CYBERFEED PREVENTING CYBER-THREATS MENACING A FINANCIAL INSTITUTION

anubisnetworks™ a BITSIGHT company

COMPANY CASE STUDY

FINANCIAL SECTOR

One of the largest financial Banks in Italy with a solid background in international financial services for individuals and organizations.

OBJECTIVE

Cyber-attacks against the banking industry have soared in the last few years. Financial institutions now face more direct and indirect attacks than any other industry: not only direct malware to banking systems, but also banking credentials stolen from its customers, and brand abuse / phishing that attempts to impersonate the bank's corporate identity.

After setting up a state-of-the-art SOC (Security Operations Center) service, this financial institution realized the limitations of having only internal events monitoring on top of the security systems, on the perimeter and endpoints. They needed to have high-quality and actionable information that could be immediately correlated with the internal events the SOC was already collecting.

The Security Operations global center, tasked with handling the incident response of the Bank and all its subsidiaries, wanted to respond to all threats as quickly and accurately as possible.

This bank looked for an external source of intelligence able to provide evidence of Infections and Compromised systems on a global scale.

CUSTOMER SOLUTION

AnubisNetworks Threat Intelligence solution, Cyberfeed, enabled this SOC to improve their incident response times.

Cyberfeed empowered this financial institution to actively monitor its environment, and gain intelligence on top level performance metrics on the entire institution down to subsidiary networks, and also provided real-time alerts, allowing it to not only identify the location of an infection within a company's infrastructure, down to the country and subsidiary level, but also necessary details to remediate the infection.

This SOCs can now easily tag events (new, acknowledged, and archived) to better prioritize infections on the organization's network.

"Cyberfeed can effectively respond following the discovery of a cyber-attack, leading to a major effect on the resultant impact, since the detection is very fast."

Bank's SOC Director

anubisnetworks™ a BITSIGHT company

BUSINESS BENEFITS

By implementing AnubisNetworks actionable threat intelligence solution, Cyberfeed, this Bank is now able to obtain real-time security data feeds via API access and combine them in their SIEM, for an augmented and faster vision on the threat landscape, such as botnets per example.

Through the use of Cyberfeed it's now possible for this Bank to detect of devices and machines related to information stealing Trojans, identify of possible phishing campaigns and brand abuse scenarios on customer networks, identify messages being flagged as SPAM and brand abuse campaigns, among other benefits.

Because the intelligence provided by Cyberfeed is from AnubisNetworks' own worldwide network of sensors and infrastructure, this bank raised its visibility over certain types of botnets which before were untraceable thus protecting more systems. Accordingly with this Bank's SOC Director: "Because banks and financial firms have very large and sophisticated systems, this means that end-to-end security is notoriously difficult. However, Cyberfeed can effectively respond following the discovery of a cyber-attack, leading to a major effect on the resultant impact, since the detection is very fast."

HOW CAN ANUBISNETWORKS PLAY A ROLE?

AnubisNetworks is a Cybersecurity Company specialized in real-time threat Intelligence, and with an established reputation for delivering innovative and effective solutions. AnubisNetworks solutions are fitted for service providers, risk and security organizations, telcos, major banks, National CERTs, Defense and Homeland Security, looking for real-time Insight on Infections and Vulnerabilities.

WHY CHOOSE CYBERFEED?

Cyberfeed provides a unique view in the early detection of cyber-threats. The combination of real-time, normalized security events with verified and contextualized data empowers Cyber Security Organizations and Business units to have a new and powerful approach to fighting cyber threats rapidly.

Cyberfeed is available through a real-time API with connectors to all major SIEMs, and as Cyberfeed Portal, the operational platform for CERTs, MSSPs, Homeland and Defense, and SOCs for the major companies. The Portal provides historical abilities, portfolio management, real-time alerts, business reporting, and incident handling.

With more than 25 000 events per second collected and streamed to security feeds as they happen, Cyberfeed's proprietary Threat Intelligence is focused on Detection of Infected Systems, from the network, on Email Malware, Spam, and phishing detection, on Malware and Website analysis, and on Information in the wild captured in Social forums.

FOR MORE INFORMATION ABOUT CYBERFEED, PLEASE VISIT OUR WEBSITE @ HTTP://WWW.ANUBISNETWORKS.COM

FOLLOW US

twitter.com/anubisnetworks

linkedin.com/company/anubisnetworks

youtube.com/user/anubisnetworks

CONTACTS

PORTO
UPTEC, Rua Alfredo Allen 455/461,
Sala EC.3.12, 4200-135 Porto, Portugal

Phone: +351 220 993 873

LISBON
Av. D. João II, Lote 1.07.2.1, 4th Floor, Parque das Nações, 1998-014, Lisbon, Portugal

Phone: +351 217 252 110

BOSTON
125 CambridgePark Drive Suite 204, Cambridge, MA 02140

Phone: +1 617 245 0469

anubisnetworks™ a BITSIGHT company