nic Cloud Connect

Oslo Spektrum
November 7 - 9

nic Cloud Connect

MVP

Cybersecurity Top Gun! Bullet proof your Hybrid Cloud!

Andy Malone MVP

Visit my YouTube Channel @AndyMaloneMVP

This Session we'll Discuss …

- State of the Cyber-Nation
- Do we go Hybrid or Cloud Native
- Pro's & Con's of the Hybrid Cloud
- Attack examples
- Defence Strategies
- Demos

State of the Cyber-Nation

- Increased Attack focus on Hybrid Weaknesses
- Successful identity attacks
  - Traditional brute-force attempts,
  - Sophisticated password spray attempts across multiple countries and IP addresses
  - Adversary-in-the middle (AiTM) attacks
- Ransomware encounters
- Targeted phishing attempts leading to device or user compromise
- Business email compromise

Common Cyber Attack Types

nic Cloud Connect

Hybrid Cloud Explained

The Hybrid Cloud – All Things to All Men!

Hybrid Attack examples

Traditional Phishing attack flow

Phishing Attack Path

Source: Widespread credential phishing campaign abuses open redirector links | Microsoft Security

Aadversary in the Middle AiTM: Example Attack Flow

Source: Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog

Windows Server DCSync attack

DCSync Anatomy of an Attack

- Compromise a standard or non-privileged user account with “Replicate Directory Changes” permission.
- Discover a DC in the specified domain name.
- Request the DC to replicate sensitive information such as password hashes using the Microsoft Directory Replication Service Remote (MS-DRSR) protocol.
- Obtain NTLM hashes of potentially useful accounts such as KRBTGT and Administrators.
- Create a Golden Ticket and run Pass the Ticket (PTT) attacks to move laterally.

```
mimikatz # lsadump::dcsync /user:attivo1\krbtgt
[DC] 'attivo1.local' will be the domain
[DC] 'rootpc1.attivo1.local' will be the DC server
[DC] 'attivo1\krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change :
Object Security ID   : S-1-5-21-2087032555-2209862856-1647013465-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 38fb5559b8b79e3657cbf45f7165a0c5
    ntlm- 0: 38fb5559b8b79e3657cbf45f7165a0c5
    ntlm- 1: 6afddb1920f4620702d740622d2ea546
    lm  - 0: db29e44c94432ce7af734efd4a450208
    lm  - 1: 184390aabe7bf26404542369d6a01afc

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : ATTIVO1.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
```

Tools used for AiTM Attacks

evilginx.

caffeine

Ref Valid for: Office365, google, AWS, facebook, twitter, Instagram and any other app using modern authentication/session cookies

Anatomy of an Attack

1 – RDP Attack

2 – Responder steals NTLM Hash

3 – Mimikatz Extracts Domain Domain Admin Accs

4 – Kerbroast to Elevate Privileges

Microsoft Confidential

Don’t Lose Control!

Zero Trust – It's the Only Way!

Zero Trust Principles

Verify explicitly

Always validate all available data points including

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

MITRE ATT&CK Framework

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

https://attack.mitre.org/

Defend Across attack chains – MCRA

Reduce the Attack Surface of Active Directory

ADDS - To Write Back or Not to Write Back!

Verify user identities with multifactor authentication (MFA)

Microsoft support a **broad range of multifactor authentication options**

Passwordless, phishing-resistant technology

- Microsoft Authenticator*
- Windows Hello (supports passkey)
- FIDO2 Security key
- Biometrics
- Certificate based Auth

- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multifactor authentication prevents 99.9% of identity-based attacks

*Must use with Conditional Access policy requiring managed devices to get protection from external phishing threats.

Enforce real-time Conditional Access policies

- Enforce access controls with adaptive policies
- Protect data inside applications
- Restrict access for vulnerable and compromised devices

Continuous access evaluation

Auto-revoke access in near-real time when critical events or policy violations are detected

- Account revocation
- Account disablement/deletion
- Password change
- User location change
- User risk increase

Demo

New Entra ID Hybrid Security Enhancements

Enhance hybrid with Defender for Identity

Microsoft Defender for Identity explained

DCSync attack Thwarted by Defender for Identity

Incidents > Suspected DCSync attack (replication of directory services) on multiple endpoints

Suspected DCSync attack (replication ...

Manage incident | Ask Defender Experts | Comments and history

Suspected DCSync attack (replication of directory services) on multiple endpoints

Attack story | Alerts (2) | Assets (3) | Investigations (0) | Evidence and Response (0) | Summary

Alerts

2/2 Active alerts | Unpin all | Show all

Sep 11, 2023 6:52 PM • New
Suspected DCSync attack (replication of directory services)
StagingServer.knausrig.com
MSOL_0ac0679d178f

Sep 11, 2023 7:27 PM • New
Suspected DCSync attack (replication of directory services)
stagingserver.internal.cloudapp.net
MSOL_0ac0679d178f

Suspected DCSync attack (replication of directory services)

Clear selection

Incident graph | Layout | Group similar nodes

— Communication ····· Association

What happened

MSOL_0ac0679d178f on StagingServer sent 36 replication requests to DC01.

Alert graph

Important information

Demo

Defender for Identity

Home - Microsoft 365 security

https://security.microsoft.com/homepage?tid=1a9c10ee-fdb3-4a94-bf5b-9376ad6c32f5

M365 | Advanced hunting | Incident | Secure Score | O365 ATP | Azure AD | AAD IP | NickC | Admin | DC1 | MDI M365 Settings | RBAC | Intune | M365 Admin | Message center | Azure | MDA | MDI

Microsoft 365 Defender

Search

- Home
- Incidents & alerts
- Hunting
  - Advanced hunting
  - Custom detection rules
- Actions & submissions
- Threat intelligence
- Secure score
- Learning hub
- Trials
- Partner catalog
- Assets
  - Devices
  - Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Email & collaboration

Home

Guided tour | What's new ? | Community | Add cards

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Azure Active Directory Identity Protection.

Deployment

MDI Sensors deployment 5 / 6

MDI health alerts

Low | Medium | High | 1 more

License

Defender for Identity
Available

Azure AD Identity Protection
Available

Quick guides

What is Microsoft Defender for Identity?

Zero Trust with Microsoft 365 Defender

Quick installation guide

Insider Risk Management

Did you know businesses are spending $500,000 per breach?

Source: Communication Compliance Microsoft Market Research, May 2021

Start identifying insider risks within your organization with Microsoft Purview Insider Risk Management today.

Get started

Microsoft Secure Score

Secure Score: 40.66%

517.62/1273 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 08/12

100% / 50% / 0%

06/15 06/22 06/29 07/06 07/13 07/20 07/27 08/03 08/10 08/17 08/24 08/31 09/07

Identity	36.41%
Data	55.56%
Device	41.59%
Apps	39.79%

Improve your score | View history

Attack simulation training

Did you know ?

- Phishing is a number one security threat
- Phishing simulation is mandated as part of regulations
- Phishing simulation can reduce phishing attacks by 40%

100% users have not experienced the simulation

Simulated users

Simulated Users | Non-Simulated Users

Go to Attack simulation training

Learn more about Attack simulation training

How Microsoft 365 Defender takes XDR-automated actions to stop AiTM phishing

- XDR – Extended Detection & Response

Detection

XDR correlated alerts:

- Unfamiliar sign-in
- Network connections from Defender for Endpoint managed device
- Microsoft Defender for Office 365 URL click information
- Threat intelligence signals

Classification

Identifies the attack type and compromised assets:

- AiTM phishing
- Compromised user and mailbox
- Fraud attempt

Disruption

Automatic response is triggered:

Disables compromised user account in Active Directory and Entra ID.

The stolen session cookie will be automatically revoked, preventing the attacker from using it for additional malicious activity.

Enhanced protection and SOC efficiency

Limits a threat actor's progress early on.

SOC team in full control to investigate all actions automatically taken by Microsoft 365 Defender and where needed, heal any remaining, affected assets.

Microsoft 365 Defender

Search

Incidents > User compromised in AiTM phishing attack

User compromised in AiTM phishing attack

Manage incident | Consult a threat expert | ...

Important! A potentially compromised account was automatically disabled by Microsoft 365 Defender's Attack Disruption. See the 'Assets' tab or go to the Action Center for more information.

Alert story | Recommeded actions (20) | Alerts (4) | Assets (2) | Investigations (4) | Evidence & Response (11) | Summary

Alerts

11/11 Active alerts | Unpin all | Show all

Nov 18, 2021 7:56:52 AM | New
Suspicious mailbox manipulation rule
Jonathan Wolcott

Nov 24, 2021 2:12:45 PM | New
Impossible travel activity
Jonathan Wolcott

Nov 24, 2021 2:18:31 PM | New
User compromised in AiTM phishing attack
cont-jonathan | Jonathan Wolcott

Nov 24, 2021 2:18:30 PM | New
Unfamiliar sign in properties
Jonathan Wolcott

Incident graph

Layout | Group similar nodes

User compromised in AiTM phishing...

What Happened

A user's credential were intercepted by a known reverse-proxy adversary-in-the-middle (AiTM) phishing site. Reverse-proxy phishing allows an attacker to intercept a user's input to a legitimate site... read more

18.11 2021 7:57:40 AM	[7200] msedge.exe
7:57:40 AM	[7200] msedge.exe -- flag-switch-begin...
7:57:40 AM	[7200] msedge.exe -- no-startup-window...
7:57:40 AM	[7200] msedge.exe -- no-startup-window...
7:57:40 AM	[7200] msedge.exe -- type=utility-...
7:57:40 AM	Network connect outbound connection from 122.233.132:60802 to 12.34.11.32:443
	User compromised in AiTM phishing atta ... High In progress Prevented

Back to incident details

User compromised in AiTM phishing

High | Detected | In progress

AiTM ATTACK | ATTACK DISRUPTION

Open alert page | Manage alert | ...

Details | Recommendations

Alert state

Classification: Not set
Assigned to: Unassigned

Alert details

Evidence

Entity Name	Verdict
login.office...	Suspicious
12.34.11.32:..	Suspicious
Voicemail f...	Suspicious

AiTM phishing campaign – Dead in the Water!

Automation disables the compromised account and invalidates the token.

Microsoft 365 Defender alert: "Suspicious network connection to AiTM phishing site"

Attacker

Date	Event
2022-10-07 1:05PM	User receives phishing email with .html attachment
2022-10-07 1:12PM	User opens the attachment. User's device connects to the IP address 1.2.3.4
2022-10-07 1:13PM	Successful sign-in with MFA from IP address 1.2.3.4
2022-10-07 3:30PM	Sign-in with the stolen cookie from IP address 4.3.2.1
2022-10-07 3:30PM- 4:30PM	Mailbox recon
2022-10-07 4:35PM	Creation of inbox rule that moves email with specific subject to "Conversation History" folder and marks them as read
2022-10-07 4:36-4:37 PM	Email sent to accounts payable team asking for immediate payment of outstanding Deletion of sent email from Sent Items
2022-10-07 4:55 PM	Accounts payable team asks for some clarification
2022-10-07 5:15 PM	Attacker sends the reply to Accounts payable
2022-10-07 6:30 PM	SOC resets victim's password

nic Cloud Connect

Demo

Thwarting an AiTM Attack with Defender for Endpoint & Microsoft Sentinel

Camtasia 2022 File Edit Modify Text View Export Window Help Sat 28 Oct 12:07

Home - Microsoft Azure

portal.azure.com/#home

Microsoft Demos | Home | Logical Op... | Sign in - go deploy | Search and Brows... | Drag and drop |... | Viddeyoze | Home - Canva | American Express... | Which? Signup | Marks Stuff | MCT Central

Microsoft Azure | Search resources, services, and docs (G+/) | PDemo@seccxpninja.on... ALPINE SKI HOUSE

- Create a resource
- Home
- Dashboard
- All services

FAVORITES

- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Microsoft Entra ID
- Monitor

https://portal.azure.com/#create/hub

Azure services

Create a resource | Virtual machines | Microsoft Sentinel | Function App | App Services | Language | SQL databases

Azure Cosmos DB | Advisor | More services

Resources

Recent | Favorite

Name	Type	Last Viewed
MB-DC1	Virtual machine	a few seconds ago
SentinelLogIngest	Function App	19 hours ago
DemoOrchestrator	SQL database	19 hours ago
mimic	Virtual machine	19 hours ago
M365D Sub	Subscription	20 hours ago

nic Cloud Connect

Protecting Hybrid Data

Hybrid Data Protection

Air Gapping – The Risks

Air-gapped systems typically fall into two categories:

1. Critical systems that are disconnected from the rest of the network for security purposes
2. Systems that are kept offline due to cost or connectivity issues.

Hybrid Data Protection Best Practice

Tips for Hybrid Data Protection

- Understand Vendor Responsibilities
- Understand Your responsibilities
- Develop an Air Gapped Back Up Solution to defend Against Ransomware Attack
- Deploy Cryptographic Protections
- Employ Safe Deletion Techniques
- Ensure Adequate Admin Controls
- Pinpoint Any Security Gaps
- Ensure compliance Controls are in Place

MAVERICK

nic Cloud Connect

Oslo Spektrum
November 7 - 9