DECEPTIVE BYTES
Distort Ransomware Perception

Added Value

Current Situation

When an organization discovers a ransomware note demanding millions of dollars, it is not the beginning of the attack - it is the culmination of a much longer, covert process. The confusion and chaos at this moment often obscure the fact that the actual attack began long before the ransom demand appeared.

Ransomware True Timeline

A ransomware attack unfolds over weeks or months, beginning with reconnaissance to identify vulnerabilities and initial access via phishing, exploit kits, or unpatched software. Attackers then establish persistence, escalate privileges, and move laterally across the network while exfiltrating data and disabling defenses. During this dwell time (often 90–180 days), they map critical systems, steal credentials, and prepare payloads. The final staging phase involves deploying ransomware, encrypting files, and triggering the ransom note, marking the attack's endgame, not its start. By the time demands appear, attackers have already compromised data, backups, and systems, leaving organizations to face operational paralysis, data leaks, and prolonged recovery.

Distorting Ransomware Perception

Deceptive Bytes offers an innovative approach to endpoint security by turning ransomware's own evasive tactics against itself. Through its preemptive and proactive defenses, the solution distorts ransomware's perception of the environment, breaks ransomware logic, and prevents attacks before they can even begin. This forward-thinking strategy not only reduces the risk of breaches but also ensures your business remains operational, resilient, and secure in the face of emerging threats - Never Let Your Business Down!

Think differently.

Protect proactively.

Stay ahead of the latest threats.

Preemptive defense: Create a hostile or unappealing environment for ransomware to operate, reducing its motivation and chances of infection.

Proactive defense: Continuously adapts the strategy based on the attacker's behavior, effectively countering evolving threats.

Multi-layered approach: Seamlessly integrate with your existing security stack, enhancing your overall defense posture and providing an extra layer of protection.

"Every day, new tactics and techniques are emerging, 'well-established' attacks remain successful, and the threat from cyber espionage continues to grow.
Deceptive Bytes' Active Endpoint Prevention provides a means to shape attackers' decision making, manipulate their behaviors, and ultimately disrupt their efforts to attack organizations."

Never Let Your Business Down

How Deceptive Bytes Help

- **To Organizations**:
  - **Prevent unknown & advanced threats** - By using ransomware evasive techniques and by distorting its perception of the environment, Deceptive Bytes' solution prevents ransomware from attacking the system 6 months before the attack actually begins, without the need to know or detect it beforehand.
  - **Prevent damage to data & assets** - Prevention means no lost or corrupted data & assets in the organization. Also, the solution is developed in User-mode, meaning there's no downtime to the environment if a bad patch is applied.
  - **Reduce operational burden** - Since there's no need for dedicated, highly skilled professionals to constantly manage & monitor the solution, any technical person can operate it. This allows security & IT teams to focus on other security aspects of the organization. In addition, preventing attacks saves time for security teams in prioritizing & investigating each attack and saves IT teams' time restoring data & endpoints for the business to continue operating.
  - **Reduce reputational risk** - By keeping organizations safe, preventing malware on their endpoints, data exfiltration & data corruption means no bad publicity due to successful cyber attacks.
- **To CISOs & IT Managers**:
  - **Automate strategy against ransomware behavior** - The solution automatically adapts its strategy based on the attacker's behavior on the endpoint without the need for constant configuration or additional load to the security or IT teams. This helps prevent attacks in seconds.
  - **Adapt to changes in IT environments** - Since IT environments constantly change in today's fast-paced world, the solution can quickly adapt to the changes in the IT environment without the complications of re-configuring or re-building the entire deployment
  - **Reduce alerts & false positives** - The solution provides high fidelity notifications ("alerts"), which reduces the alert fatigue security & IT teams are facing when handling other security tools (including next-gen anti-malware products) and reduces overall time chasing false alarms.
  - **Operate in unpatched/vulnerable environments** - Since the solution creates deceptive information on the endpoint and adapts to ransomware behavior (in real-time), it doesn't matter if the environment is unpatched or has open vulnerabilities, the solution will thwart the attack as soon as the ransomware recons the environment..

Never Let Your Business Down

- **To The C Level**:
  - **Improve employees' productivity** - Since the solution is very lightweight and doesn't use a lot of resources (memory, CPU & disk space), employees can work without interference or slowness, contrary to traditional tools such as AVs & EDRs.
  - **Reduce operational costs & resources** - The solution integrates with Windows Defender & Windows Firewall, which helps organizations benefit from their built-in security tools in the OS, having the ability to remove old, ineffective tools (like paid Antivirus/Anti-malware).
  - **Protect remote employees** - The solution can operate outside the organizational network & without the need for constant updates, helping you stay protected no matter where you are or if users connect from unsafe networks or computers.