THERE'S NO PLACE FOR GUESSWORK IN CYBER-ATTACK INVESTIGATIONS

ACCELERATING INCIDENT RESPONSE WITH DIGITAL FORENSICS

This content was first published on Toolbox, an SWZD publication, in January 2022.

exterro®

RESPONDING TO TODAY'S THREAT LANDSCAPE

You can't ignore the headlines. From the Irish health service to the Missouri teachers' pension system, we've seen that any organization, at any time, can suffer a cybersecurity attack, resulting in a devastating data breach. And IT pros are well aware that even the most sophisticated defenses can be overturned by human error or malicious internal actions.

For the past year, organizations have witnessed more (and more aggressive) data breaches than ever before. The probability – and fear – that it's likely only a matter of time before their own network comes under attack intensifies the pressure on IT and cybersecurity pros. Beyond the endpoint security, firewalls and other protective mechanisms that they have already set up, they need to seek out additional ways to bolster their network defenses.

An important element of recovering from a cybersecurity incident is a having in place a coordinated process for analyzing, reporting, and remediating as quickly as possible after the attack. But manual investigations involve too much time and too many variables to constitute an adequate post-breach strategy. For a large organization, imagine the sheer number of investigators required, assets to be reviewed, geographic locations and remote workers that get in the way of achieving a timely result.

Factors such as these, plus the need to gather data in a manner that will be defensible in a court of law, has given rise to fast-growing demand for robust post-breach response tools. And this is where digital forensic tools come in.

RESPONDING TO TODAY'S THREAT LANDSCAPE

Digital forensic toolsets automate time-consuming investigative processes, presenting IT pros, compliance, and legal teams with facts, evidence and paths to remediation quickly after an incident has been discovered. Investigators can quickly search through vast amounts of data from any system or software in use – they can even retrieve data that has been deleted.

Enhanced platforms in the market today can scale to cover tens of thousands of endpoints and defensibly record and track data throughout the collection process, including any instances where the data has been altered, which is a powerful feature in the protection of the innocent. And by running scans of the network, the forensic tool can identify anomalous activity that might signify a breach, and can immediately institute an automated, network wide investigation.

In short, forensic tools matter not only for their ability to triage an attack and find out its source but also to defend against litigation. Companies that can prove they were in compliance with privacy and other regulations when they were attacked are on far more solid legal ground.

TRIAGING THE THREAT

Post-breach forensics allow organizations to identify how attacks happened and implement the most effective response strategies in a far shorter time frame than human actions alone. The first phase of response is triage: extricating the organization from the threat as quickly as possible, keeping endpoints safe and shutting down or isolating those that have been compromised.

During triage, the number one priority is to root out any indicators of compromise (IoC) by undertaking a rapid scan of the entire network for unusual activity. For example, if one computer is being constantly hit by an IP from an unusual location, or if user accounts are accessing data using unauthorized, unknown, or accounts above their normal authorization level, either of these scenarios could point to a threat on the horizon. This allows the response teams to make key decisions about where to direct their defense and remediation efforts.

Another function of forensic toolkits is to perform analysis and preservation of both user and system data, collecting user details from hard drives, RAM, peripheral devices and more. Systems data gathering might include the type of network shares or connections; how many times a program was run or accessed, by whom and when; which files were downloaded from a browser. The permutations are almost infinite. Such capabilities are, of course, beyond the scope of endpoint detection and response (EDR) solutions which have very limited forensic capabilities.

WHAT IF...

Take any recent cyber incident, from the *Solarwinds hack* to the slew of *aviation-related attacks*, and they provide examples of where the right digital forensic toolset could have helped reduce the damage.

Automation and scalability capabilities would have allowed a rapid scan and created an alert so that the affected organization could have immediately started to collect data from endpoints even while the attack was happening. This could have allowed them to shut down the attack and bolt closed all endpoints. Cyberattack targets can then preserve defensible forensic evidence and review the data, as well as analyze their incidence response. This also enables organizations to put remedial measures in place to prevent such an incident from happening again.

While triaging a ransomware or malware attack is possible manually, industry experts advise enterprises consider the right toolkits and data analytics platforms that can orchestrate all of these moving parts on its own.

KEY DIGITAL FORENSICS TECHNOLOGY CAPABILITIES

WHAT DO WE MEAN BY 'THE RIGHT TOOLKIT'?

There are many factors at play, but customization and flexibility are key. Does the toolkit have built-in capabilities to automatically run custom scripts so that, if a particular scenario happens at an endpoint, it will trigger the collection of data as well as the disconnection of the suspect endpoint from the network and stop the transmission of unauthorized data? Will it also trigger the processing of data to determine how the attack occurred from its origin? If capabilities like these had been in place, attacks such as those on *Palo Alto Networks* might have had a different outcome.

DEFENSIBILITY

Data defensibility is one of the most critical elements of a forensic investigation. It represents the handoff from the organization's IT investigators to the legal teams who will be using this digital evidence in court. To have value in the legal context, data from an investigation must be defensible – teams must be able to prove the data they started with during an investigation is the exact same data they ended with – otherwise it will never be admissible under the law.

Investigators must therefore demonstrate a clear chain of custody, showing that the data presented has not been altered in transit, whether by human error or reviewer bias or malicious interference. Forensic toolsets should factor this in by including checks throughout the process - even down to low level imaging of an endpoint - to demonstrate that nothing has been changed. This avoids the potential of challenge to your evidence.

SCALABILITY

Scalability is another key attribute. Without high-capacity tools, there's no way to manually manage the threat vectors at sufficient scale to cover all endpoints in a mid-sized or large organization. To be effective, the toolset must scale to allow analysis of all potentially affected endpoints with a single click.

ACCURACY

All these features count for little unless organizations have confidence in the results of their forensic investigations. There is no room for doubt about the accuracy of the data; IT pros need to be sure they are looking at the right information when time is at a premium. So, when seeking a digital forensics tool, choose one that has demonstrated minimal false positives over a substantial period of time.

DEMONSTRATING THE VALUE OF DIGITAL FORENSICS

As we all know, there is no silver bullet to shut down cyberattacks, and no-one has come forward with that mythical crystal ball offering insights into hackers' minds. Attackers can find a way through most any organization: it's just a question of when and how the attacks happen, as well as what teams can do to mitigate the damage.

Digital forensics will therefore always be in demand because it provides that missing piece from cybersecurity solutions: deep and provable analysis of the how, the where, and the why. In a recent hack, where 15 servers within a large insurance company were compromised by a ransomware attack, the company launched its response.

1. Searching to understand how it had happened, the company used **Exterro FTK®** to recreate the timeline of the attack, extract critical systems information that revealed the specific IoC, and identify precisely what had enabled the attack to succeed.
2. The company found it stemmed from a phishing email to an employee: human error had triggered the installation of malware. They then found remote desktop connections that had been established and tested days prior to attack, and from this were able to create a clear picture of how long the attackers had been active in their environment.
3. With this information, the company could identify what the hackers had been able to steal. They put together a much more through breach response strategy, triaged the damage appropriately, and maintained data integrity of all of the evidence they were finding to help during litigation later, should they need it.
4. All of this was discovered within the space of hours via an automated, integrated system instead of the days or weeks it would have taken without digital forensic tools in place.

WHAT IT PROFESSIONALS NEED TO KNOW

In breach response, siloed workflows ultimately lead to chaos and inefficiency, but integrated tools will deliver all the automation, accuracy and speed that are needed. When technologies complement each other, they provide a holistic approach that improves chances of success.

Even organizations who believe they have the best defenses already in place need to stay alert. The attack landscape changes every day and hackers are just waiting for the right opportunity to arise. Organizations that have been attacked must continually look to enhance their security protocols and response posture by implementing the right policies, educating employees about cyber-safe skillsets, and deploying best-in-class forensic investigation technology.

GET A DEMO TODAY TO FIND OUT HOW EXTERRO FTK® CAN AUGMENT YOUR CYBER-INCIDENT RESPONSE.

GET A DEMO