CISCO CYBER SECURITY

סקירה חצי-שנתית 2-2016

תקציר וממצאים

הבסיס להגנת הרשת - קיצור זמן הפעולה של התוקף.

תוקפים נהנים כיום ממרחב פעולה רב ברשת. התקפותיהם מופנות כנגד פרצות ידועות, שארגונים ומשתמשי הקצה היו אמורים לטפל בהן, אך הותירו אותן חשופות לפגיעה. על-כן, מתקפות כאלה נמשכות ימים, חודשים ואף יותר, מבלי שיבחינו בהן כלל. המגנים על הרשת מנסים לזהות פעילות עויינות, ושואפים להפחית את זמן הגילוי (Time To Detection - TTD) של איומים מוכרים וחדשים כאחד. בתחום זה הושגה אמנם התקדמות, אולם הדרך לסיכול המתקפות עדיין ארוכה.

הסקירה החצי שנתית בנושא אבטחת סייבר שמפרסמת חברת CISCO מציגה את התובנות העולות ממחקרים עדכניים בנושאי הגנת הסייבר שערכה חברת CISCO. הסקירה המיועדת למומחי אבטחה, מעדכנת מחקרים שפורסמו בעבר ומאירה התפתחויות עדכניות למחצית השנייה של השנה, בעלות השלכה לאבטחת הסייבר.

לצד הכלכלה המודרנית מתגבשת לאחרונה 'כלכלת צללים' מבוססת פשעי סייבר, ההולכת ומתמקדת בתשואת התקיפה. כך הפכו התקפות 'כופרה' (Ransomware) לפעילות שכיחה ורווחית ברשת, המופנית כלפי משתמשי הקצה בארגונים.

חלק ניכר מהמגמות, ורבים מהאיומים המובאים בסקירה נוגעים לפשעי כופרה - החל משיטות פעולה לשיגור מתקפות והסתרת הפעילות הזדונית וכלה בהערכת מגמות בהתפתחות איום משמעותי זה לדורותיו הבאים.

בסקירה אנו בוחנים דרכי פעולה מגוונות ואמצעים בהם יוכלו הארגונים לנקוט להגנתם.

ההמלצות של חוקרי הגנת הסייבר של CISCO כוללות:

- הטמעת תכנית תגובה לאירוע שתאפשר התאוששות מהירה וחזרה לעבודה סדירה בעקבות מתקפת כופרה
- אין לבטוח באופן עיוור בקישורי HTTPS ואישורי SSL
- עדכון ויישום מהיר של טלאי תוכנה (PATCHES) לפרצות המתגלות בתוכנות ובמערכות מידע, כולל מתגים ונתבים המהווים מרכיב קריטי ברשתות ובתשתיות האינטרנט
- הדרכת משתמשי הקצה בארגונים אודות סיכוני התוכנות המזיקות (נוזקות) הפוגעות בדפדפניהם
- הבנת המשמעות של מודיעין איומים ותגובות (ACTIONABLE THREAT INTELLIGENCE)

סקירה זו מקיפה ארבעה נושאים:

1. מגמות בפשעי סייבר: כופרה

מומחי האבטחה של Cisco התמקדו לאחרונה את בכופרה ובחנו את ההתפתחויות והחידושים התורמים להפצת השיטה והפיכתה לשכיחה ביותר. הסקירה כוללת גם תחזית להתפתחות מתקפות הכופרה המתבססת על מגמות שנצפו ברשת. בנוסף אנו מסבירים כיצד הזנחת פרצות, דחיית עדכונים במערכות ושימוש באביזרי תקשורת מיושנים, המקנים חופש פעולה לתוקפים ותורמים לפגיעות מערכות המידע. פשעי הכופרה מכוונים כיום אל המשתמשים בארגונים, על-כן על הארגונים לאבטח ולגבות מידע קריטי במיקום מוגן וליישם תכניות תגובה שתבטיח התאוששות מהירה וחזרה לפעילות שגרתית בזמן הקצר ביותר לאחר מתקפה כזו.

2. זמן לפעולה

פרק זה בוחן את ווקטור התקיפה מנקודת מבטו של התוקף, כשמערכת המידע עצמה מספקת לו את מרחב הפעולה וההזדמנות לבצע את זממו. פגיעותן הגדלה והולכת של ההצפנות ואישורי האבטחה, מקנות לתוקפים גישה למערכות באמצעות קישורים מאובטחים. הסקירה דנה בניצול ערכות פרצות (Exploit Kits) ודרכי תקיפה כמו נטייתם של עבריינים ברשת לתקוף שרתים להשגת גישה למערכות מידע רחבות יותר. הופעתם של שירותי תקיפה מבוססי פרסום (Malvertising) מציבים אתגרי אבטחה חדשים למגנים על מערכות המידע, ומציגים שאלה נוקבת - מיהם האחראים להגנתם של המשתמשים ברשת האינטרנט.

3. זמן לאבטח

בפרק זה בחנו חוקרי Cisco את הפער בין פעילות התקיפה ופתרונות ההגנה. לדוגמה, בעוד ספקי המערכות פועלים לקיצור סבב הפיתוח בין גילוי פרצה להפצת טלאי אבטחה במערכותיהם, המשתמשים אינם ששים להתקין את הטלאים האלה. פרק זה מביא פרטים אודות פעילותה של Cisco לקיצור זמן הגילוי (סדד) והשפעתו של מימד זה על 'מרוץ החימוש' בין המגנים לתוקפים ברשת. כמוכן מוצגים פרטים אודות הגידול בשימוש זדוני בפרוטוקולי תקשורת מוצפנת כמו HTTPS, והצפנת נתוני דואר אלקטרוני (TLS).

4. פרספקטיבה גלובלית והמלצות אבטחה

פרק זה בוחן את מגמות אבטחת המידע והרשת ברמה הגיאופוליטית, כגון החשש הגובר מפגעי סייבר ברמה הממשלתית, והצורך בהבנת האיומים על המערכות ואבטחת הגישה למידע לאור השנוי הטכנולוגי המתמיד. ההמלצה למגני הרשת הן לשאוף להפחתת זמן הפעולה הזמין לרשות התוקף ברשת. בנוסף מוסבר כאן ההבדל העקרוני בין סמני פגיעה (Indicators of Compromise - IOC) לבין מודיעין איומים (Threat Intelligence).

Download the Cisco 2016 Midyear Cybersecurity Report
www.cisco.com/go/mcr2016

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacic Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.