



# תקיפות כופרה 2021

עקרונות, מגמות  
וסיפורים מהשטח

יורי קוגן – מייסד

**EOC**

**ERGO**

**O**RIENS

**C**ONSULTANTS

[INFO@ERGORIENS.COM](mailto:INFO@ERGORIENS.COM)

## סיפור קצר מהשטח

- שבת בבוקר, דצמבר 2020, ניו-יורק
- מנהל IT (מיקור חוץ) של חברת שירותים (כ- 100 עובדים) מגלה שמערכות החברה לא זמינות ומוצא קובץ הכולל דרישת כופר, ללא אולטימטום קצוב
- מחליט להתמודד עצמאית עם האירוע מבלי לעדכן את מנהלי החברה (סופ"ש...)
- פונה בדוא"ל (המופיע בהודעת הכופר) לתוקפים במטרה לנהל מו"מ. מוסר שלאור מצבה התזרימי של החברה אין ביכולתה לעמוד בתשלום הכופר
- במקביל בודק אפשרות לעלות מגיבויים, שנמצאים לא תקינים
- נמנע מלעדכן את הנהלת החברה במהלך סופה"ש
- התוקפים שולחים לחברה את טיוטת דו"ח הרווח-הפסד האחרון שלה, שהוזלג משרתיה ומצביע על רווח נאה
- מעדכנים את מנהל ה-IT שהוא נתפס בשקר ולא תהיה פשרה בנושא סכום הכופר
- מציגים אולטימטום – Within a week
- הנהלת החברה מעודכנת ומערבת חברת IR ומנהל מו"מ מקצועי
- האירוע נסגר לאחר שבמו"מ סכום הכופר יורד לרמה המייתרת המשך מו"מ למול Downtime
- צוות ה-IR מחזיר בהדרגה את מערכות החברה לתפקוד

## מסקנות

- ניהול אירוע סייבר חייב להתבצע ע"י הנהלת החברה
- קיימת סבירות שהתוקף מכיר את החברה הנתקפת ומצבה – שקר הניתן להפרכה הוא לא רעיון טוב
- ניהול מו"מ הוא מקצוע
- הנהלת החברה חייבת לנהל סיכונים במהלך האירוע ולקבל החלטות בהתאם לתפיסת הסיכון המשתנה

# תקיפות כופרה (RANSOMWARE)

- המטרה: כסף וכמה שיותר (דיסקליימר: יש אירועים הנחזים תהיות אירוע כופרה אבל הם לא...)
- האמצעים:
  - חדירה לרשת המטרה
  - הזלגת מידע לצורך סחיטת הקורבן תוך איום בפרסומו/מכירתו
  - מניעת שימוש באמצעות הצפנת בסיסי הנתונים של הארגון הנתקף
  - העתקת מידע לטובת סחיטת הקורבן ו/או מכירת המידע בדארקנט
- סוגי תקיפות כופרה:
  - רחבה (Carpet Bombing/תקיפת ממטרה)
  - ממוקדת (Targeted / Spear Attack)
  - איך יודעים ולמה זה חשוב?
- הרעה החולה והלא כ"כ חדשה: Ransomware as a Service (RaaS) זה כמו SaaS אבל הרבה פחות נחמד)
- ועוד לא דברנו על Double Extortion ו-Triple Extortion...

# תקיפות כופרה שעשו כותרות



Industries that matter



FOCUSED ON YOU.



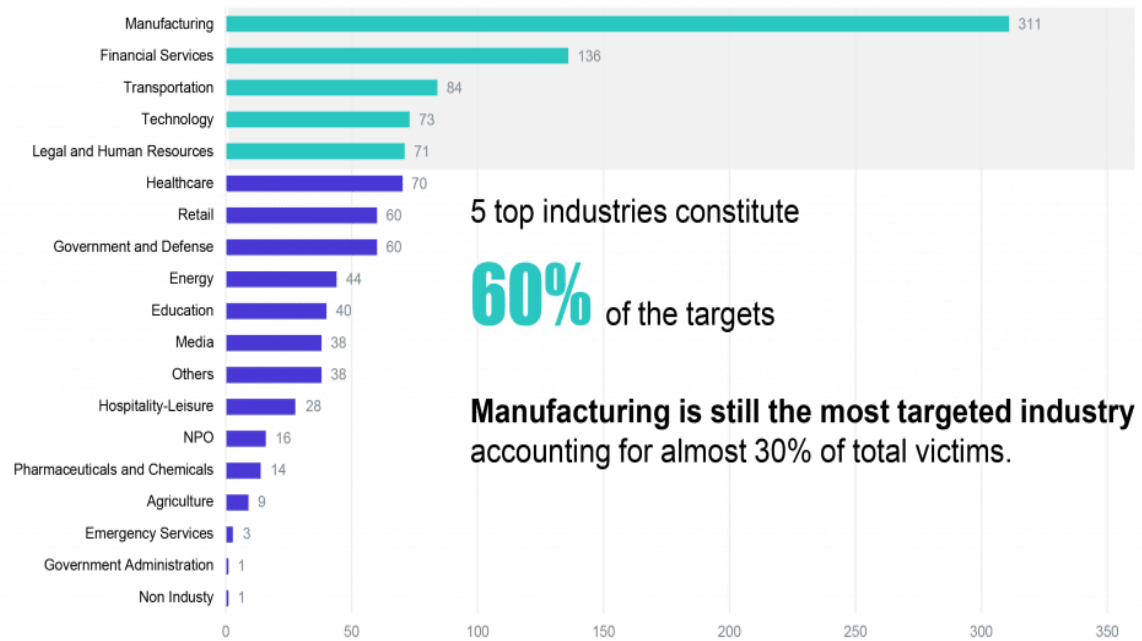
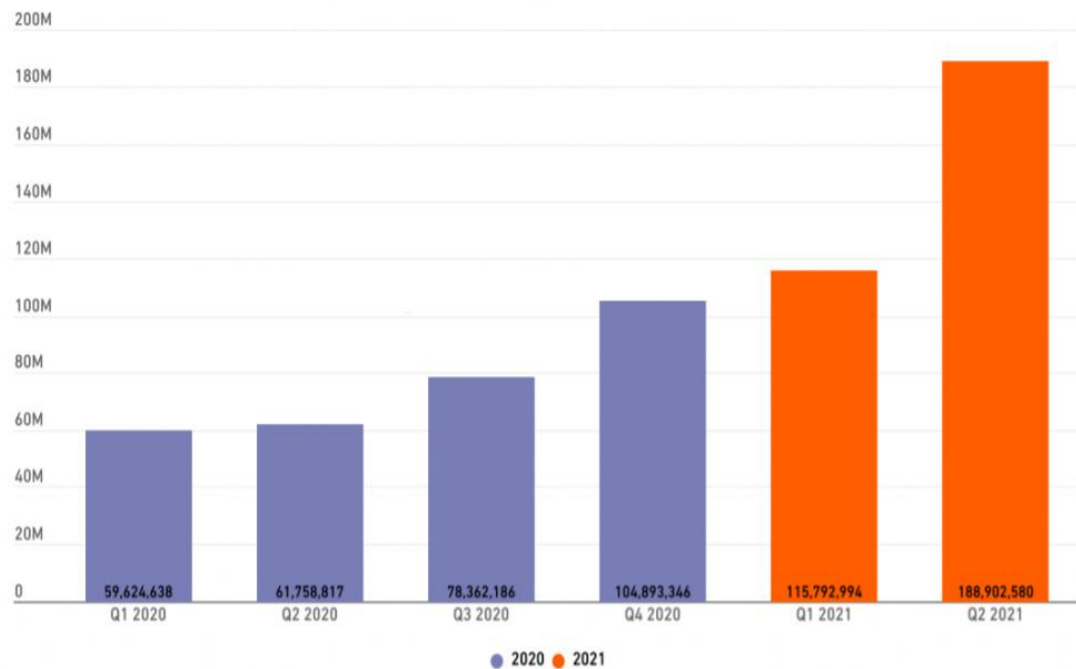
# Kaseya®



# COLONIAL PIPELINE CO.

# תקיפות כופרה – מגמות 2021

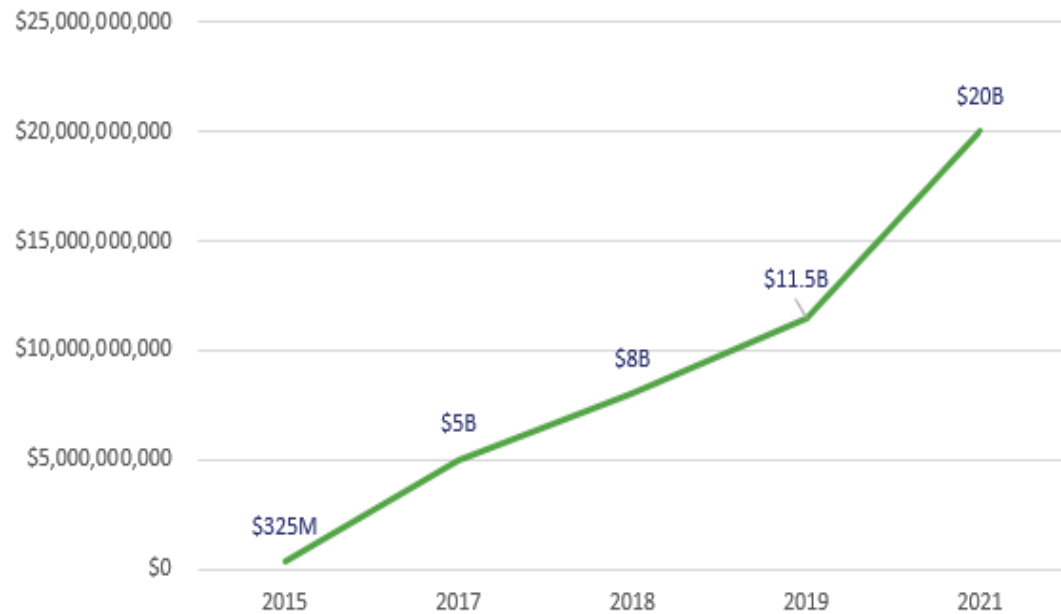
RANSOMWARE GROWTH BY QUARTER



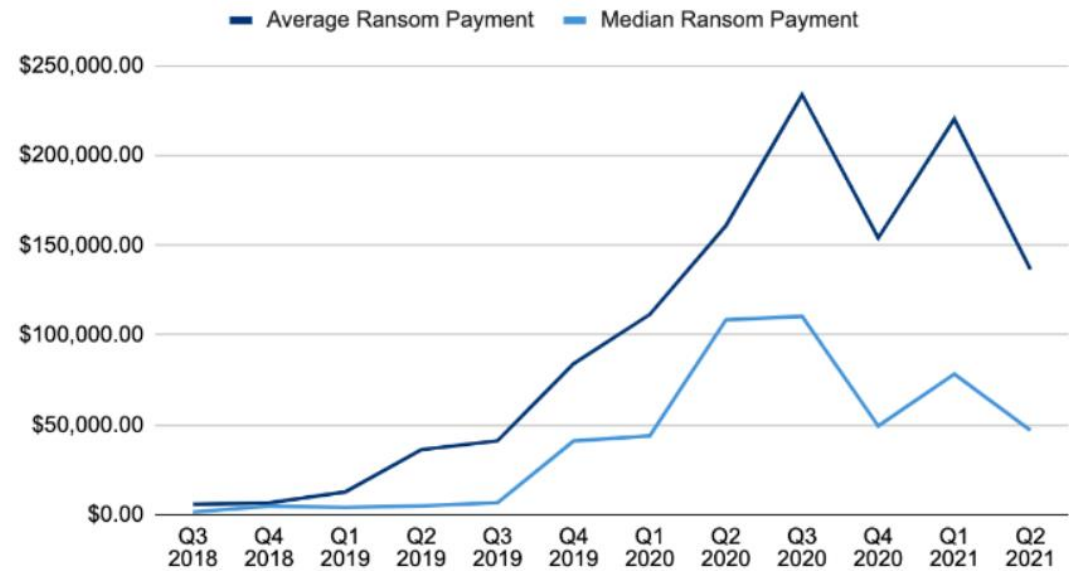
• לאחר אירוע Colonial ונספחיו ניכרת הפחתה במספר האירועים למול תשתיות מדינה ותשתיות קריטיות למול עליה באירועים מול מטרות עסקיות בסדר גודל קטן ובינוני (AP , December 2021)

# נזקי הכופרה (ישירים ועקיפים)

### Predicted Ransomware Damages 2015-2021



### Ransom Payments By Quarter



# כמה ולמה זה עולה לנו?

- עלויות ניהול משבר (IRT, מו"מ, משפטי, יח"צ ותקשורת)
- Downtime
- תשלום כופר
- קנסות רגולטוריים
- נזק תדמיתי
- תביעות והסדרים משפטיים



## איך זה קורה? תקיפה באמצעות צד ג'

- תקיפת יעד משמעותי בעל מערכות אבטחה טובות דורשת משאבי רבים וזמן היערכות ואיסוף מודיעין רב
- במקרה של תקיפה באמצעות צד ג' יבחר התוקף לחדור ליעד באמצעות גורם מאובטח פחות שהנו בעל נגישות למערכות היעד (לדוג' ספק שירותים, חברת אירוח אתרים וכו') או מערכת המותקנת אצל לקוחות רבים (תקיפת שרשרת אספקה דוגמת אירוע Solarwinds)
- דוגמאות לכמה אירועי עבר:
- מאריוט (2020) – תקיפה באמצעות חדירה דרך קבלן תוכנה (השגת סיסמאות של עובדים בחברה באמצעות פשינג)
- ג'נרל אלקטריק (2020) – גישה הושגה באמצעות תקיפת חשבון דוא"ל של ספק שירותים, שליפת רשימת עובדי GE על סמאות השימוש ברשת....
- P&N Bank (אוסטרליה, 2020) – תקיפת חברה לאירוח אתרים בה השתמש הבנק וחדירה למערכות הבנק דרך חברת האירוח
- Quest Diagnostics (ארה"ב, 2019) – חדירה באמצעות תקיפת ספק שירותי בילינג
- Target (ארה"ב, 2013) – כניסה למערכת באמצעות Fazio Mechanical, קבלן מקררים לרשתות מזון

## תקיפות כופרה – דילמות ונקודות למחשבה

- האם לנהל מו"מ עם התוקפים? אילו סוגי מו"מ קיימים?
  - תוצאתי
  - טאקטי
- לשלם או לא לשלם???
- האם יש איסור בחוק לשלם לתוקפי כופרה?
- האם קיימת Sucker list? האם כשהארגון שלי משלם כופר הוא מזמין תקיפה נוספת?
- אם אחליט לשלם, האם אקבל בחזרה את הדאטה שלי? האם התוקף יעמו במילתו ולא יפרסם את המידע ברבים?
- למה נתקפתי והאם יש דרך וודאית למנוע תקיפות כופרה?

## ניהול אירועי סייבר – נקודות למחשבה

- האם זה אירוע או משבר? מה ההבדל ולמה זה חשוב?
- מי מנהל את האירוע/המשבר? המנכ"ל הדירקטוריון? ה-CISO? מומחים חיצוניים/חברת הביטוח?
- האם קיימת בארגון תוכנית/נוהל לפעולה בעת אירוע סייבר?
- מה רמת המוכנות הארגונית לעמוד בפני אירוע סייבר ולצלוח אותו במינימום נזקים?
- האם הוגדרו תפקידי חירום לבעלי עמדות מפתח בארגון? מתי לאחרונה הארגון תורגל בהתמודדות עם אירוע סייבר?
- מה מצבנו בנוף הרגולטורי הרלוונטי?
- האם קיימים בארגון תוכנית המשכיות עסקית (BCP) ותוכנית התאוששות מאסון (DRP)?

## הביקורת הפנימית – נקודות להתייחסות

- מה ניתן היה לעשות על מנת למנוע את האירוע או למזער את נזקיו?
- האם עומדים בסטנדרטי Best practices בתחום אבטחת המידע (רכיבי אבטחה וניטור, ביטחון סיסמאות, עבודה מרוחקת/מהבית...)?
- האם בוצעה הכנה ארגונית לפעולה בעת אירוע סייבר?
- האם קיים בארגון נוהל עדכני להתמודדות עם אירוע סייבר?
- באיזה נוף רגולטורי פועל הארגון ומה סטאטוס הציות לרגולציה הרלוונטית?
- האם בוצעו תרגילים להתמודדות עם אירוע כופרה (תרגיל מנהלים / טכנולוגי hands-on)?
- האם בוצעו מהלכים להגברת המודעות לאיום בקרב בעלי התפקידים בארגון?
- האם קיימת התייחסות לסוגיות אבטחת מידע ומערכות בעת צירוף ספקים חדשים ולתקף עיתית אצל ספקים קיימים?
- האם קיימת בארגון רשימת נותני שירותים לחירום?


זכרו!

העלויות הישירות והעקיפות של ניהול משבר  
סייבר לעולם תהיינה גבוהות יותר משמעותית  
מהעלויות תהליך המוכנות לאירוע מסוג זה



תודה על תשומת הלב

 [info@ergoriens.com](mailto:info@ergoriens.com)

 +972-54-6952270