

מיני-פרויקט – נושאים במערכות הגנה לרשת

כלי הגנה לזיהוי פעילות פוגען בעמדת קצה ע"ב הפעילות התקשורתית המתבצעת בו

ערן אטיאס

אוניברסיטת בן-גוריון בנגב

eranati@post.bgu.ac.il

1. הקדמה

פוגענים רבים (Malware) מבצעים תקשורת עם שרתי ה-Command and Control (נקרא בקיצור C2 או C&C)^[1] המפעילים אותם לצורך קבלת הנחיות פעולה נוספות והעברת מידע רגיש מעמדות הקצה הנתקפת. תקשורת זו מהווה מאפיין שעל-בסיסה ניתן לזהות ולאתר פוגען בעמדת הקצה ובהמשך גם לנטרלו. Threat Intelligence^{[2][3]} זהו מידע אודות מתקפות סייבר, שהתרחשו בעבר או מתרחשות כרגע, המאפשר למשתמשים ולארגונים לעשות בו שימוש כדי להגן על מחשביהם ורשתותיהם. מידע זה הינו ברובו כתובות URL וכתובות IP של שרתים המעורבים בפעילות זדונית וערכי Hash של קבצי פוגענים. כיום ישנם ברשת האינטרנט שירותי Threat Intelligence חנימיים רבים המאפשרים להעריך את הסבירות לכך שכתובת מסוימת מעורבת בפעילות זדונית, ושימוש משולב במספר מקורות מאפשר להעריך את סבירות זו טוב יותר. במסגרת הקורס "נושאים במערכות הגנה לרשת" בחרתי לתכנן ולפתח כלי הגנה המאפשר למשתמש להעריך בסבירות מסוימת את קיומו של פוגען בעמדת קצה ע"ב הפעילות התקשורתית המתבצעת בה, ומהווה השלמה לתוכנת האנטי-וירוס המותקנת. הכלי עושה זאת באמצעות ניטור של כלל כתובות ה-IP איתן מתקשרת עמדת הקצה, בין אם בתקשורת נכנסת ובין אם בתקשורת יוצאת, ביצוע חיפוש שלהן בזמן אמת ובאופן אוטומטי במקורות Threat Intelligence שונים והצגת התוצאות למשתמש, על-מנת שזה יקבל אינדיקציה להיתכנות לקיומו של פוגען בעמדת הקצה שלו.

שפת התכנות בה בחרתי לעשות שימוש בפיתוח הפוגען היא C#, מכיוון שמבין שפות התכנות השונות זוהי השפה בה רמות הידע והניסיון שלי הן הגבוהות ביותר. הפיתוח נעשה בסביבת הפיתוח Visual Studio.

2. ניטור התקשורת

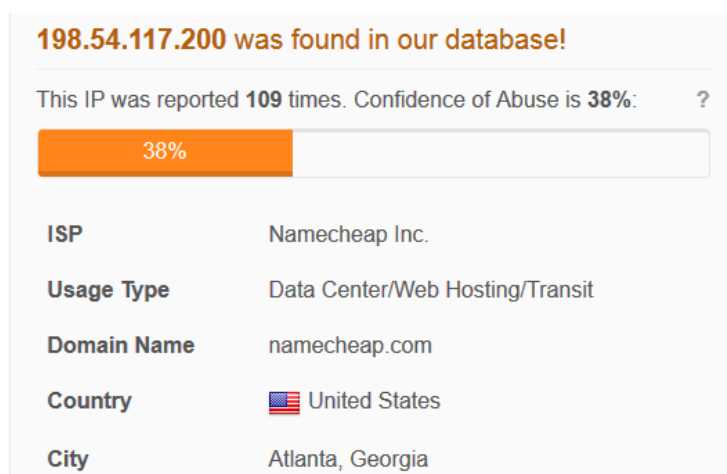
על-מנת למצוא את כתובות ה-IP איתן מתקשרת עמדת הקצה בזמן אמת יש לבצע "הסנפה"^[4] של ה-packets העוברים בכרטיס הרשת. למדתי כיצד לבצע זאת מפרויקט הקוד הפתוח MJsniiffer^[5] שבאתר CodeProject.

עבור כל packet שכלי ההגנה מסניף הוא מחלץ ממנו את כתובת המקור ואת כתובת היעד ולאחר מכן משווה אותן עם כתובת ה-IP של כרטיס הרשת – אם כתובת המקור זהה לכתובת כרטיס הרשת הרי שמדובר בתקשורת יוצאת ויש לבדוק את כתובת היעד במקורות Threat Intelligence, בעוד שאם כתובת היעד זהה לכתובת כרטיס הרשת מדובר בתקשורת נכנסת ויש לבדוק את כתובת המקור. אציין כי הכלי יודע להתעלם מכתובות IP של רשתות פנימיות^[6] (10.0.0.0/8, 172.16.0.0/12 ו-192.168.0.0/16), מהכתובות 0.0.0.0 ו-127.0.0.1 ומכתובות APIPA^[7] (169.254.0.0/16).

3. מקורות Threat Intelligence

בשלב זה נדרשתי לחפש ברשת האינטרנט שירותי Threat Intelligence חינמיים, ועבור כל שירות שמצאתי נדרשתי לבדוק האם ניתן לבצע בו חיפוש באופן תכנותי. זאת אם באמצעות שימוש ב-API, במידה והשירות מספק כזה, ואם באמצעות ניתוח תכנותי של דף ה-HTML של תוצאת חיפוש. כלי ההגנה עושה שימוש ב-**12 מקורות**, דבר שמאפשר להעריך בסבירות גבוהה את היותה של כתובת IP זדונית. בסעיף זה אפרט את השירותים אותם מצאתי כשמישים, ועבור כל אחד שתצלחתי להשמיש לחיפוש תכנותי אסביר כיצד הדבר מתבצע וכיצד הגדרתי עבור הכלי מהי תוצאה חיובית, כלומר מה מאפיין תוצאת החיפוש של כתובת IP המוערכת כזדונית.

א. [AbuseIPDB](#) – נשתמש ב-API אותו מספק השירות. הכלי בודק האם כתובת ה-IP הנבדקת דווחה בשירות ע"י משתמשים על היותה זדונית ב-30 הימים האחרונים. תוצאה חיובית היא כזו בה כתובת ה-IP אכן עולה בחיפוש וערך ה-[Confidence of Abuse](#) שלה הוא לפחות 20% (ולא 0% כדי להימנע מ-False Positives).



ב. [AlienVault Open Threat Exchange \(OTX\)](#) –נשתמש ב-API אותו מספק השירות. הכלי בודק האם ה-Threat Score של כתובת ה-IP הנבדקת גדול מ-0.

IPv4: 198.54.117.200

GENERAL DETAILS	14 PULSES	62 THREAT FINDINGS	500 PASSIVE DNS
Basic Information IP ADDRESS: 198.54.117.200 LOCATION: Los Angeles, United States 🇺🇸 ASN/OWNER: AS22612 Namecheap, Inc. FIRST SEEN: Jan. 21, 2018, 9:45 PM LAST SEEN: Jun. 18, 2018, 6:45 AM GOOGLE SAFE BROWSING: ✓ Not identified as malicious		Threat Summary THREAT SCORE: 2 (out of 7) OBSERVED ACTIVITY: Spamming Previously Malicious	
External Sources Whois VirusTotal			

ג. [Hybrid Analysis](#) – נשתמש ב-API אותו מספק השירות. הכלי בודק האם לשירות ידוע על לפחות קובץ אחד אותו הוא מגדיר כ-malicious המתקשר עם כתובת ה-IP הנבדקת.

ד. [IBM X-Force Exchange](#) –נשתמש ב-API אותו מספק השירות. הכלי בודק האם כתובת ה-IP הנבדקת ידועה בשירות הקשורה ל-Malware, Bots או Botnet Command and Control Server.

Risk 4.3

X-Force IP Report
198.54.117.200

This report does not contain tags. Add tags via the comment box.

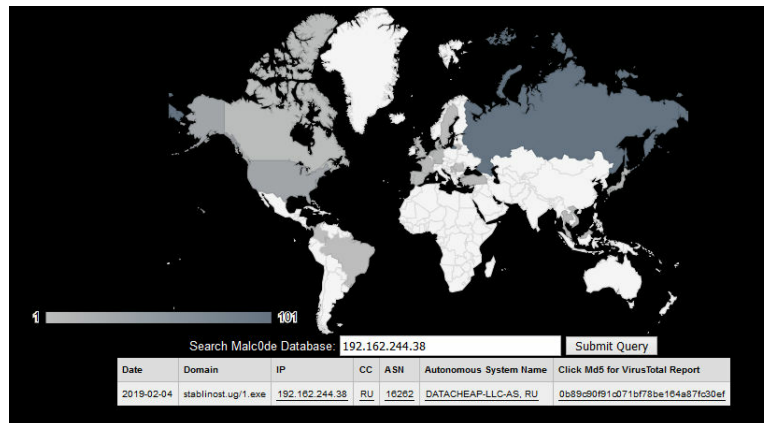
Twitter LinkedIn Facebook

Details	WHOIS Record
Categorization - Anonymization Services (43%) - Malware (43%) - Botnet Command and Control Server (43%) BOT: lokibot	Created: Nov 13, 2015 Updated: Nov 13, 2015 Registrant Organization: Namecheap, Inc. Registrant Country or Region: United States Email: abuse@namecheaphosting.com
Application : No known application Location : United States ASN : AS22612: NAMECHEAP-NET - Namecheap, Inc., US	

ה. [Malc0de](#) – ננתח את דף ה-HTML של תוצאת החיפוש של כתובת ה-IP הנבדקת הנמצאת בכתובת:

<http://malc0de.com/database/index.php?search=<IP>>

הכלי בודק האם עולה בחיפוש לפחות קובץ זדוני אחד המתקשר עם כתובת ה-IP.



1. [Open Threat Intelligence](#) – נשתמש ב-API אותו מספק השירות. הכלי בודק האם כתובת ה-IP הנבדקת דווחה לפחות פעם אחת ב-90 הימים האחרונים כקשורה לפעילות זדונית.
2. [Ransomware Tracker](#) – שירות זה עוקב אחר שרתי C&C המפעילים פוגענים מסוג Ransom. הוא מספק [קובץ טקסט](#) המכיל רשימה עדכנית של כתובות IP של שרתים כאלה. הכלי בודק האם כתובת ה-IP נמצאת ברשימה זו.
- ח. [REScure](#) – שירות זה מספק [קובץ טקסט](#) המכיל רשימה עדכנית של כתובות IP של שרתים המעורבים בפעילות זדונית. הכלי בודק האם כתובת ה-IP נמצאת ברשימה זו.
- ט. [ThreatMiner](#) – נשתמש ב-API אותו מספק השירות. הכלי בודק האם ידוע לשירות על קובץ המתקשר עם כתובת ה-IP הנבדקת שמזוהה כזדוני ע"י תוכנת אנטי-וירוס אחת לפחות.
- י. [URLhaus](#) – שירות זה מספק [קובץ טקסט](#) המכיל רשימה עדכנית של כתובות IP של שרתים המעורבים בפעילות זדונית. הכלי בודק האם כתובת ה-IP נמצאת ברשימה זו.
- יא. [VirusTotal](#) – נשתמש ב-API אותו מספק השירות. הכלי בודק האם כתובת ה-IP ידועה כזדונית ע"י לפחות 5 יצרניות של תוכנת אנטי-וירוס.

5 engines detected this URL

URL: http://198.54.117.200/
 Host: 198.54.117.200
 Last analysis: 2019-03-29 14:44:11 UTC
 Community score: -99

5 / 66

Detection Details Community 3

BitDefender	Phishing	Forcepoint ThreatSeeker	Malicious
Quttera	Malicious	Sophos AV	Malicious
Trustwave	Malicious	ADMINUSLabs	Clean

יב. [Zeus Tracker](#) – שירות זה עוקב אחר שרתי C&C ברחבי העולם המפעילים את הסוס הטרויאני המתקדם Zeus. ננתח את דף ה-HTML של תוצאת החיפוש של כתובת ה-IP הנבדקת הנמצאת בכתובת:

<https://zeustracker.abuse.ch/monitor.php?search=<IP>>

סימון CC אדום בדף תוצאת החיפוש מסמל הכתובת אכן שייכת לשרת C&C^[8].

Results in Host table (Zeus C&Cs + FakeHosts)

CC	FU	Zeus Host	IP address	Level	Status	Files Online	Country	AS number
CC		avast-mail-security.download	198.54.117.200	4	online	0	US	AS22612
CC		cy-m0ld.com	198.54.117.200	4	online	0	US	AS22612
CC		felceconserve.com	198.54.117.200	4	online	0	US	AS22612
CC		kudrnwos.as.faih	198.54.117.200	4	online	0	US	AS22612
CC		lzediamike.trade	198.54.117.200	4	online	0	US	AS22612
CC		tekadrian.pro	198.54.117.200	4	online	0	US	AS22612
CC		teksoft.pro	198.54.117.200	4	online	0	US	AS22612
CC		xbsezlma.ha.loan	198.54.117.200	4	online	0	US	AS22612

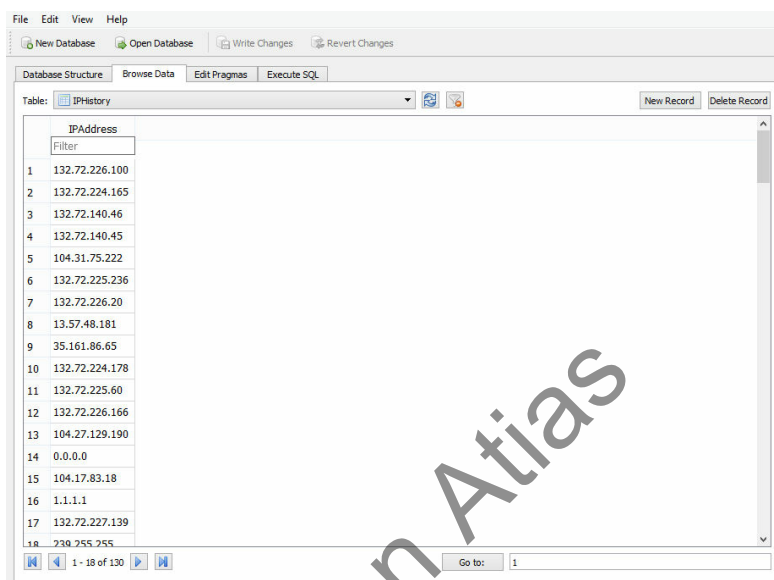
4. שמירת כתובות ה-IP שנבדקו בבסיס נתונים

על-מנת למנוע בדיקה חוזרת של אותן כתובות IP הכלי שומר בבסיס נתונים את כתובת ה-IP הנבדקת לאחר שזו נבדקה לראשונה. מימוש בסיס הנתונים בו בחרתי לעשות שימוש הוא SQLite^[9], מכיוון שבו כל בסיס הנתונים הוא קובץ אחד בלבד, דבר המקל על השימוש ולא דורש הרצה של שרת.

בעת הפעלת הכלי הוא בודק האם לצד קובץ ה-executable קיים קובץ בסיס הנתונים בשם

IPHistory.sqlite. במידה ולא, הוא יוצר אחד כזה, ויוצר בו טבלה בשם IPHistory ובה שדה אחד בשם IPAddress מסוג מחרוזת ובעל גודל של 15 תווים (הגודל המקסימלי הנדרש עבור כתובת IP).

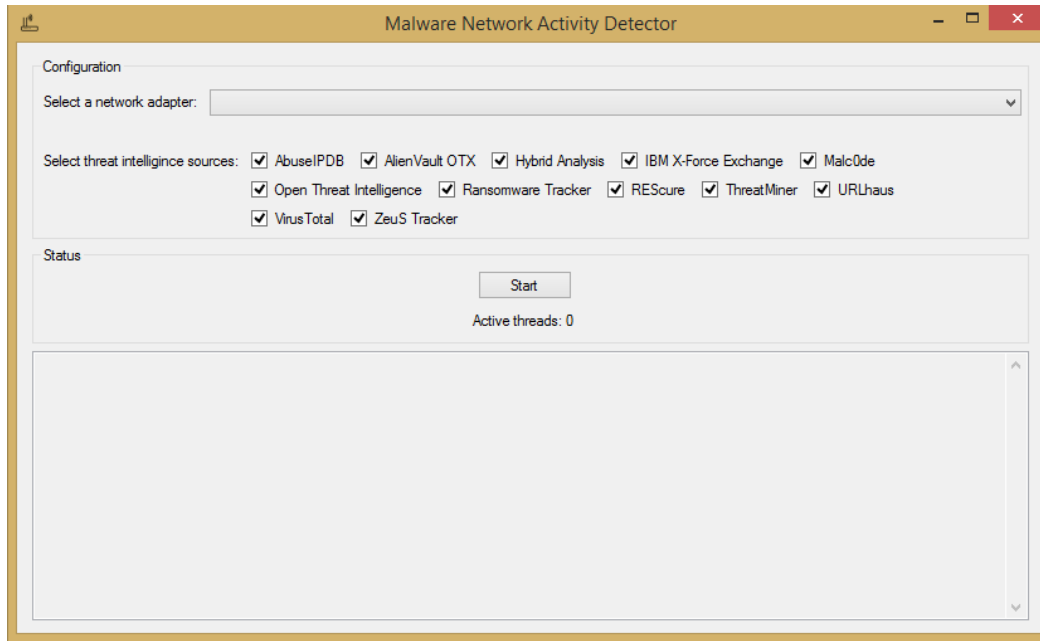
לפני בדיקת כתובת IP כלשהי במקורות ה-Threat Intelligence הכלי בודק באמצעות שאילתת SQL האם הכתובת כבר נמצאת בטבלה שבבסיס הנתונים, כלומר האם הכתובת כבר נבדקה. במידה וכן, הכלי מוותר על בדיקתה. במידה ולא, הכלי מוסיף אותה לטבלה באמצעות שאילתת SQL ולאחר מכן עובר לשלב הבדיקה. ניתן לצפות בתוכן הטבלה ובכתובות ה-IP שנבדקו ונשמרו ע"י הכלי באמצעות התוכנה DB Browser for SQLite^[10] כפי שניתן לראות בתמונה.



5. ממשק המשתמש ושימוש בכלי ההגנה

ראשית, אדגיש כי יש להפעיל את כלי ההגנה תחת הרשאת Administrator ורק כאשר עמדת הקצה נמצאת ב"מצב מנוחה", כלומר כאשר לא מתבצע בה שימוש שוטף ע"י המשתמש, וזאת על-מנת שלא להעסיק את הכלי בחיפוש כתובות רבות לגיטימיות כמו כאלו שמתבצעת איתן תקשורת בזמן גלישה ברשת האינטרנט, ולאפשר לו להתמקד בכתובות איתן מתקשרים קבצים ותוכנות הפועלים בעמדה, דבר שיאפשר "לתפוס על חם" תקשורת המבצע פוגען. בנוסף, יש להתקין טרם ההפעלה את הגירסה העדכנית של הסביבה .NET Framework.

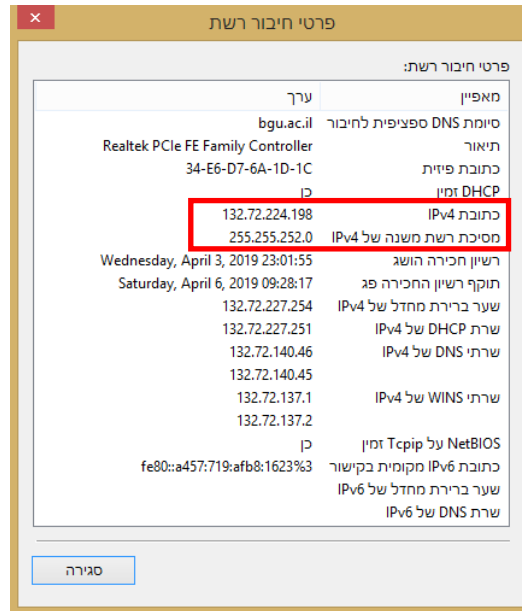
בהפעלת הכלי יש לבחור את כרטיס הרשת שאת התקשורת בו נרצה לנטר. ברשימת כרטיסי הרשת יופיעו רק כאלה שיש בהם חיבור רשת פעיל. בנוסף, לא יופיעו כרטיסי רשת וירטואליים כמו כאלה של מוצרי וירטואליזציה, Loopback וכו', כלומר יופיעו רק כרטיסי רשת מסוג Ethernet או WiFi. לאחר מכן, יש לבחור באילו מקורות Threat Intelligence הכלי ישתמש בזמן הניטור, ולפחות אחד כזה. כברירת מחדל, כל המקורות הזמינים מסומנים ככאלה שנבחרו. לאחר סיום ההגדרות יש ללחוץ על כפתור ה-Start כדי להתחיל את ביצוע הניטור. בחלון התוצאות ייכתבו מועד התחלת הניטור והמקורות שנבחרו.



כל כתובת שנדרשת לבדיקה תיבדק באמצעות Thread חדש. מספר ה-Threads הפועלים כתוב על-גבי הממשק לצורך מעקב אחר מספר הכתובות שנמצאות בבדיקה באותה נקודת זמן. בסיום פעולתו ה-Thread יכתוב בחלון התוצאות באילו מקורות הכתובת שהוא בדק נמצאה כזדונית, או יכתוב Clean במידה והיא לא נמצאה כזדונית באף מקור בו נעשה שימוש. הפסקת ביצוע הניטור לצורך שינוי ההגדרות או לצורך סגירת הכלי תיעשה באמצעות לחיצה על כפתור ה-Stop. Threads שלא סיימו את עבודתם טרם הלחיצה ימשיכו לבצע עד לסיומה. מומלץ שלא לסגור את הכלי כאשר יש Thread פועל. בעת הסגירה המידע בחלון התוצאות יתווסף לקובץ Monitoring Results.txt הנמצא לצד קובץ ה-executable. במידה וקובץ זה אינו קיים הוא ייווצר לפני הכתיבה.

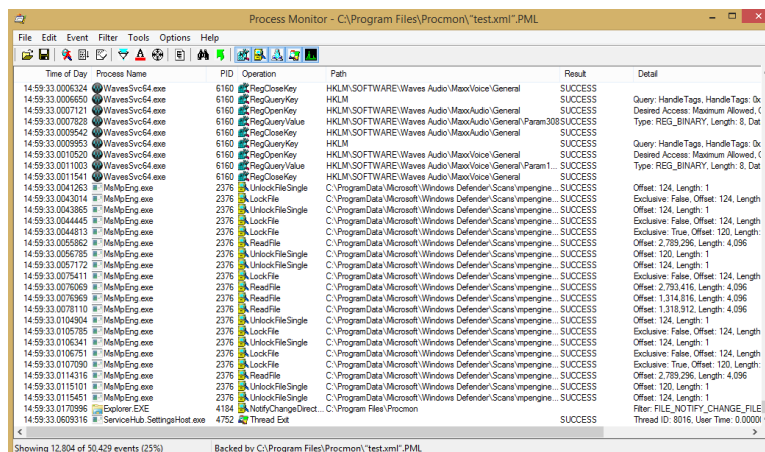
6. הבנת התוצאות והתעמקות בהן

כאמור, עבור כל כתובת IP איתה תקשרה עמדת הקצה בזמן הניטור ייכתב מהם מקורות ה-Threat Intelligence שזיהו אותה כזדונית מתוך המקורות בהם נעשה שימוש בזמן הניטור. עבור כל כתובת IP שזוהתה כזדונית ע"י מקור אחד לפחות יש להעריך את רמת האיום הנשקף ממנה לעמדה. ראשית, יש לוודא שכתובת זו אכן חיצונית ושאינה שייכת ל-VLAN (Virtual LAN)^[11] בו נמצאת העמדה, אם זו שייכת ל-VLAN כלשהו. אם הכתובת אכן שייכת ל-VLAN בו נמצאת העמדה, יש להתעלם ממנה. אחרת יש להמשיך בתהליך ההערכה. בתמונה הבאה ניתן לראות דוגמא לפרטי חיבור Ethernet השייך ל-VLAN.

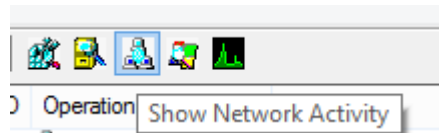


מספר מקורות ה-Threat Intelligence בהם הכתובת זוהתה כזדונית מהווה אינדיקציה ראשונית אך חשובה לרמת האיום הנשקף ממנה. אם זו זוהתה ע"י מקור אחד או שניים, ניתן לומר שיתכן כי ההערכה בסיום התהליך תהיה שלא נשקף איום מכתובת זו. אולם זיהוי ע"י 3 מקורות ויותר יצביע כמעט תמיד על קיומו של פוגען בעמדה. יש לחפש את הכתובת בכלל מקורות ה-Threat Intelligence, ובדגש על אלה בהן היא זוהתה כזדונית. לאחר שקלול כלל המידע ע"י המשתמש הוא יהיה יכול להעריך את רמת האיום ולהחליט האם הוא נדרש לאתר את התהליך המתקשר עם הכתובת.

7. **איתור תהליך המתקשר עם כתובת זדונית**
 במידה והמשתמש החליט לאתר תהליך בעמדת הקצה המתקשר עם כתובת IP שע"פ הערכתו היא זדונית, הוא יכול לעשות זאת באמצעות התוכנה Process Monitor^[12] של Microsoft. כלי זה מאפשר לצפות בזמן אמת בפעילות של תהליכים הקשורה למערכת הקבצים, ה-Registry והתקשורת.



יש להפעיל את הכלי למספר שעות כאשר עמדת הקצה נמצאת ב"מצב מנוחה". לאחר מכן יש לצפות בתוצאות כאשר מסנן התצוגה היחיד הוא Show Network Activity. יש לאתר את הרשומות המצביעות על תקשורת עם כתובת ה-IP הזדונית ומהן לאתר את התהליך המתקשר.



8. פערים ומשימות להמשך

ה-API keys בהם נעשה שימוש בקוד המקור של כלי ההגנה הינם של חשבונותי האישיים בשירותי ה-Threat Intelligence השונים. בנוסף, מפתחות חנימיים אלו מוגבלים בחלק מהשירותים למספר מוגבל של חיפושים במשך דקה אחת ובמשך יום אחד, ומספר חיפושים בלתי-מוגבל דורש מנוי Premium. מכאן ששימוש בכלי בתצורתו הנוכחית, אם יתבצע בעמדת קצה בעלת פעילות תקשורתית רבה או במספר רב של עמדות קצה, יביא לחסימת חלק מה-API keys, ואפשרות השימוש באותם המקורות לא תתאפשר ע"י הכלי. הפתרון, כמשימה אפשרית להמשך, הוא להוסיף לכלי חלון הגדרות בו המשתמש יזין את ה-API key שלו לכל שירות בו נדרש כזה, ורק כאשר יוזן API key תקין הכלי יהיה יכול להשתמש באותו המקור.

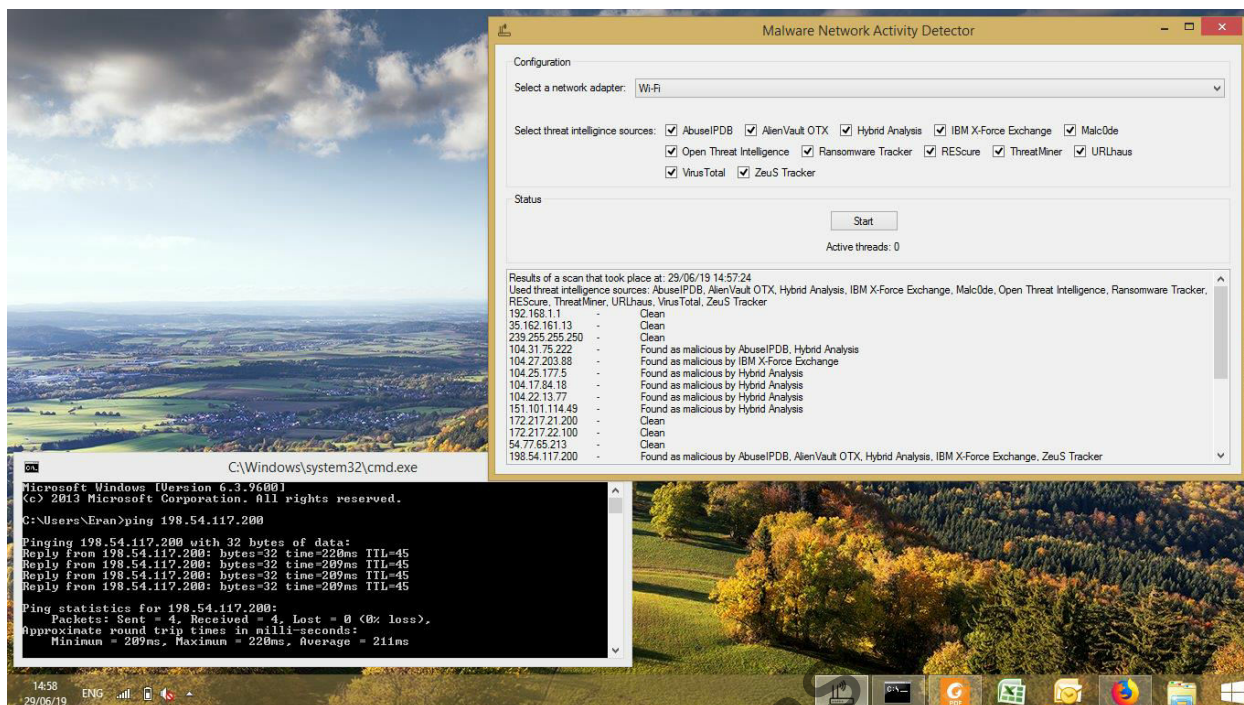
9. הדגמת כלי ההגנה

התכנון המקורי, כפי שנכתב במסמך הצעת הרעיון ותוכנית העבודה היה מציאת Sample של פוגען המקיים תקשורת עם כתובת IP המוגדרת כזדונית ע"י מקורות Threat Intelligence, הרצתו במכונה וירטואלית כאשר כלי ההגנה רץ גם הוא ותייעוד זיהוי התקשורת ע"י הכלי. בחיפוש אחר Samples מתאימים והרצתם במכונה הוירטואלית נתקלתי בכך שכולם זיהו שהינם רצים בתוך מכונה כזו והפסיקו את ריצתם. הדבר מנע ממני לייצר להדגים את יכולות הכלי.

על-מנת להדגים בכל זאת כיצד הכלי מזהה תקשורת אל כתובת IP זדונית המתבצעת ע"י תהליך

במחשב, הרצתי אותו כאשר באותו הזמן נשלחו Ping requests באמצעות ה-CMD אל הכתובת הזדונית

198.54.117.200^[13]. בתמונה הבאה ניתן לראות זיהוי מובהק של תקשורת זו ע"י הכלי.



10. ביבליוגרפיה

- [1] TrendMicro, "Command and Control [C&C] Server".
<https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server>
- [2] TechTarget, "threat intelligence (cyber threat intelligence)".
<https://whatis.techtarget.com/definition/threat-intelligence-cyber-threat-intelligence>
- [3] TechTarget, "An introduction to threat intelligence platforms in the enterprise".
<https://searchsecurity.techtarget.com/feature/An-introduction-to-threat-intelligence-services-in-the-enterprise>
- [4] Comodo, "What is Network Sniffing?".
<https://securebox.comodo.com/ssl-sniffing/network-sniffing/>
- [5] CodeProject, "A Network Sniffer in C#".
<https://www.codeproject.com/Articles/17031/A-Network-Sniffer-in-C>
- [6] Wikipedia, "Private network".
https://en.wikipedia.org/wiki/Private_network
- [7] Webopedia, "APIPA - Automatic Private IP Addressing".
<https://www.webopedia.com/TERM/A/APIPA.html>

- [8] Zeus Tracker, "Zeus Tracker :: Monitor".
<https://zeustracker.abuse.ch/monitor.php>
- [9] SQLite.
<https://www.sqlite.org/index.html>
- [10] DB Browser for SQLite.
<https://sqlitebrowser.org/>
- [11] Wikipedia, "Virtual LAN".
https://en.wikipedia.org/wiki/Virtual_LAN
- [12] Microsoft, "Process Monitor v3.50".
<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>
- [13] 198.54.117.200, IBM X-Force Exchange
<https://exchange.xforce.ibmcloud.com/ip/198.54.117.200>

© Eran Atlas