THREAT SHARING

Use Cases

keepnet LABS

WWW.KEEPNETLABS.COM
INFO@KEEPNETLABS.COM

Table of Contents

Introduction

What is Threat Sharing?

Threat Sharing is a next generation platform that provides organisations with the ability to **share real-time email-threats anonymously within trusted community groups.** The platform acts as an early warning system deployed across a network of Keepnet members, and when coupled with Keepnet's Incident Responder, **automated investigation and response to protect an entire community becomes a reality.**

Organisations can expand their identification and alert capability by leveraging **the eyes in the community**, avoiding increased costs and reducing risk from email-based attack vectors.

With Threat Sharing in place, users will no longer need to directly identify a malicious attack to initiate inbox investigations, delivering **faster response times and proactive protection against otherwise unknown threats.**

1

Financial Services

A secure, resilient financial services sector plays a crucial role to a country, its economy and citizens. As a highly-prized target, this sector has a collective responsibility to prevent fraud and stop attacks against clients' accounts, the siphoning of money, stealing of sensitive data and many are bound by regulations to share physical and cybersecurity threat intelligence. The question is, how can financial services share the vast number of email attacks using technical automation?

Establishing a Threat Sharing private community and inviting those involved with financial services to join and share email-threats is a revolutionary step, i.e., sharing threats amongst organisations with vested interests in protecting their customer's data, financial information and systems, significantly reducing financial services risk.

Benefits For A Financial Organisation To Set Up A Private TS Community

- Immediate insight into threats faced by the community, and their associated risks to the organisation.
- Minimises threats through active awareness, monitors email threats targeting financial services
- Demonstrates inherence to additional compliance and FS-ISAC directives for data protection
- Establishes security by design, indicates to prospective partners how sternly security is taken
- Allows easily determine which providers are willing to adhere to security requirements of contracts when tendering

1

Financial Services

Benefits for other organisations to join and be members of a TS Community

- Become aware of attacks impacting other third parties in their sector and take preventative measures
- Add a new cost-effective layer of security to the organisation which they did not have before
- Gain increased confidence knowing that they will be joining a resilient network able to protect both themselves and their customers from attacks
- It ensures a more consistent response to threats
- Become able to prove that their incident alert processes are working and are a respected contributor

Benefits for the end customers of all parties

- The end customer data is better protected from risk of breach if the controllers and processors of their data are collaborating on threat intelligence and response.

2

Supply Chain Industry

Organisations care about the security of its supply chain as they often play a crucial role in providing services and processing data on behalf of the organisation. Third party due diligence is an important step in vetting these companies, but how can other controls be implemented to further reduce supply chain risk?

Establishing a Threat Sharing private community and inviting the supply chain to join and share email-threats will protect them. Sharing threats amongst companies will significantly reduce supply chain risk and the suppliers will become instantly stronger in terms of their cyber security posture.

Benefits for the organisation to set up a private TS community

- Enables an organisation to determine which suppliers are willing to adhere to security requirements of contracts when tendering
- Demonstrates customers that extra precautions are in place to protect their data
- Mitigates cyber attacks via proactive actions such as monitoring email threats at all times
- Establishes security by design proving easily to potential partners how seriously cyber security is taken

2

Supply Chain Industry

Benefits for the suppliers to join and be members of a private TS community

- Adds a new cost-effective layer of security to the organisation which they did not have before
- Increased confidence in the knowledge that they will be joining a resilient supply chain
- Suppliers become aware of attacks impacting other third parties in the supply chain and take preventative measures
- Able to prove that their incident alert processes are working and are a respected contributor

Benefits for the end customers of all parties to join and be members of a TS Community

- The end customer data is better protected from risk of breach if the controllers and processors of their data are collaborating on threat intelligence and response.

3

Critical National Infrastructure

A secure, resilient critical national infrastructure plays a crucial role in providing the core services such as telecommunications, utilities and mass transportation which are the backbone of a country. Such essential services are under attack from nation states who launch co-ordinated, well-planned highly sophisticated attacks often at a high level rather than from those by other malicious groups. The question is, how can organisations quickly share threat intelligence from email attacks with others who can then launch automated investigations and mitigate their own cyber risk?

Creating a Threat Sharing private community and inviting those involved with critical national infrastructure to join and share email-threats will be a great strength. Instant access to cyber security threats will considerably minimize the risk of breach on national infrastructure.

Benefits for the organisation to set up a private TS community

- By learning from each other, minimise risk of a critical breach through proactive awareness, monitoring of email threats targeting the critical national infrastructure
- It reduces the cost of detecting and preventing data breaches
- Demonstrate to their stakeholders that extra precautions are in place to protect their data
- Establishes security by design, indicates to potential partners how seriously security is taken
- Enables an organisation to determine which suppliers are willing to adhere to national security requirements of contracts when tendering

3

Critical National Infrastructure

Benefits for partners to join and be members of a TS Community

- Aware of attacks impacting other third parties in the critical national infrastructure and take preventative measures
- Adds a new cost-effective layer of security to the organisation which they did not have before
- Access to information on new and emerging threats and threat actors.
- It takes repetitive, time-consuming tasks out of the hands of humans
- Increased confidence in the knowledge that they will be joining a resilient critical national infrastructure
- Able to prove that their incident alert processes are working and are a respected contributor

Benefits for the end customers of all parties

- The end customer data is better protected from risk of breach if the controllers and processors of their data are collaborating on threat intelligence and response.

4

MSSPs (Managed Security Service Providers)

A managed security service provider (MSSP) plays a crucial role in providing organisations with services such as managed firewall, intrusion detection, virtual private network, vulnerability scanning and antiviral services. These are vital for organisations who are unable to provide their own security and so are solely responsible for many organisations' cyber defence making them key targets for hackers wishing to gain access. The question for MSSPs is, how to ensure that their centers are able to share threat intelligence rapidly and so stop their clients' data and information from being accessed by email attacks?

Creating a Threat Sharing private community for their clients and them to join and share email-threats will be a great opportunity for MSSPs. Their clients will benefit from being able to leverage their threat sharing capability of incident response. MSSPs will be able to demonstrate to potential clients that threat sharing is a service differentiator. Only by joining the MSSP are organisations able to take advantage of this threat sharing platform that mitigates the risk of successful email attacks.

Benefits for the organisation to set up a private TS community

- Minimise risk to their clients through active awareness and monitoring of email threats
- It improves the effectiveness of the incident response plan
- Demonstrate to their clients that extra precautions are in place to protect their data
- Able to differentiate themselves from other MSSP providers who do not offer threat sharing
- Establishes security by design, indicates to potential clients how seriously security is taken
- Helps enhance their brand reputation through the quality of their threat intelligence

4

MSSPs (Managed Security Service Providers)

Benefits for organisations to join and be members of a TS Community

- Aware of attacks impacting other third parties in their sector and take preventative measures
- The ability to track the ongoing activities of cyber-criminals and hacktivists specific to your industry.
- Able to post threats openly and securely within their community gaining kudos
- Adds a new cost-effective layer of security to the organisation which they did not have before
- Access to a network who are linked by a common interest to increase cyber resilience
- Increased confidence in the knowledge that they will be joining a resilient network able to protect their own data and that of their clients
- Able to prove that their incident alert processes are working

Benefits for the end customers of all parties

- The end customer data is better protected from risk of breach if the controllers and processors of their data are collaborating on threat intelligence and response.

5

Intelligence Sharing and Analysis Organizations (ISAOs)

An effective intelligence sharing community shares critical cyber threat intelligence and builds awareness to protect its members against cyber threats and increase their resilience. The members rely on an ISAO such as ISAC to provide services including threat assessments, alerts, and insights. The question for an ISAO is, how can they facilitate sharing with actionable automated response? Often by the time a member shares an email threat, days or weeks have gone by rendering the intelligence worthless should the attack have been well-planned and coordinated.

Establishing a Threat Sharing private community and inviting those involved with critical national infrastructure to join and share email-threats will extremely protect companies. Sharing threats amongst organisations in the community who are highly inclined to protect their customer's data and systems will significantly reduce cyber security threats to the ISAO's members.

Benefits for an ISAO to set up a private TS community

- It increases the accuracy of the organisation's threat intelligence
- Minimise risk of email threats through active awareness of its community
- Facilitates threat sharing among its community members to action automated response against email attacks
- Establishes security by design, indicates to potential members how seriously security is taken
- By offering a threat sharing solution, enhances its reputation in the intelligence community

5

Intelligence Sharing and Analysis Organizations (ISAOs)

Benefits for partners to join and be members of a TS Community at an ISAO

- Aware of attacks impacting other members in the community and take preventative measures
- Active intelligence for identifying and preventing security breaches.
- Adds a new cost-effective layer of security to the community and its members which they did not have before
- It reduces the cost of detecting and preventing data breaches
- Knowledge that they will be joining an ISAO with an threat intelligence sharing community with industry professionals as fellow members
- Able to prove that their incident alert processes are working and are a respected contributor

Benefits for the end customers of all parties

- The end customer data is better protected from risk of breach if the controllers and processors of their data are collaborating on threat intelligence and response.

6

Healthcare Industries

A secure, resilient healthcare system plays a crucial and critical role in protecting the health, well-being and lives of a country's citizens through a network of hospitals, trusts, medical centers, research bodies and drug companies. The question for this sector is, how can they start to share information about attacks and threats in a unified way that decreases the threat to patients' medical records, data and ultimately lives from email attacks?

Creating a Threat Sharing private community and inviting those working in healthcare to join and share email-threats. Sharing threats amongst organisations will significantly minimize the threats against them and will ensure the security of patient and customer data, medical research and systems.

Benefits for the organisation to set up a private TS community

- It improves the security posture of the organisation
- Minimise risk through active awareness, monitoring of email threats targeting healthcare
- Demonstrate to fellow medical professionals that extra precautions are in place to protect their data and that of their patients
- Establishes security by design, indicates to potential partners how seriously security is taken
- Enables an organisation to determine which suppliers are willing to adhere to security requirements of contracts when tendering

6

Healthcare Industries

Benefits for other organisations to join and be members of a TS Community

- Gaining insight into how vulnerable or otherwise the organization's current internet presence is.
- Aware of attacks impacting other third parties in healthcare and take preventative measures
- It enhances the timeline of incident response
- Adds a new cost-effective layer of security to the organisation which they did not have before
- Increased confidence in the knowledge that they will be joining a resilient network that protects both themselves and patients
- Able to prove that their incident alert processes are working and are a respected contributor

Benefits for the end customers of all parties

- The end customer/patient/research data and lives are better protected from risk of breach if the controllers and processors of their data are collaborating on threat intelligence and response.

About us

Keepnet Labs protects businesses throughout the full lifecycle of email-based cyber-attacks. We have developed a full spectrum suite of cyber-security defence, threat monitoring, security management and user awareness products that encapsulate an integrated approach to people, processes and technology thus reducing the threat in all areas of cyber risk. We are committed to continuous innovation and expansion of our suite of security products in order to meet the needs of a dynamic and rapidly growing networked population in a constantly evolving cyber-threat environment. Our cyber defence strategy adopts three holistic elements: people, process, and technology:

People: we focus on the "human factor", using engaging, structured, content to raise cyber awareness and engender "active defence" behaviours.

Process: we support the development and management of user security awareness plans, monitor user compliance and Key Performance Indicators and embed cybersecurity as an intrinsic part of the corporate culture.

Technology: we scan and isolate malicious attachments and email content and provide system administrators with "one-click" management across the enterprise.

Keepnet Labs improve overall organisational security posture and mitigate cyber-risk by;

- Real-time analysis and management of email-borne threats
- Threat simulation designed to test the organisations' security posture.
- The availability of timely threat intelligence
- Realistic, but safe, phishing simulation
- Supporting security awareness training programmes

Our internal corporate strategy creates a stimulating and innovative environment where the Keepnet team has the opportunity to continually enhance their skills and creativity while contributing to growth.