

## **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 הפרוטוקולים הקיימים דרך "Protocol Hierarchy"

No.	Time	Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bit/s	End Packets	End Bytes	End Bit/s	PDUs
603	00:51:01.281	Frame	100.0	1049	100.0	902428	23 k	0	0	0	1049
604	00:51:01.287	Ethernet	100.0	1049	1.6	14686	389	0	0	0	1049
605	00:51:01.287	Internet Protocol Version 4	99.0	1039	2.3	20780	550	0	0	0	1039
606	00:51:01.287	User Datagram Protocol	3.9	41	0.0	328	8	0	0	0	41
607	00:51:01.289	Simple Service Discovery Protocol	0.3	3	0.0	411	10	3	411	10	3
608	00:51:01.289	Network Time Protocol	0.1	1	0.0	48	1	1	48	1	1
609	00:51:01.289	NetBIOS Name Service	0.9	9	0.1	612	16	9	612	16	9
610	00:51:01.289	NetBIOS Datagram Service	0.1	1	0.0	82	2	0	0	0	1
611	00:51:01.289	SMB Server Message Block Protocol	0.1	1	0.0	134	3	0	0	0	1
612	00:51:01.289	SMB Mailslot Protocol	0.1	1	0.0	25	0	0	0	0	1
613	00:51:01.290	Microsoft Windows Browser Protocol	0.1	1	0.0	48	1	1	48	1	1
614	00:51:01.290	Domain Name System	2.6	27	0.3	2284	60	27	2284	60	27
615	00:51:01.295	Transmission Control Protocol	95.1	998	2.2	20136	533	885	17876	473	998
616	00:51:01.295	Transport Layer Security	8.6	90	19.9	179531	4756	90	166195	4403	95
617	00:51:01.296	Simple Mail Transfer Protocol	2.0	21	0.3	2621	69	20	2616	69	21
618	00:51:01.295	Internet Message Format	0.1	1	0.2	1891	50	1	1891	50	1
619	00:51:01.295	Hypertext Transfer Protocol	0.2	2	73.7	664597	17 k	1	76	2	2
620	00:51:01.296	Media Type	0.1	1	23.6	664576	17 k	1	664576	17 k	1
621	00:51:01.306	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 McAfee הנוזקה Agent Tesla היא נוזקה ששולחת את המידע הגנוב דרך פרוטוקולים כגון FTP/HTTPS/SMTP ואפילו דרך ערוצי טלגרם :

**McAfee** Products Features Resources About Us Why McAfee Support Sign in

Topics At McAfee Search English

**McAfee Labs** | SEP 08, 2023 | 13 MIN READ

Authored by Yashvi Shah

Agent Tesla functions as a Remote Access Trojan (RAT) and an information stealer built on the .NET framework. It is capable of recording keystrokes, extracting clipboard content, and searching the disk for valuable data. The acquired information can be transmitted to its command-and-control server via various channels, including HTTP(S), SMTP, FTP, or even through a Telegram channel.

Generally, Agent Tesla uses deceptive emails to infect victims, disguising as business inquiries or shipment updates. Opening attachments triggers malware installation, concealed through obfuscation. The malware then communicates with a command server to extract compromised data.

The following heat map shows the current prevalence of Agent Tesla on field:

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

## חיפוש מקור ההדבקה:

No.	Time	Source	Destination	Protocol	Length	Info
8	00:51:00.319186	192.168.1.27	45.56.99.101	HTTP	130	GET /sav/Ztvfo.png HTTP/1.1
616	00:51:01.306290	45.56.99.101	192.168.1.27	HTTP	362	HTTP/1.1 200 OK (image/png)

<ul style="list-style-type: none"> <li>Transmission Control Protocol, Src Port: 80, Dst Port: 51952, Seq: 664614, Ack: 77, Len: 308</li> <li>[487 Reassembled TCP Segments (664921 bytes): #10(345), #11(1460), #12(1460), #13(1172), #15(1460),</li> <li><b>Hypertext Transfer Protocol</b></li> <li>HTTP/1.1 200 OK\r\n</li> <li>Connection: Keep-Alive\r\n</li> <li>Keep-Alive: timeout=5, max=100\r\n</li> <li>cache-control: public, max-age=604800\r\n</li> <li>expires: Thu, 12 Jan 2023 22:51:00 GMT\r\n</li> <li><b>content-type: image/png\r\n</b></li> </ul>	<pre> 00000000 30 30 20 000000a0 74 79 70 000000b0 0a 5c 01 000000c0 54 68 75 000000d0 20 30 33 000000e0 63 63 65 000000f0 74 65 73 00000100 67 74 68 </pre>
---	--

Frame (362 bytes) Reassembled

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

12

/ 64

Community Score

-1

12/64 security vendors flagged this file as malicious

Reanalyze

Similar

More

90d977ca0a3331d78005912d2b191d26e33fa2c6ef17602d6173164ba83f485e

Ztvfo.png

Size

649.00 KB

Last Analysis Date

7 months ago

DETECTION

DETAILS

COMMUNITY 3

Join our Community

 and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label

trojan

Threat categories

trojan

Security vendors' analysis

Do you want to automate checks?

AliCloud	<div>Suspicious</div>	ALYac	<div>Trojan.GenericKD.73123215</div>
Arcabit	<div>Trojan.Generic.D45BC50F</div>	BitDefender	<div>Trojan.GenericKD.73123215</div>
Emsisoft	<div>Trojan.GenericKD.73123215 (B)</div>	eScan	<div>Trojan.GenericKD.73123215</div>
GData	<div>Trojan.GenericKD.73123215</div>	Google	<div>Detected</div>
MAX	<div>Malware (ai Score=B1)</div>	Trellix (HX)	<div>Trojan.GenericKD.73123215</div>
Varist	<div>ABRisk.KMQC-4</div>	VIPRE	<div>Trojan.GenericKD.73123215</div>
Acronis (Static ML)	<div>Undetected</div>	AhnLab-V3	<div>Undetected</div>

תוצאות הבדיקה באתר VirusTotal מעלות את הסבירות שאכן מדובר בקובץ זדוני, מכיוון שהוא זוהה כחשוד על ידי 12 ממועי 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 המודבקות 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.

```
File Edit Search View Document Help
1 MIME-Version: 1.0
2 From: marketing@transgear.in
3 To: zaritkt@arhitektondizajn.com
4 Date: 5 Jan 2023 22:51:31 +0000
5 Subject: PW_windows11user/DESKTOP-WIN11PC
6 Content-Type: text/html; charset=us-ascii
7 Content-Transfer-Encoding: quoted-printable
8
9 Time: 01/05/2023 22:51:26<br>User Name: windows11user<br>Computer=
10 Name: DESKTOP-WIN11PC<br>OSFullName: Microsoft Windows 11 Pro<br>
11 >CPU: Intel(R) Core(TM) i5-13600K CPU @ 5.10GHz<br>RAM: 32165.83 =
12 MB<br>IP Address: 173.66.46.112<br><hr>URL:imap://mail.windows11u=
13 sers.com<br>0D=0AUsername:admin@windows11users.com<br>0D=0APass=
14 word:EBj%U7-p@q4NW<br>0D=0AApplication:Thunderbird<br>0D=0A<hr>
15 =0D=0AURL:smtp://mail.windows11users.com<br>0D=0AUsername:admin@=
16 windows11users.com<br>0D=0APassword:EBj%U7-p@q4NW<br>0D=0AApplicat=
17 ion:Thunderbird<br>0D=0A<hr>0D=0AURL:webmail.windows11users.com=
18 <br>0D=0AUsername:admin@windows11users.com<br>0D=0APassword:EBj=
19 %U7-p@q4NW<br>0D=0AApplication:Edge Chromium<br>0D=0A<hr>0D=0AURL=
20 :https://login.us.coca-cola.com/<br>0D=0AUsername:admin@windows1=
21 1users.com<br>0D=0APassword:Zp61-7$r#J_iLpCYV6jKr<br>0D=0AAppli=
22 cation:Edge Chromium<br>0D=0A<hr>0D=0AURL:https://www.linkedin.=
23 com/<br>0D=0AUsername:admin@windows11users.com<br>0D=0APassword=
24 :TqQPvG#0g%$ga_q51<br>0D=0AApplication:Edge Chromium<br>0D=0A<h=
25 r>0D=0AURL:https://www.amazon.com/ap/signin<br>0D=0AUsername:ad=
26 min@windows11users.com<br>0D=0APassword:3Fo76#PTf4P$Im!9mkLso69e=
27 T<br>0D=0AApplication:Edge Chromium<br>0D=0A<hr>0D=0AURL:https=
28 ://www.target.com/login<br>0D=0AUsername:windows11user<br>0D=0APas=
29 sword:c$Kl3w0!e#i7A&!L2<br>0D=0AApplication:Edge Chromium<br>0D=0A=
30 <hr>0D=0AURL:https://myaccount.nytimes.com/auth/login<br>0D=0AU=
31 sername:admin@windows11users.com<br>0D=0APassword:u*N210r650yBps=
32 p45awSa<br>0D=0AApplication:Edge Chromium<br>0D=0A<hr>0D=0A
33
34
```

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...

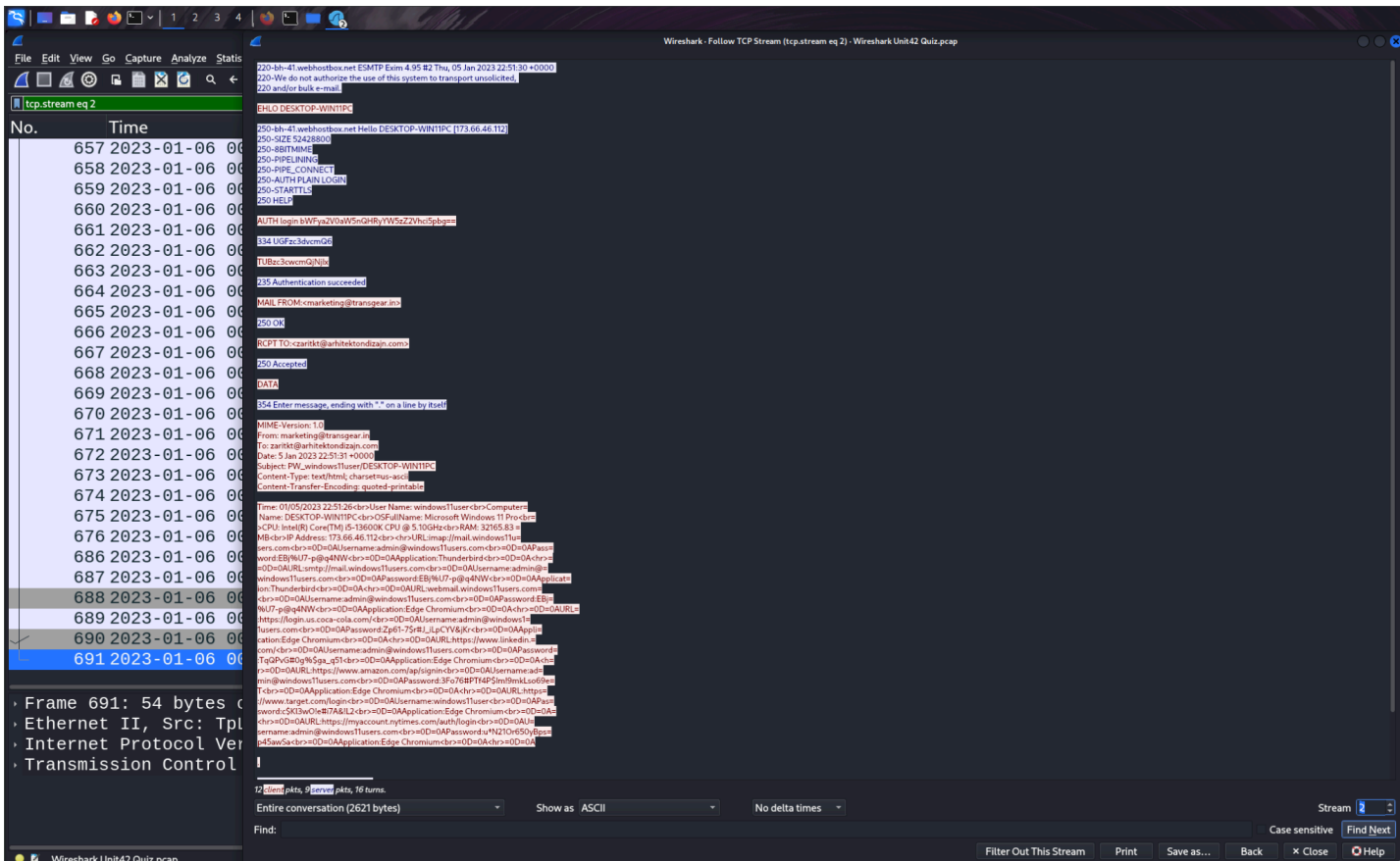
## אימות נוסף-

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 שנגבבו 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 פשינג 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 וסימאות מאתרים שונים
Collection	Data from Information Repositories	T1213	נגבו 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 נזקת 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 וחסמה אוטומטית של קבצים זדוניים

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

### **לסיים:**

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