

KOBI GINZBURG, C.P.A
L.L.M., M.B.A.

AVI JUDELEWICZ, C.P.A

EFRAT RAVIV - HALFON, C.P.A
M.B.A.

ROLY HOGEN, C.P.A
L.L.M., M.B.A.



הוגן, גינזבורג, יודלביץ ושות'
Hogen, Ginzburg, Judelewicz & Co.

רואי חשבון | Certified Public Accountants

קובי גינזבורג | רו"ח
מוסמך במשפטים, מוסמך במינהל עסקים

אבי יודלביץ | רו"ח

אפרת רביב - חלפון | רו"ח
מוסמך במינהל עסקים

רולי הוגן | רו"ח
מוסמך במשפטים, מוסמך במינהל עסקים

מגמות מטרידות בהתקפות כופרה בשנת 2020

בגיליון HandsOn מספר 5 עסקנו בהרחבה בתופעת הכופרה מניעה והשלכותיה, בגיליון החודש נציג מספר ממצאים ומגמות שעלו מניתוח עשרת אלפים התקפות כופרה שהתרחשו בשנת 2020. את הניתוח ביצעה חברת מחקר הסייבר CyberEdge בחודש אוקטובר השנה.

כופרה הורגת - ב-10 לספטמבר 2020 דווח לראשונה בהיסטוריה על מוות כתוצאה מהתקפת כופר אישה תושבת דיס לדורף, גרמניה הובהלה במצב קשה לבית החולים האוניברסיטאי י הקרוי לבית מגוריה, בית החולים לא יכול היה לקבל אותה בשל קריסת מערכות המידע עקב מתקפת כופרה והפנה אותה לבית חולים אחר המרוחק 30 קילומטרים. האישה נפטרה במהלך הנסיעה ואין ספק כי לו קיבלה טיפול מידי בבית החולים בדיסלדורף, חייה היו ניצלים.

The New York Times
Cyber Attack Suspected in German Woman's Death
Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

MIT Technology Review
A patient has died after ransomware hackers hit a German hospital
This is the first ever case of a fatality being linked to a ransomware attack.

DARKReading
Deadly Ransomware Story Continues to Unfold
A ransomware attack with fatal consequences is attracting notice and comment from around the world.

ZDNet

Duesseldorf University Hospital
September 10, 2020

UKD Universitätsklinikum Düsseldorf
Zentrale Notaufnahme
112

תובנות ומגמות שעלו מניתוח

• **מצפינים וחושפים** - עברייני הסייבר כבר לא מסתפקים בהצפנת המידע, אלא גונבים

וחושפים ברשת מידע רגיש, כאמצעי לחץ לתשלום דמי הכופר "וכענישה" על אי תשלום.

Ransomware warning: Now attacks are stealing data as well as encrypting it

SFU ransomware attack exposed data from 250,000 accounts, documents show

Nefilim Ransomware Threatens to Expose Stolen Data

Ransomware Hacking Groups Post Data from 5 Healthcare Entities

NetWalker, REvil, SunCrypt, and Pysa, or Mespinoza, ransomware hacking groups posted data allegedly stolen from five healthcare entities in recent weeks to blackmail them into paying the ransom.

Maze Ransomware Attacks Surging in 2020, Demanding Ransom, Exposing Stolen Data

Maze ransomware exposed Canon's stolen data online

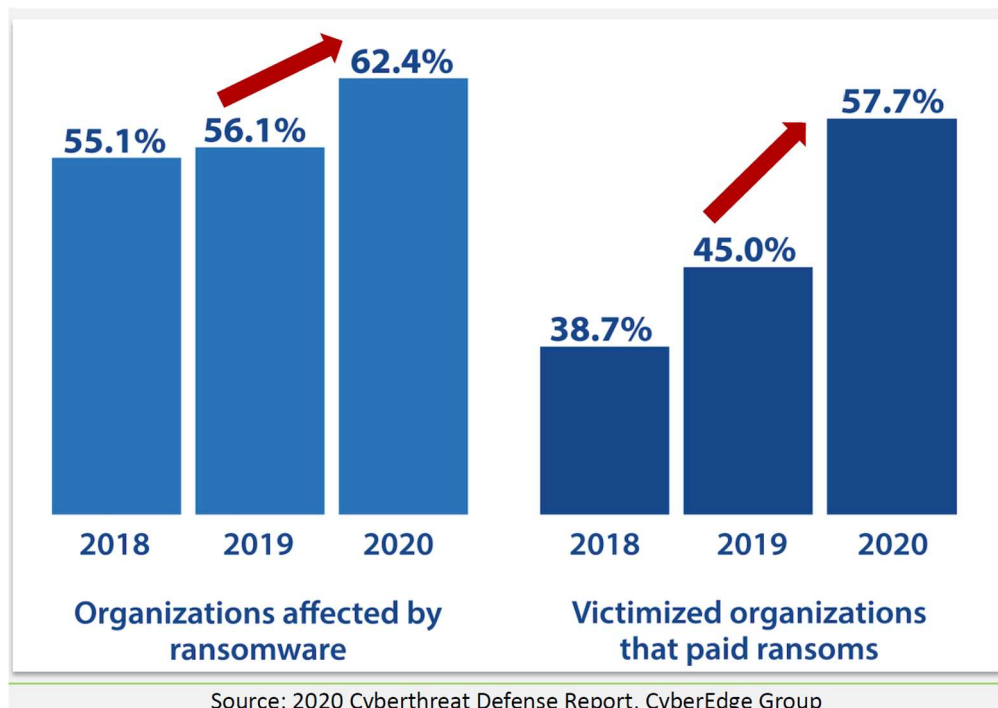
Data stolen in ransomware attack on French telco Orange

• שלושת הווקטורים המובילים למתקפות כופרה

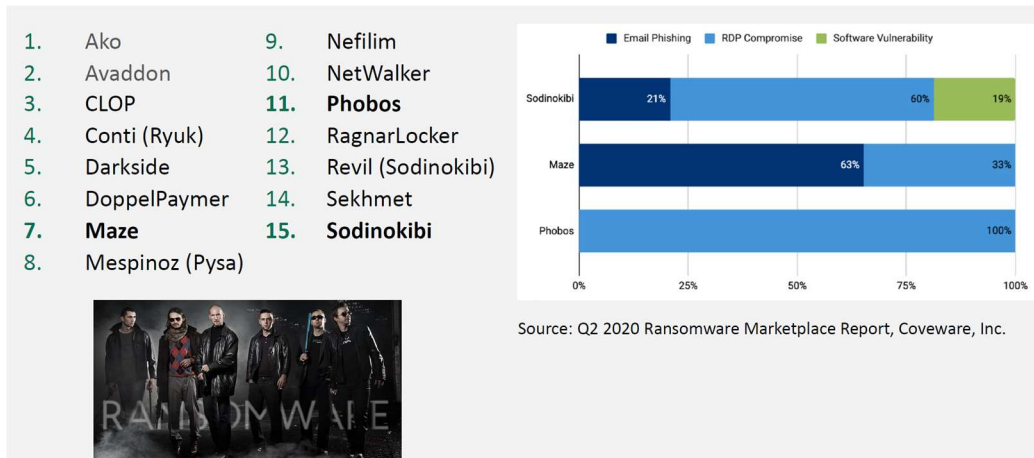
- מספר 1 : ניצול חולשות בפרוטוקול RDP.
- מספר 2 : פשינג המופץ בדואר אלקטרוני.
- מספר 3: חולשות ופגיעויות תוכנה.

• תעשיית הכופרה - הכופרה הנה תעשייה משגשגת עם אחוזי הצלחה גדלים והולכים, 62.4%

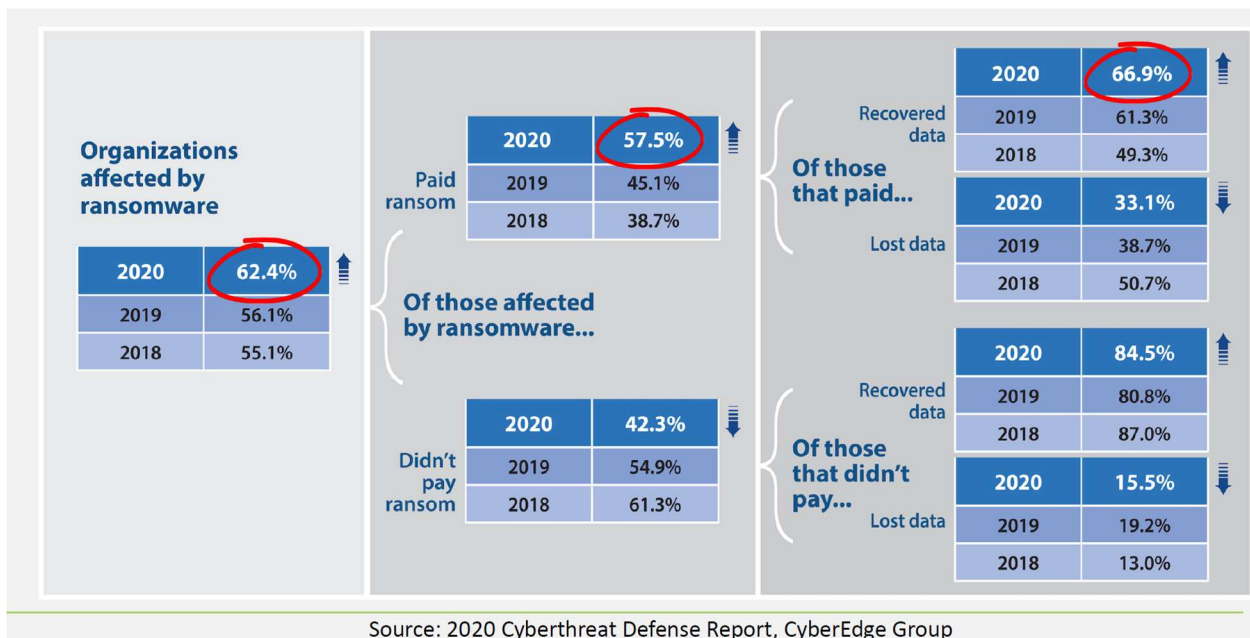
הצלחה בשנת 2020 (מסך הארגונים שהותקפו) בהשוואה 56.1% בשנת 2019. במקביל חלה עליה נאה במספר הקורבנות המשלמים 57.7% בשנת 2020 ובהשוואה 45% בשנת 2019. ולא מעט "לקוחות חוזרים" שחוו התקפות חוזרות.



- **מי מספר אחד?** - חברת Coveware חשפה את 15 "כנופיות כופרה המצליחות ביותר", יחד עם הטקטיקה החביבה עליהם, קבלו אותם:



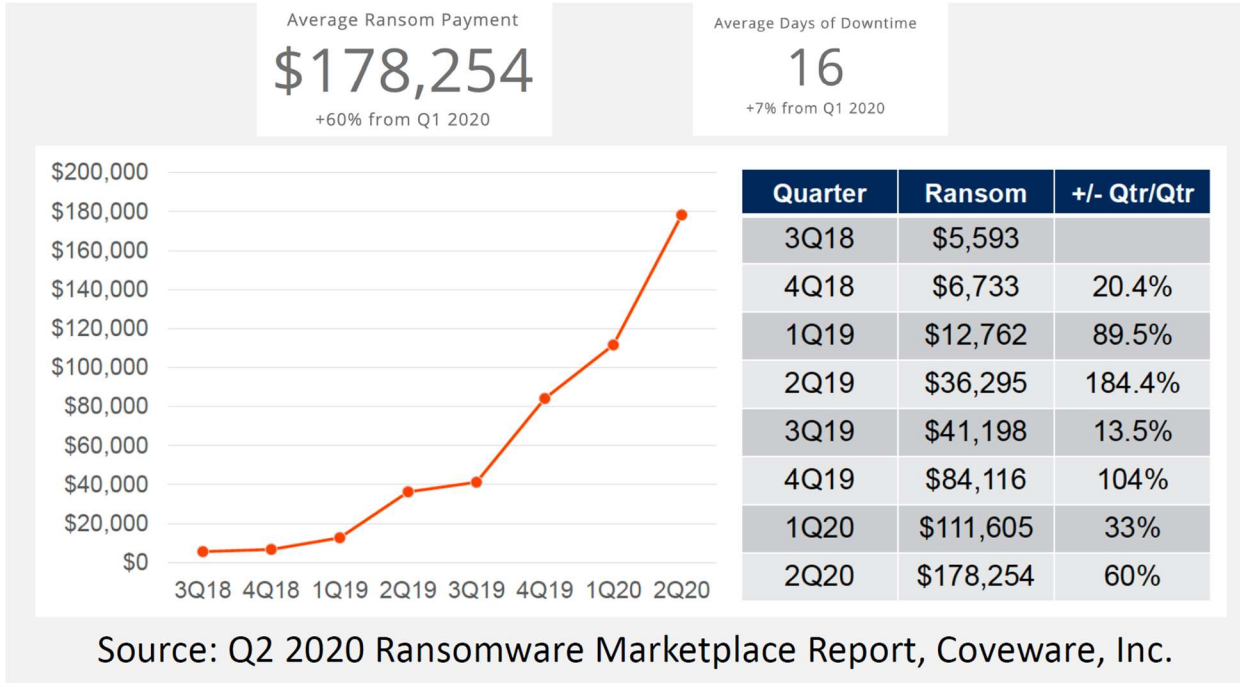
- **מעגל הקסמים** – התיאבון של פושעי הסייבר גדל ככל ההתקפות מצליחות < יותר ארגונים משלמים > יותר ארגונים מקבלים את המידע חזרה (לאחר ששילמו!).



• **המחירים עולים והימים מתארכים - סכום תשלום הכופר הממוצע גדל והולך מ-\$5,593**

בממוצע בשנת 2018 ועד \$178,254! בממוצע בשנת 2020.

- 16 ימי השבתה בממוצע (גידול של 6% בהשוואה לתחילת השנה).



• **לשלם או לא לשלם – זו כמובן שאלת \$178,254 עם שיקולים לכאן ולכאן.**

לא לשלם	כן לשלם
עלום תשלום הכופר (\$178,254 בממוצע)	פחות זמן השבתה
שחזור המידע אינו ודאי למרות התשלום	סיכוי טוב לקבל חזרה את המידע (66.9%)
מניעת פרסום שלילי	מניעת פרסום שלילי
מטרה להתקפות חוזרות	צמצום האפשרות לחשיפת המידע
מימון ארגוני פשע	חסכון בזמן השבתה

- **אז מה עושים?**

- **היו מוכנים!**

- שקלו לרכוש ביטוח סייבר עם כיסוי הולם לתרחיש אסון אפשרי.
- נסחו מדיניות תשלום כופר \ או אי תשלום יחד עם המבטח שלכם והחליטו באילו תנאים ישולם כופר ובאילו תנאים לא ישולם.
- אתרו ספק פוטנציאלי שישא וייתן בשמכם בעת הצורך (הוא עשוי להפחית 50% מדמי הכופר).
- הקימו צוות תגובה למקרה כופר שיכלול: מנהל, נציג המבטח, יועץ משפטי, איש צוות טכני ורשימת אנשי קשר לסיוע ודיווח (רשויות חוק, רגולטורים, יועצים).
- בדקו היכן ואיך רוכשים ביטקוין.

- **השקיעו ב-FIREWALL האנושי שלכם**

- בצעו הדרכות מודעות ואנטי-פישנג באופן מתוכנן ושוטף לכל העובדים.
- תלו כרזות \ שלטים, שלחו מיילים עם תזכורות מודעות.



- **השקיעו בטכנולוגיות אבטחת מידע**

- בצעו עדכוני תוכנה שוטפים ותכופים כחלק משגרת העבודה, למערכות הפעלה, יישומים, התקני תקשורת, Firewall.
- גיבוי, גיבוי, גיבוי – בצעו גיבויים קבועים ושגרתיים לכל המערכות החשובות כחלק משגרת העבודה ובדקו שהגיבויים אכן פועלים.
- השתמשו באמצעי אימות חזק MFA ובמיוחד לחשבונות ניהול מקומיים ובשירותי הענן. נהלו בקפדנות הרשאות גישה למידע רגיש וממשקי ניהול.
- יישמו מערכת בקרת התקנים ברשת (NAC).
- השתמשו במערכת EDR להגנת כל נקודות הקצה במערכות מנוהלות ולא מנוהלות.
- שקלו ליישם מערכת גלישה מאובטחת \ גלישת Proxy.