TALES FROM THE SOC

Legitimate Website Compromise Averted

Incident Overview

Threat Type: Legitimate Website Compromised with sophisticated phishing campaign leveraging compromised legitimate website

Time to Containment: 18 Minutes

Attack Characteristics: This targeted attack exploited a compromised trusted domain to gain a foothold, using social engineering rather than standard phishing links. By convincing the user to execute commands directly through the Windows Run dialog, the attacker bypassed typical detection methods, relying on the inherent trust of the source.

Alert Escalation: Low to High Priority

Initial Vendor Severity: Low priority

SOC Escalation: High priority based on behavioral analysis and threat context

Escalation Rationale: Despite the low initial severity rating provided by Microsoft Defender for Endpoint, SOC analysts identified critical behavioral indicators including suspicious registry execution patterns and the use of a compromised trusted domain. The targeted nature of the campaign and industry-specific context warranted immediate priority escalation to prevent potential widespread compromise.

This escalation decision proved critical—without analyst-driven prioritization, the alert could have been overlooked, allowing the threat to propagate across the organization.

Depth of Investigation

The SOC conducted a multi-layered investigation, utilizing registry forensics and full attack reproduction to validate the threat actor's tactics. This deep-dive analysis not only identified additional targeted users but also provided the definitive insights needed to engineer custom detection signatures and neutralize the threat vector.

Coordinated Cross-Platform Response

The incident was handled through a coordinated, cross-platform response across multiple security technologies: isolating the device in EDR, blocking C2 at the firewall and the compromised site at the proxy, and notifying the customer immediately.

Outcome

In just 18 minutes, our coordinated response isolated the affected device, severed C2 communications, and blocked access to the infected website. This rapid preventive response helped contain malware designed for lateral movement avoiding significant operational disruption.