Auteur: Arnoud Bruinsma is oprichter van BSM Business Security Management BV. Daarnaast is hij meer dan 20 jaar actief in het werkveld van cybersecurity en cybercrime. Hij is bereikbaar via: a.bruinsma@bsm.nl

ClickFix: een opvallend effectieve aanvalstechniek

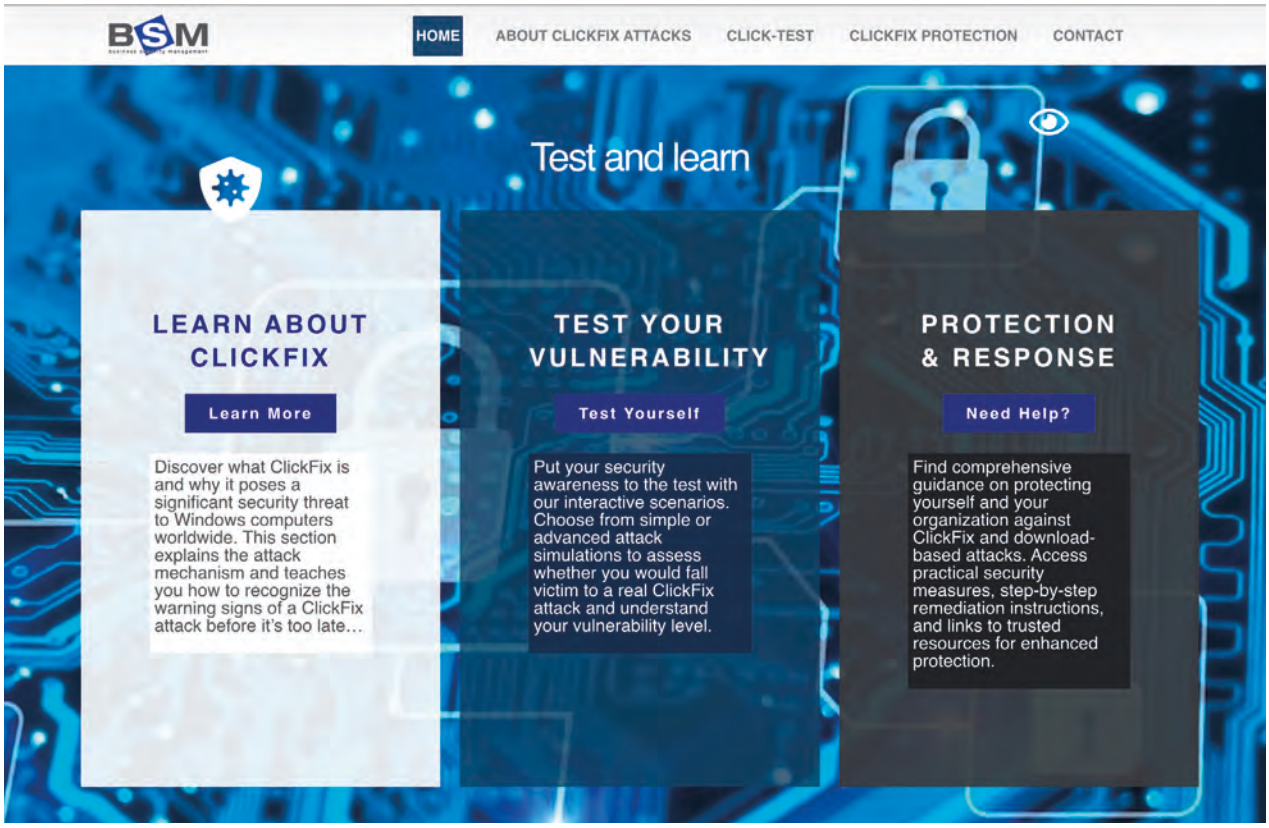
Sinds 2024 is een aanvalstechniek in opkomst die zich onderscheidt door eenvoud, effectiviteit en het vermogen om traditionele beveiligingsmaatregelen te omzeilen. Deze methode — bekend onder de naam ClickFix — maakt geen gebruik van zero-days of complexe exploits, maar combineert geraffineerde social engineering met legitieme systeemfunctionaliteit. In 2025 en 2026 is deze techniek verantwoordelijk voor een aanzienlijk aandeel in succesvolle malware-infecties wereldwijd.

In dit artikel wordt uiteengezet hoe ClickFix werkt, waarom bestaande beveiligingsmaatregelen vaak tekortschieten, hoe organisaties hun kwetsbaarheid kunnen testen en welke technische en organisatorische maatregelen de risico's kunnen beperken.

Social engineering als aanvalsvector

ClickFix-aanvallen creëren een geloofwaardige situatie waarin de gebruiker wordt verleid om zelf handelingen uit te voeren. Voorbeelden hiervan zijn: meldingen over vermeende browserupdates, foutmeldingen van ogenschijnlijk legitieme Microsoft- of Google-diensten, documentfouten die aanvullende stappen vereisen, nep-CAPTCHA-verificaties en beveiligingswaarschuwingen over een vermeend gecompromitteerd account. De verspreiding vindt vaak plaats via gecompromitteerde websites waarop de aanvalsketen is geplaatst, al wordt ClickFix regelmatig gecombineerd met phishing e-mails die de gebruiker naar zo'n pagina leiden.

De kern van de aanval bestaat uit één ogenschijnlijk onschuldige handeling: een klik op een webpagina of HTML-opgemaakte tekst. Omdat de gebruiker vervolgens zélf — onbedoeld — het script uitvoert, wordt veel werkplekbeveiliging eenvoudig omzeild. ClickFix maakt daarmee misbruik van een fundamentele zwakte in veel beveiligingsarchitecturen. Kenmerkend voor deze aanval is dat er geen exploit



Afbeelding 1: homepage click-fix.nl

wordt gebruikt en dat er geen softwarekwetsbaarheid wordt misbruikt. Een volledig lege Windows 11 laptop is voldoende om ClickFix-aanvallen te laten slagen.

ClickFix-aanvallen maken misbruik van legitieme systeemfunctionaliteit en gebruikersgedrag, waardoor traditionele beveiligingsmaatregelen vaak geen effectieve bescherming bieden.

De verschuiving is duidelijk: de aanval verplaatst zich van technische kwetsbaarheidsexploitatie naar gedragsmanipulatie. Dit deed zich eerder voor bij Adversary-in-the-Middle (AiTM)-phishingaanvallen. Het verschil is echter dat ClickFix niet alleen inloggegevens kan compromitteren, maar dat het potentieel direct volledige controle over de werkplek kan opleveren. Daarmee slaat de aanval meerdere traditionele stappen in de aanvalsketen over, zoals: exploitontwikkeling, privilege escalatie via kwetsbaarheden en klassieke malware-delivery. Dit maakt ClickFix risicovoller dan klassieke phishing, omdat één succesvolle interactie voldoende is om volledige controle over de werkplek te verkrijgen.

Gecontroleerd "spelen met virussen"

Om de werking van ClickFix beter te begrijpen, hebben wij onderzocht of we een ClickFix-aanval zelf konden nabootsen in een gecontroleerde testomgeving. Daarbij wilden we niet alleen het aanvalsscenario reproduceren, maar ook analyseren in hoeverre bestaande securitytooling dergelijke aanvallen detecteert of blokkeert.

Tijdens dit onderzoek ontstond het idee om een publieke testomgeving te ontwikkelen. Het resultaat is een voorbeeldwebsite die – vergelijkbaar met het bekende EICAR-testbestand voor antivirussoftware – gebruikt kan worden om ClickFix-scenario's veilig te simuleren.

De website stelt securityprofessionals en organisaties in staat om hun eigen werkplekken te testen en tegelijkertijd inzicht te krijgen in de werking van deze aanvalstechniek. Gebruikers kunnen het scenario in een gecontroleerde omgeving ervaren, waardoor zowel technische detectie als gebruikers-

Afbeelding 2: basic flow

bewustzijn kan worden geëvalueerd. Via https://click-fix.nl kan iedere organisatie haar eigen werkplekken eenvoudig testen.

De testscenario's

Via deze website wordt (momenteel in het Engels) uitgelegd hoe ClickFix werkt, welke tegenmaatregelen mogelijk zijn en als belangrijkste onderdeel drie verschillende testscenario's doorlopen. De meest eenvoudige test — de Basic Security Test — simuleert een eenvoudig maar effectief ClickFix-scenario. Hoewel de gemiddelde IT-professional deze aanval snel zal herkennen, blijkt dat veel reguliere Windows-gebruikers inmiddels gewend zijn geraakt aan het uitvoeren van ongebruikelijke handelingen, zoals CAPTCHA-verificaties. Waar men voorheen afbeeldingen van motoren of bruggen moest selecteren, wordt nu gevraagd bepaalde toetscombinaties uit te voeren. De essentie van de aanval is dat één klik op een webpagina ongemerkt een script naar het klembord kan kopiëren, zonder dat de gebruiker zich daarvan bewust is. Wanneer u na het uitvoeren van de Basic Security Test een pop-up ziet met de melding "Your PC is hackable", dan is uw werkplek technisch kwetsbaar voor dit type aanval en is het raadzaam aanvullende maatregelen te overwegen.
Naast de basistest — die uitsluitend een onschuldige pop-up toont — zijn ook een Advanced Test en een Download Test ontwikkeld. Deze varianten zijn eveneens ongevaarlijk, maar ingrijpender van opzet en testen aanvullende beveiligingslagen van de werkplek. Daarom is vooraf acceptatie van de gebruiksvoorwaarden vereist.

De Advanced Test demonstreert hoe - via een in PowerShell op de achtergrond gestreamd uitvoerbaar bestand - code kan worden uitgevoerd. In de testomgeving wordt vervolgens, als bewijs van een geslaagde aanval, de camera gestart en een foto gemaakt, die de computer niet verlaat, waarna de webpagina met de poll wordt geopend. De derde variant vereist dat de gebruiker zelf een bestand downloadt en uitvoert. Deze test biedt waardevolle inzichten voor securityprofessionals, zoals komen er downloadwaarschuwingen of niet? Hoe reageert de gebruiker op downloadwaarschuwingen? Op welk beveiligingsniveau (netwerk, browser, AV) wordt de test geblokkeerd? Is het mogelijk om een uitvoerbaar bestand uit te voeren vanuit de downloadmap?

Topje van de ijsberg

In onze praktijk als cybercrime-onderzoekers en operationeel securitytesters hebben wij de afgelopen maanden vastgesteld dat een groot deel van alle onderzochte werkplekken kwetsbaar zijn voor ClickFix. Daarnaast blijkt uit gesprekken met medewerkers, en met securityspecialisten, dat de kennis over deze aanvalsmethode beperkt is en dat het risico mogelijk structureel wordt onderschat. Een interessant aspect van ClickFix is dat deze aanval zich grotendeels onttrekt aan traditionele antivirusdetectie, omdat de gebruiker zelf – via legitieme functionaliteit – de aanval activeert. Daarmee wordt feitelijk een beveiligingsmechanisme omzeild zonder dat er direct sprake is van een klassieke exploit. Hoewel de techniek relatief nieuw lijkt, laat onderzoek zien dat ClickFix zich in korte tijd razendsnel heeft ontwikkeld en inmiddels ook wordt toegepast in grootschalige cybercrimecampagnes en zelfs in statelijke spionageoperaties. De onderstaande tijdslijn laat zien hoe snel deze aanvalsmethode zich heeft ontwikkeld:

Tijdslijn van ClickFix-aanvallen

Oktober 2023 — eerste waarnemingen
Onderzoekers signaleren vroege varianten van wat later ClickFix-achtige aanvallen worden genoemd. De techniek bestaat al, maar krijgt nog weinig aandacht.

Maart 2024 — naam "ClickFix" verschijnt
Securitybedrijf Proofpoint introduceert de term ClickFix, nadat de tactiek wordt waargenomen in phishingcampagnes van initial-access-broker TA571. In dezelfde periode observeert Microsoft de ClickFix-campagnes die zij volgen onder de aanduiding Storm-1607.

Mei 2024 — eerste grootschalige campagnes
Storm-1607 verstuurt tienduizenden phishingmails naar organisaties in de VS en Canada. De aanvallen leveren

onder andere DarkGate-malware af en tonen dat de methode op grote schaal inzetbaar is.

Oktober–november 2024 — adoptie door statelijke actoren
De techniek wordt ook gebruikt in spionagecampagnes. Onder meer statelijke actoren zoals APT28 (Rusland) en MuddyWater (Iran) passen ClickFix toe in gerichte phishing-operaties. Tegelijk verschijnen kant-en-klare builders op cybercrimefora.

Januari 2025 — Noord-Korea sluit aan
Onderzoekers detecteren dat Kimsuky (TA427) ClickFix gebruikt in spionagecampagnes. Daarmee wordt de techniek binnen korte tijd toegepast door meerdere statelijke actoren.

Eerste helft 2025 — sterke wereldwijde groei
Onderzoek van ESET laat zien dat het gebruik van ClickFix-achtige technieken met meer dan 500% is toegenomen. Nieuwe varianten verschijnen, waaronder macOS-gerichte campagnes en afgeleiden zoals FileFix.

ClickFix tegengaan

De voorgaande analyse laat zien hoe ClickFix-aanvallen misbruik maken van legitieme systeemfunctionaliteit en gebruikersgedrag. In dit afsluitende deel worden enkele praktische verdedigingsmaatregelen besproken.

De mens
Gebruikers leren in de praktijk doorgaans meer door te doen dan door te lezen. Wanneer een realistische doorloop of simulatie met een gebruiker wordt uitgevoerd, ontstaat er een veel duidelijker besef van het risico van bijvoorbeeld de Windows-R - toetscombinatie. Als deze toetscombinatie binnen de organisatie niet of nauwelijks wordt gebruikt, kan het risico in de basis al aanzienlijk worden beperkt. Bewustwording en gedragsverandering vormen daarmee een essentieel onderdeel van de verdediging tegen ClickFix.

De techniek
Het is belangrijk om te begrijpen dat gangbare digitale hygiënemaatregelen – zoals: het installeren van antivirus-software, het toepassen van MFA op alle accounts, het tijdig updaten van besturingssystemen en applicaties en het maken van back-ups – op zichzelf géén bescherming bieden tegen ClickFix. Maatregelen die wél effectief kunnen zijn, richten zich met name op het beperken van misbruik van legitieme systeemfunctionaliteit. Zo kan het uitschakelen van de Windows R toetscombinatie het risico aanzienlijk verkleinen, net als het blokkeren van het uitvoeren van scripts. Daarnaast kan het beperken of volledig blokkeren van PowerShell en opdrachtpromptgebruik bijdragen aan het verminderen van de aanvalsmogelijkheden. Ook het blokkeren van scriptuitvoer via e-mail kan een belangrijke rol spelen in het voorkomen van ClickFix-aanvallen.
Voor bescherming tegen geavanceerdere varianten kunnen aanvullende maatregelen worden overwogen. Daarbij valt te denken aan het toepassen van application whitelisting en het blokkeren van het uitvoeren van applicaties vanuit tijdelijke mappen of de downloadmap. Verder kan het ontwikkelen van detectiemechanismen voor het injecteren van kwaadaardige scripts in het klembord helpen om deze aanvallen eerder te herkennen en te stoppen. Ook kan onderzocht worden of het mogelijk is om het kopiëren van scripts naar het klembord te detecteren via eigen detectiescripts of – bij voorkeur – via endpoint-beveiligingssoftware die ClickFix als serieuze dreiging herkent en blokkeert.

Tot slot

Met de website click-fix.nl beschikt u over een praktische testomgeving om uzelf, uw organisatie en uw klanten te toetsen op kwetsbaarheid voor dit type aanval. Door de test zelf te ervaren wordt sneller duidelijk hoe eenvoudig gebruikers tot het uitvoeren van een kwaadaardig script kunnen worden verleid. Wij stellen het zeer op prijs als u na afloop van een test de poll op https://click-fix.nl/poll invult. De resultaten helpen ons om een beter beeld te krijgen van de werkelijke impact van ClickFix-achtige aanvallen en van de mate waarin bestaande beveiligingsmaatregelen deze technieken herkennen of blokkeren. Mocht u oplossingen tegenkomen die deze aanval wél detecteren of voorkomen, dan horen wij dat uiteraard graag. Op basis van de ervaringen en resultaten die de komende periode worden verzameld, hopen wij in een volgend artikel verder in te gaan op de effectiviteit van bestaande beveiligingsmaatregelen en mogelijke verbeteringen.

Referenties

Proofpoint – introductie en analyse van de ClickFix-techniek (TA571)
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
Proofpoint – ClickFix verspreidt zich snel in phishingcampagnes
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
Proofpoint – statelijke actoren gebruiken ClickFix (APT28, MuddyWater, Kimsuky)
https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix
ESET Threat Report – sterke wereldwijde groei van ClickFix-aanvallen
https://www.eset.com/us/business/threat-report/
Eicar testvirus: https://eicar.org