

The Future of Supply Chain Attacks

מאת ליאור יקים

הקדמה

מתקפות שרשרת אספקה מלוות אותנו משחר ההיסטוריה. קוראי המגזין עשויים לחשוב מיידית על שרשרת אספקת תוכנה, אך צריך לזכור שקיימים סקטורים נוספים החשופים למתקפות אלו. הבנת האיום במימד הפיזי תסייע לנו להתמודד עם האתגרים איתם אנו ניצבים היום. דוגמא לאיום במימד הפיזי היא הרעלת ה-Tylenol שהתרחשה ב-1982. Tylenol הוא אחד ממשככי הכאבים הנמכרים בארה"ב. אלמוני הציב לו למטרה לפגוע בצרכני התרופה (מסיבות השמורות עימו).

הוא איננו יכול לפרוץ את מעגל האבטחה הפיזית של פס הייצור, שכן הוא מאובטח כהלכה מפאת רגישותו. אותו אלמוני תהה לעצמו, מהו המסלול אותו עוברת התרופה מרגע הייצור עד לצריכתה ע"י הלקוח. החוליה החלשה שהתגלתה הייתה חנויות ה-b2c, כלומר החנויות אשר מוכרות ישירות ללקוח. הפושע הכיר את הנוהל המקובל שבו ניתן להחזיר מוצר לאחר הרכישה, רכש מספר רב של תרופות וניצל זאת כדי להוסיף מעט ציאניד בטרם ההחזרה לחנות.

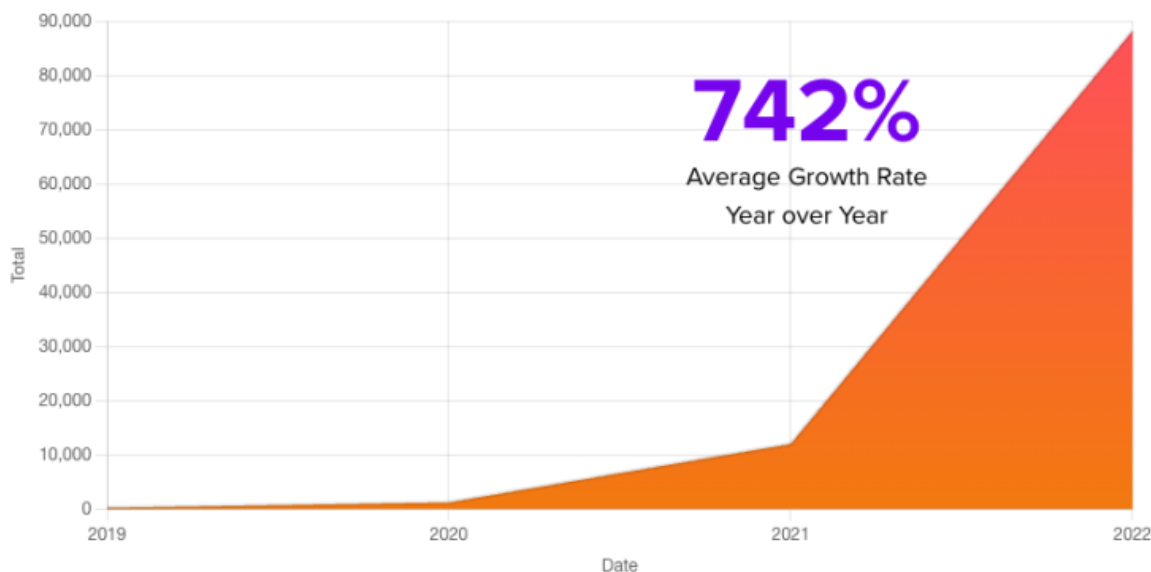
על אף שזוהי איננה הדרך היעילה ביותר לבצע מתקפת שרשרת אספקה (עבודה ידנית המשפיעה על מספר לקוחות מצומצם) מעניין לראות כי אותו מקרה גרר רגולציה מחמירה בכל עולם התרופות ויצירת אריזות anti-tampering. התפתחויות דומות נעשו בעולם התוכנה, וחברות רבות חרטו על דגלן לנסות ולאבטח את שרשראות האספקה מתוך הבנה שזהו וקטור תקיפה מרכזי בעל ערך רב עבור התוקף. היבט נוסף המקשר בין תקרית ה-Tylenol לעולם התוכנה הוא חיפוש החוליה החלשה כמטרה עיקרית. אנו עדים לנסיגות בעולם התוכנה שבהם תוקפים שואפים לפרוץ לארגונים גדולים ע"י פריצה ל-3rd party החלש ביותר שאותו ארגון תלוי בו.

במאמר זה נציג מספר מתקפות שרשרת אספקה דומיננטיות שהתרחשו בשנים האחרונות, ננתח את דפוסי הפעולה השכיחים של קבוצות התקיפה (APT - Advanced Persistent Threat) הידועות לשמצה כדוגמת Lazarus ו-Winnti. לאחר מכן נציע נקודת מבט הנוגעת לעתיד שרשראות האספקה, תוך הדגמה בעזרת תקיפה של חברה דמיונית בשם "Euro Bank".

מתקפות שרשרת אספקה

כפי שציינו בהקדמה, שרשראות אספקה הינן וקטור תקיפה מרכזי המושך תוקפים רבים. בגרף הבא ניתן לראות את קצב הגידול בהיקף המתקפות, בין השנים 2019 ל-2022. קצב גידול שנתי ממוצע של 742% אינו מותיר מקום לספק - התוקפים מרכזים מאמץ באיזור זה ועל הארגונים השונים להיערך בהתאם.

FIGURE 1.6. NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS, 2019–2022



נתחיל בסקירת המתקפות:

CCleaner (2017)

CCleaner זוהי תוכנה פופולארית מאוד לניקוי קבצים בעלת למעלה מ-2.5 מיליארד הורדות. חברת Piriform אשר פיתחה את התוכנה, נרכשה על ידי Avast ב-2017. כמות ההורדות האדירה, הופכת את התוכנה לקורבן צפוי של מתקפת שרשרת אספקה בגלל פוטנציאל הנזק האדיר - השפעה על מיליוני לקוחות.

Winnti הינה קבוצת תקיפה סינית ותיקה הפועלת מאז 2010. הקבוצה אחראית למספר תקיפות משמעותיות וחבריה מבוקשים על ידי ממשל בארה"ב. בשנת 2017 הצליחה הקבוצה לדחוף עדכון תוכנה זדוני אל האתר הרשמי של CCleaner, דרך שרת ה-build.

דריסת הרגל הראשונית התבצעה על ידי ניצול עמדתו של אחד המפתחים שהייתה במצב idle. בוצעה השתלטות מרחוק על ידי תוכנת Team Viewer, ולמזלם של התוקפים אותה עמדה הייתה מחוברת לרשת הפנימית של הארגון. ישנה הנחה שההרשאות להזדהות הראשונית הושגו בתקיפות עבר. התוקף השתמש

ב-ShadowPad בתור פלטפורמת malware. ה-loader הכיל shellcode שהיה Obfuscated עם יכולת טעינת פלאגינים דינאמית מול ה-C2. אותם פלאגינים היו מוצפנים ומכווצים, וניכר כי בוצעו התאמות בקוד הנוזקה, מה שמרמז על כך שהתוקף השיג גישה לקוד המקור של ShadowPad. הקוד הזדוני שהוזרק הכיל 2 שלבים נפרדים. הראשון שבהם (סקריפט VB) נועד לאיסוף מידע אודות הסביבה הנתקפת, תקשורת אל שרת ה-C2 (Command and Control) וטעינת השלב הבא. בשלב השני התוקף טרגט כ-40 לקוחות ספציפיים, אשר קיבלו את ה-payload דרך אותו C2.

על מנת למקסם את הנזק תוך הקטנת סיכון לחשיפה, בוצע שלב אימות אשר וידא כי למשתמש הנתקף יש הרשאות אדמין. במידה ונמצאו הרשאות נמוכות יותר, לא בוצעה כל פעולה. זוהי עדות לכך ש-Winnti בוחרים מטרות ספציפיות בעלות ערך ומוכנים לוותר על נזק פוטנציאלי לטובת Persistence. כמו כן בוצע שימוש ב-DGA (Domain Generation Algorithm) לצורך Obfuscation של התקשורת מול שרת ה-C2. ה-payload בשלב השני לא גרם לנזק משמעותי. תוכן שלב נוסף שיבוצע בעזרת ShadowPad, אך שלב זה לא התממש. הסבר אפשרי הוא גילוי מוקדם מהצפוי של התוקף.

על מנת להתגונן מול איומים מסוג זה, חשוב לוודא כי כל שינוי קוד מצריך Secondary reviewer כחלק מתהליך CI/CD מסודר. תהליך חתימת הקוד צריך להיות מבודד ומבוקר, ועלינו להציב כלי ניטור שונים לזיהוי אנומליות וגישות שאינן מורשות. כמובן שמנגנוני בקרת זהויות קלאסיים (כדוגמת MFA) נדרשים אף הם כדי למנוע גישה ראשונית למערכת ניהול הגרסאות (VCS).

ניתן להיעזר ב-ATT&CK framework על מנת למפות את ה-TTPs הרלוונטיים להתקפה זו מנקודת מבט הגנתית. דוגמאות:

[Compromise Accounts](#), [Supply Chain Compromise](#), [Domain Generation Algorithms](#), [Code Signing](#), [Obfuscated Files or Information](#)

Asus (2018)

לאחר ההצלחה המסחררת של Winnti בתקיפה על CCleaner, חיפשו חברה מטרה איכותית חדשה. Asus הינה ספקית המחשבים החמישית בגודלה בארה"ב. המחשבים שלה מגיעים עם תוכנה מובנית בשם ASUS Live Update האחראית על כלל עדכוני התוכנה הקשורים למוצרי Asus. Winnti הצליחו להשיג תעודה דיגיטלית תקנית מטעם Asus והשתמשו בה על מנת לחתום עדכון תוכנה זדוני שהוחדר אל תוך live update utility כ-backdoor. השימוש בתעודה ולידית, הקל על התוקפים ואפשר להם לחמוק מתהליכי ניטור ובדיקה שגרתיים.



כמות המשתמשים האדירה של התוכנה (מעל מליון יוזרים הושפעו) אפשרה לתוקף לבחור בקפידה את קורבנותיו. כחלק מהעדכון הזדוני, התוקף חיפש כתובות mac ספציפיות וכאשר אלו נמצאו בוצע נסיון התחברות לדומיין [.com.asushotfix]. בחירת השם אינה מקרית, זהו נסיון הטעיה בתקווה שצוותי ההגנה יפרשו כתובת זו כתעבורה לגיטימית. בדומה למתקפה של CCleaner ה-payload התחלק ל-2 חלקים. הראשון שימש ל-Reconnaissance והשני כוון אך ורק לסביבות המכילות למעלה מ-600 מכשירים. ניכר כי Winnti שחזרו מספר טכניקות פעולה במתקפה זו. נקודה ייחודית ראויה לציון היא העובדה שהתוכנה המדוברת (live update) דורשת גישה ל-BIOS, ולכן תהליך Patching סטנדרטי לא בהכרח יהיה יעיל כאמצעי התגוננות.

גם באירוע זה ניתן להיעזר ב-ATT&CK framework על מנת למפות את ה-TTPs הרלוונטיים להתקפה. דוגמאות:

[Supply Chain Compromise](#), [Code Signing](#), [Gather Victim Identity Information](#)

Okta (2022)

אוקטה היא חברה ותיקה בתחום identity security. בין לקוחותיה הרבים נמנים גופים ממשלתיים וחברות ענק. קבוצת התקיפה Lapsus\$ המרבה לתקוף חברות גדולות (Microsoft, Nvidia ועוד) הבינה את פוטנציאל הנזק, וסימנה את אוקטה כמטרה. קבוצה זו מרבה להשתמש בשיטות social engineering מגוונות הכוללות שוחד (תשלום עבור credentials ומFA approvals) ואף סחיטה.

התקיפה התרחשה דרך ספק צד שלישי בשם Sitel. ספק זה סיפק שירותי תמיכה עבור אוקטה והתאפיין ברמת הרשאה גבוהה למשאבים שלהם. תחילה הותקף עובד בעל הרשאות לרשת הפנימית. לאותו עובד הייתה הרשאה לרסט סיסמאות ומFA factors. התוקף התחבר לעמדת העובד הנתקף בעזרת RDP, בזמן שהוא היה מחובר לסביבת Okta.

Lapsus\$ סיפקו צילומי מסך כהוכחה לפריצה, ובהם ניתן לראות כלי backend admin תחת תווית של "Superuser" לניהול לקוחות. באופן טבעי, המונח "משתמש על" גרם להרבה פאניקה בתעשייה והרבה לקוחות אוקטה תהו האם הם חשופים לפריצה זו. חברות ענק כמו CloudFlare שהן לקוחות של אוקטה ביצעו פעולות פרואקטיביות כגון איפוס סיסמאות גורף לכל היוזרים שהשתנו לאחרונה. ה-CSO של אוקטה הכריז שלא התאפשרה גישת "god" כמשתמע מן האירוע. גישה לכלים פנימיים בשימוש Okta, כמו Jira ו-Slack אכן התאפשרה.

אוקטה למדה על התקרית ב-20 לינואר על ידי נסיון הוספת MFA factor ממקור גיאוגרפי חריג. אירוע זה קפץ לצוות ה-SOC במערכות ה-SIEM. בעקבות אותו זיהוי, אוקטה ניתקה את הסשן של העובד הקורבן והשעתה את חשבונו.



על פי ממצאי התחקיר המשותף של שתי החברות (Okta ו-Sitel) 366 לקוחות נחשפו כתוצאה מהפרצה. באותו הזמן כמות זו ייצגה 2.5% מכלל הלקוחות של החברה, ועדיין מדובר במאות לקוחות משמעותיים בפרופיל סיכון גבוה.

תקרית זו מדגישה את פגיעות הפקטור האנושי בתוך מערך ההגנה של ארגונים. כל עובד, ובמיוחד עובדים בעלי הרשאות גבוהות (תמיכה, IT, DevOps ועוד) צריכים להיות ערים לסיכונים הרבים של Phishing ו-Social Engineering. לא מעט מתקפות שרשרת אספקה התחילו מגניבת זהות פשוטה של עובד שלא ציית באדיקות לנהלי האבטחה בארגון. טעויות נפוצות הן סנכרון חשבונות פרטיים לחשבונות ארגוניים (gmail to service account), מחזור סיסמאות, שימוש ברשתות שאינן מוכרות ועוד.

גם באירוע זה ניתן להיעזר ב-ATT&CK framework על מנת למפות את ה-TTPs הרלוונטיים להתקפה. דוגמאות:

[Compromise Accounts](#), [Phishing](#), [Supply Chain Compromise](#), [Modify Authentication Process - MFA](#), [Data from Local System](#)

3CX (2023)

עד כה למדנו שמתקפות שרשרת אספקה מסוגלות לפגוע קשות במגוון רחב של לקוחות במקביל. מה דעתכם על מתקפת שרשרת אספקה כפולה? מייד נסביר.

לחברת 3CX יש מוצר VoIP מצליח עם למעלה מ-12 מיליון משתמשים. על מנת לחדור אל שרשרת האספקה של מוצר זה, קבוצת התקיפה Lazarus בחרה להתחיל בתקיפת שרשרת אספקה של ספק קטן יותר, אשר 3CX תלויים בו. שיטה זו מאפשרת לתוקפים להתמודד עם הגנות חלשות יותר, שהרי לא כל ספק חיצוני משקיע סכומי עתק באבטחת מידע כמו ענקיות הטכנולוגיה. דרך פעולה זו בעצם פורסת שטיח אדום עבור התוקף היישר אל תוך שרשרת האספקה של הארגון המוקשח.

במקרה שלנו Lazarus סימנו כמטרה ספק פיננסי בשם Trading Technologies. הכלי הפופולארי שלהם הנקרא X_Trader, כלל עדכון תוכנה זדוני בעת ההורדה מן האתר הרשמי. עובד של 3CX הוריד את הכלי, ונדבק ב-Malware. הנוזקה אפשרה לתוקף לאסוף credentials מהמכונה הנתקפת, מה שאפשר לו לגשת אל הרשת הפנימית דרך VPN יומיים לאחר ההדבקה. התוקף ביצע lateral movement תוך שימוש בכלי Fast Reverse Proxy בחיפוש אחר credentials. על מנת לחמוק מזיהוי, הכלי Frp שונה ל-MsMpEng.exe והועבר לתיקייה "C:\Windows\System32". התוקף ניסה להגיע אל שרתי ה-build שהם חלק מתהליך ה-CI/CD המלא של 3CX. משלב זה המתקפה הכילה שוני בין מערכות הפעלה שונות.



בסביבת Windows:

התוקף השתמש ב-DLL hijacking כנגד שירות IKEEXT אשר רץ עם הרשאות LocalSystem. מטרת הפעולה הינה Persistence, והשימוש בבינאריים של מייקרוסופט מפחית את הסיכוי לזיהוי מוקדם. התוקף הטמיע זוג נוזקות - TAXHAUL and COLDCAT.

- TAXHAUL - מפענח ומריץ shellcode, מהווה טריגר ל-downloader.
- COLDCAT - downloader מורכב, הוגדר להיות רדום למשך שבעה ימים מלאים.

בסביבת macOS:

הוטמע בשרתי ה-backdoor build בשם POOLRAT, אשר מינף LaunchDaemons לטובת Persistence. חלק מן היכולות כללו הרצת פקודות, קריאה וכתובת קבצים ועדכון קונפיגורציה.

היכולת המרכזית של הנוזקה הייתה הורדת והרצת shellcode ותקשורת מוצפנת מול שרת ה-C2. חשוב לציין שהאפליקציה הייתה חתומה ועברה תהליך notarization על ידי אפל על אף שהכילה קוד זדוני, דבר המדגיש את הצורך באחריות אישית בכל הנוגע להתמודדות עם malware. יש להציב אמצעי observability גם כאשר המידע מגיע ממקור לכאורה מהימן.

POOLRAT זוהה לראשונה ב-2020 וניתן לזיהוי ע"י חוק yara מבוסס hash.

גם באירוע זה ניתן להיעזר ב-ATT&CK framework על מנת למפות את ה-TTPs הרלוונטיים להתקפה. דוגמאות:

[Supply Chain Compromise](#), [Dylib Hijacking Code Signing](#), [Launch daemon](#), [Internal Proxy](#), [Obfuscated Files or Information](#)

נקודות נוספות שעשויות לסייע למגנים: API Hashing, ניטור תעבורת תקשורת, זיהוי התנהגות אנומלית כגון מחיקה עצמית, חסימת אפליקציות שאינן notarized (יכל לסייע במקרה של ה-build server). כמו כן Mandiant פרסמו את ה-IOCs הבאים:

Indicator	Type
D9D19ABFFC2C7DAC11A16745F4AEA44F	MD5
azureonlinecloud[.]com	C2 Domain
akamaicontainer[.]com	C2 Domain
journalide[.]org	C2 Domain
msboxonline[.]com	C2 Domain

עתיד מתקפות שרשרת האספקה



2023 הייתה השנה של Generative AI. על אף שהטכנולוגיה איננה חדשה לגמרי, ניכר כי הטכנולוגיה פרצה אל תוך המיינסטרים הציבורי. יש 2 צדדים לכל מטבע, ולצערנו אותה טכנולוגיה מרתקת זמינה גם לתוקפים אשר עשויים לנצל אותה כדי להתפשט מהר יותר בסביבות המותקפות. כפי שהדגמנו בהקדמה בעזרת תקרית ה-Tylenol, טבעם של תוקפים לחפש את החוליה החלשה במערך ההגנה של הארגון. בעידן שבו תוכנה ממוצעת תלויה במאות רבות של ספקי תוכנה אחרים, אותה חוליה חלשה עשויה להוביל למתקפת שרשרת אספקה ולהתפשטות מהירה.

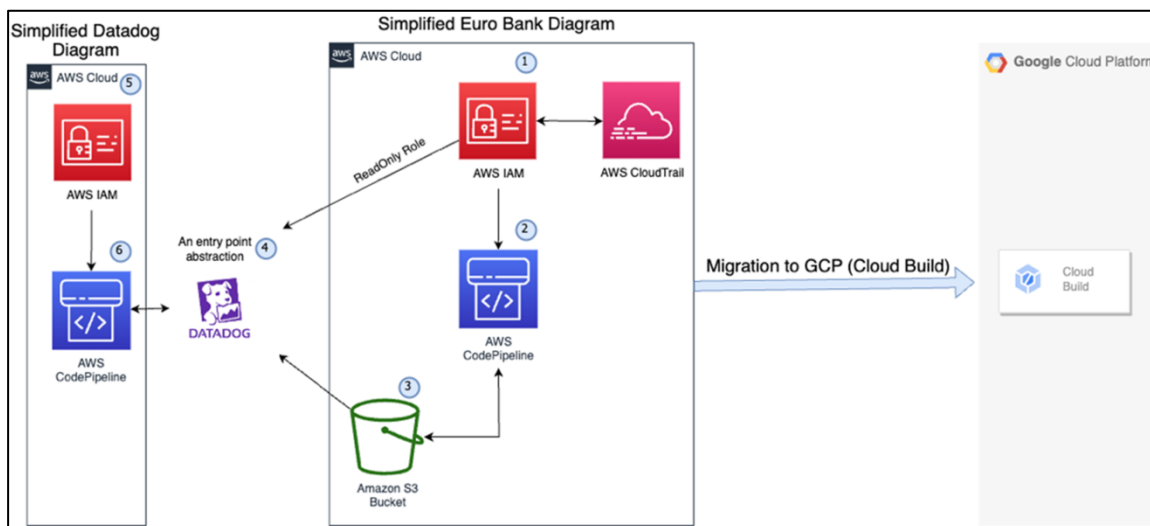
פריצה לבנק הגדול ביותר באירופה מאתגרת יותר מפריצה לספק צד שלישי החלש ביותר שלו, אך לעיתים קרובות תוביל לאותה תוצאה הרסנית. טבעי להניח כי עיקר הסיכון טמון בתלויות הישירות שלנו (לדוגמה ספק הענן) אך סיכון זה מנוהל כהלכה כחלק מתכניות DR/IR סדורות.

הבעיה היא שאין לנו יכולת לראות מעבר לקו התלויות הישירות, כלומר לענות על השאלה מי הם הספקים שהספק שלנו סומך עליהם? ישנה רשימה ארוכה של ספקי משנה אשר נותנים שירותים קריטיים לספקים הישירים שלנו, ולכן באופן טרנזיטיבי אנו סומכים עליהם ללא כל בקרה. ספקי הענק כדוגמת Amazon, Google ו-Microsoft תלויים בכמות אדירה של ספקי תוכנה. ב-2020, מייקרוסופט הודתה כי יש לה למעלה מ-10,000 תלויות צד שלישי. ניתן להניח שהמצב דומה גם בשאר ענקיות התוכנה. לכל ספקית ענן יש כמות אדירה של לקוחות, ולכן מתקפת שרשרת אספקה כנגדן עשויה להשפיע על מיליוני ארגונים ברחבי העולם.

דמיינו את התרחיש הבא: אתם CISO (Chief Information Security Officer) של הבנק הגדול ביותר באירופה. החברה שלכם מוגנת באופן יחסי, אחרי שהוצאתם תקציבי עתק על מוצרי הגנה מתקדמים. השקעתם גם זמן ואנרגיה רבה בחינוך העובדים כדי למזער ניצול גורם אנושי.

התשתיות שלכם (כולל תהליכי CI/CD) מתבססות על AWS, במקביל לספקי תוכנה נוספים. כמו כן אתם מסתמכים על DataDog כפלטפורמת ה-observability שלכם (3,4 איור 1). ביום בהיר אחד אתם למדים אודות מתקפת שרשרת אספקה משמעותית כנגד AWS, שנחשפת פומבית. מתקפה זו משפיעה על כל הלקוחות שמתמשים בשירות AWS Code Pipeline (1,2 איור 1) כולל הבנק הקריטי שלנו.

אין פאץ' זמין או הנחיה קונקרטית ללקוחות מצד AWS, וניכר כי יש לחץ רב מצד הדרגים הניהוליים. למזלכם אתם CISO אחראיים מהממוצע, וטרכתם להכין מראש תוכנית multi-cloud מקיפה, שבמסגרתה ניתן לבצע מיגרציה מלאה של תהליכי הארגון הקריטיים לענן של Google. כלומר נוכל לבצע מיגרציה מ-AWS Code Pipeline אל Google Cloud Build Service, על מנת למגר את האיום הבלתי פתיר מצד השירות של AWS:

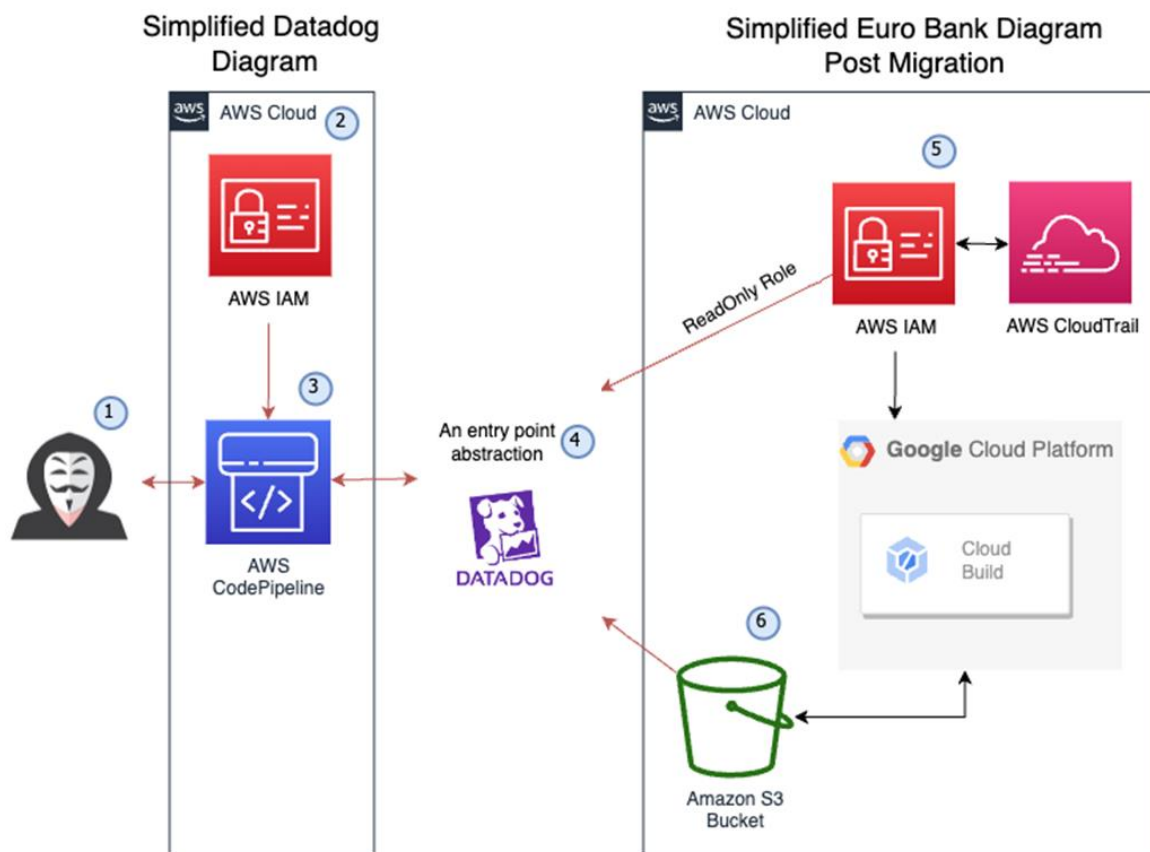


[תרשים ויזואלי מופשט של Euro Bank ושל Datadog לפני ביצוע המיגרציה]

המיגרציה עברה בהצלחה, ואתם הולכים לישון בידיעה שההיערכות המוקדמת שלכם הצילה את המצב. האמנם? לפתע הפלאפון שלכם מצלצל ב-3 לפנות בוקר. השיחה מגיעה מצוות ה-SOC, שטוענים בפאניקה כי תוקף (איור 2 אובייקט 3) מבצע exfiltration של מידע מסביבת פרודקשן, היישר מה-S3 Buckets של הארגון (איור 2 אובייקט 6). אתה מנחה את הצוות לבחון את ה-CloudTrail logs על מנת להבין מיהי הזרות הזדונית ברשת. הצוות מבחין בהתנהגות חשודה של role בשם "DataDogReadOnly" ומסיק שהוא שורש הבעיה.

מדוע לישות המוגדרת לקריאה בלבד יש הרשאות לבצע exfiltration מ-S3? אחד המהנדסים וודאי ביצע טעות קונפיגורציה ולא ציית לכלל ה-least privilege הידוע, האומר כי יש להגביל את ההרשאות למינימום הנדרש. השאלה הגדולה יותר היא למה אתו role מתנהג בצורה זדונית. היישות היחידה שיש לה גישה

לאותו role היא DataDog, חברה שעליה אנו סומכים. לבסוף האסימון נופל ואתם מבינים כי DataDog תלויים גם הם בתשתית של AWS, ועל כן הם פגיעים לאור מתקפת שרשרת האספקה על AWS. ככל הנראה התוקף השתמש ב"רגל" הנוספת אשר הייתה זמינה, שאפשרה לו לחדור לארגון שלנו למרות המיגרציה המוצלחת שלכאורה סגרה את הפגיעות:



[תרשים ויזואלי של וקטור תקיפה שתוקף יכול לנצל גם לאחר המיגרציה]

מורכבות הבעיה גדלה אקספוננציאלית, שכן DataDog הינה דוגמה בודדת מתוך אלפי תלויות צד שלישי המחוברות באופן טרנזיטיבי. למצב שבו צוות כחול מנסה להדוף ידנית גורם עוין במהירות הנמוכה ממהירות התפשטותו של התוקף (בשל כמות הרגליים האדירה הזמינה לו) נקרא golden supply chain attack.

התקפה מסוג זה ממחישה Persistence redundancy משמעותי, המתעצם לאור קצב התפתחות ה-AI. תוקפים מסוגלים למפות בצורה זריזה ואוטומטית את נתיבי התקיפה הזמינים, ואף "להחיות" רגל שנפגעה בעזרת רגליים חלופיות. התנהגות זו מזכירה תמנון - הידוע ביכולתו להחיות את זרועותיו. אם ניקח לדוגמה את נושא ההצפנות - כדי לייצר עמידות מול אתגרי post quantum לא מספיק שהארגון שלנו ישתמש באלגוריתמי הצפנה חסינים, נדרשת עמידות ואחריות רבה גם מכלל תלויות הצד השלישי שלנו.

בשל שותפות הגורל הזו, מתקפות שרשרת אספקה הן בעיה רוחבית החולשת על שלל רבדי התעשייה. ישנם פרויקטים רבים אשר חרטו על דגלם להיאבק באתגרים החשובים הללו, ובהם SBOM (Software Bill of Materials), VEX (Vulnerability Exploitability Exchange) ועוד. פתרונות אלו



מהווים צעד מעניין שיכול לסייע, אך בארגונים רבים הם אינם ממומשים או ממומשים חלקית בלבד. SBOM מתייחס לרכיבים ממבט על, ללא רזולוצייה של מודול ספציפי. הדבר מוביל ל-false positives רבים כיוון שללא שימוש במודול הפגיע הסכנה תיאורטית בלבד. VEX מתיימר לשפר זאת על ידי הוספה של פקטור ניצול (exploitability) לקשר שבין CVEs ורכיבי תוכנה.

עד שהסטנדרט האחד יאכף באופן גורף על כלל התעשייה, כל ארגון נדרש לנהל את סיכוני ה-3rd party בעצמו ולהחיל ניטור ומיטיגציות מתאימות.

לקראת סיום ארצה להדגיש מספר מגמות הנובעות מניתוח ההתקפות שביצעתי. אני מקווה שזה יעזור למגנים להיערך בצורה מיטבית למתקפות דומות אשר באופן בלתי נמנע יקרו בעתיד הקרוב.

Custom Payloads - תוקפים חודרים למנעד רחב של קורבנות על מנת לאסוף מידע, אך מטמיעים קוד זדוני שניוני (secondary payload) רק אצל קומץ מובחר. גישה זו מאפשרת להם לייצר פחות "רעש", ובכך להקטין את הסיכוי שיתגלו. על החברות לאתר אנומליות גם אם הדבר אינו כרוך בפגיעה משמעותית ישירה ב-scope נרחב.

Signature Trust - תוקפים משתמשים בטכניקות מגוונות הכוללות פשינג כדי לגנוב תעודות תקניות. חשיבות התעודות ברורה לכל קורא, והיא באה לידי ביטוי באופן מוגבר בתהליכי CI/CD. נניח שה-pipeline שלנו מורכב מ-4 שלבים מרכזיים: Source, Build, Test, Deploy.

ארגונים רבים מגדירים אמון על בסיס חתימת artifacts בטרם ביצוע deployment. על אף שגישה זו נשמעת מאובטחת, יש לה 2 סיכונים עיקריים. הראשון - מפתח (developer) המחזיק במפתח פרטי עלול לחשוף אותו במכוון או שלא במכוון. ישנם מקרים רבים שבהם תעודות תקניות נגנבו ונוצלו למתקפות שרשרת אספקה, כדוגמת Asus ו-SolarWinds. בדומה למגמת "Shift Left", הגורסת כי על המפתחים לדאוג לצרכי האבטחה בשלב מוקדם ככל האפשר, גם התוקפים עשויים לאמץ דפוס חשיבה דומה ולתקוף שלבים מוקדמים ב-pipeline טרם החתימה. ההנחה הבסיסית ששלבי ה-pipeline הקודמים מאובטחים כהלכה נאיבית ביותר. ברגע שהתוקף בעל יכולת חתימה, הוא יכול להתחזות ל-Vendor ולגרום נזק רב.

על המגנים לפרוס מנגנוני הגנה לאורך כל תהליכי ה-CI/CD. מספר דוגמאות הינן הפרדה תקשורתית הולמת בין השלבים השונים, חתימת commits, היגיינת סמאות, least privilege ועוד. כמובן שיש צורך גם בניטור פרואקטיבי וריאקטיבי של שימוש במשאבים רגישים כמו תעודות. ניתן להיעזר במיפוי של OWASP בנוגע לעשרת סיכוני ה-CI/CD הנפוצים ביותר:

<https://owasp.org/www-project-top-10-ci-cd-security-risks>

Daisy (Supply) Chain Attacks - כפי שצויין במאמר, מתקפת שרשרת אספקה יכולה להוביל למתקפות שרשרת אספקה עוקבות המייצרות עבור התוקף redundancy ו-impact רחב יותר. דוגמא לכך היא



המתקפה על 3CX, שבה מתקפת שרשרת אספקה על Trading Technologies סללה את הדרך למתקפת שרשרת אספקה על 3CX, שחקן מרכזי בתעשיית ה-VoIP. ניתן לאפיין התנהגות זו כ-vertical movement, שהרי התוקף מבצע מעין privilege escalation מחברה קטנה ופגיעה לחברה גדולה ומאובטחת. על החברות לרדד את רמת ההרשאות של 3rd parties למינימום ההכרחי, בהתאם לעקרון ה-least privilege ולנטר אותם באופן פרואקטיבי. ATT&CK matrix יכול לסייע בזיהוי מהיר ויצירת מיטיגציות בעת אירוע, כיוון שמרבית מתקפות שרשרת האספקה האחרונות כללו TTPs ידועים.

סיכום

אנו מצפים שמתקפות שרשרת אספקה ימשיכו להיות וקטור תקיפה דומיננטי ואף יתעצמו לאור מהפכת ה-AI. הכלים הזמינים לתוקפים היום, מאפשרים לפגוע בהיקף קורבנות רחב יותר, בזריזות רבה יותר ועם Persistency שלא חווינו כמותו בעבר. ה-Vertical Movement (שתוארה במסגרת "Daisy Chain") תשמש לחדירת ארגונים גדולים.

ככל שהארגון הנתקף גדול יותר, כך עולה הסיכוי ל-"golden" supply chain attack. הקורלציה נובעת מן העובדה שככל שהארגון גדול יותר, יש יותר גורמים התלויים בו ועל כן רמת ה-Persistency של התוקף צפויה לעלות בעקבות חדירתו.

על הארגונים להיות ערים לסיכוני ה-3rd party שלהם ולשאוף למפות את האמון שהם נותנים בגורמים חיצוניים כתוצאה מהתלויות הטרנזיטיביות (implicit trust). טבעה של רגולציה להתעכב אחר הטכנולוגיה, ועל כן יש להאיץ את תהליך האימוץ של framework אחיד עבור כלל התעשייה, כהכנה למתקפת שרשרת האספקה הבאה אשר עתידה לבוא.

על המחבר

ליאור יקים עובד כחוקר אבטחת מידע בחברת CyberArk.

קישורים

<https://blog.sonatype.com/2023-predictions-software-supply-chain-governance>