



TOP-5 LESSONS LEARNED FROM DEFENDING M365

Erik Remmelzwaal | CEO Zolder BV | erik@zolder.io



AtticSecurity.com
by ZOLDER

25-9-2024

ERIK REMMELZWAAL

CEO & CO-FOUNDER ZOLDER



erik@zolder.io



[@erikremmelzwaal](https://twitter.com/erikremmelzwaal)

Voormalig CEO DearBytes, CTO KPN Security



AtticSecurity.com
by ZOLDER

25-9-2024

SHOULD DEFENDING M365 BE A PRIORITY?

What do you think? Why?



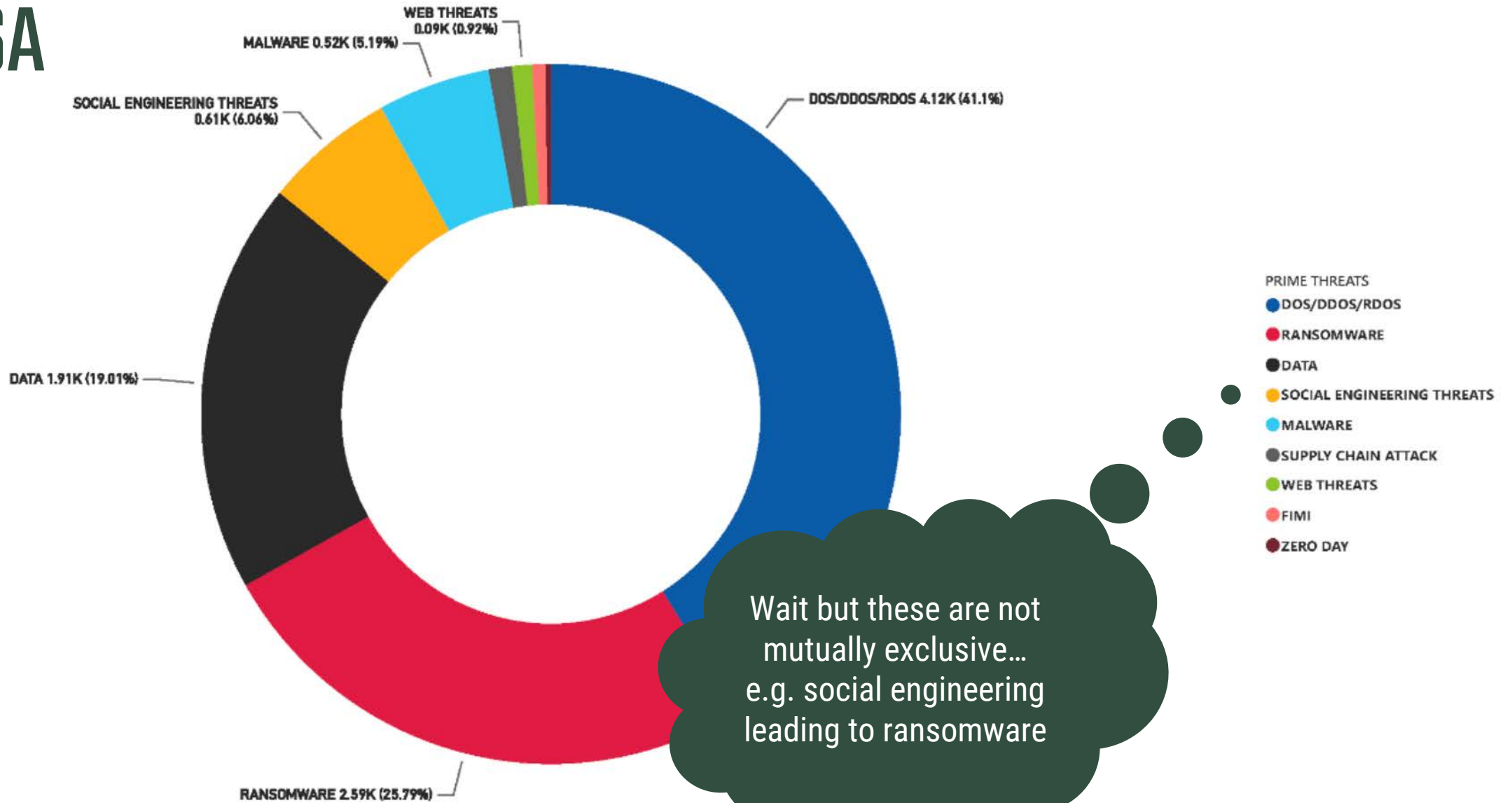
ENISA



AtticSecurity.com
by ZOLDER

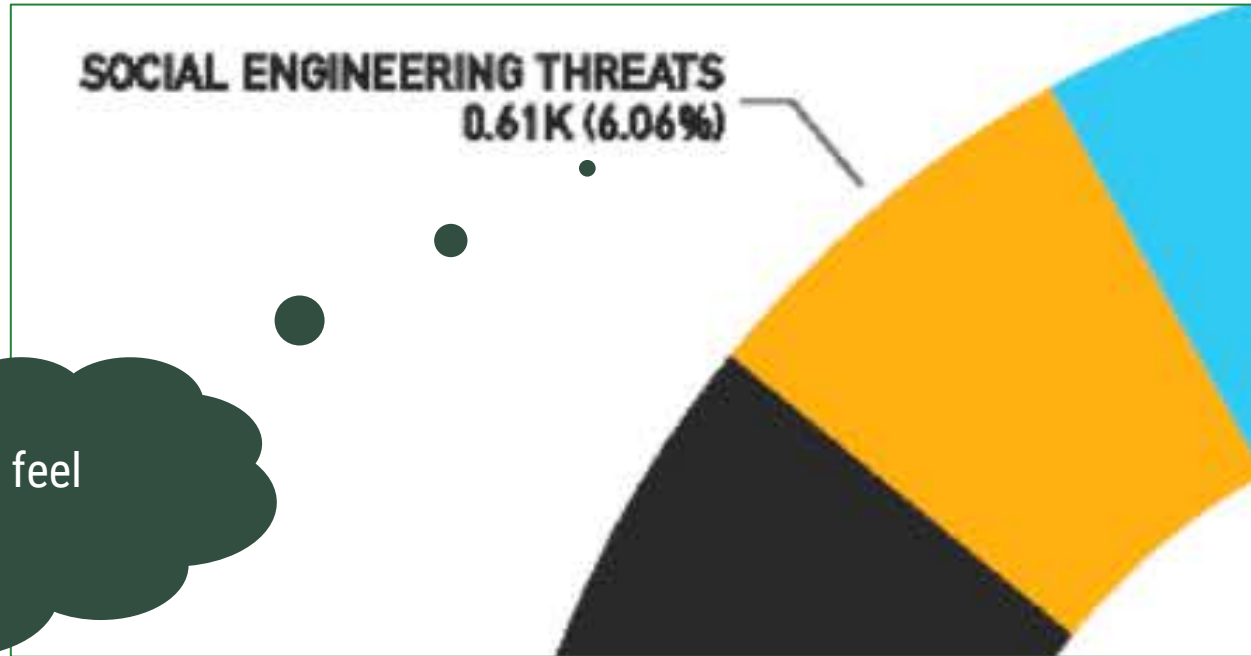
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024/>

25-9-2024



Wait but these are not mutually exclusive... e.g. social engineering leading to ransomware

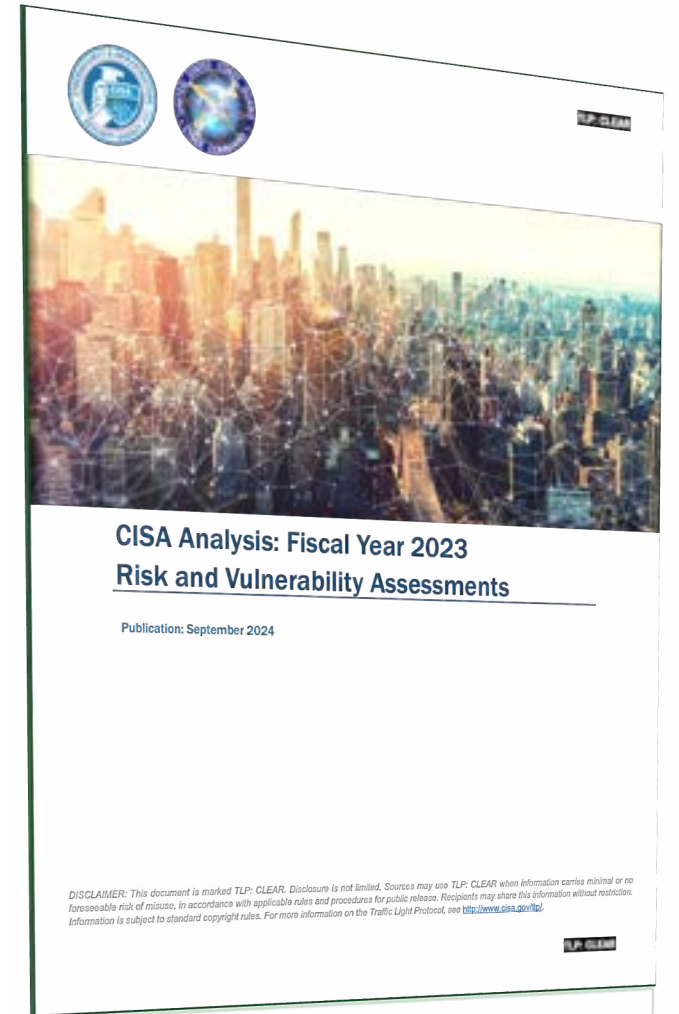
ENISA



There has also been a rise in compromises of cloud-based identities secured with multi-factor authentication (MFA). Particularly concerning is the growing use of web proxy or adversary-in-the-middle (AiTM) phishing pages, which can bypass many MFA implementations by stealing sensitive session tokens. Attackers commonly use credential-harvesting forms or phishing pages to collect login details from their victims. These phishing sites, designed to mimic popular login portals, pass the user's credentials and MFA codes to the attacker. AiTM phishing pages go beyond standard credential-harvesting techniques by using infrastructure designed to defeat typical MFA methods. Unlike traditional phishing forms, AiTM pages function as a reverse web



RISKY BUSINESS 18-SEPT-24 – CISA AUDIT



41% THROUGH STOLEN CREDS



INITIAL ACCESS

WHAT

Initial Access [TA0001] is the phase of malicious activity where threat actors attempt to obtain unauthorized access to a victim's internal network. Gaining initial access to an organization's network is one of the first active steps in a successful attack. Threat actors could use techniques—such as targeted spear phishing, valid accounts and credentials, or exploiting critical vulnerabilities and weaknesses on network edge devices—to gain an initial foothold within a network. If threat actors establish initial access, they could execute other techniques—such as privilege escalation—to ultimately steal information, disrupt operations, or preposition for future actions on objectives. Preventing initial access should be a main goal in protecting network assets and data, both internally and externally.

HOW

Threat actors use a variety of attack paths—such as, gaining access to valid accounts, targeted spear phishing, leveraging insecure ports or protocols, or exploiting public-facing applications—to compromise a victim's network. RVA analyses revealed that **Valid Accounts [T1078]** were the most common successful attack technique, responsible for **41% of successful attempts**. A common technique under this tactic is cracking password hashes, which was successful in 89% of USCG assessments to access Domain Administrator accounts. Valid accounts can be accessed internal or external to the network through default or stolen administrator accounts, or former employee accounts that have not been removed from the active directory. Additionally, initial access brokers that sell exploits and valid credentials to nation-state and criminal threat actors are seen more frequently as the profits are rising for criminal activity.^{2,3} Threat actors can compromise a valid administrator account if organizations do not change default passwords, or through brute force if a weak password is in place. In many cases, this attack technique is possible because the valid account allowed unauthorized users to install or execute insecure software (such as unpatched or out-of-date software) on a system or network. Figure 2 demonstrates a valid account execution.

TLP: CLEAR

CISA RVA 2024:

<https://www.cisa.gov/sites/default/files/2024-09/FY23%20RVA%20Analysis%20508.pdf>



AtticSecurity.com
by ZOLDER

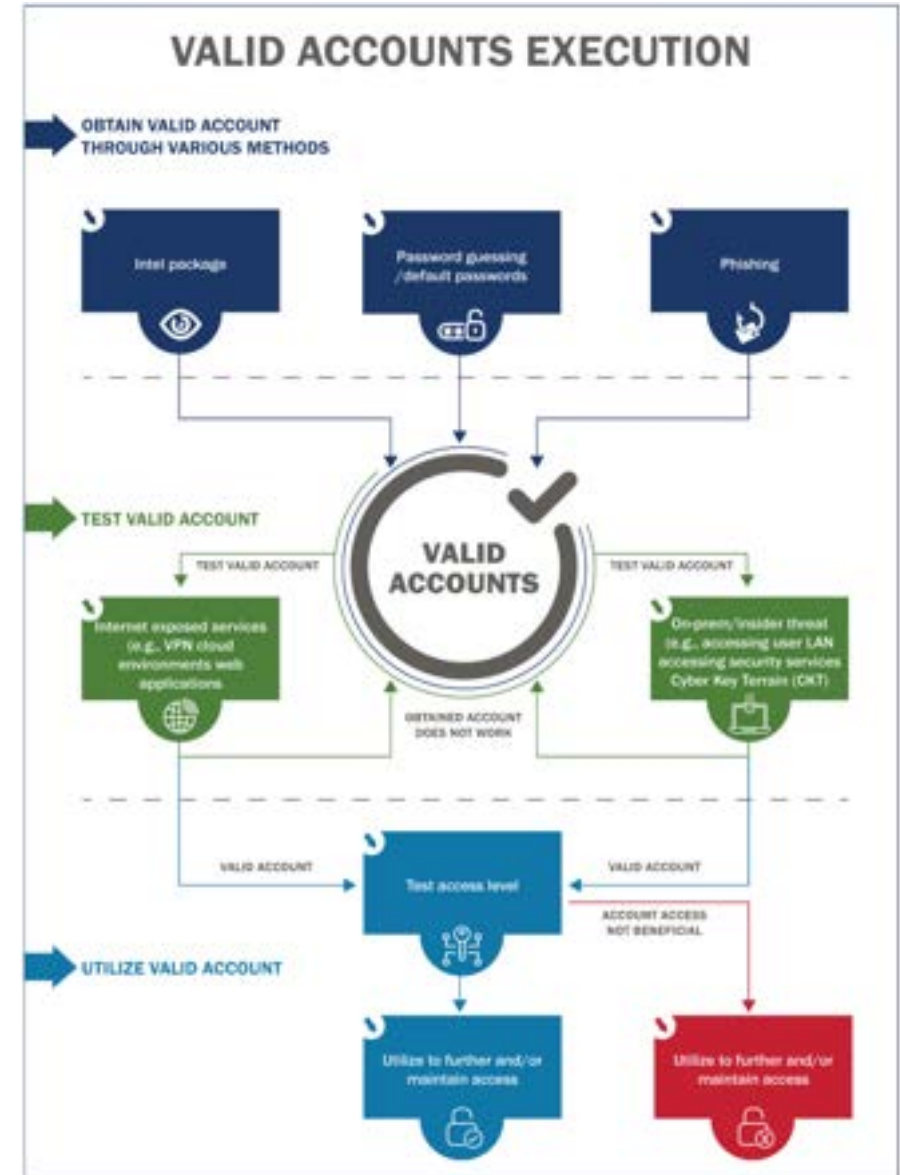


Figure 2: Valid Account Execution

25-9-2024

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Initial Access

Threat actors attempt to obtain unauthorized initial access into a victim's network. Actors use techniques, such as Valid Accounts T1078 or Spear Phishing Link T1566.002s, to gain this access. After obtaining initial access, actors can then execute other techniques to move about the network.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 1.E Mitigating Known Vulnerabilities CPG 2.A Changing Default Passwords

CPG 2.H Phishing-Resistant Multifactor Authentication CPG 2.M Email Security

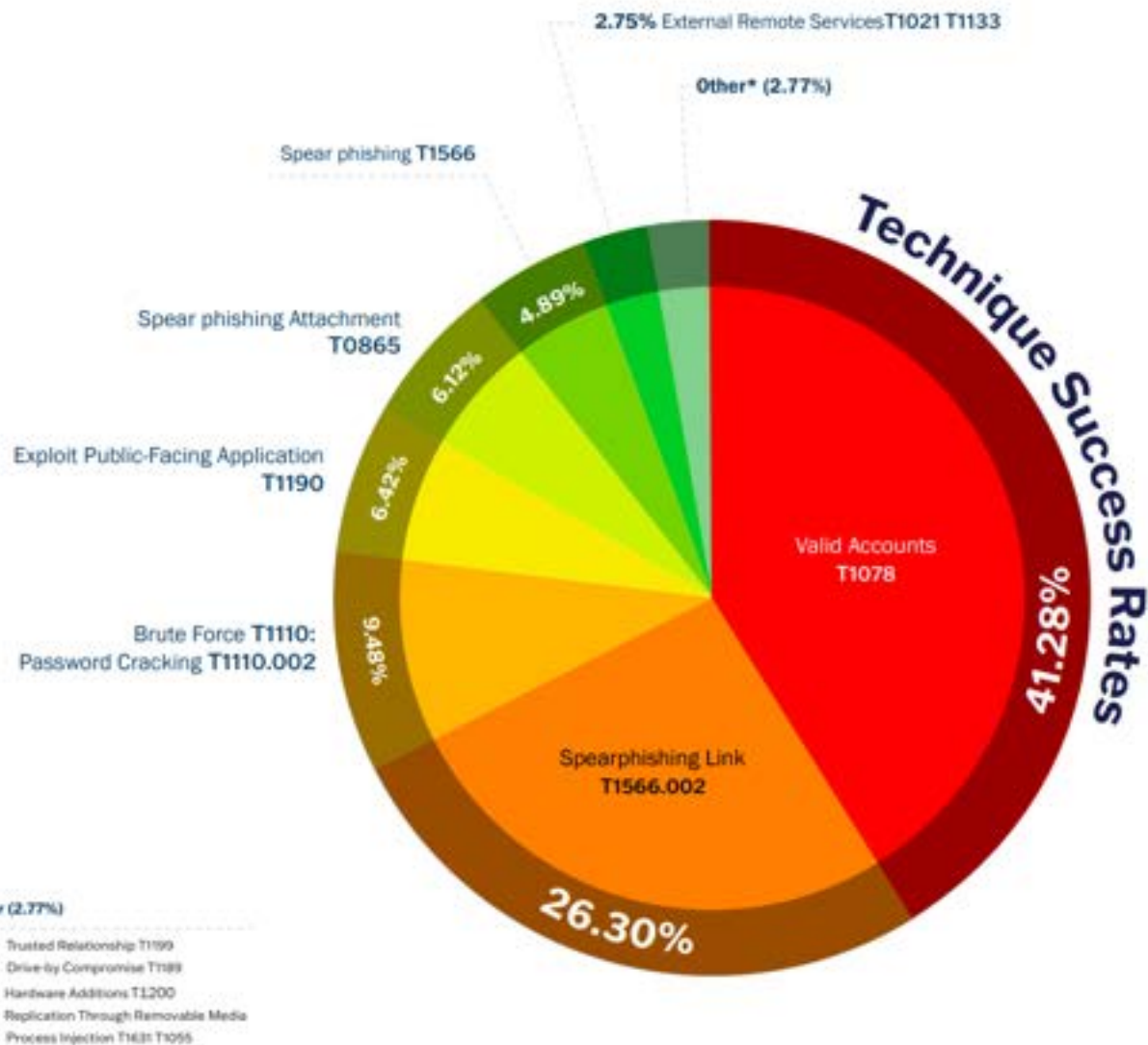
CPG 2.N Disable Macros by Default

CPG 2.W No Exploitable Services on the Internet



ATT&CK™

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks for information about other techniques. For more information about OSA assessment services, please visit [cisa.gov](https://www.cisa.gov).



5 LESSONS LEARNED



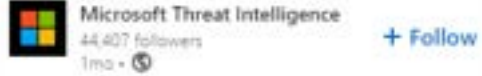
LESSON #1

AITM & TOKEN REPLAY

MFA-resilient Phishing Techniques



#1: AITM & TOKEN REPLAY



Microsoft has detected a 111% year-over-year increase in token replay attacks, and incidents are continuing to grow. In token replay attacks, attackers steal tokens – authentication artifacts that grant users access to resources – commonly via malware or adversary-in-the-middle (AiTM) attacks, and then replay the token from somewhere else to impersonate users and access their data.

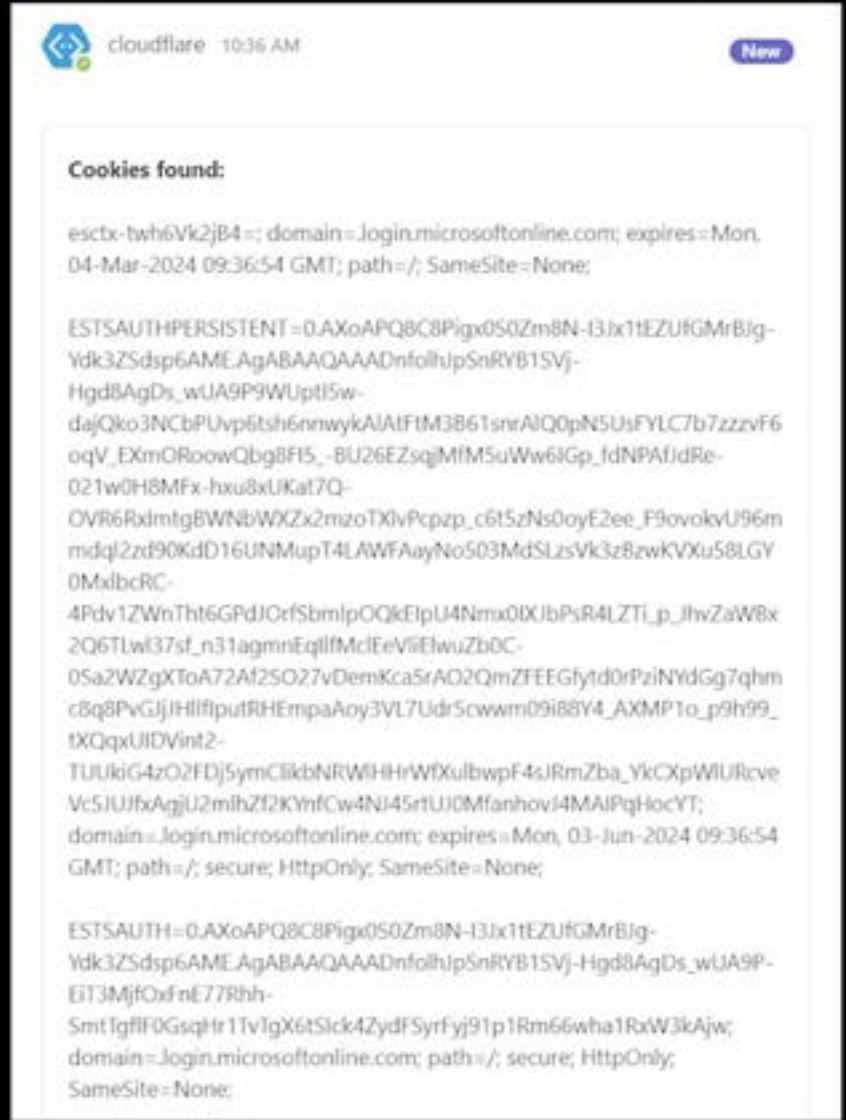
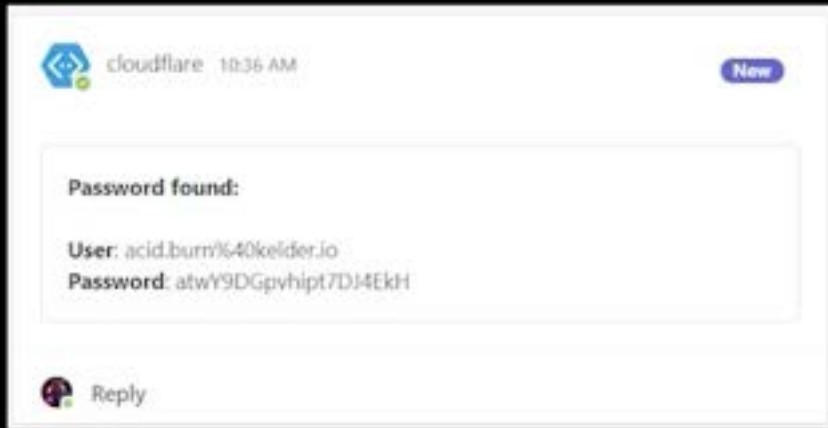
While token theft constitutes fewer than 5% of all identity compromises, Microsoft expects threat actors to continue using this technique, especially since it allows attackers to circumvent protection measures like multi-factor authentication (MFA).

In this blog post, Microsoft provides details on the mechanics of tokens, the token theft attack chain, and how Microsoft protects customers against token theft through token binding. We also provide recommendations for a systematic defense-in-depth approach to counter token theft attacks: <https://msft.it/6042ISgTq>

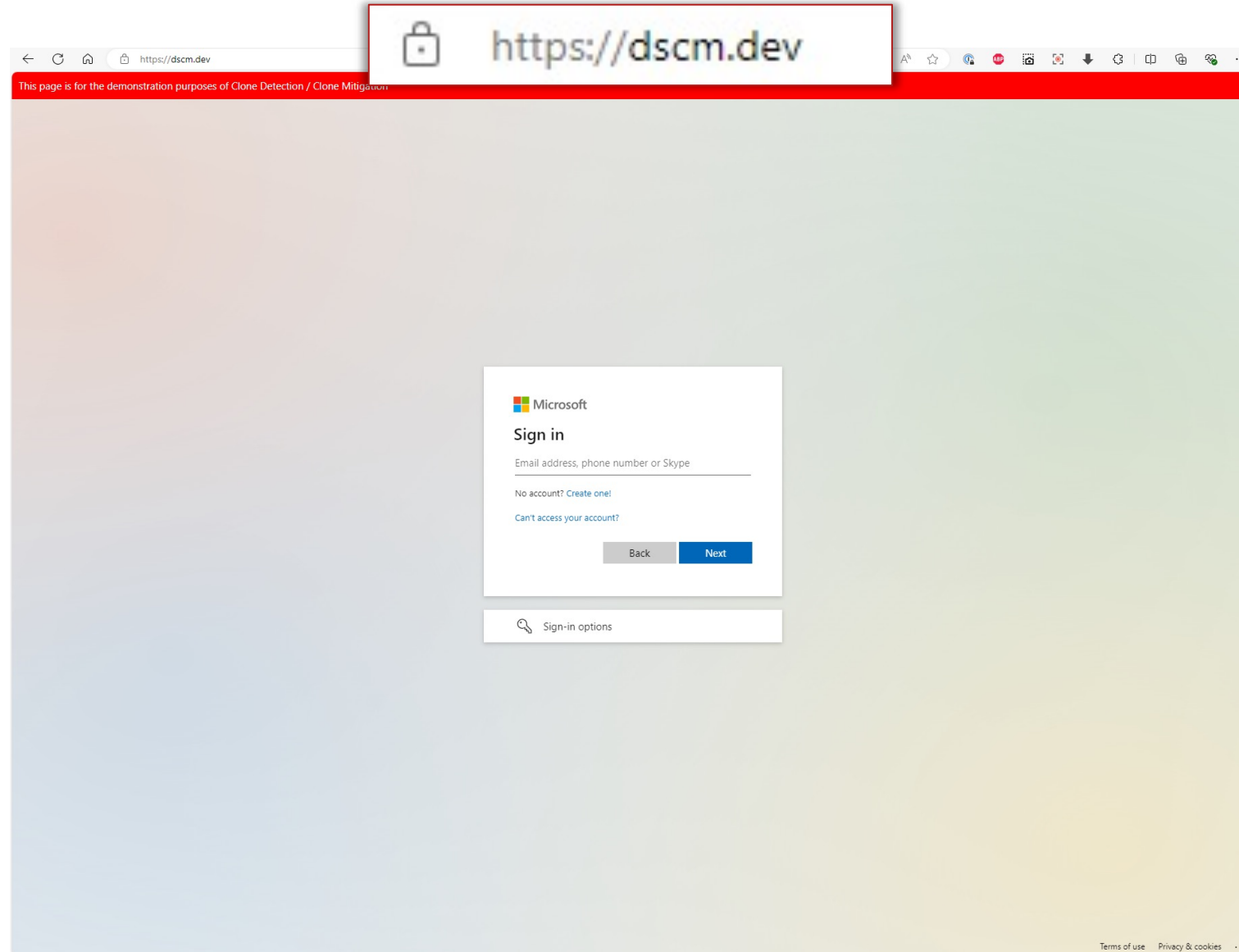


User





EVILGINX POC



CAAS > EVILPROXY

07/02/2022

evilproxy
Premium

Registration: 07/01/2022
Messages: 23
Reactions: 7

Reverse proxy
Our phishing pages are 100% identical

You get LOGIN, PASSWORD, COOKIES and more info about user

We can help you increase your resistance to phishing attacks. Phishing as a Service (PhaaS) is a security awareness program for everyone in an organization. Our phishing simulations are supported by a proprietary software platform. In particular, our backend application offers a complete set of features needed to run phishing campaigns:
Get a demo completely free for 1 day!
New users without an account in the system - minimum deposit \$250

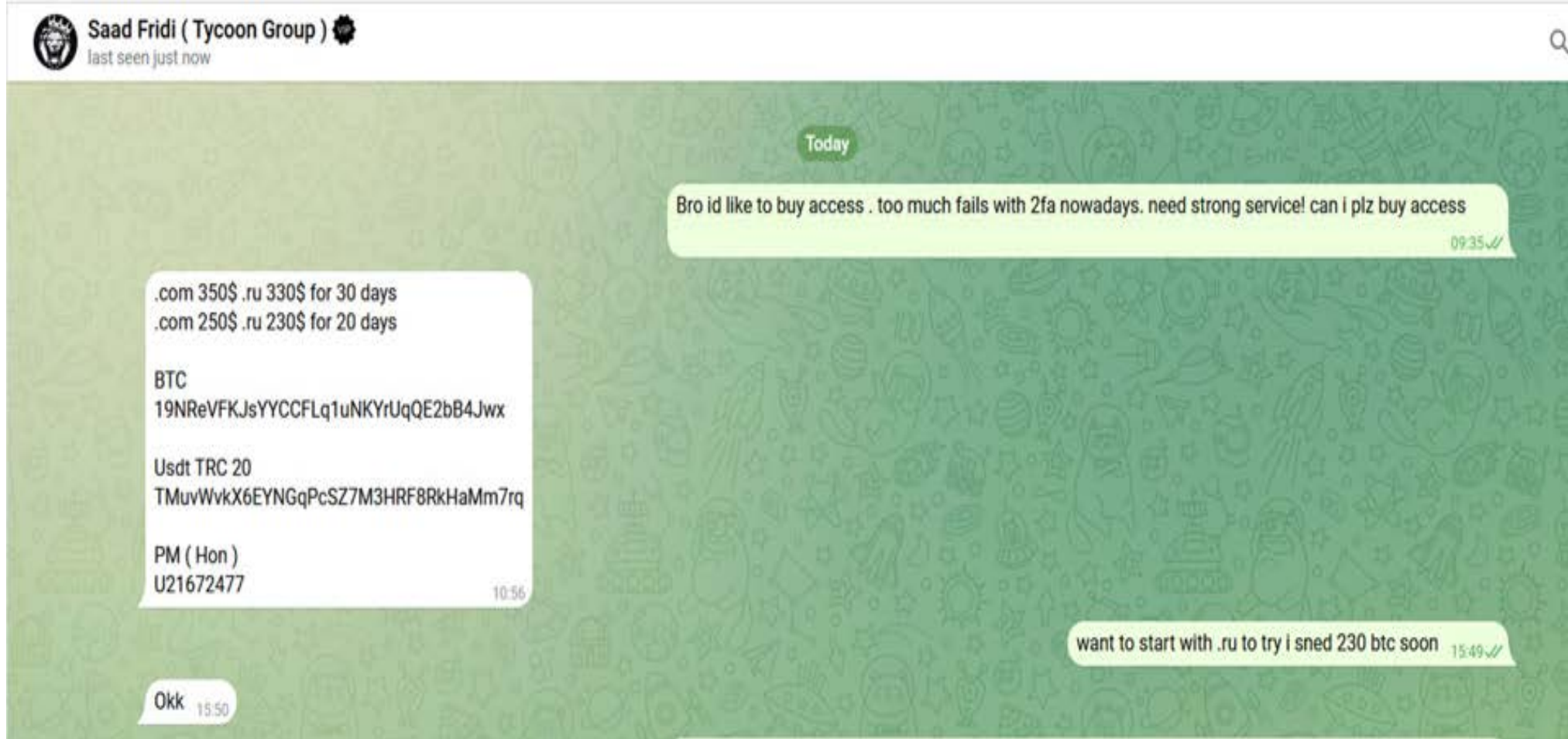
We can help you improve your resilience against phishing attacks. Phishing as a Service (PhaaS) is a security awareness program for all employees of the organization. Our phishing simulations are supported by an in-house developed software platform. In particular, our backend application offers the full set of functionalities required to conduct phishing campaigns:
Get a demo completely free 1 day!
New users without an account in the system - minimum deposit 250\$

+ Services:

- microsoft 10/20/31 days = 150\$/250\$/400\$ (Hotmail, CORP, Remote SSO, ADFS) (auto cookies refresh with internal tool)
- google 10/20/31 days = 250\$/400\$/600\$
- icloud.com 10/20/31 days = 150\$/250\$/400\$ (auto token/cookies refresh up to 2 days with internal tool)
- dropbox.com 10/20/31 days = 150\$/250\$/400\$ (also sign in with google)
- github.com 10/20/31 days = 150 \$ /250 \$ /400\$
- facebook.com 10 /20/31 days = 150 \$ /250 \$ /400\$
- yahoo.com 10/20/31 days = 150 \$ /250 \$ /400\$
- aol.com 10/20/31 days = 150 \$ /250 \$ / 400\$
- twitter 10/20/31 days = 150 \$ /250 \$ /400\$
- wordpress.com 10/20/31 days = 150 \$ /250 \$ /400\$
- pypi.org 10/20/30 days = 150 \$ /250 \$ /400\$
- npmjs.com 10/20/30 days = 150 \$ /250 \$ /400\$
- rubygems.org 10/20/30 days = 150 \$ /250 \$ /400\$



CAAS > TYCOON



MEASURES VS AITM?

- **Phishing Resistant MFA**
 - Passkeys
 - Windows Hello
 - FIDO2 key
 - Certificates
- **Compliance-based Conditional Access**
 - Non-BYOD friendly
- **Custom CSS**
- **SafeLinks**



LESSON #2

PRIVILEGE MANAGEMENT

It is not all about users...



#2: PRIVILEGE MANAGEMENT++

- Partner Tier1 Support
- Partner Tier2 Support
- Directory Synchronization Accounts
- On Premises Directory Sync Account

Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.

This application is not published by Microsoft.

This app would like to:

- ✓ Have full access to your calendars
- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to

Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

App Consents

The screenshot shows a Medium article titled "The Most Dangerous Entra Role You've (Probably) Never Heard Of" by Andy Robbins. The article discusses a hidden role in Azure Entra ID.

Hidden Admin Roles

Global Administrator | Assignments

All roles

Diagnose and solve problems

- Manage
- Assignments
- Description
- Activity
- Troubleshooting + Support

Search

Search by name

Type

All

Name	UserName	Type
<input type="checkbox"/> Samsung Email	8acd33ea-7197-4a96-bc33-d7cc7101262f	ServicePrincipal
<input type="checkbox"/> AdminAgents		Group
<input type="checkbox"/> Emergency Admin	emergency-admin@	User
<input type="checkbox"/> Erik Remmelzwaal	erik@	User
<input type="checkbox"/> Partner Technician		Group

Service Principals

... has a built-in role called "Partner Tier2 Support" that enables access to Global Admin, but this role is hidden from view in the Azure portal GUI.

... adversary may target the "Partner Tier2 Support" role to maintain persistent, privileged persistence in an Entra ID tenant

... the Azure portal GUI obscures this role, it can be challenging for Azure admins and security professionals to audit assignments for this role

<input type="checkbox"/> Samsung Email	8acd33ea-7197-4a96-bc33-d7cc7101262f	ServicePrincipal
--	--------------------------------------	------------------

LESSON #3

PUBLIC TEAMS & SITES


Modern day open SMB shares



#3: PUBLIC TEAMS & SHAREPOINT SITES

Get a team site connected to Microsoft 365 Groups

Use this design to collaborate with your team. Share documents, track events in a shared calendar, and manage project tasks.



Site name
Example
The site name is available.

Group email address
Example
The group alias is available.

Site address
Example
https://kelderio.sharepoint.com/sites/Example
The site address is available.

Site description
Tell people the purpose of this site.

Privacy settings
Private - only members can access this site
Public - anyone in the organization can access this site
Private - only members can access this site

Select the default site language for your site. You can't change this later.

Next Cancel

ZOLDER applied security research

← Alle blogs

Public SharePoint sites – the new open shares

16 september 2021 - Blog - Wesley Neelen

During one of our engagements we were investigating a Microsoft 365 environment. My colleague [Bibi](#) discovered that many SharePoint sites were publicly available within the organization. We were surprised by the amount sites that were wide open this way. A lot of sensitive information was located on those sites, for example PII-information and passwords for critical systems.

<https://zolder.io/blog/public-sharepoint-sites-the-new-open-shares/>

CSO

Home - Security - Fortinet confirms breach that likely leaked 440GB of customer data

By Shweta Sharma
Senior Writer

Fortinet confirms breach that likely leaked 440GB of customer data

News
Sep 13, 2024 - 3 mins

Only search Save article

in X f e m p

The cybersecurity company said a threat actor had unauthorized access to files on a third-party cloud-shared drive.



Credit: JIVE/Photo / Shutterstock

Fortinet has confirmed a data breach that has allegedly compromised 440GB of Azure SharePoint files containing Fortinet customer data.

<https://www.csoonline.com/article/3520517/fortinet-confirms-a-breach-that-likely-leaked-440-gb-of-customer-data.html>

LESSON #4

'FREE' SIEM

Make use of what you pay for



#4: FREE LOGGING & MONITORING



Free data sources

The following data sources are free with Microsoft Sentinel:

- Azure Activity Logs
- Microsoft Sentinel Health
- Office 365 Audit Logs, including all SharePoint activity, Exchange admin activity, and Teams
- Security alerts, including alerts from the following sources:
 - Microsoft Defender XDR
 - Microsoft Defender for Cloud
 - Microsoft Defender for Office 365
 - Microsoft Defender for Identity
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Endpoint
- Alerts from the following sources:
 - Microsoft Defender for Cloud
 - Microsoft Defender for Cloud Apps

The screenshot shows the Microsoft Sentinel 'Data connectors' page. The page title is 'Microsoft Sentinel | Data connectors' and it shows 124 connectors and 11 connected. A search filter for 'Defender' is applied, showing a list of Microsoft Defender connectors. The 'Microsoft 365 Defender (Preview)' connector is highlighted. A detailed view of this connector is shown on the right, including its status (Connected), provider (Microsoft), and last log received (11/2/2022, 10:47:17 PM). The description states that Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite. The suite includes: Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, Microsoft Defender for Cloud Apps, Microsoft Defender Alert Evidence, and Microsoft Defender Vulnerability Management. Related content includes 2 workbooks, 4 queries, and 72 analytics rule templates. An 'Open connector page' button is visible at the bottom.

<https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=simplified%2Ccommitment-tiers#free-data-sources>

LESSON #5

PREMIUM ANTI-PHISHING

Make use of what you pay for



USER IMPERSONATION

Office 365 Security & Compliance

Edit impersonation policy

User Impersonation

Editing Add users to protect

Add users to protect

Add domains to protect

Actions

Mailbox intelligence

Add trusted senders and domains

Add up to 60 internal and external users you want to protect from being impersonated by attackers. We recommend adding users in key roles. Internally, these might be your CEO, CFO, and other senior leaders. Externally, these could include council members or your board of directors.

Get tips for adding users to protect

Off

Save Cancel

Protect targeted users and domains

GCITS



PHISHING MAILTIPS

Proposal Review

Label: Tenant retention policy (30 days) Expires: Fri 2021-03-18 15:39

Megan Bowen
Wed 2020-09-02 15:39
To: Alex Wilber


You don't often get email from Megan.Bowen@contoso.com. [Learn why this is important](#) [Feedback](#)

Message

Reply | Forward

SAFELINKS

Microsoft Outlook




We've detected an unsafe link.

Visiting this website might not be safe. As a benefit of your Microsoft Office 365 subscription, Microsoft has blocked <http://www.obvious-phishing-att...>. This website might harm your computer or cause your personal information to be stolen. We recommend that you do not continue.

[Return to Outlook](#)

Continue anyway (not recommended).

 This website is classified as malicious.

Opening this website might not be safe.

www.unsafe_url/login.php

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

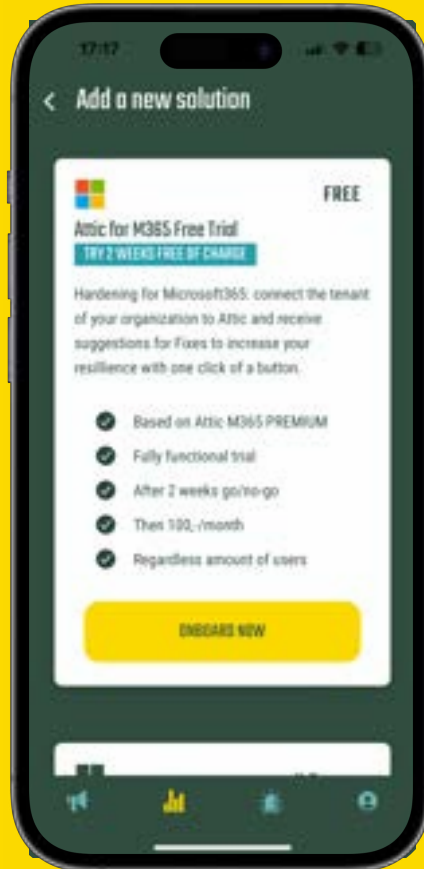
Powered by Office 365 Advanced Threat Protection



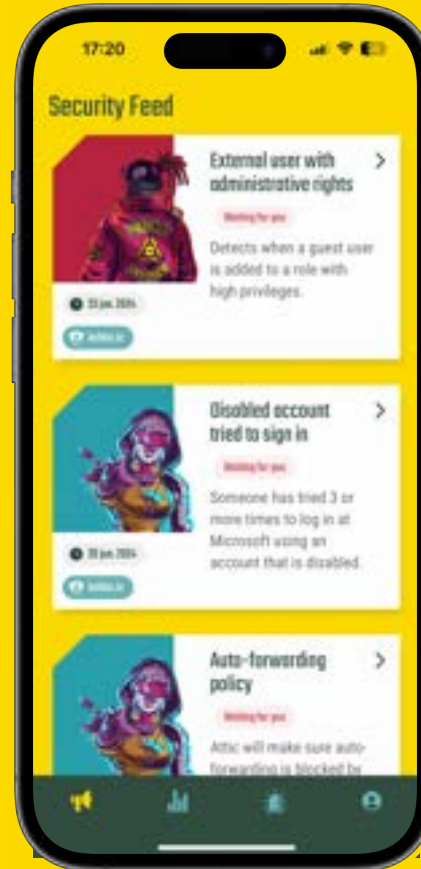
ATTIC SECURITY

Automated, scalable cybersecurity operations for SMB. We also have AI.

▶ ONBOARD



🚨 ALARM



⚙️ FIX

