מה עומד מאחורי לוחמת הסייבר של סין

גבי סיבוני וי״ר

兵之形，避實而擊虛

״במלחמה הדרך היא להימנע ממה שחזק ולתקוף את מה שחלש״

(סון טסו, **אמנות המלחמה**)

מבוא

סין מפתחת זה כמה שנים יכולות מבצעיות בתחום לוחמת הסייבר. למרות ההכחשות של הממשל הסיני מקובלת בקרב החוקרים התפיסה שסין עומדת מאחורי שורה של מתקפות סייבר[1] על ארצות־הברית,[2] יפן,[3] צרפת,[4] אוסטרליה[5] ומדינות נוספות במערב.[6] ההגדרה של תקיפת סייבר היא: חדירה שלא ברשות למערכות המחשוב והתקשורת של יחידים ושל ארגונים לשם ריגול וגנבת מידע, זאת כדי לשבש את תפקודן או לפגוע בהן, וכן לשם פגיעה במערכות נוספות המבוססות עליהן – לעתים אף עד כדי גרימת נזק פיזי.

הפעילות של סין בלוחמת הסייבר מנוהלת באינטנסיביות ובאגרסיביות. נראה כי סין מתמקדת באיסוף נרחב של מידע מודיעיני ומסחרי במגוון תחומים – החל בחברות בעלות ידע טכנולוגי ייחודי וכלה בארגונים בעלי מידע פיננסי וכלכלי, כמו תקיפת המחשבים של קרן המטבע הבין־לאומית בסוף 2011.[7] ואולם, העובדה שהותקפו גם חברות וארגונים המספקים שירותים חיוניים ותשתיות תקשורת מעידה כי ייתכן שקיימים מניעים נוספים. לנוכח זאת, מתעוררות השאלות: מה עומד מאחורי המתקפות והאם ניתן לזהות את המתווה האסטרטגי שעל־פיו פועלת סין במערב בכלל, ובארצות־הברית בפרט. לשם כך יש לבחון את האסטרטגיה שגיבשה סין בתחום לוחמת הסייבר, את הגופים העוסקים בכך בסין בשנים האחרונות ואת המשאבים המושקעים למימוש היעדים שסין מבקשת להשיג באמצעות הלוחמה הזאת. מקובלת ההנחה שלפני שנת 2009 הופנו רוב

ד״ר גבי סיבוני הוא ראש תכנית צבא ואסטרטגיה וראש תכנית לוחמת סייבר הנתמכת על ידי קרן ניובאוואר במכון למחקרי ביטחון לאומי.
י״ר הוא עובד בכיר במשרד ראש הממשלה.

התקיפות שיוחסו לסין נגד רשתות של גורמי צבא וממשל, כמו מבצע Titan Rain שהופעל נגד ארגונים ממשלתיים בארצות־הברית,[8] ומבצע GhostNet נגד מטרות דיפלומטיות באו"ם. לעומת זאת, בשנים האחרונות התקיפות המיוחסות לסין נערכו נגד מטרות אזרחיות, בהן תשתיות לאומיות בעלות חשיבות קריטית, חברות המהוות חוליות בשרשרת הנגישות לאותן המטרות וחברות שתקיפתן משרתת צורך כלכלי־מסחרי.

בשנים האחרונות נערכו תקיפות על תשתיות שהיו בבחינת קפיצת־מדרגה. הראשונה הייתה סדרת התקיפות Shady RAT שהחלו באמצע 2006 ונמשכו עד פברואר 2011.[9] סדרת התקיפות השנייה הייתה מבצע Aurora שהיה מתוחכם במיוחד ובו הותקפה בין היתר חברת Google המהווה תשתית חיונית ברמה העולמית. התקיפות האלה נערכו מאמצע 2009 ועד דצמבר אותה השנה. סדרת התקיפות השלישית – שלה היו הדים רבים בתקשורת – הייתה על חברת RSA, חברה העוסקת באבטחת מידע ושרתי אינטרנט והמספקת בין היתר שירותי SecureID והרשאות כניסה חד־פעמיות (One Time Password - OTP). השערת המחקר במאמר הזה היא שניתוח המידע הגלוי שהתפרסם בנוגע לתקיפות האחרונות מאפשר לאשש את ההנחה שסין עומדת מאחורי התקיפות האלה, ואף לזהות התאמה בין האסטרטגיה של סין בתחום לוחמת הסייבר לבין בחירת יעדי המתקפה.

הניתוח כלל בחינה של מאפייני החברות שהותקפו כדי לזהות מניעים אפשריים לתקיפה, לדוגמה: תקיפה של חברות וארגונים ספקי טכנולוגיה מאפשרת נגישות לטכנולוגיה עילית, לטכנולוגיה צבאית וכדומה. ניתן להניח שהמניעים לתקיפות כאלה הם גנבה של יכולות וריגול תעשייתי של מדינות או של חברות מתחרות. תקיפה של חברות וארגונים מן המגזר הפיננסי, המגזר הכלכלי ואף המגזר הפוליטי מאפשרת נגישות למודיעין בעל ערך בתחומים האלה. לעומת זאת, הערך המודיעיני לשימוש מידי של תקיפת חברות המספקות תשתיות חיוניות ושירותי תקשורת נמוך בדרך־כלל באופן יחסי. השגת נגישות, ולו לחלק מספקי שירותי התקשורת והאינטרנט במערב ובארצות־הברית, עלולה להקנות לתוקף יכולת לפגוע בשירותים האלה.

האסטרטגיה של סין בתחום לוחמת סייבר

האסטרטגיה של סין בתחום לוחמת הסייבר גובשה בעשור הקודם, זאת במסגרת תהליך מודרניזציה עמוק שעבר צבאה. בבסיס האסטרטגיה עומדת ההבנה שצבא סין נמצא בנחיתות מובנית ביחס לצבאות במערב, כמו צבא ארצות־הברית בכל הקשור ללוחמה קינטית. לנוכח זאת התגבשה ההבנה שכדי להתמודד עם יריב בעל יתרון טכנולוגי בתחום תעבורת המידע יש לשבש את נגישותו למידע הזה.

התפיסה נוגעת להנחתת מהלומה משולבת מקדימה הכוללת את המרכיבים הבאים: מתקפת סייבר, מתקפה אלקטרונית ומתקפה קינטית על רשת המידע ומוקדי הטכנולוגיה הצבאית של היריב. המהלומה הזאת תוביל להיווצרות "נקודות עיוורות" שיאפשרו לכוחות הסיניים לפעול ביעילות רבה יותר.[10] ההנחה של סין היא שבאמצעות שיבוש תעבורת המידע ניתן לפגוע באופן משמעותי ביכולות של היריב המתוחכם ולהשיג יתרון בשלבים הראשונים של העימות.

האסטרטגיה שפותחה בסין בעשור האחרון רואה במבצעי רשת מוכללים[11] פלטפורמה מרכזית לפיתוח התחום. האסטרטגיה הזאת מושתתת על שילוב בין ארבעה סוגים של מבצעים:[12] תקיפת רשתות מחשבים, לוחמה אלקטרונית הכוללת אמצעי נגד אלקטרוניים ומכ"ם, הגנת רשת מחשבים וניצול רשתות מחשבים (exploitation).[13] התפיסה המשולבת הזאת מקנה לסין יכולת מבצעית רב תחומית המאפשרת לה מיצוי של הכוח לשם תקיפת היריב. אחד המרכיבים המרכזיים באסטרטגיה של סין הוא שליטה על תעבורת המידע של היריב, זאת על בסיס ההנחה שליריביה של סין (בעיקר מדינות המערב, בייחוד ארצות־הברית) יש תלות רבה בטכנולוגיה המבוססת על תעבורת מידע. בבסיס האסטרטגיה הסינית עומדת ההנחה שבעת עימות, היכולת לפגוע בתעבורת המידע תאפשר לסין להשיג יתרון בשדה הקרב הפיזי.

כמה פרסומים מנתחים בפירוט את הגופים העיקריים בצבא סין בתחום מבצעי הרשת.[14] במאמר הזה נסתפק בתיאור שני גופים מרכזיים בצבא: המחלקה השלישית (במטה הכללי של צבא שחרור העם – PLA), האחראית על מודיעין סיגינט, והמחלקה הרביעית, האחראית על מודיעין אלינט ולוחמה אלקטרונית. במחלקה השלישית עובדים מומחים במגוון תחומים: טכנאים, מומחי מחשבים, מומחים לשפות, מומחי מודיעין ועוד. ההיקף הנרחב של פעילותה של המחלקה ומגוון המשימות המוטלות עליה עושים אותה מתאימה לביצוע מבצעי סייבר ברשת. למחלקה הזאת יש תחנות איסוף רבות הפזורות ברחבי סין, והיא אחראית על איסוף מודיעין בתחום השמע והנתונים ועל מיצויו, הפקתו והערכתו. המחלקה הזאת אחראית כנראה גם על איסוף מידע פנימי בצבא סין לצורכי ביטחון ואבטחת מידע פנים. להערכת כמה חוקרים במערב, היקף כוח־האדם הפועל במסגרת המחלקה השלישית הוא למעלה מ־130,000 איש.[15] המחלקה הרביעית, האחראית על מבצעי מודיעין אלקטרוני (אלינט) ולוחמה אלקטרונית, פועלת כנראה גם בתחום מבצעי רשת משולבים.[16] נראה שהמחלקה השלישית היא הגוף המרכז את כלל הפעילות בתחום הזה.[17]

נוסף על הארגון הצבאי קיימת בסין קהילת פצחנים[18] גדולה מאוד. הקהילה הזאת מעורבת כנראה גם בפעילות להשגת יעדים לאומיים. קבוצות כאלה קיבלו אחריות על כמה תקיפות. נראה שאף כי ממשלת סין פועלת לאכיפת החוק הסיני

האוסר על פעילות כזאת, היא מעלימה עין מן הפעילות, ואף תומכת חומרית בחלק ממנה – מעין מיקור חוץ לפעילות הממשלה בתחום הסייבר.[19] נוסף על כך מגייס צבא סין אזרחים ליחידות מיליציית הרשת שלו המגיעים מקרב קהילת הפצחנים וחברות טכנולוגיה.[20] המיליציה הזאת משולבת בפעילות הצבא אף כי החברים בה הם מתנדבים ואינם מקבלים שכר.

יש לציין שלעומת התפיסה הרווחת בקרב חוקרי פעילות הסייבר של סין, קיימים חוקרים הטוענים כי הפעילות הזאת נועדה בראש ובראשונה לצורכי פנים, וכי מדינות המערב אינן צריכות לחשוש ממנה יתר על המידה בכל הנוגע לאיום על מרחב הסייבר שלהן. לטענתם, היכולות מפותחות בעיקר לצורכי בקרה על מתנגדי המשטר, שליטה על התכנים המגיעים לאזרחי סין וצרכים פוליטיים שעיקרם שימור השלטון.[21] אף כי ניתן להסכים לטענה הכללית שמשטרים טוטליטריים, ובהם סין, עושים שימוש ביכולות סייבר גם לצרכים פוליטיים,[22] המציאות שונה – יעיד על כך רצף אירועי הסייבר שמקורם בסין בשנים האחרונות.

אחד המרכיבים העיקריים באסטרטגיה של סין הוא הצורך בנגישות לתשתיות התקשורת של היריב. הנגישות הזאת קריטית למימוש יעדיהם, ובלעדיה יתקשו לייצר "נקודות עיוורות" אצל היריב. יצירת נגישות אפקטיבית ברשתות תקשורת מחייבת פעילות תשתיתית לאורך זמן ובהיקף נרחב. תקיפת רשתות התקשורת של היריב יכולה להתבצע רק אם קיימת אליהן נגישות קבועה לאורך זמן, המספקת הן מודיעין איכותי והן יכולות להתקין באופן חשאי רכיבי תוכנה זדוניים שאותם ניתן להפעיל ביום פקודה. הנגישות הזאת מחייבת תחזוקה ושימור לאורך זמן בשל שינויים קבועים שעושה היריב במערכי התקשורת והמידע שלו ומכיוון שהוא מתקין מערכות הגנה חדשות העלולות לחשוף את הפעילות.

תקיפות הסייבר של סין

בשש השנים האחרונות התגלו לא מעט תקיפות סייבר המיוחסות לסין. חשיפת המבצעים האלה שופכת אור על שיטות הפעולה של סין. על פני הדברים, אלה היו מבצעי איסוף, ובאמצעות ניתוחם ניתן לזהות את טכניקות התקיפה הבסיסיות ולהקיש על המדיניות של התוקף ועל שיטות פעולה שלו, במקרה הזה – סין. מן התקיפות ניתן ללמוד על גישה של מעצמה שמטרתה להשיג נגישות תשתיתית נרחבת מאוד, והיא אינה מסתפקת ביעד נקודתי. במקרה של מבצע Aurora המטרה הייתה השגת גישה למנגנון הססמאות של Google ולתוכנת בקרת הגרסאות. במקרה של תקיפת RSA המטרה הייתה השגת גישה לרשת הפנימית שבה נוהל מידע הקשור למערכת SecureID היכול לשמש במשך הזמן להתקפה יעילה יותר על חברות אחרות העושות שימוש במערכת, ובהן חברות ביטחוניות וחברות אחרות בעלות פעילות רגישה. טכניקות התקיפה שזוהו היו דומות מאוד זו לזו. אלה היו

מתקפות מאורגנות היטב שנעשה בהן שימוש משולב ב־social engineering,[23] חולשות תוכנה, בהתקנת כלים שוהים, בהרחבת נגישות תוך ארגונית ובשאיבת מידע רב. נקיטת הפעולות השיטתיות האלה במשך כל השנים האחרונות מחזקת את הטענה שהתקיפות היו מאורגנות ושאותם גופים יזמו אותן, ומחלישה את הטענה שהתקיפות האלה בוצעו על־ידי פצחנים מזדמנים. אישוש נוסף לטענה הזאת ניתן למצוא בניתוח שבוצע על־ידי אנשי הקונצרן הביטחוני האמריקני נורת׳רופ גרומן.[24] הניתוח הזה עשה שימוש בכמה אבני בוחן כדלהלן:

א. דמיון ב"התנהגות מקלדת" (keyboard behavior) – זיהוי של מאפייני התנהגות דומים בפעולת התוקפים בתקיפות שונות. למשל, תקיפת חלקי מידע בעל מאפיינים דומים ושימוש בכלים דומים.
ב. היקף ההכנות המקדימות – התוקפים נקטו פעולות שחייבו הכנות וידע מקדים שנבע כנראה מפעולה מקדימה שנעשתה במשך כמה חודשים לפני ביצוע התקיפה בפועל. לדוגמה, התוקפים הכירו את ארכיטקטורת הרשת שאותה תקפו.
ג. המשמעת של התוקפים – התוקפים התאפיינו במשמעת גבוהה. לדוגמה, הם לא פתחו קבצים לפני העתקתם כדי לסקור באופן ראשוני את התוכן. ככל הנראה הם פעלו על־פי מידע מוקדם.

מבצע Nitro

מבצע **Nitro** כלל סדרת תקיפות שרובן נערכו מסוף יולי עד אמצע ספטמבר 2009. המידע על המבצע פורסם על־ידי חברת סימנטק.[25] ההנחה היא שהיעד העיקרי של המבצע היה ריגול טכנולוגי. המבצע התנהל בכמה גלים שהתבצעו ברציפות וניתן לאפיין אותם על־פי יעדי התקיפה. בתחילה הותקפו ארגוני זכויות אדם בסין, אחריהם הותקפו תעשיות מנועים ובחודשים האחרונים לפני שנחשפו הותקפו 29 חברות בתחום הכימיה. החברות שהותקפו היו ברשימת Fortune 100 העוסקות במחקר ופיתוח כימי וחומרים מיוחדים, בעיקר לתעשיית הרכב הצבאית, וחברות העוסקות בהקמת תשתיות לתעשיות כימיות ובייצור חומרים מתקדמים. שיטת התקיפה הייתה דומה לזו שננקטה בתקיפות נוספות שביצעו הסינים (ראו להלן) וכללה את המרכיבים הבאים:

א. שליחה של קוד מפגע שהוסווה בדרך־כלל כעדכון אבטחה. נשלחו כמויות גדולות של דואר אלקטרוני לארגונים ללא התאמה אישית. זאת בניגוד למבצעים אחרים שבהם הושקעו מאמצים רבים יותר בהתאמת הדואר האלקטרוני לנמען.
ב. התקנת דלת אחורית (סוס טרויאני) במחשב היעד.

ג. הגברת הנגישות ברשת המותקפת תוך שימוש בשרידים של סיסמאות שנמצאו על המחשב שהותקף כדי להגיע לשליטה במחשב המרכזי ברשת.
ד. איסוף החומר בשרתי ביניים ושידורו מחוץ לרשת. בסך־הכול הותקפו כ־100 מחשבים, מהם 29 – של חברות שעסקו בתחום הכימיה ו־19 נוספים – של גופים במגזר הביטחוני. רוב החברות שהותקפו היו בארצות־הברית (כ־30%) בבנגלדש (כ־20%) ובבריטניה (כ־15%). יתר המחשבים היו בכ־20 מדינות ברחבי העולם.

מבצע Aurora

מבצע Aurora כלל סדרת תקיפות שהחלו באמצע 2009 ונמשכו עד דצמבר 2009. על התקיפות דיווחה לראשונה חברת Google בינואר 2010. מהחברה נמסר כי תוקפים חדרו לחשבונות gmail של פעילי זכויות אדם סינים הפועלים בארצות־הברית, באירופה ואף בסין.[26] גם חברת Adobe דיווחה על תקיפה במסגרת אותו מבצע. בסך־הכול הותקפו לפחות 34 ארגונים וחברות.[27] חברת אבטחת המידע McAfee ערכה ניתוח של התקיפה הזאת. מממצאי הניתוח עלה שמטרת התקיפה הייתה השגת נגישות לקוד המקור של החברות שהותקפו, בפרט לתוכנת ניהול הגרסאות Periscope שבה משתמשות מאות חברות תוכנה גדולות. החברה אפיינה כמה שלבים בתהליך התקיפה:[28]

א. מפעיל המחשב המותקף קיבל דואר אלקטרוני או מסר מידי שנראה תמים ממען שלכאורה היה בטוח.
ב. המפעיל התפתה והפעיל את הקישור המצורף להודעה אשר הוביל לשרת שהכיל קוד זדוני.
ג. סייר האינטרנט במחשב המותקף הוריד קוד בינארי שהוסווה כקובץ תמונה והפעיל דלת אחורית שהתקשרה לשרת שליטה שהיה ממוקם בטייוואן.
ד. התוצאה – התוקפים השיגו שליטה מלאה על המחשב, ובאמצעותו – על מידע רגיש שהיה מקושר ברשת.

השיטה הזאת ננקטה ברבות מן התקיפות המכונות APT (Advanced Persistent Threat). בתחילה המשמעות של המונח הזה הייתה תקיפות מתוחכמות על רשתות צבא וממשל, אך כיום נעשה במונח הזה שימוש כדי לציין תקיפה בעוצמה רבה (עוצמה של מדינה) על מטרה אזרחית.

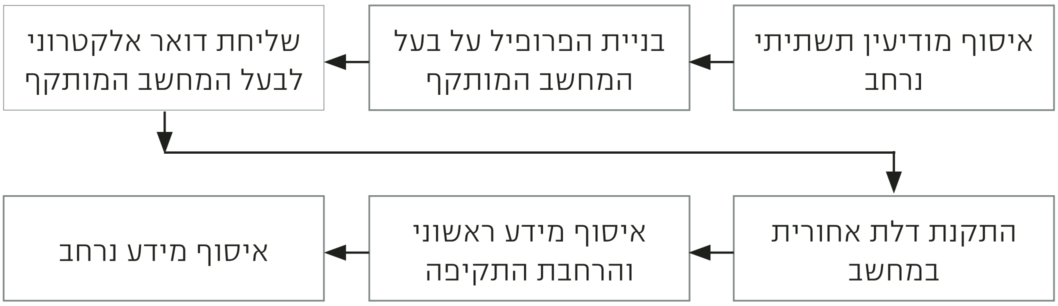
גלי התקיפה Night Dragon ו־Shady RAT

גלי התקיפה החלו באמצע 2006 ונמשכו עד פברואר 2011. חברת McAfee, שהשיגה נגישות לשרת שליטה אחד שבו עשו התוקפים שימוש, זיהתה בשרת הזה, לאחר ניתוח של קובצי לוג,[29] כי הותקפו כ־70 יעדים.[30] לנוכח העובדה

שהושגה נגישות לשרת שליטה אחד בלבד, ניתן להניח שלתקיפה הזאת היו יעדים נוספים. בניתוח אופיינו החברות שהותקפו ומשכי־הזמן שבהם המחשבים בחברות האלה היו בשליטת השרת אשר דרכו שאבו התוקפים מידע רגיש. הניתוח של חברת McAfee סיפק תמונה בנוגע לחברות שהותקפו – חברות ממשל (21 חברות), תעשייה ואנרגיה (6 חברות), תקשורת, מחשבים ואלקטרוניקה (13 חברות), תעשייה ביטחונית (13 חברות) ופיננסים (6 חברות). בהקשר הזה בולטות התקיפות על חברות הנפט והגז של נורווגיה.[31] תקיפה של חברות המהוות תשתית לאומית, כמו חברות אנרגיה, יכולה להעיד על רצון ליצור נגישות לפגיעה בעתיד בתשתיות האלה.

תקיפת RSA

תקיפת RSA מספקת מצע לניתוח עומק בשל העובדה שאחד מן השרתים שהיה מעורב בה בוטנט[32] בהיקף של כ־2,000 מחשבים. חדירה לשרת המרכזי של הבוטנט אִפשרה לנתח את רשימת המחשבים הנגועים שמהם התקבלה רשימה של 763 חברות.[33] התקיפה דווחה לראשונה על־ידי RSA במרס 2011.[34] ניתן לתאר את השלבים של התקיפה, ששיטתה אפיינה תקיפות אחרות, כדלהלן:



להלן הסבר על תהליך התקיפה המתואר:

איסוף מודיעין תשתיתי נרחב – השלב המקדמי לתקיפה הנו איסוף של מודיעין תשתיתי נרחב על הגוף שאותו מתכוונים לתקוף. המודיעין הזה נאסף בדרך־כלל מתוך הרשתות החברתיות וממידע גלוי אחר. מטרת המידע היא לאתר ממלאי תפקידים המועמדים לתקיפה, כדי שאלה יוכלו להוות את הנתיב שדרכו ניתן יהיה לפעול בצורה המיטבית בתוך הארגון המותקף. לדוגמה, באירוע תקיפת RSA נבחרו שתי קבוצות קטנות של עובדים. אלה לא היו בהכרח יעד התקיפה הסופי אלא נבחרו כנראה משום שהתוקפים העריכו שיהיה נוח להתחיל את התקיפה באמצעות המחשבים של העובדים האלה.

בניית הפרופיל של בעל המחשב המותקף – לאחר איתור יעדי החדירה נבנה פרופיל של המותקפים. הפרופיל הזה מחייב בניית תמונת מידע מלאה דיה כך

שתתאפשר יצירת הודעת דואר אלקטרוני שתיראה למקבל המותקף כהודעה תמימה ולא תעורר את חשדו. יש לזכור שאיסוף מידע כזה ובניית פרופיל מתאים מחייבת אף היא פעילות איסוף ענפה וממוקדת הדורשת ארגון ומשאבים לא מעטים (בפרט עובדים בעלי ידע באנגלית).

שליחת דואר אלקטרוני מפגע המותאם לבעל המחשב המותקף (ZeroDate spear phishing email) – שליחת הדואר האלקטרוני המפגע מחייבת נקיטת שתי פעולות. הראשונה היא בניית נוסח, מבנה ומראה של הודעה תמימה שתגרום לבעל המחשב העובד בארגון המותקף לא למחוק אותו ולפתוח את הקישורים בו. הדואר האלקטרוני נשלח לקבוצה ממוקדת של עובדים שנבחרו. לעתים מותאמת ההודעה לכל עובד בנפרד בהתאם לפרופיל שנבנה. הפעולה השנייה – הצמדת קובץ מצורף דבוקה, (attachment) להודעת הדואר האלקטרוני הכוללת חולשת אבטחה עם דלת אחורית. חולשות הן פרצות אבטחה בתוכנה המאפשרות להחדיר דרכן את הקוד המפגע. לעתים החולשה היא חולשה מקורית שזוהתה בתהליך איתור חולשות על־ידי המפגע (כך נעשה כנראה במבצע Aurora), ולעתים החולשה ידועה ומפורסמת (ZeroDate) כשהתוקף מסתמך על האפשרות שבמחשבי היעד עדיין לא הותקן טלאי תיקון לחולשה הזאת.[35] לדוגמה, בתקיפת RSA הנושא של הדואר האלקטרוני היה "Recruitment Plan 2011", וצורף אליו קובץ האקסל Recruitment plan 2011.xls. חולשת ה־ZeroDate הייתה CVE-0609-2011 ב־Adobe Flash. ברגע שאחד העובדים פתח את הקובץ במחשבו הוא נדבק בדלת אחורית. בעת התקיפה החולשה נחשבה לא ידועה, ולא היה לה עדכון אבטחה; העדכון הופץ כשבוע לאחר התקיפה.

התקנת דלת אחורית במחשב – הכוונה היא לקוד זדוני המותקן במחשב הנגוע ומאפשר לתוקף לשלוט עליו באמצעות שרת שליטה.[36] בדרך־כלל הדלת האחורית המותקנת יוצרת קשר עם שרת התוקף, ומשם היא מופעלת בהתאם להוראות המועברות מן השרת הזה על־ידי מפעילים אנושיים הפועלים בדרך־כלל במשמרות. הכיוון הזה של התקשורת – מתוך הארגון כלפי חוץ – מקשה על איתורה.

איסוף מידע ראשוני והרחבת התקיפה – בשלב הזה נאסף חומר ראשוני. למעשה, לכל מחשב מותקף מוצמדת קבוצת תקיפה המנתחת את תכולת המחשב ומנסה להעריך כיצד ניתן לאסוף מידע מן המחשב המותקף ואיזה מידע ניתן לאסוף ממנו. בדרך־כלל נעשית בשלב הזה הערכה בנוגע לנגישות של המחשב המותקף לשרתים ולמקורות מידע אחרים בארגון כדי לזהות את מפת הרשת ולהבין כיצד ניתן להרחיב את התקיפה.

איסוף מידע נרחב – זהו שלב האיסוף המרכזי המתרחש לאחר שנוצרה נגישות לשרתי החברה וזוהה המידע הנדרש. העברה של כמויות מידע גדולות באופן שאינו מעורר חשד ובדרך שאינה מאפשרת זיהוי על־ידי תוכנות ניטור המותקנות

בדרך כלל ברשתות של ארגונים גדולים הנה פעולה מורכבת. זו נעשית בדרך־כלל באמצעות מחשב אחר ברשת שהנגישות שלו וההרשאות שלו הן ברמה גבוהה כך שהוא משדרג את ההרשאות של אותם שרתים לייצא מידע תוך שימוש בהצפנה ואלגוריתמים של דחיסת מידע. לדוגמה, במקרה של RSA הגיעו התוקפים בסופו של התהליך למחשב שבו נשמר מידע רגיש הקשור למערכת SecureID, שאִפשר בהמשך נגישות למידע בחברות אחרות.[37] כל זאת בצורה שעקפה את התראות חוקי מערכות הניטור בארגון.[38]

הגישה שתוארה לעיל מחייבת הקצאת משאבים מקצועיים רבים. בתקיפה הזאת פעלו כנראה שתי קבוצות במקביל באמצעות כלים שונים. הראשונה פעלה לאיתור המידע הנדרש ברשת החברה, והשנייה פעלה בנפרד כדי לייצר את ערוץ הוצאת המידע. ייתכן שפעלה אף קבוצה שלישית שתפקידה היה לשמר את הנגישות לשימוש מאוחר יותר בעתיד. הגישה הזאת מעידה על תפיסה של מעצמה הפועלת ברמה מקצועית גבוהה תוך השקעה במשאבים רבים של כוח אדם איכותי ושל יכולות מודיעין. ניתן לזהות בתקיפה הזאת כמה מרכיבים המעידים על כך שמאחוריה עומדת מעצמה וההערכה המקובלת היא שמדובר בסין. להלן פירוט המרכיבים האלה:

גישה תשתיתית – פריצה למנגנון הססמאות החד־פעמי של החברה (OTP) במטרה להשיג נגישות רבה לחברות נוספות מצביעה על גישה של פעולה נרחבת המחייבת משאבים גדולים.

היקף התקיפה – בפרסומים הגלויים דווח על 763 מחשבים נגועים שנמצאו על אחד השרתים שהיה מעורב בתקיפת RSA. לפחות עבור חלק מן היעדים האלה היה צורך בפעילות ידנית מקדימה כפי שפורט בשיטת העבודה, כלומר, היה צורך באיסוף מידע מקדים על היעד, בבניית דואר אלקטרוני בשפה האנגלית ששימש כפתיון ובניתוח ראשוני של הנגישות. תקיפה בעוצמה רבה כזאת חייבה התארגנות תשתיתית ברמה של מעצמה ומעידה על כך שאין המדובר בפעולה של בודדים.

תוכנת הדלת האחורית Sykipot[39] – התוכנה הזאת, שהיא וריאנט של PoisonIvy,[40] משמשת בתקיפות של סין כפי שתוארו לעיל. נעשה בה שימוש (בגרסאות דומות) כבר ב־2006, והוא נמשך גם בתחילת 2012.[41] השימוש בתוכנה דומה (עם שינויים קלים באופן יחסי) מעיד על תיאום ארגוני בין תוקפים שונים במהלך השנים האחרונות.

סימנים מזהים – בתוכנת הדלת האחורית נמצאו קישורים חזקים לסין. על־פי ניתוח הטקסט בתוכנה זוהו סימנים מובהקים של השפה הסינית כולל שיירי מידע בשפה הסינית בקוד הבינארי (debug information). נוסף על כך אותרו הודעות שגיאה בשפה הסינית, ולבסוף, ספר המשתמש היחיד לגרסה של הדלת האחורית כתוב בסינית.

שרתי השליטה – ניתוח האתרים שבהם הוצבו שרתי השליטה, ושמהם הופעלו המחשבים הנשלטים, העלה כי רובם המכריע היו בסין (299 מתוך 329 שרתי שליטה).[42]

הממצאים האלה מאששים את ההנחה הבסיסית שסין עומדת מאחורי התקיפה שחייבה שימוש במערך ארגוני תשתיתי נרחב ושיטתי. לנוכח זאת, אין להתפלא על הודעתו של הגנרל קית' אלכסנדר ראש NSA שאישר לאחרונה כי סין עומדת מאחורי תקיפת RSA.[43]

רשימת 763 החברות שהופיעו באחד השרתים שהיה מעורב בתקיפת RSA נותחה כדי לבחון האם ניתן להפיק מן המידע הזה מסקנות בעלות ערך. הניתוח כלל איתור של החברה באינטרנט ואפיון עיסוקה. החברות אופיינו באחת משלוש קטגוריות: חברות טכנולוגיה שהותקפו כנראה לצורך ריגול טכנולוגי; חברות פיננסים וכלכלה שתקיפתן יכולה לאפשר גְנֵבת מידע מסחרי; וספקי תקשורת. המשמעות של הממצא הזה בדרך־כלל היא שהמחשב הנגוע היה מחובר דרך ספק גישה ציבורי לאינטרנט (ISP).[44]

הניתוח מלמד שקרוב ל־80% מכלל החברות והארגונים שהותקפו היו בקטגוריית ספקי תקשורת. יתר ה־20% נחלקו בין חברות טכנולוגיה, חברות פיננסים ואחרות. הנתונים האלה מצביעים על פילוח בוטנט אופייני הכולל מספר רב של מחשבים נגועים השייכים לאנשים פרטיים שהתחברו לרשת באמצעות ISP. רוב המחשבים ברשימה (34%) היו מארצות־הברית. יתר המחשבים שהותקפו נחלקו בין כ־90 מדינות, בהם חמישה מישראל.

תובנות מסכמות

סדרות התקיפות מאז 2006 מצביעות על מעבר לתקיפה של חברות תשתית חיוניות הן בתחום התקשורת והן בתחום האנרגיה. בהקשר של תקיפת RSA קיימת אפשרות שרשימת החברות שנמצאה על השרת כללה רשימה אקראית של בוטנט שנבנתה על־ידי הסינים בתהליך שנמשך זמן רב לפני גילוי התקיפה כדי לשמש תשתית להתקפות בעתיד. מכל מחשב נגוע ניתן לשלוח דואר אלקטרוני למטרות תקיפה, להעביר קבצים או להסתיר את זהות התוקף. ואולם, קיימת האפשרות שחלק מן הרשימה הזאת אינו אקראי וכולל חברות שהן היעד המתוכנן של התקיפה.

הממצאים של התקיפות בשנים האחרונות מאששים את השערת המחקר ומאפשרים לקבוע שהתקיפות שתוארו הן חלק ממערכה סדורה ושיטתית המתבצעת על־ידי סין. ניתן לזהות התאמה בין האסטרטגיה של סין בתחום לוחמת סייבר לבין בחירת חלק מיעדי התקיפה, בעיקר אלה הנוגעים לתשתיות חיוניות. הן תקיפת גוגל במבצע Aurora, הן תקיפות Shady RAT, וכמובן תקיפת

RSA מצביעות על מעבר לתפיסה מערכתית הכוללת יעדי תקשורת ויעדי תשתית חיוניים. האסטרטגיה של סין, שמטרתה לפגוע במרחבים החלשים והפחות מוגנים של היריב במהלך המקדים להפעלת הכוח הקינטי, מחייבת פעולה נרחבת ליצירת נגישות לאורך זמן לתשתיות חיוניות, בהן תשתיות תקשורת. יש לציין שבניגוד למבצעי איסוף הרועשים מטבעם, ולכן מתגלים מעת לעת, קשה יותר לגלות מבצעי תשתית להשגת נגישות ליום פקודה לגילוי וייתכן אף כי לא יתגלו כלל.

נוסף על התקיפות שהוזכרו לעיל, הואשמה סין באפריל 2011 ביירוט של לא פחות מ־15% מתעבורת האינטרנט.[45] לפיכך ההערכה היא שחלק מן התקיפות מיועדות ליצור נגישות מודיעינית לתעבורת האינטרנט וליירוט תשדורות לפני שהן מוצפנות. יש לזכור שהמסקנות במאמר הזה מתבססות על ידע שהצטבר כתוצאה מניתוח של מידע על תקיפות שהתגלו ופורסמו. מכיוון שלא ניתן תמיד לגלות תקיפות, ולעתים גם אם הן מתגלות הדבר אינו מתפרסם, ניתן להניח שסין מפעילה מבצעי סייבר נוספים. קשה לדעת מה מתרחש בדיוק בחברות מותקפות. אחת האפשרויות היא שהותקנה בהן דלת אחורית שונה מאלה שבהן נעשה שימוש לצורך שימור הנגישות וזו עלולה להיות מופעלת, לפי החלטה, כדי לפגוע בתשתית התקשורת הרלוונטית. יתֵרה מזו, דלת אחורית הנמצאת במצב רדום כמעט בלתי ניתנת לגילוי בטכנולוגיות ההגנה הקיימות כיום כמו תוכנות האנטי וירוס השונות.[46]

המשמעות של הדברים חמורה במיוחד בהקשר של ארצות־הברית שבה אינה רווחת הפרדה פיזית של רשתות התקשורת, כלומר, רווח שימוש באינטרנט "אזרחי"[47] גם במערכות המחשוב במתקנים ובארגונים רגישים, ואף בתשתיות לאומיות קריטיות כמו כורים גרעיניים לייצור חשמל ומערכות הבקרה של תשתיות התחבורה. זאת ועוד – בחלק מן המקרים עושה המערכת הביטחונית של ארצות־הברית שימוש נרחב בתשתיות האינטרנט האזרחיות, והפרדת הרשתות של מערכים מבצעיים רגישים אינה מפותחת דיה. זוהי חולשת אבטחה מהותית המאפשרת לתוקפים נגישות רבה לתשתיות האלה באמצעות תקיפה של מערכים אזרחיים פחות מוגנים. משמעות הדבר היא יצירת יכולת לשבש באופן חמור ביום פקודה את תהליכי העברת המידע. בשל החולשה הזאת, פגיעה מקדימה בתשתיות התקשורת והטלפוניה בעת עימות עלולה לשבש מערכים מבצעיים וביטחוניים המבוססים על התשתיות האלה.

המענה לחולשה הזאת מחייב תפיסה מערכתית כוללת, ולא ניתן להסתפק בניסיונות לשפר את ההגנות על ספקי תשתיות התקשורת כדי לנסות למנוע תקיפות בעתיד. השימוש ברשת האינטרנט לצורך תקשורת של מערכות רגישות אינו יכול להתבסס אך ורק על הרשאות גישה. מוגנות ככל שיהיו, ההרשאות האלה הן פרצה משמעותית בהגנה. אחד המרכיבים החשובים במענה לחולשה שתוארה

נוגע לבידול שבין רשתות תקשורת. מוצע לבודד את הרשתות המבצעיות של מגוון מערכות קריטיות – מערכות ביטחוניות, מערכות תקשורת מבצעית ומערכות פיקוד ובקרה של מתקנים המוגדרים תשתיות לאומיות קריטיות. היכולת להפעיל מערכות בקרה של מתקנים חיוניים באמצעות רשת האינטרנט עלולה להתגלות כאבן נגף ברגע שבו יחליט תוקף מתוחכם להפעיל דלתות אחוריות ביום פקודה.

הערות

1 Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 9, 2009, p. 67.

2 Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, The Brookings Institution, February 2012.

3 ראו: מתקפה על חברת מיצובישי ביפן באוגוסט 2011, Hiroko Tabuchi, "U.S. Expresses Concern About New Cyberattacks in Japan", *New York Times*, September 21, , 2011. http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html?_r=1

4 *Chinese 'hacked French ministry for G20 data'*, *The Week, 8* Mar 2011, http://www.theweek.co.uk/technology/7229/chinese-%E2%80%98hacked-french-ministry-g20-data%E2%80%99

5 Erik Helin, "Fingers Point to China in Australian Prime Minister Hack", *Brick House Security*, March 30, 2011, http://blog.brickhousesecurity.com/2011/03/30/australia-pm-hack

6 ראו על תקיפת אתרי ממשל בקנדה: Greg Weston, "Hackers Attack Canadian Government", CBS News, February 16, 2011, http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html

7 David Sanger and John Markoff, "IMF Reports Cyberattack Led to 'Very Major Breach'", *New York Time,* June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html

8 Nathan Thornburgh, "Inside the Chinese Hack Attack", *Time (US)*, August 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html

9 Dimitri Alperovitch, *Revealed: Operation Shady RAT*, Version 1.1, McAfee, 2011, http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

10 DeWeese, 2009, p. 69.

11 Integrated Network Electronic Warfare

12 Tim Stevens, "Breaching Protocol – The Threat of Cyberespionage," *Jane's Intelligence Review*, March 2010, pp. 8-13.

13 Timothy L. Thomas, "Chinese and American Network Warfare", *Joint Forces Quarterly*, Vol. 38, p. 76. http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf

14 DeWeese, 2009, p.31; Mark A. Stoke, Janny Lin and L.C. Russell Hsiao, *The Chinese PLA Signal Intelligence and Cyber Reconnaissance Infrastructure,* Project 2049 Institute, November, 2011. pp. 6-14.

15 קיים קושי לאמת את ההערכה הזאת.

16 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations and Capability", in: Roy Kamphausen, David Lai, and Andrew Scobell (eds.), *Beyond the Strait: PLA Missions Other Than Taiwan*, Washington, DC: National Bureau of Research, 2009, p. 273.

17 **שם.**

18 **פצחן –** Hacker, במנדרינית 黑客 Hēikè **– מילולית "אורח שחור".**

19 Stevens, March 2010, pp. 8-13.

20 Timothy L. Thomas, "Comparing US, Russian and Chinese Information Operations Concepts", Foreign Military Studies Office, Fort Leavenworth, KS 66048, February 2004, pp. 12-13.

21 Thomas Rid, "Think Again: Cyberwar - Don't fear the digital bogeyman. Virtual conflict is still more hype than reality", *Foreign Policy*, March 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,6

22 ראו פרסומים על ריגול הסייבר הסיני נגד הממשלה הטיבטית הגולה ופריצה לתשתית המחשב של הדלאי לאמה.: Stevens, 2010, pp. 8-13

23 בהקשר של המאמר הזה המונח מתאר את היכולת להונות את בעל המחשב המותקף תוך יצירת מצג המתאים לפרופיל שלו, כדי שיבצע פעולות שבהן התוקף מעוניין; לדוגמה, יגיב לדואר אלקטרוני המופנה אליו באופן מנוגד למדיניות האבטחה של הארגון שבו הוא עובד.

24 Steve DeWeese, 2009, p. 60.

25 Eric Chien and Gavin O'Gorman, *The Nitro Attacks, Stealing Secrets from the Chemical Industry*, Symantec Security Respond, 2011, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

26 ייתכן שלא היה קשר בין פריצה לחשבונות gmail של פרטים לבין התקיפה להשגת קוד המקור של google ו־Adobe.

27 Ariana Eunjung Cha and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say", *Washington Post,* January14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

28 McAfee Labs and McAfee Foundstone Professional Services, *Protecting Your Critical Assets, Lessons Learned from "Operation Aurora",* http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

29 קובצי לוג (log files) הם קבצים המתעדים באופן רציף ואוטומטי פעילות מוגדרת במחשב.

30 Alperovitch, 2011, p. 3. http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

31 "Hackers attack Norway's oil, gas and defence businesses", BBC News, November 18, 2011, http://www.bbc.co.uk/news/technology-15790082

32 בוטנט הוא אוסף של סוכני תוכנה המותקנים במחשבים מארחים. במקרים רבים אלה הם מחשבים נגועים שהודבקו בסוכן התוכנה ללא ידיעת בעל המחשב. סוכני התוכנה יכולים להיות מופעלים בכפוף לתנאים קבועים מראש או על־ידי פקודות משרת שליטה.

33 Brian Kerbs, *Who Else Was Hit by the RSA Attackers*, October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers

34 Uri Rivner, *Anatomy of an Attack*, April 1, 2011, http://blogs.rsa.com/rivner/anatomy-of-an-attack

35 חולשות ZeroDate הן פרצות אבטחה בתוכנות המזוהות ומפורסמות ברבים. עם הפרסום ניתן בדרך־כלל מענה על־ידי המפתח טלאי תיקון המופץ ברבים. בדרך־ כלל עובר זמן בין הפצת טלאי התיקון עד להתקנתו במחשבי המשתמשים. חלון ההזדמנויות לתוקף הנו הזמן שבין פרסום החולשה לבין הזמן שבו מותקן טלאי התיקון במחשב היעד. בזמן הזה יכול התקף להחדיר קוד מפגע דרך אותה פרצה.

36 סמוך לנובמבר 2010 חלק ממחשבי החברות המותקפות כבר התקשרו לרשתות השליטה של התוקפים.

37 אחת החברות שהותקפו תוך שימוש במידע שהושג בתקיפת RSA הייתה לוקהיד מרטין – ראו: Mathew J. Schwartz, “Lockheed Martin Suffers Massive Cyberattack”, *Information Week*, May 31, 2011, http://www.informationweek.com/news/government/security/229700151

38 בארגונים גדולים מותקנות בדרך־כלל מערכות המנטרות את התעבורה ברשת המחשבים כדי לאתר התנהגויות שאינן מקיימות את החוקים שהוגדרו מראש. למערכות האלה יש כמה שמות מקובלים כמו: SEIM – Security Event and Information Management או: NBA – Network Behavioral Analysis. בתוכנות האלה קיים מערך חוקים שמטרתו להתריע על פעילות לא מורשית או לא שגרתית ברשת וכן למנוע אותה.

39 Stephen Doherty et al. *The Sykipot Attacks,* December 14, 2011, http://www.symantec.com/connect/blogs/sykipot-attacks

40 Mathew J. Schwartz, “More Sykipot Malware Clues Point To China”, *Information Week,* April 17, 2012, http://www.alvandsolutions.com/index.php?option=com_content&view=article&id=457%3Amore-sykipot-malware-clues-point-to-china&Itemid=136

41 Mathew J. Schwartz, “More Sykipot Malware Clues Point To China”, *Information Week*, December 21, 2011, http://www.informationweek.com/news/security/attacks/232300940

42 Kerbs, October 2011.

43 Nicholas Hoover, “NSA Chief: China Behind RSA Attacks”, *Information Week*, March 27, 2012, http://www.informationweek.com/news/government/security/232700341

44 Internet Service Provider.

45 Stew Magnuson, “Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic”, *National Defense*, December 11, 2010 http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249

46 Gunter Ollmann, *Serial Variant Evasion Tactics Techniques Used to Automatically Bypass Antivirus Technologies*, Damballa, 2009, http://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics.pdf

47 המונח אינטרנט אזרחי מציין תשתיות תקשורת אינטרנט שבהן עושה שימוש הציבור הרחב ושאין להן הגנה מיוחדת.