CASE STUDY:

INCIDENT RESPONSE

Building a timeline of events can simplify malware investigations

US ENERGY AND DEFENSE CORPORATION

US-based HQ with offices worldwide | 15,000+ employees | Privately-held

Corporations in the defense and energy sectors are rich with highly innovative and valuable IP are attractive targets for cybercrime and therefore potential data breaches. Malicious actors are often seeking highly sensitive and innovative IP that can be used for their own gain or sometimes sold to foreign governments.

THE CHALLENGE

Cyber attacks like network intrusions and data breaches are on the rise. In 2019, the average cost of a data breach was $3.92M.[1] Unfortunately, it's not necessarily a question of if a network intrusion will happen, but more appropriately when.

In fact, many data breaches go undetected for almost 6 months.[2] During this time, the network is under constant attack while bad actors research network behavior and user patterns to try take as much as they can. Piecing together evidence in an investigation that spans several months can be an arduous task, even for seasoned investigators.

The Incident Response process is mission-critical for many organizations to safeguard themselves from cybercrime. And one of the most important steps in that process is the Analysis phase.

When a data breach occurs, intimately understanding the security event—including its point of origin, what was done and how—is crucial to preventing future attacks but also for attempting to recover any stolen data.

> Timeline is a game changer for us! Using AXIOM Cyber's Timeline feature, we were able to identify what happened within the malware infection. Honestly, I don't think we would have found the details we were looking for if we were using another tool. We probably would have missed some of those events that we caught within the AXIOM Timeline.
>
> **— DFIR Analyst, Cybersecurity Threat Analysis Center**

[1] https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html

[2] https://www.ibm.com/security/data-breach

HOW AXIOM CYBER HELPS

REMOTE ACQUISTION

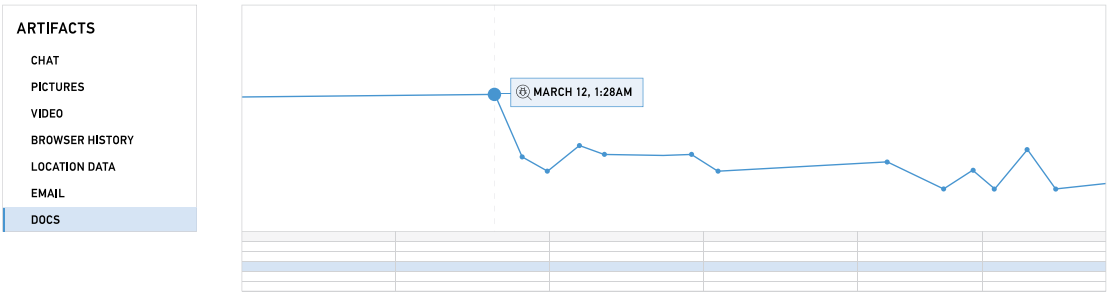
AXIOM Cyber has built-in remote acquisition capabilities from target endpoints enabling you to collect as much or as little evidence that you need:

1. Acquire drives, process memory, and logical files from the file system even if the drive is encrypted. You can download files and folders representing a logical image that contains all files and folders on the file system.
2. Targeted locations is a curated list of typical files and folders that you might want to download during a remote acquisition. Targeted locations include items from the default locations of the User, Desktop, Documents, and Downloads folders, Web browsing activity, registry files, event logs, Pagefile.sys, Swapfile.sys, and $MFT.
3. You can download drives representing a physical image of the drive. You can select and download individual partitions or the complete drive.

BUILD A TIMELINE OF EVENTS

Using AXIOM Cyber, you can quickly and easily track down malware using relative time filters that are applied to all timestamped evidence items including data from the file system, memory or even other sources like the cloud or mobile devices.

Since data breaches aren't necessarily immediately detected, being able to follow an artifact or a file throughout its entire journey can help lead your investigation to other relevant evidence items and quarantine any and all infected vectors faster.



SEE AXIOM CYBER IN ACTION FOR YOURSELF

If you'd like to learn more about Magnet AXIOM Cyber and how it can help you simplify your remote forensic investigations, visit magnetaxiomcyber.com. While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM Cyber expert, and request a free trial version.

Learn more at magnetforensics.com

Book a demo today, call us at 1-844-638-7884 or email sales@magnetforensics.com

MAGNET FORENSICS®