

**לא משאירים אבנים לא
הפוכות: מאבק במתקפות
כופר בתחנות העבודה
ובשרתים כאחד**

מתקפת כופר היא אחת מסוגי התוכנות הזדוניות המתאפיינים בהתפשטות מהירה ביותר. התוקפים לא טורחים לגנוב ולמכור את המידע החשוב שלך או של העסק – כל שעליהם לעשות הוא להצפין אותו ולדרוש כופר. במהלך השנים, תוכנות הכופר שהיו בתחילה חוסמי מסך פשוטים המלווים בדרישת תשלום, הלכו והתפתחו לכדי גל עצום של תוכנה זדונית מסוכנת בהרבה. אינך יכול להרשות לעצמך להשאיר אבנים לא הפוכות במאבק בהתקפות ה-Crypto-locker.

מה היקף הבעיה הטמונה במתקפות כופר?

כיצד פועלות במתקפות כופר ומדוע הן כל כך קטלניות? תוכנה זדונית מסוג זה מבוססת על **Cryptors** – סוסים טרויאנים שמסתננים למערכת בעת פתיחת קובץ זדוני המצורף להודעת דוא"ל שקיבלת או כתוצאה מלחיצה על קישור תמים למראה שמעביר אותך אל אתר אינטרנט שנבנה במיוחד למטרה זו. הקוד הזדוני סורק את הנתונים שלך ומצפין אותם ללא ידיעתך, חלקם עלולים להיות חשובים מאוד, כגון: תמונות אישיות, ארכיונים, מסמכים, מסדי נתונים, תרשימים ועוד. בהמשך, תוכנות ה-Crypto-locker מציגות דרישת תשלום – לעתים קרובות סכומים ניכרים – כדי לשחרר את החומר שהוצפן.

מובן שהתוקפים שומרים על אלמוניות מוחלטת. לפיכך התשלום הנדרש יכול להיות באמצעות Bitcoin, בעוד ששרתי הבקרה והשליטה של התוקפים מסתתרים ברשת Tor בלי שניתן יהיה לחשוף אותם. אם מיירטים את התעבורה בין הסוס הטרויאני לבין שרת המקור שלו, שימוש בתוכניות הצפנה לא שמרניות, כגון Tor או אלגוריתמים מקובלים של הצפנה, מבטל את אפשרות הפענוח של הקובץ (Trojan-Ransom.Win32.Onion, למשל, עושה שימוש בכל הטכניקות הללו).

כיום, חלק מתוכנות ה-Crypto-locker דורשות תשלום לא רק עבור הנתונים שהוצפנו, אלא גם עבור 'שירותים' נוספים מסוימים. לדוגמה, התוקף יכול 'להגדיל את ההימור' באמצעות סחיטה: "שלם כעת, ולא – נשלח את היסטוריית הגלישה שלך לכל אנשי הקשר שלך."

באיזו מידה נפוצה מתקפות הכופר?

במתקפות כופר שהתגלו (באמצעות Kaspersky Security Network)	
121238	2014
448430	2015
554267	בסה"כ

במהלך 2015, מספר ההתקפות הכולל של תוכנות כופר שנתגלו על ידי Kaspersky Security Network היה כמעט פי 4 מזה של 2014: כמעט **ארבע מאות חמישים אלף זיהויים** בסך הכל. קיים שלל סוגים ומשפחות של תוכנות כופר, כגון CryptoWall, TeslaCrypt, TorrentLocker ו-Locky. [CTB-Locker](#), ACCDFISA ו-GpCode נמנו עם הידועים ביותר לשמחה. הנתונים הלקוחים מ-Kaspersky Security Network (להלן) מספקים מושג לגבי היקף התקפות הכופר שהתרחשו במדינות האיחוד האירופי ב-2015:

2015

כינויים ידועים נוספים לתוכנת כופר זו	משתמשים ייחודיים (KSN), במשולב	משתמשים ייחודיים (KSN)	Kaspersky Lab verdict
TeslaCrypt	81180	80017 1163	Trojan-Downloader.JS.Cryptoload Trojan-Ransom.Win32.Bitman +
CTB-Locker	25062	16491 8571	Trojan-Ransom.NSIS.Onion + Trojan-Ransom.Win32.Onion
CryptoDefense (גרסאות מוקדמות), CryptoWall (גרסאות מאוחרות)	7346	7346	Trojan-Ransom.Win32.Cryptodef
	4998	4998	Trojan-Ransom.Win32.Snocry
	4955	4955	Trojan-Ransom.Win32.Cryakl
	1681	1681	Trojan-Ransom.Win32.Crypren
	1390	1390	Trojan-Ransom.Win32.Shade
	1173	1173	Trojan-Ransom.Win32.Crypmod
TorrentLocker	717	717	Trojan-Ransom.Win32.Rack
	395	395	Trojan-Ransom.Win32.CryFile

לא משאירים אבנים לא הפוכות: מאבק במתקפות כופר בתחנות העבודה ובשרתים כאחד

Locky, הכלי ששימש כנראה בהתקפה על Hollywood Presbyterian Memorial Hospital, בא לעולם באמצע פברואר באותה שנה וכבש את מקומו כאחת מתוכנות הכופר המובילות הפעילות בתחום.

דגימות של **TeslaCrypt** התגלו לראשונה בפברואר 2015, והוואריאנט שלה עובר מוטציות מתמידות במאמץ להתחמק מגילוי. TeslaCrypt מתואר באופן נרחב בתקשורת בתור 'קללת' הגיימרים, מכיוון שהוא מתמקד בקבצים הקשורים למשחקי מחשב (Game saves, פרופילי משתמש ועוד). הסוס הטרויאני תקף בארה"ב, גרמניה, ספרד ובארצות נוספות.

פתרונות אבטחה

על אף כל המנגנונים המתקדמים המיושמים כיום בתוכנות זדוניות, ניתן להפחית בקלות את האיום שתוכנות כופר מפנות כלפיך וכלפי העסק שלך. האסטרטגיה של Kaspersky Lab כנגד מתקפות כופר עושה שימוש במספר [אמצעי מנע](#).

פתרון האבטחה צריך להיות מופעל באופן קבוע עם שכבות אבטחה פעילות רבות ככל האפשר. בנוסף, הפתרון **צריך להיות עדכני**.

בשלב זה לא ניתן לפענח כהלכה קבצים שהוצפנו על ידי תוכנות הצפנה זדוניות בנות זמננו, ולכן הדרך היחידה להישמר מפני התקפה היא על ידי גיבוי קבצים. אולם לא די בגיבוי כללי (לדוגמה, באמצעות Acronis או מוצרים ייעודיים אחרים), גם אם מבוצע באופן שוטף, מאחר שהקבצים שהשתנו לאחרונה אינם מוגנים ועדיין קיים סיכון להחלפתם בקבצים המוצפנים.

הגנה על תחנות קצה מפני מתקפות כופר

זו אחת הסיבות שבגללן מוצרי Kaspersky Lab מכילים את טכנולוגיית Kaspersky System Watcher. System Watcher המורץ בתחנה מנתח את נתוני האירועים הרלוונטיים של המערכת, לרבות מידע על שינויים שנערכו בקבצים. בעת זיהוי של יישום חשוד שמנסה לפתוח קבצים אישיים של המשתמש, השירות יוצר באופן מיידי עותק גיבוי מוגן של הקובץ המותקף. אם היישום מזהה כתוכנה זדונית מסוג Crypto-locker (או מכל סוג אחר), Kaspersky System Watcher מחזיר לאחור את כל השינויים הבלתי מורשים. כל מה שתראה הן הודעות שמציינות את ביצוע התהליך המתואר – לא חלים שיבושים בעבודה ואיך נדרש לעשות מאומה.

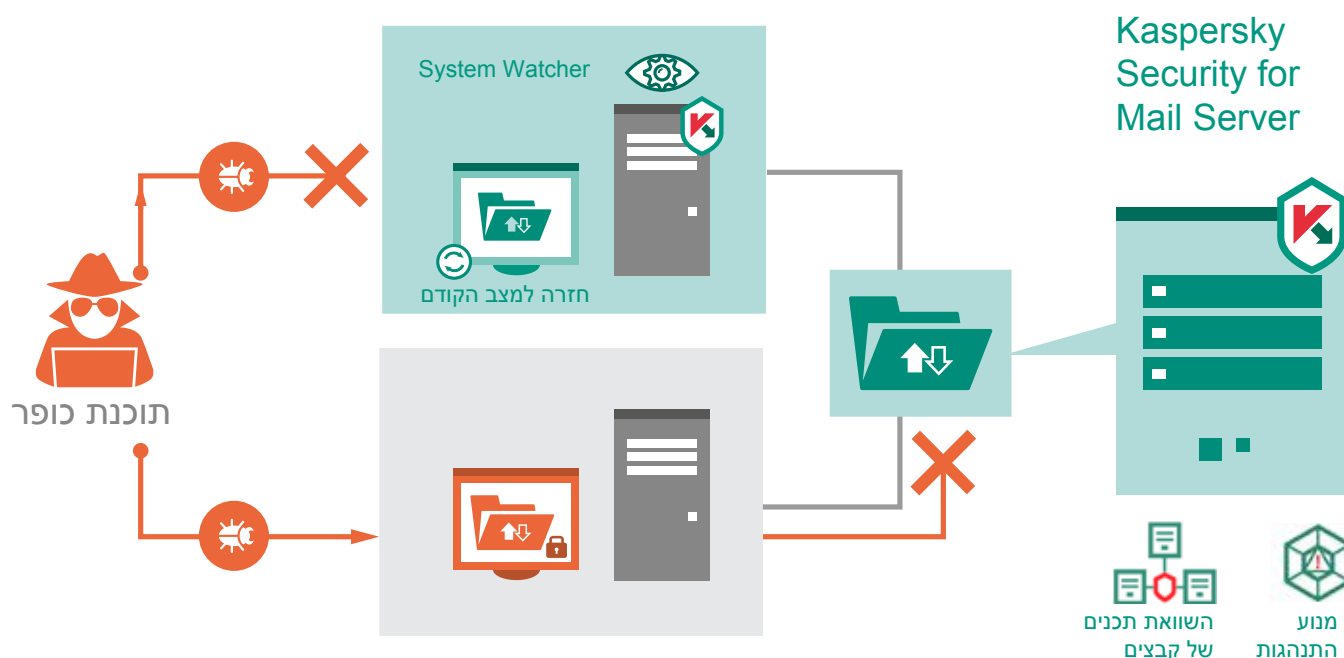
Kaspersky System Watcher שומר את הנתונים במצב בטוח ומסכל את מזימת עברייני האינטרנט לסחוט כספי כופר שמזינים את הפעילות הנפשעת ומעודדים יצירה של תוכנות זדוניות נוספות.

שירותים נוספים המורצים בתחנה מבית Kaspersky Lab להפחתת סיכוני Crypto-locker מבוססים על יצירת כללי Application Startup Control (בקרת הפעלת יישומים), שמונעים הפעלה של יישומים בלתי מורשים.

פתרון להגנה על שרתים מפני מתקפות כופר

שרתים מארחים מסוימים במערך האבטחה ההיקפי עשויים לעשות שימוש בתיקיות SMB/CIFS בשרתים ארגוניים. לא בכל שרת מארח קיים System Watcher במצב פעיל. שרתים מסוימים עשויים להיות בלתי מוגנים או שכלי ההגנה שלהם אינם כוללים פונקציית הגנה מפני תוכנות כופר. במקרה כזה, כל Cryptor שחודר למערכת באמצעות דוא"ל ישפיע גם הוא על תיקיות משותפות שנמצאות בשרתי הארגון. בתרחיש זה, ניתן להגן על הנתונים באמצעות תוכנת אבטחה בצד השרת בלבד.

פונקציית ההגנה מפני תוכנות כופר מבית Kaspersky Lab מיועדת לנקודות קצה, ויותר מכך – לשרתי Windows. הפתרון Kaspersky Security for Windows Server משלב רובד הגנה חדש נוסף שפותח במיוחד לצורך הגנה מפני איומי Cryptor. הפתרון סורק את תיקיות הנתונים שנבחרו, לרבות משאבי שיתוף קבצים, ותוך כדי כך **משווה את התוכן של כל אחד מהקבצים לפני** כל ניסיון גישה וגם לאחר מכן. ברור שה-Crypto-lockers משנים באופן דרמטי את תוכן הקבצים עקב תהליך ההצפנה שבוצע! לפיכך, מנגנון הפעולה האמור יזהה כמעט בלי יוצא מהכלל את הנוכחות של תוכנת כופר ויחסום את המשך פעולתה.



בנוסף לגילוי, Kaspersky Security for Windows Server כולל גם מנגנון מניעה. פרוטוקולי SMB/CIFS אינם מסוגלים לספק מידע על התהליך המתרחש בשרת של תוכנת הכופר, אך באפשרותנו להשיג את כתובת ה-IP של השרת. בהמשך, טכנולוגיית **Host Blocker** מסוגלת למנוע מהשרת המארח הנגוע לפעול על תיקיות משותפות.

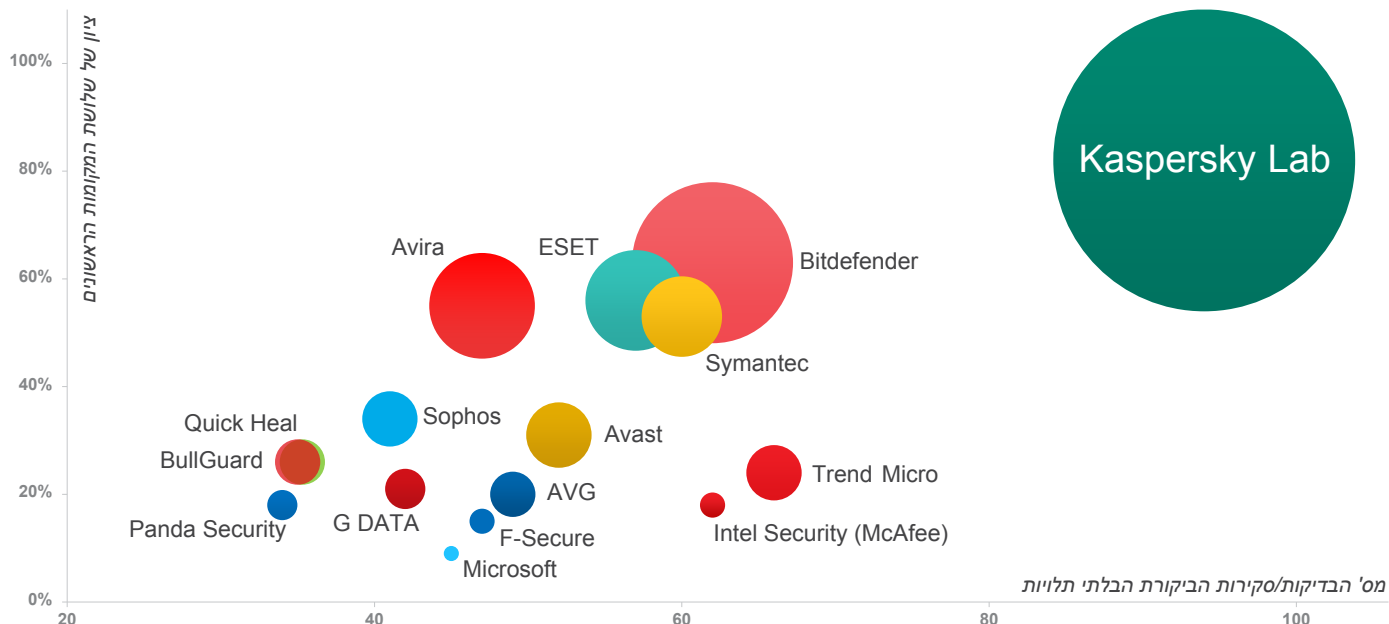
הצפנה חוקית של תיקיות בשרתים מסוימים עשויה להתבצע במסגרת הפעילות הכשרה של מערך האבטחה הארגוני. Kaspersky Security for Windows Server **מאפשר למנהל המערכת להוסיף כללי החרגה** לספריות שבהן אמורה הצפנה זו להתבצע.

לא משאירים אבנים לא הפוכות – אבטחה מפני מתקפות כופר באמצעות Kaspersky Lab

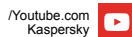
מרחב האימונים מתפתח בהתמדה, ו-Kaspersky Lab מתחייבת לעמוד בקצב יצירת האימונים החדשים ולספק אבטחה רב-שכבתית להגנה על הלוקוחות שלנו. אנו מוכנים לטפל בבעיית תוכנות הכופר בתחנות עבודה (Kaspersky System Watcher) וגם בצד השרת (Kaspersky Security for Windows Server).

Kaspersky Lab מחדשת בקביעות את ארסנל הטכנולוגיות שלה המושתת על מודיעין האבטחה המוכח שלנו. הוכחות להצהרות הביצועים שלנו ניתן למצוא בתוצאות בדיקות בלתי תלויות ובחוות דעת של אנליסטים (TOP3).

בשנת 2015 השתתפו המוצרים של Kaspersky Lab ב-94 בדיקות וסקירות ביקורת עצמאיות. מוצרינו זכו 60 פעם במקום הראשון והגיעו לשלישייה המובילה 77 פעמים.



כל המידע על מדדי TOP3 בקישור www.kaspersky.com/top3



/Youtube.com
Kaspersky



/Facebook.com
Kaspersky



/Twitter.com
Kaspersky

חפש שותף בקרבת מקום:
www.kaspersky.com/buyoffline

כל המידע על אבטחה באינטרנט:
www.securelist.com

Kaspersky Lab, Moscow, Russia
www.kaspersky.com