

Anatomy of a Breach

The Malware Triage Pipeline: A rapid, methodical response to contain threats, preserve volatile evidence, and analyze an artifact's purpose to define the scope of a breach.

The Triage Protocol: The First 60 Minutes

The actions taken immediately following detection are the most critical for evidence preservation. Follow this non-negotiable sequence.



1. Isolate

Immediately disconnect the machine from all networks. This prevents lateral movement and halts data exfiltration.



2. Memory Dump

Acquire a full memory image (RAM dump). This is the *only* way to preserve volatile evidence like running processes and encryption keys.



3. Disk Image

Create a bit-for-bit forensic image of the hard drive using a write-blocker to ensure evidence integrity.

Analysis Methods: From Observation to Execution

Once evidence is preserved, analysis begins. These two methods provide a complete picture of the malware's capabilities and actions.



Static Analysis (No Execution)

Examining the suspicious file without ever running it. This is the safest way to extract initial intelligence.

- **Hashing:** Check against threat databases like VirusTotal.
- **String Extraction:** Find hardcoded IPs, domains, and file paths.
- **Import/Export Tables:** Identify intended system calls and capabilities.



Dynamic Analysis (Sandbox Execution)

Safely executing the file in a monitored, disposable virtual machine to observe its behavior and identify Indicators of Compromise (IOCs).

- **File System Changes:** What was created, deleted, or encrypted?
- **Registry Modification:** Which keys were altered for persistence?
- **Network Activity:** Did it beacon to a C2 server? What data was sent?

Decoding the Signals

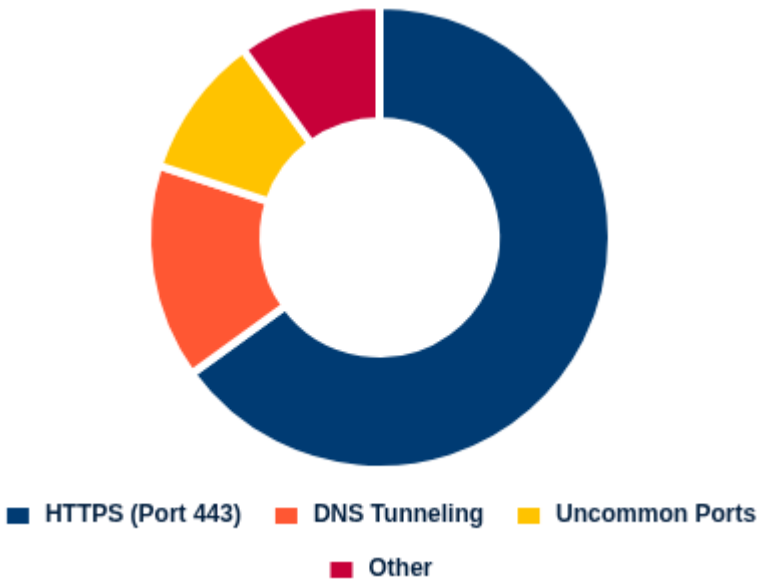
Analysis of thousands of breach incidents reveals common patterns in attacker behavior. Understanding these helps investigators quickly identify the nature of a threat.

C2 Communication: How malware "calls home" for instructions.

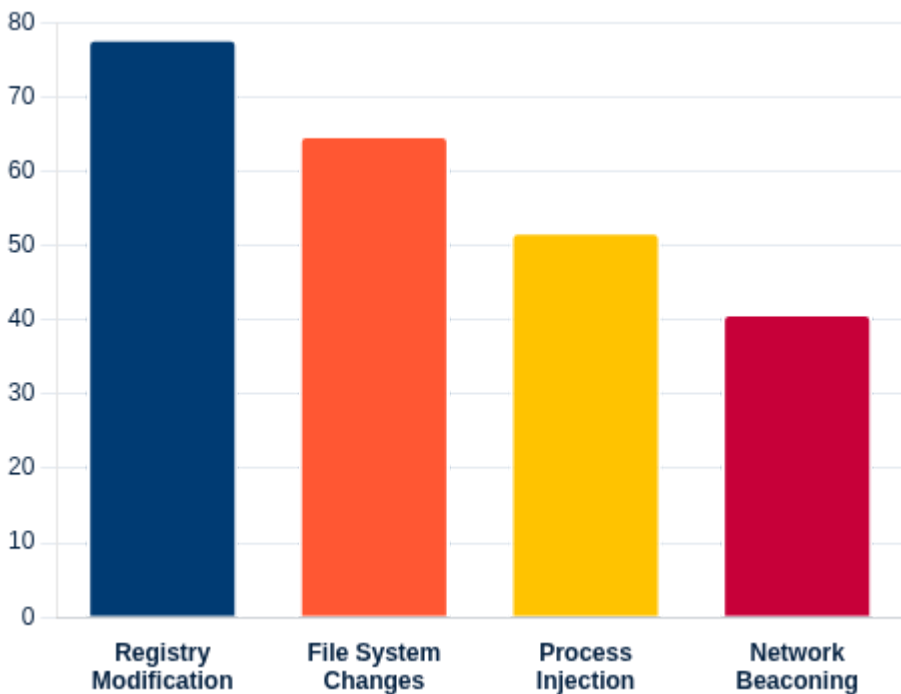
Indicators of Compromise (IOCs): The digital footprints left behind.

Registry modifications are the most common IOC, as they are a primary method for achieving persistence on a compromised system.

Common C2 Communication Methods



Frequency of Observed IOCs in Breaches



Post-Incident Response: The Human Firewall

Technical fixes are not enough. The final step of any investigation is to use the findings to train the most common point of failure: the end user.

The "See Something, Say Something" Protocol

Train employees to disrupt, not diagnose. Report any of these three symptoms immediately.

Unexpected Behavior

Slow computer, strange pop-ups.

Unusual Logins

Prompts for passwords unexpectedly.

Odd Phrasing/Urgency

Emails with poor grammar or threats.

82%

of breaches involve a human element, like falling for a phishing email.