Third-party palooza – the Minus Touch

2018 Data Breach Digest

verizon✓

The situation

We handle a lot of forensic evidence at the VTRAC | Labs and process it quickly because the VTRAC | Investigative Response Team investigators eagerly awaits it, ready to pore over the system images and associated volatile data.

One Tuesday morning, the investigators were especially anxious. The start of a new investigation had been delayed because the customer's data was hosted at a co-location data center. They had to wait for the data center's "hands team" to connect hard drives to the in-scope servers for data collection.

Several days passed before the VTRAC investigators received a call that the imaging had completed. An additional day passed before they received a tracking number for the evidence shipment via courier.

Finally, we were notified that the evidence shipment had arrived. We retrieved the package from the courier, completed the chain-of-custody and inventory record, and connected the drive for staging. After connecting the drive, we found it contained no data!

So what happened?

Mitigation tips

- Keep an inventory of all assets; document and label systems in remote locations
- Maintain an updated contact list for any co-location services providers
- Test and validate Incident Response (IR) procedures; include co-location services providers

Investigative response

A few days prior, during the engagement scoping process, the VTRAC investigators learned the in-scope servers were housed in a co-location data center. We offered to send investigators onsite for collection. However, the co-location services provider, as a matter of policy, prohibited our access. We were forced to rely on their local team for collection.

Though generally simple, some co-location data centers are well-equipped to handle these requests while others struggle to coordinate with the folks on the ground. There's often no documented process to convey which servers need to have hard drives connected to them, or which physical appliance is hosting a virtual machine.

For this situation, the customer was sharing a physical system with other customers which could prevent the ability to image the drive at all due to commingled customer data.

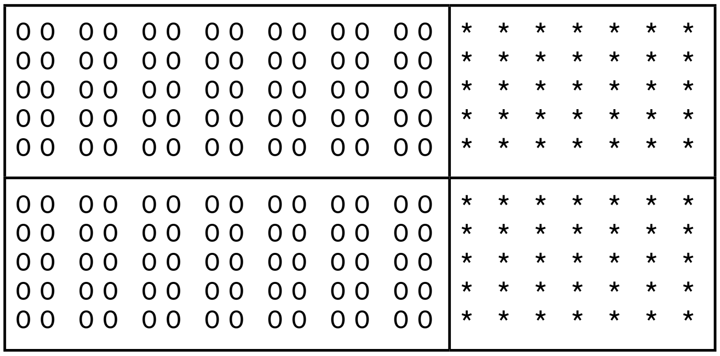
Co-location data center considerations

Accessing data in co-location data centers should be planned well ahead of time. Some of these investigative planning are:

- Know which co-location data center has the in-scope evidence. When using multiple co-location data centers, knowing exactly where your systems, memory, logs, and data is can reduce evidence collection and preservation time
- Know who does what. Not knowing who does what in a data breach causes confusion and wastes valuable resources. Consider using a RACI matrix for stakeholder tasks
- Know who can physically access the systems in the co-location data center. Working through authorization to gain access to your data storage during a cybersecurity incident introduces unnecessary delay
- Know how to and collect the data at the co-location data center. Understanding and testing the evidence collection process ahead of time reduces evidence collection acquisition delays

Response tips

- Integrate third-party contact procedures into the IR Plan; periodically test contact and escalation procedures prior to cybersecurity incidents occurring
- Use co-location services providers with first responders experienced in collecting digital evidence
- Require and validate co-location services providers allow access to digital evidence, to include systems and network logs, quickly



```
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
----------------------------------+---------------------
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
0 0  0 0  0 0  0 0  0 0  0 0  0 0 | *  *  *  *  *  *  *
```

Figure 1. “Zeroed-out” hard drive sectors

An additional day’s delay occurred when the co-location services provider requested that our customer provide the collection drives. This required our point of contact to scramble to arrange one-day shipping.

The customer reported no issues with the collection process or with the instructions for encrypting the collection drives prior to shipping to our labs. Still, when we mounted the evidence drives and discovered they were empty, we were shocked.

Typically, an encrypted drive presents itself in one of two ways. If an encrypted container has been used, the file is within the image. If the entire drive is encrypted, the Microsoft Windows operating system will indicate it must be initialized.

Another, less common situation involves one of multiple encrypted partitions, in which case the disk appears initialized but the data is not accessible. Neither thing occurred here.

Suspecting there might be a separate disk partition or some other encryption method involved, we examined the disk with one of our forensic tools. Unfortunately, the hard drive sectors only contained the hexadecimal character “00” which meant it housed no data. We immediately contacted our customer’s point-of-contact to figure out what happened.

Our contact explained that the person responsible for making the shipment initially claimed they’d followed our collection and shipping instructions. However, after some additional probing they admitted consolidating all the data on to a single drive. We never learned exactly why they did this but in doing so, they must have somehow not actually copied the data to the drive. The next day, we received the correct drives in evidence bags and with the chain-of-custody completed. This was a costly lesson as it took several days for the collection effort to begin. The hosting provider’s missteps in collecting the evidentiary data further delayed the commencement of our investigation and disrupted our customer’s business.

Lessons learned

During the engagement, the customer questioned their decision to move their data to a co-location data center. They moved this data without a firm understanding of how relevant data would be collected and without having a solid procedure in place for obtaining the data.

Mitigation and prevention

- Keep an inventory of all assets; document and label systems in remote locations
- Maintain an updated contact list for any co-location services providers
- Test and validate Incident Response (IR) procedures; include co-location services providers

Detection and response

- Use co-location services providers with first responders experienced in collecting digital evidence
- Integrate third-party contact procedures into the IR Plan; periodically test contact and escalation procedures prior to cybersecurity incidents occurring
- Require and validate co-location services providers allow access to digital evidence, to include systems and network logs, quickly