Secureworks

Making the most of Microsoft cloud bug bounty programs: How I made \$65,000 USD in bounties in 2021

@DrAzureAD

https://linkedin.com/in/nestori





About the speaker



Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks CTU
- Creator of AADInternals toolkit
- MVP (Identity & Access), MVR

Contact details

- nsyynimaa@secureworks.com
- Twitter: <u>@DrAzureAD</u>
- https://linkedin.com/in/nestori
- https://o365blog.com









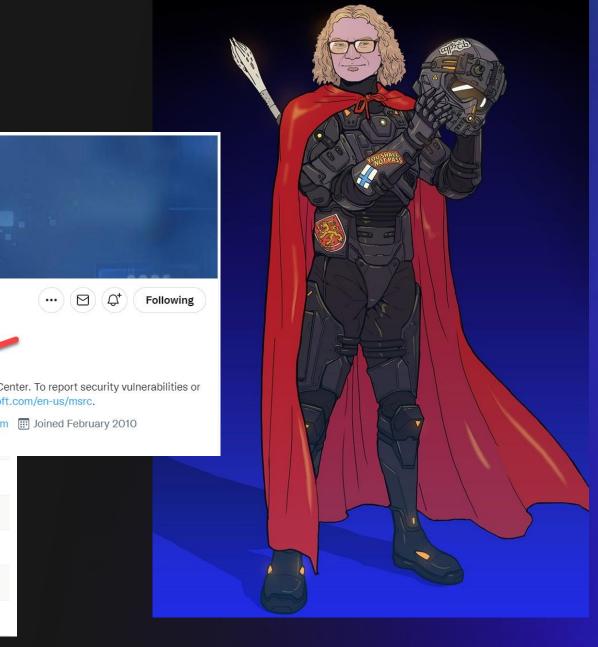






Working with MSRC

61	YUHAO WENG	
63	ADITI SINGH	
63	DYLAN RYAN-ZILAVY	
63	MIKHAIL MEDVEDEV (M3IK SHIZUKA)	MSRC 🖂 🗘
63	RONEN SHUSTIN (@RONENSHH)	Security Response 🔮
63	SHILONGAN	@msftsecresponse Follows you
68	PEACEMAKER	We are the Microsoft Security Response Center. To report security vulne abuse in Microsoft products, visit microsoft.com/en-us/msrc.
69	ANONYMOUS	
		75 Following 145.3K Followers
70	ANONYMOUS	165
70	AVISHAI REDELMAN	165
Me!	DR NESTORI SYYNIMAA (@DRAZUREAD)	165
70	HA VAN CUONG	165
70	YANIR TSARIMI (@YANIR_)	165



Contents

- Introduction
- Case 1: Spoofing and tampering with Azure AD sign-ins logs
- Case 2: Azure AD OSINT
- Case 3: From "by-design" to \$40k
- Bonus:
 - Access packages
 - Azure AD OSINT part 2

Spoofing and tampering with Azure AD sign-ins logs

- Write-up: https://o365blog.com/post/hybridhealthagent/
- Vulnerability walkthrough
 - ADFS Health Agent is providing sign-in activity from on-prem AD FS to Azure AD
 - Compromising AD FS server allowed overwriting existing signines events
- Bug bounty report \$10k bounty
- Takeaways:
 - The new features often have BL vulnerabilities

- Write-up: https://www.secureworks.com/research/azure-active-directory-exposes-internal-information
- Vulnerability walkthrough
 - Microsoft Support and Recovery Assistant (SaRA) is a tool to help users analyze and fix problems connecting MS cloud services
 - SaRA performs checks for the local computer, but also to cloud using API calls.
 - The API endpoints used by SaRA allowed extracting certain details of any user and any tenant.

- Bug bounty report on (legacy) endpoint A
 - \$5k bounty
 - Fixed by disabling cross-tenant access and endpoint A
 - Another (current) endpoint B was still working and provided same information

- Bug bounty report on endpoint B
 - \$5k bounty
 - Fixed by disabling cross-tenant access.
 - Regular users were still access information of their home tenant they had no privileges
- Bug bounty report on elevation of privilege
 - \$5k bounty
 - Fixed

- Takeaways
 - Submit similar findings in new reports AFTER the fix has been provided
 - If you got bounty for the first finding, they "must" give you one for the second one too
 - Look for different categories, fixing "information disclosure" may still leave "privilege escalation"..

From "by-design" to \$40k

- No write-up published yet.
- Vulnerability walkthrough
 - Azure AD Connect server synchronizes objects from on-prem AD to Azure AD using synchronization API
 - Synhronization API allows CRUDing also cloud-only (not synced from on-prem) users and reset their passwords
 - Compromising Azure AD Connect server allowed account takeovers for Global Administrators and enabled extortion/ransom by deletion (and restoration) of all administrators

From "by-design" to \$40k

- Bug bounty report
 - Categorized as "by-design"
 - Multiple replies and contacts
 - Finally \$20k bounty
 - Fix provided over 500 days after the initial report
 - The fix was introducing a new setting only Global Administrators could change
 - Azure AD Connect server allowed changing this setting
 - MS said they were "re-opening" the case

From "by-design" to \$40k

- Submitted a new report on bypassing fix
 - \$20k bounty
 - Fixed
- Takeaways
 - Study the provided fix carefully
 - Look for things that exists independently: The flaw on changing settings had been there for years.
 - Don't accept "re-opening" old cases but always file a new one!
 MS product groups are different organization than MSRC;)

Azure Access Packages

- Found by Sravan Akkaram. No write-up published yet.
- Vulnerability walkthrough
 - Azure Access Packages can be used to provide access to internal and external users
 - Backend API allowed external users to view packages and their metadata, including their creators
- Bug bounty report
 - Categorized as moderate severity information disclosure no bounty

Azure Access Packages

- Challenging the severity
 - According to documentation, user names are either Global Administrators or User Administrators – looks severe to me
 - Result: Severity raised to Important and \$7500 bounty!
- Takeaways
 - Argue using the documentation
 - Reporting moderate or low vulnerabilities still give you points!

Azure AD OSINT part 2

- Write-up: https://www.secureworks.com/research/azure-active-directory-exposes-internal-information
- Vulnerability walkthrough
 - A partner API allowed querying organization information of any tenant, including the full name and phone number of tenant creator (usually Global Administrator)
- Bug bounty report
 - Categorized as by-design

Azure AD OSINT part 2

- Disclosure
 - Threat analysis report with technical details
 - Microsoft fixed the issues withing a week
 - Report re-assessed as important information disclosure and resulted in \$2000 bounty, as the report quality was medium
 - Asked reason for the medium quality
 - After two months, an extra \$3000 bounty (not paid yet though)

Azure AD OSINT part 2

- Takeaways
 - If you feel the assessment is not correct, ask for reasons.

Secureworks