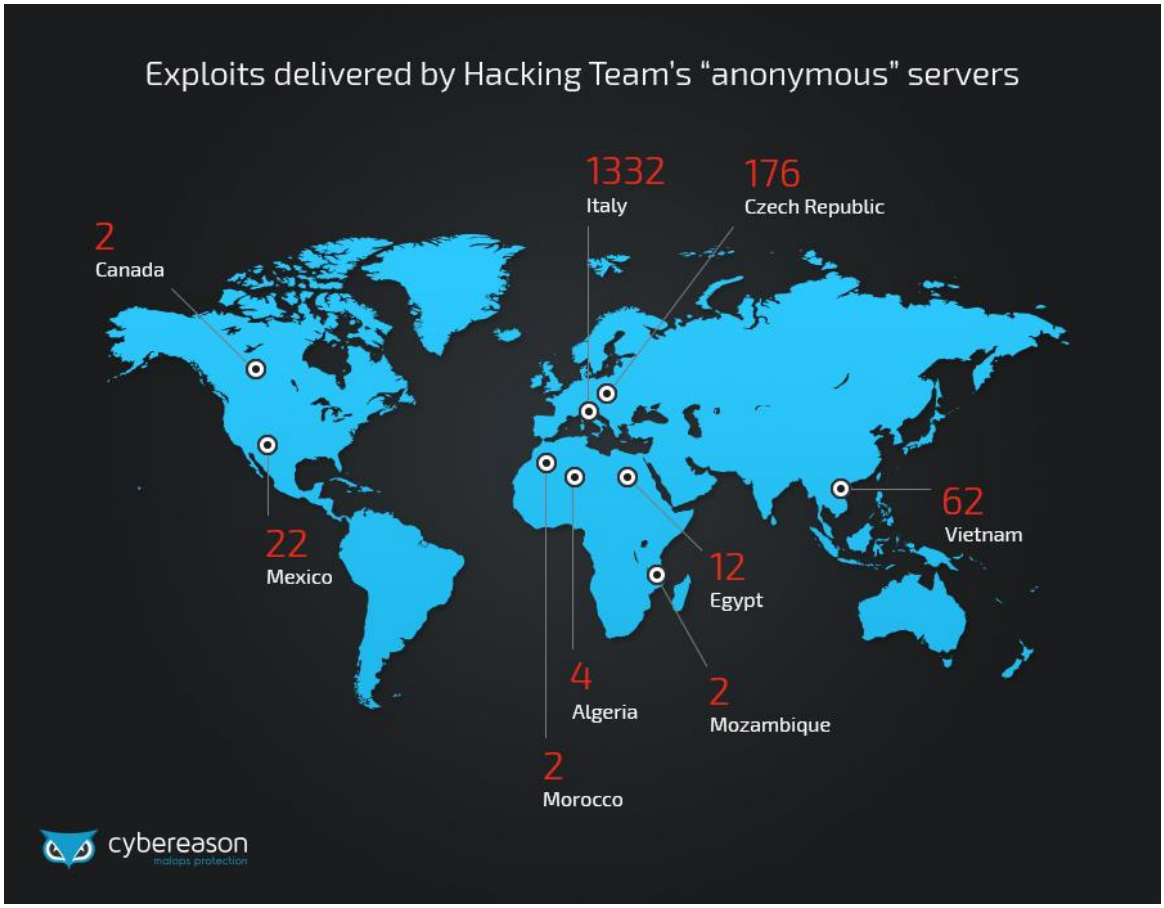
digital whisper
Technologic Papers

זליגת שיטות התקיפה של קבוצת HackingTeam: שידרוג מיידי לכל האקר מתחיל

מאת איאן מילר, עמית סרפר ואלכס פרייזר

רקע

במאמר זה נציג ניתוח אשר בוצע על-ידי אנשי קבוצת המחקר של Cybereason על שיטות וכלי התקיפה של HackingTeam, המציע יכולות מיסוך, התחזות ותקיפה מתוחכמות, הזמינות לכל דורש.



לאור הפרסומים על תקיפת הסייבר על חברת HackingTeam וזליגת הידע של החברה לאינטרנט, קבוצת החוקרים שלנו החליטה לחקור לעומק ולגלות את שיטות התקיפה שעמדו לרשות אנשי החברה.

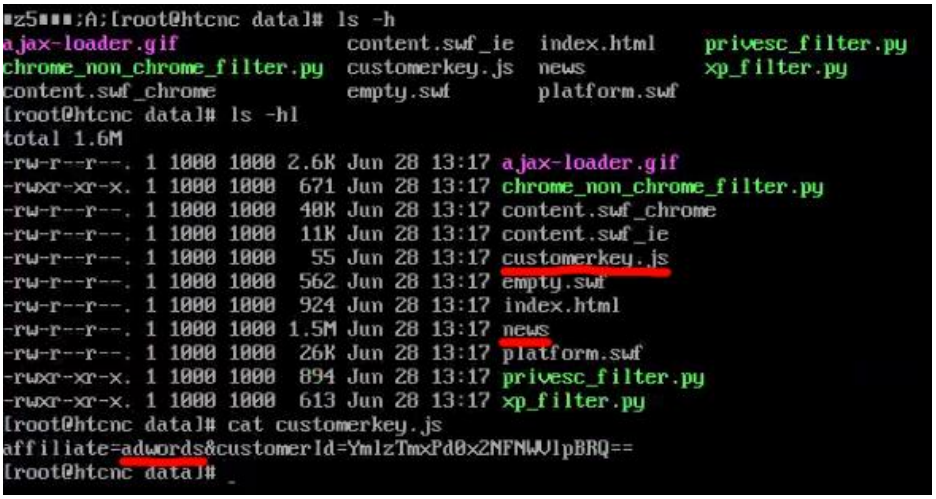
לחוקרי אבטחת מידע, מידע כזה הוא מכרה זהב, המעניק אשנב לשיטות פעולה של האקרים ולדרך המאפשרת להם לקיים את התקיפות לאורך זמן. שניים מבין חוקרי אבטחת המידע של חברת Cybereason גילו במאגר המידע שנפרץ פרטים על פעילויות הקבוצה ויעדי התקיפה שלה.

הזמינות הגבוהה של המידע עשויה להעצים את יכולותיהם של האקרים מרחבי העולם, ולשים בידיהם כלים ושיטות עבודה מתוחכמים יותר להוצאה לפועל של תקיפות הסייבר עליהם הם עומלים, כמו גם חולשות Zero-day חדשות ששוחררו מבלי שניתנה לחברות הרלוונטיות השהות לתקן אותן. על אף שהתקיפות החדשות שיצאו לפועל בחסות המידע שנלמד מ-HackingTeam יהיו בעלות חתימה שונה ממבצעי HackingTeam, אנו מעריכים כי מכיוון שאנשי החברה השאירו על שרת ההדבקה שלהם קוד קל לקריאה והערות שימוש מפורטות, התוקפים יעקבו אחרי הוראות אלו בדיוק רב, דבר שעשוי לאפשר לאנשי אבטחת מידע לפתח יכולות זיהוי שלהם בעתיד.

ברצוננו לבחון מקרוב כיצד אנשי HackingTeam כיוונו את תקיפותיהם אל מטרותיהם ואת השיטות בהם השתמשו כדי לשמר את אחיזתם ביעד המטרה לאורך זמן ממושך.

חיקוי שיטת התקיפה של Flame בניסיון להסתיר את מקור התקיפה

קבוצת HackingTeam השתמשה באסטרטגיה חכמה על מנת לחדור למחשב היעד. ראשית, מבצעי החברה חיקו את פעילות התוכנה הזדונית Flame אשר נחשפה ב-2012. Flame התחבר לשרת ה-C&C (שרת פיקוד ובקרה) באמצעות ממשק משתמש אשר נראה כמו אתר חדשות או שירות של adwords, אשר הציע לכאורה ל"לקוחות" (אנשי HackingTeam השתמשו במושג זה ככינוי למטרות שלהם) לינק לשרת "איחסון פרסומות", אשר לחיצה עליו גרמה להתקנה של התוכנה הזדונית. רבות מהפקודות והפרוטוקולים בהם נעשה שימוש בתקיפות "Flame" השתמשו בז'רגון מעולם החדשות והפרסום על מנת להתל בכלי זיהוי ובאנליסטים, וקבוצת ה-HackingTeam השתמשה באותה אסטרטגיה.



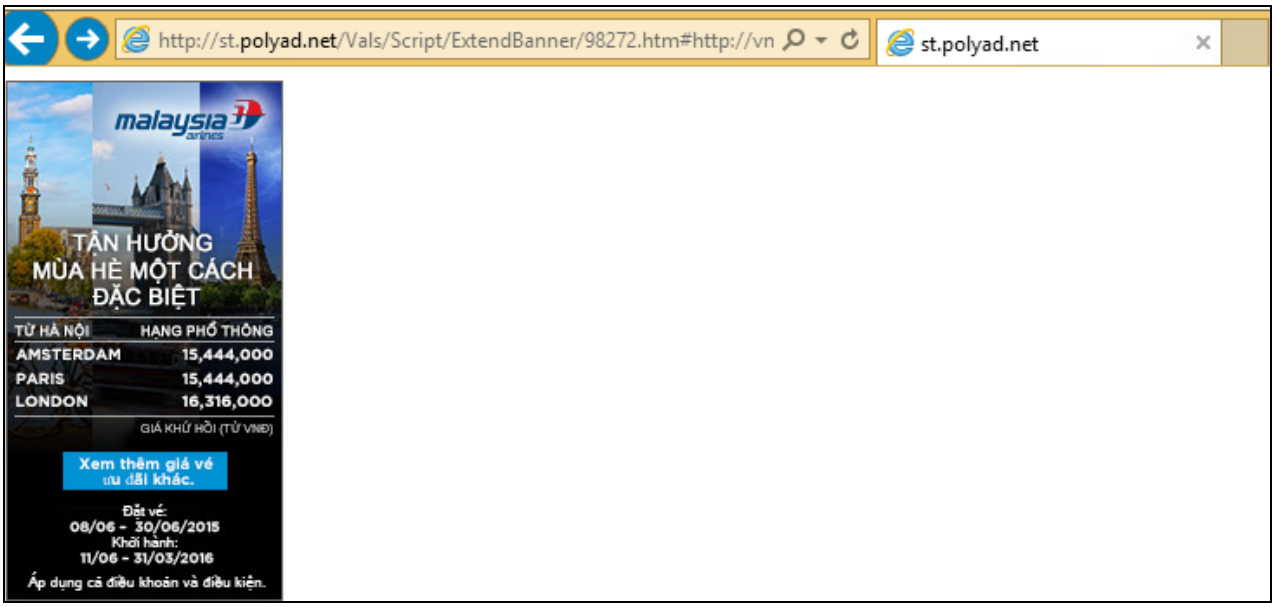
[בתמונה - שימו לב למילים "news" ו-"adwords" בקוד ובשמות הקבצים]

שיטת ההדבקה

על שרת ההדבקה של ה-HackingTeam מצאנו קובץ בינארי מסקרומבל ב-base64 עם השם "חדשות" ("news"), שגילינו שהוא למעשה היה ה-Payload. כאשר פיענחנו את קובץ ה-base64 התגלה בפנינו קובץ מוצפן ב-AES-256 המכיל 0day שמבצע Privilege escalation ל-System באמצעות ניצול חולשה ב-Driver של Adobe .

על ידי שימוש במגוון שיטות מקובלות, ביניהן פישינג והנדסה חברתית קיבלו המטרות לינק. ברגע שמקבל הלינק לחץ עליו, שרת ההדבקה בדק האם זהות המותקף נכונה. באם לא - המקליק הופנה ישירות לעמוד שגיאה 404 או לעמוד בית כלשהו הקשור לחדשות (וניתן להתאמה לפי הלקוח) על מנת שלא לעורר חשד. לעומת זאת, אם המקליק היה אכן היעד הנכון לתקיפה - השרת המשיך לאבחן את המחשב ממנו התחבר על מנת לזהות את מערכת ההפעלה והדפדפן בהם נעשה שימוש. השרת זיהה האם המטרה עושה שימוש ב-Internet Explorer, Firefox או Chrome, ואיזו מערכת הפעלה רצה על המחשב, על מנת להתאים את השימוש בחולשת Adobe Flash מתאימה אשר תאפשר לתוקף להשתלט על מחשב היעד.

מנקודה זו מערכת השליטה מרחוק הפכה מותקנת ופעילה על המחשב ואיפשרה לתוקפים להתקדם לצעד הבא במבצע התקיפה שלהם.



[צילום המסך לעיל מראה דוגמא של תקיפה מוכוונת ליעד בויטנאם אשר שולחת לפרסומת משתמש אשר לא זוהה כיעד לתקיפה ומשתמש ב-Internet Explorer]

הצלחנו לעקוב אחרי התהליך הנ"ל באמצעות קריאת קוד המקור (המתועד היטב!) של הקבצים על שרת ההדבקה ושל הלוגים של תקשורת ה"לקוח". כשהתעמקנו עוד יותר במידע, יכולנו לראות מתי חדרו אנשי HackingTeam למטרה (עד לכדי רמת דיוק של מיקרו שניות), איפה הם היו ממוקמים, באיזה ספק שירותי

אינטרנט עשו שימוש, באיזו מערכת הפעלה עשו שימוש, ואפילו באיזו תצורה של הדפדפן הם עשו שימוש על מנת להשתמש בשרת ההדבקה. לדוגמא, על מנת להדביק מטרה הממוקמת במצרים, ראינו כי המטרה השתמשה בכרום build 43.0.2357.130, אשר עודכן והותקן ב-22 ביוני. HackingTeam חדרו למחשב של הנתקף המצרי באמצעות חולשה בפלאש, שישה ימים לאחר מכן, ב-28 ביוני. זהו מידע חשוב ואף משעשע, בהתחשב בכך שכרום משווק כדפדפן המאובטח ביותר למשתמש הממוצע, בעוד שהתוקפים ניצלו פרצה בדפדפן ימים ספורים לאחר שהתוכנה עודכנה.

```
[root@htcnc 03dF2q]# cat data/chrome_non_chrome_filter.py
#!/usr/bin/env python

import os
import sys
import struct

def main():
    browser = os.environ.get('_BROWSCAP__browser')
    target_dir = os.path.dirname(os.path.realpath(__file__))

    if 'IE' in browser:
        sys.stdout.write(open(os.path.join(target_dir, 'content.swf_ie')).read())
        sys.stderr.write('[*] IE swf size {}'.format(len(open( os.path.join(target_dir, 'content.swf
_ie')).read())))
    else:
        sys.stdout.write(open(os.path.join(target_dir, 'content.swf_chrome')).read())
        sys.stderr.write('[*] Chrome swf size {}'.format(len(open( os.path.join(target_dir, 'content
.swf_chrome')).read())))

if __name__ == '__main__':
    main()
[root@htcnc 03dF2q]# _
```

[צילום מסך של קוד זיהוי הדפדן מתוך תקיפה על יעד מצרי]

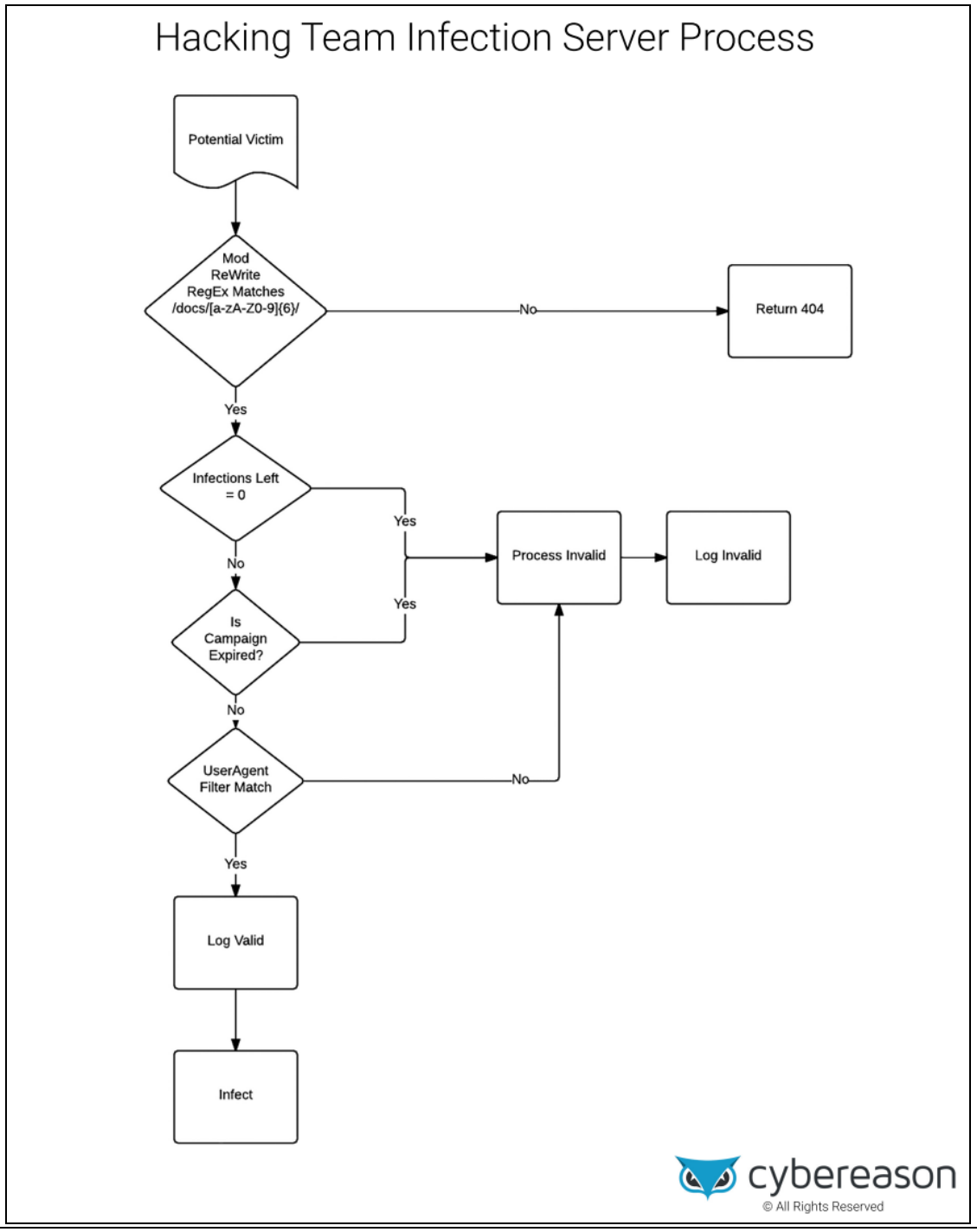
בנוסף, חזינו בדבר מעניין בשרת ההדבקה עצמו, אשר כתובתו היא **mynewsfeeds.info** (אנו ממליצים לקוראים לבדוק את הפיירוול ואת הפרוקסי הארגוני לכתובת זו, כדי לבדוק האם הייתם מטרה של HackingTeam): עקבנו אחרי כתובות ה-URL ופרטי ה-WhoIs כדי לברר היכן רשמו אותם אנשי הקבוצה. פרטי הרישום של הדומיין הצביעו על בניין מגורים בדרום תל אביב! אולם המיקום והשם שנמצאו ב-WhoIs - דויד כהן - נראים כאמצעי הטעיה מכוון. HackingTeam מנסים לקשר את התקיפה לישראל: הם שיכפלו את שיטות הפעולה של Flame, המזוהות עם ישראל, וכיוונו את רישום הדומיין להיראות כאילו מקורו בישראל.

קובץ אחד שגילינו ב-VirusTotal.com כקשור לדומיין של mynewsfeeds.info היה tmp_privesc, קובץ שמכיל חולשת Privilege Escalation (בגרסתו המסקרומבלת והמוצפנת) העושה שימוש בדרייבר של Adobe הקיים במערכות ההפעלה של Windows ו-Mac. יתכן ועובדה זו איפשרה את השימוש הנרחב בחולשה זו, דבר שיאפשר לנו בעתיד לזהות אותה על יחידות קצה כאשר יעשה בה שימוש. חשוב לציין כי לדומיין mynewsfeeds.info קושרו רק מעט hash-ים לפני זליגת המידע של HackingTeam. לעומת זאת, מאז הזליגה הצטרפו עוד תריסר חדשים. למרות שהם לא נמצאו כמזיקים, הם הכילו את ה-hash של

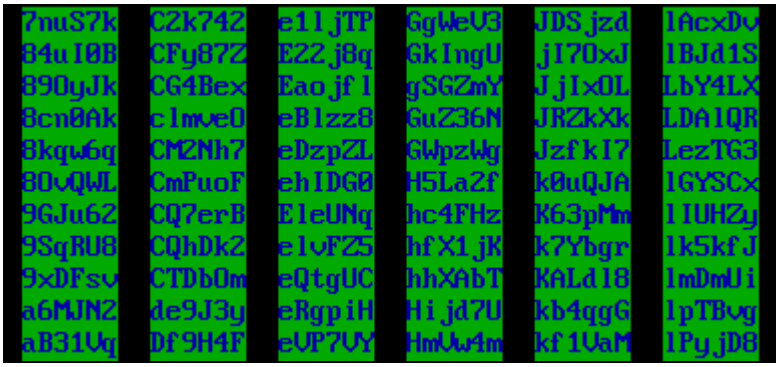
דומיין החדשות - ככל הנראה כתוצאה של מספר הקבוצות שכעת מורידות, מריצות ועורכות את הקוד בעצמן.

שרת ההדבקה: מותאם למטרה ובר תוקף

על מנת להבין את תהליך התקיפה של HackingTeam בחנו את פעילות שרת ההדבקה. להלן תרשים זרימה המתאר את התהליך:

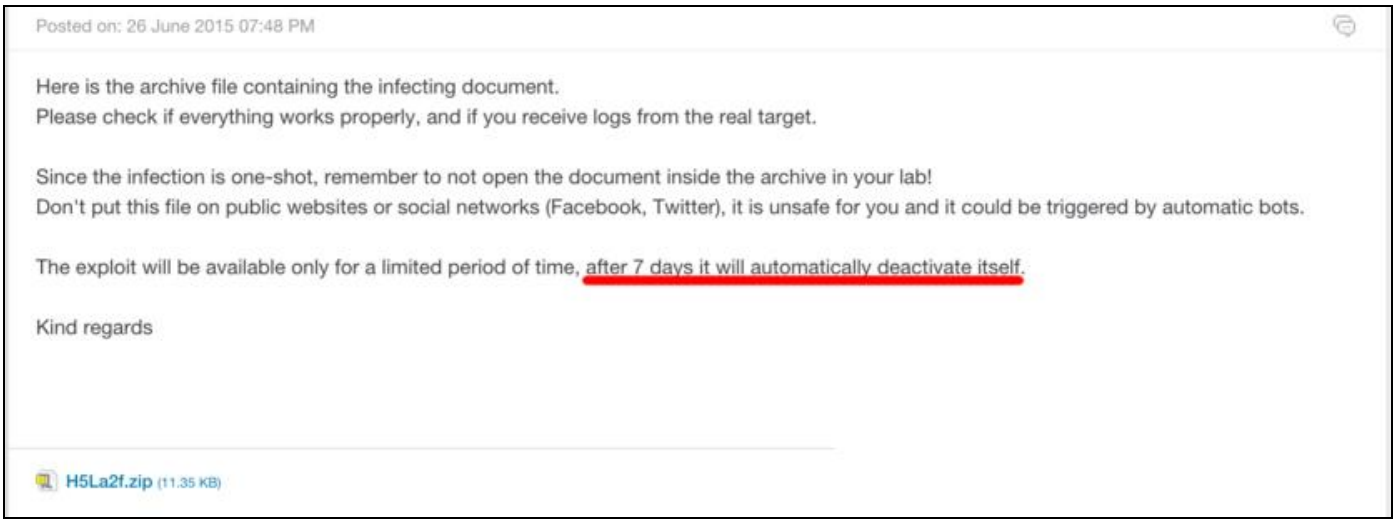


התרשים מתאר את התהליך הבא: בתחילה, השרת מעביר את המבקר לדומיין המודבק דרך Regular Expression של Mod_rewrite, על שרת ה-Apache על מנת לבדוק התאמה בין מזהה הקמפיין בן ששת התווים לבין ערכת ה-exploit ול-Payload בקובץ /var/www/files/campaignID. כאשר לא קיימת התאמה בין מזהה הקמפיין, השרת מוביל את המבקר ישירות לעמוד שגיאה 404. באם קיימת התאמה, התוכנה מתקדמת לשלב השני.



[דוגמא של אוסף מזהי קמפיין בין שישה תווים לתקיפות מבוססות מערכת הפעלה Windows]

בשלב השני, התוכנה בודקת את מונה הכניסות לקמפיין הספציפי על מנת לוודא שהוא עומד על אפס, דבר המעיד על כך שאיש עדיין לא הודבק על ידי הקמפיין הנוכחי. בנוסף, התוכנה בודקת את תאריך התפוגה של הקמפיין הספציפי לוודא שהוא בר תוקף. עד כה כל הקמפיינים של הקבוצה אותם בחנו הכילו תאריך תפוגה אחיד בן שבוע מיום יצירת הקמפיין.



Posted on: 26 June 2015 07:48 PM

Here is the archive file containing the infecting document.
Please check if everything works properly, and if you receive logs from the real target.

Since the infection is one-shot, remember to not open the document inside the archive in your lab!
Don't put this file on public websites or social networks (Facebook, Twitter), it is unsafe for you and it could be triggered by automatic bots.

The exploit will be available only for a limited period of time, after 7 days it will automatically deactivate itself.

Kind regards

H5La2f.zip (11.35 KB)

[צילום מסך של אימייל משירות לקוחות של HackingTeam המדגיש את תאריך התפוגה בן השבוע של שרת ההדבקה]

```
[general]
expiry=1435912656  Campaign Expiration Date - Fri, 03 Jul 2015 08:37:36 GMT
hits=0
pos=first

[valid]
type=data
headers[Content-Type]=text/html
headers[Cache-Control]=no-cache, no-store, must-revalidate
headers[Pragma]=no-cache
headers[Expires]=0
path=./index.html
visitdate=1435488470054  Last Valid Target - Sun, 28 Jun 2015 10:47:50 GMT
visitaddress= Vietnamese IP Address
visitagent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.130 Safari/537.36

[invalid]
type=301
headers[Content-Type]=application/octet-stream
headers[Cache-Control]=no-cache, no-store, must-revalidate
headers[Pragma]=no-cache
headers[Expires]=0                    Invalid Target Redirection:
headers[Location]=http://st.polyad.net/Vals/Script/ExtendBanner/98272.htm#http://vnexpress.net/&pos=BigLogo5&link=&otherlink=
visitdate=1435488501132
visitaddress= Vietnamese IP Address
visitagent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.130 Safari/537.36

[filters]
platform=/win/i
browser=/^(IE|Chrome|Firefox)$/

[related]
platform.swf=+2min
content.swf=+2min
customerkey.js=+2min
```

[דוגמא של קוד התיקוף של שרת ההדבקה - מתוך קמפיין תקיפה של יעד בויטנאם]

אם מונה הכניסות ותאריך התפוגה תקפים, התוכנה משווה את ה-user-agent בדפדפן של הנתקף בעזרת שימוש בספריית PHP בשם BrowseCap אשר מותקנת על שרת ההדבקה, על מנת להבטיח שהמחשב המותקף עומד בדרישות הקמפיין. לדוגמא, ראינו מקרה בו התוכנה בדקה האם מותקנים על מחשב המטרה מערכת הפעלה Windows7, ודפדפן כרום גירסה 43.0.2357.130.

עוד פריט מידע מעניין שגילינו הוא סקריפט Python בשם xp_filter.py. הסקריפט בודק את מערכת ההפעלה של הקורבן על מנת לקבוע באם היא מריצה Windows XP. במקרה והמערכת אינה ווינדוס XP, שרת ההדבקה יריץ חולשה שאינה מבוססת Windows XP. ובאם המערכת מבוססת Windows XP היא תגיש קובץ SWF מדומה: empty.swf.

```
#!/usr/bin/env python

import os
import sys
import struct


def main():
    platform = os.environ.get('_BROWSCAP__platform')
    sys.stderr.write(platform)

    target_dir = os.path.dirname(os.path.realpath(__file__))
    if platform.lower().find('xp') == -1:
        # not xp, serve the exploit
        sys.stderr.write('\nnot xp')
        sys.stdout.write(open( os.path.join(target_dir, 'platform.swf')).read())
    else:
        # xp, serve fake swf
        sys.stderr.write('\nxp')
        sys.stdout.write(open( os.path.join(target_dir, 'empty.swf')).read())


if __name__ == '__main__':
    main()
```

[סקריפט סינון XP : ההערות נכתבו ככל הנראה על ידי גורם חיצוני, ממנו קנו אנשי HackingTeam את ה-exploit]

המשך ההדבקה: השגת System Privelege ושליטה מרחוק

בשלב הבא הסקריפט מעתיק את התוכן של Payload ה"חדשות" אל STDOUT, על מנת לשלוח את ה-Payload דרך שרת הווב ומשם להעביר אותו למטרה. ה-Payload הוא למעשה אותו קוד base64 מוצפן עליו התייחסנו מוקדם יותר במאמר, המכיל את רכיב ה-RCS (רכיב השליטה מרחוק) ואת חולשה ה-privilege escalation.

עתה, יש לתוקפים יכולת הרצת Shellcode על מחשב הנתקף. ה-shellcode מריץ את חולשת ה-privilege escalation כדי לקבל הרשאות SYSTEM. לאחר מכן, מורד מהשרת הקובץ Agent.exe שהוא למעשה ה"רושעה" עצמה של HackingTeam - הלקוח של מערכת ה-RCS. חברת Trend Micro סקרה את חולשת ה-privilege escalation במאמר שבקישור הבא:

http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/

בנוסף לשרת ההדבקה הנ"ל אשר תוקף מערכות מבוססות Windows, ל-HackingTeam היו גם שרתי הדבקה אשר יועדו לתקוף מערכות מבוססות אנדרואיד, אשר השתמשו בטכניקות דומות מבלי לעשות שימוש בחולשת Flash אלא בחולשות במערכת Android.

```
#!/usr/bin/env python

import os
import sys
import struct


def main():

    browser = os.environ.get('_BROWSCAP__browser')

    sys.stderr.write('[*] Browser {}'.format(browser))
    target_dir = os.path.dirname(os.path.realpath(__file__))

    privesc = open(os.path.join(target_dir, 'news')).read()

    if 'IE' not in browser:

        article_number = os.environ.get('_REQUEST__article')


        if int(article_number) == 61441:
            sys.stdout.write(open(os.path.join(target_dir, 'news')).read())
            sys.stdout.write(privesc)
            sys.stdout.flush()
            sys.stderr.write('[*]..server')

        sys.stderr.write('[*] Chrome/FF News {}'.format(article_number))
    else:
        sys.stdout.write(privesc)
        sys.stdout.flush()
        sys.stderr.write('[*] IE len {}'.format(len(privesc)))
```

[סקריפט ה-privilege escalation והתקנת ה-Payload]

כהערת שוליים ברצוננו לציין כי המערכת של Cybereason זיהתה באופן מיידי את השימוש בחולשת ה-privilege escalation כבר עם הניסוי הראשון שלנו של המערכת במעבדה שבחברה ☺

[מערכת Cybereason מזהה את חולשת ה-privilege escalation ב-elevator.exe]

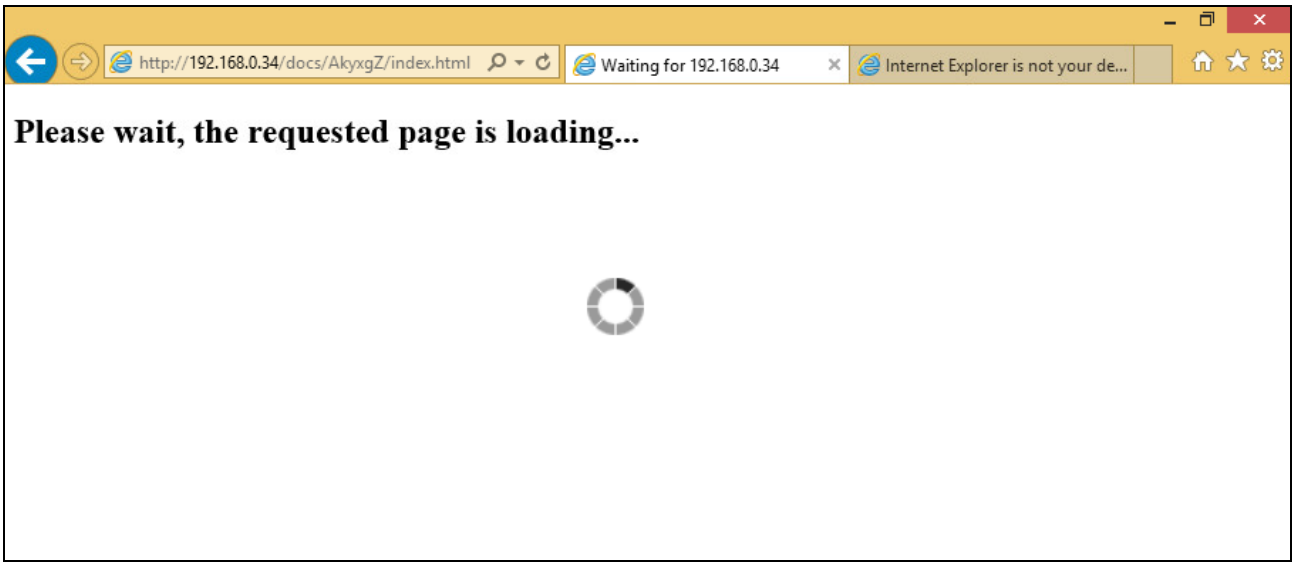
תהליך הטמעת ה-payload מרשים ברמת התחכום שלו. בעוד שרבים יטענו כי הכלים והחולשות שבהם השתמשו אנשי הקבוצה אינם מתוחכמים בפני עצמם, שיטות השימוש בהן והצירופים בהם עשו שימוש היו יצירתיים במיוחד. בנוסף, המגוון הרחב של שיטות פעולה איפשרו ללקוחות הקבוצה יכולת פעולת נרחבת כנגד יעדים שונים.

עם ביצוע ההדבקה של המטרה, רכיב ה-RCS נכנס לפעולה. ברשות HackingTeam עמד מגוון רחב של מודולים אותם יכלו להתקין, בהתאם לבקשת הלקוח, ביניהם: מודול צילום תמונות ממצלמת הרשת, מודול הקלטת שיחות סקייפ, מודול מעקב אחרי טקסט המוקלד במקלדת, מודול מעקב אחרי פעולות בנקאיות (הכוללות תשלום בביטקוין או במטבעות מקוונים אחרים), או מודול לזיהוי מיקומו הגאוגרפי של היעד.

בנוסף לכך, לקבוצה היו יכולות המותאמות לשימוש בתקיפות של טלפונים ניידים, ביניהן היכולת לשלוח הודעות SMS בלתי-נראות שעשו שימוש בחולשות במערכת ה-SMS של הטלפון ואיפשרו ל-HackingTeam להתקין את התוסף שלהם לטלפונים ניידים אשר ביצע פעולות כמו הפעלת המיקרופון של הנייד, ושידור בזמן אמת מהחדר בו נמצא הטלפון הנתקף.

Network Injector, Melter וה-Anonymizer: כלים ייחודים ל-HackingTeam

התהליך המתואר לעיל הוא רק דוגמא אחת להליך תקיפה של הקבוצה. HackingTeam העניקו מגוון פתרונות שהותאמו לצרכי הלקוח, ביניהם פתרונות שהותאמו לתקיפות של מדינות וצבאות. דוגמא אחת לכך היתה השימוש ב-network injector, כלי אכזרי במיוחד שהתחבר לתשתית שרת האינטרנט. עם הפעלתו, ה-network injector זיהה את המטרה/ות בהתאם לסט כללים שהוגדרו לו מראש על ידי הלקוח, וחיכה שהקורבן יבקר בכתובת אינטרנט מסויימת, לדוגמא - YouTube.com. כניסה לאתר המוגדר מראש על ידי הקורבן גרמה להעברתו לשרת ההדבקה במקום לאתר המבוקש. לקורבן הוצג מסך שבו נכתב "האתר בטעינה".



[זהו המסך אותו ראה היעד בזמן שה-exploit יותקן על המחשב שלו]

במקביל לשימוש ב-network injector עשו אנשי הקבוצה שימוש בכלי המכונה Melter. כלי זה איפשר ללקוחות "להתיך" את רכיב ה-RCS אל תוך הקוד של תוכנה תמימה כלשהי. על אף ששיטה זו אינה חדשה לכשעצמה, בשילוב עם ה-Network Injector היא מאפשרת לקמפיין לתקוף הורדות תוכנה ומוודאת למעשה שהמטרה/ות התקינו את רכיב ה-RCS יחד עם התוכנה התמימה אותה רצו להוריד מהרשת.

מובן שכל אחת מהשיטות שתוארו לעיל ניתנות לגילוי - ועל כן אנשי HackingTeam בנו גם תשתית להסתרת כתובות ה-IP של מערכות התקיפה: ה-Anonymizer. האנונימיזר היה פתרון מבוסס ענן שהוצע עלי ידי HackingTeam. הוא איפשר לכל לקוח להתקין שרת וירטואלי פרטי - VPS - virtual private server - אשר יכול להיות משורשר לפרוקסי אנונימי על מנת למנוע יכולת מעקב אחרי ה-collectors החיצוניים הרצים על ידי כל לקוח.

דבר זה הושג על ידי העברת המידע שנאסף מהקורבנות דרך מספר של מכונות אנונימיזציה עד ל-collector node אשר העביר את המידע חזרה ל-master node (שרת ה-C&C). להלן מספר דוגמאות של תיעוד כלי ה-Anonymizer, כפי שנאספו מתוך הוראות השימוש ב-RCS 9.6 של HackingTeam:

Introduction

An Anonymizer is used to redirect data from a group of agents and Network Injectors. The Anonymizer is installed on a server connected to Internet which cannot be reconnected to the rest of the infrastructure like, for example, a VPS (Virtual Private Server), rented for this purpose.

Several Anonymizers can be set up in a chain to increase the level of protection. Each chain leads to one Collector.

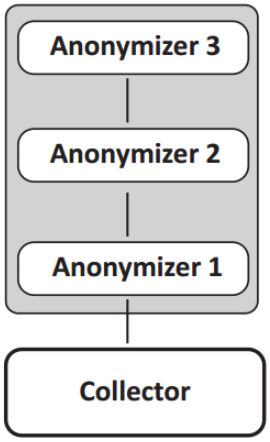


Figure 5.1: Anonymizer chain example

Communications between Anonymizer and Collector

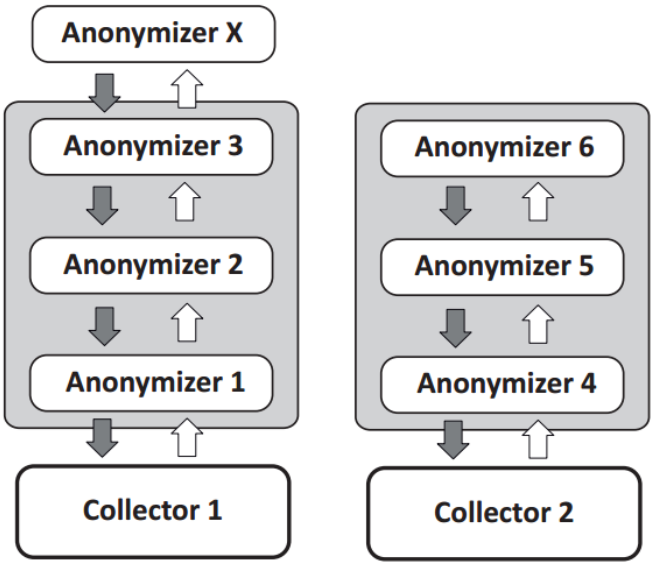
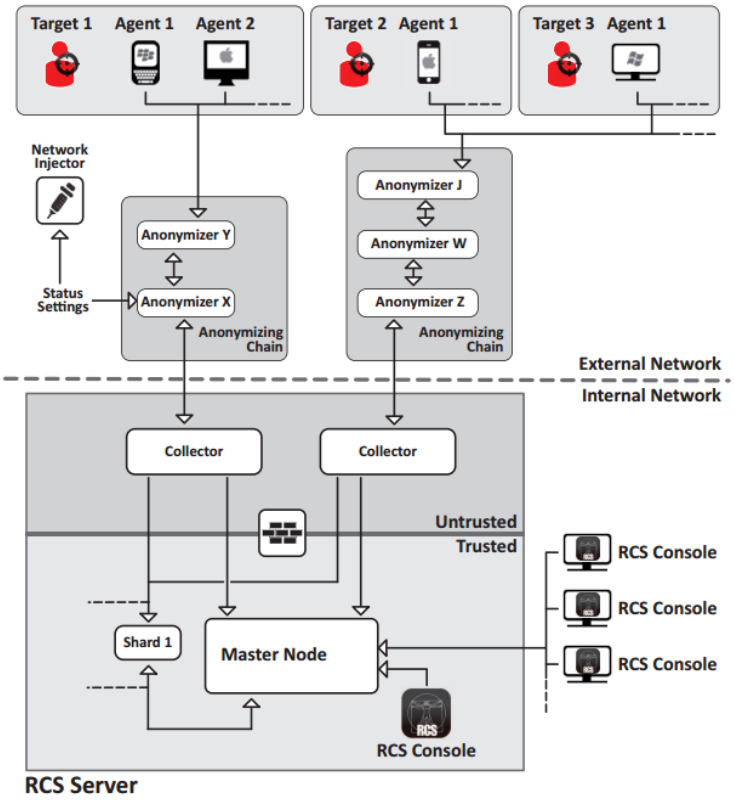


Figure 5.2: Information flow between Anonymizer and Collector



חשוב לציין כי קוד המקור של כל הכלים שתוארו לעיל זמין כעת להורדה ושימוש על ידי כל החפץ בכך. למעשה, היכולות שתוארו להלן שוחררו לאוויר העולם והן זמינות לשימוש חינם על ידי כל האקר מומחה או מתחיל. יכולות אלו, בשילוב עם הדיווחים על BGP hijacking attack (לקריאה: כאן וכאן), איפשרו ל-HackingTeam לפחות באופן תאורטי (ובהנחת נגישות מתאימה לעורקי תעבורה) להעביר את כל משתמשי האינטרנט דרך המערכות שלהם ולהדביק אותם.

לסיכום

דליפת המידע של קבוצת HackingTeam בעקבות תקיפת הסייבר על החברה חשפה שיטות תקיפה חדשות, כלים המנצלים חולשות לא ידועות, ויכולות מיסוך, הסוואה והטעיה. יכולות תקיפה מתוחכמות אלו היו עד כה ברשות האקרים הפועלים בחסות מדינות וגופים גדולים, ומעתה הן חופשיות לשימוש לכל דורש. הדו"ח לעיל חושף מספר שיטות פעולה של הקבוצה על מנת לאפשר פיתוח אמצעי זיהוי והתגוננות מפניהם.

עמית סרפר ואלכס פרייזר הינם חוקרים בחברת Cybereason, חברת סטארט-אפ המייצרת פתרון מתקדם לאיתור מבצעי תקיפות רשת מורכבים. עקבו אחרינו בטוויטר:

@0xAmit and @awfrazer