ATTIC

2024-2025 AitM Threat Report

Based on detection data coming from the Attic Lab platform in didsomeoneclone.me and Attic Bouncer for M365

ATTIC

Erik Remmelzwaal

CEO, Co-founder

AitM is the biggest cyber threat today. It's the criminal answer to multi-factor authentication.

“

Anyone who carefully reads media-reported incidents will realize that they often don't start with a computer virus or hacked webservers anymore. But with "phishing links" or "logged-in sessions." Those responsible for cyber resilience would do well to understand the threat of AitM.

Executive Summary

The extent of the AitM threat needs to be understood at C-level to allow tough decision-making about countermeasures.

1 in 5

Each quarter 20% of companies is hacked by a fake login page using AitM technique to circumvent multi-factor authentication.

Indentity = Perimeter

Because of remote working and cloud services, a user's identity often is the only active protection of access to sensitive data. Consider stronger MFA, layered defenses.

Intel Sharing

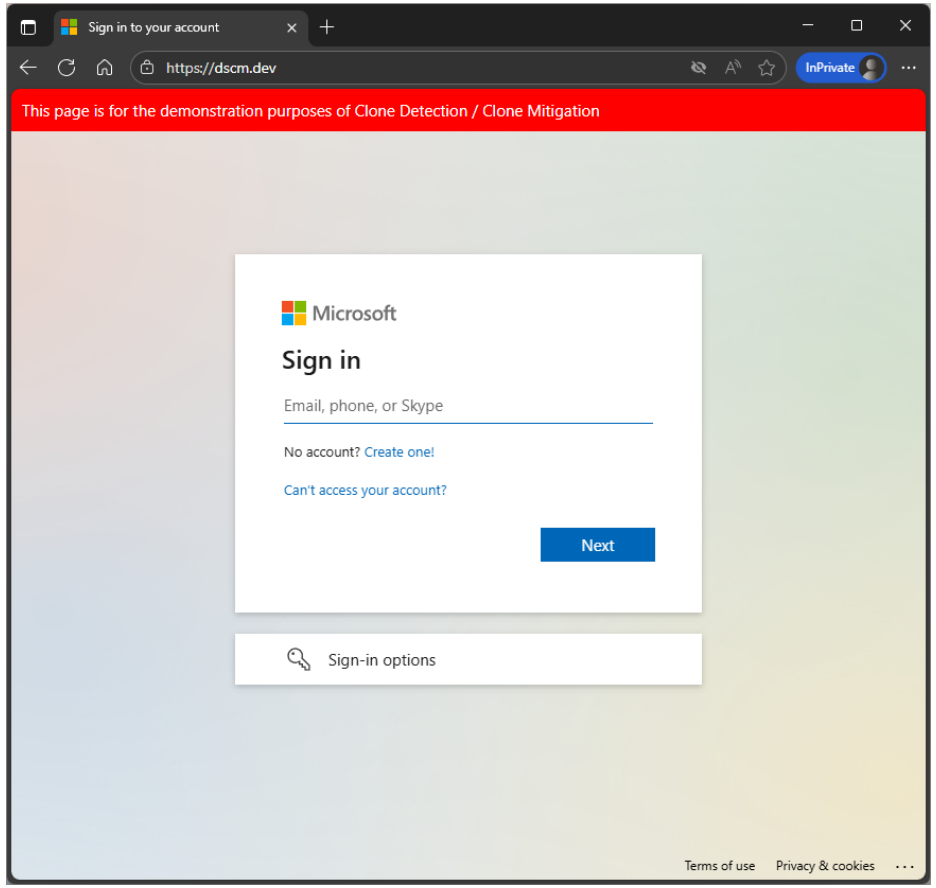
AitM attacks are often very broad in nature, not targeting anyone particularly. Sharing indicators of compromise amongst peers will improve resilience of all.

User Awareness

Users have a hard time recognizing the fake login pages used in AitM attacks. They especially seem to be clicker happy around Tuesday's lunch time.

The Problem

Adversary-in-the-Middle (AitM) introduces a new innovation in Phishing, capable of circumventing multi-factor authentication



Unlike traditional phishing websites, crimeware used in AitM attacks such as Evilginx, does not actually act as a webserver. Instead, it is a proxy server sitting between victim and legitimate website. It connects to a webserver on behalf of the victim, retrieves the website and serves a copy of it to the victim.

It relays all interaction between victim and server this way, including the submission of username, password and ultimately the logged in session token. This token can than be replayed in the attackers' browser to get access to the logged in session. From there, they can perform anything on behalf of the victim. Leading to incidents like Business Email Compromise, Invoice Fraud, Datatheft, Ransomware, etcetera...

Learn More Here

Scope & methodologie

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

In January 2024, Attic launched a detection service which works by placing dynamic CSS code in the company branding settings of a M365 Tenant's Entra ID configuration. Throughout the year this was installed by customers of didsomeoneclone.me and Attic for M365. This report is based on actual detections ending up in the same backend. Read this blog about the initial technique.

1592 visits to AitM sites.
492 real clicks.

Scope: july 2024 – june 2025.

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

NL-subset: only notifications where the customer's mail ends with **.nl**.

Perimeter: based on ASN from ipinfo.io

Scope & methodologie

Data from Attic Security's own detection backend and Didsomeoneclone.me

1592 visits to AitM sites.
492 real clicks.

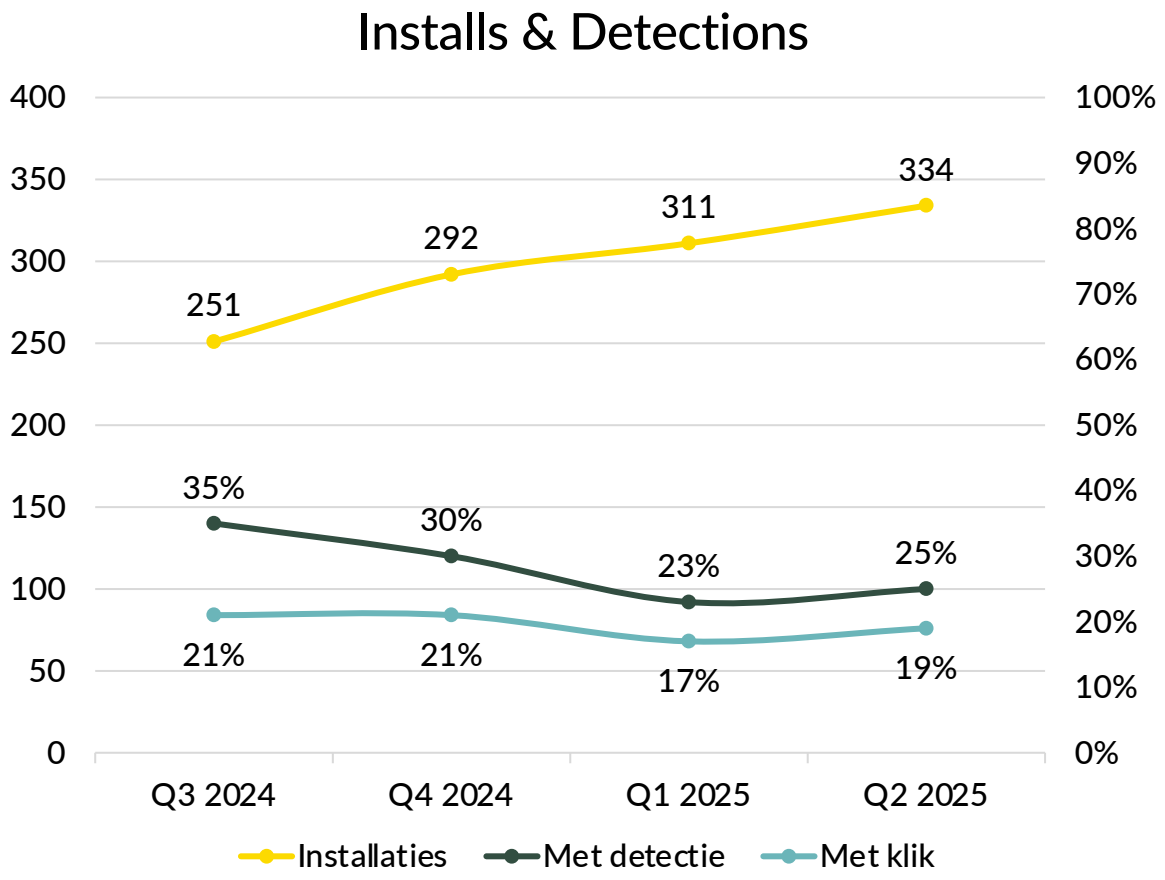
Scope: july 2024 – june 2025.
Filters: InvalidVictim=TRUE verwijderd (Microsoft's eigen scans), ParsedClonedDomain=dscm.dev uitgesloten.
NL-subset: only notifications where the customer's mail ends with **.nl**.
Perimeter: based on ASN from ipinfo.io

Installs & Detections

How many organizations were affected?

1 in 5 organizations
fall victim each quarter

On average, at least one AiTM detection was detected each quarter at 28% of participating organizations. In some cases, this was caused by Microsoft's scanning processes, but most were caused by employees who actually clicked the link and at least went as far as entering their email address.

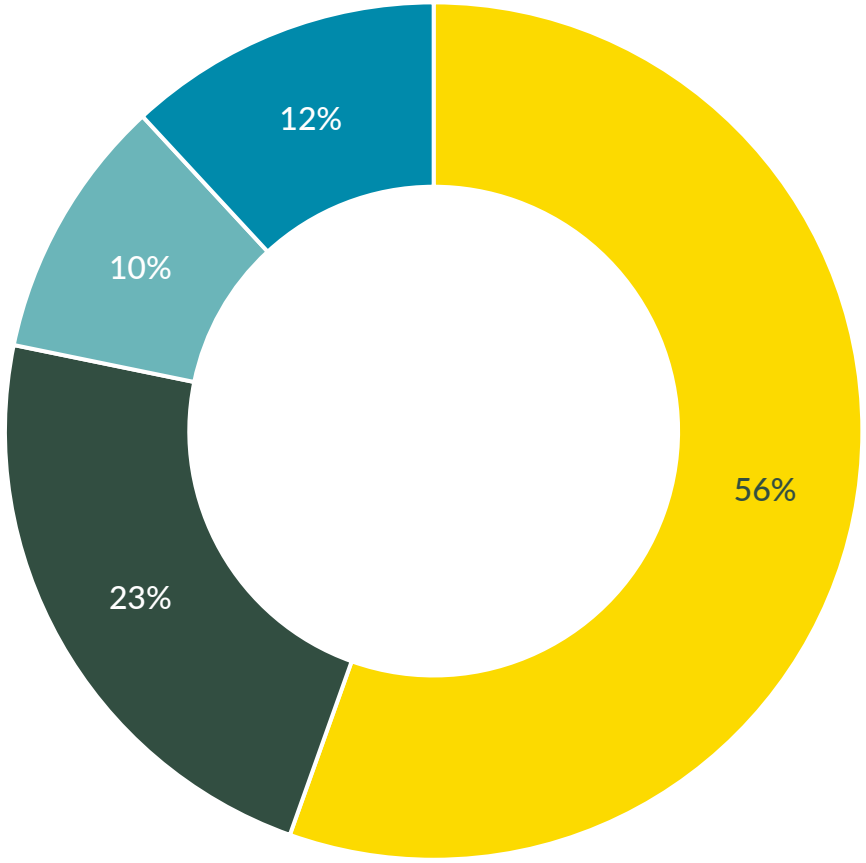


Networkcontext – NL

How are users connected when visiting the phishing page?

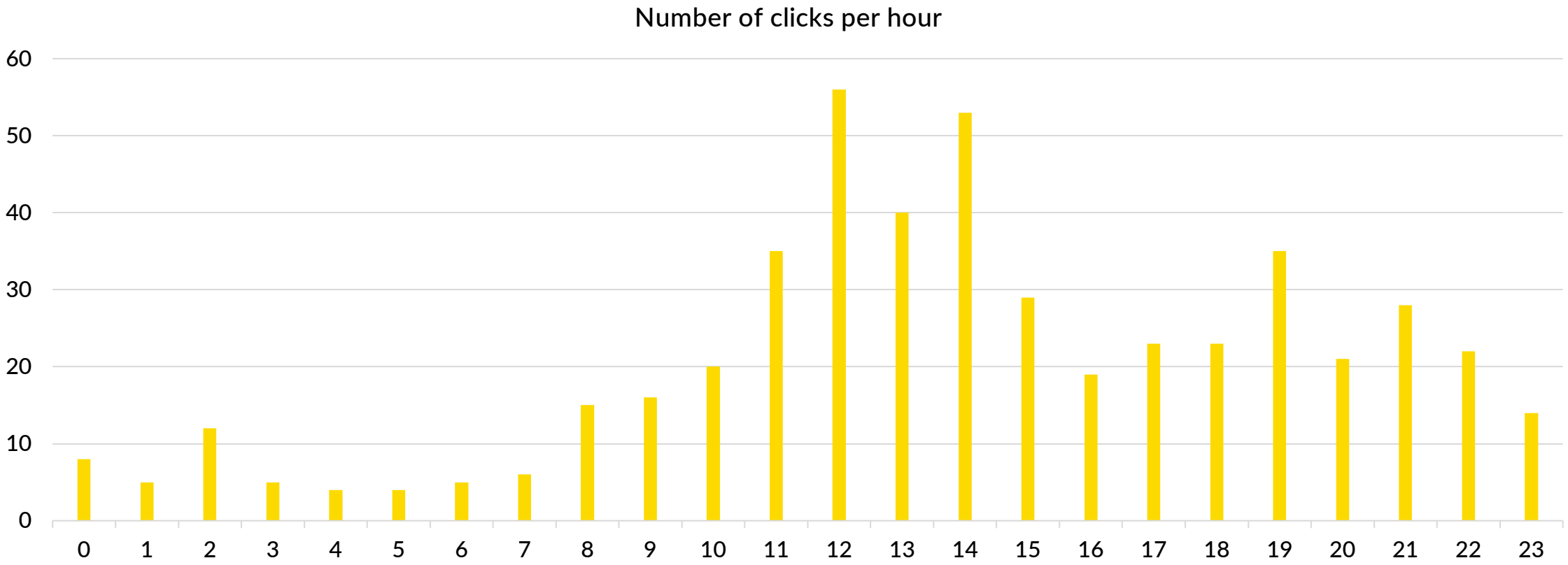
44% of visits are from outside corporate perimeter.

Nearly half of the clicks are made by employees who are not using the corporate internet connection at the time. In 23% of cases, it involves a personal/mobile connection, and the employee is likely at home or on the road, outside the protection of any network security measures the organization might have.



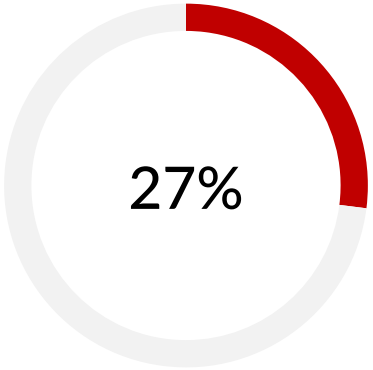
Time of Clicking – NL

Employees mostly visit AitM sites on Tuesdays and during around lunch time



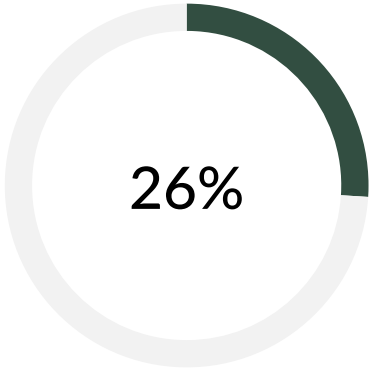
Reuse and spread

AitM phishing sites are used in broad campaigns and end up at multiple organizations



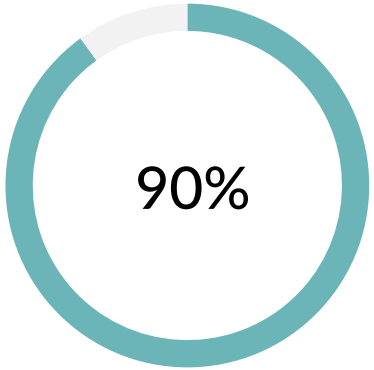
>1 detections

Number of unique phishing URLs visited multiple times. Often on the same day (<4 hours), sometimes with many days between visits.



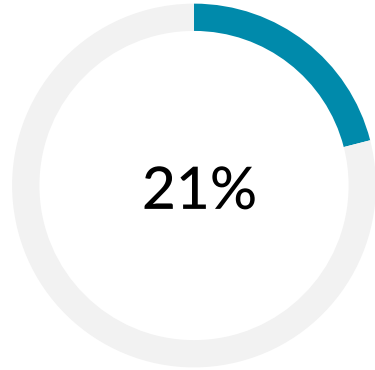
At >1 orgs

The number of unique phishing URLs visited from multiple organizations. Sharing threat intelligence is therefore beneficial.



Microsoft scans

Number of duplicates where at least 1 detection was caused by a Microsoft scan, by Defender or SafeLinks.



No direct effect

Number of times a URL previously scanned by Microsoft was subsequently visited by a human.

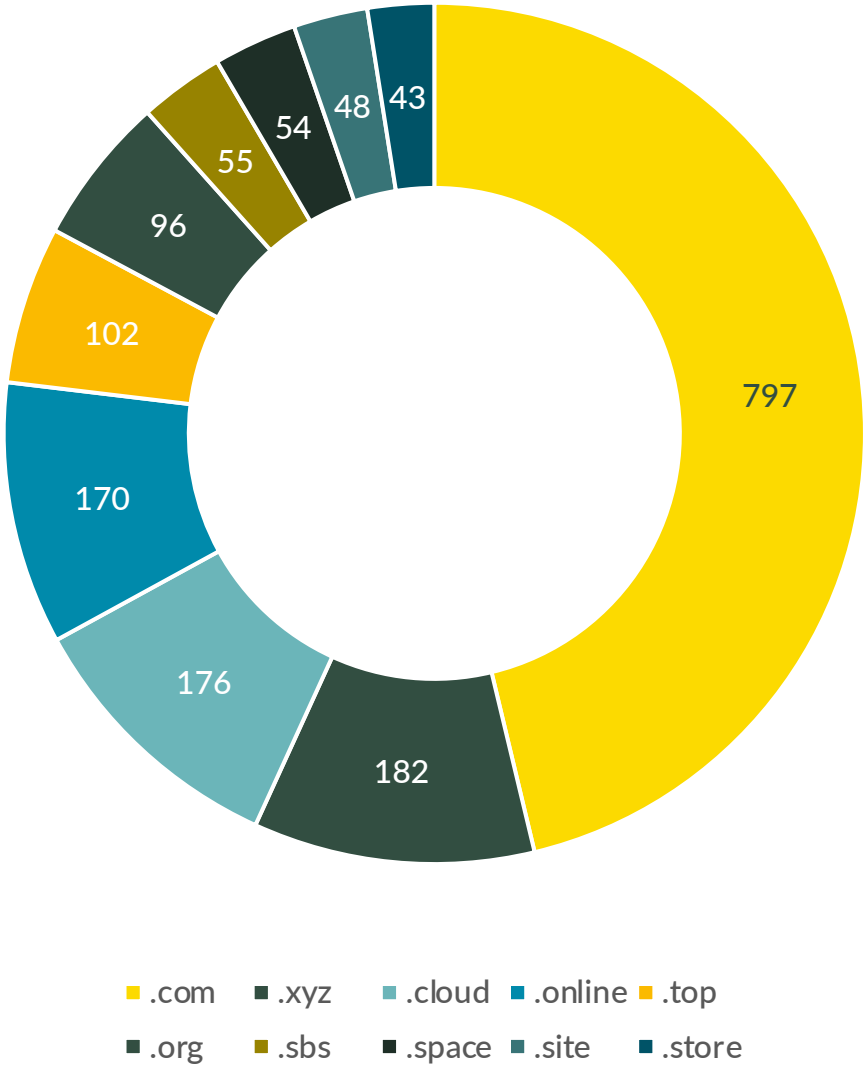
Domainextensions - intel

Registered phishing domains and their TLD's

Found based on
AitM fingerprinting.

Phishing domains are primarily registered in .com, but lesser-known domain extensions, such as .xyz and .sbs, are popular. This is likely because registration is easier or cheaper.

Adversaries also like to use recognizable words in domain names, such as office, onedrive, sharepoint, etc.

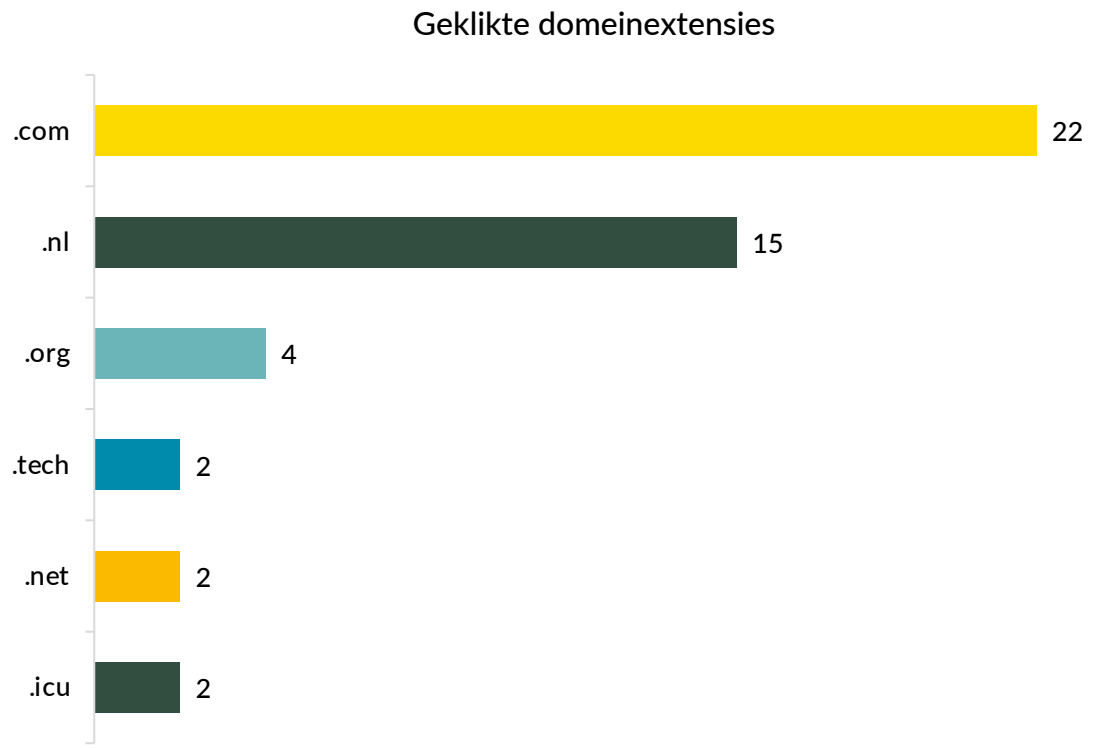


Domeinextensions – clicks

What is the extension of phishingdomains which Dutch victims fall for?

.com and .nl are most successful in misleading.

Although intelligence shows that attackers like to use risky TLDs (domain extensions), Dutch victims seem to be mainly misled by well-known extensions such as .com and .nl



Recommendation #1

To protect your organization from the consequences of AitM Phishing

Phishing-resistant MFA: FIDO2 hardwarekey or passkey

Force phishing resistant MFA for Admins as soon as possible. FIDO2 USB keys like Yubikeys and Passkeys are phishing-resistant. When users are forced to log in with this MFA method, they are no longer vulnerable to AitM.

Token binding may already work for some, but it still has limitations.

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

Recommendation #2

To protect your organization from the consequences of AitM Phishing

AitM Intervention in Company Branding

Display a clear warning to users when they visit a known AitM phishing site. This is possible through dynamic configuration in the Entra ID Company Branding settings.

Attic offers a free service to easily enable this and process alerts.

atticsecurity.com/free

Recommendation #3

To protect your organization from the consequences of AitM Phishing

Conditional Access & MDM from outside perimeter

Compliance-based authentication prevents the reuse of a token from an unknown device. It's less BYOD-friendly, but it's an effective tool against this type of abuse.

If this doesn't work for your entire organization, consider implementing it in some cases.

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

Recommendation #4

To protect your organization from the consequences of AitM Phishing

IOC-sharing & quick takedowns

By exchanging URLs and IP addresses of identified AitM sites, reuse detection can be accelerated.

Moreover, this can aid in the takedown of such sites, effectively preventing them from being live in the first place.

stats.didsomeoneclone.me

Recommendation #5

To protect your organization from the consequences of AitM Phishing

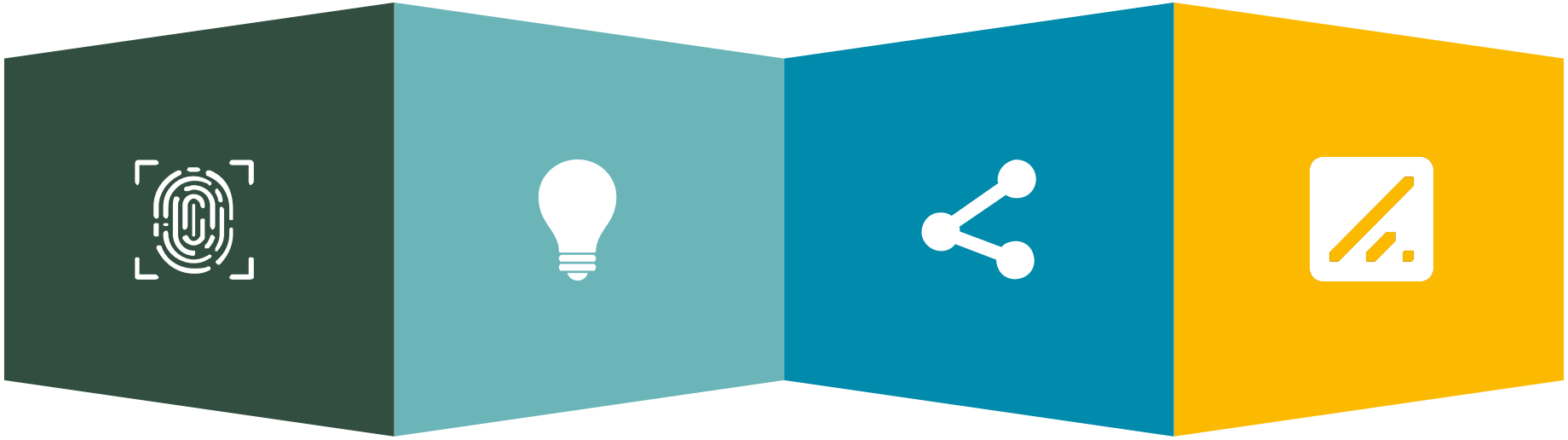
Stimulate extra awareness around lunch time

Recognize that click behavior primarily occurs around lunchtime. Your user awareness program can consider ways to nudge employees about these risks specifically during these times.

atticsecurity.com/awareways

Summary & Call-to-Action

Wrap up



Identity = Perimeter

The identity is the new perimeter. Only 1 boundary to get into your data. Prioritize implementation of layered defense.

User Awareness

Invest in user awareness for the growing threat of AitM, certainly during lunch time on Tuesdays when guards are down, so it seems.

Reuse

Register and share ioc's from your detections with peers, to improve resilience for us all. Consume in solutions that work outside corporate perimeter.

Wanna know more?

Follow Attic Security on socials. Register for our newsletter or simply get a free account in MyAttic.app and enable our free services.

Our Service: Attic #BOUNCER

Block hackers from entering your organization through the front door.

CYBERSECURITY™
MADE IN EUROPE

#01 AitM Intervention Screen

Protect the Microsoft365 login portal with smart CSS code that will detect it is being proxied and changes into a red warning sign.

#02 SignIn Logs Monitoring

Match patterns from your SignIn Logs with the latest threat intelligence and identify users visiting AitM pages.

#03 AitM Blocker Browser Plugin

Deploy extension to Chromium browsers (Chrome, Edge) to block access to known AitM sites based on the latest threat intelligence from proactive AitM scanners of Attic Lab.

ATTIC

€ 30,- per month with 20 users included. € 1,- per extra user.
On-board in 5 minutes. Start here: atticsecurity.com/bouncer

Contact Info.

To protect our digitalizing society, we need agile and skilled defense.

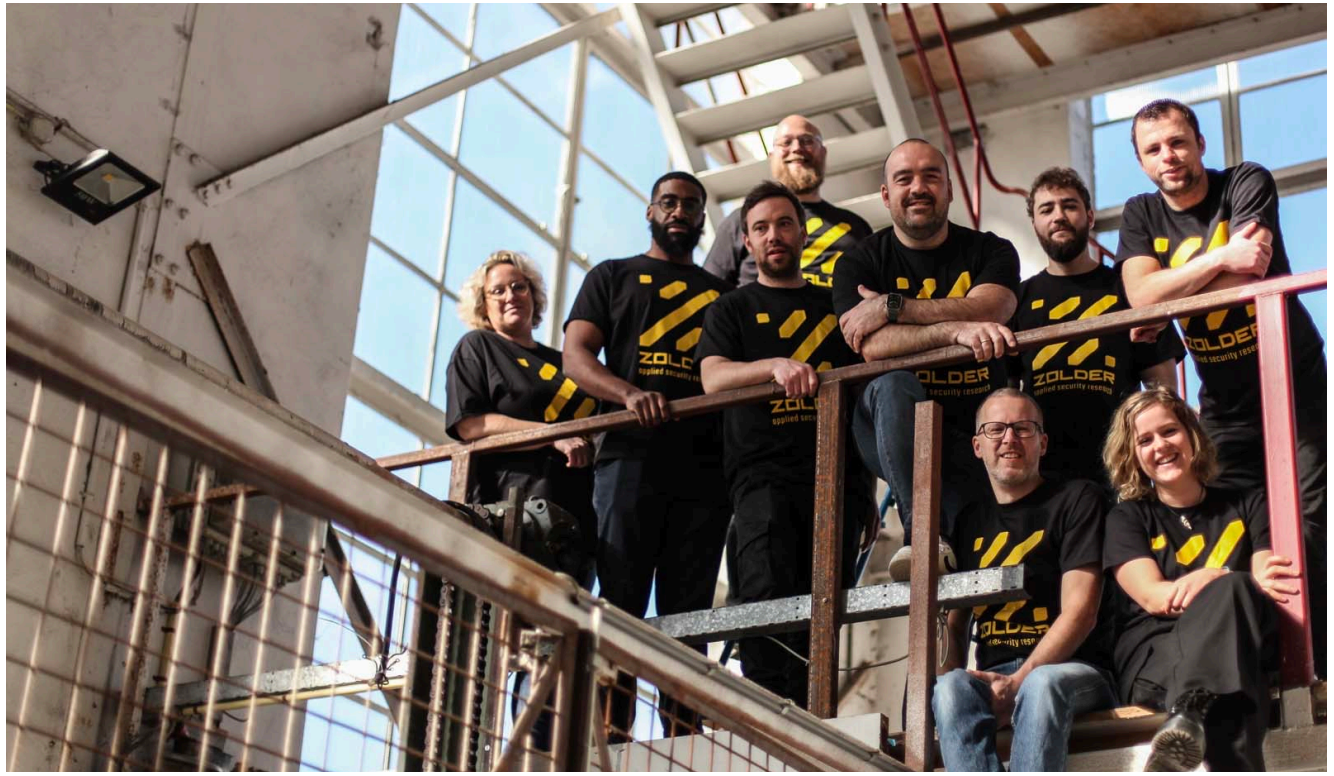
Molenstraat 36
4761 CL Zevenbergen

+31 168 794 020

atticsecurity.com

linkedin.com/company/atticsecurity

x.com/attic_security



ATTIC

2024-2025 AitM Threat Report

Based on detection data coming from the Attic Lab platform in didsomeoneclone.me and Attic Bouncer for M365