TALES FROM THE SOC

ENERGY SECTOR · HIGH PRIORITY

Hiding in Plain Cache

A ClickFix social-engineering attack, contained in 7 minutes.

Incident Overview

Threat Type: ClickFix fake-CAPTCHA social engineering

Target: Energy sector endpoint

Time to Containment: 7 Minutes

A trusted website was compromised to display a fake CAPTCHA that coached the user to copy a command and run it through the Windows Run dialog. The PowerShell was double-encoded to evade defenses, wrapping a steganography loader that recovered hidden payload data from image pixels staged in the browser cache. CRITICAL**START**®'s SOC peeled back each layer of obfuscation to prove the threat rather than guess at it.

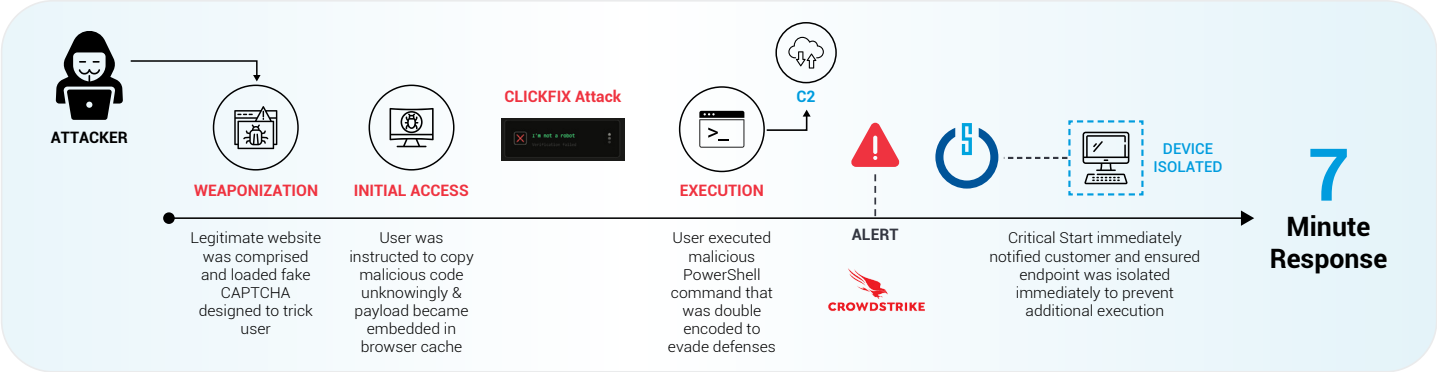
Detection & escalation

Detection: Endpoint detection and response (EDR) flagged malicious PowerShell launched directly from the desktop session and tagged it as an AI-generated command.

SOC Escalation: Escalated high priority. Analysts decoded each layer — Base64 over an assembly/steganography layer — accelerated by Critical Start's AI assistant and validated by a human analyst before action.

Depth of Investigation

Analysts confirmed a steganography-based loader that read concealed instructions from the least-significant bits of image pixel data, then traced the related network and DNS activity to the attacker's infrastructure. Endpoint defenses had blocked the payload, but the script still reached execution — so the SOC moved immediately to contain the host and confirm scope with the customer.



Outcome

In 7 minutes, the Critical Start SOC confirmed the threat with the customer and isolated the endpoint, preventing any further execution. Because the team reached out directly, the customer reimaged and re-provisioned the laptop the same day — turning a potential compromise into a quick, fully contained event.

"You guys are the best. I keep telling my boss that Critical Start is worth the cash — and this proved it."

— Customer, energy sector