31/07/2024
כ"ה תמוז תשפ"ד
סימוכין: 1781

קמפיין מדינתי כנגד המשלחת הישראלית לאולימפיאדה

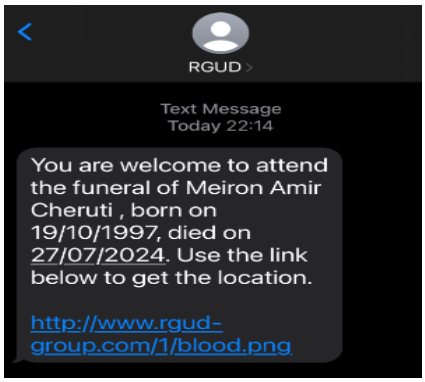
תקציר

1. לאחרונה חשף מערך הסייבר הלאומי קמפיין של קבוצת תקיפה איראנית כנגד הספורטאים המשתתפים במשלחת הישראלית לאולימפיאדת פריז.
2. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל אמצעי האבטחה הארגוניים הרלוונטיים.

פרטים

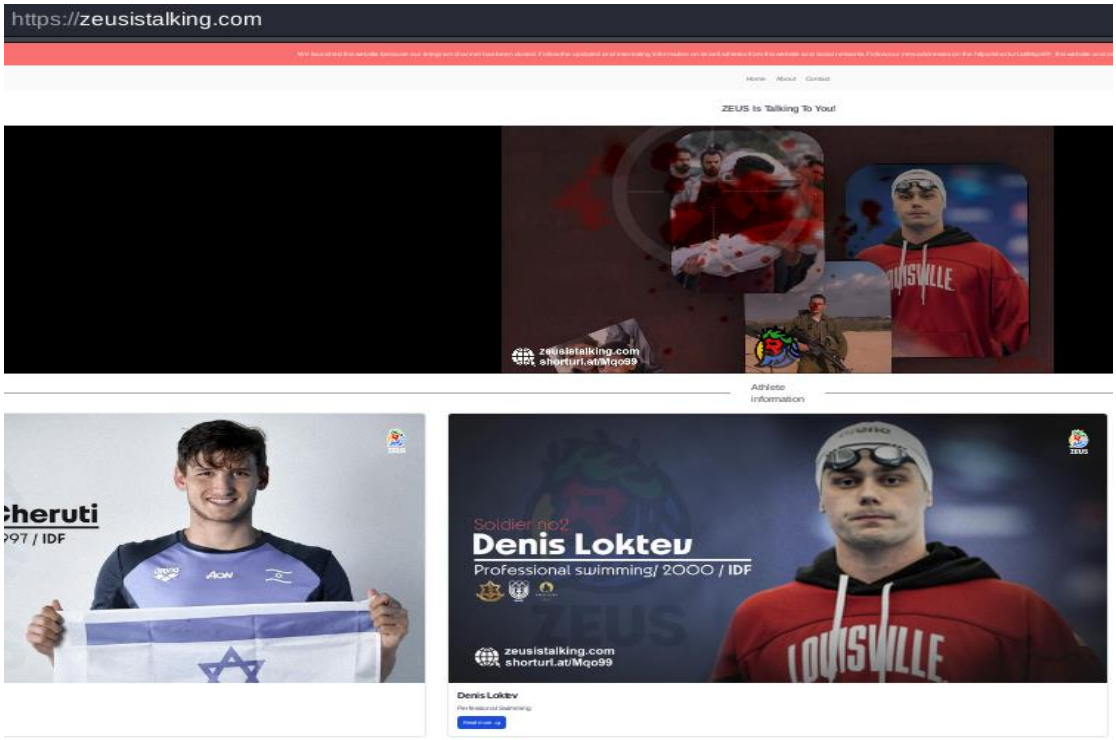
1. המערך חשף כי איראן עומדת מאחורי קמפיין השפעה חדש כנגד חברי המשלחת הישראלית לאולימפיאדה, המכונה "זאוס", במטרה לפגוע פסיכולוגית ומורלית בחברי המשלחת ובני משפחותיהם, ובביצועי הספורטאים בתחרויות השונות.
2. במסגרת הקמפיין נפתחו אתרים וערוצים ברשתות החברתיות בהם פורסמו תכנים אנטי-ישראליים הקוראים לחרם על ישראל, במטרה לגרום לאי השתתפותה במשחקים האולימפיים.
3. פורסם מידע אישי של חברי המשלחת וכן נשלחו מסרוני הפחדה לחברי המשלחת הישראלית וקרוביהם, תוך התחזות לארגון צרפתי בשם GUD (ארגון רדיקלי צרפתי).
4. מערך הסייבר פועל להסרת ערוצים אלו באמצעות יחידת הסייבר של פרקליטות המדינה.
5. במקביל לפעילות הקמפיין זוהתה פעילות האקטיביסטית כנגד ארגוני ספורט בישראל, בפרט מתקפות מניעת שירות (DDOS) והשחתות אתרים.
6. להלן חלק מפרטי הקמפיין:
    1. נפתח חשבון ברשת X (לשעבר טוויטר) בשם zeus_is_talking. נכון לכתיבת התרעה זו חשבון זה מושעה מפעילות.
    2. נפתחו מספר קבוצות טלגרם: ZEUS_Is_Talking, ZEUS_leak, ZEUS_Is_Talking_back_up. בערוצים אלו מפורסם מידע אישי על חלק מחברי המשלחת הישראלית.
    3. נפתח פרופיל פייסבוק בשם –Zeus.Is.Talking.

7. אנו מעריכים בסבירות גבוהה כי יפתחו ערוצים נוספים בפלטפורמות השונות להדהוד הפרסומים. מערך הסייבר פועל לסגירת ערוצים אלו בהקדם.
8. משלוח מסרוני הפחדה:
   1. נשלחו מספר הודעות SMS מאיימות למשתתפי המשלחת. ההודעות כוללות הפניה לקישור הזדוני: rgud-group[.]com/1/blood.png.



9. בכל הנראה הודעות אלו נשלחו מפלטפורמה ייעודית לשליחת הודעות SMS בתפוצה רחבה. התוקפים בקמפיין זה מנסים להשיג נגישות לחשבונות קיימים בפלטפורמות מסוג זה, בדרך כלל לחשבונות ללא אימות דו שלבי, כך שההודעות נשלחות בפועל מחשבון תמים לכאורה.
10. דומיינים שנפתחו לטובת הקמפיין:
    1. rgud-group[.]com – אתר המתחזה לארגון צרפתי רדיקלי בשם GUD ובו מסר לספורטאים הישראלים.

2. zeusistalking[.]com – האתר מפרסם פרטים אישיים על חברי המשלחת הישראלית הכוללים צילומים פרטיים, מסמכים אישיים וכו'. לאחר שאתר זה נסגר, נפתח אתר דומה בכתובת zeusistalking[.]net, וכן נפתח שרת גיבוי העושה שימוש ברשת TOR בכתובת: du3th2b4pvhidh5guvmb2g5hy7cepzl7wahnfnoxl7gynaxvljhhxbad[.]onion.



11. השחתות אתרים:

1. זוהו ניסיונות רבים לביצוע השחתות אתרים, חלקם בהצלחה. ניסיונות אלו התמקדו באתרים המשויכים לארגוני ספורט בישראל.
2. להלן דוגמה להשחתת אחד מאתרי הספורט בישראל

דרכי התמודדות

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל אמצעי האבטחה הארגוניים הרלוונטיים.
2. מומלץ מאד ליישם את הנחיות מערך סייבר הלאומי לגביי מתקפות DDOS והתמודדות עימן. ראו קישורים 1, 2.
3. מומלץ לבחון ביצוע החלפה יזומה של סיסמאות גישה.
4. מומלץ מאד ליישם מערכת אימות דו שלבית עבור כל שירות הנגיש מרשת האינטרנט.
5. מומלץ לוודא כי הפרטים הנדרשים לשחזור סיסמה של המשתמשים לא שונו על ידי תוקף. לדוגמה: כתובת הדוא"ל ו/או מספר הטלפון לקבלת מסרונים (SMS).
6. מומלץ לבחון הפעלת סינון מסוג GeoLocation – מניעת גישה ממדינות עוינות ובאלו שלא צפויה מהן תעבורה לגיטימית. תשומת לב כי זהו פתרון חלקי בלבד.
7. מומלץ לבחון חסימת גישה של כתובות עם מוניטין נמוך. לדוגמא, שרתי Proxy ושרתי VPN חינמיים ובתשלום, כתובות המוכרות כמשמשות לתקיפה וכד'.
8. מומלצת העלאת מודעות המשתמשים בנוגע לאבטחת סיסמאות, שיטות התחזות, הודעות דיוג וכד'.
9. מומלץ לבחון המלצות מערך הסייבר בנוגע לפגיעויות שכיחות המנוצלות על ידי תוקפים ולפגיעויות במערכות ניהול תוכן (CMS). ראו קישורים 3, 4.

מקורות

1. https://www.gov.il/he/pages/alert_1626
2. https://www.gov.il/he/departments/general/ddospr
3. https://www.gov.il/he/pages/alert_1667
4. https://www.gov.il/he/pages/cms

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה בלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

ניתן לשתף מידע המסווג TLP:CLEAR עם כל קבוצת נמענים, לרבות ערוצים פומביים