ATTIC

2024-2025 AitM Threat Report

Gebaseerd op detectiegegevens afkomstig van het Attic Lab-platform in didsomeoneclone.me en Attic Bouncer voor M365

ATTIC

Erik Remmelzwaal

CEO, Co-founder

AitM is de grootste cyberdreiging van nu. Het is het criminele antwoord op multi-factor authenticatie.

“

Wie mediaberichten over incidenten goed leest, ziet in dat ze vaak niet meer starten met een computervirus of gehackte webservers. Maar met ‘phishing-links’ of ‘ingelogde sessies’. Ben je verantwoordelijk voor cyberweerbaarheid? Dan kan je maar beter zorgen dat je AitM goed begrijpt.

Executive Summary

De omvang van de AitM-dreiging moet op bestuursniveau bekend zijn om moeilijke beslissingen over maatregelen te steunen.

1 van 5

Elk kwartaal wordt 20% van de bedrijven gehackt door een nep-inlogpagina die de AitM-techniek gebruikt om multi-factor authenticatie te omzeilen.

Indentity = Perimeter

Door thuiswerken en de cloud is de identiteit van een gebruiker vaak de enige bescherming van gevoelige data. Overweeg sterkere MFA, gelaagde beveiliging.

Kennisdeling

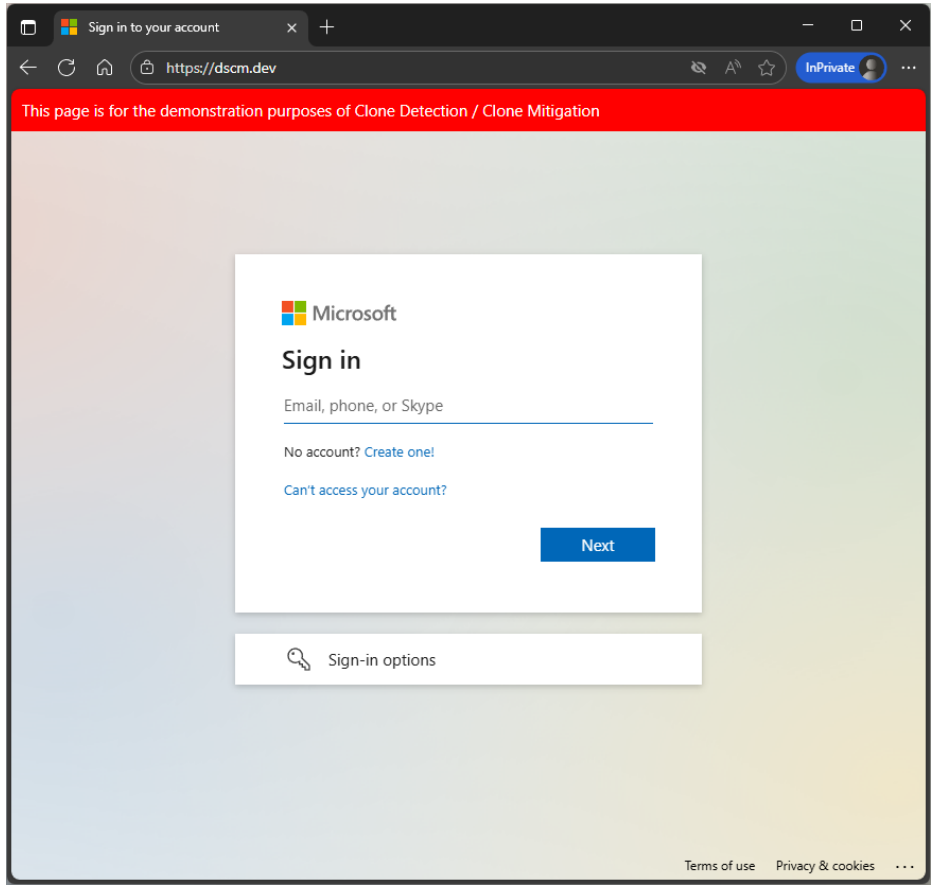
AitM-aanvallen zijn vaak zeer breed van aard en richten zich niet specifiek op één bedrijf. Het delen van dreigingsinformatie vergroot de cyberweerbaarheid van allen.

User Awareness

Gebruikers hebben moeite met het herkennen van de nep-inlogpagina's die bij AitM-aanvallen worden gebruikt. Vooral rondom de lunch op dinsdag lijken ze veel te klikken.

Het probleem

Adversary-in-the-Middle (AitM) introduceert een nieuwe innovatie in Phishing, waarmee multi-factor authenticatie omzeild wordt.



In tegenstelling tot traditionele phishingwebsites fungeert crimeware die wordt gebruikt in AitM-aanvallen zoals Evilginx, niet als een webserver. In plaats daarvan is het een proxyserver die tussen het slachtoffer en de legitieme website staat. De proxy maakt namens het slachtoffer verbinding met een webserver, haalt de website op en stuurt een kopie ervan naar het slachtoffer.

Op deze manier wordt alle interactie tussen slachtoffer en server doorgegeven, inclusief gebruikersnaam, wachtwoord en uiteindelijk de token voor de ingelogde sessie. Deze token kan vervolgens worden geladen in de browser van de aanvaller om toegang te krijgen tot de ingelogde sessie. Van daaruit kunnen ze alles namens het slachtoffer doen, wat kan leiden tot incidenten zoals diefstal van zakelijke e-mails, factuurfraude, datadiefstal, ransomware, enzovoort.

Learn More Here

Scope & methodologie

Data uit eigen detectie backend van Attic Security en Didsomeoneclone.me

In januari 2024 lanceerde Attic een detectieservice die werkt door dynamische CSS-code te plaatsen in de company branding instellingen in Entra ID van een M365-tenant. Gedurende het jaar werd deze service geïnstalleerd door klanten van didsomeoneclone.me en Attic voor M365. Dit rapport is gebaseerd op daadwerkelijke detecties die in dezelfde backend terechtkomen. Lees deze blog over de oorspronkelijke techniek.

1592 bezoeken aan AitM sites.
492 echte kliks.

Scope: juli 2024 – juni 2025.

Filters: InvalidVictim=TRUE verwijderd (Microsoft's eigen scans), ParsedClonedDomain=dscm.dev uitgesloten.

NL-subset: alleen notificaties waarbij Mail van de klant eindigt op **.nl**.

Campagnereuse: telling op geldige kliks;

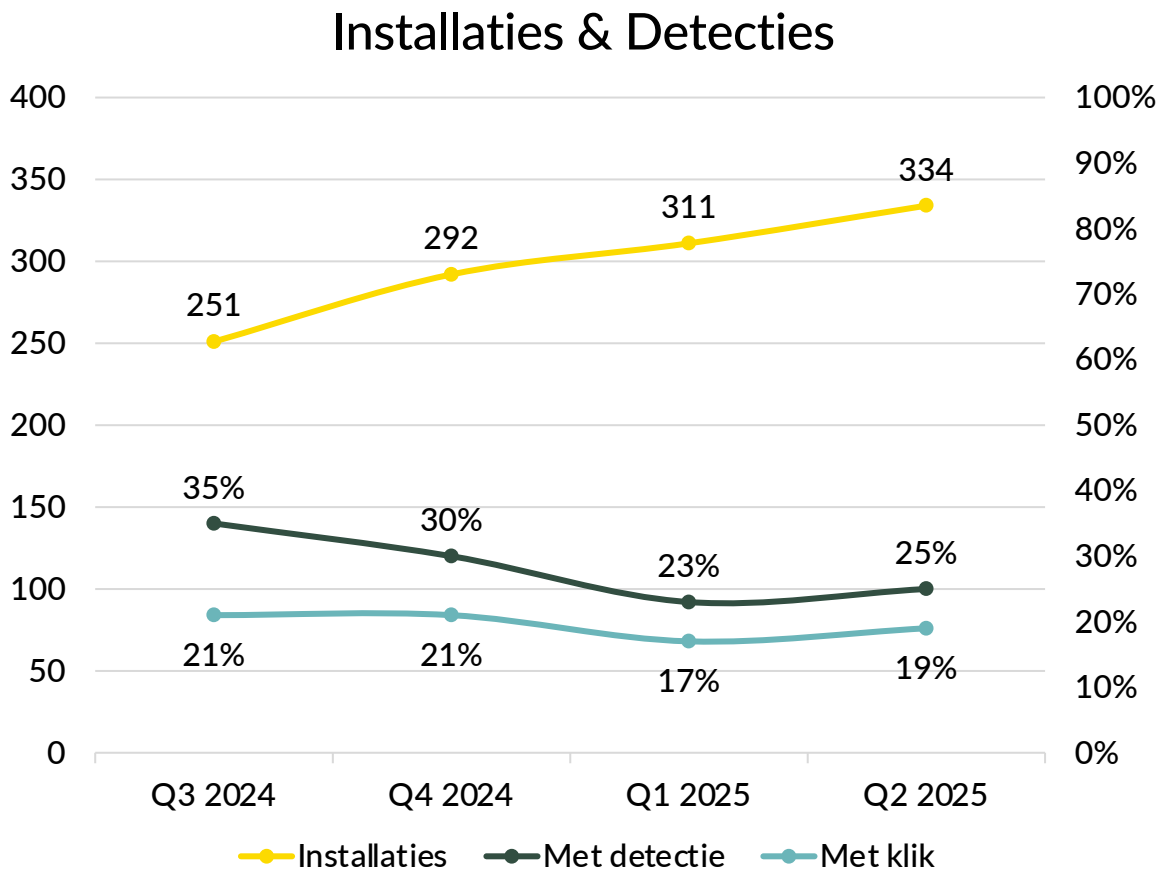
Perimeter: op basis van ASN vanuit ipinfo.io

Installaties & Detecties

Hoeveel organisaties werden getroffen?

1 van 5 organisaties
wordt slachtoffer per kwartaal

Elk kwartaal werd gemiddeld bij 28% van de aangesloten organisaties tenminste 1 AiTM detectie geconstateerd. In een deel van de gevallen werd dat veroorzaakt door de scanprocessen van Microsoft, maar het grootste deel door medewerkers die daadwerkelijk de link hebben aangeklikt en in elk geval zover zijn gegaan als het invullen van het emailadres.

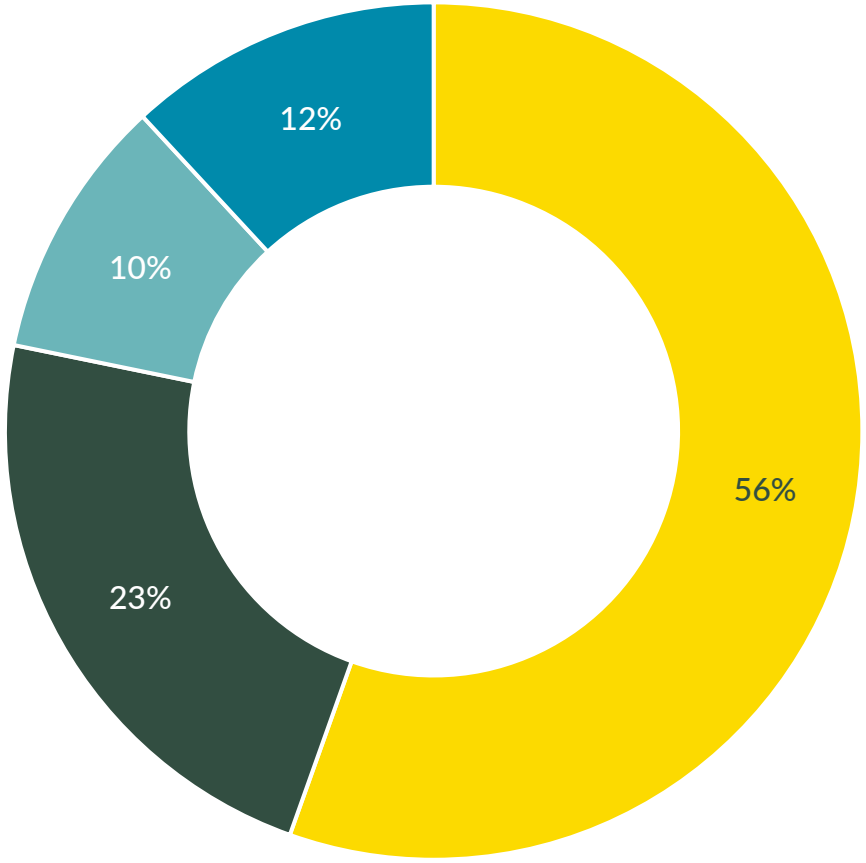


Netwerkcontext – NL

Hoe zijn slachtoffers verbonden met het internet als zij de phishing site bereiken?

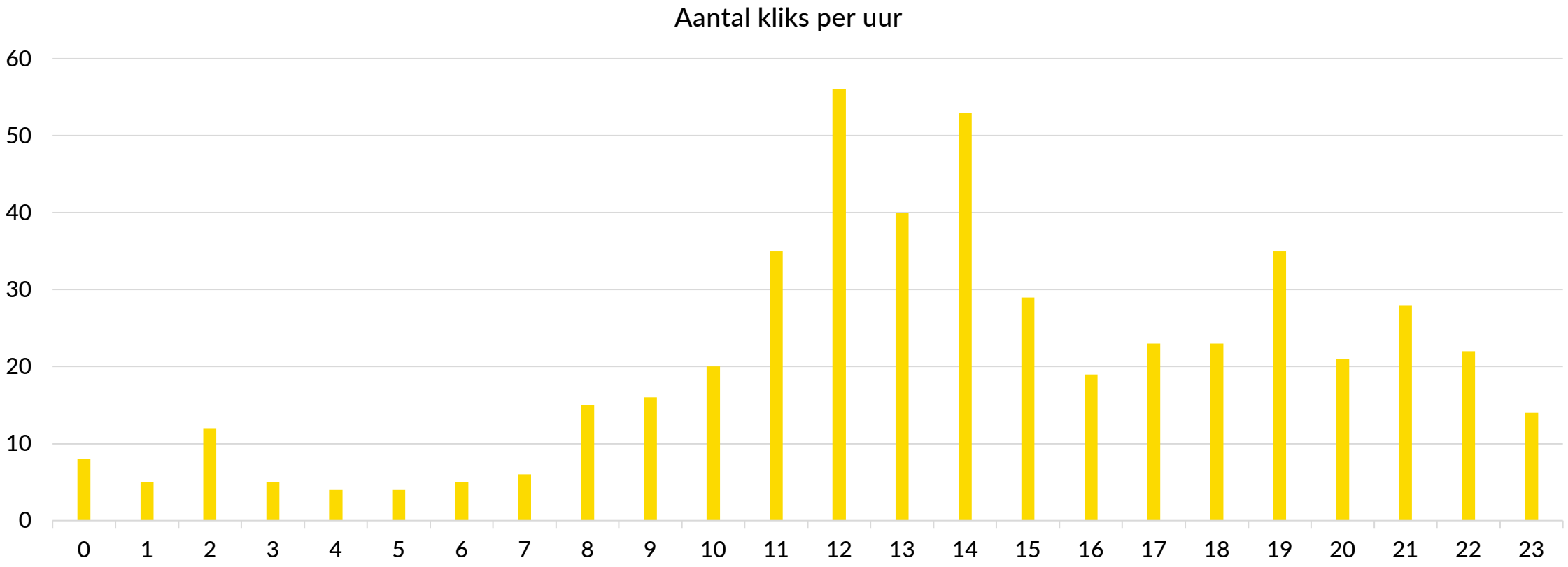
44% van bezoeken gebeurt van buiten de corporate perimeter.

Bijna de helft van de kliks gebeurt door medewerkers die op dat moment niet van de corporate internetverbinding gebruik maken. In 23% van de gevallen betreft het een particuliere/mobiele verbinding en is men waarschijnlijk thuis of onderweg, buiten de bescherming van eventuele netwerkbeveiliging van de organisatie.



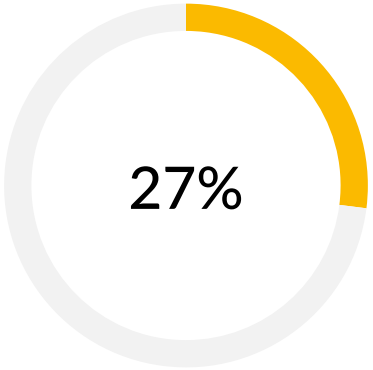
Tijdstip van Klikken – NL

Slachtoffers bezoeken de AitM sites het vaakst op dinsdagen en rond lunchtijd.



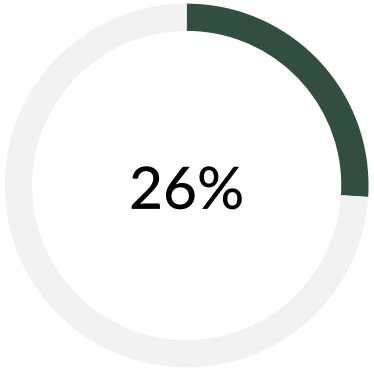
Hergebruik en spreiding

AitM-phishingsites worden gebruikt in brede campagnes en komen bij meerdere organisaties terecht



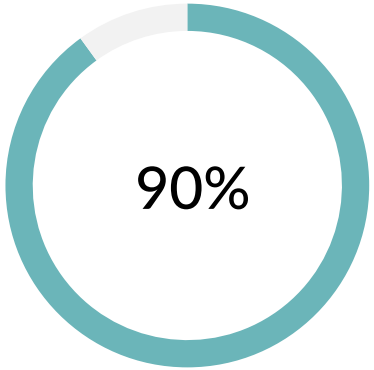
>1 detectie

Aantal unieke phishing URLs dat meerdere keren werd bezocht. Vaak dezelfde dag (<4 uur), soms met veel dagen ertussen.



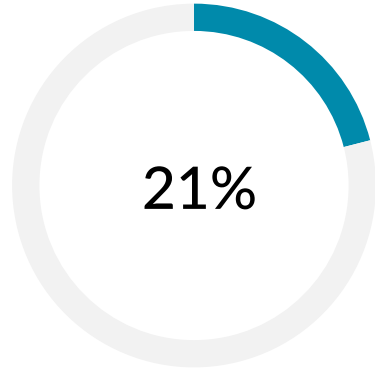
Bij >1 organisaties

Aantal unieke phishing URLs dat vanuit meerdere organisaties werd bezocht. Uitwisselen van dreigingsinformatie heeft dus zin.



Microsoft scans

Aantal duplicaten waarbij tenminste 1 detectie werd veroorzaakt door een Microsoft scan, door Defender of SafeLinks.



Niet altijd effectief

Aantal keren dat een URL die eerst door Microsoft werd gescand, daarna nog werd bezocht door een mens.

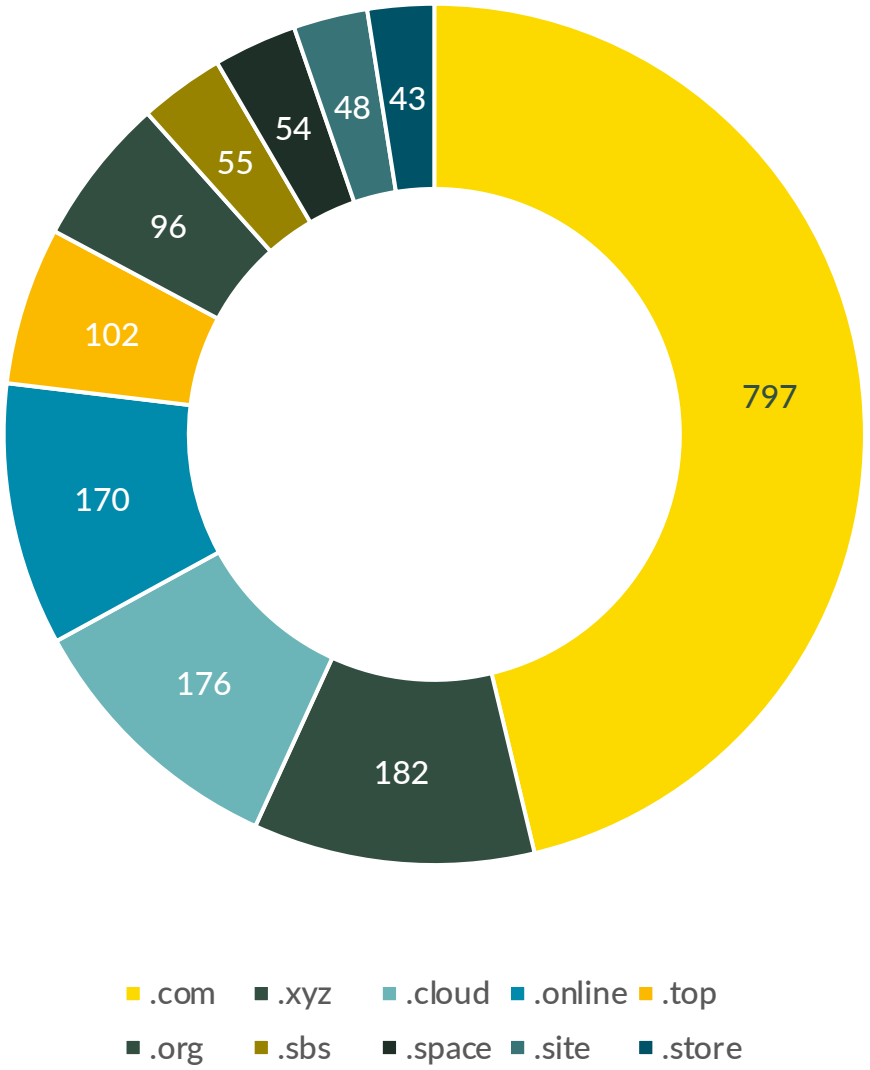
Domeinextensies - intel

Geregistreerde phishingdomeinen en hun TLD's

Gevonden door proactief AitM fingerprinting van nieuwe domeinen.

Phishing domeinen worden vooral in .com geregistreerd, maar daarna zijn domeinextensies popular die minder bekend zijn, zoals .xyz en .sbs. Vermoedelijk omdat daar de registratie eenvoudiger of goedkoper voor is.

Daarnaast gebruiken aanvallers graag herkenbare woorden in de domeinnaam, zoals office, onedrive, sharepoint, enzovoorts.

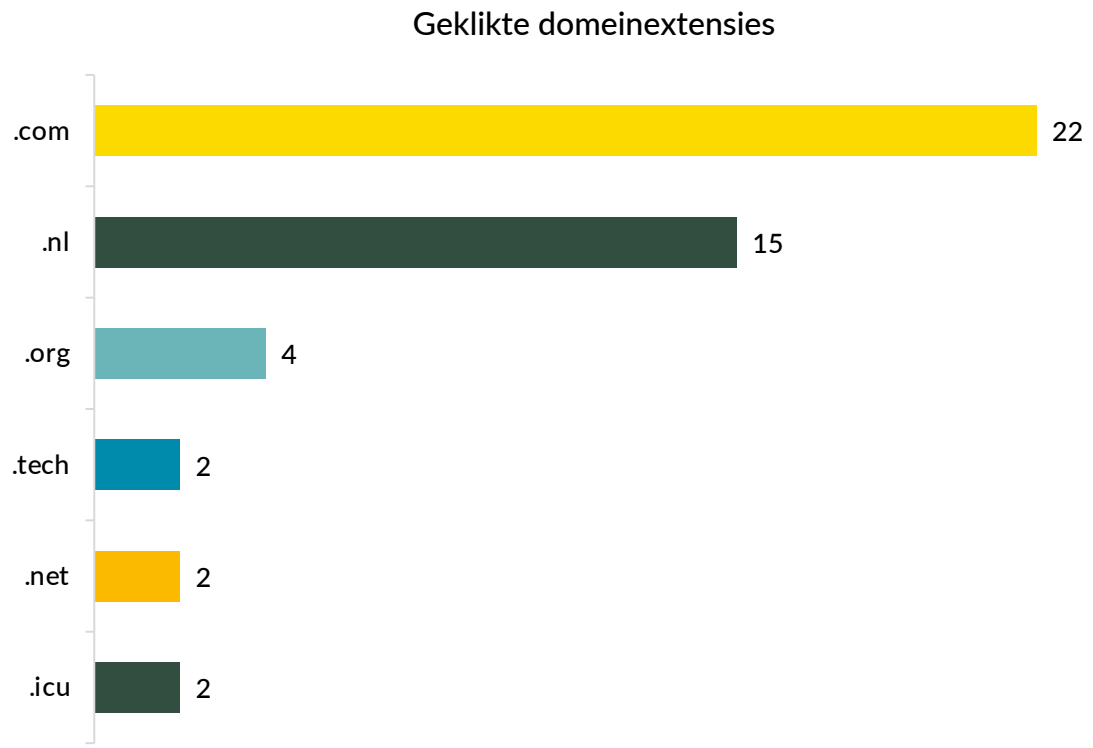


Domeinextensies – clicks

Welke extensie hebben de phishingdomeinen waar Nederlandse slachtoffers in trappen?

.com and .nl zijn het meest betrouwbaar en dus misleidend .

Ook al blijkt uit de intel dat aanvallers graag risky TLD's (domeinextensies) gebruiken, Nederlandse slachtoffers lijken vooral misleid te worden door bekende extensies zoals .com en .nl



Aanbeveling #1

Om uw organisatie te beschermen tegen de gevolgen van AitM Phishing

Phishing-resistente MFA: FIDO2 hardwarekey of passkey

Forceer phishing-resistente MFA voor beheerders zo snel mogelijk. FIDO2 USB sleutels zoals Yubikeys en Passkeys zijn phishing-resistent. Wanneer gebruikers gedwongen worden om met een dergelijke MFA methode aan te melden, zijn zij niet langer kwetsbaar voor AitM.

Token-binding kan voor sommigen al werken, maar heeft nog beperkingen.

learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2

Aanbeveling #2

Om uw organisatie te beschermen tegen de gevolgen van AitM Phishing

AitM Interventie in Company Branding

Toon een duidelijke waarschuwing aan gebruikers wanneer zij een bekende AitM phishing site bezoeken. Dit is mogelijk via dynamische configuratie in de Company Branding settings van Entra ID.

Attic biedt een gratis service om dit eenvoudig te activeren en alarmen te verwerken.

atticsecurity.com/free

Aanbeveling #3

Om uw organisatie te beschermen tegen de gevolgen van AitM Phishing

Conditional Access & MDM van buiten perimeter

Compliance based authenticatie maakt hergebruik van een token vanaf een onbekend device onmogelijk. Minder BYOD friendly maar wel een effectief middel tegen deze vorm van misbruik.

Als dit niet werkt voor de hele organisatie, overweeg het dan alsnog voor een deel toe te passen.

learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-device-compliance

Aanbeveling #4

Om uw organisatie te beschermen tegen de gevolgen van AitM Phishing

IOC-delen &
snelle takedowns

Door URLs en IP's van geïdentificeerde AitM sites uit te wisselen, kan detectie bij hergebruik worden versneld.

Bovendien kan dit helpen bij de takedown van dergelijke sites, waardoor ze uberhaupt niet meer in de lucht zijn.

stats.didsomeoneclone.me

Aanbeveling #5

Om uw organisatie te beschermen tegen de gevolgen van AitM Phishing

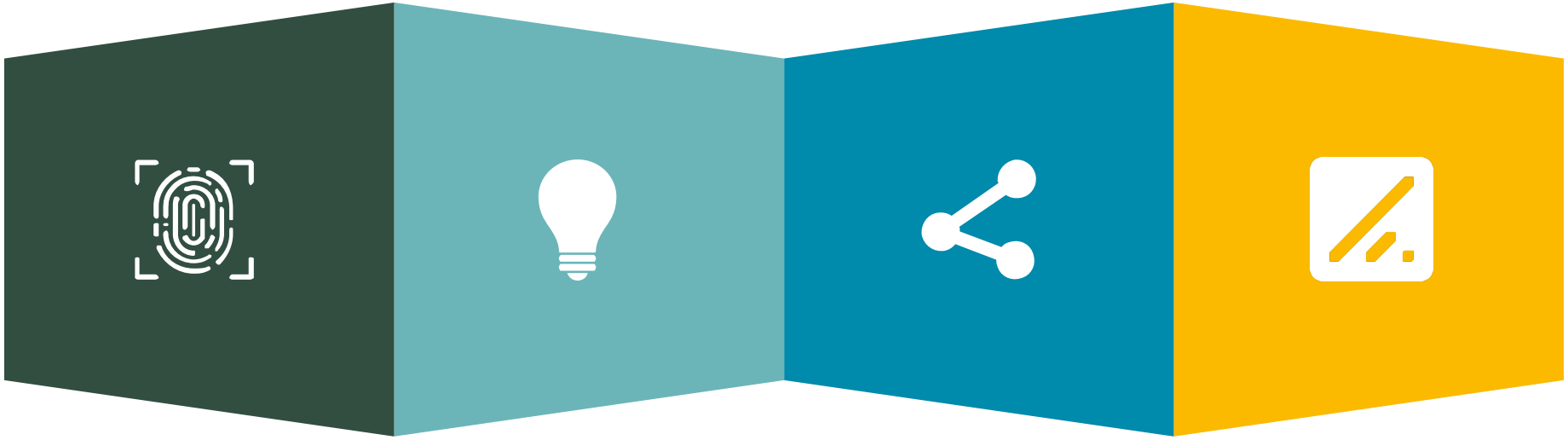
Stimuleer extra awareness rond lunchtijd

Realiseer dat klikgedrag voornamelijk ontstaat rondom lunchtijd. In het user awareness programma kan nagedacht worden over manieren om juist op die tijdstippen medewerkers te attenderen op risico's.

atticsecurity.com/awareways

Samenvatting & Call-to-Action

Wrap up



Identity = Perimeter

Identiteit is de nieuwe perimeter. Slechts één controle om toegang te krijgen tot uw data. Prioriteer implementatie van sterke, gelaagde verdediging.

Risicobewustzijn

Investeer in het bewustzijn van gebruikers over de groeiende dreiging van AitM, vooral tijdens de lunchpauze op dinsdag, wanneer de oplettendheid blijkbaar laag is.

Reuse

Registreer en deel IOC's van uw detecties met collega's om de weerbaarheid van ons allemaal te verbeteren. Gebruik oplossingen die buiten de bedrijfsgrenzen werken.

Wanna know more?

Volg Attic Security op social media. Meld u aan voor onze nieuwsbrief of maak een gratis account aan in MyAttic.app en activeer onze gratis diensten.

Onze dienst: Attic #BOUNCER

Voorkom dat hackers via de voordeur uw organisatie binnendringen.

CYBERSECURITY™
MADE IN EUROPE

#01 AitM interventiescherm

Beveilig het Microsoft365-inlogportaal met slimme CSS-code die detecteert dat er een proxy wordt gebruikt en verandert in een rood waarschuwingssignaal.

#02 Monitoring aanmeldingslogboek

Vergelijk patronen uit uw aanmeldingslogboeken met de nieuwste bedreigingsinformatie en identificeer gebruikers die AitM-pagina's bezoeken.

#03 AitM Blocker Browser Plugin

Implementeer een extensie voor Chromium-browsers (Chrome, Edge) om de toegang tot bekende AitM-sites te blokkeren op basis van de meest recente bedreigingsinformatie van proactieve AitM-scanners van Attic Lab.

ATTIC

€ 30,- per maand met 20 gebruikers inbegrepen. € 1,- per extra gebruiker.
Aan de slag in 5 minuten. Begin hier: atticsecurity.com/bouncer

Contact Info.

Op een missie om het mkb weerbaar te maken, voor een veilige gedigitaliseerde toekomst.

Molenstraat 36
4761 CL Zevenbergen

+31 168 794 020

atticsecurity.com

linkedin.com/company/atticsecurity

x.com/attic_security

ATTIC

2024-2025 AitM Threat Report

Gebaseerd op detectiegegevens afkomstig van het Attic Lab-platform in didsomeoneclone.me en Attic Bouncer voor M365