Digital Whisper
Technologic Papers

אז מה קרה החודש?

מאת ים מסיקה

צנזר- אות-

בין הוויכוחים הלוהטים ביותר שיוצא לי לנהל בשנים האחרונות הוא על נייטרליות הרשת ועל החופשיות של האינטרנט. ממשלה צריכה להתערב? לספקיות מותר להתערב? התוכן צריך לעבור צנזורה או להישאר ללא מגע ידם של גופים ושל ממשלות?

נרצה או לא, כיום המצב הוא שממשלות אכן משפיעות על דברים שנמצאים באינטרנט. אם מדובר בחוקי זכויות־יוצרים שגורמים לסגירתם של אתרי הורדות ואתרים אחרים, אם אלו חוקי הימורים שגורמים לחסימת אתרי הימורים בעולם ואם אלו חוקי הצנזורה שמגבילים את התבטאויותיהם של כלי התקשורת.

מדינות קיצוניות יותר אף מגדילות לעשות וחוסמות אתרים שמכילים תוכן שמבקר את הממשלה או מפלגות מסוימות. באותן מדינות הגישה לעבודות עיתונאיות ושל קבוצות בעלות דעה שונה משל השלטון עלולה להיאסר.

מאחר שכיום בתי־המשפט בעולם מסוגלים לדרוש מספקיות האינטרנט להוריד אתר מסיבה כזו או אחרת, נוצר HTTP Status code שמספרו 451 ומטרתו לציין "חוסר זמינות עקב סיבות חוקיות". בפועל: נחסם עקב הוראת בית־משפט. שרת שמגיש דף שכזה עלול לכלול את כל המידע החשוב הנוגע לחסימה, כולל קישורים לצו בית־המשפט הרלוונטי, איך "לאתגר" את החסימה והסבר על החוק שמאפשר לבית־המשפט לחסום אתרי אינטרנט במדינה. ה־הצעה ל־Status code אושרה על ידי ה־IETF ב־18 בדצמבר.

מספר ה־Status code נבחר לא במקרה, ויש בו ריח חזק של אמירה נוקבת. הוא קורץ לספרו הדיסטופי של ריי ברדבורי ששמו "451 פרנהייט", המתאר עולם שבו ספרים הם מחוץ לחוק.

מדובר ברעיון מבורך, אבל במקומכם לא הייתי ממהר לבזבז את בקבוקי האלכוהול שקניתם לנובי־גוד. בשבועיים האחרונים הספקתי לראות את הצהלה ההזויה במדיה שאומרת ש"ממשלות כבר לא יוכלו להסוות שהן צנזרו דפים באינטרנט". כמובן שמדובר בשטויות מוחלטות, שכן בתי־המשפט תמיד יוכלו לכפות על אתרים להחזיר שגיאת 404 עבור עמודים שצונזרו.

שני רווחים בביטים... והופ, אתם בפנים

ב־14 לדצמבר התפרסמה פרצה ב־Grub2 (ה־Boot loader הנפוץ במערכות Linux) שהצליחה לעשות הרבה מאוד באזז. הגרסאות הפגיעות הן כל הגרסאות מ־1.98 (דצמבר 2009) ועד 2.02 (דצמבר 2015).

הדבר שאולי הקנה למתקפה הכי הרבה פרסום הוא הפשטות המגוחכת להפליא שלה: בזמן שאתם במסך ה־GRUB2 והוא מבקש מכם שם משתמש, לחצו 28 פעמים על מקש ה־Backspace. במידה ואתם פגיעים - מזל טוב, יעלה לכם מסך של GRUB Rescue ומפה אתם יכולים לעשות מה שבא לכם.

הפרצה ניתנת לניצול רק בעזרת גישה פיזית למכונה, ומאפשרת לתוקף לעקוף כל סוג של אימות, בין אם הסיסמה נשמרה כטקסט או מוצפנת. תוקף שיבצע את המתקפה בהצלחה יזכה בגישה מלאה למחשב דרך ה־GRUB Rescue shell.

על איך עובדת החולשה מאחורי הקלעים, בקצרה[1]: על ידי לחיצה על Backspace 28 פעמים אתם גורמים ל־Overflow וכותבים על ה־Return address של הפונקציה שבה אתם נמצאים, מה שגורם לקוד שלכם לקפוץ לכתובת 0x0 בזיכרון, שם יש שם לולאה שעורכת את עצמה ובסופו של דבר קופצת לפונקציה grub_rescue_run, שמריצה את ה־Grub rescue.

אם כל העניין הזה עושה לכם Déjà vu, יכול להיות שזה בגלל הבאג המוזר שהתפרסם לפני כשנה וחצי ב־Unity, מעטפת הממשק של הפצת הלינוקס Ubuntu, בזכותו אדם עם גישה פיזית למכונה יכול היה ללחוץ ארוכות על מקש ה־ENTER ולעקוף את מסך הנעילה.

באג מיליון הדולר

במאמר שפרסמו בלומברג על תכנית ה־Bug bounty של Facebook ב־2012 כתבו ש"אם יהיה תקל ששוויו מיליון דולר, אנחנו נשלם את זה". החודש יצא לבחור אחד, וסלי, לבחון את האמת של האמירה הזו.

בשיחה ב־IRC, חבר נתן לו טיפ. הוא מצא כתובת מעניינת, תת־דומיין של Instagram בכתובת https://sensu.instagram.com שמאחוריה יש שירות Sensu-Admin שרץ מעל Ruby On Rails ועלול להיות פגיע. הבחור הסתכל על הקוד של Sensu-Admin ומצא שם מפתח סודי שמוגדר כברירת מחדל, ושאם Instagram לא שינו אותו הוא עלול לעזור לזיוף Session ואפילו להרצת קוד מרוחקת. למרבה ההפתעה, כך קרה - והוא הצליח להריץ קוד מרחוק ודיווח על כך.

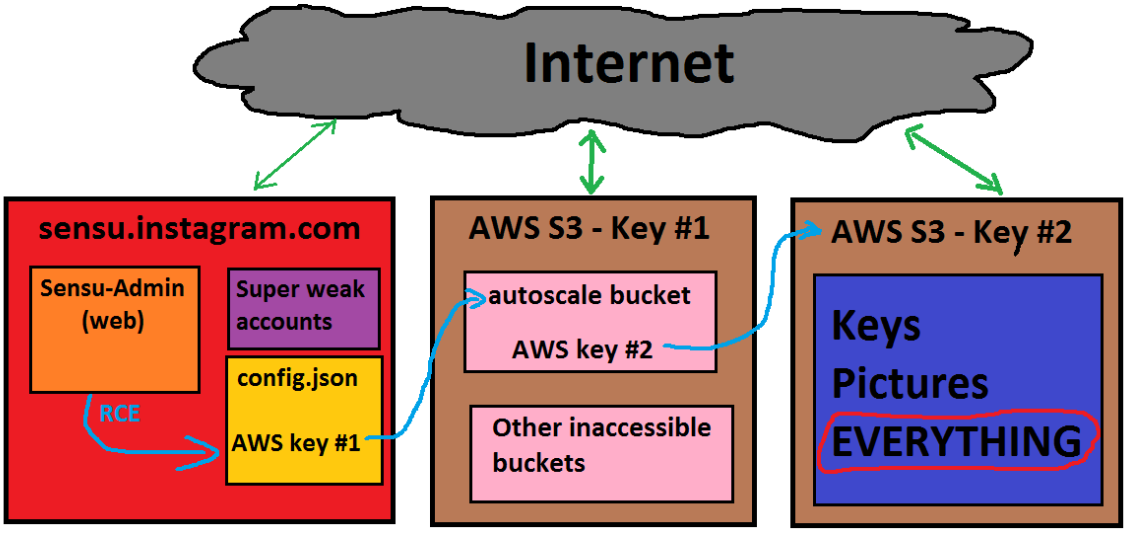
למרות זאת, הוא עדיין לא הצליח להתחבר לממשק בכתובת הזו. הוא השתמש ב־RCE כדי לקבל גישה למסד־הנתונים, ומשם שלף את שמות המשתמש והסיסמאות לממשק (שהיו כמובן מוצפנות; אפילו עם

[1] לפרטים טכניים מקיפים אמליץ לכם לקרוא את הפרסום המלא.

bcrypt). אחרי ממש מעט זמן הוא הצליח בעזרת JTR לגלות 12 סיסמאות שהיו מובנות מאליהן: password, changeme, Instagram וסיסמאות שזהות לשם המשתמש. הוא שלח דיווח שני.

במקביל, הוא בדק מה יכול להיות ב־/etc/sensu/config.json. הוא מצא שם הרשאות לא רק למסד הנתונים, אלא גם לחשבונות דואר אלקטרוני ול־Pagerduty,[2] ואפילו מפתח לחשבון AWS.[3] הוא התחיל בלבדוק מה הוא יכול לגלות אם הוא יסתכל על חשבון ה־S3[4] שלהם, וגילה שהוא לא יכול לגשת לשום דבר - פרט לתיקייה אחת. התיקייה הזו הכילה קובץ tar.gz בו לא היה שום דבר מעניין, אבל בגרסאות הקודמות של אותו קובץ היה קובץ Vagrant עם עוד מפתח לחשבון AWS, שהפעם כלל גישה לכל שאר תיקיות ה־S3.

מה היה שם, אתם שואלים? מעבר לתמונות של משתמשי Instagram: קוד המקור של גרסה די חדשה של Instagram, SSL Certificates ומפתחות פרטיים, מפתחות API לכל שירות אפשרי (Twitter, Facebook, Thumblr, Flickr, OAuth, reCAPTCHA) ומפתחות שנועדו לייצר את העוגיות ב־Instagram. וסלי שלח דיווח שלישי, הפעם עם 7 סעיפי חולשה חדשים. בדיווח שלו, הוא כלל את הסעיף "אם ישנם כלי תיעוד מופעלים, הרי שאף אחד לא בודק אותם שכן בשום שלב לא זיהו את הנתונים אליהם ניגשתי".



עד מהרה הדיווח התגלגל להיות ויכוח של ממש. בתגובה לדיווחים של וסלי ענו בחברת Facebook: "שלום וסלי. תודה שדיווחת לנו. אנחנו שולחים את המידע לצוות המוצר הרלוונטי למחקר נוסף. אנו נעדכן אותך בנוגע להתקדמות שלנו. אנא קח בחשבון שנקיטת צעדים נוספים אחרי שמצאת פרצה מפרים את תכנית הפרסים שלנו. בעתיד אנחנו מצפים שמתוך רצון טוב תעשה מאמץ להימנע מהפרות של פרטיות, הרס מידע והפרעה או פגיעה לשירותים שלנו במהלך המחקר שלך".

[2] שירות שמספק כלי מעקב אחרי הזמינות והביצועים של השירות שלך.
[3] שירות Amazon Web Services. מספקים הרבה שירותים מגניבים כמו S3 (אחסון קבצים ב־Cloud) ו־EC2 (שרתי Cloud).
[4] שירות אחסון הקבצים בענן של Amazon.

משם החלו חילופי דברים שגרמו מהר מאוד לסגירת הדיווח של וסלי בלי לתת לו פרטים נוספים. כשפתח וסלי קריאה נוספת וביקש תשובות, ענו לו "שלום וסלי. אנו מעריכים את הדיווח שלך, אך הוא אינו זכאי להיות חלק מתוכנית הפרסים שלנו. ניצור עמך קשר אם יהיו לנו שאלות נוספות". כששאל האם הוא יכול לפרסם את ממצאיו, ענו לו: "ההחלטה האם לפרסם בידיך, אנו לא נותנים או מונעים אותה באופן מפורש".

נשמע שכאן היה יכול להסתיים הסיפור, אבל בבוקר שלמחרת הדיווח השלישי, כך לפי דבריו של וסלי, הוא קיבל טלפון מהמנהל שלו. המנהל אמר שהוא היה בשיחה עם מנכ"ל החברה בה וסלי עובד. מסתבר שאל המנכ"ל התקשר בחור בשם אלכס סטמוס, ה־CSO של Facebook. הוא אמר שוסלי השתמש במידע רגיש שהוא השיג על ידי פרצת אבטחה, ובזמן שהיא הייתה "טריוויאלית ובעלת ערך זעום" היא גרמה לדאגה גדולה בקרב עובדי החברה.

לפי דבריו של וסלי, אלכס אמר שהוא לא בטוח אם הוא רוצה לפנות לרשויות החוק, ושהוא לא רוצה לערב את הצוות המשפטי של Facebook. הוא דרש שוסלי לא יפרסם את פרטי החולשה, שישמור את כל הגילויים לעצמו ולא יפרסם אותם, יאשר שהוא לא ניגש לפרטי משתמשים ושימחק את כל המידע שהוא השיג ממערכות Instagram.

וסלי כתב בבלוג שלו שבקשותיו של אלכס הן ההפוכות מהכתוב במדיניות של Facebook: "אם תאפשר לנו זמן מספיק להגיב לדיווח שלך לפני שתהפוך מידע לפומבי, ומתוך רצון טוב תעשה מאמץ להימנע מהפרות של פרטיות, הרס מידע והפרעה או פגיעה לשירותים שלנו במהלך המחקר שלך, אנחנו לא נפתח בשום תהליך משפטי כנגדך או נבקש מרשויות אכיפת־החוק לחקור אותך". הוא ציין את האיומים לכאורה של Facebook ואת הפנייה למעבידים שלו ישירות לרעה.

אלכס הגיב בעצמו לדבריו של וסלי ואמר שהציעו לו 2,500$ למרות שהוא לא היחיד שמצא את הפרצה, ושהפנייה למעסיק נעשתה מכיוון שחשבו שוסלי מייצג את החברה. הוא אמר שהם ביקשו לא לפרסם רק את הפרטים של הגישה ל־S3 וכל מה שקרה אחר־כך, מכיוון שמדובר בניצול לרעה של תכנית הפרסים.

את טענות כל אחד מהצדדים תוכלו לקרוא כאן (אלכס) וכאן (וסלי).

ערער מעורער

חברת ציוד התקשורת Juniper Networks יצאה בהודעה דרמטית משהו שפורסמה ב־17 לחודש. עיקר ההודעה, שנוגע למוצר ה־Firewall שלה, היא פִּסְקָה שהצליחה להצית גל תקשורתי רחב של ידיעות וספקולציות:

> "במהלך סקירת קוד פנימית שביצענו לאחרונה, Juniper גילתה קוד לא מורשה ב־ScreenOS שיכול לאפשר לתוקף בעל ידע להשיג הרשאות ניהול למכשירי NetScreen® ולפענח חיבורי VPN מוצפנים. מרגע שזיהינו את הפגיעות הזו, פתחנו בחקירה לעניינם של הדברים, ועבדנו על־מנת לפענח ולשחרר גרסאות מתוקנות עבור הגרסאות האחרונות של ScreenOS."

אם לקחת את התוכן מהפסקה הזו ולהסתכל על ה־Security advisory, Juniper אומרת בהודעה שישנן שתי פרצות, שתיהן מזוהות כ־CVE-2015-7756: הראשונה מדברת על כך שניתן לפענח את כל התעבורה שעוברת ב־VPN שהגדרנו ל־Firewall, והשנייה אומרת שניתן לגשת לאפשרויות ניהול במוצר גם אם אין לכם באמת הרשאות לכך.

בפרסומיה Juniper כמעט ולא נותנת לנו מידע קונקרטי על הפרצה ואיך היא עובדת, ומשתדלת לשמור על נוסח כמה שיותר מעורפל בכל הקשור לפרטים טכניים. בנוגע לפרצה שנוגעת לכניסה כמנהל, כתוב בכמה מילים על כך שאם ניצלו אותה התיעוד יראה לנו[5] שמשתמש בשם system התחבר למערכת. בנוגע לפרצה שנוגעת לפענוח תעבורה שעוברת מעל VPN הם לא מרחיבים מעבר לכך ש"שהתוקף צריך להאזין לתעבורה המוצפנת".

ה"קוד הבלתי מורשה" שהם מדברים עליו, כך נראה, הוכנס למערכות לראשונה בספטמבר 2012, וטלאי שמתקן את הפרצות שהוכנסו לקוד שוחרר ביום פרסום ההודעה. בכל מקרה, הסיפור הזה מדיף ריח מוזר מאוד שגרם לקהילת ה־Security לשאול הרבה שאלות:

1. "קוד לא מורשה"? האם זה אומר שמישהו חיצוני הצליח לגשת ל־Code repository של Juniper ולערוך אותו? מי יכול לבצע דבר כזה?
2. בהודעה מאוחרת יותר מיקדו Juniper את הניסוח: "חולשת פענוח ה־VPN עלולה לאפשר לתוקף בעל ידע[6] שיכול להאזין לתעבורת VPN לפענח את התעבורה הזו". מה זה אומר "תוקף בעל ידע"? אנשים רבים ברחבי האינטרנט טענו שמדובר ב־NOBU קלאסי.[7]
3. למה Juniper נמנעה מלהכניס פרטים טכניים לתוך כל אחת מההודעות שלה?

מיד אחרי הפרסום, ואולי בעקבות הניסוח המעורפל וסימני השאלה הרבים שצצים ממנו, החלו חוקרים למיניהם עטים על המציאה ומנסים לנתח כל דבר אפשרי שקשור לאותה הודעה של Juniper. אנשים

[5] אם לא שינו אותו. לא סביר בשום צורה שהיא. אם אתם הייתם כותבים Backdoor, זה לא בדיוק מה שהייתם מחפשים להעלים מהתיעוד?
[6] במקור: "Knowledgeable Attacker".
[7] Nothing But Us. פרצות קטנות שמושתלות על ידי ארגוני ביון בצורה שאף־אחד לא יוכל לזהות או להשתמש בהן חוץ מהם.

החלו להשוות את ההבדלים בין הגרסה של לפני התיקון לזו שאחריה, HD Moore פרסם ניתוח שמפרט בדיוק איפה הושתלה הדלת־האחורית ומה הסיסמה שהושתלה ובעזרתה ניתן להתחבר למוצרי Juniper(!), ראלף פיליפ פרסם ניתוח שמראה איך אפשר לפענח את התקשורת מעל ה־VPN, ומת'יו גרין דיבר על הקריפטוגרפיה שמאחורי הדלת־האחורית ב־VPN.

ניסיתי לסכם את זה בקצרה (כי אפשר לקרוא על זה המון - כמעט - בכל - מקום), אבל לא כזה הלך לי. אז הנה הסיפור הכמה־שיותר־מלא[8]: כש־Jupiter רצו ליצור מפתח שיצפין את התקשורת של המוצרים שלהם, הם השתמשו בתקן שה־NSA קידמו. לתקן קוראים Dual_EC DRBG ומטרתו יצירת מספרים אקראיים. ב־2007 רשות התקינה הלאומית של ארצות־הברית (NIST) הכירה בו ועודדה את השימוש בו.

כדי להשתמש ב־Dual_EC DRBG לצורך יצירת מספרים אקראיים, יש צורך לספק לו שני פרמטרים, P ו־Q, כאשר אותם P ו־Q הן שתי נקודות על עקום אליפטי כלשהו. NSA סיפקו 2 נקודות "ברירת מחדל" כחלק מהתקן שקידמו (תודה רבה באמת). זמן קצר לאחר שהוכר כתקן על ידי ה־NIST, מצאו בו שני חוקרים ממיקרוסופט חולשה משמעותית.

הם הראו שאם P ו־Q נבחרים באופן מאוד מסוים, כך שיש משוואה שמקיימת Q=P*e עבור e כלשהו (שנשמר בסוד), מי שיצר את אותם פרמטרים חשודים (P, Q) יכול לחזות מה יהיה הפלט ה"אקראי". בשביל לגלות את e יש צורך בכוח חישובי רב מאוד. בשלב הזה אולי כדאי לציין שלפי הדלפות של סנודן משנת 2013, נראה שהחולשה לא הפתיעה מדי את ה־NSA. למעשה, היא די הייתה שם בכוונה תחילה.

אחרי אותה הדלפה ב־2013, Juniper מיהרו לצאת בהצהרה שהם אכן עושים שימוש בתקן Dual_EC DRBG, אך הם אינם עושים שימוש בפרמטרים המומלצים (בפועל הם השתמשו ב־Q משלהם). יותר מזה, המערכת משתמשת בתקן יצירת מספרים אקראיים נוסף, שנקרא ANSI X.9.31 ושהפלט של Dual_EC עובר דרכו.

הפתעה! עקב באג מוזר שנמצא במערכת, האלגוריתם השני לא באמת עבד. התוצאה הסופית הייתה בפועל הפלט של ה־Dual_EC, מה שחוקרים הגדירו אחר־כך כ"תקל קטסטרופלי".

אבל רגע! טכנית, אנחנו אמורים להיות בטוחים! יהיה בלגאן רק אם ה־Q הוא Q שנבחר בקפידה על ידי התוקף, ו־Juniper הרי השתמשו ב־Q משלהם, לא?

אז... כן. ולא. מסתבר שאותו Q מיוחד שהוגדר על ידי Juniper שונה ב־2012 על־ידי אותו תוקף מסתורי, שכנראה יודע מה ה־e המתאים. בתיקון שהם הוציאו החודש, Juniper החזירו את Q למה שהיה לפני 2012, וכך פתרו את הבעיה.

[8] המתמטיקאים שביניכם יאלצו לסלוח לי על חוסר־הדיוק והשמטת הפרטים הרבים. מי שבאמת מעוניין, כדאי שיקרא את המאמר של ראלף.

למרות זאת, גם אחרי התיקון עולות שאלות רבות לגבי התנהלות Juniper. למה הם משתמשים באלגוריתם שיש בו סיכון ועוטפים אותו באלגוריתם אחר לצורך הגנה? האם מדובר בצירוף מקרים ש"בטעות" לא עשו שימוש באותו אלגוריתם שני? למה התיקון שלהם כולל רק את החזרת ה־Q למצבו הקודם, ולא טיפול בטעויות המימוש הפונקציונליות? ובכלל, למה Juniper מסרבת לגלות איך היא יצרה את ה־Q? יכול להיות שהיא בעצמה מחזיקה ב־e מסוים ורוצה לעקוב אחרי המשתמשים שלה?

בחלק מהעיתונים ואמצעי המדיה נפוצה הסברה שמדובר ב־FEEDTROUGH, יכולת של ה־NSA שדלפה בעבר ומאפשרת לה לשתול דלתות־אחוריות במוצרי חומת־אש של Juniper, ושלפי המסמכים שדלפו "הופעלה במערכות רבות". הדבר לא סביר מכיוון שבמסמכים שדלפו נראה שמדובר בהשתלת חומרה שמתבצעת במכשירים לפני שהם נשלחים ללקוח.

מסמך חדש שהודלף על ידי סנודן מופץ גם הוא בתקשורת. במסמך, שנכתב בשיתוף פעולה בין ה־NSA לבין ה־GCHQ ומסווג כ־"TOP SECRET", כתוב בבירור שה־NSA מכירה פרצות אבטחה קיימות במוצרי Juniper עוד מאז שנת 2011. נוסף על־כך, מסתמן שיתוף פעולה פורה בין שתי סוכנויות הביון בכל הנוגע לניצול המוצרים של Juniper לצורכי מודיעין: "השיתוף של ה־NSA בכל הקשור בטכנולוגיה של Juniper שופר בצורה דרמטית במהלך שנת 2010 לצורך ניצול מספר רשתות יעד ש־GCHQ הייתה נגישה אליהם קודם לכן".

חשוב לזכור שנראה שהפרצות הקשורות למאמר הושתלו רק ב־2012, מה שמעיד על כך שהמסמך המודלף אינו קשור למקרה הנוכחי, לפחות לא באופן שהוא יותר מהצהרת כוונות.

עוקרים מהשורש

ב־30 בנובמבר בשעה 6:50 (UTC) קיבלו שרתי השורש (DNS Root Servers)[9] בעולם כמות בקשות בלתי סבירה בעליל, במה שנראה כמתקפת DDoS על השרתים. הכמות עלתה ועלתה במשך כמעט 3 שעות, עד שהגיעה בשיאה לכ־5 מיליון בקשות עבור כל שרת בכל שנייה, ופסקה לחלוטין בשעה 9:30. ההתקפה חודשה למשך שעה בדיוק ב־1 בדצמבר בשעה 5:10.

ב־30 בנובמבר כל השאילתות שנשלחו כחלק מהמתקפה היו על־אודות דומיין מסוים, ובהתקפה ב־1 בדצמבר השאילתות היו על־אודות דומיין אחר. הבקשות הגיעו מכמות מרשימה של כתובות IP, כך שקשה לנחש מי הוא שעומד בבסיס המתקפה[10], והמניעים העומדים מאחוריה אינם ברורים. ברוס שנייר העלה את ההשערה שמדובר בניסוי ליכולת תקיפה.

רשת האינטרנט תלויה במידה רבה בשרתי ה־DNS, והארכיטקטורה שלהם חסינה ויציבה מאוד על־מנת לתת מענה למקרים שבהם מנסים להזיק להם או להשבית אותם בהתקפות שכאלו. כך, לדוגמה, בעולם יש 13 שרתי שורש[11], הם מופעלים על ידי 12 ארגונים שונים ונמצאים ב־6 יבשות שונות. ה"שרתים" האלו הם לא באמת שרתים, אלא חוות שרתים גדולות שמורכבות משרתים פיזיים רבים - שרת L הועתק ל־128 מקומות שונים שנמצאים ב־127 ערים שונות ב־68 מדינות, מארגנטינה ועד תימן.

למרות הכול, יש חדשות רעות: בשלב מסוים, מספר פניות לגיטימיות לשרתי השורש אכן הסתיימו ב־Timeout מצד חלק מהם. מנגד, החדשות הטובות הן שחלק מהשרתים היו נגישים מכל מכונות הבקרה לכל אורך המאורע, כך שלא היו דיווחים מצד משתמשי הקצה על בעיות, והבלגאן הסתכם בעיכובים כמעט לא מורגשים עבור שאילתות מסוימות.

בעקבות המתקפה חסרת התקדים הוציאו root-servers.org, האחראיים על שרתי השורש, הודעה לכלל הציבור, בה פרסמו פרטים בסיסיים על ההתקפה (שהובאו כאן במלואם) והמליצו לספקיות לאמץ את BCP-38, הצעה שמטרתה אימות כתובת המקור של התעבורה היוצאות ממכונה מסוימת וכבר מיושמת ברוב גדול של הספקיות.

למרות שעדיין לא יצא לנו לחזות בהתקפות בסדר גודל שכזה על שרתי ה־DNS, זו בהחלט לא פעם ראשונה שמהלך שכזה מתבצע. מתקפות דומות קרו עוד ב־2002 וב־2007, ואיום משעשע להחשכת האינטרנט שוגר מצד אנונימוס בשנת 2012.

[9] תאשימו את איגוד האינטרנט הישראלי.
[10] אף שייתכן שכתובות אלו זויפו.
[11] שמו של כל שרת מיוצג על ידי אות. A, B, C... עד M.

החודש זכינו במאמר חדש מהחבר'ה ב־ESET, שמספרים לנו שהם גילו משהו מוזר שקרה בחודש אוקטובר באתר של Ammyy, תוכנת שליטה מרחוק. אלו שבחרו להוריד את הגרסה החינמית זכו לקבל תוספת במתנה.

בשביל הגיוון והעניין, כמעט כל יום המורידים של התוכנה זכו לקבל תוספת אחרת: ב־26 הם קיבלו את Lurk, ב־29 את Corebot, את Buhtrap ב־30 ואת Ranbyus או את Netwire RAT ב־2 בנובמבר. נראה שאותו אחד שפרץ לאתר מכר גישה לבעלי הכלים השונים, ונראה שהיו די הרבה קופצים על המציאה...

Buhtrap נשמע לכם מוכר? זה לא במקרה. בשלהי שנת 2014 זיהו חברת ESET מספר מחשבים ברוסיה, שנראה שמתנהגים מוזר במשך השנה האחרונה. היה נראה שכלי כלשהו שמוגדר לפעול רק על מחשבים רוסיים עושה כמה דברים לא נחמדים בכלל. הוא מנצל תוכנה פופולארית ברוסיה בשם Yandex Pluto[12] לצורך רחרוח אחרי דברים שהמשתמש מקליד, הוא דואג שיהיה backdoor על המכונה, ועל הדרך הוא גם מתקין רכיב זדוני שמרגל אחרי פעילות המחשב ובין היתר יודע לקרוא כרטיסים חכמים.

הכלי, שמטרותיו היו בעיקר עסקים ובנקים רוסיים, הוא כלי חתום שנראה שבמסגרת כתיבתו נעשה מאמץ רציני כדי להתחמק מזיהוי. "מבצע בוח'טראפ"[13], כך מדווחים ESET, מעניין במיוחד מכיוון שהוא נראה כניסיון להפיק רווח כלכלי על ידי תקיפות ממוקדות - שילוב של שני דברים שקיים אצל מעטים מהכלים שאנחנו מכירים.

מהצד של הפרטים הטכניים, הכלי השתמש ב־CVE-2012-0158, פרצה בתוכנת Microsoft Word שהחברה סגרה לפני 3 שנים. הפתיון הוא מסמכי Word ברוסית (קבלות וחוזי טלפוניה) שנשלחו לאנשים מסוימים בבנקים ובחברות. כשאותם אנשים פתחו את המסמך, תוכנת ה־Word הורידה והריצה טרויאני שארוז במנהל ההתקנות של Nullsoft, ודואג להשמיד את עצמו אם הוא מזהה שהוא רץ בתוך מכונה וירטואלית או על מכונה שמותקנים בה כלי מחקר Maleware למיניהם. בצעד מעניין למדי, הוא גם בודק שמותקנת חבילת שפה רוסית למערכת ההפעלה (חלונות), ואפילו בודק בעזרת ה־Registry האם הוקלדו בדפדפן כתובות שקשורות לבנקים או שמותקנות על המכונה תוכנות הקשורות לבנקאות[14].

אם הכול הלך חלק, הוא מוריד קובץ נוסף שנועד לרגל אחרי המחשב של הקרבן. הסיפור המגניב באמת פה הוא שבהתאם לתוצאות של הסריקות, עלול לרדת אחד משני קבצים: קובץ תמים או קובץ מזיק. לדוגמה, אחד מהקבצים התמימים היה התקנה של Windows Live Toolbar, שבעזרתו ככל הנראה קיוו התוקפים להסתיר ולהפוך את הפעילות שלהם ללגיטימית מול כלי הגנה שונים (שכן נעשה שימוש בפרצה, אבל בסופו של דבר הותקן כלי לגיטימי).

[12] תוכנה שמטרתה לשנות את השפה של המקלדת בהתאם למילים שהמשתמש מקליד.
[13] באנגלית: Buhtrap. שילוב של Buhgalter (Бухгалтер; "רואה חשבון" ברוסית) ו־Trap.
[14] הרשימה מקיפה באופן מרשים מאוד, וכוללת גם תוכנות אחרות, כמו כאלו שנועדו לקריאת כרטיסים, לדוגמה.

אחרי שהורידו למחשב הקרבן כלי זדוני שהריץ את install.cmd. עכשיו הגיע הזמן לבדוק באיזה הרשאות אנחנו. אם הכלי מתבאס על זה שהוא רץ בהרשאות נמוכות, הוא הולך להשתמש ב־2 טריקים: הראשון הוא CVE-2013-3660, והשני הוא הטריק שראינו בקוד שהודלף מ־Carberp.

בגדול, כדי לקבל הרשאות גבוהות באופן אוטומטי במערכת ההפעלה חלונות, אתם צריכים שקובץ ההרצה שלכם ישב בתיקייה בטוחה (כמו system32), שהוא יהיה חתום ושב־manifest שלו יוגדר המאפיין autoElevate. על כל ההגדרות האלו עונה הקובץ שאחראי על העדכונים של מערכת ההפעלה, wusa.exe, שזכאי לקבל הרשאות גבוהות אוטומטית. הכלי מנצל את זה, מעתיק את הקובץ cryptbase.dll ל־%USERPROFILE%, משנה אותו כך שיגרום לכלי עצמו לעלות בזמן ההרצה, יוצר ממנו קובץ cab, משנה לו את הסיומת ל־msu ואז משתמש ב־wusa.exe על קובץ ה־msu כדי לחלץ את עצמו לתוך תיקיית המערכת.

הכלים שהותקנו במחשב השתנו בהתאם לפרופיל שזוהה במכונה - נראה שעל מכונות שונות הותקנו כלים שונים, ביניהן גרסה ערוכה של התוכנה mimikatz שמשמשת לגניבת סיסמאות, התוכנה LiteManager שמאפשרת שליטה מרחוק על המכונה, ואת הקובץ pn_pack.exe - שמתקין את התוכנה המדוברת של Yandex ומשתמש ב־DLL Side Loading כדי לצרף מודולים של Keylogging, קריאת כרטיסים חכמים וטיפול בתקשורת מול ה־C&C.

מעניין לראות שכמעט שנה אחרי הזיהוי של מבצע Buhtrap, הקבוצה שאחראית לו עדיין רצה וממשיכה לשנות את הכלי שלה לעיתים תכופות. נראה שלאט לאט הם מתקדמים לכיוון הדבקת שוק רחב, ומתרחקים מיצירת APT, סוג העבודה בה הם התחילו.