

From the trenches: Working with Microsoft as a researcher

Dr Nestori Syynimaa **@DrAzureAD**

People of Microsoft, I come in peace!



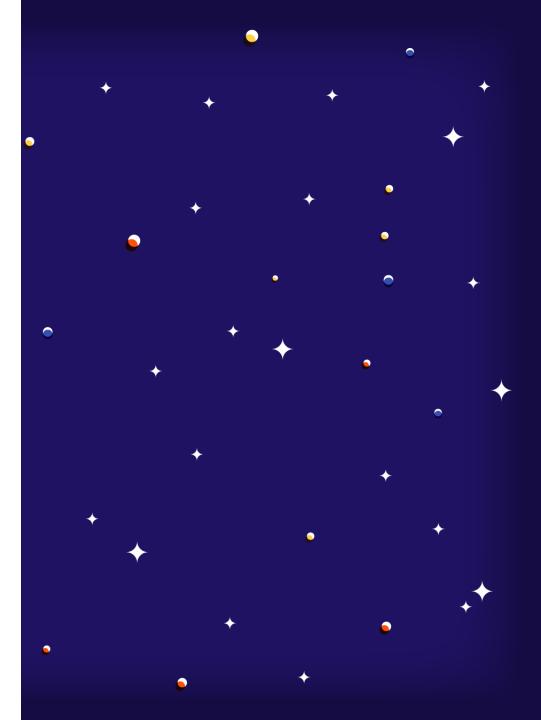
- Microsoft



Contents

My experiences working with Microsoft over five decades

- 80's Pre-historical era
- 90's Early years
- 00's Love and hate
- 10's Making a living
- 20's Partnering



80's: Pre-historical era



- Teenager
- Hobbyist programmer (Commodore 64 basic/assembler, C)

0









 \rightarrow



80's: Operating Systems

MS-DOS version 1.25 Copyright 1981,82 Microsoft, Inc.	MS-DOS version 4.00 Copyright 1981,82,83,84,85 Microsoft Corp.
Version 2.11 (C)Copyright Columbia Data Products, Inc	Internal revision 6.7, 85/11/26 Command v. 4.00 Copyright (C) 1981,1985 Microsoft Corp.
Current time is 0:00:06.15 Enter new time:	Current date is Fri 1-04-1980 Enter new date (mm-dd-yy): Current time is 0:00:25.04 Enter new time: A>_
Microsoft(R) MS-DOS(R) Version 3. (C)Copyright Microsof A>_	



90's: Early Years

0

l was

- Teenager & early 20s
- Father (1996 & 1998)
- Working as IT support (summers) & graphic designer
- Hobbyist programmer (C/C++)
- Tried to study a bit (with no luck)



Microsoft was

 A company making DOS (including MS-DOS Editor), Windows, and dev tools



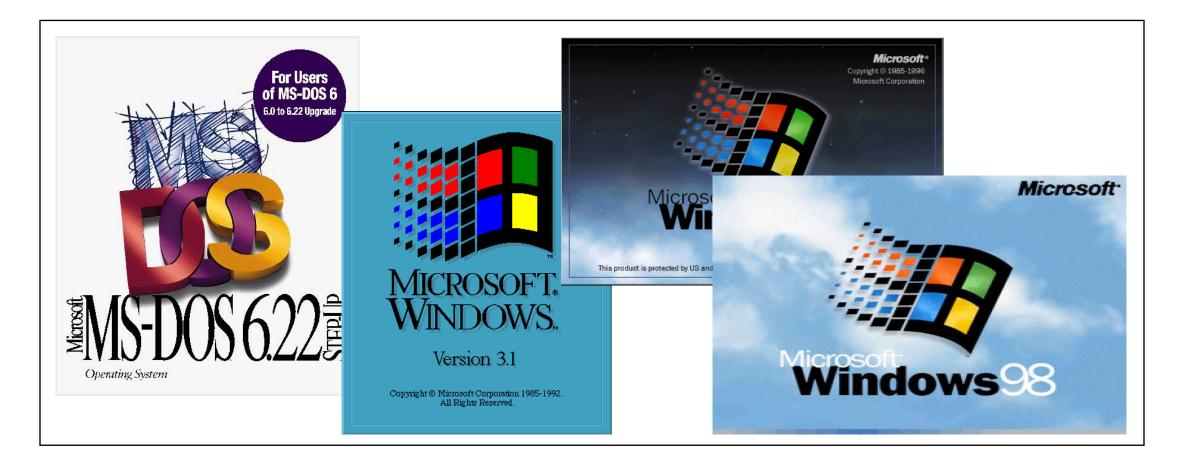








90's: Operating System



•

-

 \Rightarrow



90's: Dev tools

Source: <u>https://www.pcworld.com/article/917478/microsofts-biggest-software-release-came-in-a-box-two-feet-long.html</u>

BLUEHAT

2023

NEWS

Microsoft's 'biggest' software release came in a 40 lb, two foot long box

The C/C++ Compiler version 7.0 with Windows SDK weighed over forty pounds.



By Michael Crider Staff Writer, PCWorld | AUG 26, 2022 8:57 AM PDT









00's: Love and hate

0

l was

- Late 20s, early 30s
- Father (2000)
- Working as a developer (Lotus Notes/Domino, Java), CTO & CIO
- Started to study again (BBA 2007, MSc 2009), MCP 2001



Microsoft was

- Making my life miserable (SharePoint, Exchange, Windows, Active Directory (20)
- Business Partner (Dynamics CRM, HMC 4.0, BPOS)



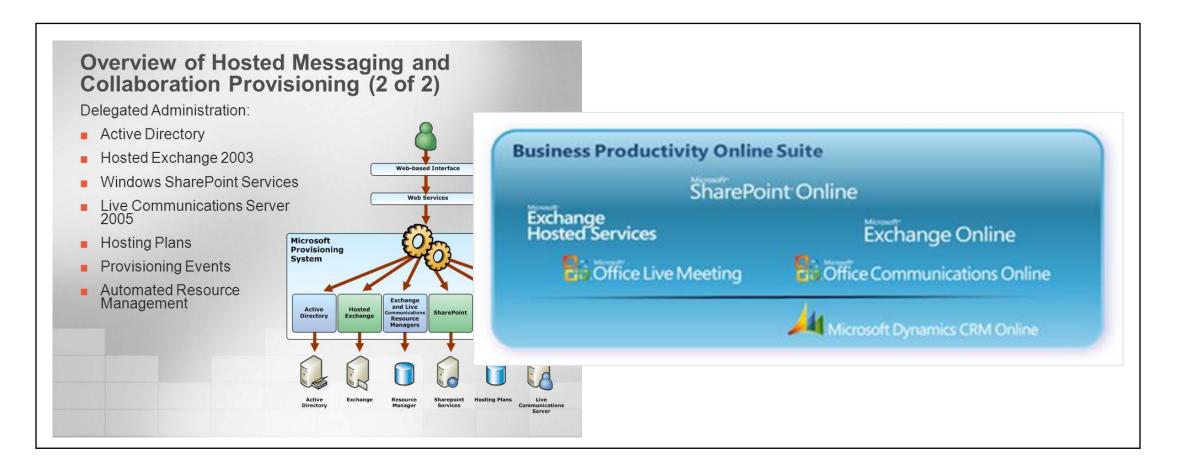


00's: Business productivity & OSs





00's: SaaS & Cloud!





10's: Making a Living

0



- Late 30s, early 40s
- Grandfather (2018, 2019)
- Working as CIO & IT trainer (Office 365 administration) & CIO
- Continued to study (PhD 2015), MCT since 2013
- First version of AADInternals 2018



Microsoft was

- Business partner (training)
- Supplier (Windows, Office 365, Azure)
- MSRC







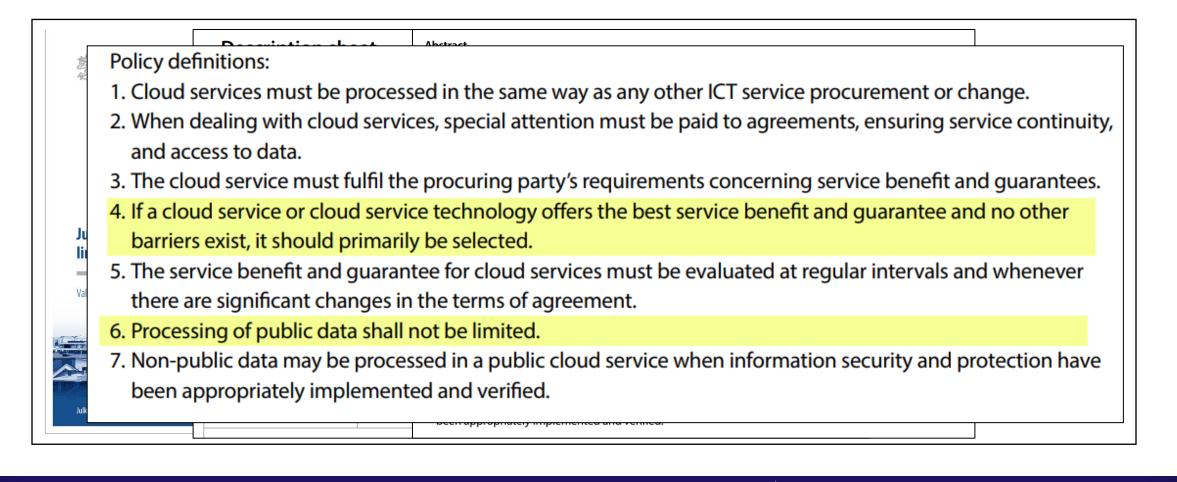


10's: Making a living





10's: Making a living





20's: Partnering

0

l was

- Mid 40s
- Working as Security Researcher
- MVP since 2020
- MVR since 2021



Microsoft

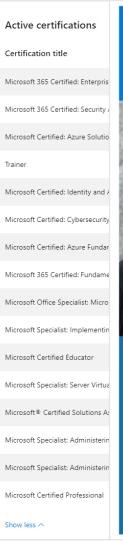
Microsoft was

• Business partner

 \rightarrow

• Pandora's box for security issues









Award Categories Security

First year awarded: 2020

Number of MVP Awards:

Nestori Syyni

Finland

Senior Principal Security Rese

Biography

Dr Nestori Syynimaa is one of the lea cloud services over a decade and ha Secureworks Counter Threat Unit. Be university lecturer for almost 20 year

Dr Syynimaa has been speaking in m DefCon, TROOPERS, and RSAC.

Creator of AADInternals toolkit https

MSRC 2021 Most Valuable **Security Researchers**

1. YUKI CHEN 🐵 卒 2. CAMERON VINCENT 👓 3. SURESH CHELLADURAI ∾ 4. DHANESH KIZHAKKINAN 🕀 🚥 5. DAVID DWORKEN 🐵 🚥 6. ZHINIANG PENG (@EDWARDZPENG)∞ 7. WTM 🐵 ∞ 🎯 8. CLAUDIO BOZZATO ∞ 8. LILITH 丶 (=_= ;) / 💱 💀 ∞ 10. TERRY ZHANG @PNIGOS 🚥 🎯 11. ANAS LAABAB ᅇ 12. STEVEN SEELEY (MR ME) ∞ 13. CALLUM CARNEY ∞ 14. RAMZES ∞ 15. ENDRI DOMI (KDOT) 🔁 ∞ 🎯 16. LÊ HỮU QUANG LINH ∞ 17. HAO LI 🚥 🎯 18. RYOTAK (@RYOTKAK) 💮 ∞ 19. QUAN JIN(@JQ0904) ∞ @ 20. YANG KANG(@DNPUSHME)∞ 21. FANGMING GU 🚥 22. XUEFENG LI ᅇ 23. LIUBENJIN 🐵 🚥 24. HUYNH PHUOC HUNG 🚥 🎯 24. PHILIPPE LAULHERET (@PHLAUL) 🕀 🚥 26. WAYNE LOW 🚥 27. REZERODAI 💮 ∞ 🎯 28. ORANGE TSAI ᅇ 29. LUO QUAN ∾ 🎯

 $\mathbf{+}$

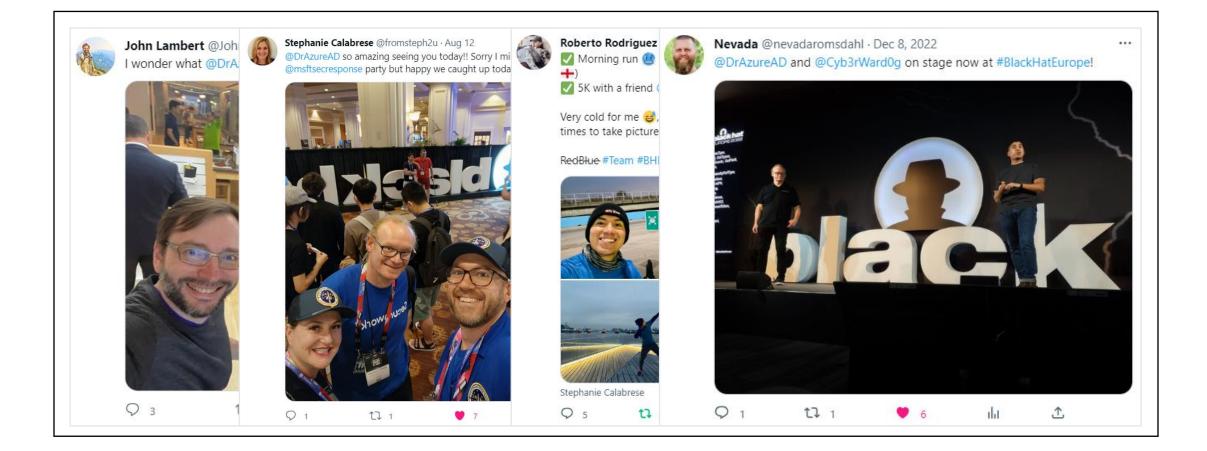
30. ADRIAN IVASCU ᅇ 30. ĐĂNG THẾ TUYẾN ∞ 30. MINGSHEN SUN • @ 33. ABDELHAMID NACERI 🔁 ∞ 34. FABIAN SCHMIDT 🐵 🎯 34. JEONGOH KYEA 🔁 🚥 36. PAUL LITVAK 🚥 🎯 36. WEI 🐵 🎯 38. BATRAM 🚥 39. IVAN FRATRIC 🚥 🎯 40. HECTOR PERALTA (P3RR0) ∞ @ 40. OSKARS VEĢERIS 🐵 42. ERIK EGSGARD(@HEXNOMAD)∞@ 43. LM0963 ᅇ 🎯 44. AAPO OKSMAN 🐵 🎯 44. HA ANH HOANG 🐵 44. PHAM VAN KHANH 👓 🎯 47. WENQUNWANG ∞ 🎯 48. HOSSEIN LOTFI 🔁 🚥 48. RON RESHEF 🚥 50. ANONYMOUS 🚥 50. BÙI QUANG HIẾU ∞ 🎯 50. MATT EVANS 🚥 🎯 53. ERFAN FAZELI 🗪 🎯 54. ADITYA GUJAR ᅇ 🎯 55. DAWID MOCZADŁO ∞ 56. JORDI SASTRE ∞ 🎯 57. WEN ZHIHUA ∾ 🎯

58. NESTORI SYYNIMAA 🚥

Microsoft



20's: Personal Connections









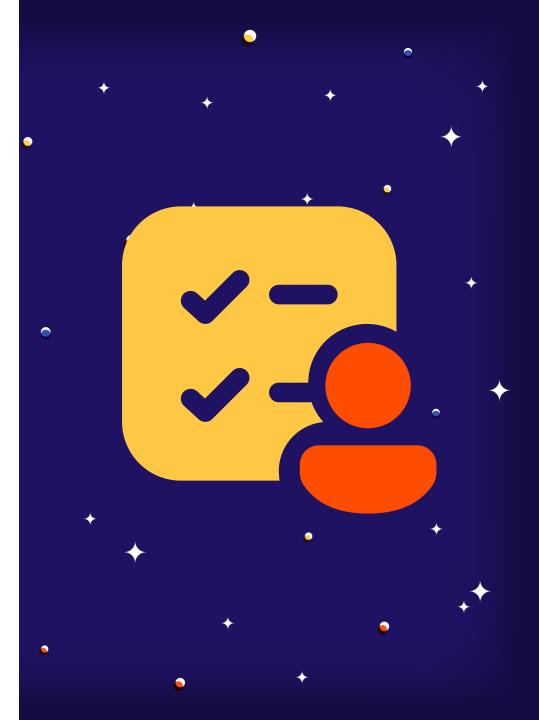




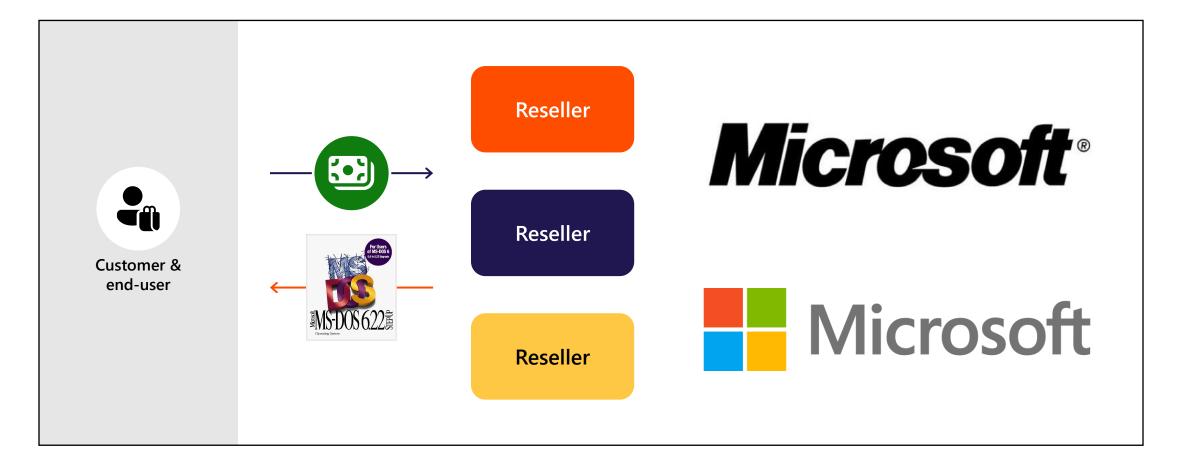
What do I do now?

Senior Principal Security Researcher @ Secureworks® CTU[™]

- Find security issues and attack vectors from Microsoft (cloud) products
- Create countermeasures
- Report to Microsoft
- Update AADInternals toolkit
- Publish findings

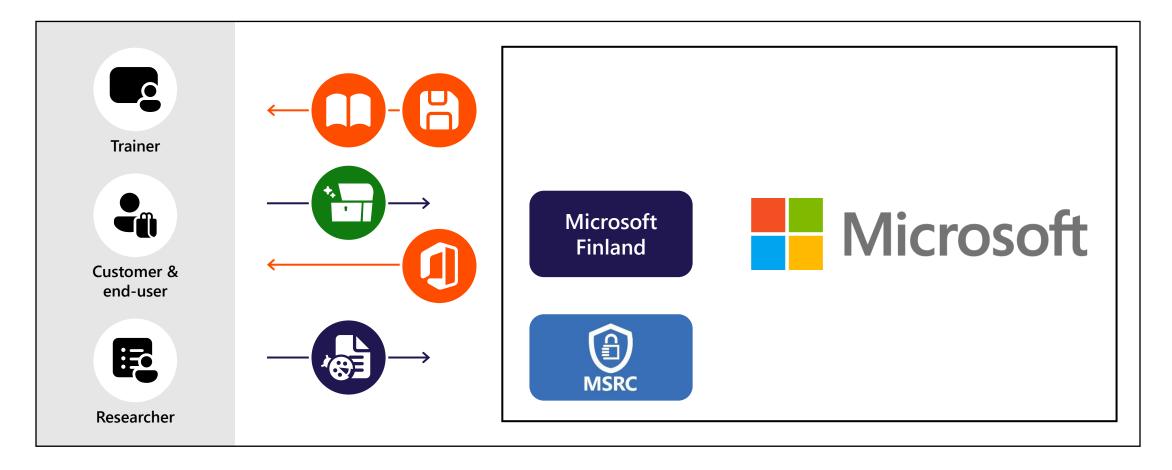


Working with Microsoft: 80's to 00's



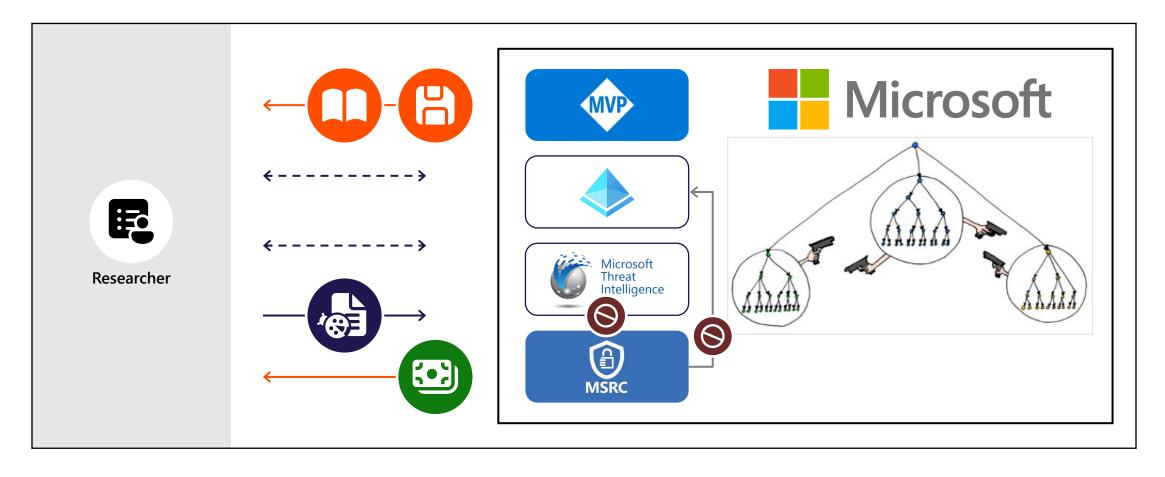


Working with Microsoft: 10's





Working with Microsoft: 20's





Jun 29 Reported to MSRC Jul 21 MSRC: By-design Sep 09 Shared draft to MSRC Sep 21 Leaked to public Sep 29 Published Sep 30 Updated

Source: <u>https://www.secureworks.com/research/undetected-azure-active-directory-brute-force-attacks</u>

THREAT ANALYSIS

Undetected Azure Active Directory Brute-Force Attacks

WEDNESDAY, SEPTEMBER 29, 2021 BY: COUNTER THREAT UNIT RESEARCH TEAM

Ƴ in f ⊠

Updated: September 30, 2021

Summary

In late June 2021, Secureworks® Counter Threat Unit[™] (CTU) researchers discovered a flaw in the protocol used by the Azure Active Directory Seamless Single Sign-On feature. This flaw allows threat actors to perform single-factor brute-force attacks against Azure Active Directory (Azure AD) without generating sign-in events in the targeted organization's tenant.

CTU[™] researchers reported the flaw to Microsoft on June 29. Microsoft confirmed the behavior on July 21 but ruled that it was "by design." As a result, it is unclear if or when the flaw will be fixed. In the meantime, organizations are vulnerable to stealthy brute-force attacks.

Microsoft



Sep 07 Reported to MSRC

Sep 22 MSRC: Fixed

Sep 23 Reported to MSRC

Dec 02 MSRC: Fixed

Dec 02 Responded, 2 issues not fixed

Jan 28 MSRC: Closed as fixed

Apr 05 Published

Apr 12 Updated

Source: <u>https://www.secureworks.com/research/azure-active-directory-exposes-internal-information</u>

THREAT ANALYSIS

Azure Active Directory Exposes Internal Information

TUESDAY, APRIL 5, 2022 BY: COUNTER THREAT UNIT RESEARCH TEAM

🎔 in f 💌

Updated: April 12, 2022

Summary

Microsoft Azure Active Directory (Azure AD) is an identity and access management solution used by over 88 percent of Fortune 500 companies as of this publication. This market penetration makes Azure AD a lucrative target for threat actors. In the second half of 2021, Secureworks® Counter Threat Unit[™] (CTU) researchers analyzed Azure AD tenants and were able to extract open-source intelligence (OSINT) about organizations. Threat actors frequently use OSINT to perform reconnaissance. CTU[™] researchers identified several application programming interfaces (APIs) that access internal information of any organization that uses Azure AD. Collected details included licensing information, mailbox information, and directory synchronization status.

CTU researchers shared their findings with Microsoft, and all but two of the issues have been mitigated as of this publication. Microsoft applied the updates automatically to all Azure AD tenants, so there are no actions required for Azure AD administrators. Microsoft classified the unmitigated issues as "by-design." The first issue allows anyone to query the directory synchronization status. In some scenarios, Azure AD reveals the name of the high-privileged account used for synchronization. The second issue could reveal internal information about the target Azure AD tenant, including the technical contact's full name and phone number. The technical contact usually holds Azure AD Global Administrator privileges.

Microsoft

Update: Microsoft addressed the remaining issues in April 2022.

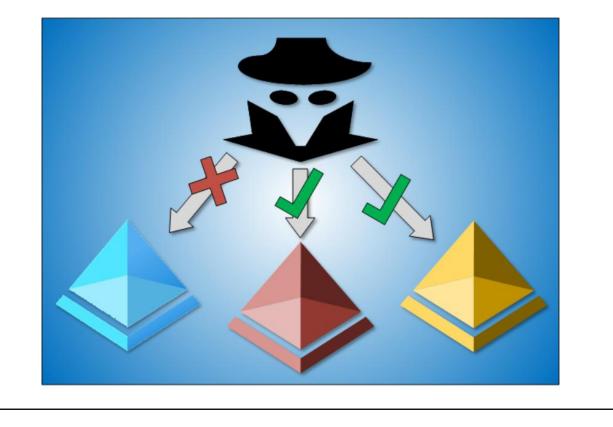


Jul 18 Reported to MSRC Mar 11 MSRC: By-design (1/2) Aug 22 MSRC: By-design (2/2) Nov 08 Published

Bypassing Azure AD home tenant MFA and CA

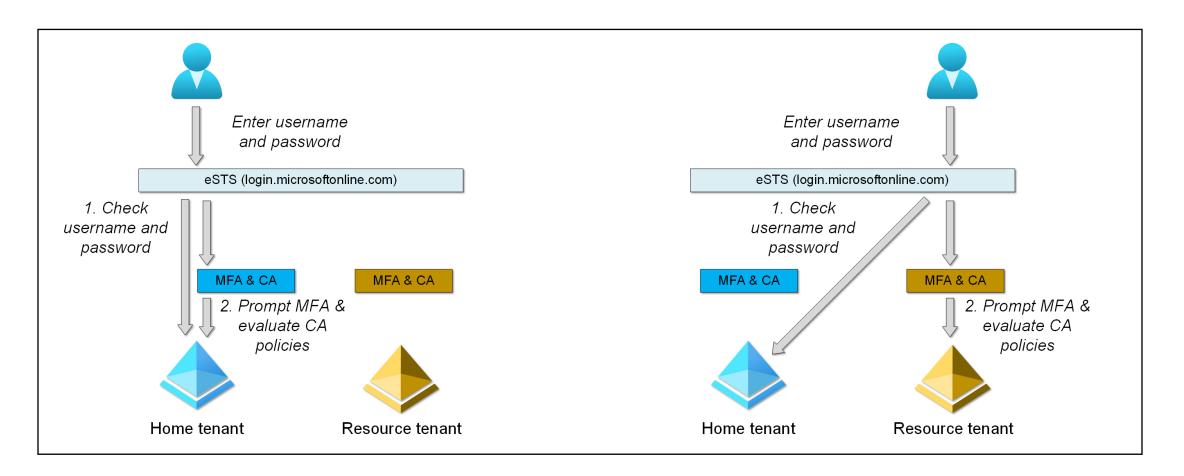
🕓 November 08, 2022 (Last Modified: November 13, 2022) 🖿 blog





Source: https://aadinternals.com/post/ests/







PS C:\> Import-Module AADInternals Loading module..

v0.8.1 by @DrAzureAD (Nestori Syynimaa)

PS C:\>I

Script 🕥

	ning can be bypassed when miscofigured. There are configured in a config	2mo ••• guration	>	M ht	2mo (edited) icrosoft Cybersecurity lisconfigured. We have this functionality: ttps://learn.microsoft.com/en-us/azure/active-directory/external- lentities/authentication-conditional-access
Like ·	 Reply · 2 Replies Like · 2 2 Reply 		"clickbait" removed ©		Authentication and Conditional Access for B2B users - Azure AD - Micro learn.microsoft.com Like · 🕑 1 Reply · 5 Replies
٤.	Dr. Nestori Syynimaa • You Senior Principal Security Researcher at Secureworks CTU (PhD, Which options are you referring to? Like · 🕑 1 Reply	2mo ••••			Dr. Nestori Syynimaa • You 2mo Senior Principal Security Researcher at Secureworks CTU (PhD, Can you elaborate what is misconfigured and where (home/resource tenant)? I mean, we already did mention cross tenant access settings in the blog. Like · 🕥 1 Reply







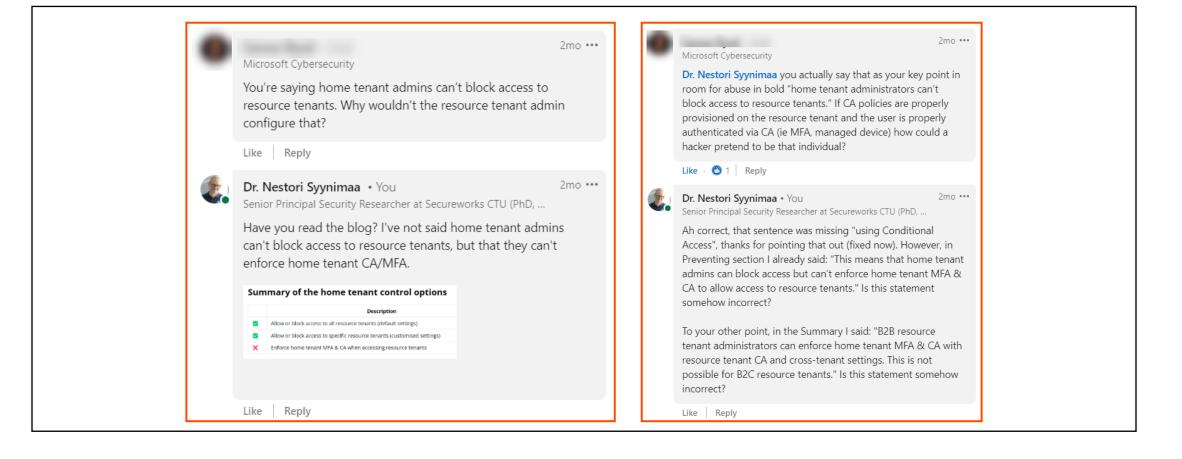
+



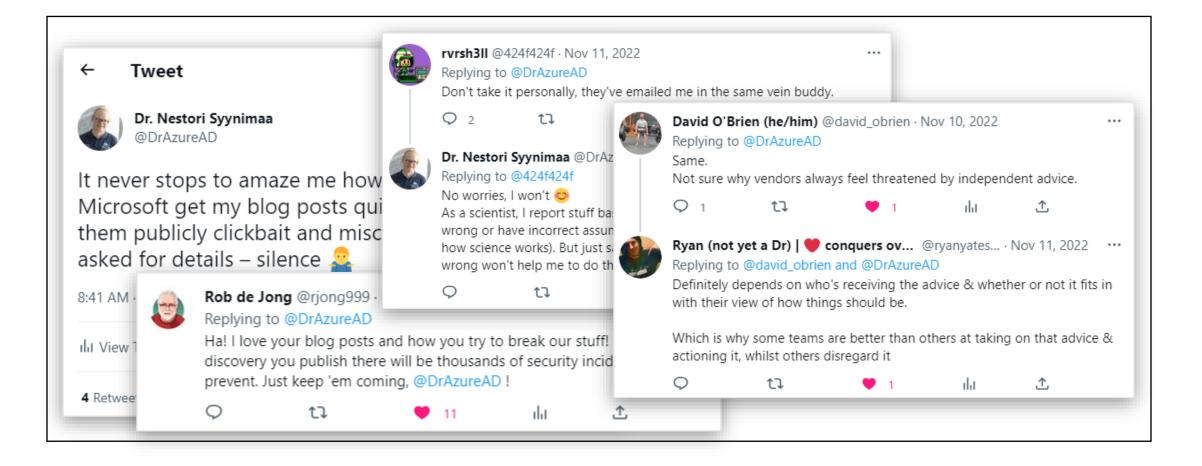
 \checkmark

BLUEHAT

2023









Microsoft



We (researchers) are the good guys – we want things to be fixed Researchers would really like to talk directly to engineering/PGs

(Most) people outside Microsoft sees Microsoft as one entity

When we provide draft blogs etc., it is okay to ask to postpone

MSRC is suffering from the "broken-telephone" If we say something that is wrong, just tell us how









How to follow me?

