Network Forensics Report – Agent Tesla Malware Traffic Analysis

By : Elian Mingov

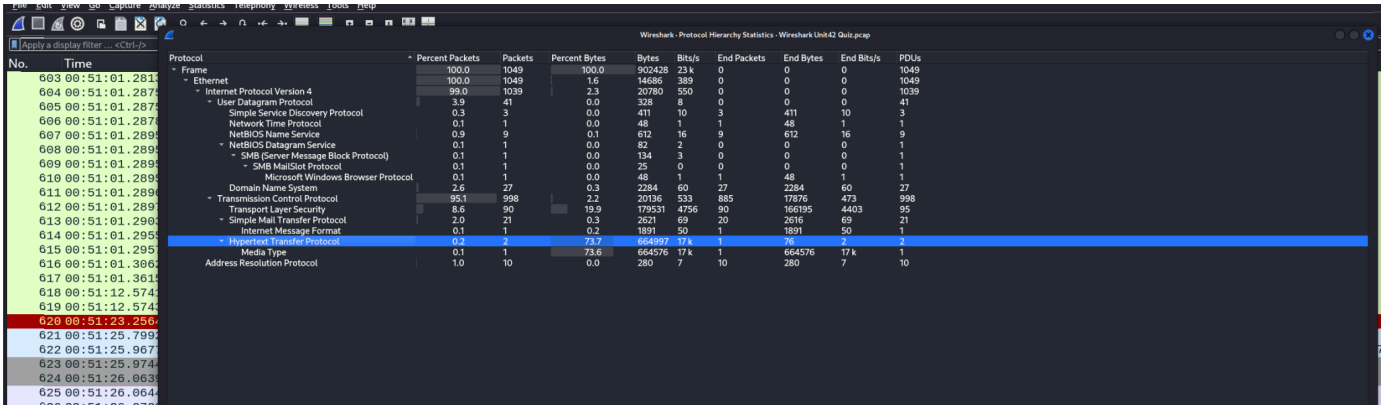
רקע - קובץ התעבורה שסופק (PCAP) מתעד תקשורת של מחשב בעל מערכת הפעלה Windows 11 שנדבק בנוזקת Agent Tesla.
הקובץ התקבל כחלק ממעבדת ניתוח של חברת Palo Alto יחידה 42, ונמסר לנו כבסיס לחקירה של תהליך שליחת המידע מהמחשב המודבק לשרת התוקף.
הנתונים שניתנו מראש מצביעים על כך שהמחשב כבר נדבק – והמטרה כעת היא לנתח את התעבורה שלאחר ההדבקה, לזהות את פרטי המחשב, את המידע שנשלח, ואת הדרך בה פעלה הנוזקה.

מהי הנוזקה Agent Tesla:
Agent Tesla היא נוזקה נפוצה מסוג Remote Access Trojan. מטרתה העיקרית היא לרגל אחרי המשתמש ולהעביר לתוקף מידע רגיש מהמחשב הנגוע. היא מתמקדת בגניבת סיסמאות, תיעוד הקשות מקלדת, לכידת צילומי מסך, והעברת המידע החוצה,המידע עובר במרבית המקרים דרך הפרוטוקולים-
SMTP - Simple Mail Transfer Protocol
FTP - File Transfer Protocol
HTTPS- HyperText Transfer Protocol Secure
אופן הפצת הנוזקה בדרך כלל עם סיומת .exe.
נוזקות דומות ל-Agent Tesla:
FormBook -אותו רעיון, לוכד סיסמאות והקשות מקלדת
LokiBot - גניבת סיסמאות מדפדפנים, גניבת מידע מתוכנות אימייל וגניבת קבצים ספציפיים

מטרת החקירה:
מטרת החקירה היא לאתר פעילות זדונית בתוך קובץ תעבורת רשת בעזרת Wireshark, לזהות את המחשב שנפגע, להבין כיצד הועבר המידע מתוך המערכת, ולבצע מיפוי מלא של שלבי התקיפה.

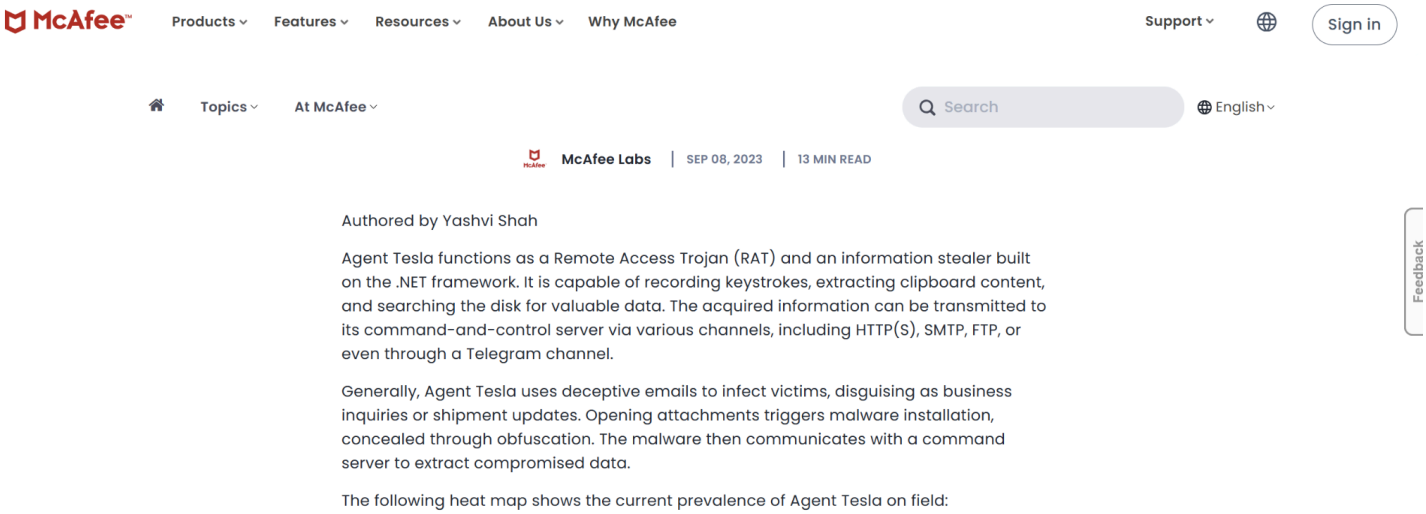
ניתוח תעבורה חשודה/תחילת תהליך החקירה :

נבדוק את הפרוטוקלים הקיימים דרך "Protocol Hierarchy"-



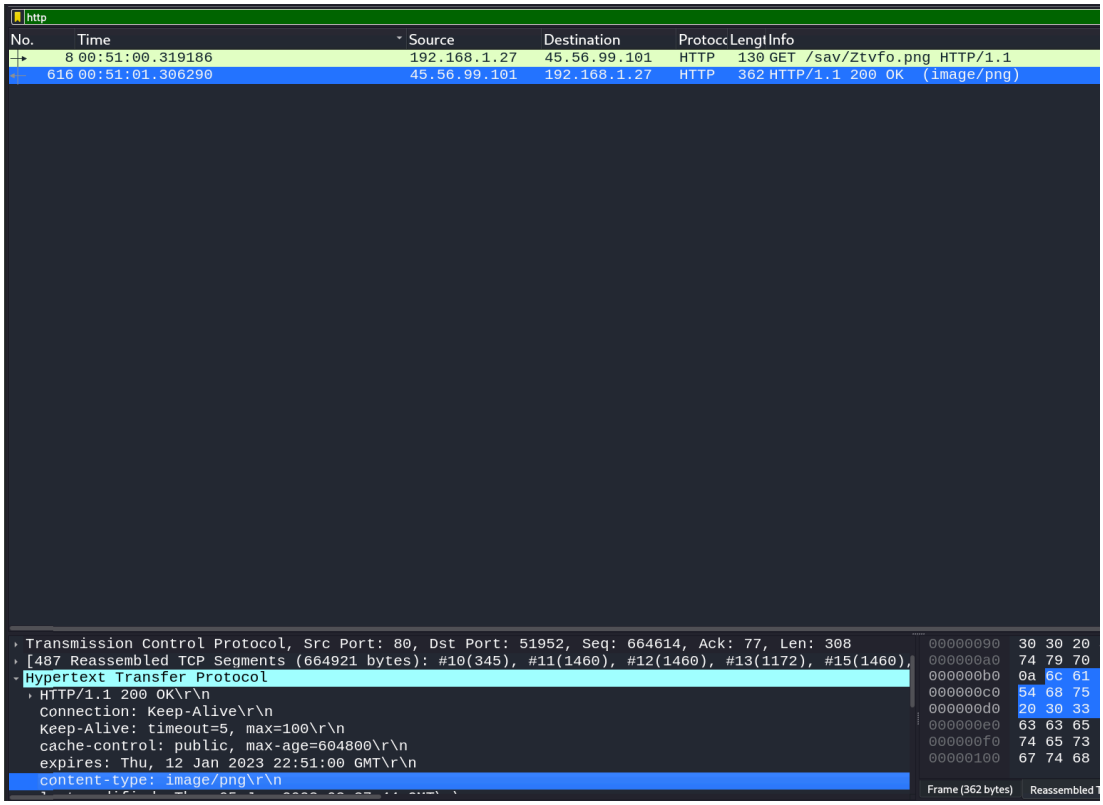
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	1049	100.0	902428	23 k	0	0	0	1049
Ethernet	100.0	1049	1.6	14686	389	0	0	0	1049
Internet Protocol Version 4	99.0	1039	2.3	20780	550	0	0	0	1039
User Datagram Protocol	3.9	41	0.0	328	8	0	0	0	41
Simple Service Discovery Protocol	0.3	3	0.0	411	10	3	411	10	3
Network Time Protocol	0.1	1	0.0	48	1	1	48	1	1
NetBIOS Name Service	0.9	9	0.1	612	16	9	612	16	9
NetBIOS Datagram Service	0.1	1	0.0	82	2	0	0	0	1
SMB (Server Message Block Protocol)	0.1	1	0.0	134	3	0	0	0	1
SMB MailSlot Protocol	0.1	1	0.0	25	0	0	0	0	1
Microsoft Windows Browser Protocol	0.1	1	0.0	48	1	1	48	1	1
Domain Name System	2.6	27	0.3	2284	60	27	2284	60	27
Transmission Control Protocol	95.1	998	2.2	20136	533	885	17876	473	998
Transport Layer Security	8.6	90	19.9	179531	4756	90	166195	4403	95
Simple Mail Transfer Protocol	2.0	21	0.3	2621	69	20	2616	69	21
Internet Message Format	0.1	1	0.2	1891	50	1	1891	50	1
Hypertext Transfer Protocol	0.2	2	73.7	664997	17 k	1	76	2	2
Media Type	0.1	1	73.6	664576	17 k	1	664576	17 k	1
Address Resolution Protocol	1.0	10	0.0	280	7	10	280	7	10

ניתן לראות כי בקובץ התעבורה קיימת פעילות במספר פרוטוקולים, ביניהם: HTTP, SMTP, IMF, DNS ואחרים.
מתוך כלל הפרוטוקולים, תעבורת HTTP העבירה קובץ מדיה (PNG) במשקל של כ 650KB,
לפי בלוג שנכתב באתר של McAffe הנוזקה Agent Tesla היא נוזקה ששולחת את המידע הגנוב דרך פרוטוקולים כגון FTP/HTTPS/SMTP ואפילו דרך ערוצי טלגרם :

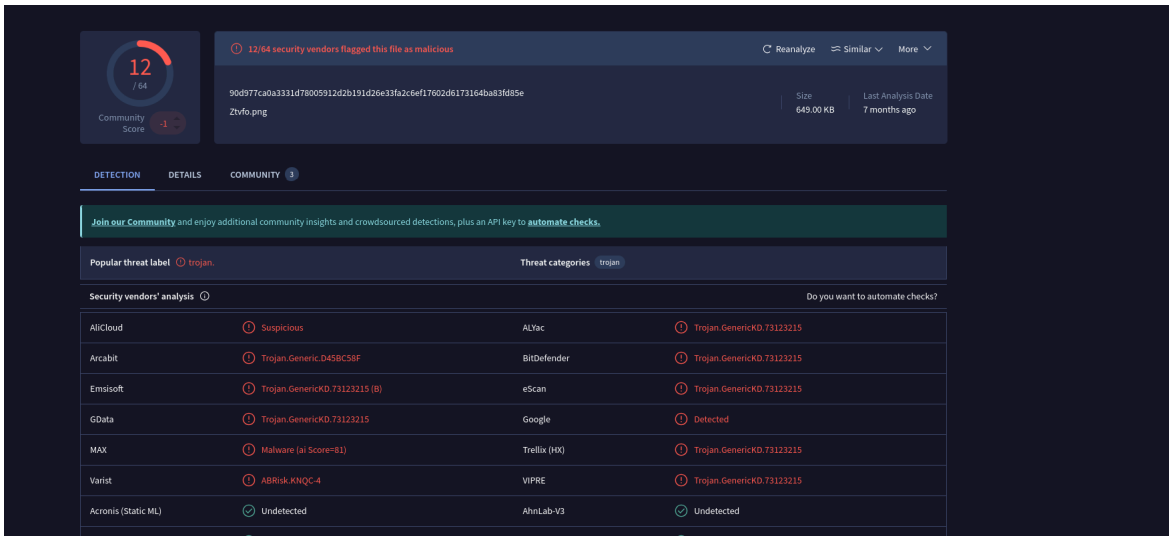


לפי "Protocol Hierarchy" נראה שבאמת קיימת תעבורה בפורוטוקול SMTP.
נסנן כך שנוכל לראות רק את הפרוטוקולים של HTTP ונחפש את התעבורה שמראה שקובץ מדיה ירד בהצלחה ונבדוק אותו כדי לוודא האם אכן מדובר בקובץ זדוני.

חיפוש מקור ההדבקה:



נוכל לראות כאן שתמונה מסוג "PNG." בשם Ztvfo ירדה בהצלחה ב-12 לינואר 2023 בשעה 22:51:00 מהכתובת - 45.56.99.101 לכתובת - 192.168.1.27 דרך פרוטוקול לא מוצפן (HTTP), מאפיינים אלו כגון הורדת קובץ מפרוטוקול לא מוצפן (HTTP) עם שם לא סטנדרטי וכתובת IP חיצונית מהווים IOC נשמור את הקובץ ונעלה ל-VirusTotal על מנת לוודא שהאינדיקציה נכונה



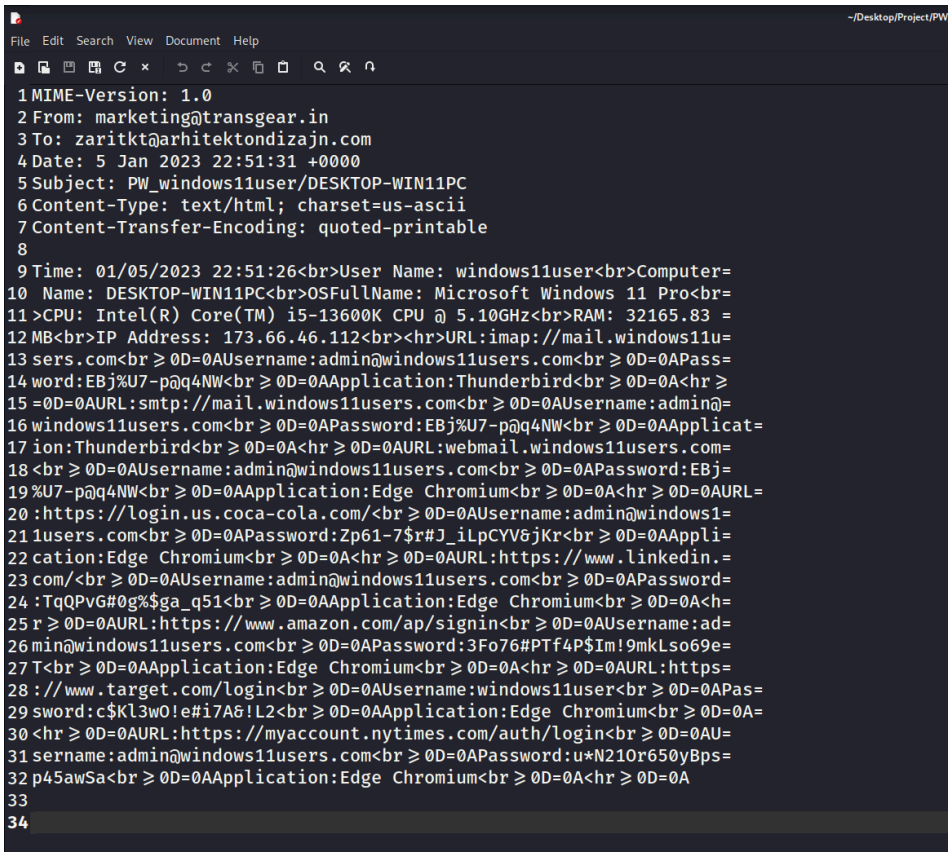
תוצאות הבדיקה באתר VirusTotal מעלות את הסבירות שאכן מדובר בקובץ זדוני, מכיוון שהוא זוהה כחשוד על ידי 12 מנועי אנטי־וירוס שונים.

מסקנות עד כה וניתוח הקובץ בפורמט imf-

מתוך ניתוח תעבורת הרשת, ניתן להבין כי המחשב שכתובת הIP שלו הוא 192.168.1.27 הוא המחשב שנדבק.
לאחר זיהוי זהות המחשב, נשמור קובץ הדוא"ל שנשלח ממנו, בפורמט .imf, אשר כולל את תוכן ההודעה המלא שנשלח מהמערכת המודבקת אל הכתובת החיצונית.
ניתוח תוכן ההודעה חושף את הפרטים הבאים:

Name: windows11user
Computer Name: DESKTOP-WIN11PC
CPU: Intel(R) Core(TM) i5-13600K CPU @ 5.10GHz
RAM: 32165.83MB
IP Address: 173.66.46.112
Time: 01/05/2023

הפרטים מעלה כוללים את החומרה של המחשב שהודבק, בנוסף לכתובת הIP שלו ושם משתמש המחשב, ניתן לראות בצילום מסך את הקובץ שממנו הוצא המידע.



מתוך תוכן ההודעה, ניתן לראות כי הנוזקה שלפה ושלחה שמות משתמשים וסיסמאות מאתרים ושירותים שונים, לדוגמא :
חשבונות דוא"ל (mail.windows11users.com
שירותי Webmail - webmail.windows11users.com
אתרים חיצוניים כמו:
login.us.coca-cola.com
linkedin.com ועוד…

אימות נוסף-

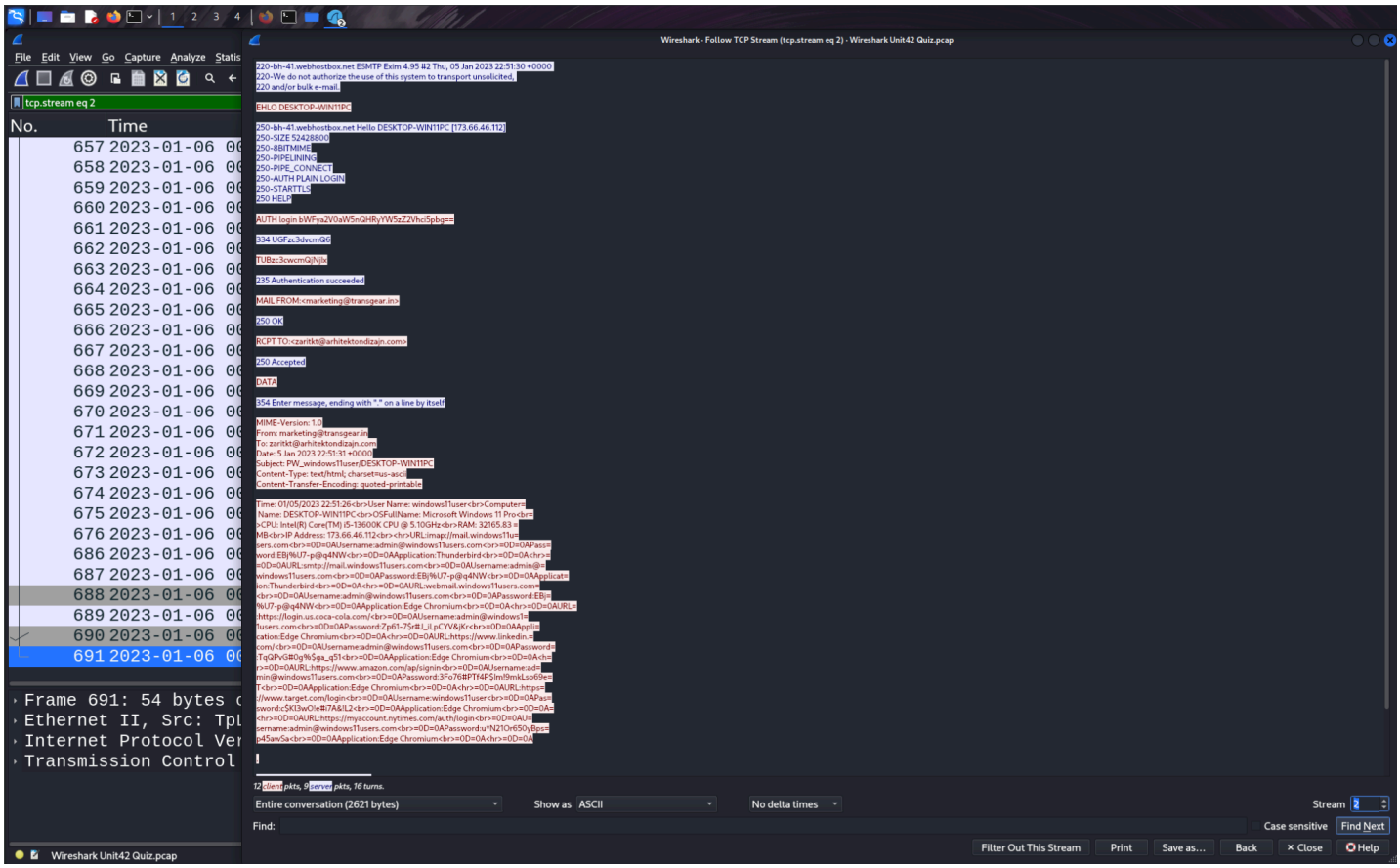
כדי לוודא שלא דלפו נתונים נוספים מעבר למה שתועד בהודעת הדוא"ל שנמצאה, בוצע סינון תעבורת הרשת לפי הפילטר: SMTP

בהמשך לכך בוצע שימוש בפונקציה:

Follow → TCP Stream

על מנת לאחד את כלל התעבורות המרכיבות שיחה אחת מול שרת הדואר, ומציגה את ההודעה בשלמותה.

מתוך סך של 10 סטרימים של TCP, נמצא כי רק סטרים אחד הכיל תוכן משמעותי שהוא Stream 2-



צורת שאר ה-Streams :

שאר הסטרימים היו מוצפנים ונראים מהצורה הבאה-

מהתוכן שנשלח על ידי הנוזקה, ניתן לראות שנגנבו שמות משתמשים וסיסמאות לחשבונות שונים של המשתמש.
בין השירותים שנפגעו ניתן למצוא:

- כתובות מייל פנים ארגוניות
- אתרים חיצוניים כמו Coca-Cola, LinkedIn ו NYTimes
- ועוד אתרים נוספים

המידע נשלח כטקסט לא מוצפן אל כתובת דוא"ל חיצונית - "zariktk@arhitektondizajn.com" שנשלטת ככל הנראה על ידי התוקף.

סיכום ביניים -

ניתוח קובץ ה־PCAP שנמסר הוביל לזיהוי תעבורת רשת של מחשב שנדבק בנוזקת Agent Tesla.
זוהתה הורדה של קובץ מסוג PNG מחוץ לרשת, אשר אומת כקובץ זדוני על ידי 12 מנועי אנטי־וירוס.
לאחר ההדבקה, המחשב שלח הודעת דוא"ל הכוללת מידע כגון פרטי התחברות, חומרה, IP חיצוני ועוד – אל כתובת דוא"ל חיצונית "zariktk@arhitektondizajn.com".
בוצע ניתוח של כל תעבורת ה־SMTP, ונמצא כי רק Stream מספר 2 כלל את המידע המלא שנשלח החוצה, שאר הסטרימים היו מוצפנים.
המידע כלל פרטי גישה לחשבונות דוא"ל, אתרים חיצוניים ושירותים נוספים, ונשלח כטקסט גלוי.

מיפוי לפי MITRE ATT&CK

שלב	טכניקה	מזהה	ממצאים מהחקירה
Initial Access	Spear phishing Attachment	T1566.001	קובץ PNG זדוני (Ztvfo.png) הורד דרך HTTP – כנראה מייל פישינג או הורדה ממקור מזויף
Execution	Malicious File Execution	T1204.002	הרצה של קובץ שהורד כקובץ תמונה אך הכיל נוזקה
Defense Evasion	Masquerading	T1036	קובץ נראה כתמונה (image/png) אך בפועל מכיל קוד זדוני
Credential Access	Input Capture: Keylogging / Credential Dumping	T1056.001 / T1555	הודעת הדוא"ל כוללת שמות משתמשים וסיסמאות מאתרים שונים
Collection	Data from Information Repositories	T1213	נגנבו סיסמאות משירותי Webmail, LinkedIn, Target ועוד
Exfiltration	Exfiltration Over Email	T1048.003	המידע נשלח באמצעות SMTP לכתובת zariktk@arhitektondizajn.com
Command and Control	לא זוהה במסגרת התחקור		

סיכום והמלצות

סיכום החקירה:
קובץ ה־PCAP שנבדק תיעד תקיפה שבוצעה על מחשב בעל מערכת הפעלה Windows 11 באמצעות נוזקת Agent Tesla.
התקיפה כללה הורדה של קובץ זדוני במסווה של תמונה, איסוף מידע רגיש מהמחשב, ושליחתו אל כתובת דוא"ל בשליטת התוקף.
במסגרת החקירה זוהו פרטי מערכת, סיסמאות מחשבון מייל ואתרים חיצוניים, ותהליך שליחת המידע התבצע בפרוטוקול SMTP.
בנוסף בוצע טבלת מיפוי לפי MITRE ATT&CK.

המלצות למניעת מקרים דומים:
הדרכת משתמשים לזיהוי קבצים חשודים

הטמעת פתרון EDR לזיהוי וחסימה אוטומטית של קבצים זדוניים

שימוש בפתרונות Web Filtering למניעת גישה לאתרים זדוניים או להורדת קבצים חשודים

לסיום:
הדוח מבוסס על ניתוח קובץ תעבורה PCAP מתוך מעבדת תרגול של חברת פאלו אלטו יחידה 42.
במסמך מוצג מה עשתה נוזקת Agent Tesla על מחשב שנדבק, כולל שלבי ההדבקה, גניבת המידע ושליחתו החוצה.
לבסוף, מוצעות מסקנות והמלצות שיעזרו למנוע מקרים דומים בעתיד.