INSURANCE COMPANY CASE STUDY

RAPID PII IDENTIFICATION/ CYBER-SECURITY ASSESSMENT

facebook/Heurekasoftware

twitter/Heurekasoftware

1382 W 9th St #410, Cleveland, OH 44113
888.968.7199
info@heurekasoftware.com

CLIENT BACKGROUND:

Insurance provider that offers a comprehensive and competitively priced portfolio of personal, farm, and commercial insurance products.

- Over 600 locations in the midwest
- Protecting over 170,000 households
- Rated A (Excellent) by A.M Best Company for 50+ years
- Over 250 associated and over 2,500 licensed agents

THEIR CHALLENGE:

There were two main challenges. The first involved the identification of PII information in unstructured data across the enterprise and the second was cyber-security and potential ransomware droppers.

The Reasons

- Lack of visibility about what PII information existed in unstructured data on employee computers
- No large-scale software specifically focused on PII identification
- Limited ability to find or remediate file risk.
- Lack of ability to easily scan endpoints for file-based IOC's (Indicators of Compromise)

What They Needed

- A cloud-based system to ensure security and allow for rapid, same- day deployment and automated updating capability
- Automatic PII detection for social security numbers, credit cards and bank routing information across all endpoints deployed
- A single risk dashboard showing instant feedback on endpoint risk
- Ability to create file or hash value groups in order to search enterprise wide for file intelligence

THE SOLUTION:

The client installed over 4,000 endpoints in a single day using off-the-shelf deployment methods. The installation consisted of laptop and desktop computers. This installation included the following:

- **A cloud-based system and UI** – Allows for rapid deployment (less than 2 minutes) and the ability to proactively manage endpoints, PII risk, view risk trends, create reports, conduct searches or take file action.

- **Heureka's automatic classification engine** – Our engine identifies specific PII such as social security numbers, credit card numbers and bank routing information.

- **Custom grouping capability** – Ability to create unique file name or hash groups for reuse and targeted searching based on acquired intelligence on indicators of compromise.

- **Custom search scheduling** – Ability to schedule searches for automatic daily, weekly, monthly runs.

RAPID ASSESSMENT:

In less than 48 hours Heureka indexed and classified over 10M files consisting of over 3TB of total size. Upon completion of the index and classification, the Heureka team in conjunction with the client created a data assessment report based on the common file types and presented the report back to the client.

10,000,000
Files Indexed and Classified in First 48 Hours

$650,475
Risk Identified From Unstructured Data

$450,000
Total PII Risk Reduction After Just Two Months

Heureka's Risk Assessment Report shows file counts containing SSN, Credit Cards and Bank Routing numbers. Duplicates were removed and the remaining files had a total breach value applied to them. The total potential risk cost beginning in October of 2018 was $650,475.

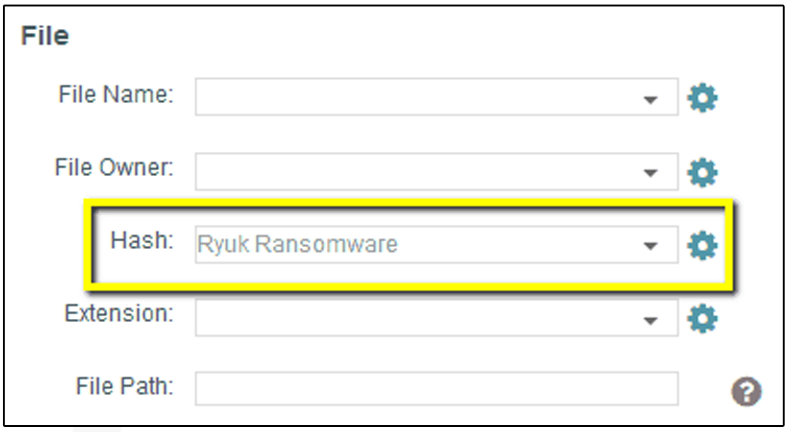
The next step for the client was to investigate risk based on the file data and then remediate files using Heureka's quarantine and delete tools. A repeat of the Assessment Report was performed two months later which showed a total PII risk reduction of over $450,000.

RAPID ASSESSMENT (CONTINUED):

Indicators of Compromise Searching (IOC)

The second concern for this client was Heureka's ability to search for specific indicators of compromise including file names and SHA-1 or MD5 hash values. IOC information obtained by this client consisted in part of either hash values or file names.

Heureka's indexing engine creates both MD5 and SHA-1 hash values for each and every file that it encounters. This client chose to index their endpoints at the root directory on each system thus providing potential intelligence to the point where malware or ransomware may live. Scheduled searches for malware packages were set up so that the system is sweeping for specific IOC's on a user-selected schedule.



File

File Name:	
File Owner:	
Hash:	Ryuk Ransomware
Extension:	
File Path:	

CONCLUSION:

In less than two days Heureka was installed and helped our client identify over $650,000 worth of potential risk. Our client was able to use Heureka Software to locate not only the risky files but the exact computer and file location for reporting and remediation.

Once files were identified as needing remediation, our client used Heureka's file delete and quarantine functions to reduce their overall potential risk by over **$450,000**.

Finally, our client uses Heureka's search capability to look for ransomware and malware packages via filename and hash groups and performs regularly scheduled hash and filename sweeps across all endpoints and using Heureka's quarantine or delete tools to remove potential threats before they cause harm.

REQUEST A DEMO

facebook/Heurekasoftware

twitter/Heurekasoftware

1382 W 9th St #410, Cleveland, OH 44113
888.968.7199
info@heurekasoftware.com