Win-DDoS Turns Trusted Infrastructure Into a Threat

Business Impact Brief

Contact
Steve Mulhearn
VP, Global Security Services & Customer Experience
steve.mulhearn@corero.com

Executive Summary

Researchers have uncovered a new tactic that allows cybercriminals to launch distributed denial of service (DDoS) attacks using your own infrastructure. The technique, called Win-DDoS, takes advantage of how Windows servers process normal network requests. Attackers do not need malware, passwords, or any access to your systems. They send a few carefully crafted requests, and your infrastructure becomes the weapon.

The threat comes from domain controllers that are exposed to the internet. These servers manage user identity and access. If misconfigured, they can be triggered to send large volumes of traffic to any target. The attack traffic looks legitimate and is difficult to trace. Our engineering team replicated the behavior in the lab and confirmed how easily attackers could use this method. The risk increases when many organizations unknowingly contribute to the same attack.

Risk Score Without Protection: 4 out of 5

Win-DDoS is simple to trigger, hard to detect, and widely applicable. It puts service availability and operational stability at real risk.

Risk Score With Corero Protection: 1 out of 5

With Corero, the risk is significantly reduced. Our SmartWall ONE™ solution applies automated defenses in real time, stopping suspicious behavior before it impacts availability. When paired with our DDoS Intelligence Service, powered by Corero's Threat Research Team, customers receive continuous rule updates that provide pre-emptive protection against emerging attack vectors. This means early visibility into new attack patterns without waiting for product lifecycle updates. This proactive defense lowers your exposure to Win-DDoS compared to unprotected networks.

What to Do Next

Check your defenses. SmartWall ONE already provides real-time inspection and automated mitigation to protect against active threats. By adding our DDoS Intelligence Service, you extend that protection with continuous updates sourced from global threat research. This ensures you are covered not only against known attacks but also against emerging tactics like Win-DDoS. If you are not using our DDoS Intelligence Service today, we can help you review your exposure and strengthen your defenses.

Read the full technical breakdown from our engineering team

Win-DDoS: Under the Microscope