

↘ CASE STUDY

COMPANY / OVERVIEW

A Managed Security Service Provide (MSSP) based in the United States covering over 20 different industries including financial, healthcare, energy, among others.

CHALLENGE

This company is committed to stopping and preventing cybercrime by delivering a vast range of cyber security services to its customers. The cornerstone of their approach relies on the combination of the best available technology with great human analysis, ensuring their customer safety against cyber threats by covering, in real-time, different attack vectors and mapping malware campaigns.

To complement their current offer and continuous effort to provide the most advance cyber security solutions, this organization is always looking for different sources of actionable threat intelligence to gain a richer insight which will enable them to rapid breach detection and containment of threats thus mitigating their customers risk and exposure to data breaches.

SOLUTION

By implementing AnubisNetworks actionable threat intelligence solution, Cyberfeed, this MSSP was able to obtain real-time security data feeds via API access, a live dashboard and plugins to its SIEM system (SPLUNK). In this particular case, the customizable data feeds that were subscribed were

those which enable the detection of devices and machines related to information stealing Trojans.

By using the Trojans security feed, this MSSP can now help its customers to:



Detect networks and devices compromised with persistent or new malware families;



Understand malware landscape at the company, network, local, country level;



Track botnet behavior, growth, dispersion and lifetime;



Intercepts and monitors all communications between the malware and C&C server;



Ability to define business rules to query communication data details between compromised devices and C&C.

“Having access to real-time, actionable information about the compromised machines and the type of malware we were facing was central in stopping the threat. For our business, Cyberfeed has proved to be an actionable, valuable, and reliable threat intelligence solution. The master key against Cyber threats.”

BUSINESS BENEFITS

When contacted by one of their customers that manage a pro stadium concerning fears of having being breached, this MSSP used Cyberfeed to pinpoint the compromised

machines allowing for a quick response and stopping criminals from gaining control over the stadium systems and security.

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

- 5 and enriched into meaningful knowledge to help stop cyber threats and attacks.
- 6 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](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 02140I
Phone: +1 617 245 0469

