THREATDOWN™

2026 State of Malware

5 Critical Attack Behaviors

ThreatDown has identified five critical attack behaviors criminals use to stay hidden when attacking small and mid-sized businesses.

1	**Faster attacks** Complex, multi-stage cyberattacks can now be completed in hours instead of days, shrinking the time for defenders to respond.
2	**Working at night** Attackers stay hidden by working at night, on weekends, and during holidays, when IT and security staff are least likely to be watching.
3	**Living off the land** Attackers use legitimate tools, credentials, and administrative commands instead of malware to blend their activity into routine IT operations.
4	**Staging from blind spots** Attackers seek out unmonitored blind spots to launch remote encryption attacks against other parts of a network.
5	**Attacking security and recovery software** Security controls and backup systems are targeted to disrupt a target's detection, response and recovery capabilities.

ThreatDown Managed Detection & Response (MDR) counters modern attack behaviors with 24 x 7 x 365 expert monitoring and fast, decisive action, closing the gaps attackers rely on to stay hidden.

For more information on how to defend your organization against the five critical attack behaviors, cybercriminals' latest stealthy tactics, and the emerging danger of AI-orchestrated attackers, read the **2026 State of Malware**.

Download now