Courtesy of
MST Insurance Solutions, Inc.

ClickFix Cyberattacks Explained

Social engineering has long been a tactic employed in different cyberattacks against businesses, often relying on deceptive communications and programming to trick targets into divulging sensitive data, sharing corporate funds or downloading harmful software. Over the years, some social engineering methods have become increasingly sophisticated, making them more difficult to detect and spawning large-scale losses. One of the most prevalent of these methods is ClickFix cyberattacks.

Also known as ClearFake attacks, these incidents involve cybercriminals deploying fraudulent error messages or verification prompts through compromised browsers and phony software updates, manipulating targets into executing malicious commands under the guise of resolving supposed device or system issues. From there, cybercriminals can launch destructive malware, potentially stealing affected businesses' private information and assets and causing significant financial, operational and reputational fallout. Recent years have seen ClickFix cyberattacks continue to expand in scope and severity, infiltrating multiple popular platforms, evading traditional security mechanisms and gaining traction among advanced threat actors.

With this in mind, it's critical for businesses to better understand this emerging attack method and effective defense strategies, thereby limiting potential losses. This article provides an overview of ClickFix cyberattacks, outlines how they can impact businesses and highlights related mitigation tips.

Overview of ClickFix Attacks

ClickFix cyberattacks begin with cybercriminals leveraging stolen credentials to install fake plugins in compromised web platforms or other digital environments. Upon installation, these plugins inject deceptive programming language to create fraudulent variations of well-known browser and software notifications, using technology such as blockchain and smart contracts to acquire malicious payloads.

When ClickFix cyberattacks are launched, targets are first presented with the phony notifications, which may include the following common phrases:

- "Something went wrong while displaying this webpage."
- "There was an error during the latest update of your browser/software."
- "Your browser/device does not support the necessary files/attachments/plugins."
- "Please verify that you are a human to proceed."

These notifications then provide specific instructions for targets to follow to "fix" supposed problems with their devices or systems. Unlike standard social engineering methods, which use automated exploits or attachments that download harmful software as soon as targets open or click on them, ClickFix cyberattacks take the deception a step further by manipulating targets into manually executing malware, prompting them to copy malicious commands (e.g., PowerShell) into their devices' dialog boxes or similar utilities (e.g., Windows Run). At that point, cybercriminals can move forward with payload delivery and utilize the downloaded malware to wreak havoc on targets' devices or systems.

Because they center around human-driven execution, ClickFix cyberattacks are often more difficult to identify as malicious and, as a result, frequently sidestep traditional security measures. In the years since they first

gained prominence, these incidents have steadily evolved and, consequently, become more dangerous for impacted businesses. While they initially only had the capacity to spoof certain browsers and be launched via specific software, these incidents now span a range of impersonated platforms (e.g., Google Chrome, Facebook, PDFSimpli and reCAPTCHA) and include variants that can affect Windows, macOS, iOS and Android devices.

Complicating matters, sophisticated hackers have begun packaging the plugins needed to deploy ClickFix attacks as a product on the dark web, feeding into the Crime-as-a-Service (CaaS) model and allowing a growing number of cybercriminals—including nation-state threat actors—to launch these incidents with little to no expertise. The proliferation of these incidents through the CaaS model has also paved the way for a new variation of the ClickFix method to appear, known as the FileFix method. Instead of having targets copy malicious commands into their dialog boxes, FileFix cyberattacks trick them into copying these commands into the address bar of their respective browsers. Because targets are often more familiar with address bars than dialog boxes, this poses serious concerns about the continued growth of such attacks. Going forward, ClickFix cyberattacks are only expected to continue advancing, making it vital for businesses to take steps to defend against them.

How ClickFix Attacks Impact Businesses

ClickFix attacks can affect businesses in many ways, leading to the following ramifications:

- **Stolen funds and assets**—Through these attacks, cybercriminals can take over targets' accounts and gain unauthorized access to confidential business records, private stakeholder information and intellectual property. This could enable them to steal critical funds and assets, leaving businesses with considerable financial losses. In some cases, cybercriminals may employ ClickFix attacks to launch disruptive ransomware incidents, potentially leading to additional financial challenges.
- **Damaged systems and technology**—Such attacks may also allow cybercriminals to leverage compromised devices and systems to move laterally across corporate networks, escalate their privileges and infiltrate businesses' larger IT infrastructures, resulting in more widespread damage and operational disruptions.
- **Regulatory and legal penalties**—When ClickFix attacks impact sensitive stakeholder information, businesses could be held liable for failing to properly protect such data, prompting costly lawsuits. Furthermore, businesses could face substantial regulatory penalties for breaching applicable international, federal and state data privacy laws. Depending on the severity of such litigation and penalties, this could cause lasting reputational damage, eroding customer loyalty and diminishing businesses' profitability for the foreseeable future.

Risk Mitigation Strategies

There are various risk management measures businesses can implement to help lower the likelihood of ClickFix attacks and limit associated losses if these incidents do happen:

- **Promote a culture of cybersecurity.** First and foremost, businesses should foster a workplace culture that prioritizes cybersecurity. This primarily entails providing routine awareness training to all staff—regardless of department or tenure—on cyber hygiene best practices, the latest cyberthreats, and related prevention and response tips. As it pertains to ClickFix attacks, this training should highlight common formats and phrasing for such incidents, as well as guidelines for reporting suspected social engineering plots. Employees should be instructed to never interact with or respond to potentially malicious commands.
- **Establish safe browsing and script execution policies.** Alongside staff training, businesses should establish workplace policies that clearly outline safe browsing behaviors (e.g., using strong passwords across all accounts, verifying website security, installing any available privacy tools and clearing browser data on a regular basis) and restrict the types of commands that can be launched from dialog boxes and address bars. These policies can help reduce the risk of employees being targeted in

ClickFix cyberattacks and render cybercriminals' efforts useless by blocking the accidental execution of malware in the event that staff do fall victim to such incidents.

- **Maintain updated software.** Businesses should make it a priority to regularly update all workplace devices and systems to help patch known vulnerabilities and other security weaknesses, thereby blocking cybercriminals from exploiting this technology amid ClickFix attacks. Enabling automatic software updates and using patch management tools can simplify this process.
- **Utilize advanced security solutions.** Although ClickFix attacks often bypass traditional security measures, equipping devices with advanced threat identification systems, antivirus programs, firewalls, and endpoint detection and response (EDR) tools can help businesses ensure greater visibility of their entire IT infrastructures and detect any abnormal activity. Such solutions may also help stop cybercriminals in their tracks, addressing malware before it causes more severe damage.
- **Create segmented networks and access controls.** To prevent lateral movement through their systems amid ClickFix attacks and expanded attack surfaces, businesses should segment their networks. This way, cybercriminals will only be able to compromise a small portion of corporate resources, minimizing the risk of large-scale damage and disruptions. In addition, businesses should enforce strict access controls and uphold the principle of least privilege, only allowing employees to handle systems and data deemed necessary for their roles.
- **Vet all software and technology vendors.** Because ClickFix attacks start with cybercriminals compromising digital environments, businesses should carefully evaluate all software and technology vendors, especially niche or lesser-known providers, for possible security flaws before finalizing contracts and purchases. In doing so, businesses can avoid introducing new vulnerabilities and offering further avenues for ClickFix attacks.
- **Have a plan.** Cyber incident response plans can help businesses ensure that necessary procedures are taken when attacks occur, thereby minimizing related losses. These plans should be well documented, practiced often and address a range of scenarios (including ClickFix attacks).

Besides these strategies, it's imperative for businesses to secure ample insurance to help cover losses stemming from potential ClickFix cyberattacks. In particular, cyber insurance may help reimburse costs associated with ransomware, data breaches, business interruption and incident response stemming from malware delivered via social engineering scams, including ClickFix attacks. However, the level and scope of such coverage may vary based on policy wording. For instance, some insurers may limit or fully exclude coverage for losses resulting from cyberattacks caused by social engineering scams that manipulated honest employees—albeit unknowingly—into openly participating in the incidents. Since ClickFix attacks involve employees manually executing malware, this may hinder coverage for such events.

What's more, insurers willing to offer protection for these attacks are adopting increasingly strict underwriting guidelines, demanding policyholders demonstrate effective security awareness training regimens, EDR deployment, access controls and incident response readiness as a prerequisite for coverage. Considering these developments, it's best for businesses to consult trusted insurance professionals to assess their unique ClickFix exposures, determine their specific coverage needs and, if necessary, explore additional policy endorsements and alternative risk transfer solutions to minimize any gaps in protection.

Conclusion

ClickFix cyberattacks pose numerous risks. As these attacks grow more prevalent, it's vital for businesses to have proper safeguards in place. By maintaining awareness of these events and taking sufficient steps to address them, businesses will be better equipped to navigate this evolving cybersecurity landscape and, in turn, prevent major losses. Contact us today for more risk management guidance and coverage solutions.