Morphisec Launches Exfiltration Prevention to Stop Ransomware and Data Exfiltration Cold

Powered by Automated Moving Target Defense (AMTD), Morphisec Proactively Stops the Top 10 Ransomware Exfiltration and Impact Techniques Before They Begin

BOSTON, MA, UNITED STATES, June 5, 2025 /EINPresswire.com/ -- Morphisec, the trusted global leader in prevention-first security and anti-ransomware protection, raises the bar in ransomware defense with Exfiltration Prevention, a revolutionary solution that stops ransomware and data exfiltration tactics cold. By combining patented Automated Moving Target Defense (AMTD) technology and its Anti-Ransomware Assurance Suite Morphisec ensures unmatched protection against the most sophisticated threats.

> With Exfiltration Prevention, we're continuing to shift the conversation from reaction to true prevention."
>
> *Michael Gorelik, CTO*

Ransomware attackers are evolving rapidly, leveraging AI while combining encryption and exfiltration in double and triple extortion schemes. Traditional tools cannot keep pace with these techniques and are losing ground to AI-powered threats. Morphisec neutralizes ransomware and data exfiltration before execution, protecting organizations from disruption and reputational damage.

"With Exfiltration Prevention, we're continuing to shift the conversation from reaction to true prevention," said Michael Gorelik, CTO at Morphisec. "Morphisec is the only solution that combines Adaptive Exposure Management (AEM), Infiltration Protection, and Impact Protection to effectively stop ransomware and data exfiltration before they start, keeping organizations resilient in an era of increasingly complex and intertwined techniques."

Key features of Morphisec's Exfiltration Prevention include:

- Automated Moving Target Defense (AMTD): Dynamically randomizes memory structures, making endpoints unpredictable and unexploitable, effectively preventing exfiltration exploits.
- Adaptive Exposure Management (AEM): Proactively identifies and mitigates vulnerabilities, misconfigurations, high-risk software, and misuse of privileged accounts to reduce the attack surface and prevent potential data exfiltration paths.
- Real-Time Prevention: Instantly disrupts unauthorized data exfiltration attempts without relying on alerts or manual intervention, ensuring attacks are neutralized before they can cause harm.

Top 10 Ransomware-Specific Exfiltration and Impact Techniques

Morphisec's Exfiltration Prevention addresses both data exfiltration and impact techniques used by ransomware attackers. These combined techniques disrupt operations and compromise sensitive data.

- T1486: Data Encrypted for Impact: Encrypts data to disrupt operations and demand ransom.

- T1490: Inhibit System Recovery: Disables backups and recovery points to force ransom payments.

- T1489: Service Stop: Stops critical services like EPP/EDR or backup solutions to ensure successful encryption.

- T1567: Exfiltration Over Web Service: Uploads stolen data to cloud services for double extortion.

- T1048: Exfiltration Over Alternative Protocol: Uses DNS tunneling or other non-standard protocols to evade detection.

- T1052: Exfiltration Over Physical Medium: Copies sensitive data to USB drives or other physical devices for ransom leverage.

- T1029: Scheduled Transfer: Automates data exfiltration during off-hours to avoid detection.

- T1537: Transfer Data to Cloud Account: Uploads data using compromised cloud credentials.

- T1020: Automated Exfiltration: Automates the collection and transfer of sensitive data to minimize detection risks.

- T1485: Data Destruction: Deletes data after exfiltration to amplify ransom pressure or obscure attacker activity.

Why Morphisec Stands Out

"Attackers are becoming more sophisticated, but so are we," said Gorelik. "Morphisec's signatureless technology is designed to neutralize new and unknown threats by disrupting the attack chain itself. Automation tools rely on predictable patterns that Morphisec's AMTD technology can disrupt."

Unlike reactive solutions, Morphisec takes a prevention-first approach, using AEM and AMTD to stop exfiltration and encryption before harm occurs. Its technology neutralizes ransomware

payloads, blocks unauthorized access, preserves recovery tools, and disrupts exfiltration via cloud services, scripts, and command-and-control channels. This prevents attackers from gaining leverage and minimizes disruption.

Morphisec is the only cybersecurity company to hold a patent on ransomware prevention using decoys, ensuring unmatched protection against encryption-based attacks.

Exfiltration Prevention is available today as part of Morphisec's Anti-Ransomware Assurance Suite. Morphisec protects millions of endpoints in organizations worldwide. Request a demo today by visiting https://www.morphisec.com/demo.

About Morphisec

Morphisec, a leader in Preemptive Cyber Defense, provides prevention-first security against ransomware attacks that others don't — from endpoint to cloud. Powered by patented Automated Moving Target Defense (AMTD) technology, Morphisec stops ransomware, supply chain attacks, zero-days, and other sophisticated threats. Thousands of organizations trust Morphisec to protect millions endpoints, servers, and workloads. Customers include Lenovo/Motorola, TruGreen, Covenant Health, Citizens Medical Center, and many more.

Learn more at www.morphisec.com.

Brad LaPorte
Morphisec
+1 617-826-1212
email us here