**הנדסה לאחור וניתוח תוכנות זדוניות – מטלת סיום**

**NjRAT – Bladabindi**



**מגישים:**

מגישים:

נתנאל פדואים, ת.ז 203797816

יקיר קוממי, ת.ז 300487303

**תוכן עניינים**

1. היסטוריה ורקע כללי ........................................................................3
2. מנגנונים טכניים..............................................................................5
3. פירוט טכנולוגי פרטני......................................................................14
4. פירוט טכני קצר על CVE / חולשות....................................................24
5. שני מנגנונים טכניים למניעה הגנה ולמיטיגציה .....................................25
6. תיאור נוזקה לAPPLE.....................................................................26
7. תיאור נוזקה לIOS .........................................................................27
8. מנגנון טכני מסוג BYOVD .............................................................. 28
9. מנגנון הגנה למערכות מחשוב...........................................................28
10. מנגנון טכני עבור Anti-Debug ...................................................29
11. מנגנון טכני עבור Privilege Escalation ........................................30
12. החדרת נוזקה Supply Chain Attack ........................................31
13. מודול RAT פופולארי.................................................................. 32
14. קבוצת תקיפה בסייבר המשויכת לאיראן ........................................33
15. שימוש בכלי AI .........................................................................34
16. ביבליוגרפיה – בסוף המטלה ובקובץ המצורף.................................35

2.) **התייחסות היסטורית ורקע כללי:**

הנוזקה שנבחרה הינה ממשפחת ה RAT, מתת משפחת NjRAT וידועה בשם Bladabindi, Lime-Worm.

הנוזקה הינה וריאנט של הנוזקה הוותיקה jRAT.

ב2013 לראשונה התגלתה הנוזקה ע"י חברת הסייבר הישראלית Synet,

הנמצאת בשימוש בעיקר במזרח התיכון, נגד אנשים פרטיים ואתרים ממשלתיים, בעיקר נגד ענף התקשורת, הבנקאות וענף האנרגיה.

בשנים 2014-2016 הנוזקה הייתה בשימוש בולט וזאת לאחר שב2014 מייקרוסופט הסירה מיליוני אתרים שהכילו את הנוזקה וב2016 חברת האנטי-וירוס Softpedia זיהתה שימוש בנוזקה כחלק מפרויקט תקיפה.

מתקפה בולטת היתה ב2017 כאשר האתר הרשמי של ISIS נפרץ והכיל קישור להורדת התוכנה Adobe Flash Player שהכילה את הנוזקה.

התגלתה ב2023 עלייה בשימוש בנוזקה בצפון אפריקה ובמזרח התיכון נגד בנקים – גניבת סיסמאות מידע רגיש ומטבעות דיגיטליים.

התפתחות הנוזקה:

Bladabindi התפתח כחלק מנוזקה קיימת בשם jRAT שהופיעה לראשונה בשנת 2012.

הנוזקה מבוססת ג'אווה וחוצה פלטפורמות כדלת אחורית, מיוחסת לתוכנות:

Jsocket, AlienSpy, Frutas, jFrutas, Unrecom, Adwind, jBiFrost, Trojan.Maljava

הנוזקה התחילה בתור Frutas, שודרגה באופן פרטי ל JFrutas RAT v1.0 Version

בהמשך השם שונה ע"י היוצר ל Adwind RAT.

הנוזקה Adwind RAT שומשה ברחבי העולם יחד עם הנוזקה DarkComet RAT.

ב2013 הוסיפו לנוזקה Adwind יכולת לפגוע גם במערכת ההפעלה אנדרואיד – מה שהפך אותה באמת לחוצת פלטפורמות. שומשה בעיקר נגד ארגונים פיננסיים, וענפי הייצור וההנדסה ומטרות ממשלתיות ומדיניות.

בשנת 2015 – נוצרה הגרסה המחודשת האחרונה של הנוזקה בשימוש פתוח לכולם Jsocket בינואר 2016. לגרסה זו יש מינוי המקנה תמיכה טכנית, אופציות תקיפה ופריצה רחבות יותר ומודולים מתקדמים בתוספת תשלום, אפשרות לרכישת שירותים משלימים של הסתרה מפני אנטי-וירוס, שירותי VPN עם אופציות למיפוי פורטים לתקשורת נכנסת בנקודת החיבור של הVPN באמצעות עשרות מנועי אנטי-וירוס.

Bladabindi ידועה בשימוש ע"י קבוצות תקיפה מרכזיות כגון: AQUATIC PANDA, Earth Lusca, Operation C-Major, The Gorgon Group.

3.)

**מנגנונים טכניים בולטים:**

הנוזקה תוקפת פלטפורמות Windows בכל הגרסאות.

כאשר מחשב נדבק בנוזקה, הנוזקה תאסוף מידע רב על המחשב כגון:

שם המחשב, סוג מערכת ההפעלה, המדינה שבה נמצא המחשב, שמות משתמשים וגרסת מערכת ההפעלה.

הנוזקה נותנת דלת אחורית לתוקף שדרכה התוקף יכול לבצע מס' פעולות, בנוסף ליכולות שהורחבו בסעיף קודם, בשנים האחרונות הנוזקה שודרגה עוד וכעת לנוזקה יש את היכולת לפרוץ לארנקים דיגיטליים מוצפנים.

לאחר הדבקת מחשב, הנוזקה מעתיקה עצמה לתוך תיקיות TEMP, APPDATE, USERPROFILE.

בנוסף, לתוכנה יש את היכול להעתיק עצמה לקבצי EXE לשרידות מרבית, ע"מ לוודא כי תופעל בכל עליית מערכת ההפעלה.

דרכי התחמקות הנוזקה מתוכנות לגילוי נוזקות:

מנגנון ההתחמקות של NjRAT מתוחכם. הנוזקה מסתירה עצמה מזיהוי ע"י תוכנות אנטי-וירוס באמצעות מספר טכניקות:

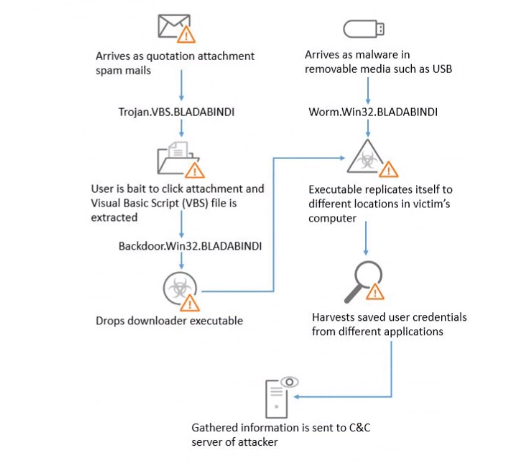
1. שימוש במערבלי קוד בשפת .net ע"מ להקשות על גילוי הנוזקה.
2. הסוואת הנוזקה לריצה כתהליך קריטי, כך שלמשתמש אין גישה לכבות או למחוק אותו ממנהל התהליכים.
3. הנוזקה יכולה לכבות תהליכי אנטי-וירוס – דבר המקשה על גילוייה.
4. הנוזקה יודעת לזהות אם היא רצה על מכונה וירטואלית כדי להפעיל אמצעי נגד כנגד חוקרי נוזקות.

יכולות התוכנה בעיקר: קריאת לחיצת מקשי המקלדת ושמירת ההקשות, גישה למצלמת הנתקף, גניבת סיסמאות ומידע מהדפדפן, פתיחת cmd, העלאת והורדת קבצים, צפייה בשולחן העבודה של המשתמש, פתיחת תהליכים קבצים ומניפולציות על הregistry , מתן יכולות לתוקף לבצע עדכונים, הסרות, ריסטארט, סגירה וניתוק של הנוזקה וגם שינוי הID.

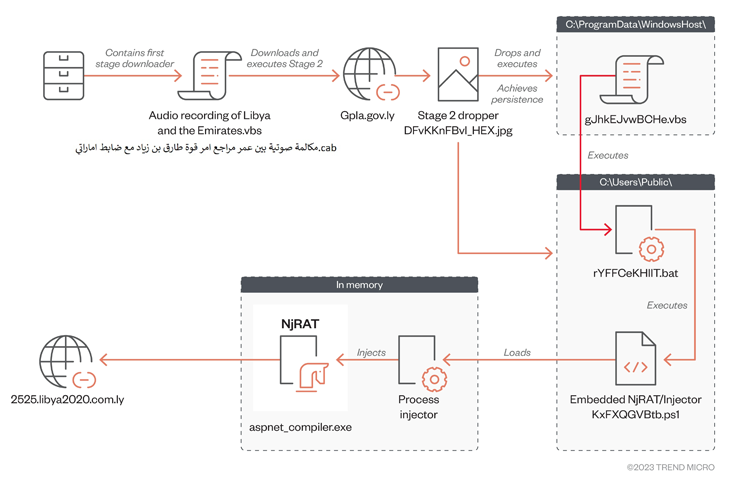
באמצעות מחשב הניהול והשליטה, לתוקף יש יכולות ליצור ולקנפג את פיזור הנוזקה גם דרך כונני USB.

מנגנוני הפצת הנוזקה העיקריים:

* הפצת הנוזקה יכולה להתבצע באמצעות כונני USB חיצוניים – התוכנה מגלה אותם ותעתיק עצמה אליהם ע"מ להדביק מחשבים אחרים.
* קובץ המצורף למייל (לדוגמה למשתמשי פלטפורמת דיסקורד).

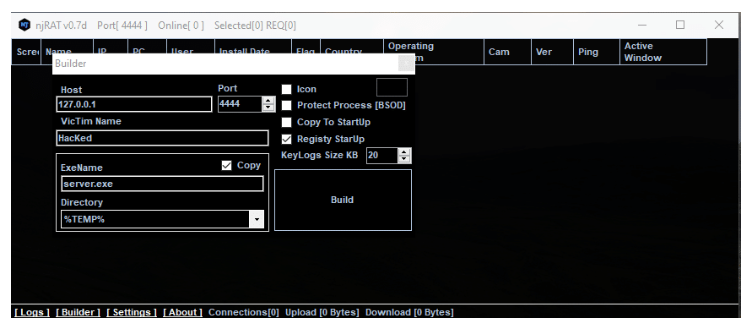


* הורדת הנוזקה מהאינטרנט בתור תוכנה לגיטימית שהמשתמש מחפש.

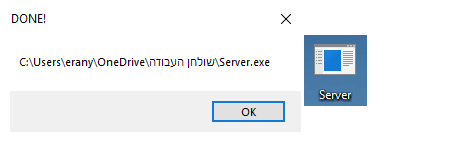


לנוזקה קיים ממשק ניהול עבור התוקף, בעזרתו אפשר לבצע את כלל הפעולות המפורטות מעלה והם מפורטות לתוקף בצורה נוחה:

כשלב מקדים לתקיפה עצמה, התוקף יוצר קובץ של הנוזקה ע"י ממשק הניהול שבו הוא נותן לנוזקה הגדרות ראשוניות – כגון פורט תקשורת לנוזקה, שם ייצוגי לנתקף.



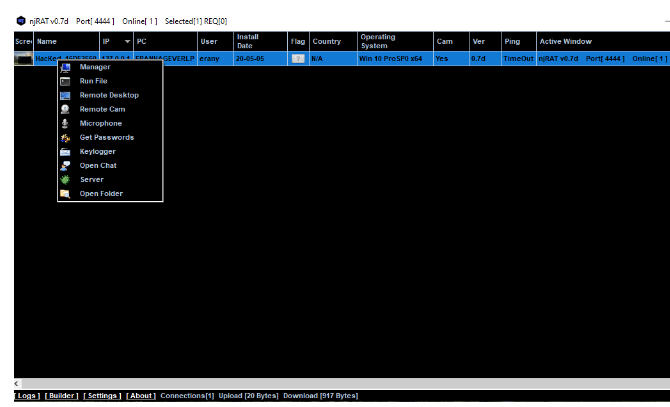
בעת סיום הגדרת קובץ השרת – ניצור קובץ EXE:



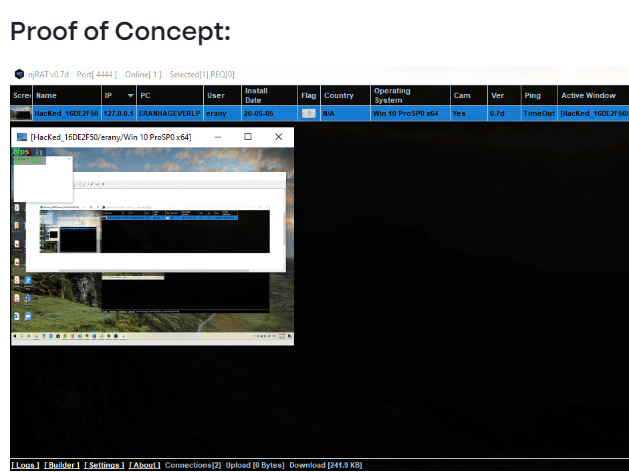
את קובץ הEXE נשלח אל משתמשים באמצעות מנגנוני ההפצה.

כאשר הנתקף פותח את הקובץ, הנוזקה פותחת חיבור רשת עם שרת התוקף ובכך מאפשרת גישה לתוקף למחשב הנגוע.

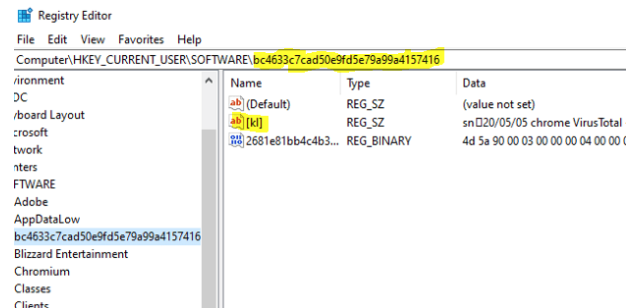
ברגע שמחשב הודבק יש לתוקף גישה לביצוע פעולות – התוקף מקבל חלונית התראה במכונה של הנתקף.



נראה את הגישה למחשב הקורבן:



הנוזקה מבצעת שינויים ברג'יסטרי ע"מ להפעיל את עצמה אוטומטית בעת עליית המחשב:



**טכנולוגיות בשימוש הנוזקה:**

Bladabindi משתמשת בקטעי קוד backdoor של הסוס הטרויאני Adwind, הידוע גם כ: AlienSpy, Frutas, Sockrat, Jsocket ו jRAT.

במקור הינו כלי גישה מרחוק (RAT) הרשום בשפת JAVA ומאפשר גישה ותקיפה לפלטפורמות רבות כגון ווינדוס, לינוקס, מק, אנדרואיד.

* שימוש באינטרפרטר מובנה – הנוזקה מריצה פקודות POWERSHELL ו/או פקודות WINDOWS COMMAND SHELL.
* הנוזקה נכתבה בשפת התכנות VB.NET.
* הנוזקה משתמשת בפורטים ייעודיים המיועדים עבור נתקפים ספציפיים (לפי קובץ הקונפיגורציה שנוצר עבור כל התקפה.) פורט ייעודי המשומש עבור תקשורת HTTP 2C הינו 1177.
* NjRAT משתמש במנגנון קידוד base64 להצפנת תעבורה אל שרת cnc – c2.
* אין מנגנוני בדיקת סיסמאות ע"פ מילון או brute force כי הנוזקה משתמשת בKEYLOGGER הקורא את הקלדות מכשירי ה I/o ושומר אותם ונותן לתוקף גישה מלאה אליהם.

שימוש וניצול חולשות:

* לא בוצע שימוש בחולשות מכיוון שהנוזקה מגיעה אל הנתקף באמצעות כונני USB נגועים או הורדת קבצים נגועים מהאינטרנט או פתיחת קבצים מצורפים לאימיילים.
* לא בוצע ניצול חולשות לצורך הסלמת הרשאות מכיוון שהמשתמש בלא-יודעין פתח את הנוזקה והתוקף מקבל גישה למלוא ההרשאות של הנתקף.

מנגנוני הפצת הנוזקה:

נעזרים בוקטורי חדירה שאינם נוזקות – הורדת הנוזקה דרך אימייל/אתר אינטרנט או הדבקה דרך כונן חיצוני:

* מנגנוני הפצה עצמית – הנוזקה מדביקה כונני USB חיצוניים ובכך מגדילה את כמות המחשבים הנדבקים בחיבור אליהם.
* מנגנוני הפצה רשתיים – הנוזקה עוברת באימייל כתוספת לקבצים וגם דרך העברת קישורים באימייל לאתרים מפוקפקים והורדת תוכנות מאתרים פיקטיביים.

4.)

**פירוט טכנולוגי טכני פרטני של הנוזקה:**

שלב ראשון:

בתחילה, הנוזקה יוצרת קובץ Mutex חדש ע"מ למנוע הדבקות חוזרות על אותו מחשב.

(יצירת אובייקט במערכת המסמן כי מחשב זה נדבק.)

הנוזקה לרוב מעתיקה עצמה לתיקיית TEMP תחת השם svchost.exe.

באמצעות השימוש בשם זה הנוזקה יכולה לחמוק ממנגנוני הגנה בWINDOWS מכיוון שזהו שם של תהליך לגיטימי השכיח במערכת.

לאחר מכן הנוזקה יוצרת חוקה בחומת האש המאפשרת לה גישה חיצונית דרך הרשת מהמחשב התוקף אל המחשב הנגוע.

שלב הבא של הנוזקה הינו הפעלת מנגנון הישארות בחיים בעיקר ע"י השיטות:

1. יצירת מפתח ברג'יסטרי להפעלה אוטומטית בנתיב: HKCU\Software\Microsoft\CurrentVersion\Run\.
2. העתקתה לתיקיית STARTUP (עליית מערכת) בתור קובץ נסתר.

שלב שני

כאשר הנוזקה מתחילה בפעולתה היא מפעילה שלושה "פועלים" עיקריים:

1. פועל הממתין לקבלת פקודות משרת השליטה וביצוע הפקודות.
2. Keylogger המקליט את כל פעולות המשתמש במכשירי i/o.
3. פועל שמטרתו להגן על הנוזקה מפני תוכנות הגנה ומכשירי ניתוח (analysis tools)

הרחבת המידע עבור כל "פועל":

פועל ראשון: ברגע שהפועל מתחיל הוא מנסה ליצור קשר עם שרת הבקרה בפורט שהוגדר מראש ע"י התוקף.

כאשר הקשר עם השרת נוצר, הנוזקה שולחת נתונים על המערכת המותקפת לשרת השליטה: שם מחשב, שם משתמש, סוג וגרסת מערכת ההפעלה, תאריך וכד'.

לאחר השליחה הפועל ממתין לקבלת פקודות נוספות לביצוע משרת השליטה.

פעולות אפשריות נפוצות ששרת השליטה יכול לשלוח אל הפועל במחשב הנגוע הינן:

כיבוי מחשב, אתחול מחשב, יצירת תהליכים חדשים, שליחת קונפיגורציות, ניתוק המשתמש הקיים במערכת, הפעלת רמקול המחשב, פתיחה וסגירה של כונן הדיסקים, כיבוי והדלקה של הצג ועוד.

פועל שני:

Keylogger – התהליך עובר על רשימת המקשים שמוקשים במחשב ומתעדם ברג'יסטרי.

התיעוד מתבצע ע"י תאריך, שם תהליך, חלון התוכנה שרצה והמקשים עצמם שהוקשו.

פועל שלישי:

פועל ההגנה – פועל זה עוקב אחרי מספר תהליכים וביניהם – task manager, process viewer וגם process hacker.

באם נמצאה הרצה של אחד מתהליכים אלה – הנוזקה מבטלת את אופציית המשתמש לעצור אותה ע"י ביטול כפתור הסגירה וע"י כך הנוזקה מגנה על עצמה.

שלב שלישי:

כעת הנוזקה מאפשרת לתוקף את היכולות הבאות:

Cmd – פתיחת חלון לצורך הרצת פקודות shell.

Credentials – גניבת סיסמאות המשתמש השמורות בדפדפנים.

Custom protocol – שימוש בפרוטוקול ייעודי לתקשורת הנוזקה עם שרת השליטה.

Data collection – איסוף מידע על המערכת הנגועה.

Disabling security tools – פתיחת חוקות בחומת האש.

File & directory – התוקף מקבל גישה לכלל הקבצים של הנתקף.

File deletion – לתוקף יכולת מחיקת קבצים במחשב הנגוע.

Input capture – תיעוד הקשות מקלדת ועכבר.

Modify registry – שינוי הרג'יסטרי במחשב הנגוע.

Device discovery – הנוזקה תעדכן את התוקף אם קיימת מצלמה במחשב הנגוע.

RDP – התחברות מרחוק למחשב הנגוע.

File copy – העתקת קבצים אל/מ המחשב הנגוע אל/מ המחשב התוקף.

Remote System Discovery – זיהוי מחשבים נוספים ברשת.

Distribution – זיהוי כוננים חיצוניים והעתקת הנוזקה אליהם.

Screen capture – צילום מסך המחשב הנגוע.

Uncommonly used port – שימוש בפורטים לא שכיחים עבור תקשורת.

Webcam capture - גישה למצלמת הרשת במחשב.

* בנוזקה אין שימוש בהזרקות קוד בזמן ריצה, אלא רק בזמן עלייתה הראשונית ז"א לדוגמה בהורדת קובץ מסוג Microsoft file כגון קובץ word, בהפעלתו הראשונית הקובץ ייפתח כקובץ רגיל אבל יכיל בתוכו קוד שיתקין את הנוזקה על המחשב הנתקף.
* בנוזקה לא התגלה עד כה KILL SWITCH.
* התגלו עבור הנוזקה עדכוני גרסאות ואף קיימת הפקודה up אשר מעדכנת את הנוזקה במחשב הנגוע – לדוגמה מגרסה 0.11 ועד גרסה 0.7. לכל גרסה ישנה ייחודיות משלה כגון – בדיקת פורטים בגרסת GOLD מול חלון חדשות בגרסת DANGER.
* ישנם payload downloads כגון הפקודה pas המורה לנוזקה להוריד רכיבים נוספים עבור hard-coded URL, הפקודה inv – תוספת המורה לנוזקה להריץ פלאגין חיצוני.
* נעשה שימוש בקוד ורעיונות מנוזקות אחרות מאותה המשפחה – jRAT, עקב התפתחות הנוזקה מנוזקות כגון Adwind ו Frutas.
* הרעיון המרכזי הוא יצירת backdoor וגישה מרחוק בRDP ומשפחת NjRAT פיתחה אותן ליכולות נוספות.
* הנוזקה לא מנצלת Backdoors קיימים אלא יוצרת backdoor משלה ומשנה הגדרות מחשב ע"מ לפתוח דרכי תקשורת לנוזקה עם התוקף – לדוגמא פתיחת חוקים ייעודיים עבורה בחומת האש (כמפורט למעלה).

בנוזקה Bladabindi השייכת למשפחת NjRAT ישנם מרכיבים מודולריים כחלק מהתפתחות של הנוזקות ממשפחת jRAT שאחת ההפצות ממשפחה זו היא הנוזקה Jsocket – אשר לנוזקה זו קיימת אפשרות לרכישת הנוזקה אונליין ואף רכישת מינוי המקנה תמיכה טכנית במשתמשים וכד'.

לנוזקה אין מרכיבים שניתן לקנותם בנפרד. התשלום עבור jSocket מקנה פרקי זמן של השתמשות בנוזקה אבל ברכישתם קונים אותה כbundle יחיד.

קיימת אופציה של רכישת מודולים נוספים בתוספת תשלום אך רק לאחר רכישת מינוי לנוזקה.

קיימים indicators of compromise עבור הנוזקה:

**IOCs:**

* cefa4ebf82b3d077a68ce1933be3dc6e9cadce8bc27671a5fcd76ee2f4d04977.ppam — 6175e14e465756c626ccc0f398fcdcb0
* stage3.vbs — edf8f50f318c20bccb889743172d9fd2
* out1.dll — 4b7d118b20d8854372129f53365d529f
* out2.exe — d189af41737b287469ca5f5589dcbdf1
* hxxps://pt[.]textbin[.]net/download/itm1dkgz7c
* hxxps://paste[.]ee/d/ESa4q/0
* hxxps://pt[.]textbin[.]net/download/tmo7gc3cgs
* hxxps://pt[.]textbin[.]net/download/igvxdijw4q
* hxxps://paste[.]ee/d/jtSmT/0
* hxxps://paste[.]ee/d/ea2Mw/0
* hxxps://pt[.]textbin[.]net/download/insdj4bhn2

חיווי זה עבור הימצאות הנוזקה פורסם ב 18/3/2024.

בנוסף ישנים חיוויים שפורסמו ב9/12/2020:

03c7015046ef4e39a209384f2632812fa561bfacffc8b195542930e91fa6dceb

205341c9ad85f4fc99b1e2d0a6a5ba5c513ad33e7009cdf5d2864a422d063aba

2270b21b756bf5b5b1b5002e844d0abe10179c7178f70cd3f7de02473401443a

54cf2d7b27faecfe7f44fb67cb608ce5e33a7c00339d13bb35fdb071063d7654

54d7ee587332bfb04b5bc00ca1e8b6c245bb70a52f34835f9151b9978920b6d7

678a25710addeefd8d42903ceddd1c82c70b75c37a80cf2661dab7ced6732cd3

67cbb963597abb591b8dc527e851fc8823ff22d367f4b580eb95dfad7e399e66

6817906a5eff7b02846e4e6a492ee57c2596d3f19708d8483bef7126faa7267f

69366be315acc001c4b9b10ffc67dad148e73ca46e5ec23509f9bb3eedcd4c08

94c2196749457b23f82395277a47d4380217dd821d0a6592fc27e1e375a3af70

94e648c0166ee2a63270772840f721ba52a73296159e6b72a1428377f6f329ad

96640d0c05dd83bb10bd7224004056e5527f6fad4429beaf4afa7bad9001efb7

97227c346830b4df87c92fce616bdec2d6dcbc3e6de3f1c88734fe82e2459b88

97b943a45b4716fcea4c73dce4cefe6492a6a51e83503347adcd6c6e02261b84

9ba0126bd6d0c4b41f5740d3099e1b99fed45b003b78c500430574d57ad1ad39

bd2387161cc077bfca0e0aae5d63820d1791f528feef65de575999454762d617

#### ****Second Stage****

9982c4d431425569a69a022a7a7185e8c47783a792256f4c5420f9e023dee12a

d347080fbc66e680e2187944efbca11ff10dc5bfcc76c815275c4598bb410ef6

30c071a9e0207f0ca98105c40ac60ec50104894f3e4ed0fb1e7b901f56d14ad4

231d52100365c14be32e2e81306b2bb16c169145a8dbcdc8f921c23d7733cef0

fd5c731bb53c4e94622e016d83e4c0d605baf8e34c7960f72ff2953c65f0084c

b3730931aaa526d0189aa267aa0d134eb89e538d79737f332223d3fc697c4f5a

75b833695a12e16894a1e1650ad7ed51e6f8599ceaf35bbd8e9461d3454ab711

6d0b09fe963499999af2c16e90b6f8c5ac51138509cc7f3edb4b35ff8bef1f12

2af1bb05a5fde5500ea737c08f1b675a306150a26610d2ae3279f8157a3cb4df

db8ca46451a6c32e3b7901b50837500768bb913cafb5e12e2111f8b264672219

5ebb875556caefb78d5050e243f0efb9c2c8e759c9b32a426358de0c391e8185

bdc33dbdfd92207ad88b6feb3066bb662a6ca5cf02710870cae38320bb3a35bf

08f378fe42aec892e6eb163edc3374b0e2eb677bd01e398addd1b1fca4cd23c4

da8d01720b72d4924634030496665779624e5fbb291a6346bf54cb61beec5020

cf3d42642c7f3867849464351e2cdacab7b5c73f50f0ac7075583a8a210d6675

ad640f1084f2228aede77674dfa5078844fd4163694234021bfe72b73f30f060

ebe8e001726ccb5df470d650b4afd2fe6d4ae087e8aba9e1bcd18bbd217022d6

0f6b5e0bd39fa3eb5e33212d1c180bacf9441a908986bd5e36eadaddb22e80ea

f84b23d6d06956922d90093c2cc18f6cb23564285fc4b482f41eb5b360cb5874

0c649e8575cdd0baf7ffcbe08c1e906a0d6adcc3e7612c86ebdd93882854ddee

633d16bb4f3465574d0e020165fb4d3f2a2c94e440c521d8dc6034f9d369a989

7cfc8fdc124e034579cfd665c38fc3f66de2fa8e47350e09f8e91f6000f96b3f

add358e91095ffee6f3232965ecc4fdee386fea3a5e9b7bc540434aece1da3d1

7b6f26c5cdec1f5dc21c46cf26889ce1349629944fd45a684c94af1174c201df

83667a9a99db9e89d9b0d39b0cd2fb94c59085f4d3b7b3c37206228f22bdc081

9425d9099bf4dd1cd2c41434fe45de21ac1659110d121342849077eb6770437a

3ec0a49b394c159a2a2833fc5009948abf485d3328d37931c1a8e0469c784824

MD5: 10666134095758789aa4d120d232945d

**Indicators of Compromise (IOCs)**

Related hashes (SHA-256):

* c46a631f0bc82d8c2d46e9d8634cc50242987fa7749cac097439298d1d0c1d6e —Worm.Win32.BLADABINDI.AA
* 25bc108a683d25a77efcac89b45f0478d9ddd281a9a2fb1f55fc6992a93aa830 — Win32.BLADABINDI.AA

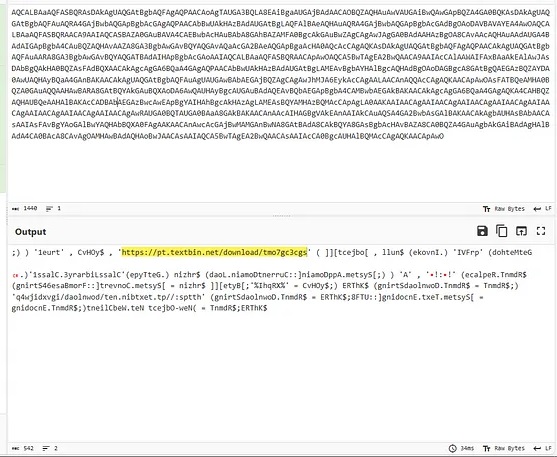
|  |  |
| --- | --- |
| File  SHA256 | **Server-**aedb5b5a2dcb788f2474f929173151db8eb6d7489b00c85e7303755cfd7a59ef  **njRAT-** bf853789b938bdc5da8aaeb52511379a332c7cf238266a21bfcb0318a62e85cb |

|  |  |  |
| --- | --- | --- |
| Known IP addresses | ****Inactive URL’S**** | ****Active URL’S**** |
| 3.124.142.205  185.204.1.236  149.154.154.78  3.134.39.220  3.127.181.115  3.134.125.175  91.109.178.2  3.67.112.102  3.64.4.198  3.133.207.110  3.125.188.168  91.192.100.37  195.123.221.123  37.1.217.131  147.185.221.224  3.141.142.211 | hxxp://pastebin[.]com/raw/TWQYHv9Y  hxxp://pastebin[.]com/raw/0HpgqDt2  hxxp://pastebin[.]com/raw/1t8LPE7R  hxxp://pastebin[.]com/raw/3vsJLpWu  hxxp://pastebin[.]com/raw/6MFWAdWS  hxxp://pastebin[.]com/raw/AqndxJKK  hxxp://pastebin[.]com/raw/SdcQ9yPM  hxxp://pastebin[.]com/raw/XMKKNkb0  hxxp://pastebin[.]com/raw/ZM6QyknC  hxxp://pastebin[.]com/raw/pMDgUv62  hxxp://pastebin[.]com/raw/yEw5XbvF | hxxp://pastebin[.]com/raw/JKqwsAs6  hxxp://pastebin[.]com/raw/pc9QbQCK  hxxp://pastebin[.]com/raw/Rpx7tm9N  hxxp://pastebin[.]com/raw/hsGSLP89  hxxp://pastebin[.]com/raw/HNkipzLK  hxxp://pastebin[.]com/raw/Z3mcNqjz  hxxp://pastebin[.]com/raw/h5yBCwpY  hxxp://pastebin[.]com/raw/zHLUaPvW  hxxp://pastebin[.]com/raw/V6UWZm2n  hxxp://pastebin[.]com/raw/rTjmne99  hxxp://pastebin[.]com/raw/JMkdgr4h  hxxp://pastebin[.]com/raw/yPTNdYRN  hxxp://pastebin[.]com/raw/q56JPtdY  hxxp://pastebin[.]com/raw/a3U5MMj2  hxxp://pastebin[.]com/raw/E4MB4MFj  hxxp://pastebin[.]com/raw/770qPDMt  hxxp://pastebin[.]com/raw/YtuXz7YX  hxxp://pastebin[.]com/raw/LKRwaias  hxxp://pastebin[.]com/raw/ZFchNrpH  hxxp://pastebin[.]com/raw/8DEsZn2y |

בנוסף לIOCs , פורסמו מדריכים מפורטים לגבי גילוי הנוזקה ומחיקתה ומחיקת נספחיה כגון מחיקת כתובות DNS חשודות, תהליכים חשודים ברג'יסטרי וכד'.

שימוש בטכניקות הסתרה בנוזקה:

* משתנים המכילים מחרוזות המוצפנות ב base64 שנדרשות להיות מקודדות ומפוענחות. לדוגמה:



* השימוש באי ערבול לדוגמא ע"י הפונקציה:

$rhzin = [system.convert]::FromBase64String( $RdmnT.Replace( ‘!x:!y’ , ‘A’ )

להפוך כל X או Y מהקוד לA.

* טכניקות anti-debug לא קיימות בנוזקה.
* טכניקות Anti-VM קיימות כגון - Modify Registry keys, create registry key,

NjRAT will add persistence via the Registry key: HKCU\Software\Microsoft\CurrentVersion\Run\.

* טכניקות anti-forensic משומשות בנוזקה: – מחיקת קבצים, Fileless Attacks – באמצעות פקודות power shell, מדובר בהזרקת קוד בינארי המטורגט ע"י תוכנות גילוי,
* פקודות רג'יסטרי כגון מחיקת ערכים ומניפולציות על הרג'יסטרי והחבאת מידע ברג'יסטרי, מחיקה ומניפולציה על לוגים במערכת ווינדוס ועוד.

9.) **פירוט טכני על CVE / חולשות שהנוזקה נעזרת בהם**

לא קיימים מספרי CVE לנוזקה מכיוון שהנוזקה לא מנצלת חולשה בקוד מסוים אלא את חולשות המשתמש – תמימותו, שם משתמש וסיסמה חלשים וכד'.

כן ישנן ניצולי חולשות של משתמשים:

1. RCE – פגיעויות הפעלת קוד מרוחק נותנות לתוקף אופציה להפעלת קוד שרירותי על מערכת מרחוק. כך Bladabindi מנצל פגיעות להשגת גישה לא מורשית למערכות והפעלת פקודות פוגעניות כלפי המערכת והמשתמש.
2. File Format – קבצים כמו PDF, מסמכי אופיס או קבצי מדיה עלולים להיות מנוצלים ע"י הנוזקה, להעברת payloads והעברת קטעי קוד זדוניים כגון סקריפטים כאשר המשתמש פותח או מבצע אינטראקציה עם הקובץ הנגוע ומאפשר גישה לRCE.
3. Unpatched software – Bladabindi עלול לנצל פגיעויות ידועות בתוכנות שלא ביצעו עדכונים (כולל עדכוני אבטחה) יזומים ע"י המשתמש או מערכת ההפעלה. כולל אי ביצוע עדכונים בדפדפנים, פלאגינים ותוכנות נפוצות נוספות.
4. Social engineering – היא אינה פגיעות הקיימת בתוכנה ישירות אך מדובר בתחבולות על משתמשים ע"מ להפעיל payloads זדוניים כגון – מיילים זדוניים, עדכוני תוכנות פיקטיביים או אתרים מזויפים העובדים על הקורבנות להוריד קבצים זדוניים.
5. Weak or Default Credentials – Bladabindi מנצל הרשאות התחברות חלשות או דיפולטיביות בטירגוט מערכות כגון שם משתמש וסיסמה עבור רשתות כמו Wi-Fi, שרתים ומכשירי IOT.
6. Drive-by Downloads – Bladabindi מנצל פגיעויות בדפדפנים ותוכנות שרתי ווב ע"מ לבצע הורדת נוזקה באופן אוטומטי והרצתה כאשר משתמש נכנס לכתובת URL זדונית.

<https://www.cynet.com/attack-techniques-hands-on/njrat-report-bladabindi/>

11.)

**שני מנגנונים טכניים למניעה הגנה ו/או למיטיגציה**

1. בחרנו מקטגוריה **Harden**  את השיטה **message Encryption**.

זוהי שיטת הצפנת גוף הודעה ע"י מפתח קריפטוגרפי.

יש שני סוגי הצפנות עיקריים, התהליך מתבצע בצורה הבאה:

1. הצפנה סימטרית – ישנו שימוש במפתח הצפנה יחיד עבור שני הצדדים המתכתבים, המידע מוצפן ומפוענח בשני הצדדים באמצעות אותו מפתח הצפנה.
2. הצפנה אסימטרית – ישנו שימוש בשני מפתחות – לכל צד בשיחה ישנם 2 מפתחות – ציבורי ופרטי.

המפתח הציבורי נגזר מהמפתח הפרטי – מה שאומר שכדי לפענח הודעה מוצפנת באמצעות הקוד הציבורי חייב שימוש במפתח הפרטי שהוא נשאר סודי עבור אותו משתמש.

הסבר מפורט – כאשר צד א רוצה לדבר עם צד ב באופן מאובטח הוא יצפין את ההודעה באמצעות המפתח הציבורי של צד ב, ובגלל שהמפתח הציבורי של ב נגזר מהמפתח הפרטי של ב רק משתמש ב יצליח לפענח את ההודעה בצורה נכונה.

כך המידע מאובטח הרבה יותר מאשר בהצפנה אסימטרית שבה עלולים לפענח את המפתח הצפנה ובכך את המידע.

שיטה זו באה לתת סודיות למידע שתוקפים לא יצליחו לטרגט את המידע.

2.בחרנו מקטגוריה **Detect** את השיטה **File Hashing**

זוהי שיטה לגילוי קבצים נגועים במערכת.

לכל קובץ במערכת הקבצים מייצרים hash – חותמת דיגיטלית של הקובץ. (בהבדל מחתימה דיגיטלית המכילה מאפיינים נוספים)

אם חותמת הדיגיטלית נמצאת ברשימת הhash הנגועים אז הקובץ הינו קובץ זדוני.

זהו מנגנון שבא להגן על המשתמש מפני נוזקות ידועות.

12.)

**איתור שם נוזקה למערכת הפעלה של APPLE**

שם הנוזקה שבחרנו הוא **DazzleSpy**.

מטרת הנוזקה היא ביצוע מעקב על משתמשי - mac. מסוג watering hole.

<https://www.macworld.com/article/608716/mac-dazzlespy-malware-backdoor-hackers-patch.html>

נוזקה זו מנצלת חולשה בדפדפן Safari של mac שבו בעת גישה לאתר זדוני אז הנוזקה יורדת ומותקנת על מחשב הנתקף ומאפשרת ליצור backdoor לתוקף.

הנוזקה יצאה בשנת 2021 והתגלתה באוגוסט ע"י TAG, דווחה כנוזקת Zero-day ליצרן מיידית.

דיווח על הנוזקה תועד ב Cve-2021-30869 .

גרסאות פגיעות של מערכת mac : 10.15.2 (Catalina) ומעלה.

החולשה תוקנה בגרסה 11.2.

13.)

**נוזקה ל IOS Malware**

שם הנוזקה: NSO – Pegasus.

מטרות פעולת הנוזקה – ריגול.

לינקים למאמרים המתארים את Pegasus:

<https://www.helpnetsecurity.com/2023/10/05/cve-2023-42824/>

<https://www.helpnetsecurity.com/2023/09/08/cve-2023-41064-cve-2023-41061/>

<https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html>

<https://en.wikipedia.org/wiki/Pegasus_(spyware)>

הנוזקה ניצלה חולשה שבה קבצים מצורפים זדוניים לתמונות נשלחו לנתקף ע"י אפליקציית iMessage.

מספרי CVE ידועים:

* CVE-2023-41064
* CVE-2023-41061
* CVE-2016-4657
* CVE-2016-4656
* CVE-2016-4655
* CVE-2021-30860

הנוזקה משתמשת בטכניקות sandbox-Escape .

הנוזקה היא אכן מסוג zero-click. רצה ללא אינטראקציה מהנתקף.

לא מצאנו שום מידע לגבי שימוש במנגנון פרסיסטנטיות בנוזקה.

14.)

**מנגנון טכני מסוג Bring Your Own Vulnerable Kernel Device-Drive**

שם הנוזקה – ZINC.

שם הדרייבר – Viraglt64.sys

CVE-2017-16238

16.)

**מנגנון להגנה של מערכות מחשוב**

מנגנון ההגנה שבחרנו הוא file integrity monitoring .

במנגנון זה מתבצע מעקב אחרי קבצים מסויימים למציאת שינויים בקבצים.

יש אופציה להגדיר גם קבצים ע"י המשתמש.

מתבצע באמצעות שמירת המצב הראשוני של הקובץ ואח"כ השוואת הקובץ לאחר זמן מסויים למצב הראשוני. ברגע שיש שינוי מסויים לא יודע בקובץ – קופצת התראה.

17.)

**מנגנון טכני לצורך Anti-Debug**

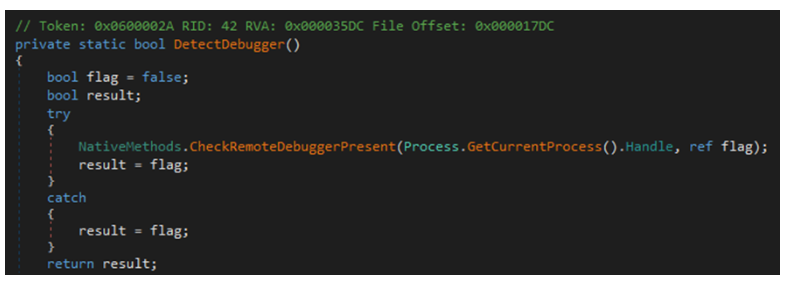
המנגנון שבחרנו מאתר checkpoint בחרנו תחת אנטי-דיבאג הינו Debug Flags.

במערכת ההפעלה קיימים "דגלים" מיוחדים בתוך הזיכרון המסמנים אם תהליך מסויים הינו תחת דיבאג או לא.

אחת הדרכים לבדיקה הינה באמצעות הפונקציה CheckRemoteDebuggerPresent () השייכת למערכת ההפעלה windows.

פונקציה זו מחזירה תשובה האם תהליך מסויים נמצא דיבאג או לא.

דוגמא לנוזקה שמשתמשת בטכניקה הזו היא snip3:



18.)

**מנגנון טכני לצורך Privilege-Escalation**

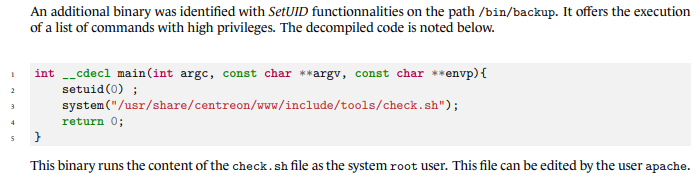
הטכניקה שבחרנו הינה Abuse Elevation Control Mechanism והמנגנון הטכני שנבחר מתוך טכניקה זו הינו Setuid and Setgid .

מדובר במנגנון העלאת הראשות שבו תוכנה יכולה להעלות את הרשאות הריצה שלה למשתמש עם הרשאות חזקות יותר.

<https://attack.mitre.org/techniques/T1548/001/>

המאמר מצורף בקבצי הביבליוגרפיה כקובץ PDF תחת השם:

SANDWORM INTRUSION SET CAMPAIGN TARGETING CENTREON SYSTEMS



19.)

**החדרת נוזקה ב Supply Chain Attack**

הנוזקה שנבחרה הינה **notPetya**.

הנוזקה הייתה מיועדת לפגיעה בעיקר במוסדות פיננסיים אוקראינים, ממשלתיים ותעשיית האנרגיה.

הפגיעה בשרשרת האספקה הייתה באתר אוקראיני של חברה המספקת עדכוני תוכנות פיננסיות וחשבונאות ובכך פוגעת בכל מי שעובד עם התוכנות, אך כל העולם נפגע.

27/6/2017 הינו תאריך תחילת ההתקפה בעזרת נוזקה זו. יום חג באוקראינה.

תאריך הגילוי והפרסום הינו 28/6/2017 – ביום שאחרי כבר פורסמו כתבות על כך שמחשבים במשרדים ממשלתיים ופיננסיים נעולים ודורשים דמי כופר ע"מ לקבל את המפתח לפתיחתם.

כמות המשתמשים שנפגעה באוקראינה – לפחות 4 בתי חולים בקייב, 6 חברות אנרגיה, 2 נמלי תעופה, 22 בנקים כספומטים ומכשירי סליקה.

כ300 חברות נפגעו וההערכות מדברות על 10% מכלל המחשבים באוקראינה שנמחקו.

ישנו מאמר ניתוח טכני של הרוגלה –

<https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>

20.) **מודול Rat פופולארי**

המודל שבחרנו הינו **NetSupportManager RAT**.

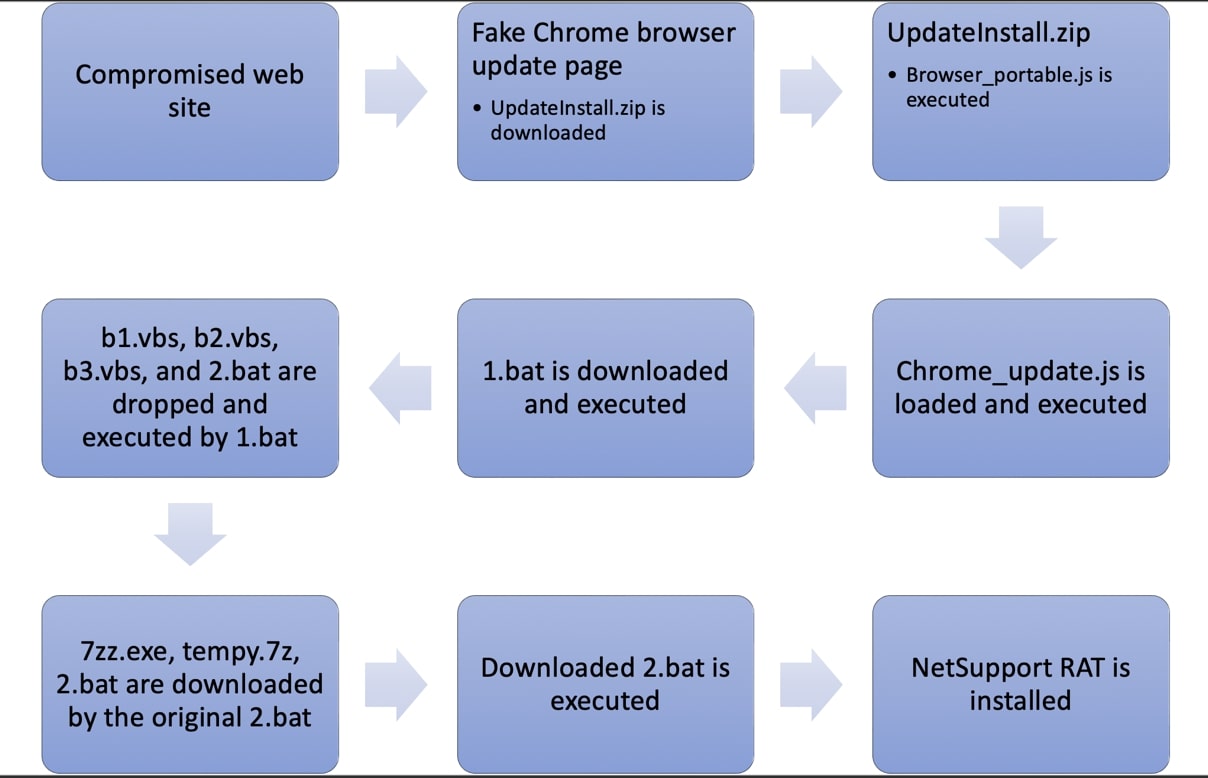
הנוזקה מסווה עצמה כעדכון לגיטימי לדפדפן כרום ע"מ לגרום למשתמשים תמימים להוריד עדכון זה ובעצם להתקין תוכנת ניהול מרחוק הנקראת NetSupportManager.

בעזרת כלי זה תוקפים חודרים למחשבים וגונבים מידע ויכולים להשתלט על מחשבים נתקפים.

הנוזקה מתמקדת בתקיפת דפדפני כרום מכיוון שהוא הדפדפן הפופולארי בעולם – עם נתח שוק של כ 63.5% שימוש בחברות הגדולות.

קבוצת תקיפה דומיננטית המשתמשת בנוזקה - TA505.

אופן ההדבקה:



התוקף מקים אתר לעדכוני תוכנה, שדרכו יורידו את הנוזקה.

התוקף שותל קישור לאתר שהוא הקים בתוך אתר לגיטימי שעליו הוא השתלט.

האתר עליו השתלט יוביל לאתר הפיקטיבי שהקים – להורדת עדכון הדפדפן – כשבפועל ההורדה מכילה את הנוזקה.

24.)

**איתור מידע על קבוצת תקיפה בסייבר הקשורה לאיראן**

קבוצת תקיפה איראנית בסייבר הינה OilRig.

שמות נוספים של הקבוצה: APT34, ATK40, Cobalt Gypsy, Helix Kitten, EUROPIUM

כלים בשימוש הקבוצה בין היתר: RDAT, SideTwist, Saitama.

טכניקות בשימוש RDAT:

צילום מסך, התחזות לתוכנות לגיטימיות כגון VMware, התחזות לשם של סרוויס ועוד.

טכניקות בשימוש SideTwist:

איסוף פרטי מחשב ושם משתמש, שימוש בAPI קיימים כגון GetUserNameW ו GetComputerNameW ע"מ לאסוף מידע, יכולת הורדת קבצים נוספים לשימוש הנוזקה, חיפוש קבצים במחשב, שימוש בפורט 443 עבור תקשורת C2 אבל גם לעבור לשימוש בפורט80 במצב כשל בתקשורת. פתיחת tunnel תקשורת C2, הצפנה ופענוח של הודעות ויצירת מפתח הצפנה רנדומלי. העלאת קבצים. שימוש בget ו POST בHTTP.

הקבוצה התמקדה במדינות במזרח התיכון בעיקר.

התעשיות הנתקפות ביותר היו ממגזרי התעשיה הפיננסית, אתרי ממשלה, התעשיה האנרגיה, התעשיה הכימית ותעשיית התקשורת .

הקבוצה פועלת עד היום.

מקורות גם מצורפים בקבצי הביבליוגרפיה.

<https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/>

<https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/>

<https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/>

25.)

**בחרנו את שאלות 16 ו 20 לענות עליהם שוב**.

השתמשנו ב ChatGPT בגרסה 3.5 וגם בגימיני גרסה פרו 1.0.

כל המידע נמצא בנוסף בקישורים המצורפים – לינקים וצילומי מסך.

טכניקות מובילות לכתיבת פרומפטים אשר מתגברים על מגבלות ה ChatGPT:

Prompt injection, prompt leaking, jailbreaking, Roll playing.

* ­­Prompt injection - הרעיון הינו הזרקת פקודה להתעלם מההוראה המקורית של התוכנה ולהזריק הוראה חדשה שיכולה לתת פלט זדוני לבקשת המשתמש.
* Prompt leaking – הרעיון הינו שהמשתמשים המקוריים בתוכנה מכניסים מידע שאינו אמור להיות גלוי לציבור – ובעזרת סוג של injection מטרתו להדליף מידע זה שגם יכול להיות סודי.
* Jailbreaking – בעזרת תחכום בצורת שאלת השאלה – בשינוי ההקשר של השאלה, אפשר לעקוף את מניעת המודלים לביצוע בקשות זדוניות.
* Role playing – זהו סוג של jailbreaking, בו נאמר למודל להעמיד פנים שהוא בתפקיד של ישות אחרת – ללא מגבלות ובכך אפשר לקבל פלט שלא נקבל בצורה רגילה. טכניקה מובילה – DAN (do anything now).

**ביבליוגרפיה**

**רשימת מאמרים:**

https://malpedia.caad.fkie.fraunhofer.de/families עליו התבססנו בחיפוש נוזקה.

https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat מצאנו משפחת NJRAT

**מאמרים ואתרי תוכן:**

https://attack.mitre.org/software/S0385/

https://www.virusbulletin.com/index.php/global-search-results/?search\_paths%5B%5D=&query=NjRAT&submit=Search%21

https://www.trellix.com/search/?q=Njrat

https://www.microsoft.com/en-us/wdsi/threats/threat-search?query=NjRAT

https://securelist.com/?s=NjRAT

https://www.cynet.com/attack-techniques-hands-on/njrat-report-bladabindi/

https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-njrat-malware/

https://www.hamichlol.org.il/NjRAT

https://www.youtube.com/watch?v=YLaLHNLeiZ0&ab\_channel=ManageEngineIAMandSIEM

https://cyberint.com/blog/research/njrat-bulletin/

https://www.youtube.com/watch?v=2akJcCZ3Dd0&ab\_channel=Rubik%27sHacker

https://blogs.cisco.com/tag/njrat

https://unit42.paloaltonetworks.com/njrat-pastebin-command-and-control/

https://thehackernews.com/2023/01/earth-bogle-campaign-unleashes-njrat.html

https://dbpedia.org/page/NjRAT

https://malware.news/t/malware-analysis-njrat/79786

https://msrc.microsoft.com/blog/2019/05/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

https://www.fortinet.com/blog/threat-research/bladabindi-remains-a-constant-threat-by-using-dynamic-dns-services

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bladabindi

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Behavior:Win32/Bladabindi.gen&threatId=-2147281575

https://blog.sonatype.com/bladabindi-njrat-rat-in-jdb.js-npm-malware

https://www.trellix.com/blogs/research/cyberattacks-targeting-ukraine-increase/

https://hidocohen.medium.com/njrat-malware-analysis-198188d6339a

https://medium.com/@b.magnezi/malware-analysis-njrat-5633847bd6f1

**הסתמכנו בעבודת החקר בעיקר על האתרים:**

https://www.cynet.com/attack-techniques-hands-on/njrat-report-bladabindi/

https://unit42.paloaltonetworks.com/njrat-pastebin-command-and-control/

https://hidocohen.medium.com/njrat-malware-analysis-198188d6339a

**סעיף 9**

מאמר חולשות

https://www.cynet.com/attack-techniques-hands-on/njrat-report-bladabindi/#heading-6

**רשימת מאמרים לסעיף 12:**

https://www.macworld.com/article/608716/mac-dazzlespy-malware-backdoor-hackers-patch.html

https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/

https://support.apple.com/en-us/103158

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30869

**סעיף 13**

https://www.helpnetsecurity.com/2023/10/05/cve-2023-42824/

https://www.helpnetsecurity.com/2023/09/08/cve-2023-41064-cve-2023-41061/

https://en.wikipedia.org/wiki/Pegasus\_(spyware)

**סעיף 14**

https://www.rapid7.com/blog/post/2021/12/13/driver-based-attacks-past-and-present/

https://www.microsoft.com/en-us/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

https://www.greyhathacker.net/?p=990

**סעיף 16**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview

https://d3fend.mitre.org/technique/d3f:FileIntegrityMonitoring/

https://linux.die.net/man/8/tripwire

**סעיף 17**

https://telefonicatech.com/blog/snip3-investigacion-malware

**סעיף 18**

https://attack.mitre.org/techniques/T1548/001/

קובץ PDF - CERTFR-2021-CTI-005

**סעיף 19**

https://cyberlaw.ccdcoe.org/wiki/NotPetya\_(2017)

https://www.bbc.com/news/technology-40428967

https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef\_story.html?noredirect=on

https://attack.mitre.org/software/S0368/

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

<https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>

**סעיף 20**

https://www.trellix.com/blogs/research/new-techniques-of-fake-browser-updates/

https://perception-point.io/blog/operation-phantomblu-new-and-evasive-method-delivers-netsupport-rat/https://www.embeeresearch.io/advanced-cyberchef-operations-netsupport/

https://medium.com/@ad12347/netsupport-rat-hits-again-with-new-iocs-37318de44cfc

https://blogs.vmware.com/security/2023/11/netsupport-rat-the-rat-king-returns.html

https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager\_rat

**סעיף 24**

https://nsfocusglobal.com/apt34-unleashes-new-wave-of-phishing-attack-with-variant-of-sidetwist-trojan/

https://attack.mitre.org/groups/G0049/

https://malpedia.caad.fkie.fraunhofer.de/actor/oilrig

**סעיף 25**

https://www.promptingguide.ai/

https://github.blog/2023-07-17-prompt-engineering-guide-generative-ai-llms/

https://developers.google.com/machine-learning/resources/prompt-eng?hl=he

https://circleci.com/blog/prompt-engineering/

https://www.kdnuggets.com/prompt-engineering-101-mastering-effective-llm-communication

https://realpython.com/practical-prompt-engineering/

https://learn.microsoft.com/en-us/ai/playbook/technology-guidance/generative-ai/working-with-llms/prompt-engineering

**קישורים נוספים עבור סעיף 25 - טכניקות לכתיבת פרומפטים:**

https://github.com/dair-ai/Prompt-Engineering-Guide/blob/main/guides/prompts-adversarial.md

https://www.wikihow.com/Jailbreak-Chatgpt

**בנוסף מצורפים לעבודה צילומי מסך, מאמרים, קבצים וקישורים בתיקיית הפרויקט.**