# מלחמת הזומבים הראשונה

## ארה"ב הכריזה מלחמה כנגד אחד האיומים הגדולים ברשת: ה-botnets ויש לכך סיבה טובה. מאמר מיוחד של ד"ר גיל דוד

**מאת ד"ר גיל דוד**

איור: SHUTTERSTOCK

חודש אפריל השנה התקיימה ועידת אבטחה במדינת ווירג'יניה שבארה"ב. בוועידה השתתף גם נציג הבית הלבן לענייני סייבר (Cybersecurity), ושם הוא הודיע, לראשונה, שממשלת ארה"ב עוברת שלב במלחמתה כנגד אחד האיומים הקיברנטיים שמתרחבים באופן המהיר ביותר: botnets-ה.

למעשה, עד עתה לא נקטה ארה"ב צד פעיל במיוחד במאבק כנגד botnets-ה ומפעיליהם, ואולם לנוכח גילויים שנחשפו לאחרונה, לפיהם בכל חודש מודבקים ומצטרפים מעל 4 מיליון מחשבים לצבאות הוירטואלים של botnets-ה, הודיע נציג הבית הלבן כי ארה"ב מכריזה מלחמה כנגדם.

הבית הלבן הבין שאנו נמצאים בשלב קריטי במלחמה כנגד botnets-ה, ושאם נאחר את הרכבת אנו עלולים למצוא את עצמנו במלחמת הסייבר הבאה מתמודדים כנגד צבאות וירטואליים המורכבים מעשרות ואף ממאות מיליוני מחשבים.

אם בעבר נחשבו botnets-ה כנחלתם הבלעדית של הפושעים באינטרנט, אשר השתמשו בהם למטרות spam, גניבת זהויות, הונאה, גניבת מידע רגיש כגון סיסמאות ומספרי כרטיסי אשראי, הרי שכיום מבינים שבעתיד הלא רחוק יקחו ה-botnets חלק בהתקפות הקטלניות ביותר כנגד מדינות, מתקנים חיוניים, מוסדות פיננסים ועוד.

למשל, התקפה של מיליוני botnets כנגד אתרי הבורסה בארה"ב יכולה לשתק את מרכז הפעילות הכלכלית לחלוטין. ארוע כזה כבר קרה בעבר: בחודש אפריל 2007 החלה התקפת סייבר מתואמת כנגד אסטוניה. ההתקפה, המכונה בשם DDoS - Distributed Denial of Service, בה לקחו חלק מספר botnets גרמה להשבתה של המוסדות החיוניים במדינה – החל ממוסדות ממשלה, דרך מוסדות פיננסים ועד עיתונים ואתרי חדשות. מלחמת סייבר זו, שההערכות מדברות כי בוצעה ע"י רוסיה, סיפקה לנו טעימה קטנה לגבי הכח העצום של צבא botnets ולגבי היכולת להפנותו מ-cybercrime מסורתי ל-cyberwarfare עתידני.

### מהם botnets?

Botnet זה רשת מבוזרת של מחשבים הפרוסים ברחבי העולם, כאשר המחשבים ה"חברים" בה, ה-bots (המכונים גם זומבים), הם למעשה מחשבים של משתמשים תמימים שהודבקו בתוכנה זדונית כגון סוס טרויאני. אותה תוכנה גרמה להם להצטרף בחשאי, ללא ידיעת המשתמש החוקי של המחשב, לשורות רשת ה-bots ובכך להגדיל את ה-botnet. בעוד שהמשתמש החוקי של המחשב משתמש בו כהרגלו, הוא איננו מודע לכך שמחשבו גוייס לצבא הוירטואלי.

על אוסף ה-bots שנאספו ממקומות שונים בעולם שולט ה-bot herder, הגירסא הוירטואלית של רועה הצאן המסורתי. תפקיד ה-bot herder הוא לארגן את ה-bots ברשת שלו, להעביר להם פקודות לביצוע, לקבל מהם דיווחים מהשטח וכמובן גם להרחיב את ה-botnet ולגייס אליו חיילים וירטואלים חדשים.

לרשות ה-bot herder עומדות שיטות מגוונות לביצוע תקשורת עם ה-bots. למשל, ה-bot herder יכול ליצור מספר "ספינות אם", mother ships, שהן למעשה אתרי אינטרנט תמימים למראה המפוזרים במקומות שונים בעולם ובהם הוא משאיר את ההוראות ל-bots. אתרים אלה מכונים גם command & control servers שכן באמצעותם שולט ה-bot herder ב-botnet ודרכם הוא מעביר להם פקודות.

ה-bots (כלומר התוכנה הזדונית שמותקנת בהם) יודעים שבכל פרק זמן מסויים עליהם לגלוש בצורה אוטומטית לאחד מה-mother ships ולבדוק אם מחכות להם הוראות לביצוע, כגון לגנוב סיסמאות ממחשב המשתמש. הם גם יכולים לדווח לספינת האם על תוצאות הפעולות שהם ביצעו, להעלות אליה מידע שהם גנבו וכולי.

על מנת לפגוע בפעילות ה-botnet, יש להוציא מכלל פעולה את אחת מהחוליות שמרכיבות את צבא ה-botnet: ה-bots, ה-bot herder או האמצעי דרכו מעביר ה-bot herder את הפקודות ל-bots.

מכיוון ש-botnet מורכב מעשרות אלפי ועד עשרות מיליוני מחשבים תמימים, קשה מאוד לאתר את כולם ולהסיר מהם את התוכנה הזדונית, ובכך לחלץ אותם מה-botnet. מדובר במחשבים של משתמשים שכתובות האינטרנט שלהם משתנות כל הזמן ומיקומם מתחלף בכל עת ועל כן דרך זו לא ישימה בדרך כלל.

לעומת זאת, ה-bot herder הוא יחיד (או מורכב מקבוצה קטנה של מפעילים) ועל כן הוא מטרה נוחה יותר לאיתור.

אולם, ה-bot herders הינם שועלי אינטרנט וותיקים שמכירים שיטות רבות לשמור על האנונימיות שלהם ובכך למנוע את איתורם. הם נעים במהירות, מחליפים זהויות ומתחבאים במקומות האפלים ביותר באינטרנט.

על כן, הדרך שנראית הכי מבטיחה לפרק botnet הינה להוציא מכלל פעולה את ערוץ השליטה והבקרה של ה-bot herder דרכו הוא מתקשר עם ה-bots. למשל, במקרה של ספינות האם המוסוות באתרי אינטרנט, יש לנתק אותן מהאינטרנט כך שאף bot לא יוכל לגשת אליהן ואף bot herder לא יוכל לתקשר דרכן עם ה-bots שלו. אולם, גם משימה זו איננה פשוטה בכלל. ראשית, ספינות האם מפוזרות ברד"כ במדינות שונות אשר חלקן לא תשתפנה פעולה עם אותו גוף שמנסה להשבית את השרתים. שנית, ה-bot herders פיתחו שיטות מתוחכמות ביותר שמונעות את איתורן של ספינות האם.

לדוגמא, הם משתמשים ב-bots רנדומליים מתוך ה-botnet שיהוו מתווכים הין שאר ה-botnet לבין ספינות האם. כלומר, אף bot אינו ניגש ישירות אל ספינת האם אלא הוא ניגש ל-bot מתווך שמקשר בינו לבין ספינת האם. באופן הזה, כתובת האינטרנט האמיתית של ספינת האם מוסוית מאחורי כתובת האינטרנט של ה-bot המתווך ואף אחד לא יכול להגיע אל מיקומה האמיתי של ספינת האם. בנוסף, ה-bot herder דואגים להחליף בכל כמה דקות את ה-bots המתווכים ב-bots אחרים מתוך הרשת ובכך למעשה הופכים את ספינת האם למטרה הנעה במהירות מקצה אחד של העולם לקצהו השני בכל מספר דקות, דבר שהופך את איתורה של ספינת האם למשימה כמעט בלתי אפשרית. רשת כזאת מכונה fast flux network והיא יושמה בהצלחה במספר botnets בעבר שאחד המפורסמים שבהם כונה בשם Storm.

ההתמודדות אל מול ה-botnets הינה משימה קשה ומסובכת הדורשת משאבים רבים וכן שיתוף פעולה בין מדינות.

הדוגמא המרתקת הבאה תמחיש עד כמה מורכבת המשימה: בשנת 2009 הוקם ברוסיה botnet בשם BredoLab. בשיאו הכיל BredoLab צבא וירטואלי של כ-30 מיליון bots, עם קצב גיוס של 3 מיליון bots חדשים בכל חודש, והוא עסק בעיקר בפעילות החביבה על ה-bot herders, הפצת מיליארדי הודעות ספאם דרך האי-מייל בכל יום. הנתון היותר מעניין הינו שה-bot herder נהג להשכיר חלק מה-bots ברשת שלו לצד שלישי. כלומר, ה-bot herder פיקד על צבא של היילים וירטואלים שהורכב מחטיבות שונות אותן הוא שיווק כצבא וירטואלי להשכרה לכל דורש. ההערכות הן שה-bot herder הרוויח באופן הזה מאות אלפי דולרים בכל חודש והצבא השכיר שימש גורמים שונים למגוון מטרות כגון תקיפה של אתרי אינטרנט, הפצה של תוכנות זדוניות, ספאם ועוד.

ה-bot herder תיקשר עם ה-botnet דרך מערך של מעל 140 ספינות אם אשר הוסוו באתרי אינטרנט שהושכרו מספק אינטרנט הולנדי. בשנת 2010, כאשר גודל ה-botnet הגיע כבר למימדים מפחידים, פשט כח משימה מיוחד של משטרת הולנד על מתקני ספק האינטרנט ההולנדי והצליח לאתר את כל ספינות האם שעגנו שם, להשתלט עליהן ולנתק אותן מהאינטרנט.

בשלב זה נראה היה שדינו של BredoLab נחרץ שכן ערוץ השליטה של ה-bot herder הושמד. אולם למרות זאת ה-bot herder ניסה להשתמש במספר דרכים על מנת להחזיר את שליטתו ב-botnet אך כולן נכשלו. במהלך אחרון של ייאוש, ה-bot herder פתח במתקפה מבוזרת כנגד הספק ההולנדי שבה השתתפו מעל 200 אלף bots בהם הוא עדיין הצליח לשלוט. מספר ימים לאחר מכן נעצר בארמניה ה-bot herder הראשי של BredoLab, בחור בן 27 בשם Georgy Avanesov. בחודש מאי השנה נגזר דינו ל-4 שנים בכלא בעוון פשעי מחשב חמורים.

בכך, למעשה, תם סיפורו של ה-botnet מהמסוכנים ביותר שנראו עד כה ושל מפעילו הראשי אולם סיפורו לא נשלם.

קבוצה חדשה של bot herders השתלטה בצורה מתוחכמת ביותר על מה שנשאר מ-BredoLab, הקימה מערך חדש של ספינות אם ברוסיה ובקואחסטן ולמעשה החזירה לחיים לפחות חלק מה-botnet האימתני שככל הנראה נמצא בשימוש גם בימים אלה.

החשש הגדול של ממשלת ארה"ב, כפי שהתחוור מדבריו של נציג הבית הלבן, הינו מוצדק לחלוטין. מה שבעבר היה נחלתם של אירגוני מאפיה ופשיעה באינטרנט, הופך כעת לכלי רב עוצמה של טרוריסטים, ארגוני גרילה וגם מדינות.

גופים אלה ישתמשו ב-botnets לא למטרות ספאם או הונאות אלא למטרות לוחמה קיברנטית גרידא: תקיפה רבת עוצמה של מוסדות ממשלה, מוסדות פיננסים, גופי צבא ומודיעין ותשתיות קריטיות. לדוגמא, התקפות כנגד בנקים ובורסות עלולות להשבית את הפעילות הפיננסית במדינה, התקפות כנגד תשתיות תקשורת עלולות לפגוע קשות בשירותי הטלפון, הסלולאר והאינטרנט במדינה וההתקפות כנגד תשתיות תחבורה וחשמל עלולות לעצור את תנועת הרכבות ולהחשיך ערים שלמות.

כאשר צבא של עשרות מיליוני bots מכל קצוות האינטרנט פותח במלחמה חזיתית ומתואמת מראש כנגד כל תשתית המחוברת לאינטרנט, קשה מאוד להתמודד מולו.

אז איך בכל זאת ניתן להתכונן למלחמת הזומבים?

במלחמה כמו במלחמה, היצירתיות והחשיבה מחוץ לקופסא יכולה להפוך את הקערה על פיה ודווקא איום רציני כמו botnet יכול להוות יתרון משמעותי למדינה הנתקפת. למשל, על ידי השקעת משאבים טכנולוגיים ומודיעיניים ניתן לאתר צבאות של botnets ברחבי האינטרנט. לאחר איתורם ניתן ללמוד את דרכי הפעולה שלהם, להבין את דרכי התקשורת שלהם מול המפעיל, לנתח את התוכנה הזדונית שמפעילה אותם ולמצוא בה חולשות אותן ניתן לנצל. מכאן והלאה אפשר לנקוט בשיטות מעולם המודיעין. למשל, ניתן לשתול באופן מכוון bots כפולים ב-botnet. מפעיל ה-botnet יחשוב שהצבא שלו גדל אך למעשה הוא מכיל כעת מרגלים שיכולים לדווח על תנועת ה-botnet וכוונות המפעיל שלו. בנוסף, בעת איתור ספינות האם של התוקף, במקום לנסות להשמיד אותן ניתן לגייס אותן ללא ידיעת התוקף לצד של המגן. באופן זה, הצד המגן יוכל להעביר דרכן פקודות ל-botnet כרצונו. כאשר הצד המגן משיג שליטה ב-botnet ללא ידיעת המפעיל, הוא משיג יתרון עצום במערכה הקיברנטית. ביום פקודה, שבו מפעיל הצבא הוירטואלי יפתח במלחמת חורמה קיברנטית, יוכל הצד המגן להוציא לפועל את התחבולה שלו ולהפנות בחזרה את הצבא הוירטואלי שהופנה נגדו כנגד מפעיל את ה-botnet עצמו (המדינה התוקפת או ארגון הטרור) או פשוט לשלוח פקודה שתשמיד את הצבא הוירטואלי של התוקף.

ההבנה ששיטות אלה ואחרות יכולות מצד אחד לשפר את מערך ההגנה של המדינות אך מצד שני גם להעצים את כוחן במערכה הקיברנטית, תגרום להפניית משאבים חיוניים לצורך הוצאתן אל הפועל. ◉

ד"ר גיל דוד הוא הבעלים והמנכ"ל של חברת Brainstorm Private Consulting לייעוץ בעולם הסייבר והמודיעין. הוא משמש כפרופסור אורח באוניברסיטה באירופה ומשתף פעולה עם גופים ביטחוניים, מסחריים ואקדמיים בארץ ובעולם.
www.gostorm.net