

# DMA UPDATE

## ATM DMA Threat Activity Now Observed in the United States

Call for  
more info



**952-942-9191**

NuSource is monitoring a new wave of ATM attack activity in the United States that reflects Direct Memory Access (DMA) techniques previously identified in South America. While the method itself is not new, its presence in the U.S. is a notable shift and worth understanding.

### What's Different About These Attacks?

- Require physical access to the terminal
- Use unauthorized devices connected to internal ports
- Introduce malicious files directly into system memory
- Bypass traditional software-based defenses

Once access is gained, small external devices can be connected to exposed PCIe or internal ports, allowing interaction directly with system memory at the hardware level.



ATM security is no longer limited to software. Physical access points, terminal configuration, and system age all contribute to overall risk. This is not cause for alarm. It is a signal to review and prepare. Institutions that take measured steps now are in a strong position to reduce exposure.

### Recommended Actions

#### Short-Term Considerations

- Review terminal placement and accessibility
- Evaluate exposure across the lobby and free-standing units
- Assess internal port protections

#### Long-Term Strategy

- Upgrade or replace systems to supported platforms (Windows 10 2019/2021 and Windows 11)
- Reduce reliance on legacy infrastructure
- Align hardware with current security standards

NuSource works with financial institutions to assess ATM and ITM environments, identify vulnerabilities, and develop practical strategies for mitigation and modernization. Our OEM-trained teams are available to assess, update, and maintain your assets as needed to keep them safe.

**NuSource continues to monitor evolving threats and provide practical guidance to help institutions stay prepared. Contact your NuSource representative today.**