In Search of the Elusive Rogue Employee

Case #47: Mr. Dee Leet

Having been laid off by his previous employer, Mr. Dee Leet was determined to prove his worth to his current employer. Because he wasn't intentionally malicious, he was unaware of how unethical or even illegal his proof might be.

Whenever Dee finished a project, he did what most employees do: went on to the next one.

Unlike most employees, he waited until his co-workers had also moved on to their next projects. Then he'd creep back into the previous project folder and DELETE ALL his work. His reasoning was, "If they want that data, now they have to come to me."

He didn't view it as *stealing* his employer's data… no, he merely made it impossible to find the data without him. Perhaps a copy was in his desk drawer, or in his car, or at home – where he could claim it was off-site backup.

Usually any work done by an employee legally belongs to the employer who pays that employee. Dee didn't care for those laws. As far as he was concerned, if he did the work, it belonged to him. That data was his job security.

Who owns the data?

When an employee uploads onto his work laptop family pictures, house construction contract or medical exam records, who owns the files?
Who is responsible for file security?
Can the employee take them when leaving the company?

On the company file storage those questions are irrelevant, because all data belongs to the company. The company IT department is responsible for securing, regularly backing up, and testing restoration of the data.

It's normal to expect workers leaving the company will leave company files alone. You do not expect them to do whatever they want with company data.

Yet users like Dee Leet treat company data as if they own it. They copy complete folders, delete files, and store files wherever they think is convenient.

Can you prevent this kind of unrestrained file frenzy in your organization?
Without slowing and encumbering productivity?

And do so within budget?

Discover how easily you can protect your data with a single security guard

[Link to the following on its own page. Every story in the series will link to this page, so you can track the number of interested readers each story brings.]

Easily protect your data from inside and outside threats

Claim ownership of your data

From the moment it's installed, ITsMine Data Active Protection (DAP) protects your files, monitors traffic to file storage and uses a machine learning algorithm to daily map the hottest areas of a file share – from Red, through Yellow to Green.

Using this heatmap as a guide, ITsMine DAP focuses data protection efforts on red folders, educating users when they access red folders, monitoring the data use inside those folders, and protecting the folder content by planting *Software Mines™*.

Inquiring mines want to know

A *silver Software Mine™* is data that simulates real data, marked daily with a unique identity number (UIN) and planted automatically according to the heatmap. *Software Mines™* are real files, requiring no more than 5% of storage. Corporate data is not changed. Attackers cannot distinguish between real company data and *Software Mines™*.

External attackers are blocked when caught encrypting, deleting or changing *Software Mines™* or company data.

TOB swoops in to the rescue

Transparent, Obtain evidence and Block (*TOB™*) is a disposable agent installed on employee devices that access *Software Mines™* or behave suspiciously.

That's how ITsMine automatically caught and obtained evidence against Dee Leet in Case #47. [Link to Case #47 page]

A user is considered innocent until additional suspicious activity is recorded. When no additional action is recorded the severity level of the case is kept at 0, and after 24 hours *TOB™* deletes itself.

User education is key

Data security requires users be taught what behavior is expected towards company data and how that behavior is enforced.

Pre-Access education – ITsMine can show a popup to users accessing a red folder. While customers can change the wording to whatever they like, an example popup message is…

> “You are now entering an important area. You may access files that belong to you. Please keep in mind if you touch any files that do not belong to you, any action you take will be tracked and recorded.”

Post-Access education – Employee behavior determines the risk level of each case and what action *TOB*™ takes – block, educate or send clear evidence to security managers.

For example, if Dee Leet in Case #47 [link to # 47 page] deleted the *Software Mines*™ the popup message would read...

> Dear Dee Leet:
> We found you deleting files in a company folder that do not belong to you. That is prohibited according to company policy. Read the full policy here.
>
> Please avoid such activity in the future.
> Thank you,
> Al Wayson Guard, company security team

Problem-free regulatory compliance

ITsMine handles both rogue employee and external threats automatically. It provides gives high visibility on the most important asset – data – which eases compliance with regulations like HIPAA, GDPR, PCI and others.

Cyber security pros need not apply

When ITsMine is protecting your data, a security guard can watch for threats – just like the olden days, when human guards prevented file folders from walking out the door. The guard can investigate each case, obtain evidence, and contact HR or managers for more information about the user’s activity, or act on the employee’s endpoint.

You won’t need to hire an expensive information security professional, who because they are so rare, may spend a portion of his/her time reading job offers from your competitors.

ITsMine brings DLP into this millennium

About

ITsMine is a new solution founded and run by experienced Information Security professionals (link to Meet the Team page), who realized cyber security had to be simplified if it was going to meet new and existing threats.

They truly care about their customers, which is why they provide so much personalized service. Providing that level of service however, requires time.

If you have between 100 and 4,000 users and you'd like to find the elusive rogue employee *before* he ruins your organization, place yourself on the ITsMine waiting list (link to Contact page) and they'll contact you asap.