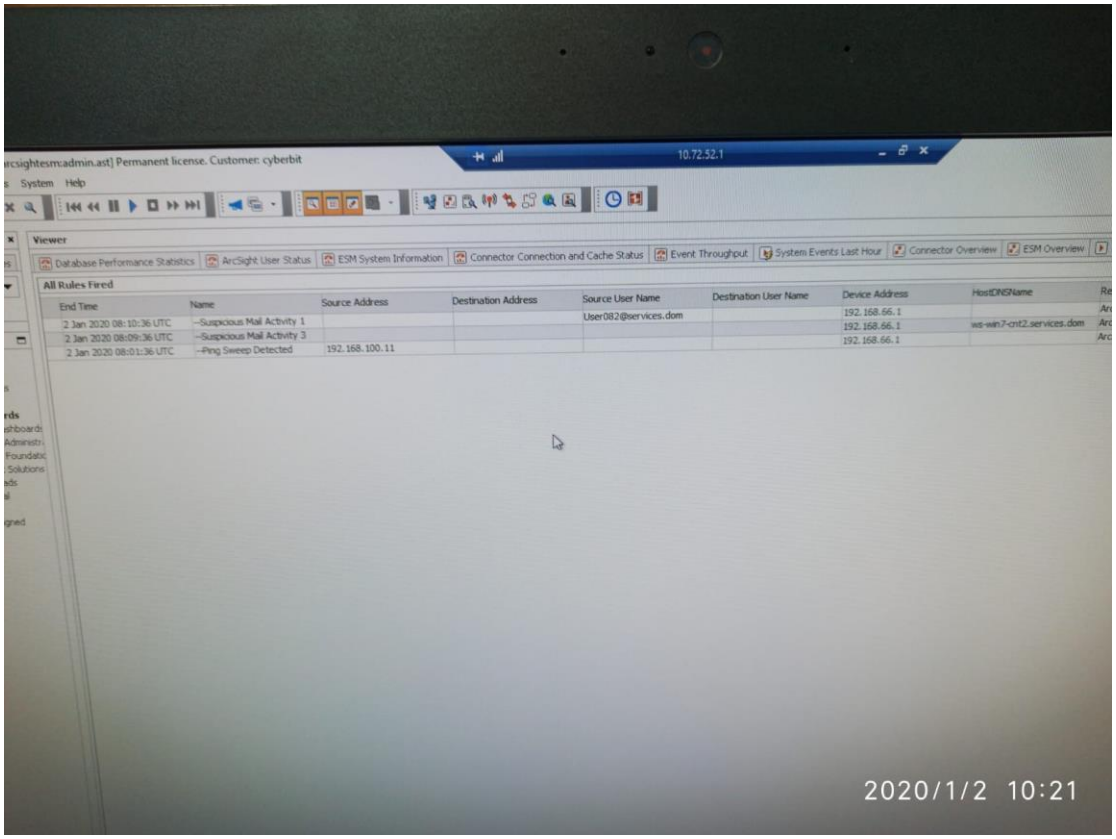
דוח אירוע

מגיש: דור לבקוביץ – 203565015

שם התרחיש: DNS Poisoning

תהליך ההתקפה – התוקף ביצע הרעלת DNS וכך מישהו מהארגון התחבר לאתר המשויך לתוקף מה שגרם לירידה של קובץ זדוני למחשב ללא ידיעתו ובכך יצר בעצם BACKDOOR לרשת הפנימית של הארגון והצליח לשים יד על מיילים של עובדים בחברה.

תהליך הזיהוי – לאחר בדיקה בתוכנת ה- arksight גילינו תנועה חשודה בשרת המיילים של החברה ולאחר בדיקה מעמיקה נוכחנו לגלות בשרת המיילים שיש תנועה גדולה של מיילים שנשלחים החוצה.



תהליך ההגנה הראשוני – התחברנו לשרת המיילים על מנת לברר מה נשלח, לאן נשלח, כמה נשלח ומתי. ובנוסף לבדוק איך נוצר BACKDOOR בארגון.

תהליך הגנה מונעת – חיזוק ההרשאות בשרת ה-DNS, הדרכות ותזכורים של עובדי החברה כל תקופת זמן מסויימת על חשיבות אבטחת מידע וריענונים של סכנות מניעתם, והכי חשוב לחסום גישה של עובדי החברה להוריד תוכנות ולהתקינן ללא הרשאה מגורם מוסמך.

כלים חדשים שפיתחתם/השתמשתם – לא היה כלי חדש בתרחיש זה

אופן עבודת הצוות – עבודה מבולגנת של הצוות חוסר סינכרון ואי עידכון של ממצאים חדשים המובילים לפיתרון.