Articles + Publications | December 2, 2022

Forensic Artifacts Play Legal Role in Cyber Incident Response

WRITTEN BY

Sadia Mirza | Kamran Salour

Authors:
Kamran Salour, Partner, Troutman Pepper
Sadia Mirza, Associate, Troutman Pepper
Kayla Barker, Director of Incident Response, Tetra Defense
Zack Doyle, Senior Forensic Analyst, Tetra Defense
Derek Berger, Forensic Analyst, Tetra Defense

When a business experiences a data security incident, there is invariably one principal question that the affected business wants answered: Who do we tell?

While this is a simple question, the answer is not. Ideally, after an incident, an affected business can decide whom it: (1) must tell about the incident; and (2) should tell about the incident. The first decision is a legal one. The second is a business decision.

After an incident, however, an affected business often does not have enough information to make these decisions.

Forensic Artifacts: A Business and Legal Issue

Enter forensic artifacts. In the context of incident response, forensic artifacts help explain what happened during the incident. These include things like registry keys, IP addresses, files, timestamps and event logs — things that help piece together the nature and scope of the incident.

Forensic artifacts serve both legal and business purposes. They answer questions such as:

- What was the root cause of the incident?
- When did the incident occur?
- What data was affected?

- Where should the business focus its containment and remediation efforts?

From a business perspective, the answers to these questions may assist the business with restoring affected systems, restoring altered or corrupted data needed for business critical functionality, preventing further damage to other systems, and improving the overall information security protocols.

From a legal perspective, the answer to these questions may help defend against potential claims, determine whether contractual requirements have been triggered, assist with identifying possible resolution options in a dispute and, critically, determine who the business must and should tell about the incident.

Legal teams often do not appreciate the legal purpose of forensic artifacts until it's too late. Instead, forensic artifacts are viewed as a security issue — resulting in legal teams having no input into what forensic artifacts a business should collect, and how long the business should retain them.

Understanding how forensic artifacts may save a business from declaring an incident as a data breach is critical, and should incentivize security and legal teams to work together before an incident occurs, to ensure they are positioning the business in the best way possible.

Log and Tell: Business Email Compromise Example

To better explain the legal role of forensic artifacts, consider what happens in a business email compromise, or BEC, attack. Who a business must tell generally depends on whether there is evidence of unauthorized access or acquisition of personal information — i.e., whether the incident qualifies as a data breach.

If a business has its full complement of logs, that business may be able to determine if the threat actor accessed or acquired personal information from the email environment and the specific files that the threat actor accessed or removed.

Without a full complement of logs, the business may not be able to determine if there is unauthorized access or acquisition of personal information — or the scope of unauthorized access or acquisition.

To assess a business's statutory notification obligations, it is critical to determine which emails the threat actor accessed or acquired. Not knowing the scope of an incident creates uncertainty. Does the affected business have to notify anyone about the incident, absent conclusive evidence of unauthorized access or acquisition of personal information?

In such a scenario, the affected business may find itself with two potentially unfavorable options: (1) Assume the worst-case scenario, namely, that all its customers' and employees' personal information has been subject to unauthorized access or acquisition, and notify everyone; or (2), assume none of its customers' and employees' personal information has been affected, and notify no one. Both scenarios pose unique risks from the litigation and regulatory perspectives.

Logs are also important in ransomware attacks. Firewall logs provide insight into the scope and timing of data

exfiltration. VPN logs can provide insight into when and from where the threat actor accessed the environment.

Having this information available after an incident may be able to narrow the scope of the incident, possibly resulting in a smaller notification population.

Legal and Security Teams Need to Work Together

Drawing on our combined legal and security backgrounds, we compiled a comprehensive list of artifacts that forensic analysts typically request following a BEC incident or ransomware attack.

Different logs provide different information, and have varied retention periods. Legal and security teams should discuss what logs a business should retain, and for how long.

If an organization that uses Office 365 experiences a BEC incident, there are a bevy of logs that can provide insight into the incident itself and the organization's response to it. Microsoft Purview audit logs provide insight into user logins, mailbox activity, SharePoint/OneDrive file access or downloads, and other Office 365 network related activity. The standard retention period for them is 90 days.

Admin audit logs record actions by global administrators, record cmdlets executed and objects affected. These logs have a 90-day standard retention period. Mailbox search terms provide insight into what information an unauthorized user was searching for — i.e., "wire," "wire transfer," "bank information," etc.

Inbox and forwarding rules provide insight into whether the threat actor sent emails outside the business's email environment. Message trace logs provide a high-level metadata report of all incoming or outgoing emails for a specific user. These logs have a 90-day retention period.

A compromised user mailbox file allows an analyst to view a business email inbox as the legitimate user would. It therefore aids in viewing potential phishing emails, and understanding the regular use patterns of the user.

If an organization that uses Google Workspace experiences a BEC, Google Workspace has logs that retain certain information too. Audit logs provide insight into user logins, mailbox activity, Google Drive file access or downloads, and other network related activity. The standard retention period for these logs is six months.

User reports may show the last IMAP/POP3 login, the last web-based login, and password length, and provide other account status checks. These logs are retained for six months.

Mailbox search terms from Google Workspace also provide insight into what information an unauthorized user was searching for. Inbox and forwarding rules provide insight into whether the threat actor sent emails outside the business's email environment.

Email search logs provide a high-level metadata report of all incoming or outgoing emails for a specific user. These logs are retained for 30 days, and are similar to message trace logs in Office 365.

Google Vault allows an analyst to view a compromised user mailbox as the legitimate user would. It therefore aids

in viewing potential phishing emails, and understanding the regular use patterns of the user.

Logs are also instructive in ransomware incidents. Firewall logs and admin console access monitor access into and out of the environment, including IP addresses, and the size or number of bytes being transferred in and out of the network. And VPN activity logs provide session history and length, IP addresses used by network protocols or user agents, and network bandwidth usage.

Conclusion

While these artifacts are useful in understanding what happened after an incident, it is important to discuss logging and retention long before an incident occurs. Legal and security teams should be aligned on their approach before, during and after an incident.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber