ISACA
Netherlands Chapter

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

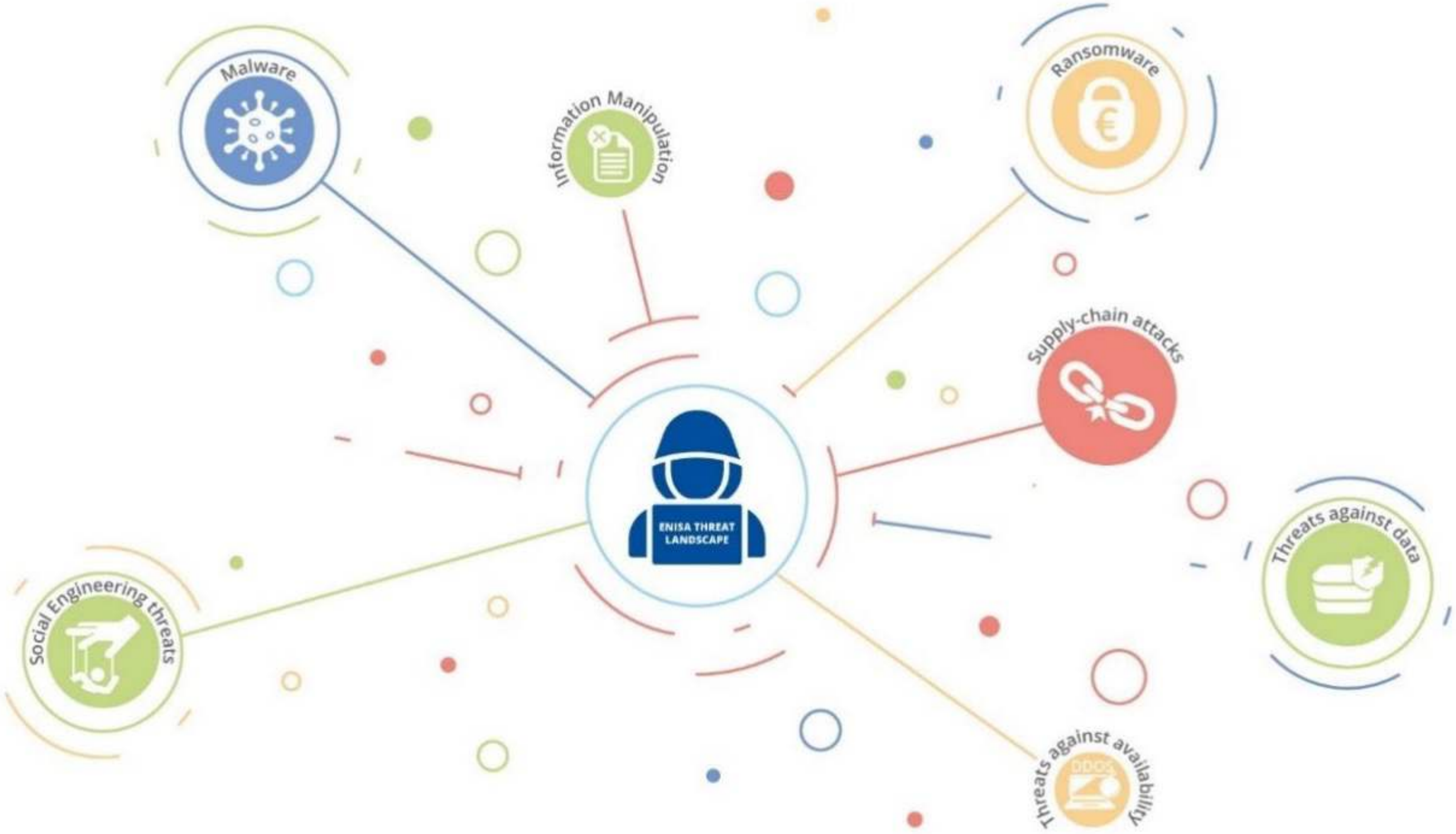
@erikremmelzwaal

Voormalig CEO DearBytes, CTO KPN Security

SHOULD DEFENDING M365 BE A PRIORITY?

What do you think? Why?

ENISA



enisa 20 years!

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2024

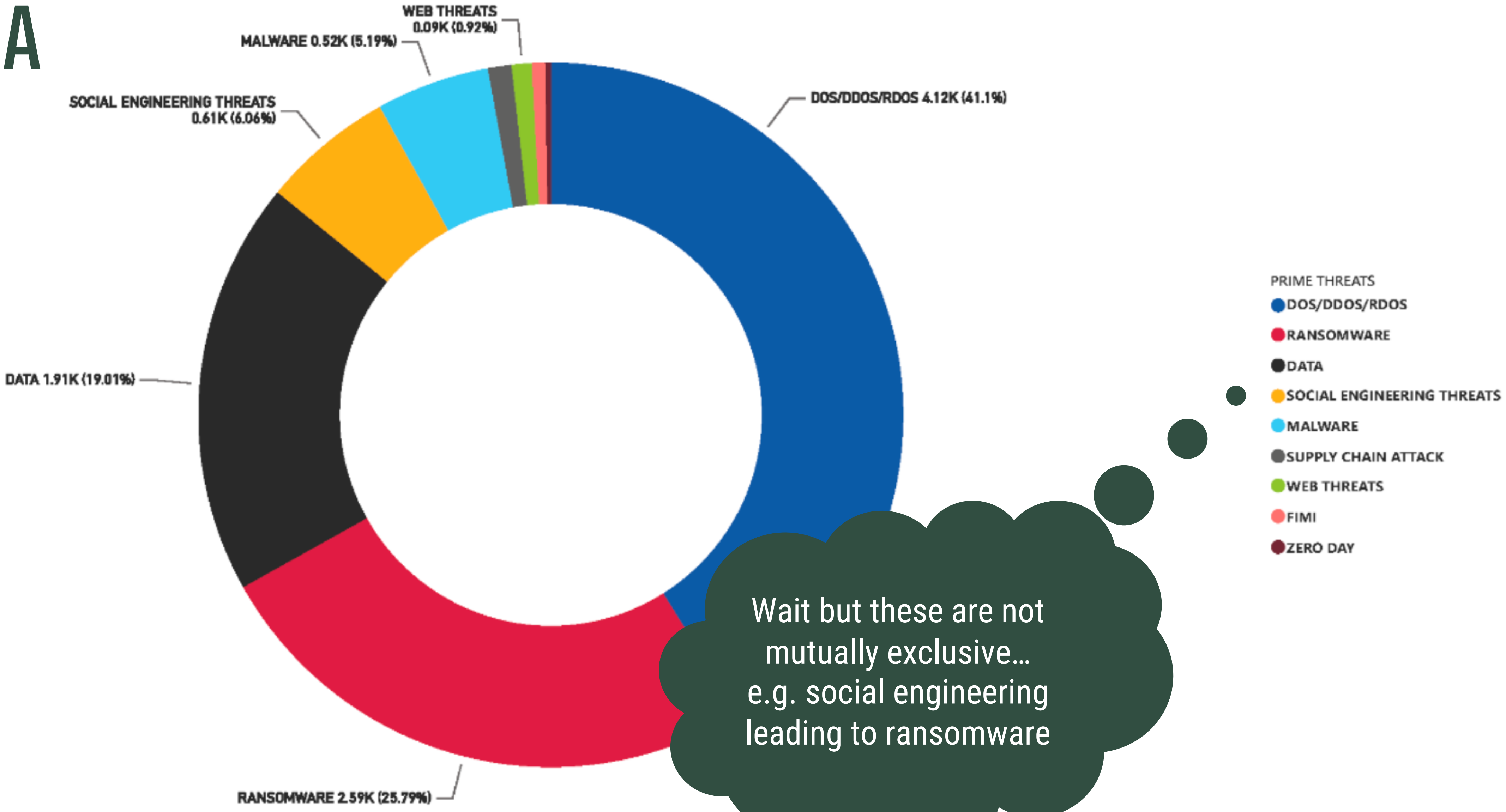
July 2023 to June 2024

SEPTEMBER 2024

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

25-9-2024

ENISA



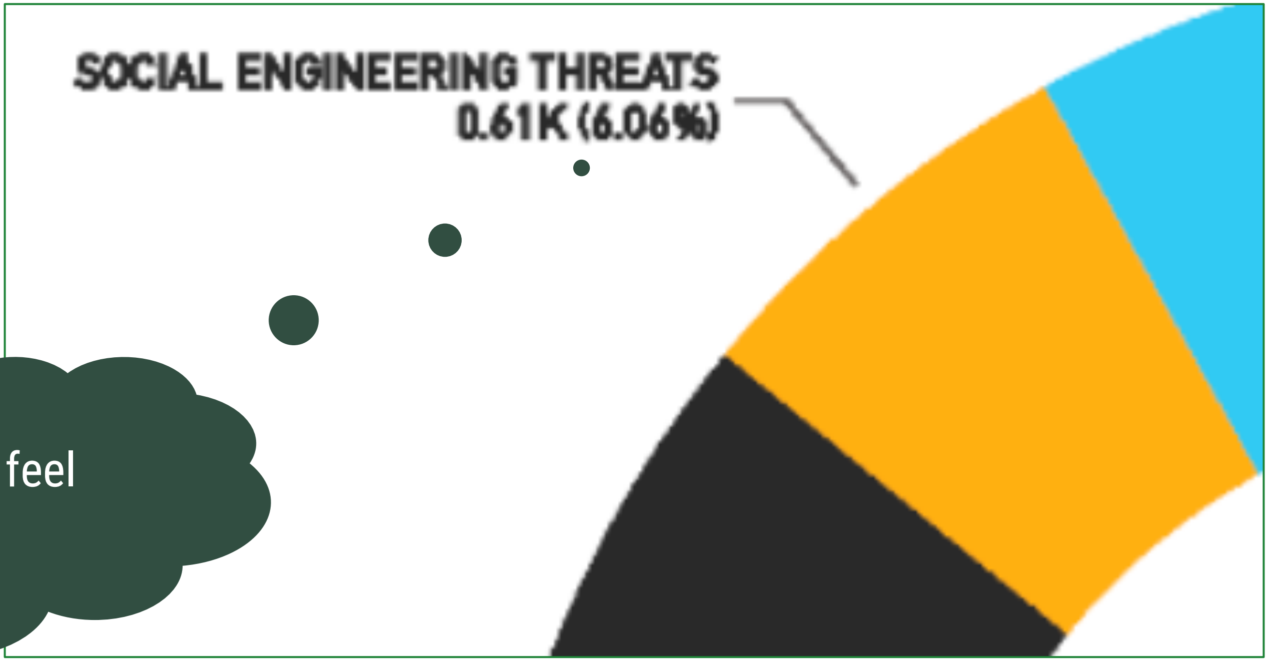
Wait but these are not mutually exclusive…
e.g. social engineering
leading to ransomware

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

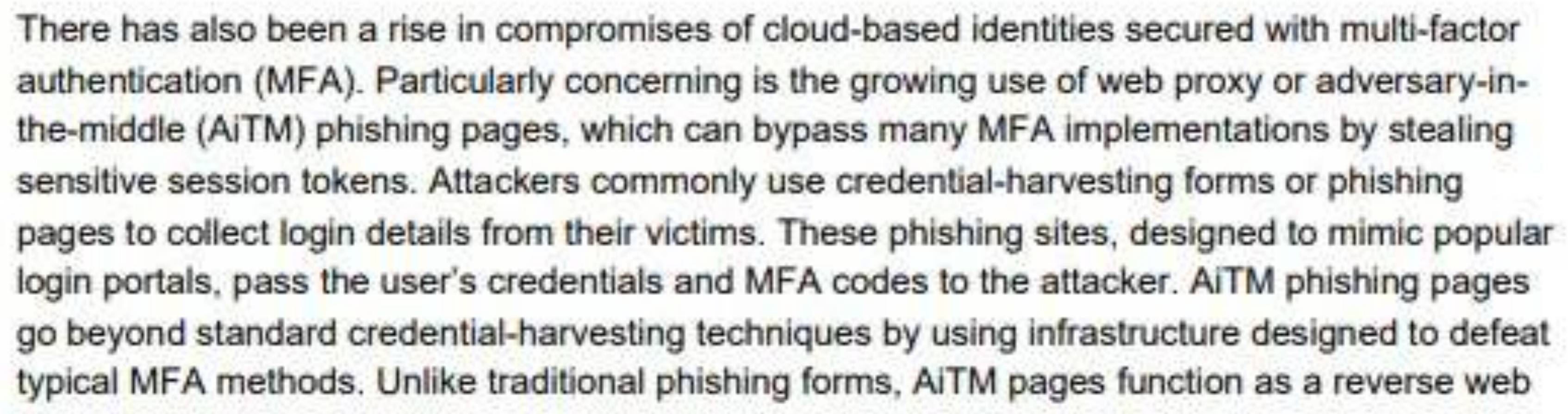
AtticSecurity.com
by ZOLDER

25-9-2024

ENISA



This doesn't feel right…

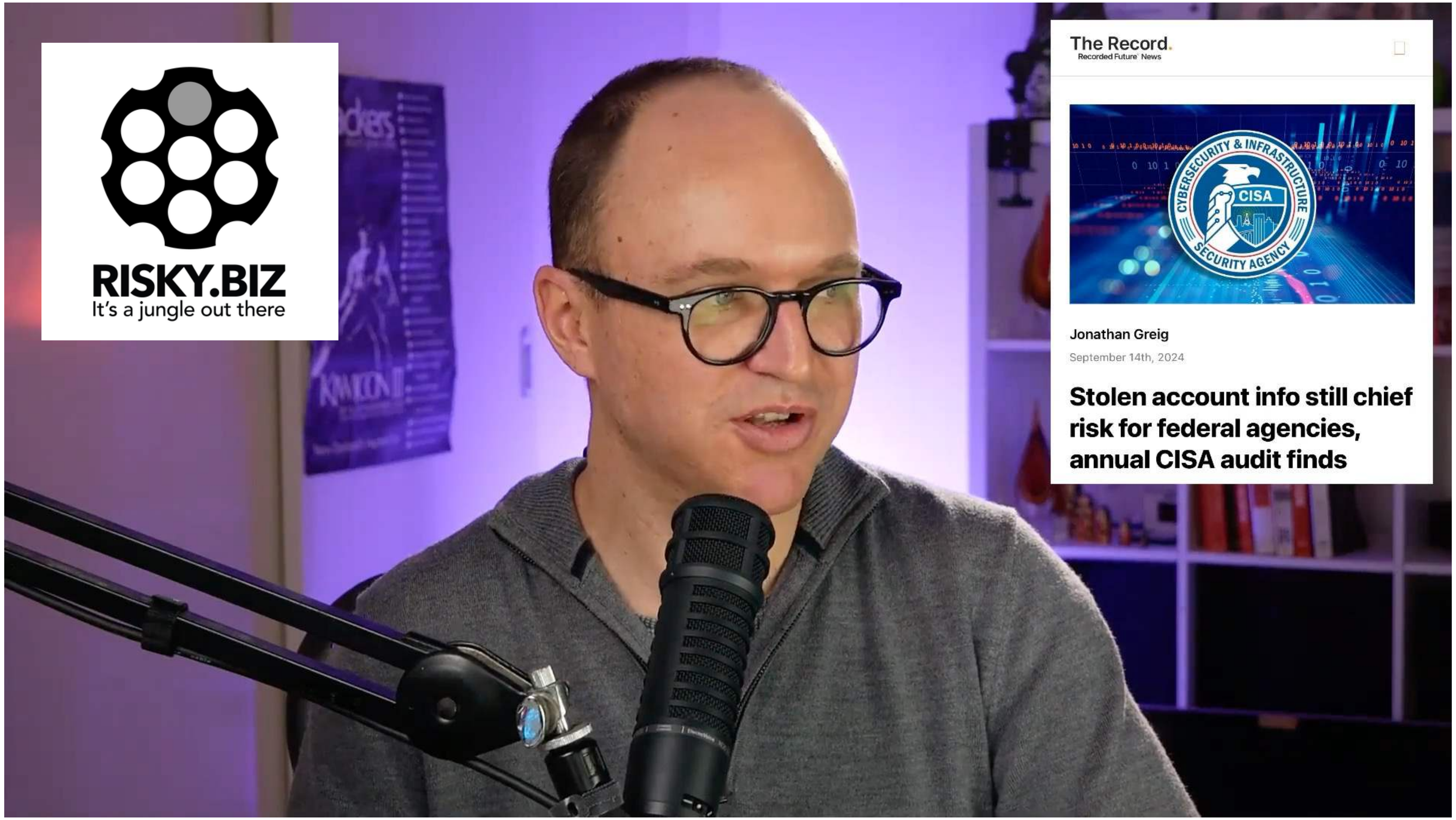


There has also been a rise in compromises of cloud-based identities secured with multi-factor authentication (MFA). Particularly concerning is the growing use of web proxy or adversary-in-the-middle (AiTM) phishing pages, which can bypass many MFA implementations by stealing sensitive session tokens. 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

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

25-9-2024

RISKY BUSINESS 18-SEPT-24 – CISA AUDIT

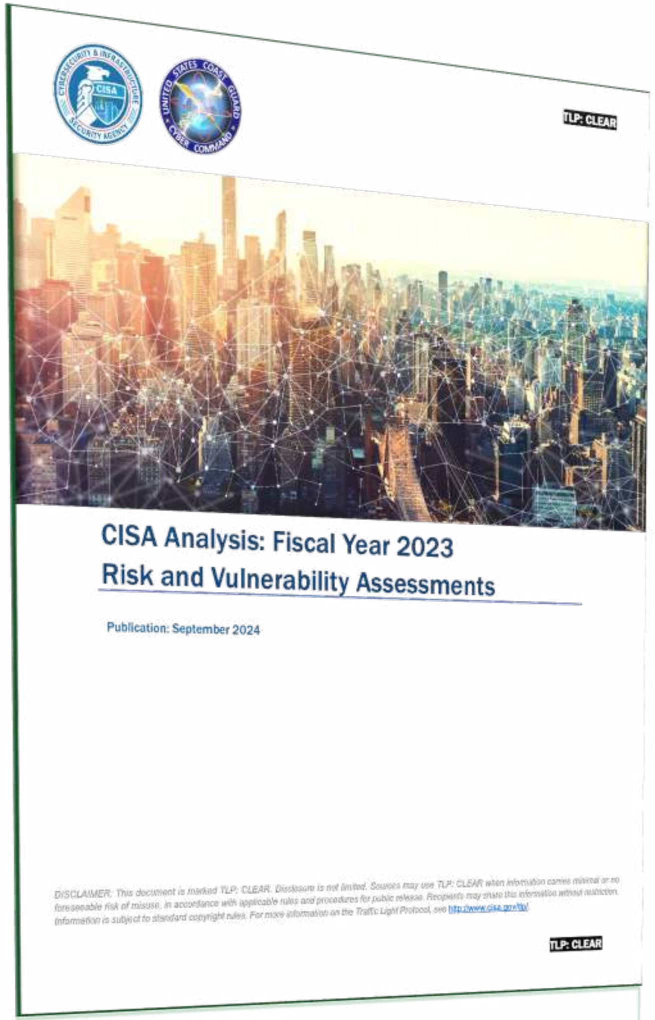


RISKY.BIZ
It's a jungle out there

The Record.
Recorded Future News

Jonathan Greig
September 14th, 2024

Stolen account info still chief risk for federal agencies, annual CISA audit finds



TLP: CLEAR

CISA Analysis: Fiscal Year 2023
Risk and Vulnerability Assessments

Publication: September 2024

DISCLAIMER: This document is marked TLP: CLEAR. Disclosure is not limited. Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

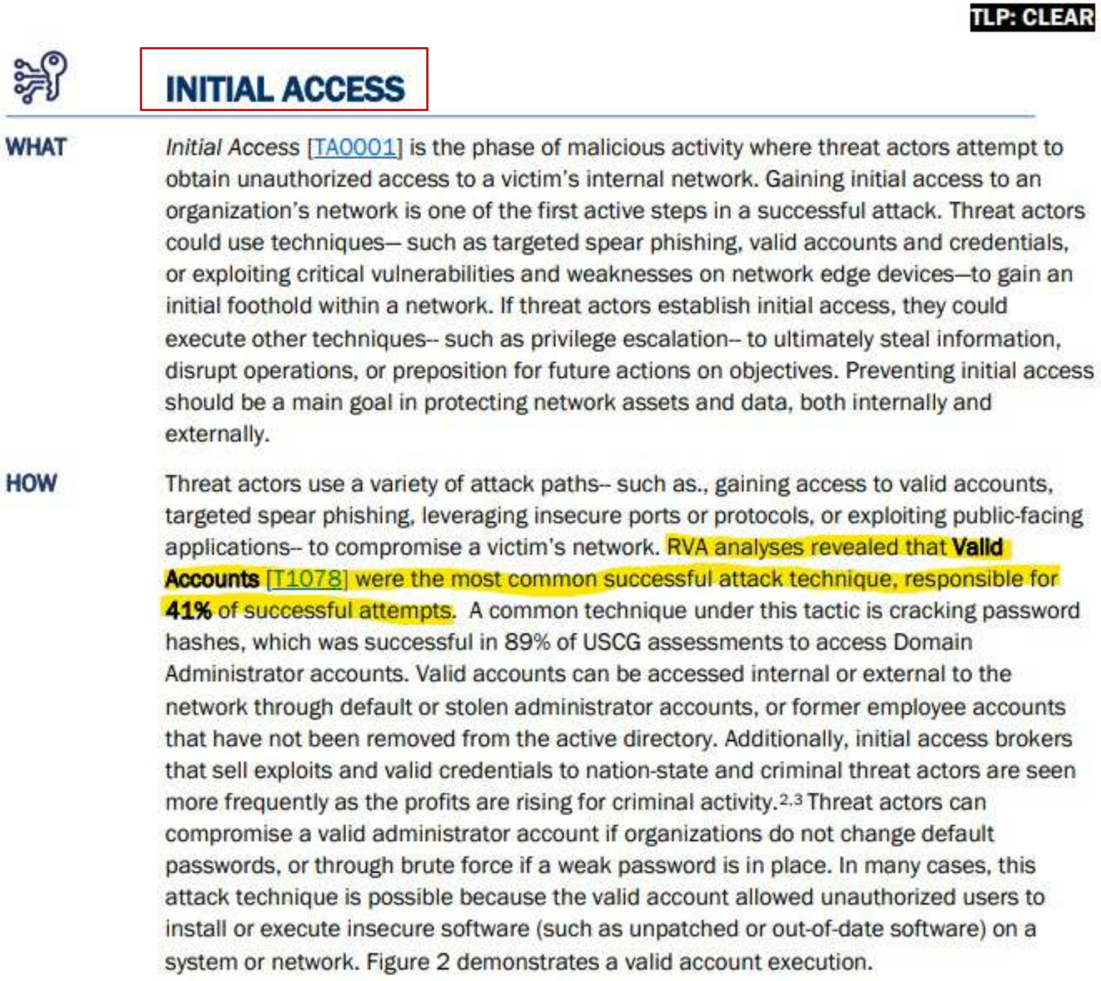
TLP: CLEAR

https://youtu.be/uPjcpKPYF8g?t=1267 (from 21:07)

AtticSecurity.com
by ZOLDER

25-9-2024

41% THROUGH STOLEN CREDS



TLP: CLEAR

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.

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

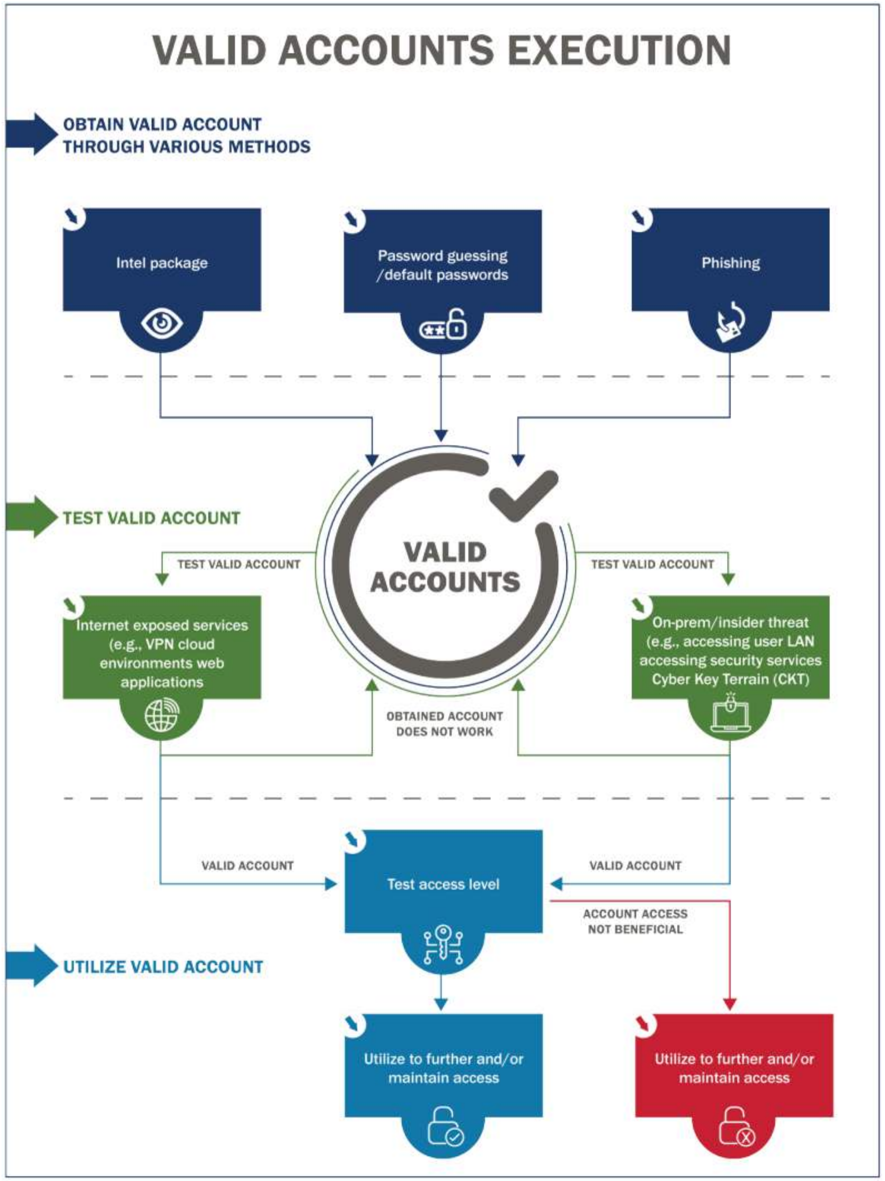
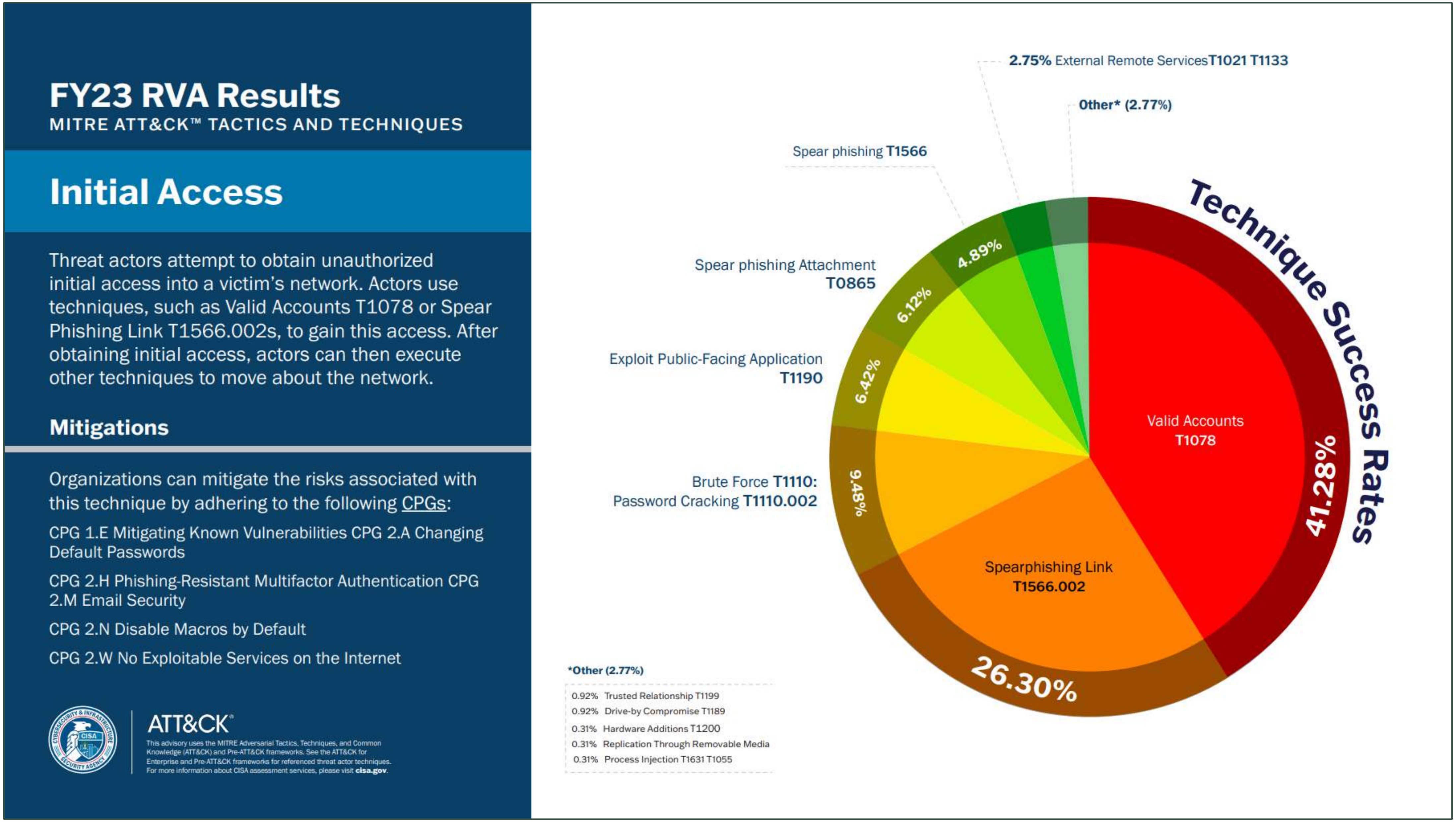

VALID ACCOUNTS EXECUTION
OBTAIN VALID ACCOUNT THROUGH VARIOUS METHODS
Intel package
Password guessing /default passwords
Phishing
TEST VALID ACCOUNT
TEST VALID ACCOUNT
TEST VALID ACCOUNT
VALID ACCOUNTS
Internet exposed services (e.g., VPN cloud environments web applications
On-prem/insider threat (e.g., accessing user LAN accessing security services Cyber Key Terrain (CKT)
OBTAINED ACCOUNT DOES NOT WORK
VALID ACCOUNT
VALID ACCOUNT
Test access level
ACCOUNT ACCESS NOT BENEFICIAL
UTILIZE VALID ACCOUNT
Utilize to further and/or maintain access
Utilize to further and/or maintain access

Figure 2: Valid Account Execution



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 referenced threat actor techniques. For more information about CISA assessment services, please visit **cisa.gov**.

Technique Success Rates
2.75% External Remote ServicesT1021 T1133
Other* (2.77%)
Spear phishing T1566
4.89%
Spear phishing Attachment T0865
6.12%
Exploit Public-Facing Application T1190
6.42%
Brute Force T1110: Password Cracking T1110.002
9.48%
Valid Accounts T1078
41.28%
Spearphishing Link T1566.002
26.30%

***Other (2.77%)**

0.92%	Trusted Relationship T1199
0.92%	Drive-by Compromise T1189
0.31%	Hardware Additions T1200
0.31%	Replication Through Removable Media
0.31%	Process Injection T1631 T1055

https://www.cisa.gov/sites/default/files/2024-09/InfographicFY23RVA508.pdf

5 LESSONS LEARNED

LESSON #1
AITM & TOKEN REPLAY

MFA-resilient Phishing Techniques

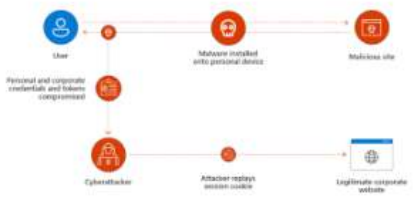
#1: AITM & TOKEN REPLAY

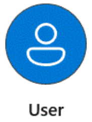
Microsoft Threat Intelligence
44,407 followers
1mo •
+ Follow

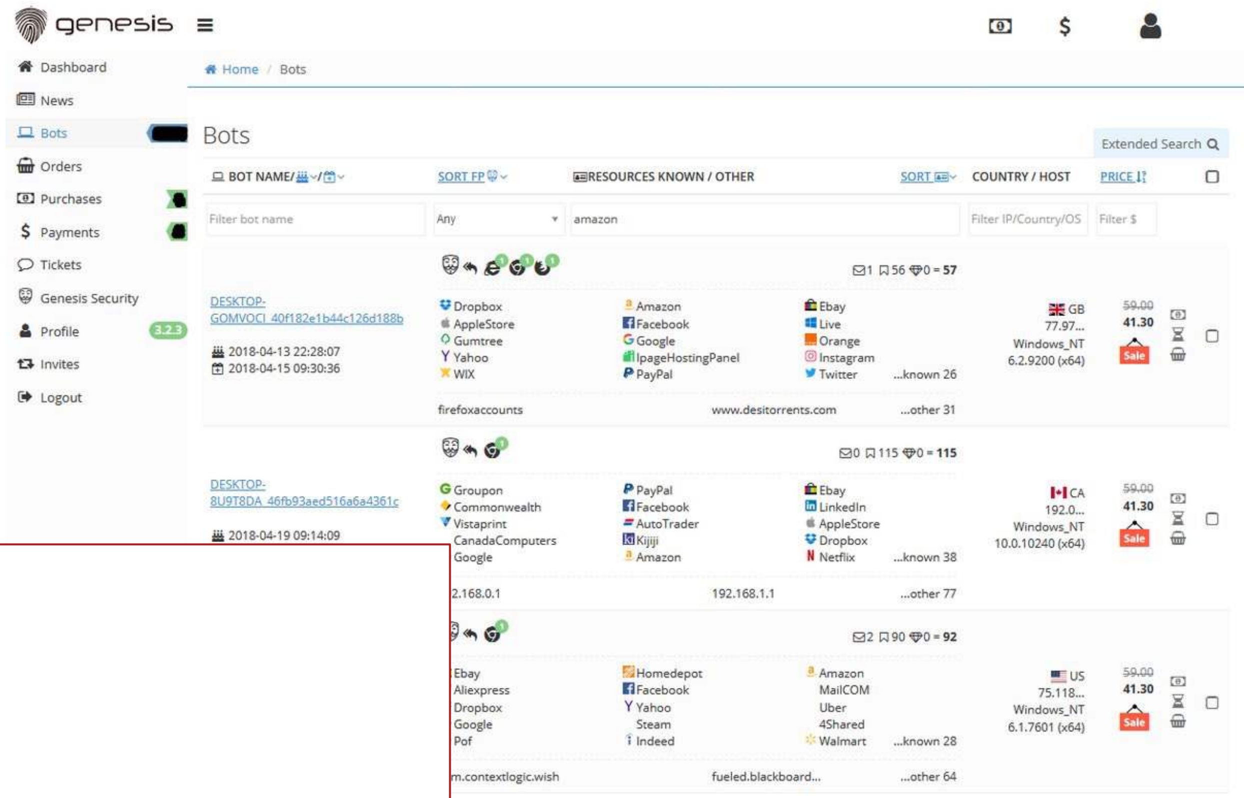
Microsoft has detected a 111% year-over-year increase in token replay attacks, and incidents are continuing to grow. In token replay attacks, attackers steal tokens – authentication artifacts that grant users access to resources – commonly via malware or adversary-in-the-middle (AiTM) attacks, and then 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/6042lSgTq

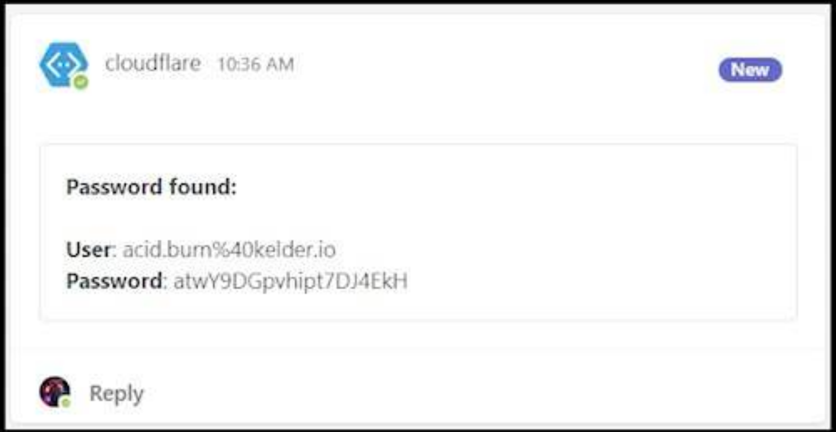

User
Malware installed onto personal device
Malicious site
Personal and corporate credentials and tokens compromised
Cyberattacker
Attacker replays session cookie
Legitimate corporate website





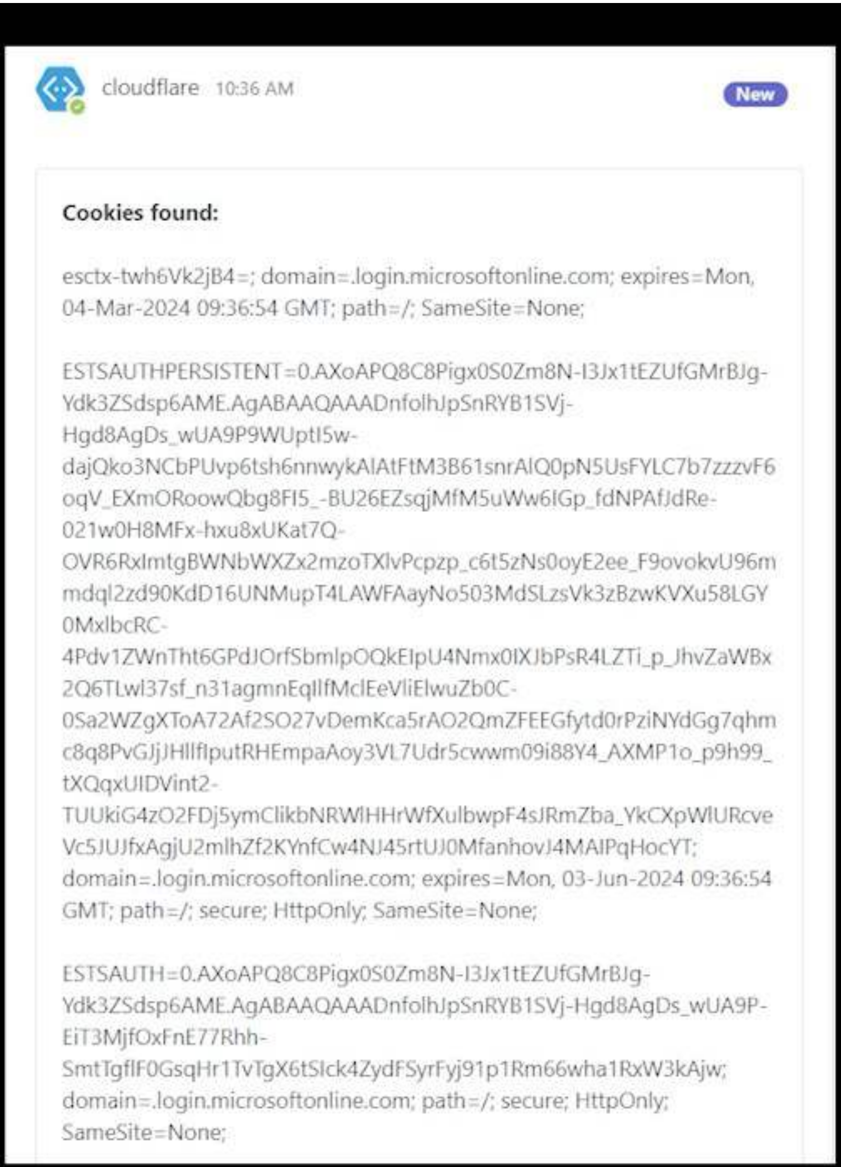
Bots

BOT NAME/ /	SORT FP	RESOURCES KNOWN / OTHER			SORT	COUNTRY / HOST	PRICE	□
Filter bot name	Any	amazon				Filter IP/Country/OS	Filter $	
DESKTOP-GOMVOCI_40f182e1b44c126d188b 2018-04-13 22:28:07 2018-04-15 09:30:36		Dropbox AppleStore Gumtree Yahoo WIX firefoxaccounts	Amazon Facebook Google IpageHostingPanel PayPal www.desitorrents.com	Ebay Live Orange Instagram Twitter	1 56 0 = 57 ...known 26 ...other 31	GB 77.97... Windows_NT 6.2.9200 (x64)	~~59.00~~ 41.30 Sale	□
DESKTOP-8U9T8DA_46fb93aed516a6a4361c 2018-04-19 09:14:09		Groupon Commonwealth Vistaprint CanadaComputers Google 2.168.0.1	PayPal Facebook AutoTrader Kijiji Amazon 192.168.1.1	Ebay LinkedIn AppleStore Dropbox Netflix	0 115 0 = 115 ...known 38 ...other 77	CA 192.0... Windows_NT 10.0.10240 (x64)	~~59.00~~ 41.30 Sale	□
		Ebay Aliexpress Dropbox Google Pof m.contextlogic.wish	Homedepot Facebook Yahoo Steam Indeed fueled.blackboard...	Amazon MailCOM Uber 4Shared Walmart	2 90 0 = 92 ...known 28 ...other 64	US 75.118... Windows_NT 6.1.7601 (x64)	~~59.00~~ 41.30 Sale	□



Password found:

User: acid.burn%40kelder.io
Password: atwY9DGpvhipt7DJ4EkH



Cookies found:

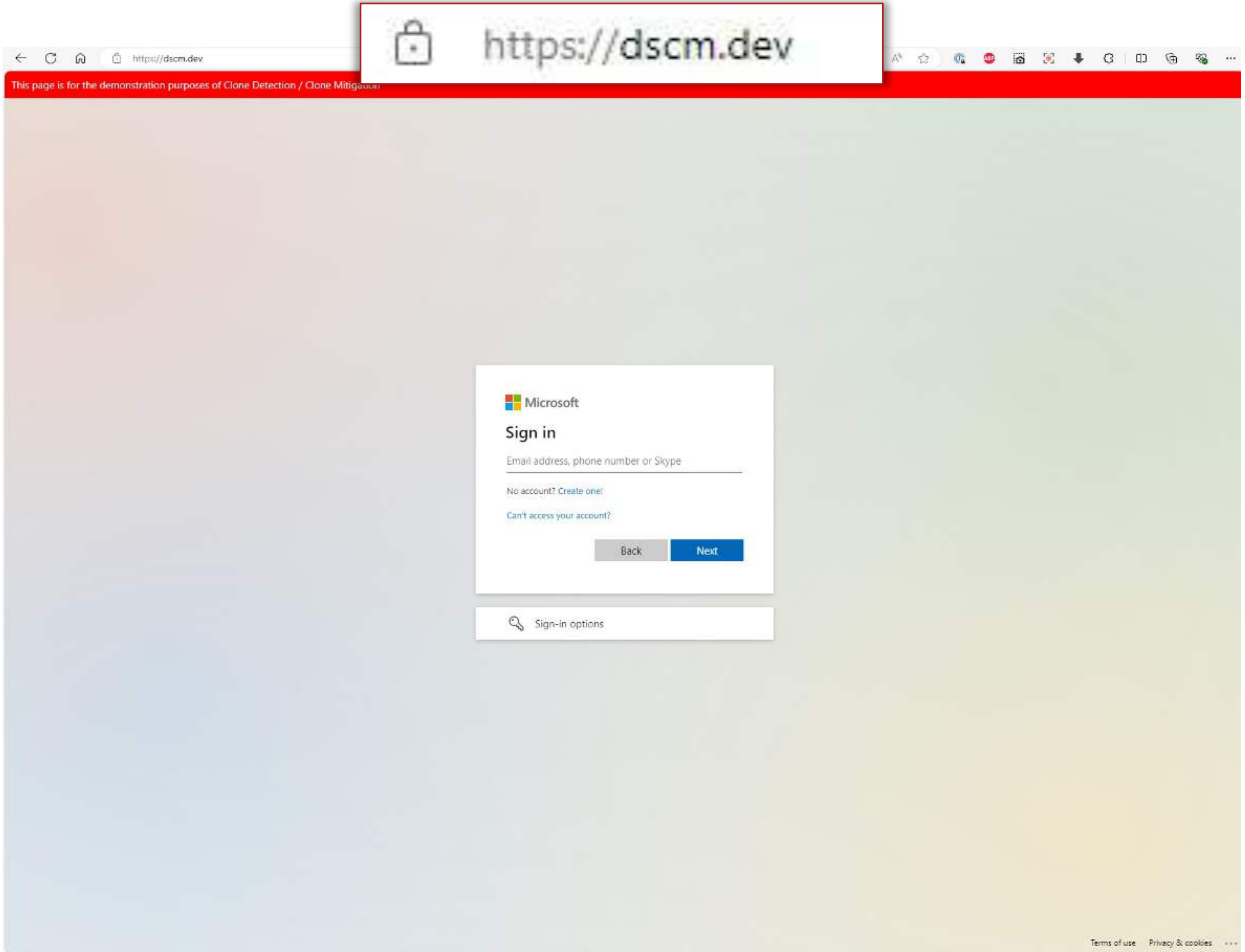
```
esctx-twh6Vk2jB4=; domain=.login.microsoftonline.com; expires=Mon,
04-Mar-2024 09:36:54 GMT; path=/; SameSite=None;

ESTSAUTHPERSISTENT=0.AXoAPQ8C8Pigx0S0Zm8N-I3Jx1tEZUfGMrBJg-
Ydk3ZSdsp6AME.AgABAAQAAADnfolhJpSnRYB1SVj-
Hgd8AgDs_wUA9P9WUptI5w-
dajQko3NCbPUvp6tsh6nnwykAIAtFtM3B61snrAIQ0pN5UsFYLC7b7zzzvF6
oqV_EXmORoowQbg8FI5_-BU26EZsqjMfM5uWw6IGp_fdNPAfJdRe-
021w0H8MFx-hxu8xUKat7Q-
OVR6RxImtgBWNbWXZx2mzoTXlvPcpzp_c6t5zNs0oyE2ee_F9ovokvU96m
mdql2zd90KdD16UNMupT4LAWFAayNo503MdSLzsVk3zBzwKVXu58LGY
0MxlbcRC-
4Pdv1ZWnTht6GPdJOrfSbmlpOQkElpU4Nmx0IXJbPsR4LZTi_p_JhvZaWBx
2Q6TLwl37sf_n31agmnEqIlfMclEeVliElwuZb0C-
0Sa2WZgXToA72Af2SO27vDemKca5rAO2QmZFEEGfytd0rPziNYdGg7qhm
c8q8PvGJjJHllfIputRHEmpaAoy3VL7Udr5cwwm09i88Y4_AXMP1o_p9h99_
tXQqxUIDVint2-
TUUkiG4zO2FDj5ymClikbNRWlHHrWfXulbwpF4sJRmZba_YkCXpWIURcve
Vc5JUJfxAgjU2mlhZf2KYnfCw4NJ45rtUJ0MfanhovJ4MAIPqHocYT;
domain=.login.microsoftonline.com; expires=Mon, 03-Jun-2024 09:36:54
GMT; path=/; secure; HttpOnly; SameSite=None;

ESTSAUTH=0.AXoAPQ8C8Pigx0S0Zm8N-I3Jx1tEZUfGMrBJg-
Ydk3ZSdsp6AME.AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-
EiT3MjfOxFnE77Rhh-
SmtTgflF0GsqHr1TvTgX6tSIck4ZydFSyrFyj91p1Rm66wha1RxW3kAjw;
domain=.login.microsoftonline.com; path=/; secure; HttpOnly;
SameSite=None;
```

https://youtu.be/v6qDYYVfQd4?si=6a7Lo6z-gacQdL9D

EVILGINX POC



https://dscm.dev

This page is for the demonstration purposes of Clone Detection / Clone Mitigation

Microsoft

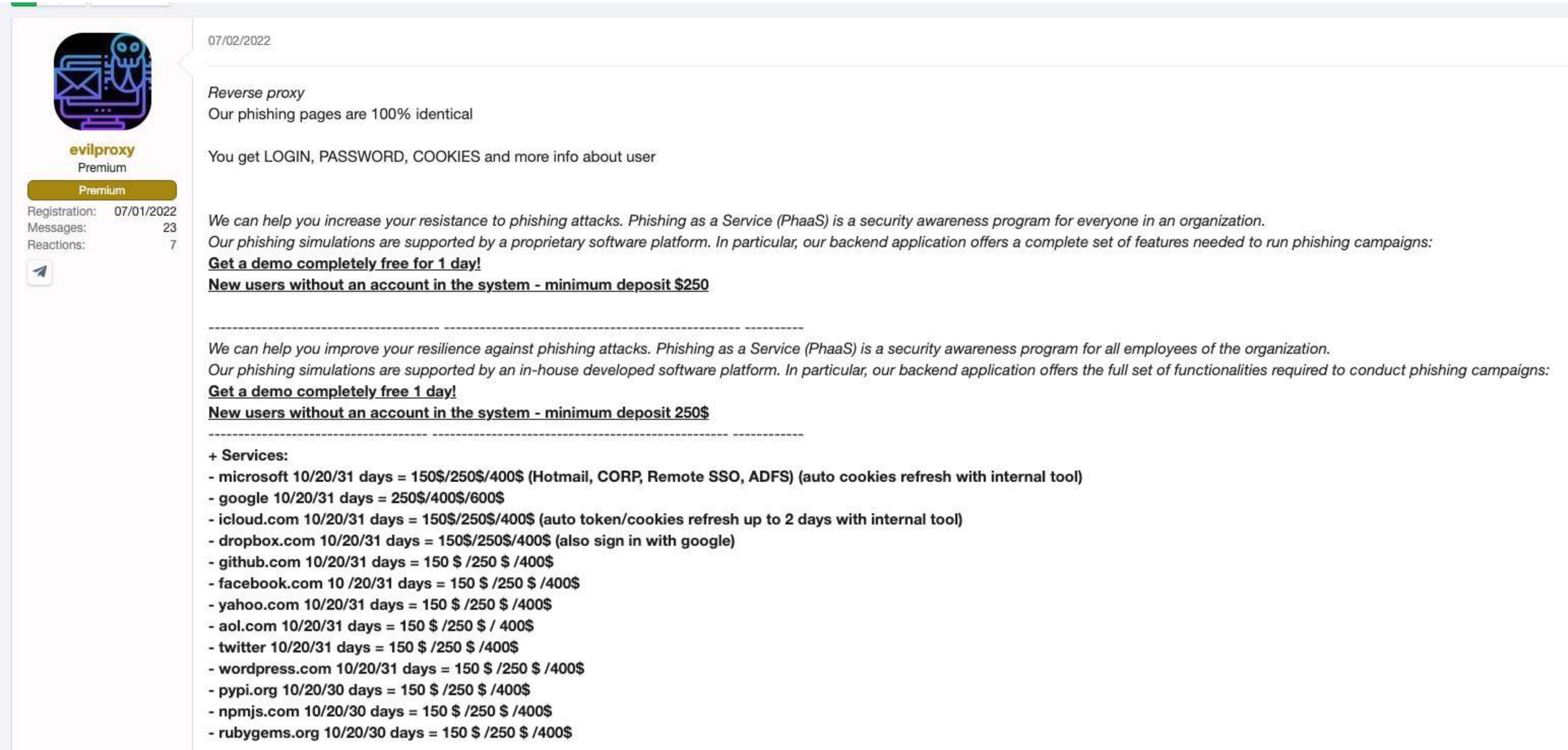
Sign in

Email address, phone number or Skype

No account? Create one!

Can't access your account?

CAAS > EVILPROXY



evilproxy
Premium

Premium

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

07/02/2022

Reverse proxy
Our phishing pages are 100% identical

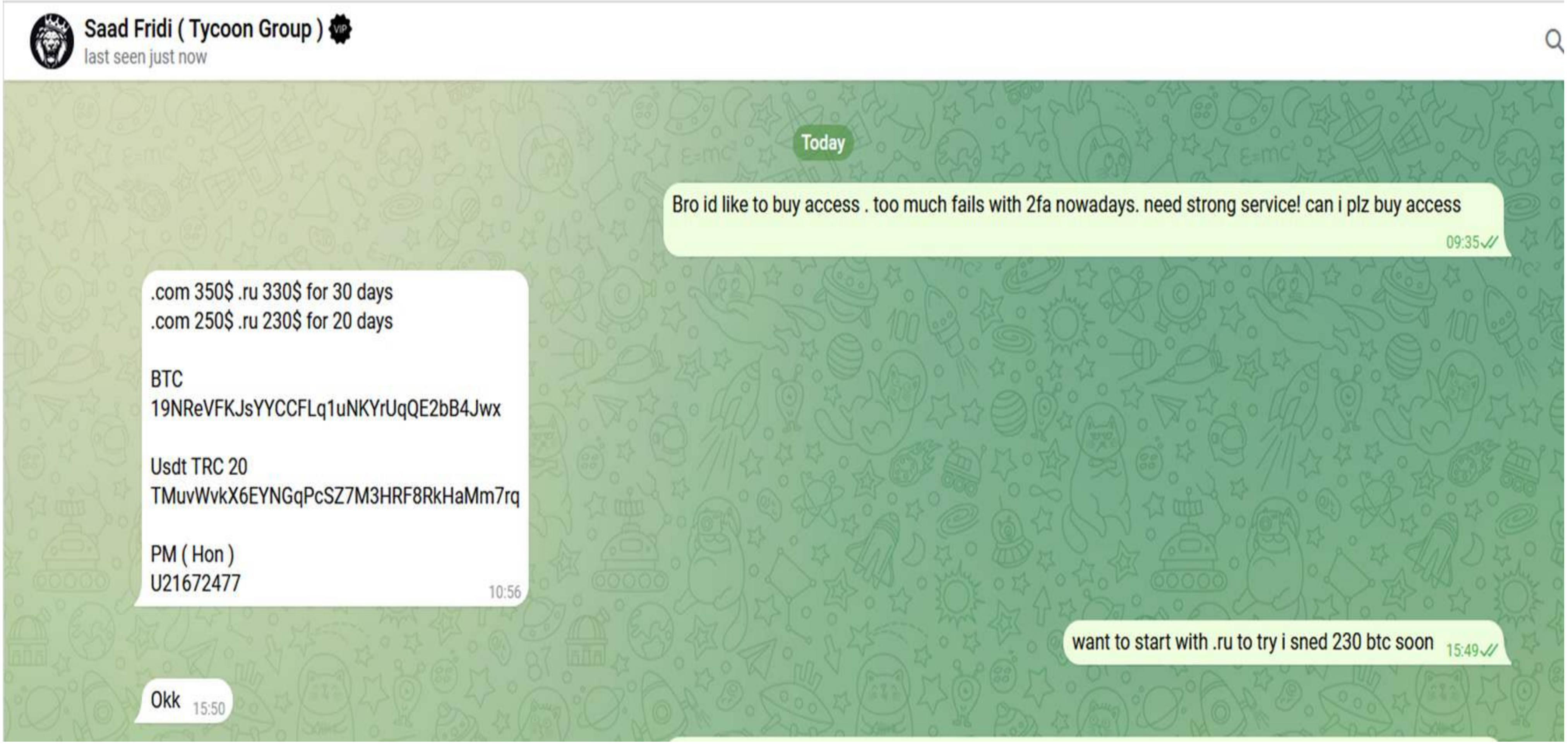
You get LOGIN, PASSWORD, COOKIES and more info about user

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



Saad Fridi (Tycoon Group)

last seen just now

Today

Bro id like to buy access . too much fails with 2fa nowadays. need strong service! can i plz buy access 09:35

.com 350$ .ru 330$ for 30 days
.com 250$ .ru 230$ for 20 days

BTC
19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx

Usdt TRC 20
TMuvWvkX6EYNGqPcSZ7M3HRF8RkHaMm7rq

PM (Hon)
U21672477 10:56

want to start with .ru to try i sned 230 btc soon 15:49

Okk 15:50

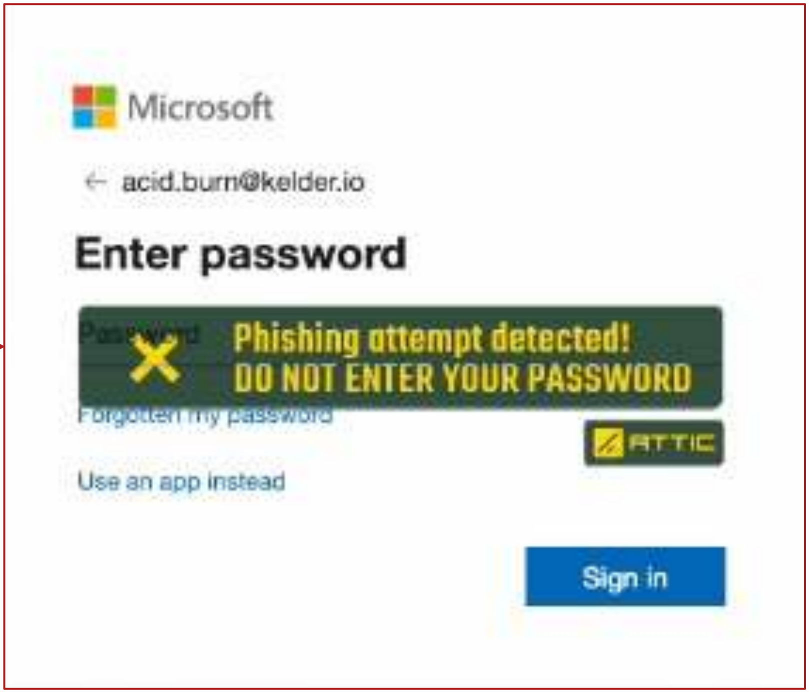
MEASURES VS AITM?

- **Phishing Resistant MFA**
  - Passkeys
  - Windows Hello
  - FIDO2 key
  - Certificates

- **Compliance-based Conditional Access**
  - Non-BYOD friendly

- **Custom CSS**

- **SafeLinks**



Microsoft

← acid.burn@kelder.io

Enter password

Password

Phishing attempt detected!
DO NOT ENTER YOUR PASSWORD

Forgotten my password

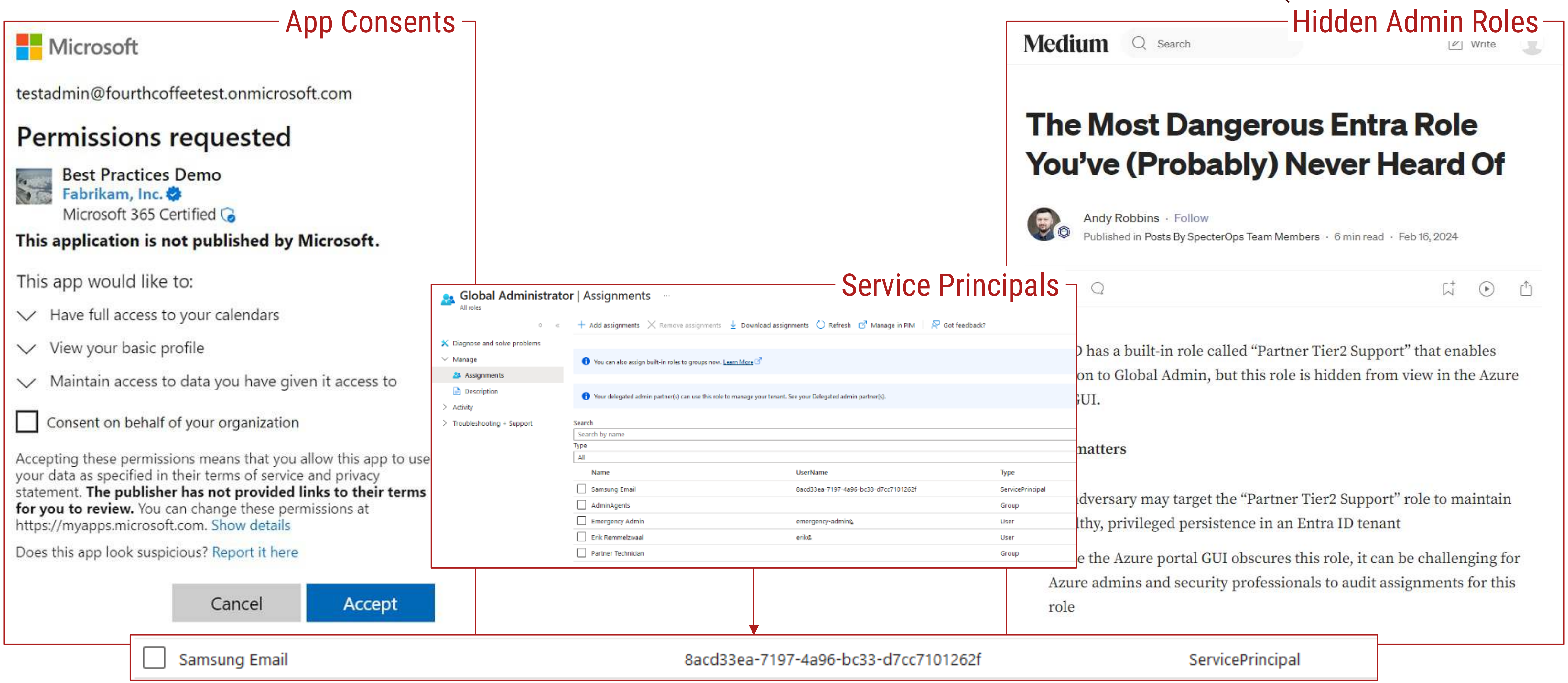
Use an app instead

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



Hidden Admin Roles

App Consents

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

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

Service Principals

Global Admininistrator | Assignments

All roles

You can also assign built-in roles to groups now. Learn More

Your delegated admin partner(s) can use this role to manage your tenant. See your Delegated admin partner(s).

Search: Search by name

Type: All

	Name	UserName	Type
□	Samsung Email	8acd33ea-7197-4a96-bc33-d7cc7101262f	ServicePrincipal
□	AdminAgents		Group
□	Emergency Admin	emergency-admin@	User
□	Erik Remmelzwaal	erik@	User
□	Partner Technician		Group

□	Samsung Email	8acd33ea-7197-4a96-bc33-d7cc7101262f	ServicePrincipal

The Most Dangerous Entra Role You’ve (Probably) Never Heard Of

Andy Robbins · Follow

Published in Posts By SpecterOps Team Members · 6 min read · Feb 16, 2024

D has a built-in role called “Partner Tier2 Support” that enables
on to Global Admin, but this role is hidden from view in the Azure
GUI.

matters

dversary may target the “Partner Tier2 Support” role to maintain
lthy, privileged persistence in an Entra ID tenant

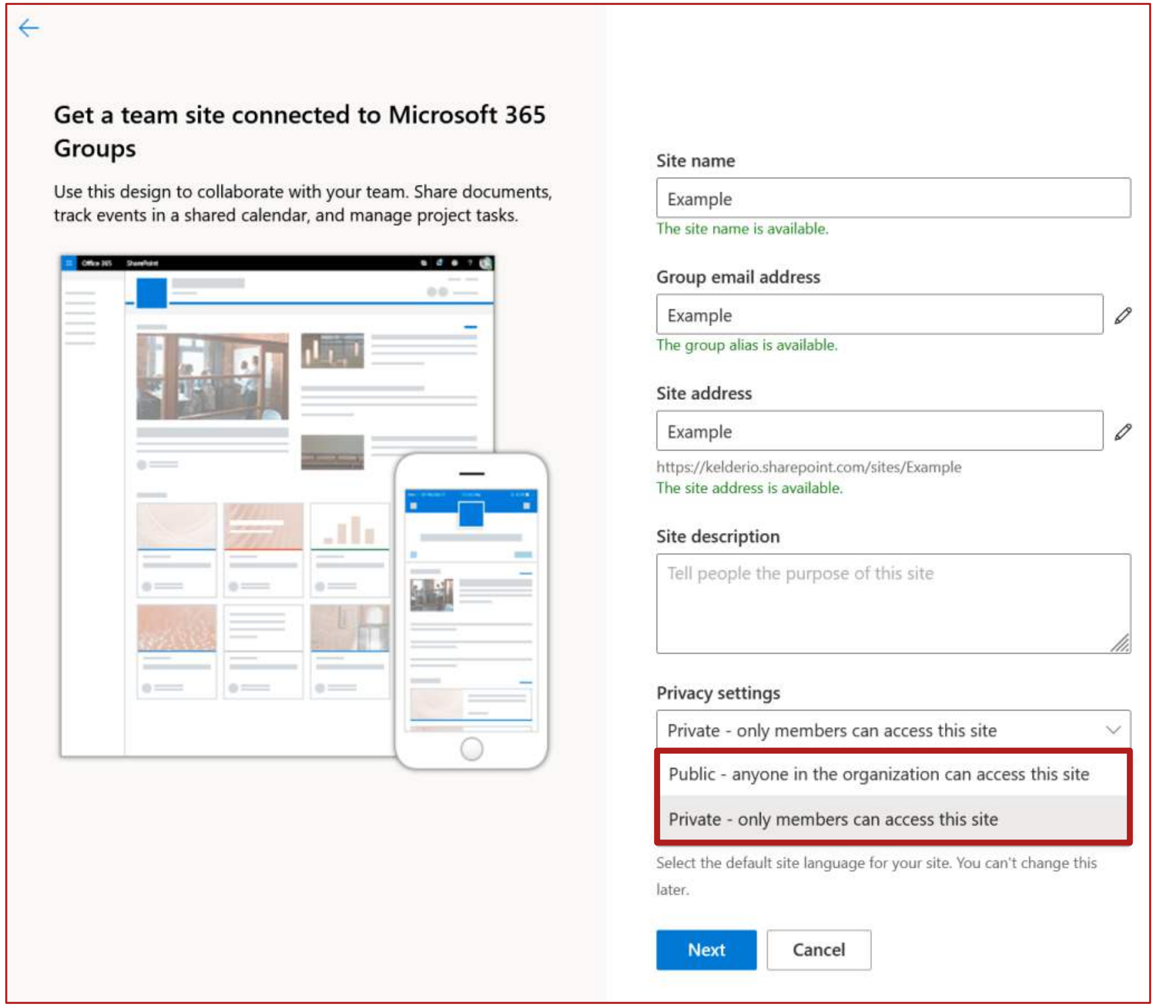
e the Azure portal GUI obscures this role, it can be challenging for Azure admins and security professionals to audit assignments for this role

25-9-2024

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

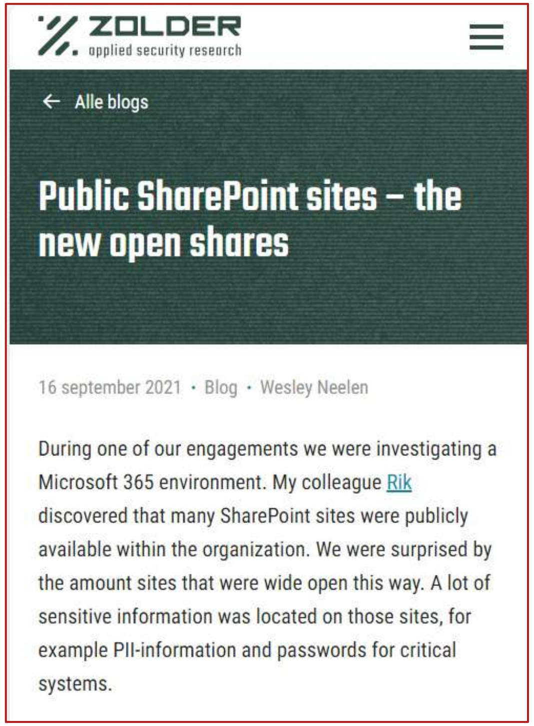
Privacy settings

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.

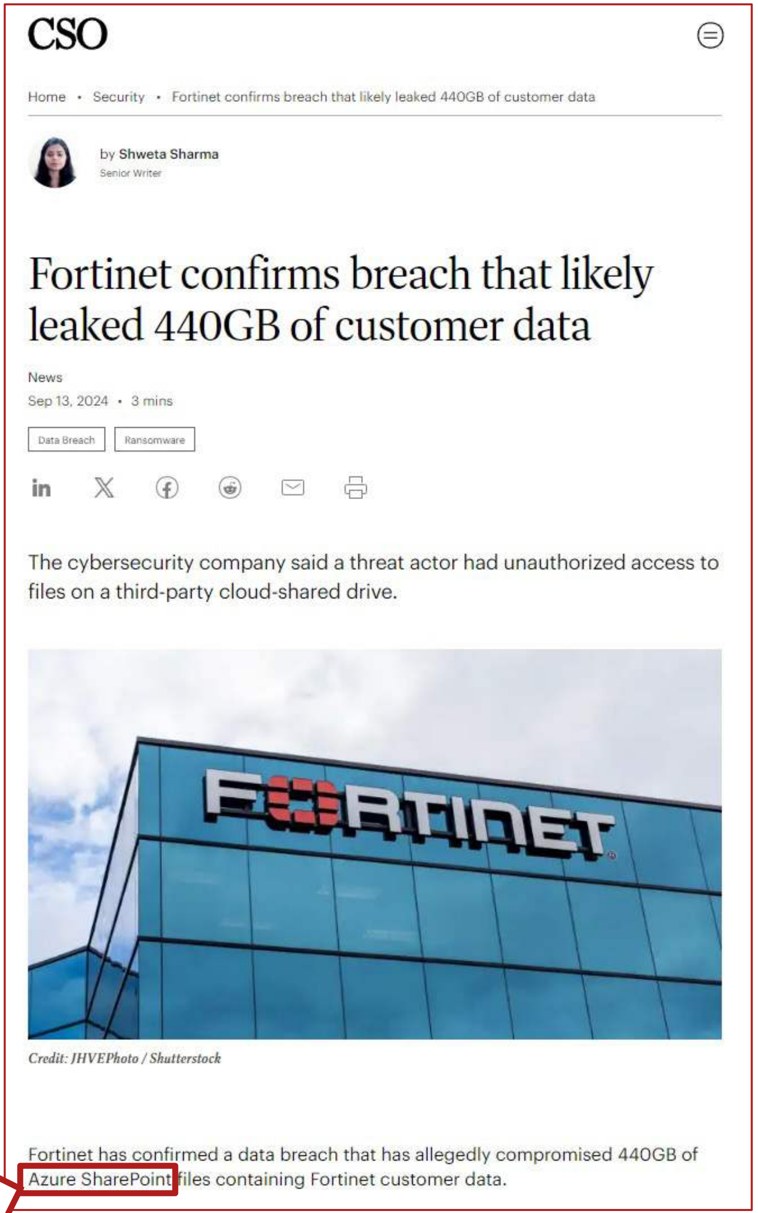


Public SharePoint sites – the new open shares

16 september 2021 • Blog • Wesley Neelen

During one of our engagements we were investigating a Microsoft 365 environment. My colleague Rik 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/



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

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

Credit: JHVEPhoto / 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

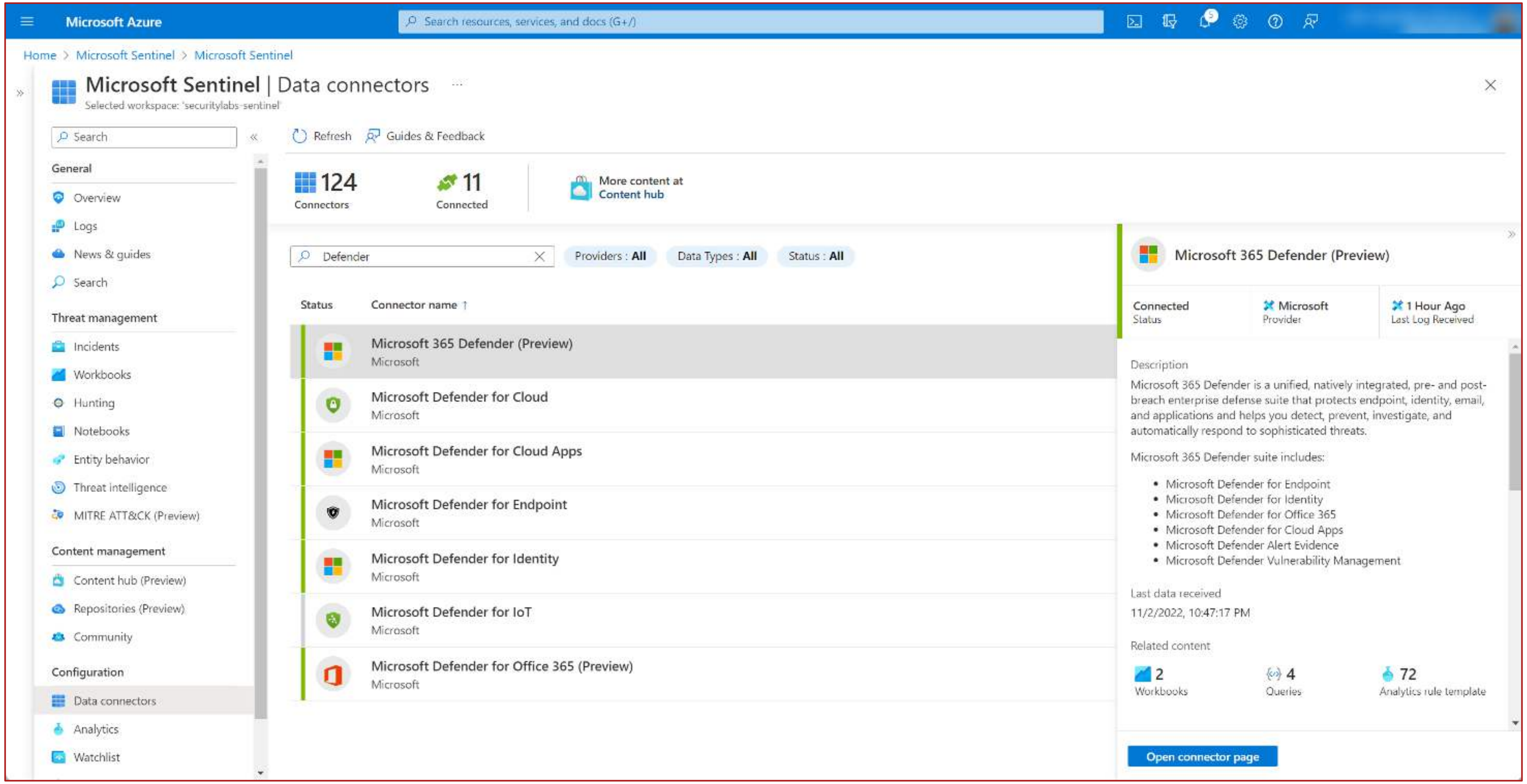
#4: FREE LOGGING & MONITORING

Microsoft Sentinel

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



Microsoft Sentinel | Data connectors

Selected workspace: 'securitylabs-sentinel'

124 Connectors

11 Connected

Defender

Status	Connector name ↑
	Microsoft 365 Defender (Preview) Microsoft
	Microsoft Defender for Cloud Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft
	Microsoft Defender for IoT Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft

Microsoft 365 Defender (Preview)

Connected
Status

Microsoft
Provider

1 Hour Ago
Last Log Received

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence
- Microsoft Defender Vulnerability Management

Last data received

11/2/2022, 10:47:17 PM

Related content

2 Workbooks

4 Queries

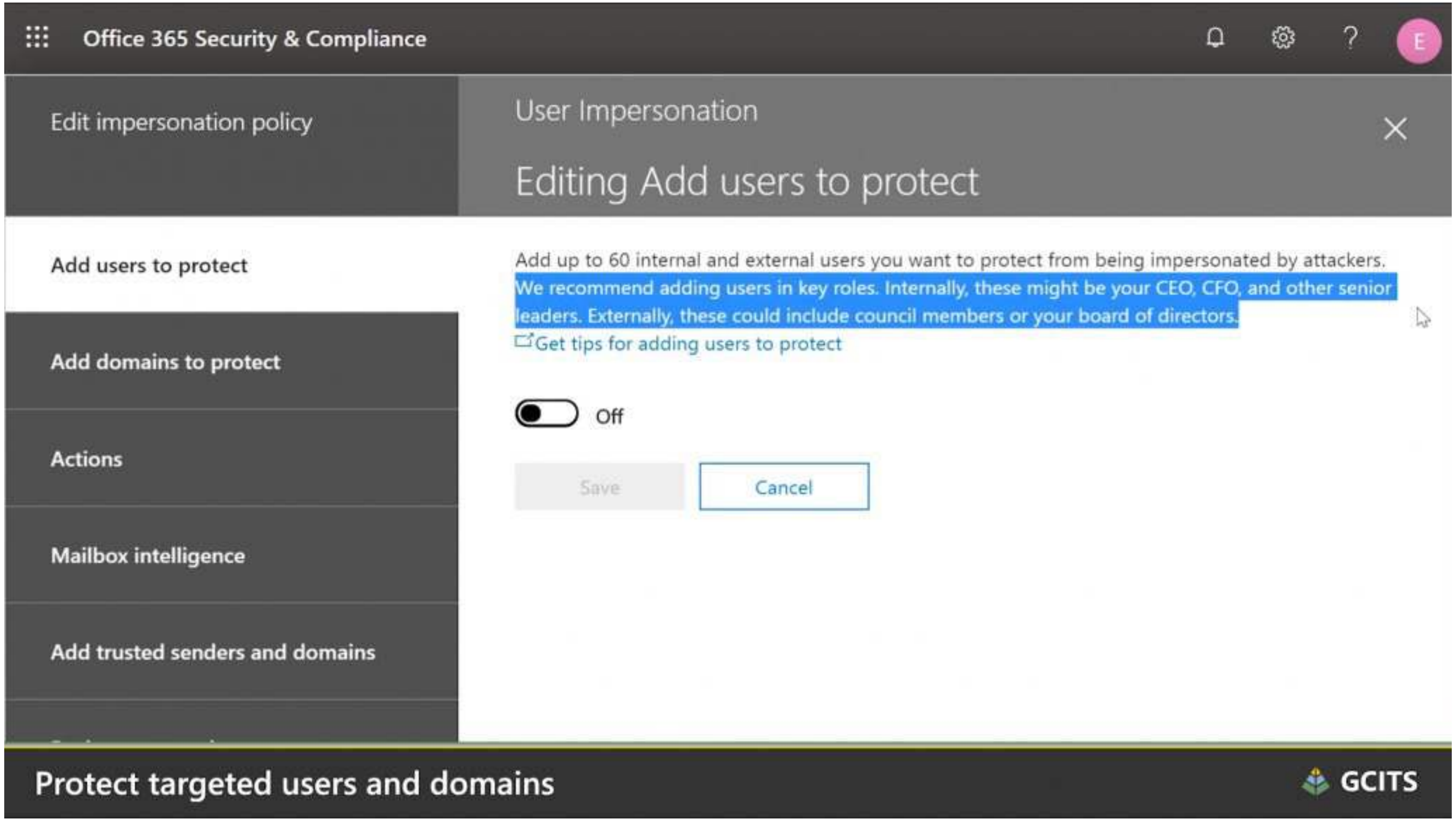
72 Analytics rule template

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
E
Edit impersonation policy
Add users to protect
Add domains to protect
Actions
Mailbox intelligence
Add trusted senders and domains
Save
Cancel
GCITS

User Impersonation

Editing Add users to protect

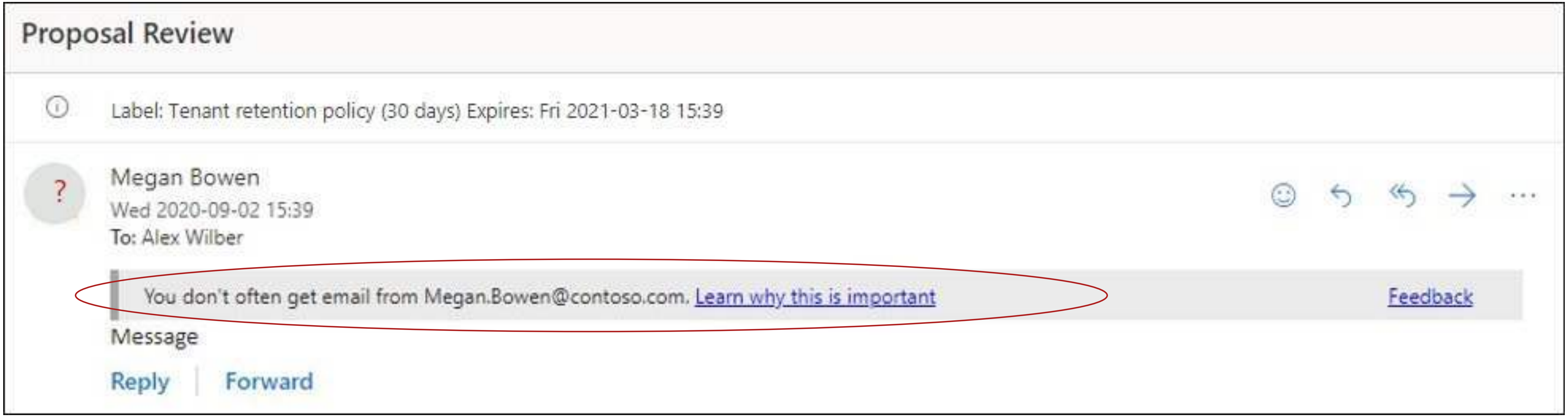
Add up to 60 internal and external users you want to protect from being impersonated by attackers. We recommend adding users in key roles. Internally, these might be your CEO, CFO, and other senior leaders. Externally, these could include council members or your board of directors.

Get tips for adding users to protect

Off

Protect targeted users and domains

PHISHING MAILTIPS



Proposal Review

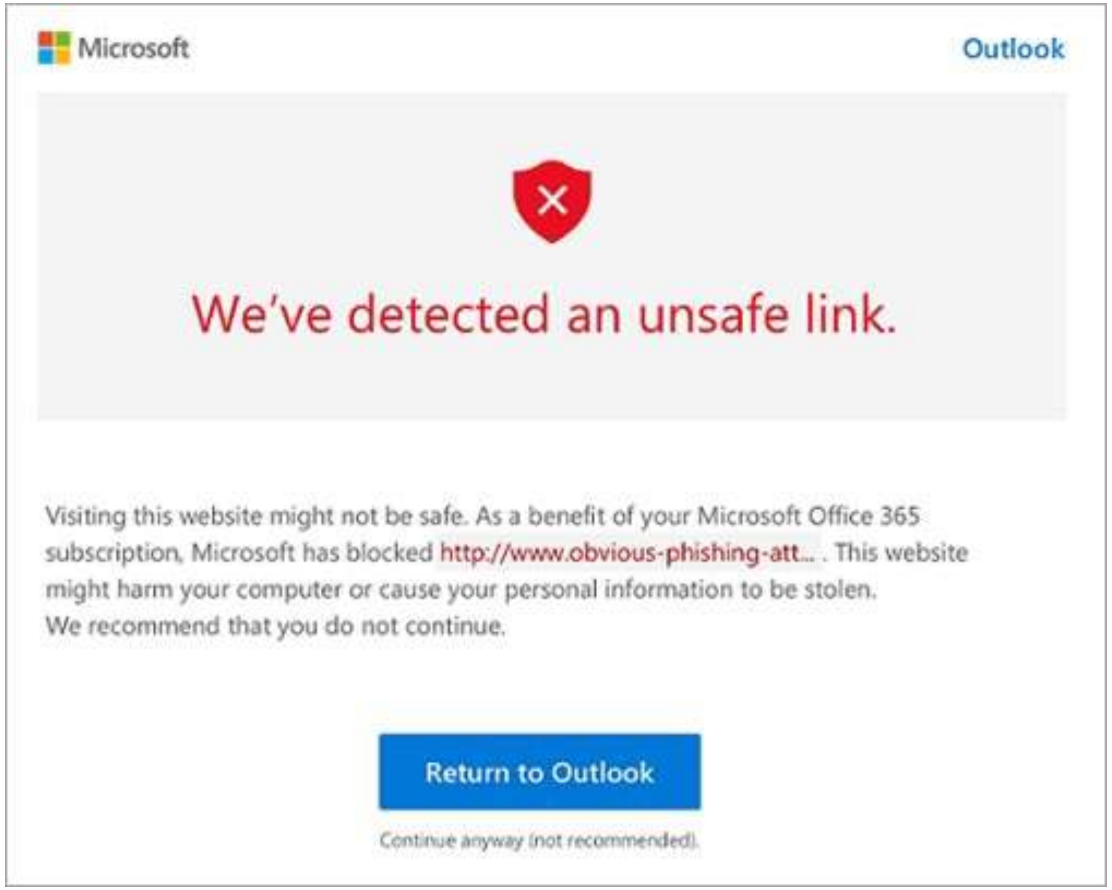
Label: Tenant retention policy (30 days) Expires: Fri 2021-03-18 15:39

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

SAFELINKS

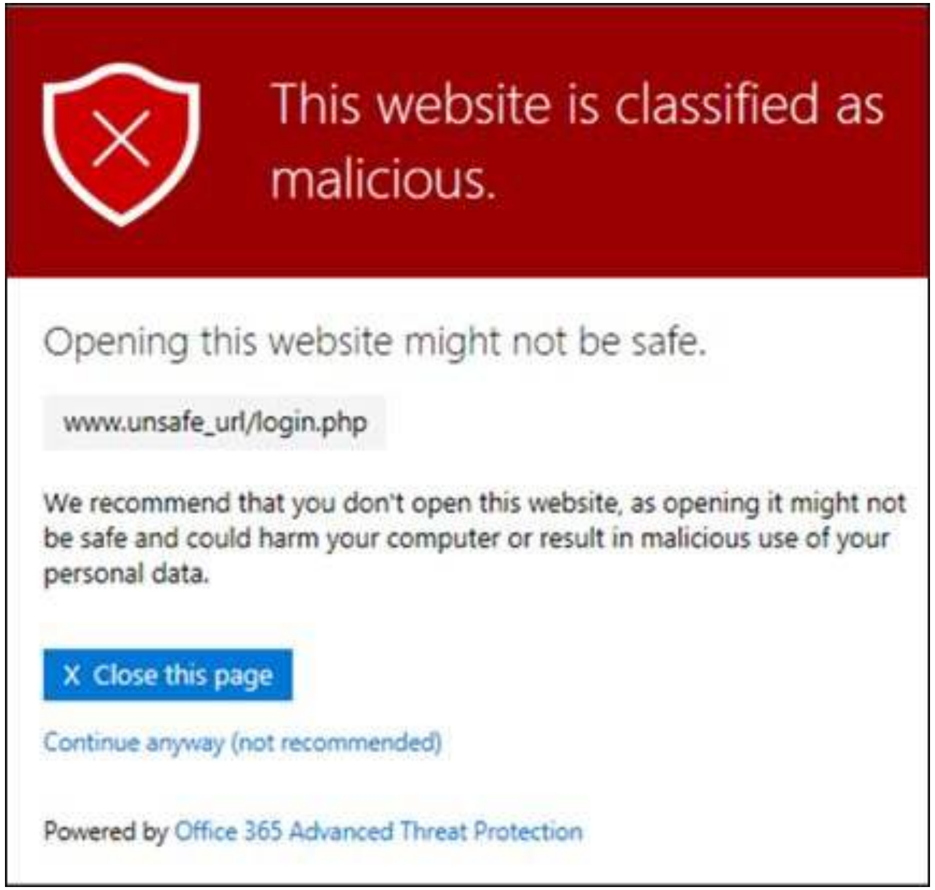


Microsoft

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.



This website is classified as malicious.

Opening this website might not be safe.

www.unsafe_url/login.php

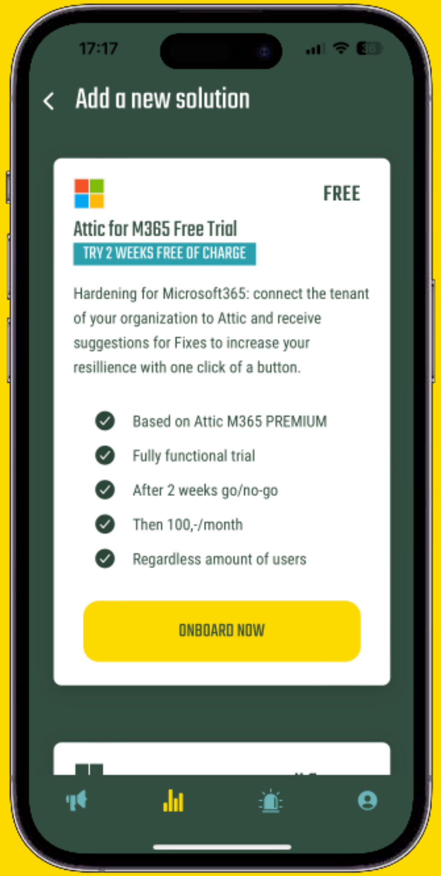
We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

Powered by Office 365 Advanced Threat Protection

ATTIC SECURITY

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

ONBOARD



17:17

Add a new solution

FREE

Attic for M365 Free Trial

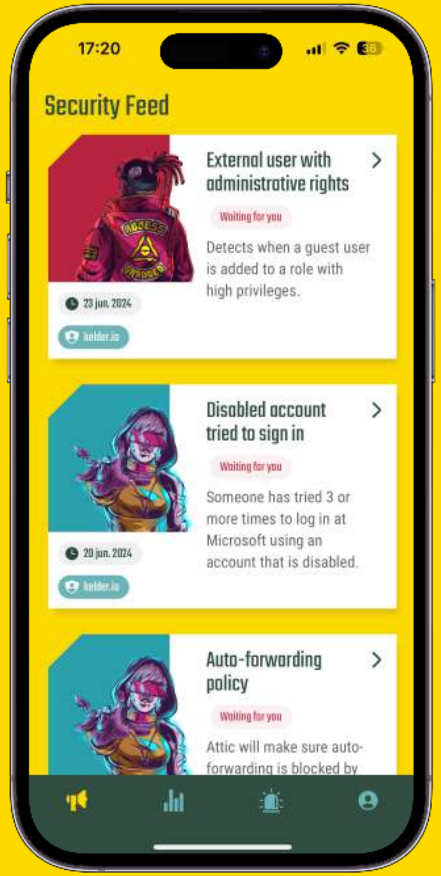
TRY 2 WEEKS FREE OF CHARGE

Hardening for Microsoft365: connect the tenant of your organization to Attic and receive suggestions for Fixes to increase your resillience with one click of a button.

- ✓ Based on Attic M365 PREMIUM
- ✓ Fully functional trial
- ✓ After 2 weeks go/no-go
- ✓ Then 100,-/month
- ✓ Regardless amount of users

ONBOARD NOW

ALARM



17:20

Security Feed

External user with administrative rights

Waiting for you

Detects when a guest user is added to a role with high privileges.

23 jun. 2024

kelder.io

Disabled account tried to sign in

Waiting for you

Someone has tried 3 or more times to log in at Microsoft using an account that is disabled.

20 jun. 2024

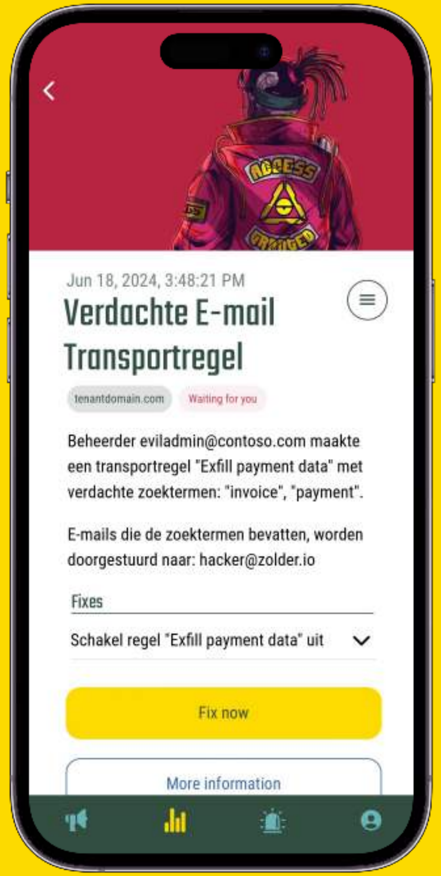
kelder.io

Auto-forwarding policy

Waiting for you

Attic will make sure auto-forwarding is blocked by

FIX



Jun 18, 2024, 3:48:21 PM

Verdachte E-mail Transportregel

tenantdomain.com

Waiting for you

Beheerder eviladmin@contoso.com maakte een transportregel "Exfill payment data" met verdachte zoektermen: "invoice", "payment".

E-mails die de zoektermen bevatten, worden doorgestuurd naar: hacker@zolder.io

Fixes

Schakel regel "Exfill payment data" uit

Fix now

More information

AtticSecurity.com
by ZOLDER

1 minute explanatory video: https://youtu.be/MvdgQUVUCy8