operations went online and were back to normal in no time. Their Threat Hunting capabilities provided us with deep incident analysis that helped us take timely measures to secure our networks. With ColorTokens’ solutions, we have now adopted a proactive approach towards cybersecurity.”

- Co-founder

Based in Amsterdam, the customer is an online deals company focused on providing end customers the best daily deals in their city of residence. Each day, subscribers are presented recommended deals from the most popular and prominent businesses including hotels, food & delivery, wellness, courses, and workshops among other services, in more than 90 locations across Europe including Belgium, Germany, and the Netherlands.

The customer stores all of its data in 135 autoscaling servers in AWS cloud. In addition, the customer has more than 150 endpoints across multiple locations to enable remote work for employees.

The Challenge

The customer suffered a ransomware attack that struck remote machines, development servers, and an AWS environment. The breach targeted more than a million offer codes and related details, as well as customer Personal Identifiable Information (PII) and client sensitive data. It was observed that an AWS Linux server was executing suspicious curl requests to publicly expose confidential data.

Because of weak firewall rules, the customer was unable to protect critical data retention systems from unauthorized access. The customer’s security team became aware of the breach when the attacker demanded ransom with a threat to publish the sensitive data on the internet.

While the customer wanted to contain the breach and minimize the damage, they also wanted to achieve cyber resilience and take a proactive approach towards securing against future cyberattacks.

The Solution

After the attack, the customer immediately swung into action and wanted a deep analysis of what had happened. ColorTokens, along with its partner Nixu Corporation, deployed a three-tiered approach to contain the ransomware attack and protect critical assets.

- ColorTokens was instrumental in stopping the breach by safely bringing down the servers, applications, and networks to prevent further damage, and segmenting them to isolate critical assets and data
- ColorTokens also immediately deployed agents on all endpoints and enforced rules to lockdown and stop any further damage
- These two steps were successfully completed before the cybercriminal executed the ransomware, enabling the customer to avoid significant damage

Business Benefits

- Just-in-time threat investigation and solution deployments ensured business continuity
- The solution prevented 30 GB of data exfiltration from exposed servers
- Micro-segmentation policies blocked more than 10 unwanted applications from executing

ColorTokens Solution Stack

- ColorTokens Xshield for Workload Visibility and Protection
- ColorTokens Xprotect for Endpoint Protection
- ColorTokens Managed Services

“ColorTokens was quick to respond to the customer need. They immediately went into action, and together we successfully stopped the damage and removed ransomware from all servers and systems. The solution is comprehensive yet simple to use, we deployed the lightweight agents with minimal training. ColorTokens is our trusted partner when it comes to providing cybersecurity solutions.”

- Robert Stoot, Sales Manager, Nixu Corporation

Xshield Visualization and Micro-Segmentation

ColorTokens ultra lightweight agents were deployed on AWS servers and endpoints to provide granular visibility into network traffic, application workloads, and endpoints – all managed through a single dashboard. The visualization dashboard uncovered the attack path, as well as unwarranted open ports and misconfigurations in applications, operating systems, firewalls, and VLAN asset control lists. Micro-segmentation policies were then created and enforced within minutes to prevent lateral movement with the help of a dynamic policy engine.

Xshield’s security policies were defined and enforced at the user, role, and department levels – regardless of the geolocation – to support remote employees.

Xprotect Proactive Security for Endpoints

ColorTokens Xprotect delivered highly granular security controls to restrict unauthorized access to endpoints and USB sticks. With Xprotect, the customer implemented proactive security by enabling dynamic whitelisting for endpoints (Mac, Linux, Windows), local and remote workers, and AWS auto-scaling servers (Amazon Linux 2). Coupled with Xshield micro-segmentation, this proactive security approach helped create a Zero Trust posture, where access is granted on role-based credentials, and not locations or specific hardware.

Continuous Threat Hunting and Monitoring

ColorTokens’ Threat Monitoring Services helped the partner and customer unearth security gaps, open ports, and attack paths. ColorTokens cybersecurity experts provided threat monitoring reports that helped the customer visualize the chain of events and investigate threat behavior.

Results & Benefits

ColorTokens’ just-in-time analysis of the attack, workload micro-segmentation, and endpoint lockdowns saved the customer from paying the large ransom the attackers demanded and ensured business continuity. The customer realized rapid time-to-value with ColorTokens’ solution set, protecting both their corporate networks and database servers hosted on AWS cloud which store the mission-critical data. The customer also implemented proper security and access controls to prevent the attacker from exfiltrating 30 GB from a server that was exposed to the internet. In addition, ColorTokens’ micro-segmentation policies stopped more than 10 potentially unwanted applications from executing.

In a moment of extreme stress, ColorTokens provided the customer a solution that was intuitive in design, easily deployed and scalable, automated, and streamlined when it comes to policy orchestration. It also provided a comprehensive audit trail, allowing around-the-clock coverage and a clear view into who was doing what, across both the internal network and in AWS cloud.