לקראת Opisrael 2016 - קמפיין מתקפת הסייבר על ישראל צפוי ב-7.4.16

Google Search

Telecom News 0.

לקראת Opisrael 2016 - קמפיין מתקפת הסייבר על ישראל צפוי ב-7.4.16
מאת: **מערכת Telecom News**, 4.4.16, 10:29

מבזקים נוספים לגבי היערכות הגורמים השונים (כמו CERT, MadSec) ועדכונים שוטפים לגבי Opisrael 2016 בתחתית הכתבה.

עד כה זוהו 4 קב' הצפויות להשתתף במתקפה. יוקם חמ"ל אזרחי, בהשתתפות נציגי משטרה, ביטחון לאומי וארגוני סייבר בתעשייה, שינטר את המרחב הקיברנטי, ידווח על תקיפות בזמן אמת ויעניק סיוע טכני לכל דורש. מובאות המלצות למזעור סיכונים.

לקראת Opisrael 2016, מתקפת הסייבר השנתית הצפויה ב-7.4.16, תקים חברת מודיעין הסייבר הישראלית White-Hat ביום התקיפה, חמ"ל אזרחי עם מיטב מומחי החברה, שינטרו את המרחב הקיברנטי, ידווחו על תקיפות בזמן אמת ויעניקו סיוע טכני לכל דורש.

White-Hat תקים את החמ"ל בהתנדבות כמדי שנה, בשיתוף עם גופי משטרה וביטחון לאומי, כמו גם נציגים של חברות סייבר נוספות בתעשייה. החברה אף הוציאה דף הנחיות לקראת Opisrael 2016 ובו היא מנחה כיצד לפעול על מנת למזער סיכונים.

קמפיין Opisrael מתקיים זו השנה הרביעית ובמהלכו קבוצות האקרים מכל העולם, בעיקר ממדינות ערב, מנסות לפגוע בגופים ישראליים באמצעות השחתת אתרים, מניעת שירות (DDOS) וגניבת מידע ממסדי נתונים.

בין היעדים הישראליים, שנפגעו ב-2015, היו אתרי רשויות, אתרים של ספקיות שירותי אינטרנט, אתרים של גופי חינוך ואקדמיה, גופים משפטיים ופיננסיים. צוות חוקרי המודיעין של White-Hat אסף ב-2015, כתוצאה מפריצות, שחשף לקראת ובמהלך הקמפיין, מידע שכלל יותר מ-400 כתובות מייל ממשלתיות, עשרות כרטיסי אשראי, שפרטי בעליהן נחשפו במלואן, יותר מ-10,000 כתובות דוא"ל, מגורים ומספרי טלפון, עשרות רבות של מיילים וסיסמאות מוצפנות של המכון הישראלי לייצוא ושיתוף פעולה בינלאומי, השירות המטאורולוגי ובנק ישראל, כמו גם עשרות פרופילים בפייסבוק של עסקים ואנשים פרטיים, שהכילו סיסמה. אנשי החברה פנו לכל הגורמים הללו, התריעו על הפרצות וסייעו במידת הצורך.

שרון נימירובסקי, מנכ"ל White-Hat: "מדי שנה המודעות לקראת יום זה גדלה והולכת. התוקפים מודעים לכך ולכן התקיפות מתחילות עוד הרבה קודם, עד מספר חודשים, כאשר, למעשה, ב-7 לאפריל נחשף "השלל" של אותן תקיפות. ב-2015, היינו עדים למספר כלים וטכניקות התקפות סייבר שונות כנגד רשתות ותשתיות. למרות שההתקפות היו צנועות בהיקפן ובמידת הנזק שגרמו, ההאקרים עדיין הצליחו למנוע שירות באתרים של גופים מרכזיים, להשחית אתרים ולהדליף נתונים. מודעות לנושא ונקיטה במספר צעדים בסיסיים יכולים לסייע במזעור הנזקים".

לקראת Opisrael 2016, עקבה יחידת המחקר של White Hat בשבועות האחרונים אחר קבוצות התקיפה ב-DarkNet ובערוצי ה-IRC המשויכים ל-Anonymous כדי לספק מודיעין טקטי מהיר ואיכותי לארגונים הנמנים על לקוחות החברה וחשופים לתקיפה. **עד כה זיהתה White Hat 4 קבוצות** הצפויות להשתתף בקמפיין השנה – AnonGhost, RedCult, Fallaga Team, Anonymous.

הנחיות בסיסיות, שנועדו למזער את רמת הסיכון בארגונים:

- לוודא בכל התחנות והשרתים, שגרסת האנטי וירוס מעודכנת לגרסה החדשה ביותר,
- לנקות חוקי FW,
- לא לפתוח מיילים משולחים לא מוכרים,
- לא להשתמש במיילים אישיים במחשבי הארגון'
- לא להתקין תוכנות או תוספים בלתי מאושרים בדפדפן,
- לדווח לממונים על כל אירוע או חשד לאירוע אבטחת מידע.

עדכון 18:14: ה-**CERT הישראלי** נערך ומקים חדר מצב באירוח Hacktics במשרדי EY ארנסט אנד יאנג ישראל, שברח' עמינדב 3 בתל אביב. מומחי IL-CERT סבורים, שניתן להתמודד בהצלחה עם האיום, לתקן נזקים ולהימנע מהם כליל. להערכתם, התוקפים לא יצליחו להפיל אתרים חיוניים, או להשפיע על שגרת החיים בארץ. את פעילות המרכז מלווים דרך פייסבוק אלפי מתנדבים מרחבי הארץ, שמספקים מידע והתראות על תקיפות.
ניתן להשתתף ולשלוח התראות על התקפות או מודיעין רלוונטי ל- report@il-cert.org.il
או בפייסבוק בקבוצה: https://www.facebook.com/groups/israeli.cert/
חדר המצב האונליין יתעדכן באופן שוטף.

14:27 YNET **הרמטכ"ל החליט: קצינים בכירים ישתתפו בטקסי יום הזיכרון**

14:10 YNET **איילת שקד: קוראת למנהיג הלייבור להילחם באנטישמיות**

14:05 YNET **בריטניה: שני חברי לייבור נוספים הושעו בעקבות הערות**

לצפיה מיטבית באתר TelecomNews המתקדם גלוש בדפדפן מתאים.

לוח מודעות

מהשנה האחרונה מצויים כאן.

מחפש תוכנות חופשיות? תוכל למצוא משחקים, תוכנות לפרטיים ותוכנות לעסקים, תוכנות לצילום

בנוסף, פורסם **מדריך התגוננות** המסייע במספר שלבים פשוטים להגן מפני OpIsrael.

עדכון 23:31: סביר להניח, שבמסגרת Opisrael 2016 לא יקרה במימדים עצומים מה שקרה היום בטורקיה, כאשר האקר המתנגד לנשיא טורקיה העלה לרשת נתונים של 50 מיליון טורקים הכוללים מס' תעודות זהות, כתובות, מקומות ותאריכי לידה ושמות הורים.
הדליפה לוותה במסר הבא נגד ארדואן ונגד היעדר הגנה ראויה:
Who would have imagined that backwards ideologies, cronyism and rising religious extremism in Turkey would lead to a crumbling and vulnerable technical infrastructure
bit shifting isn't encryption

עדכון 6.4.16, 11:49: צוות מודיעין הסייבר של **MadSec** מדווח, שקב' ההאקרים "תומכי דאע"ש" AnonGhost, הודיעה ברשתות הפנימיות שלה, שתתקוף משרדי ממשלה, מוסדות חינוך אקדמיים, רשויות לאומיות, משפטיות ופיננסיות, בנקים, ספקיות אינטרנט ושגרירויות של ישראל. קבוצות נוספות של האקרים, שמשתתפות במבצע, כוללות את קבוצת האקטיביסטים Red Cult, שהשתתפה בעבר בהתקפות כנגד דאע"ש, וקבוצות תוניסאיות דוגמת Fallaga Team.

צוות המודיעין של החברה הצליח להשיג מידע אודות קב' טלגרם, שהוקמה ע"י AnonGhost לקראת OpIsrael. בקב' יעבירו התוקפים בזמן אמת מידע על המתקפות: Telegram.me/OpIsrael.

ההאקרים משדרגים השנה את טכניקות התקיפה ומשתמשים בכלים חדשים, שלא נראו במבצעים הקודמים. כדי להגדיל את היעילות של המבצע, ההאקרים מפרסמים מדריכים טכניים לשימוש בכלים ורשימה של מטרות תקיפה. ארגונים נדרשים להתכונן מראש ולבחון את מוכנותם. ההאקרים פרסמו אירועים ברשת הפייסבוק הקשורים לתקיפה המקוונת נגד ישראל כדי לשתף ולחשוף את עבודתם ובכך לגרום לתומכיהם להצטרף ולהשתתף במבצעי התקפה.

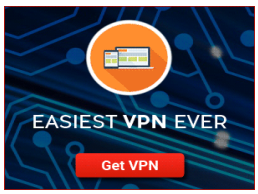
לוח האירועים **המלא** לגולשים מצוי כאן.

הכי ניצפים

התקשורת מוחבאת מאחורי "חסיון" - כאן

מה כן מקדם אתרים ועסקים באינטרנט? לא העלוקות שחיות סביב גוגל ופייסבוק - כאן

זרקור חברות



כמהזה?

ChinaBuy

שדי היראון

עדכון 6.4.16, 18:14: **מאבנת אבטחת מידע** נמסר, שספקיות האינטרנט הן בראש הכוונת של מתקפת ההאקרים השנה. ספקיות האינטרנט מחזיקות מספר רב של אתרים שיתופיים ושרתים פרטיים. אחריהם נמצאים אתרי ממשלה ומוסדות פיננסיים.

עדכון 7.4.16, 11:14: עד כה לא נרשמו מתקפות. פורסמו רק רשימות של **יעדי** פריצה של מוסדות ישראלים למשל - כאן.

עדכון 7.4.16, 12:14: לקראת OpIsrael 2016 הוקם מיזם Cyber Feed של חברת Cyber Hat מקבוצת **SECOS.** השירות מאפשר קבלת התראות ועדכונים שוטפים ישירות ל-WhatsApp המוצפן. כדי לקבל את השירות יש לשלוח הודעה ל-054-6942341 עם השם ושם הארגון, ולהתחיל לקבל עדכונים בזמן אמת. העדכונים ימשיכו עד ל-10.4.16. כדי לצאת מהשירות יש לשלוח הודעת "הסר אותי".

עדכון 7.4.16, 19:33: מחברת **White-Hat** נמסר, שההתקפות היום לא גרמו לנזקים משמעותיים ולא היו נרחבות מבחינת ההיקף. **מספר האתרים שנפרצו היה קטן יחסית ובחלקו הגדול פגע באתרים קטנים**. זמני מניעת השירות במהלך המתקפות היו קצרים והאתרים התמודדו עם המתקפה במהירות ובמקצועיות.

עד כה, התבצעו החל מאתמול מתקפות מניעת שירות (DDoS) לזמנים קצרים של אתר הכנסת, אתר משרד הכלכלה, אתר משרד התיירות, אתר בנק דיסקונט ואתר MAKO (למשך שעה וחצי, בזמן גמר תוכנית "האח הגדול"). תקיפה והשחתה של אתר לשכת רואי החשבון ואתר שגרירות רוסיה בישראל. המתקפה כללה פריצה לאתרים וניסיון לגנוב פרטים ממסד הנתונים של אתר "וואלה שופס" ו"יגואר" וכן של אתר "סירוב", תנועה של לוחמים במילואים הקוראים לסיום הכיבוש.

מ-**CERT** נמסר, שעד כה, לא הצליחו התוקפים לגרום לנזק גדול או משמעותי: הם הצליחו להפיל אתר של בנק, שחזר לפעול תוך דקות ספורות, פרסמו רשימות ישנות של נתוני אשראי, שאינן תקפים, ומספר אתרים קטנים הושחתו ונשתלה בהם תעמולה אנטי-ישראלית. מומחי IL-CERT סבורים, שגם השנה לא יצליחו התוקפים לגרום לנזקים גדולים או לשבש את שגרת החיים ברשת הישראלית.

עדכון 7.4.16, 19:59: עפ"י **MadSec**, הודלף בעיקר לרשת האפלה וגם ל-pastebin מידע מאתרים כמו מנהרות הכרמל, Ashra לביטוח סיכוני סחר חוץ, מזגני אלקטרה, אלטמן תעשיית רוקחות, איגוד מכוני הרישוי, מי עכו, מי חדרה, מי גני-תקווה, מי ציונה, אתר גב מערכות מידע, ארגון המורים בישראל, עיריית נס ציונה, עיריית נתניה, מועצה מקומית כפר שמריהו, קריית אונו, קרני שומרון, חברת הרכב פיג'ו ישראל, אתר "קווים", דור אלון גז, מגדלי קירור ירושלמי בע"מ.

עדכון 7.4.16, 20:48: המשך הודעות **MadSec**: הודלף מידע גם מהאתרים הבאים: בית חולים וולפסון, בית החולים הילל יפה,המכון למדיניות ואסטרטגיה-הבינתחומי הרצליה, הראל פנסיה (3000 רשומות), חברת גדות, חברת Mamanaviation.

עדכון 8.4.16, 10:21: לסיכום נראה, שמימדי ההתקפה השנה היו קטנים יחסית, במיוחד לנוכח למשל מה שקרה בפיליפינים, שם דלפו נתונים של 55 מיליון מצביעים...

ההגנה המושלמת על הגלישה הניידת והנייחת ועל הפרטיות מפני כל תוקף - לחץ כאן

Get VPN

תזכורת: ב-2014, המחשב היחיד שנפל ב- 7.4 היה של המשרד שהזהיר מפני התקפות ב- 7.4 - משרד התקשורת - לחץ כאן

0 תגובות

מיין לפי **הישנות ביותר**

הוסף תגובה...

Facebook Comments Plugin

SHARE

הגב בשם:

הוסף תגובה

תגובות: (צפה ב- 5 תגובות בעמוד זה)

07/04/2016 Anachtos
Years (2063) Israel be ready

05/04/2016 ggggggg
כלים להתקפת DDOS וסריקת ופריצה לאתרים
http://pastebin.com/uAZd7XAm
http://pastebin.com/PGQGhcjE

05/04/2016 ggggggg
/https://www.facebook.com/groups/193657587680078

04/04/2016 זיכרוני
לתזכורת
השנה לא ירגישו במשרד בכלל שהמחשב ייפול כי תמי אחראית כיום על המחשוב
שאל אותה אם היא יודעת להחזיק עכבר...
אז איך היא תבחין שהמחשב פועל או נפל?

04/04/2016 תזכורת
למיטב זכרוני, אשתקד המחשב היחיד שנפל ב 7.4 היה של משרד התקשורת

שירותנט Your IP מהירות גלישה מפת הביטקוין

שלח לחבר

+12 G+1 Like 351 fotolia

גאדג'טים

שאלות ותשובות | ספר אורחים | מידע נוסף | סקר TelecomNews

לייבסיטי - בניית אתרים