



SILVERSKY
Elevate your Cybersecurity

Case Study

Preventing Financial Fraud at a Credit Union Through Early Threat Detection

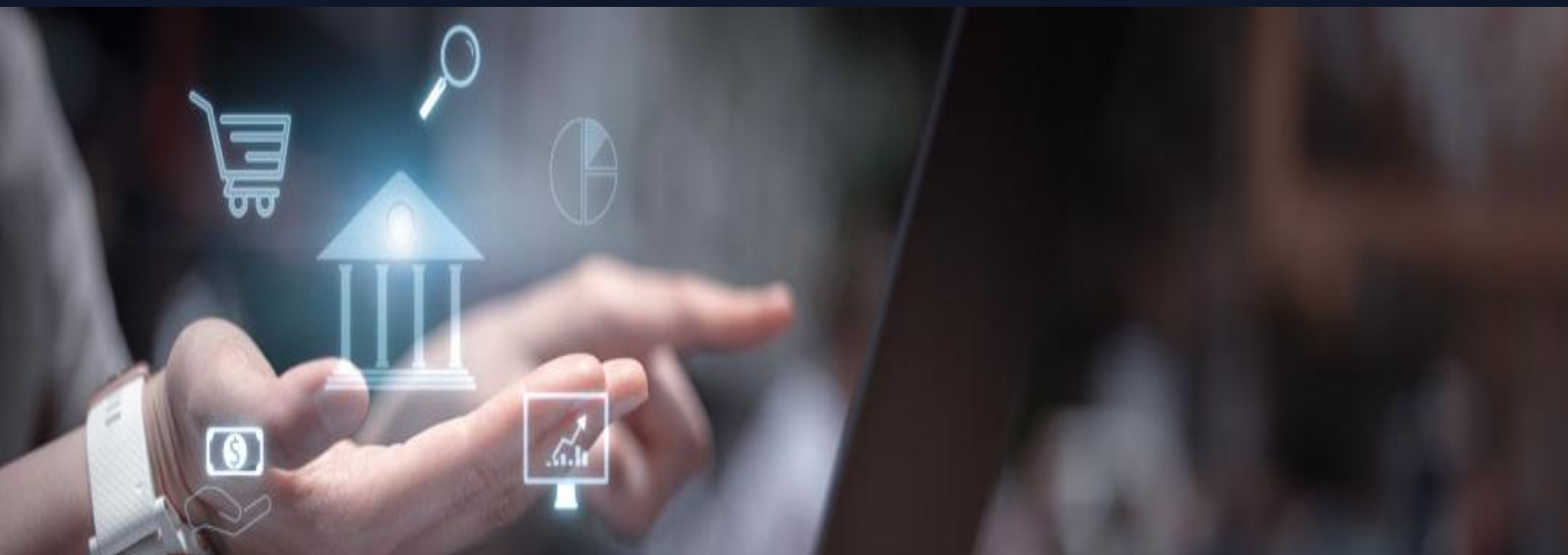


The Incident

A regional credit union experienced a credential-stealing malware infection following a phishing email. The malware was designed to harvest credentials and enable unauthorized financial activity.

Overview

Shortly after deploying SilverSky Lightning MxDR, suspicious outbound communications associated with the malware were detected. Early identification allowed the credit union to contain the threat before attackers could initiate fraudulent wire transfers or access sensitive financial systems.



The Challenge

Like many credit unions, the organization maintained several security technologies including firewalls, email security, and antivirus protection. However, these tools primarily relied on traditional signature-based detection.

When a phishing email delivered a malicious file to an employee workstation, the malware installed successfully because the variant had not yet been identified by antivirus signatures.

Without centralized visibility into system behaviour and network communications, the threat had the potential to remain undetected long enough for attackers to attempt financial fraud.

For financial institutions, incidents of this nature can lead to:

- Unauthorized wire transfers
- Compromise of financial systems
- Exposure of member information
- Regulatory scrutiny

Detection

After onboarding to SilverSky's MxDR service, the platform detected unusual outbound communications originating from internal systems.

The traffic was associated with malicious infrastructure and matched behavior commonly observed in credential-harvesting malware campaigns targeting financial institutions.

SilverSky analysts quickly identified the activity as a high-severity event and initiated an investigation with the credit union's IT team.

The detection occurred before attackers could execute the intended fraud attempt.

Investigation and Response

SilverSky analysts traced the incident to a phishing email that had delivered the malware through a malicious download.

Further investigation revealed the presence of a malicious agent running on several hosts within the environment.

SilverSky worked directly with the credit union to contain and remediate the threat by:

- Identifying affected endpoints
- Reimaging compromised systems
- Removing the malicious agent
- Verifying that no persistence mechanisms remained

Continuous monitoring ensured that the environment was fully secured following remediation.

Outcome

Because the activity was detected early, the credit union successfully prevented a potential fraud attempt and avoided disruption to operations.

Following the incident, the organization strengthened its security posture through improved monitoring and greater visibility into endpoint activity.

The institution was also able to demonstrate to its leadership and board that proactive security monitoring had delivered measurable value by preventing a potentially costly security event.

SilverSky has supported credit unions and financial institutions since the late 1990s, building deep operational expertise in the regulatory and security challenges unique to the industry.

SilverSky is a trusted cybersecurity partner with decades of experience securing regulated organizations, including credit unions and financial institutions across the United States. SilverSky provides Professional Services, Managed Security Services, and Managed Extended Detection and Response (MxDR) to help organizations strengthen security operations, maintain regulatory alignment, and reduce risk over time.