Cache method of DNS fingerprinting, Case of Citizenlab & NSO's Pegasus spyware.

**שימוש ב cache של שרת DNS לבניית fingerprints**

ב cache של שרתי DNS נשאר מיפוי כתובות IP לשמות דומיין באופן זמני, למשך זמן שהוגדר מראש לרוב על ידי בעל הדומיין. כאשר host פונה לשרת DNS לכתובת מסוימת השרת בודק ב cache שלו אם רשומה קיימת ושולח תשובה. כאשר DNS שולח תשובה חזרה שהגיעה מהcache, יש שדה נוסף בעל ערך ttl המציין מתי הרשומה תיפוג. אם ערך ttl המוחזר נמוך ממה שנקבע מראש סביר שנעשה חיפוש קודם של אותה כתובת על ידי משתמש אחר לאחרונה. שליחת בקשות לשרת DNS כדי לצפות בערך ttl נקראת DNS cache probing. בעזרת שיטה זו ניתן לעקוב אחר קשרים של hosts לשרתים שונים לפי בקשות DNS ומסלול ה query והתשובות שחוזרות אולי מרמות שונות של שרתי DNS. (בגלל קיום רשומה קודמת - יש host שרוצה ליצור קשר עם כתובת מסוימת).

**פגסוס**

לפי מסמכים שהתפרסמו קבוצת NSO מציעה שני וקטורי התקפה עם פגסוס. One click vector - המטרה צריכה ללחוץ על הלינק בהודעה על מנת שישלחו החולשות והתקנת פגסוס. Zero-click vector לא דרוש לחיצה של המטרה אלא המפעיל שולח הודעה עם אותו לינק דרך סוג מיוחד של הודעת SMS שגורמת לטלפון לפתוח באופן אוטומטי את הלינק. בשתי הדרכים נוזקות חודרות למחשב ופגסוס מותקנת על הטלפון ללא ידיעה או אישור של בעל המכשיר. לאחר התקנה המכשיר מתחיל בתקשורת עם שרתי המפעיל (C&C), מרגע התקשורת המפעיל יכול לשלוח, לבצע פקודות, לקבל גישה למידע פרטי ויכול להפעיל את המצלמה והמיקרופון. קישורי הנוזקות ושרתי המפעיל משתמשים בפרוטוקול HTTPS לכן המפעיל מחויב ברישום דומיין ואחזקתו. הדומיין מתחזה לאתר שנראה בטוח לשימוש כמו אתרי בנק, ספקי תקשורת ושירותי נוספים. לרוב שרתי הדומיין מובילים לשרתי ענן וירטואלים פרטיים המושכרים על ידי קבוצות NSO או המפעיל והם נקראים front end servers. שרתי front end מעבירים תעבורה דרך שרשרת של שרתים עד לשרתים במיקום המפעיל - back end servers.

**The Citizen Lab**

היא מעבדה בינתחומית הפועלת באוניברסיטת טורונטו ומתמקדת במחקר, פיתוח ובמדיניות אסטרטגיה ויישום חוקי של טכנולוגיות מידע ותקשורת, זכויות אדם וביטחון גלובלי. המעבדה המשתמשת בטכניקות משולבות של מדעי המדינה וחוק ומדעי המחשב, המחקר שלה כולל חקירה של ריגול דיגיטלי נגד החברה ושיטות שונות המשפיעות על חופש הביטוי ברשתות. בנוסף מנתחת מדיניות פרטיות, ביטחון ומידע של אפליקציות פופולריות, שקיפות ואחריות של מוסדות וסוכנויות על מידע פרטי ופעולות ניטור אחרות.

מעקב המעבדה אחרי מבנה פגסוס של NSO התחיל מקישור שנעשה כאשר חקרו פעיל סייבר (Threat actor) של איחוד האמירויות בשם Stealth Falcon, הוא רשם שם דומיין שעמוד הבית שלו הכיל לינק של פגסוס, ושם הדומיין שומש לשמות כתובות אימייל עבור מוצרי ריגול אחרים הידועים למעבדה. כך אספו מאפיינים של קישורים וכתובות הקשורות לפגסוס, חיפשו כתובות ושרתים בעלי מאפיינים דומים כדי לגלות את המבנה של תוכנת פגסוס. באוגוסט 2016 קיבל אחמד מנסור (פעיל זכויות אדם באמירויות) הודעות עם לינק עם הבטחה לקבלת סודות. אחמד מנסור היה כמה פעמים בעבר מטרה לריגול דרך שליחת לינקים לאימייל שלו. המעבדה קיבלה ממנו את ההודעה והקישור בה. הם לחצו על הקישור וקיבלו 3 zero days exploits והתקנה של תוכנת פגסוס. מהלינק שקיבלו הם בנו טביעות אצבע, סרקו את הרשת לשרתי front-end נוספים. הם סרקו את הרשת למציאת /redirect.aspx וגם /support.aspx, שרתי פגסוס החזירו דפי פיתיון (decoy pages). דפים המוצגים כאשר משתמש שאינו רצוי ניגש לשרת, מוצגים כדפים בטוחים.הפעולה של הצגת הדפים האלו נמצאת בקוד של שרת תוכנת הריגול ובחקירה הדפים המעבדה מצליחה לבנות טביעות אצבע כדי לזהות שרתים נוספים בתקשורת עם אותו שרת או למצוא מפעילים אחרים אם תוכנת הריגול משומשת על ידי כמה מפעילים.

לאחר לחיצה ראשונה על הקישור שקיבלו מאחמד מנסור ולפני שפרסמו את הממצאים שלהם, כל שרתי front end ש citizen lab מצאה הורדו כנראה על ידי קבוצת NSO, לאחר שבועיים חלק מהשרתים עלו לרשת שוב אבל הוסרו דפי /redirect.aspx ו /support.aspx ונעשו שינויים בקוד השרת כדי לאפשר סגירת חיבור התקשורת עם השרת ללא החזרת מידע מהשרת אלא אם החיברו נעשה דרך לינק exploit שהשרת מזהה כתקין. השינויים האלו מתאימים לשינויים שבוצעו ממקרים קודמים של המעבדה לאחר שחשפו טביעות אצבע של מתחרים. השרתים שעלו מחדש לא תאמו יותר את טביעות האצבע שהמעבדה אספה ולכן חקרו מחדש לבניית טביעות אצבע חדשות וסקרו רשת תדירות. בין השנים 2016-2018 מצאו 1091 כתובות IP ו 1014 שמות דומיין המתאימים לטביעות אצבע 'החדשות'.

המעבדה חקרה את התנהגות של כמה שרתים החשודים כשרתי פגסוס ופיתחה 3 טביעות אצבע.

טביעת אצבע ראשונה ב TLS - transport layer security.

TLS הוא פרוטוקול להצפנת תקשורת מבוססת web בין הלקוח לשרת, בעזרת חבילות ואלגוריתמי הצפנה שונים. לאחר סיום חיבור TCP מתבצעת גם לחיצת יד של TLS, מצד הלקוח נשלחת הודעת client hello עם פרטי ההצפנה שמתאימים לו.השרת מנתח את ההודעה משווה בין רשימת ההצפנות של הלקוח לרשימת הצפנות שהשרת תומך בהם ושולח בחזרה הודעת server hello ולאחר פרטים, בדיקות ותקשורת נוספת מסתיימת לחיצת יד של TLS כאשר השרת והלקוח מתואמים עם שיטות ההצפנה. בהודעות שמתחלפות בין הלקוח לשרת וההפך יש שדה של רשימת הצפנות- הרשימה תלויה בספריות TLS שונות, ניתן לבנות טביעות אצבע לפי TLS והספריות הנמצאות של שרת או לקוח בהשוואה לאותם ספריות, ולהתאים hosts ושרתים לפי ספריית ה TLS. לפי פרטי השדות בתקשורת של TLS handshake המעבדה הצליחה לבנות טביעת אצבע.

שתי טביעות אצבע נוספות הציגו הגדרות קונפיגורציה שונות שצפו במהלך הסריקות. אם שרת מתאים לטביעת אצבע 1 ולאחת מהטביעות 2 או 3 השרת מוגדר כחלק ממבנה פגסוס של קבוצת NSO. הם השתמשו בטכניקת athena כדי לקבץ את התוצאות ל 36 קבוצות שונות. כל קבוצה מייצגת מפעיל של פגסוס אך עלול לייצג מערכות הדגמה ובדיקות. במהלך הסקירה והתוצאות citizen lab לא פרסמה טביעות אצבע ספציפיות או טכניקות כדי למנוע נזק משימוש של קבוצות חיצוניות ליצירה רשימות דומיינים של NSO. במהלך הסריקות כחלק משמירת אתיקה של DNS probing הם התחשבו בהשפעת הפעולות והסריקות שלהם על משתמשים שאינם מטרתם ושאפו לצמצם את הסיכוי של כל הפרעה.

**שיטות נוספות ל DNS fingerprinting:**

גישה פסיבית לבניית טביעות DNS - גישה שונה לטכניקת טביעות אצבע לזיהוי התוכנה המותקנת על שרתי DNS resolver. אוסף מידע באופן פסיבי לפי התעבורה, בשיטה זו אין צורך בשליחת בקשות במהלך הסריקה. בתחילה יבחנו דפוסים של שאילתות DNS בכוונה מתוכננת וינסחו חוקים הנצפים בתוצאות כדי לזהות תוכנה ומערכת הפעלה של השרת DNS.

DONUT -

Domain oriented network unmasking tool, מערכת לזיהוי ע"י טביעות אצבע וגילוי של סוג מערכת הפעלה, סוג המכשיר, תוכנות ומבנה התקשורת לפי תעבורת DNS. גישת התוכנה היא שימוש בחוקים כדי לזהות מאפיינים מסוימים ומאפשר להרחיב את השרת הנתונים שלה. בנוסף התוכנה מסוגלת לזהות הגדרות NAT ולחלק לבצע de-NAT לתעבורת DNS - לזהות את כתובת המקור אמיתית ללא השפעת NAT.

Fpdns - DNS server fingerprinting tool

תוכנה לזיהוי מרחוק וקביעת גרסאות שרתי DNS על ידי שליחה שאילתות DNS והשוואה מול טבלה של תשובות וגרסאות שרתים שונות.

ביבליוגרפיה

<https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

<https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

<https://fingerprint.com/blog/what-is-tls-fingerprinting-transport-layer-security/>

<https://www.researchgate.net/publication/262347575_Towards_passive_DNS_software_fingerprinting>

<https://linux.die.net/man/1/fpdns>