CYBERFEED
EMPOWERING SECURITY TEAMS TO QUICKLY REACT AND MITIGATE RISK

anubisnetworks™
a BITSIGHT company

CASE STUDY

COMPANY / OVERVIEW

This enterprise is a global leading Energy company (gas and electricity), being one of the most important producer of wind energy. AnubisNetworks' actionable Threat Intelligence is consumed by this company's SOC (Security Operations Center) team, which is primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cyber security incidents.

CHALLENGE

The company has an important international presence in the Energy and Utilities sector. It possesses critical infrastructure, which represent high value targets to cyber criminals, state sponsored hackers, and environmental hacktivists.

For this reason, the company wanted to ensure its own cyber security posture was highly reliable, comprehensive, and able to quickly adapt to cyber threats as they occur.

The company's Information Security and IT Risk Director was searching for increased cyber intelligence on the company network. In addition, the client wanted better awareness of performance across the Energy sector and a countrywide threat landscape. Understanding these threat perspectives, enriched with actionable data on infected networks, botnet activity, and systems exposed to vulnerabilities are a key initiative for the client. In addition, any new technology or intelligence needs to be compatible with their other systems - namely their SIEM. This company centralizes all security events at this infrastructure, for Incident Response Operations.

SOLUTION

By implementing AnubisNetworks' Threat Intelligence solution, Cyberfeed, this company was able to consume real-time security data feeds in three ways:

- API – directly querying the real time API for events;
- Live analytics Dashboard – for providing KPIs on the live traffic;
- API Connectors – For integration with the SIEM;

In this particular case, the customizable data feeds to which the enterprise subscribed were those which enable the detection of devices and machines infected with information stealing malware.

By using Cyberfeed, this company's security decision makers can now access critical Threat Intelligence insights, receiving rich context about the threat, and delivering historical and real-time reporting and notification for a quicker mitigation and efficiency. It's now possible for this company to:

- Understand the correlation of different attack vectors (e.g. Spam and Botnet Infections), in real-time;
- Decipher the campaign method and propagation stages;
- Obtain qualified insight and unique intelligence about the threat, for example the Communication payload of the malware;
- Avoid mistakes with a very low false positive rate;
- Analyze a 6 months historical view of the threat landscape.

BUSINESS BENEFITS

This company is now empowered to better detect and respond to vulnerabilities, malware and compromised systems after the adoption of the SaaS-based Cyberfeed solution. An added benefit is the ability to augment data within other platforms, such as the client's SIEM platform, and to help identify forgotten machines in their IT infrastructure.
In summary, the client identified three key differentiators of the Cyberfeed platform that enabled them to address their business needs:

- Contextualized information regarding compromised machines within their infrastructure; information that was previously unknown, putting them at risk;
- Institutional competence, efficiency and unique knowledge concerning threat intelligence subject-matter and data collection);
- AnubisNetworks' strong reputation in the market as a leading provider in Threat Intelligence related to Infected Systems.

"Cyberfeed has bolstered our ability to detect both network infections and compromised machines within our infrastructure that other best of breed security tools have missed. By assisting with the tactical remediation of issues we are more prepared to present a positive image of security to our leadership. Overall, we are very satisfied with the performance of Cyberfeed to date."

IT Risk Director

HOW CAN ANUBISNETWORKS PLAY A ROLE?

AnubisNetworks is an IT Security Company specialized in real-time threat Intelligence for B2B. With an established reputation for delivering innovative and effective solutions, AnubisNetworks has worked with multiple service providers, risk and security organizations, telcos, major banks, media groups and large corporations delivering Real Security in Real-Time against Real Threats.

WHY CHOOSE CYBERFEED?

Cyberfeed provides a unique view in the early detection of cyber-threats. The combination of real-time security events on actual incidents, context, and "smart eyeballs" empowers organizations and government agencies to have a new and powerful approach to fighting cybercrime. **What makes Cyberfeed stand out?**

1. More than 25 000 events per second collected and **streamed** to security feeds as they happen.
2. Provides **real-time** data on cyber-attacks, allowing organizations to mitigate risks as they arise.
3. Since the information is processed in real-time, users do not need to invest in data storage, making this a **lean and very light** service.
4. Turning data into actionable **intelligence** is the cornerstone of Cyberfeed. Events collected from disparate sources, including botnets only tracked by AnubisNetworks, are transformed and enriched into meaningful knowledge to help stop cyber threats and attacks.
5. It **dynamically** provides full context of what is happening and not a snapshot of the past, enabling cybersecurity analysts to obtain increased visibility into a situation and allowing informed decision-making.
6. Cyberfeed API **flexibility** allows customizing and processing data feeds in real-time, including measuring, filtering and de-duplicating events on the fly. Cybersecurity analysts can slice and dice data to better fit their requirements and build the necessary knowledge to stop threats.

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

FOLLOW US IN

twitter.com/anubisnetworks | **linkedin.com/**company/anubisnetworks | **youtube.com/**user/anubisnetworks

CONTACTS

PORTO
Address
UPTEC, Rua Alfredo Allen 455/461,
Sala EC.3.12, 4200-135 Porto, Portugal
Phone: +351 220 993 873

LISBON
Address
Av. D. João II, Lote 1.07.2.1, 4th Floor, Parque das Nações, 1998-014, Lisbon, Portugal
Phone: +351 217 252 110

BOSTON
Address
125 CambridgePark Drive
Suite 204, Cambridge, MA 02140l
Phone: +1 617 245 0469

anubisnetworks™ a BITSIGHT company