Technologic Papers

Subdomain Takeover ב-Azure

כשה-DNS נשאר מאחור

מאת שירה זיו

הקדמה

בשנים האחרונות יותר ויותר ארגונים נתקלים בתופעה שנקראת Dangling Subdomain. מה בעצם קורה כשמוחקים שירות בענן אבל שוכחים לעדכן את רשומות ה-DNS? מבחינת ה-DNS שום דבר חריג. הוא ממשיך לעשות את מה שהוגדר לו: להפנות תעבורה ליעד מסוים. אז איפה מתחילה הבעיה? כשהיעד הזה כבר לא קיים.

בסביבות Azure זה קורה לא מעט. שירותים עולים ויורדים, סביבות בדיקה נמחקות וארכיטקטורות משתנות. אבל רשומות DNS נוטות להישאר. לפעמים חודשים. לפעמים שנים. לפעמים זה בדיוק מה שצריך כדי להפוך טעות תפעולית קטנה ל-Subdomain Takeover.

במאמר הזה נסתכל על התופעה הזו מזווית פרקטית: איך נוצרים Dangling Subdomains ב-Azure, למה זה נפוץ דווקא שם, איך מבינים מתי זה באמת מסוכן, מה תוקף יכול לעשות עם זה, ומה אפשר לעשות כדי לצמצם משמעותית את הסיכון בארגון. למרות שהתופעה רחבה יותר, הדוגמאות והניתוח במאמר זה מתמקדים ב-Azure.

אז איך נוצרים Dangling Subdomains ב-Azure?

Dangling Subdomain נוצר כשיש רשומת DNS (לרוב CNAME) שמפנה למשאב שכבר לא קיים. אין כאן חולשה מתוחכמת או באג מתוחכם בקוד. זו פשוט תצורה שנשארה בלי בעלים כי לא טופלה כמו שצריך.

ב-Azure, מחיקת משאב מתבצעת ברמת המשאב עצמו. אבל ברוב הארגונים ה-DNS מנוהל בכלל במקום אחר. לפעמים על ידי צוות תשתיות, לפעמים אצל ספק חיצוני, לפעמים ב-Azure DNS נפרד או במערכת On-prem שלא מחוברת לתהליכי העבודה בענן. כשהמשאב נמחק, אף אחד לא מבטיח שמישהו יזכור גם להסיר את רשומת ה-DNS. וכך נשאר סאב-דומיין שממשיך להפנות ליעד שלא קיים יותר.

אז מה זה בעצם Subdomain Takeover?

Subdomain Takeover קורה כשמישהו אחר תופס שם של משאב שהתפנה בזמן שה-DNS הארגוני עדיין מפנה אליו.

ב-Azure יש לא מעט שירותים שבהם שם המשאב הוא חלק מה-FQDN הציבורי. כל עוד המשאב קיים, אז השם שמור. ברגע שהוא נמחק, במקרים רבים השם מפסיק להיות שמור לארגון. לפעמים הוא זמין מחדש כמעט מיד, לפעמים אחרי פרק זמן קצר.

אם באותו זמן קיימת רשומת CNAME מסאב דומיין ארגוני לשם הזה, תוקף יכול לנצל את זה וליצור משאב חדש ב-Azure עם אותו שם בדיוק. מרגע זה, כל התעבורה שמגיעה לסאב הדומיין הארגוני תנותב למשאב שנמצא בשליטתו, כלומר תחת דומיין שנראה לגמרי לגיטימי.

חשוב להדגיש: לא כל Dangling Subdomain מאפשר Takeover בפועל. כדי שזה יקרה צריכים להתקיים שלושה תנאים:

- יש CNAME פעיל שמצביע לשירות Azure
- המשאב המקורי כבר לא קיים בצד Azure
- השירות מאפשר שימוש מחדש בשם ואינו שומר אותו ללקוח המקורי

איזה שירותים ב-Azure באמת רלוונטיים ל-Takeover?

לא כל שירות ב-Azure רלוונטי ל-Subdomain Takeover. ברוב המקרים מדובר בשירותים שבהם שם המשאב הוא חלק מהכתובת הציבורית, והשם יכול להפוך לזמין מחדש אחרי מחיקה.

השירותים הנפוצים כוללים:

- Azure App Service - *.azurewebsites.net
- Azure Blob Storage - *.blob.core.windows.net
- Azure Traffic Manager - *.trafficmanager.net
- Azure CDN - *.azureedge.net
- Azure Cloud Services ו-VMs - *.cloudapp.azure.com

יש שירותים ששומרים שמות לפרק זמן מסוים, ויש כאלה שלא מאפשרים בכלל שימוש חוזר. אז אם הצלחנו לזהות Dangling Subdomain זה לא מספיק... זאת לא הוכחה שבאמת אפשר לבצע את ה-Takeover.

איך מזהים ומאמתים Dangling Subdomain?

השלב הראשון הוא מיפוי. אוספים סאב-דומיינים שמוגדרים כ-CNAME לשירותי Azure, למשל blob.core.windows.net, azurewebsites.net, cloudapp.azure.com או trafficmanager.net.

בשלב הבא בודקים אם יש בכלל משאב פעיל מאחורי היעד. לפעמים נקבל NXDOMAIN, ובמקרים אחרים תגובת שגיאה אופיינית של Azure, כמו "Resource not found". בשני המקרים זו תהיה אינדיקציה לזה שה-DNS מפנה למשהו שכבר לא קיים.

השלב הבא יהיה לאמת האם Azure עדיין מאפשרת ליצור משאב חדש עם אותו שם שמופיע ב-CNAME. אם כן, אז מדובר ב-Dangling Subdomain עם פוטנציאל ל-Takeover. דוגמה מלאה לזה מוצגת בהמשך המאמר.

ואם הצלחנו לעשות Takeover, מה עכשיו?

הרבה פעמים קורה שסקריפטים, משתמשים ותהליכי CI/CD בארגון עדיין מתקשרים עם הסאב דומיין שעשו עליו Takeover.

אחרי Takeover, תוקף יכול למשל:

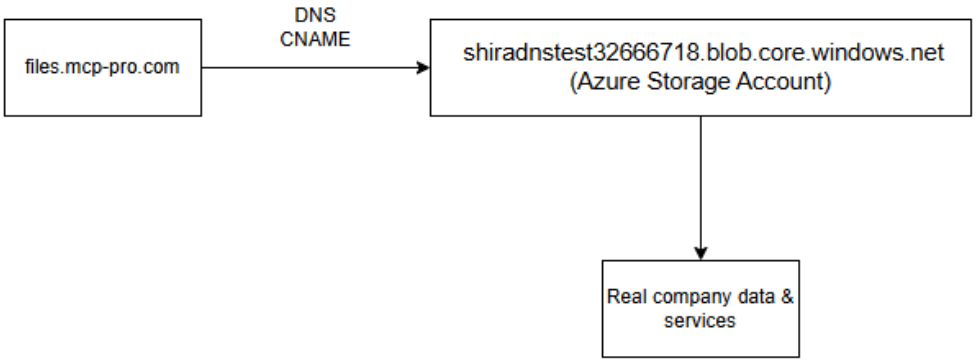
- להעלות קבצים זדוניים לסאב דומיין לגיטימי.
- לבצע קמפיין פישינג או Social Engineering דרך פורטלים ישנים.
- להשתלט על API או endpoint שמערכות עדיין קוראות אליו.
- לנצל Redirect URIs ישנים ב-OAuth או OIDC.

בהרבה ארגונים יש סקריפטים, Agents ותהליכי CI/CD שרצים כבר שנים וממשיכים לדבר עם אותו סאב-דומיין "ישן". בכל בקשה כזו הם עלולים להעביר מידע רגיש, למשל:

- SAS-tokens שמופיעים ב-query string כדי לגשת ל-Blob או לקבצים.
- Bearer token, API-Key
- Payload-ים שיכולים להכיל מידע רגיש.

דמו: השתלטות על Blob Storage

נניח שהארגון שלך משתמש ב-Azure Blob Storage שמאוחסנות בו תוכנות, קבצי קונפיגורציה או artifacts של CI/CD. ונניח שסקריפטים, משתמשים ו-Agents בארגון מורידים אותם באופן שוטף. לצורך זה הוגדר סאב-דומיין ייעודי בשם files.mcp-pro.com:



כעת, דמיינו שמבצעים בחברה שלכם שדרוג תשתיות. עוברים ל-pipeline חדש או לשירות אחסון אחר ומוחקים את חשבון ה-Storage הישן מתוך מחשבה שהוא כבר לא בשימוש. אבל שוכחים להסיר את רשומת ה-CNAME ב-DNS zone של החברה.

תוקף שממפה את הדומיינים של הארגון יכול לראות שה-CNAME של files.mcp-pro.com מפנה ל-Storage Account שכבר לא קיים ב-Azure (לא מחזיר תוכן תקף):

```
$ dig files.mcp-pro.com

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> files.mcp-pro.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8700
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
  EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;files.mcp-pro.com.             IN      A

;; ANSWER SECTION:
files.mcp-pro.com.      3473    IN      CNAME   shiradnstest326606718.z13.web.core.windows.net.

;; Query time: 3 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sat Oct 18 21:13:54 IDT 2025
```

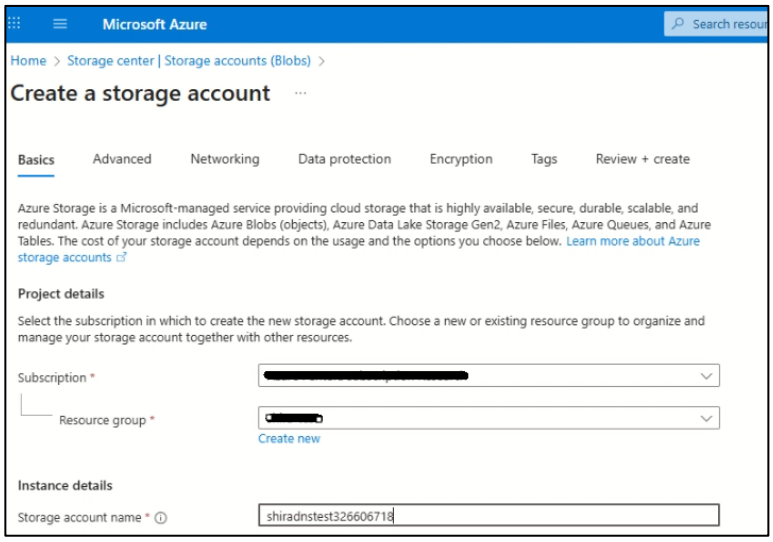
```
$ curl -I https://shiradnstest326606718.blob.core.windows.net
curl: (6) Could not resolve host: shiradnstest326606718.blob.core.windows.net
```

בשלב הזה ניתן להסיק שהסאב דומיין יכול להיות פגיע ל-Takeover.

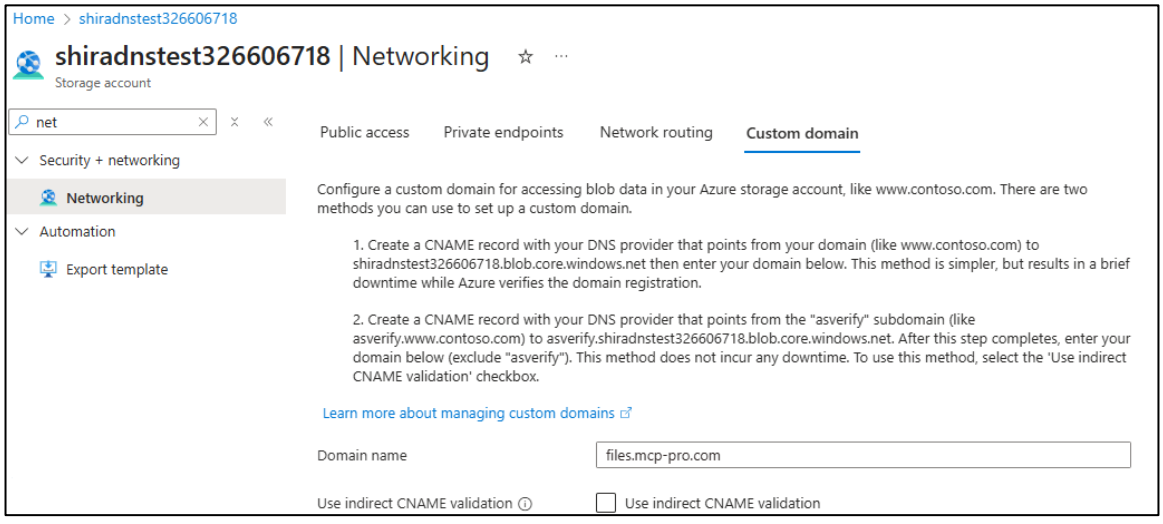
כדי לוודא זאת, נשתמש בכלים כמו Nuclei עם תבניות ייעודיות ל-Subdomains Dangling ב-Azure:

```
nuclei -t dns/azure-takeover-detection.yaml -u files.mcp-pro.com -vv

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.4.10

                projectdiscovery.io

[INF] Current nuclei version: v3.4.10 (latest)
[INF] Current nuclei-templates version: v10.3.0 (latest)
[INF] New templates added in latest release: 124
[INF] Templates loaded for current scan: 1
[INF] Executing 1 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[azure-takeover-detection] Microsoft Azure Takeover Detection (@pdteam) [high]
[azure-takeover-detection] [dns] [high] files.mcp-pro.com ["shiradnstest326606718.z13.web.core.windows.net"]
[INF] Scan completed in 116.951893ms. 1 matches found.
```

אם הסריקה מסמנת שהשם פנוי, התוקף יצור תחת ה-Subscription שלו Azure storage account חדש עם אותו השם תחת blob.core.windows.net:



כדי לסיים את תהליך ההשתלטות, התוקף צריך להגדיר תחת הבלוב את הסאב דומיין הפגיע (לשונית Custom domain):

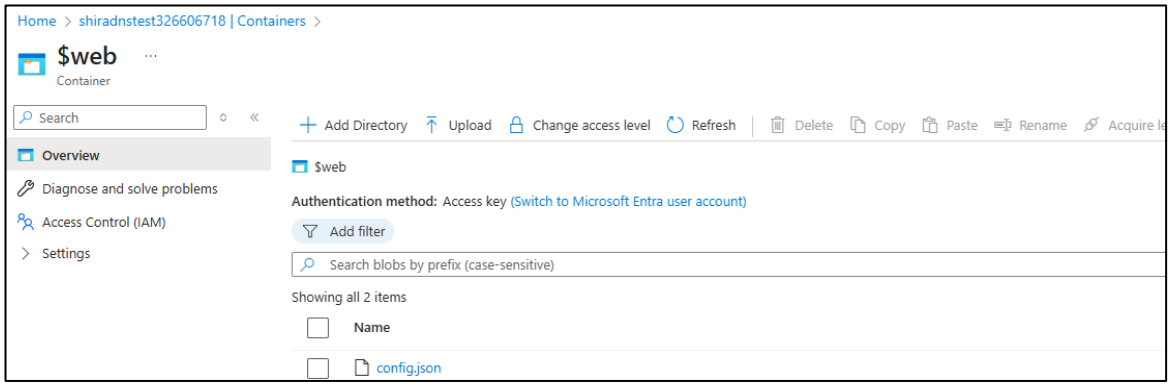


מרגע זה, כל בקשה ל-files.mcp-pro.com תנותב לחשבון שבשליטת התוקף.

מכאן האפשרויות פשוטות. התוקף יכול להעלות למשל קובץ config.json לדוגמא שנראה זהה למקורי. סקריפטים ותהליכי CI/CD ישנים ימשיכו להוריד אותו מ-files.mcp-pro.com, בלי לדעת שהקובץ מגיע מחשבון זדוני.

או שהתוקף פשוט יכול להקליט כל בקשה שמגיעה ל-files.mcp-pro.com ולנסות לחלץ ממנה טוקנים, מפתחות ו-payloads רגישים.

מבחינת המערכות, סקריפטים וכל תהליכי הדיפלוי, הם עדיין מתקשרים עם אותו הבלוב. בפועל, כל התעבורה נאספת על ידי התוקף.



איך מוצאים את זה בארגון?

למען האמת, אין כאן בדיקת קסם שהיא חד-פעמית. סביבות ענן משתנות כל הזמן, ולכן גם איתור Dangling Subdomains צריך להיות כחלק מפעילות שוטפת.

מומלץ שיהיה תהליך עבודה בסיסי בארגון שיכלול:

- מיפוי סאב-דומיינים חיצוניים, כולל כאלה שנראים ישנים או נשכחים.
- נקודה נוספת שקל לפספס היא ש-Dangling Subdomains לא מגיעים רק מה-DNS עצמו, אלא גם מקוד. סקריפטים, pipelines, קבצי קונפיגורציה ותיעוד ישן עלולים להכיל כתובות לשירותים שכבר נמחקו מזמן, אבל ממשיכים לחיות בריפוזיטוריז של הארגון. סריקה בסיסית של קוד לחילוץ FQDNs ובדיקה אם המשאבים שאליהם הם מפנים עדיין קיימים, יכולה לחשוף לא מעט מקרים כאלה, במיוחד בסביבות עם הרבה קוד.
- זיהוי רשומות CNAME שמפנות לשירותי Azure.
- בדיקת זמינות המשאבים בצד Azure.

כלים כמו **Nuclei** או **Subjack** יכולים לעזור בשלב האיתור הראשוני, אבל הם לא מחליפים הבנה של הסביבה בארגון.

אז איך מונעים זאת?

התשובה הפשוטה היא גם הנכונה: למחוק רשומות DNS כשמוחקים משאב.

בפועל זה עובד רק כשאותו גורם בארגון שולט גם בענן וגם ב-DNS וזה לא תמיד המצב. לכן חשוב לבנות תהליך בארגון:

- לשלב בדיקות DNS כחלק מתהליך הסרה וניקוי של משאבים.
- לוודא שמחיקה של משאב כוללת גם ניקוי אוטומטי של רשומות DNS רלוונטיות.
- להוסיף ולידציה שמוודאת שלא נשארו רשומות פעילות שמפנות למשאב שכבר נמחק.
- לוודא שלכל רשומת CNAME יש owner ברור ואחריות על הסרה.
- לבצע ביקורות DNS תקופתיות ולהצליב אותן מול משאבים שעדיין פעילים.

מיקרוסופט מתייחסת ל-Subdomain Takeover כבעיה מוכרת, וממליצה בין היתר על שימוש ב-Azure DNS alias records, רשומות asuid לאימות בעלות ב-App Service, והפעלת Microsoft Defender for App Service.

ועדיין, הפתרון הוא לא רק טכנולוגי. Azure לא יודעת מה קורה ב-DNS החיצוני שלכם, ולא שומרת שמות עבור משאבים שנמחקו. האחריות נשארת אצל הארגון.

סיכום

Subdomain Takeover ב-Azure הוא כמעט תמיד לא עניין של חולשה מתוחכמת, אלא של תהליך. משאב נמחק וה-DNS פשוט נשאר מאחור. כל עוד DNS ומשאבי ענן מנוהלים כשני עולמות נפרדים, Dangling Subdomains ימשיכו להופיע. החדשות הטובות הן שלא צריך פתרון מיוחד או מוצר יקר. רק מיפוי, תהליך ברור, וקצת מודעות. בסוף זו לא בעיה Azure-ית ולא בעיית DNS. זו בעיית תהליך בארגון. וכמו הרבה בעיות כאלה בענן, היא נפתרת הרבה לפני שמגיעים לקוד.

על המחברת

שירה זיו היא חוקרת סייבר המתמחה במחקרי Cloud ו-Post-Exploitation בסביבות ארגוניות מורכבות. היא הובילה מחקרי חולשות ענן ב-Microsoft, וכיום היא חלק מצוות המחקר של Cyera, שם היא עוסקת במחקר התקפי על סביבות ומוצרי ענן.

מקורות מידע

- Microsoft Learn - Prevent dangling DNS records and subdomain takeover: https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover
- Nuclei Azure Takeover Templates: https://github.com/projectdiscovery/nuclei-templates/blob/main/dns/azure-takeover-detection.yaml
- Subjack - Subdomain Takeover tool: https://github.com/haccer/subjack