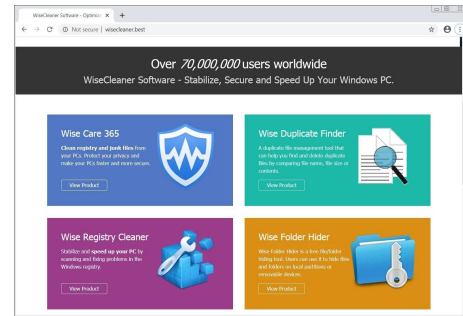
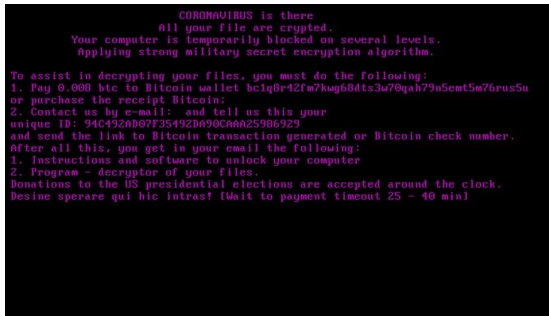


17/03/2020

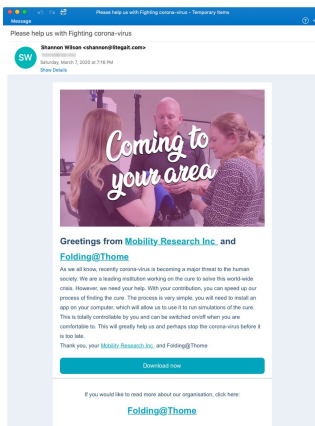
הגנת הסייבר ונגיף הקורונה (Covid 19) - עדכון יומי 17/03/2020

1. תוכנת כופר חדשה בשם CoronaVirus, שמאפשרת גניבת סיסמאות וקבצי cookies וגם נועלת קבצים שניתן לשחררם רק באמצעות תשלום ביטקוין - מופצת דרך האתר המוצג בתמונה (wisecleaner.best). אם נתקלתם באתר (המוצג כאן) אל תפעילו את הקבצים הבאים: **WSHSetup.exe, file1.exe, file2.exe**.



2. קמפיין phishing חדש מנצל את בהלת הקורונה העולמית.

הקמפיין מציג את עצמו כיוזמה לאגד משאבי מחשוב של ממשותמים רבים, כדי לתת עזרה למחקר על יורוס הקורונה - ואכן קיים קמפיין אמיתי כזה. בפועל, קמפיין ה-phishing מספק כתובת מייל מזויפת במטרה להערים על משתמשים דרך גניבת פרטי זיהוי אישיים, סיסמאות ופרטי אשראי שלהם. אם נתקלתם במייל מהכתובת **Folding@Thome** אל תפתחו אף קישור.



3. שיתוף פעולה נגד פייק ניוז על נגיף הקורונה.

פעילות משותפת בין ענקיות המדיה החברתית העולמיות Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter ו-Youtube החלה כדי לצמצם הפצת תכנים מזויפים ופייק ניוז בנושא הקורונה. בשבועות האחרונים, ידיעות כוזבות מופצות בקצב מהיר והחברות משתפות פעולה על מנת ליצור מנגנוני עדכון אמינים, בהתאם למידע המתפרסם על ידי מוסדות בריאות בעולם.

1

<https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/>

2

<https://www.proofpoint.com/us/threat-insight/post/new-redline-stealer-distributed-using-corona-virus-themed-email-campaign>

3 <https://twitter.com/fbnewsroom/status/1239703497479614466>