CASE STUDY

Europol and Security Leaders Declare War on Ransomware

Barracuda and AWS Keep NoMoreRansom.org Safe Despite Thousands of Attacks

In the summer of 2016, a unique coalition was formed to address the rapid growth of cybercrime conducted through the use of ransomware. Spearheaded by Europol's European Cybercrime Centre, Dutch Police, Kaspersky, and Intel security, the goal of the No More Ransom Coalition is to provide a central, public repository of knowledge and resources to help individuals and organizations fight ransomware.

Authorities estimate global losses from ransomware at more than $200 billion for 2016. In order to fight back, No More Ransom provides an online source of information about the latest ransomware variants, including decryption keys that have worked to retrieve files encrypted in previous attacks.

In less than a year, more than 80 partners from public and private sectors have joined the coalition, a number that keeps growing every month and shows the global commitment to fight ransomware together.

The Decision to Use AWS

A key part of the No More Ransom website is an application that analyzes user-submitted samples in order to identify particular strains of ransomware. The site also hosts an ever-growing database of decryption keys that may be able to retrieve visitors' encrypted files without paying ransom, and directs users to the most likely ones to use. Finally, it aims to educate people around the world about the dangers of ransomware and ways to recognize and avoid it.

The No More Ransom coalition understood that the site they intended to launch would be an instant and irresistible target for cyber attackers, making security a prime concern. Cybercriminals would like nothing better than to compromise a site designed specifically to combat them, and to use it to infect visitors with malware.

Amazon Web Services (AWS) was approached by the No More Ransom coalition in order to provide hosting and security to the project. AWS agreed to collaborate in the initiative offering maximum agility and flexibility. Along with the best possible baseline security, Amazon integrated its native security with best-of-breed application security using Barracuda CloudGen WAF.

"NO MORE RANSOM," A COALITION

- Dutch High Tech Crime police
- Europol's Cybercrime Centre
- A growing number of cyber security companies

WWW.NOMORERANSOM.ORG

- Hosted on Amazon Web Services (AWS)
- Protected by Barracuda CloudGen WAF for AWS

CHALLENGE

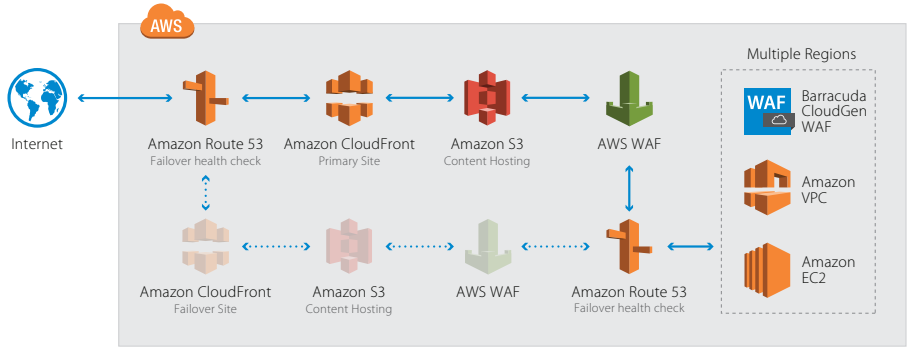
Create an online resource center for cybercrime victims, and keep it secure against inevitable attacks.

SOLUTION

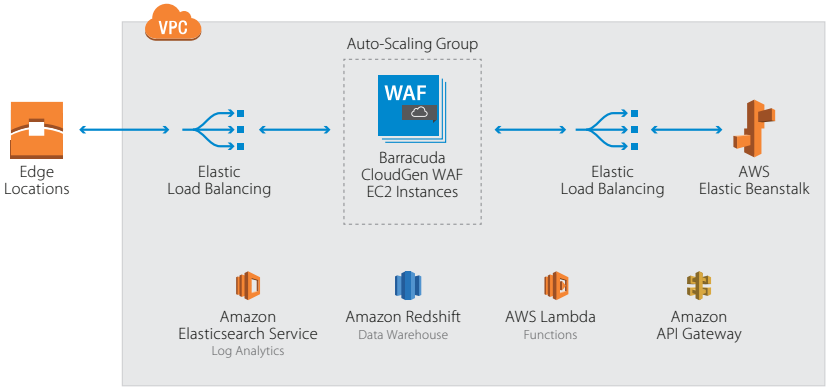
Layer native AWS security with Barracuda CloudGen WAF to ensure complete security.

RESULTS

51,000 attacks blocked within days of launch, and more than 1 million VPN-based attack requests identified and blocked to date. NoMoreRansom.org has never been taken down by cyber attackers.



NoMoreRansom.org Edge Architecture



NoMoreRansom.org Regional Architecture

Agility and Security

The flexibility and security provided by Barracuda CloudGen WAF for AWS was key for the success of the project. From the moment the No More Ransom site went live, the number of visitors coming to the portal went beyond any predictions.

AWS made it easy to adjust resources to meet the unexpected demand—and Barracuda CloudGen WAF automatically scaled to secure additional instances as they spun up—without affecting performance.

A Great Big Target for Cybercriminals

To the surprise of no one, the No More Ransom site came under attack as soon as it went live. Within days, Barracuda CloudGen WAF had blocked more than 51,000 attacks, ranging from standard DDoS attacks to more exotic and sophisticated attacks on portions of the infrastructure.

Even attack requests that go through VPN systems to mask their true nature—more than a million and counting—have been successfully identified and blocked.

Despite this nonstop barrage of attacks—and despite the huge numbers of legitimate visitors—the No More Ransom site continues to operate smoothly, and has never been brought down by attackers.

ABOUT CLOUDGEN WAF

The Barracuda CloudGen WAF blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target the applications hosted on web servers and the sensitive or confidential data to which they have access. Placed between the Internet and web servers, the Barracuda CloudGen WAF scans all inbound web traffic to block attacks and scans outbound traffic, providing highly effective data loss prevention.

Rajesh Mani, Chief Technology Officer for Intel Security, adds, “AWS have been absolutely critical for us…. It wasn’t just their security posture, but in addition to that it was their understanding of the bigger picture. We had 2 individuals working around the clock to get the site up, but it continues to remain up. That level of attention to detail was really quite comforting to us.”

“No More Ransom is the best example of Public Private Partnership I have seen to date, with key industry partners bringing their individual skills to a not for profit initiative that has made a real difference to protecting people and businesses online. The professionalism of these companies and their ability to deliver was integral to the success of the project.”

Steven Wilson
Head of European Cybercrime Centre, Europol

Ongoing Protection

The No More Ransom initiative has been successful in bringing together law enforcement and cyber security resources and information to help individuals and organizations around the globe fight back against ransomware. Going forward, the website database will continue to grow, and in all likelihood will acquire more sophisticated public-facing applications.

Throughout the process of developing and launching new applications and capabilities, Barracuda CloudGen WAF will continue protecting the No More Ransom website. Regular and on-demand vulnerability scans will make it simple to protect users while working to improve their experience in the fight against ransomware crime.

For additional information on the technology protecting No More Ransom visit https://www.barracuda.com/programs/aws/application-security.

ABOUT AWS

For 11 years, Amazon Web Services has been the world’s most comprehensive and broadly adopted cloud platform. AWS offers over 100 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 42 Availability Zones (AZs) across 16 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, Singapore, and India. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit http://aws.amazon.com.

ABOUT BARRACUDA NETWORKS, INC.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data, regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda’s customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.