19.5.22 - התרעה - התקפה של כופרת LockBit על חברת אוטוסופט - קופות ממוחשבות – תקיפת שרשרת אספקה

תקציר האירוע

חברת אוטוסופט הישראלית שלה מערכת קופות ממוחשבת הותקפה בתאריך 17.5.2022 ע"י כופרת Lockbit.
כופרת LockBIt 2.0 מופעלת הן ע"י קבוצה מרכזית הנושאת את שם הכופרה כמו גם ע"י פושעים הקונים את שירותי הפעלת הכופרה מהקבוצה הראשית Ransomware as a service. הקבוצה והכופרה משויכות לעולם הפשע ומוכרות כשנתיים לפחות.
הקבוצה פעילה מאוד בעולם ובארץ ומצפינה מדי שבוע עשרות ארגונים.
נראה כי בהמשך להצפנה שהתרחשה בחברת אוטוסופט הודבקו חלק מלקוחות החברה גם הם בכופרה. דיווחים על כך הועלו לרשתות החברתיות (מצ"ב צילום מסך בהמשך)
בהודעת החברה המצורפת להתרעה זו נטען כי הכופרה הופעלה ע"י גורמים לאומניים. אין בידינו מידע היכול לאושש או להפריך אמירה זו. אנא בידקו קשר למערכות החברה.

תמונת מסך מתוך לקוח של החברה שהוצפן

(C) כל הזכויות שמורות ל ClearSky Cyber Security Ltd. 2021
TLP:AMBER אין להעביר את תוכן המסמך מחוץ לארגון הממוען

הודעת החברה כפי שנשלחה ללקוחותיה

אוטוסופט הופכים פוטנציאל, **למזומן**.

18/05/2022

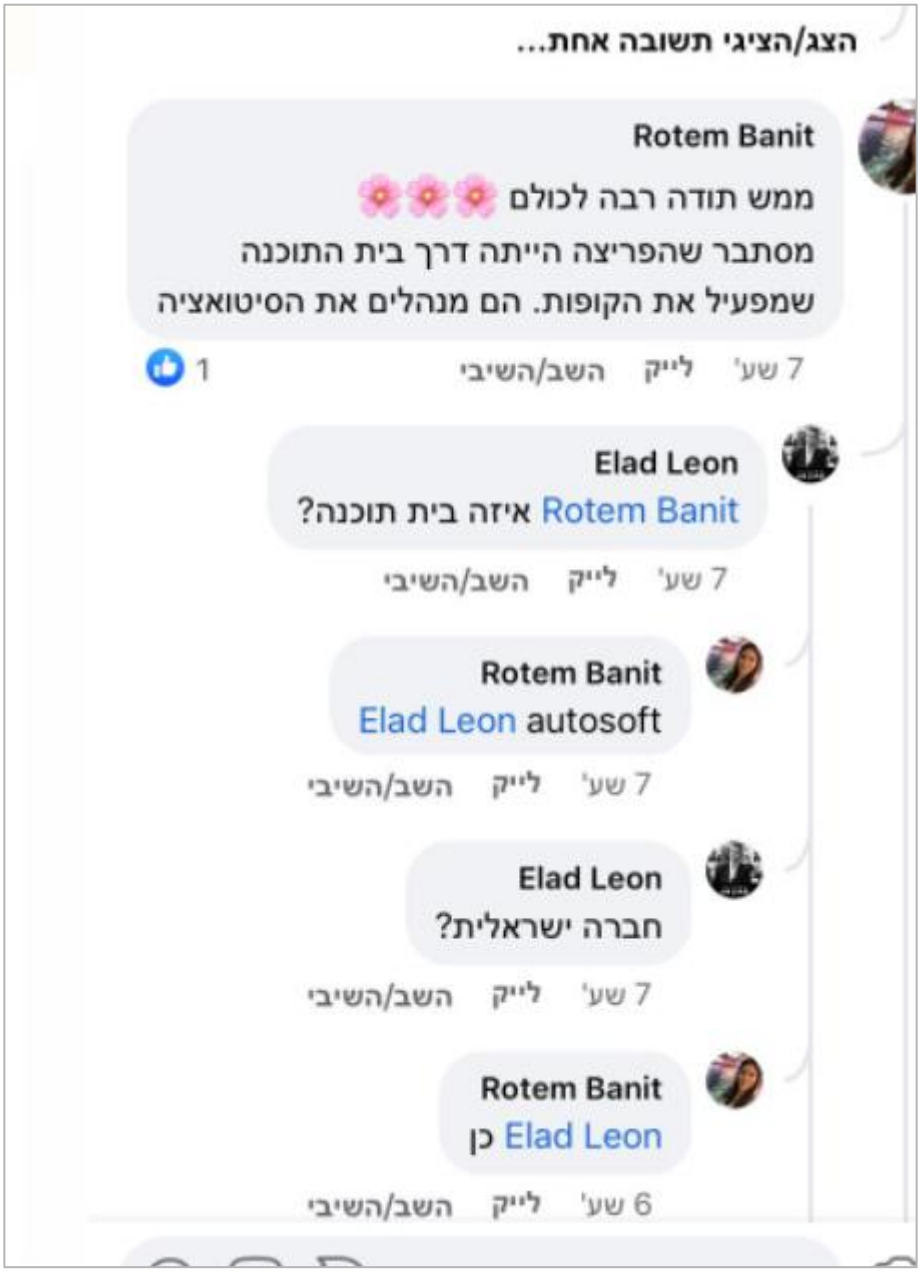
לקוח יקר,

אתמול, 17/05/2022, בשעה 20:54 החלה מתקפת סייבר על שרתי חברת אוטוסופט.
ההתקפה היתה באמצעות חדירה אל אחד משרתי החברה וניסיון להכנס דרכו לכל אחד מאלפי המחשבים שמחוברים אלינו בכל דרך שהיא. בתוך מספר דקות זיהינו את הדבר באמצעות כונני מחלקת התמיכה שקיבלו הודעות, הופעלו אנשי סיסטם שזיהו את מקור הבעיה ובשעה 21:10 הצליחו לעצור את התפשטות הקובץ הזדוני.
עצירת ההתקפה התאפשרה באמצעות אנשי הגנת הסייבר בחברת בזק שמנהלת את מערך האבטחה לשרתי החברה, אנשי בזק עצרו את המשך ההתקפה. במקביל, מיד עם התבררות הדברים עירבנו את מערך הסייבר הלאומי שנכנס לפרטי המקרה וליווה אותנו במהלך ההתמודדות.
אנשי המקצוע בחברה הגיעו בתוך זמן קצר למשרד החברה והחלו לסרוק את המחשבים, הקובץ הזדוני התגלה והוסר, אולם כאמור, נפגעו מספר רב של עמדות. התחלנו בבדיקה לתוך הלילה של כל העמדות, עברנו מחשב אחר מחשב, תוך מיפוי המצב של כל עמדה.
לצערינו, במהלך 15 הדקות שבהן היתה ההתקפה, נפגעו כ 200 עמדות מחשב בקובץ הזדוני, אשר מבצע הצפנה על כל הכוננים במחשב, מה שבעצם נועל את הגישה למידע.
מערך הסייבר הלאומי אספו פרטים ומנסים לעזור בבדיקת סוג הקובץ הזדוני כדי לנסות ולשחזר את המידע המוצפן.
לגבי העמדות שנפגעו, יש לבדוק האם קיים גיבוי על אמצעי חיצוני שניתן ממנו לשחזר את המידע.
לגבי כל עמדה שנפגעה נבצע אבחון בהתאם לקונפיגורציה של כל עמדה ונמליץ על אופן הפעולה.
אנו פועלים באופן אינטנסיבי כדי לסייע לכל מי שנפגע, נבקשכם לגלות אורך רוח ולהבין את מורכבות המצב. מטרתנו היא להביא את העמדה בחזרה לעבודה במהירות האפשרית, תוך סיוע בהחזרת מידע מגיבוי חיצוני.
לצערינו הפריצה הצליחה למרות מערך אבטחה מוקפד של שרתי החברה שמוגן ע"י Firewall מעודכנים ומתקדמים שמנוהלים ע"י מקצועני אבטחה.
בדיקה ראשונית של הקובץ הזדוני העלתה שלמרות שמצוין לכאורה שמדובר בדרישת כופר, נראה שזה לא המקרה מאחר ואין כל הפניה לתשלום כופר, מה שמעלה חשד לניסיון לפגיעה ממניעים לאומניים שנועדו לגרום לנזק.
מדובר בעבירת טרור סייבר ועל כולנו להטות כתף ולהלחם בה, חברת אוטוסופט תעשה הכל על מנת לסייע בשיקום המצב במהירות האפשרית, לכן אנו מבקשים את שיתוף הפעולה שלכם.

בכבוד רב
יריב ודני, מנהלי החברה

(C) כל הזכויות שמורות ל ClearSky Cyber Security Ltd. 2021
TLP:AMBER אין להעביר את תוכן המסמך מחוץ לארגון הממונן

תמונת מסך מתוך רשתות חברתיות המראה התבטאויות של לקוחות החברה



(C) כל הזכויות שמורות ל .ClearSky Cyber Security Ltd 2021
TLP:AMBER אין להעביר את תוכן המסמך מחוץ לארגון הממוען