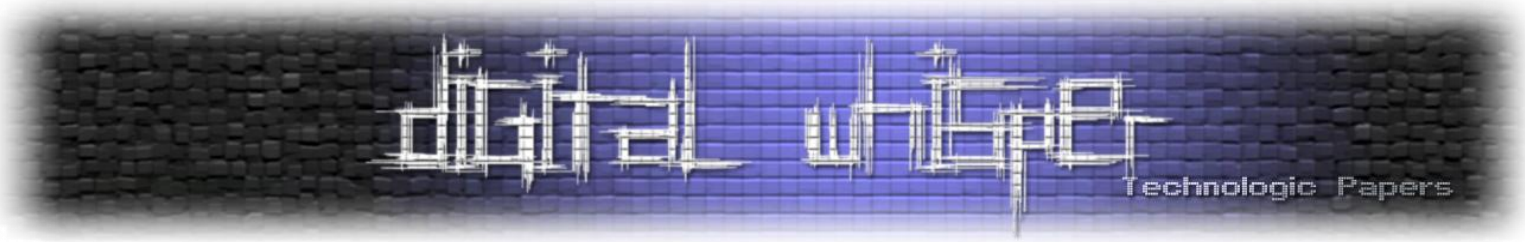


BotNet- מה זאת החיה הזאת?

מאת אפיק קסטיאל (cp77fk4r)

ביום שישי, 25 לאוגוסט שנת 2006, קיבל כריסטופר מקסוול, בחור בן 21, את גזר דינו בבית המשפט הפדרלי בסיאטל על ידי השופטת מרשה פצ'מן- למעלה משלוש שנות מאסר ולאחריהם עוד שלוש שנים של שחרור תחת פיקוח, בנוסף לפיצויים בסך 252,000$ שהוא נאלץ לשלם. מקסוול, בין השאר, היה אחראי על כתיבת והפצת תולעת Botnet שפעלה במשך למעלה משנתיים. בין שאר המחשבים שהצליחה תולעת זאת להדביק, נכללו גם למעלה מ-400 מחשבים של רשויות הבטחון של ארצות הברית.

המקרה של כריסטופר מקסוול הוא אחד מני מקרים רבים שבהם אנחנו שומעים על החיה הזאת, לאחרונה, אנו שומעים על מקרים אלו יותר ויותר (ויותר ויותר ויותר ויותר).

חוקרי אבטחת מידע ואינטרנט מעריכים כי קיימות עשרות (אם לא מאות) של רשתות כאלה והן רק גדלות ומתחזקות מיום ליום.

מה זה בכלל Botnet?

תוכנת Botnet היא שילוב מתבקש וקטלני במיוחד בין מספר תוכנות זדוניות בעלות אופי ותכונות שונות שהולחמו לתוכנה אחת. הרעיון הוא לקחת תכונות שונות של מזיקים שונים, לשלבן יחד וכך ליצור תוכנה זדונית אחת ש"נהנית" מתכונות אלו. לדוגמא:

- התכונה העיקרית של **תולעת** היא יכולת ההתרבות שלה, אם זה בעזרת מנגנוני Mass-Mailing (כמו ה-Mydoom) או ע"י הדבקה של קבצים (כמו ה-Melissa), אם זה ניצול חולשה באחד מרכיבי המערכת (כמו ה-SQL Slammer) או אם זה בעזרת שימוש ברשתות Peer to Peer (כמו ה-Tibick.f)
- התכונה העיקרית של **Rootkit** היא יכולת ההסוואה שלו, אם זה בעזרת התחפשות לכלי מערכת קיימים או השתלטות עליהם (כמו למשל ה-SHV4 או ה-SHV5), אם זה בעזרת הזרקת הקוד

שלו לתוך תהליך קיים (Vanquish), אם זה בעזרת ביצוע Hooking לפונקציות מערכת או אם זה בעזרת שינויי ערכים חשובים בתהליכי מערכת.

- התכונה העיקרית של **Trojan Horse** היא יכולת השליטה בו מרחוק, כמו למשל ה-Back Orifice שכתב Sir Dystic מ-Cult o the Dead Cow (cDc).

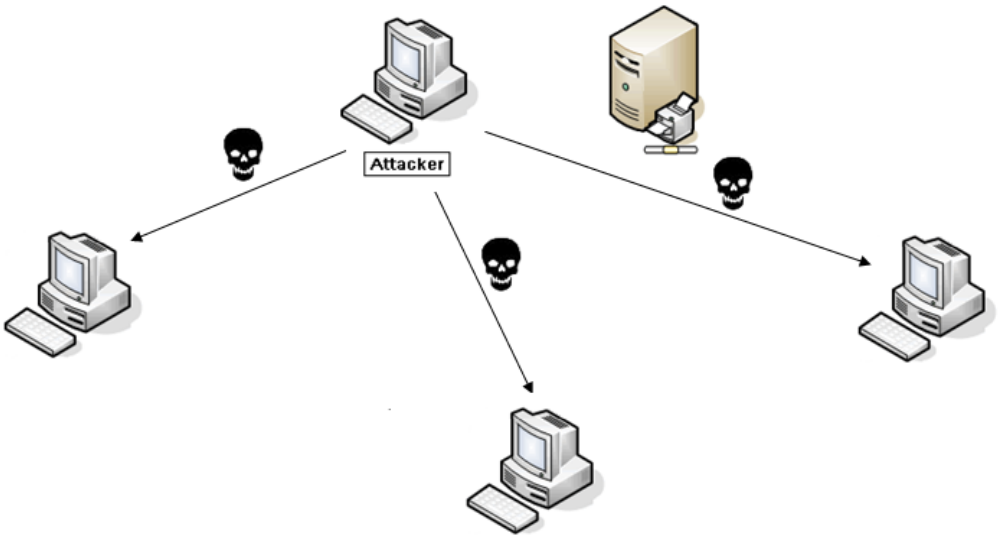
שילוב של שלושת מנגנונים אלה יוכלו ליצור תוכנה זדונית שגם תפיץ את עצמה כמו תולעת, בעזרת מנגנוני Mass-Mailing או ניצול חולשה במערכת ההפעלה, גם תסתיר את הפעולות שלה בעזרת מנגנונים המאופיינים בעיקר ל-Rootkits כך שהן יהיו כמעט שקופות, וגם תאפשר ליוצר שלה לשלוט על המחשב מרחוק.

אם כלי בעל יכולות כאלה או דומות נכתב בצורה נכונה, תוך פרק זמן קצר מאוד יהיו בידי היוצר שלו מספר רב מאוד של מחשבים הנמצאים בשליטתו ורק מחכים לקבל ממנו פקודות. מחשב אחד כזה נקרא "זומבי" (או Bot) וכלל המחשבים הנמצאים תחת רשת (Net) כזאת נחשבים "צבא", או פשוט- Botnet.

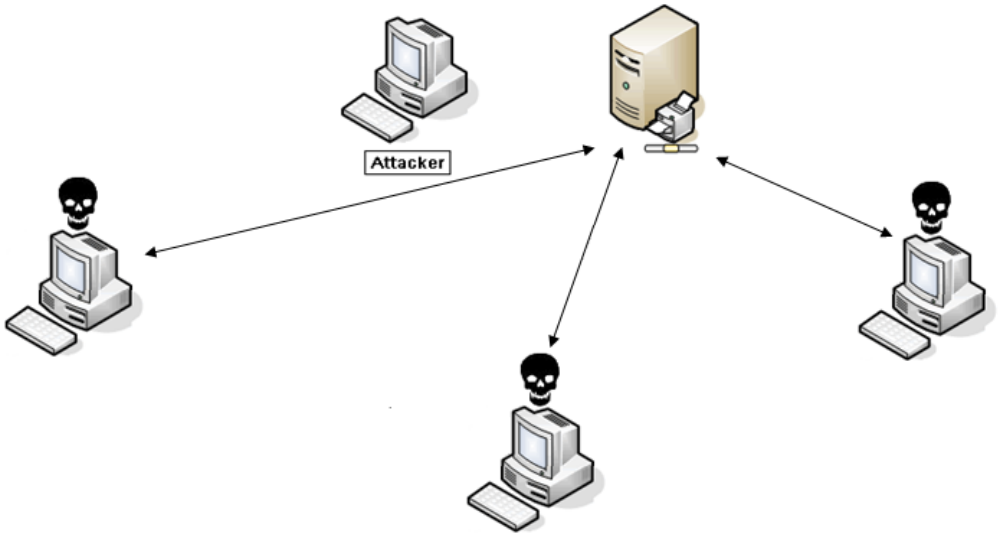
בשל הפוטנציאל הענקי שיש לכלי שכזה, לא מנהלים את צבא הזומבים בעזרת אפליקציה ממחשב יחיד, אלה בעזרת שרתי IRC או שרתי HTTP.

מעגל החיים של Botnet

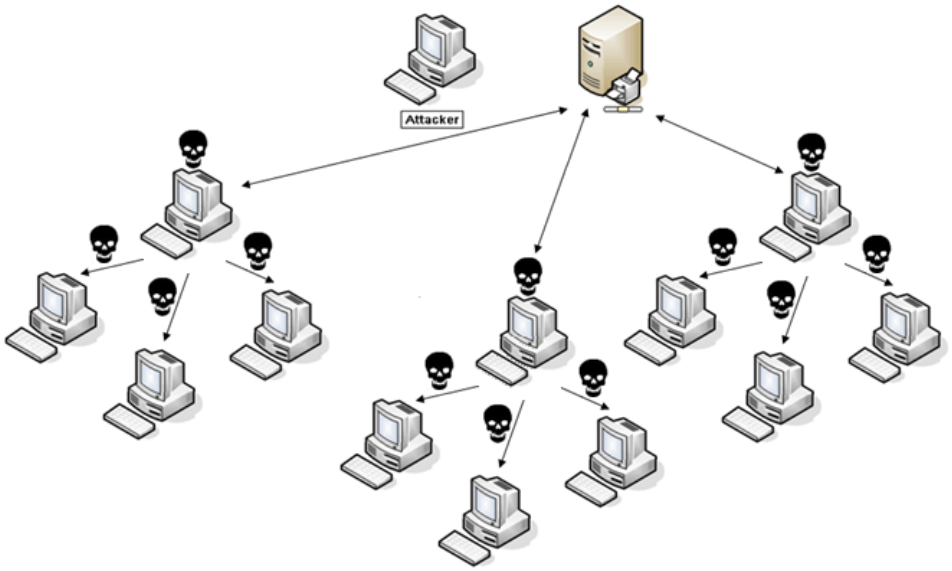
- **שלב ראשון-** התוקף מפיץ את ה-Botnet למספר קורבנות:



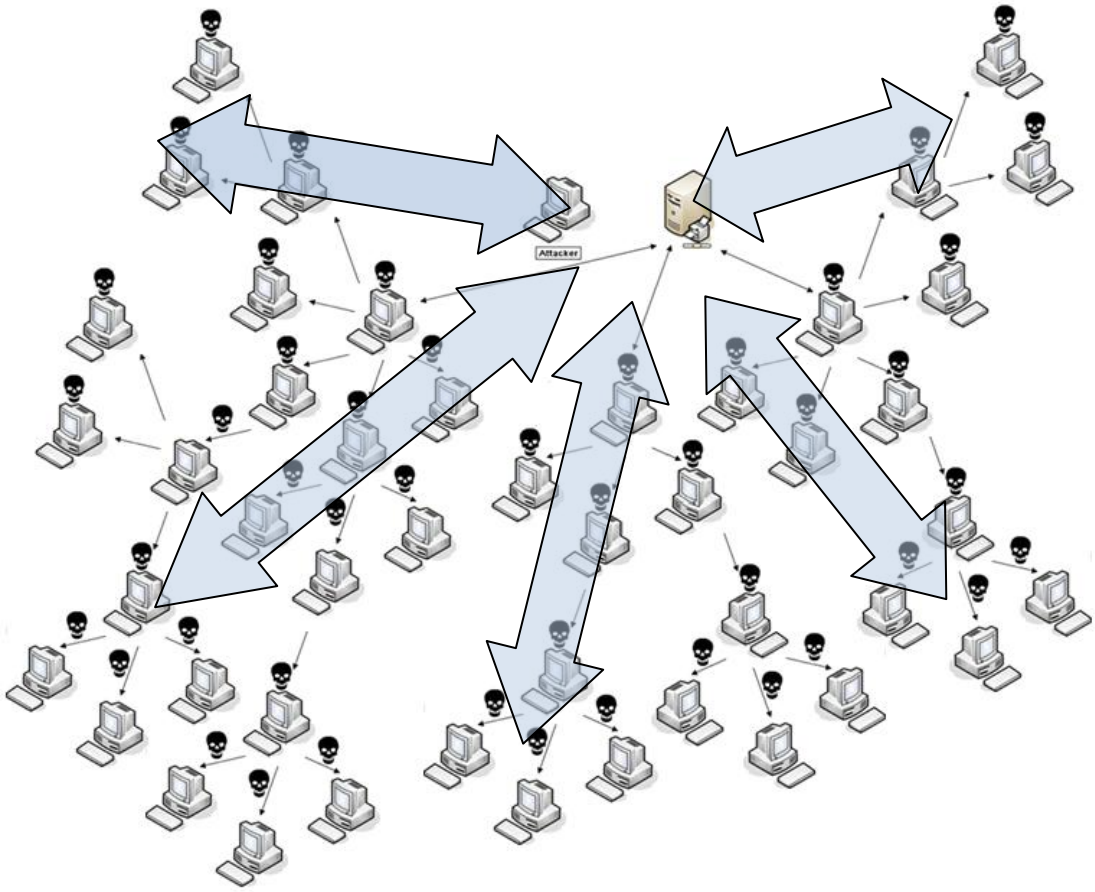
- **שלב שני-** ה-Botnet מדביק את הקורבנות, מחבר באופן שקוף את המחשבים לשרת ה-IRC (שרת ה-"Command & Control") ומחכה לפקודות מהתוקף:



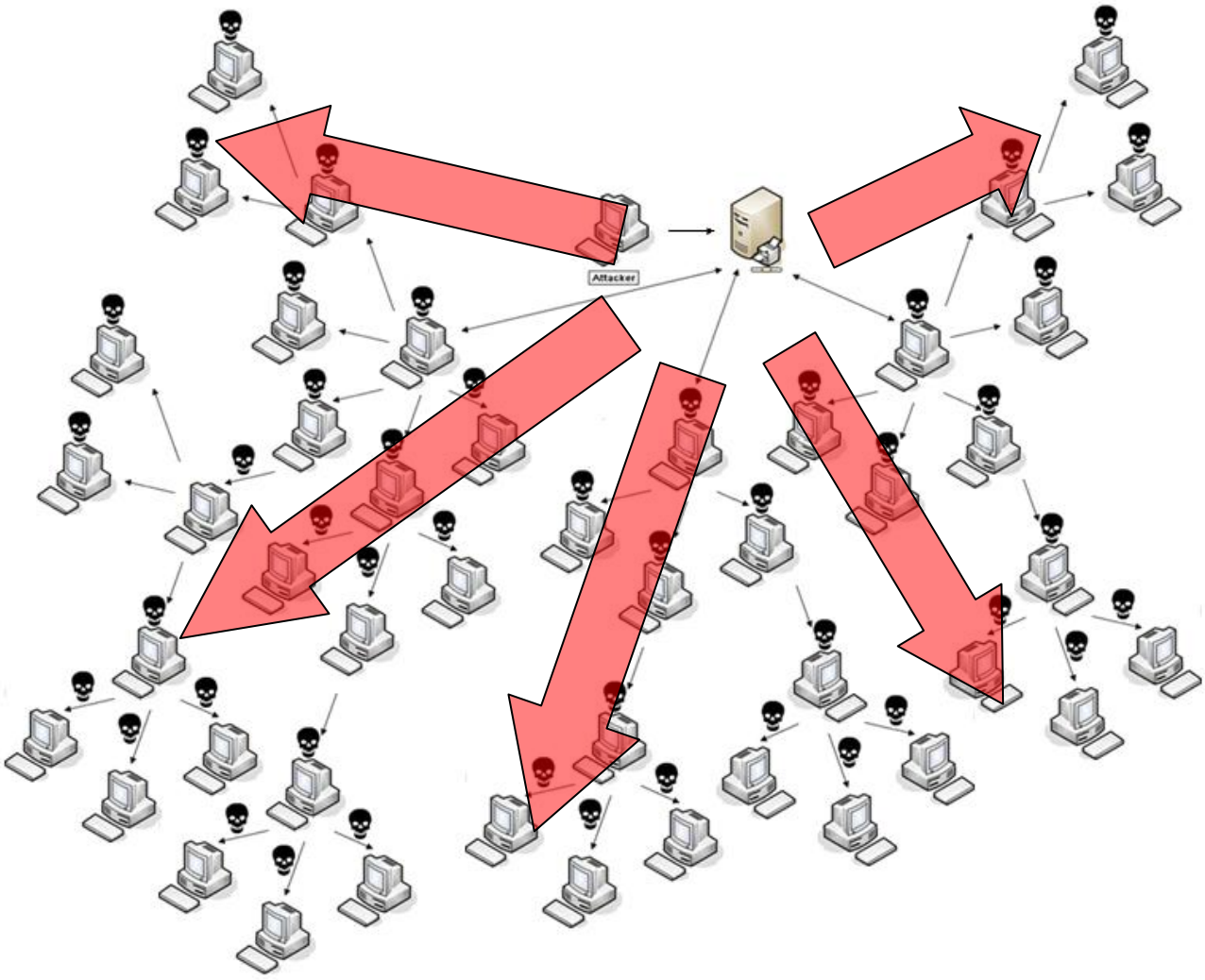
- **שלב שלישי-** במקביל להתחברות לשרת הבקרה של התוקף, מתחילים המחשבים הנגועים לסרוק את הרשת או לשלוח מיילים עם קוד זדוני במטרה להדביק עוד ועוד מחשבים:



- **שלב רביעי-** התחברות המחשבים הנגועים לשרת הבקרה של התוקף ונסיון הדבקה של מחשבים נוספים:



- **שלב חמישי –** לתוקף שליטה מלאה על כלל המחשבים ברשת ה-Botnet שלו. בכדי לשלוח פקודה, הוא מתחבר לשרת ה-Command & Control, משגר פקודה וכלל המחשבים מבצעים אותה. מה הוא יעשה בהם? זה תלוי מי ישלם יותר. האפשרויות שעומדות לרשותו רבות:
  - **ביצוע DDoS על מאסיבי אתרים ברשת**
  - **שימוש במחשבים להפצת ספאם**
  - **גניבת סיסמאות ופרטים אישיים של בעלי המחשבים**
  - **ניצול כח המיחשוב של הרשת ליישום Rainbow Cracking למפתחות RSA/MD/SHA וכו'**
  - **מכירת הרשת לאירגוני Cyber-Mafia (כמו למשל ה-RBN)**



כח עיבוד שכזה מאפשר לתוקפים לבצע התקפות על אתרים של חברות אנטי וירוס או אתרים שמספקים תמיכה וכלים להסרת ה-Botnet וכמובן - ככל שיעבור הזמן כך רק תגדל אותה הרשת ותהפוך חזקה יותר.

טכניקות בשימוש ה-Botnets

לא פשוט לצוד רשת כזאת, וקיימות מספר טכניקות בהן משתמשים כותבי ה-Botnets בכדי לעשות את התהליך קשה אף יותר.

שימוש ברשתות Fast-Flux

במידה ותצורת ההתקשרות של המחשבים הנגועים עם שרת ה-Command & Control הייתה ישירה, לא הייתה כל בעיה להאזין לתעבורה ולראות מאיפה המחשבים הנגועים מקבלים את הפקודות ואז להוריד את שרת השליטה. אך כותבי ה-Botnets משתמשים במנגנון DNS המכונה "Fast-Flux".

העקרון הוא שברשתות IP-Flux כתובת DNS אחת תחזיר בכל פעם את המידע מכתובת IP שונה המשוייכת כל פעם לשרת Proxy שונה המגשר בין המחשב הנתקף לבין שרת ה-Command & Control. בידי התוקפים נמצאים אלפי מחשבים כאלה המרכיבים את רשתות ה-Fast-Flux. קיימים מספר סוגי רשתות Fast-Flux. רשת Fast-Flux המבוססת על IP-Flux יכולה להיות ממומשת באופן של:

- Single-Flux
- Double-Flux

בנוסף קיים מנגנון בשם Domain-Flux, כאשר הרעיון הוא בדיוק הפוך מ-IP-Flux, במקום ש-DNS אחד יפנה למספר רב של כתובות IP, מדובר במספר רב של כתובות DNS שמפנות לכתובת IP אחת. מימוש אחד לדוגמא הוא השימוש ב-Domain Wildcarding, פשוט מאוד:

```
sdfasdsffds.digitalwhisper.co.il
vzcvvcas34.digitalwhisper.co.il
efasaa32ds.digitalwhisper.co.il
vs1caddbbs.digitalwhisper.co.il
xxf555fdg.digitalwhisper.co.il
```

כולם מפנים לאותה כתובת IP, אך כך שרת ה-Command & Control יכול לזהות פניה ספציפית. העניין דומה מאוד לרעיון שעומד מאחורי טכנולוגיות ה-Balancing המומשים באתרים בעלי תעבורה נרחבת.

ישנן רשתות המוסיפות עוד שכבת אנונימיות בעזרת שימוש במנגנון הנקרא "Blind-Proxy Redirection".
למידע נוסף אודות רשתות ה-Fast-Flux אפשר לקרוא בסדרת המאמרים KYE של Honeynet בנושא:

http://www.honeynet.org/papers/ff/

מנגנוני עדכונים

כותבי ה-Botnets מיישמים מנגנונים לעדכון וקטורי התקיפה של התולעים שלהם, ממש כמו שיצרנית תוכנה בשוק מיישמת מנגנון המאפשר לה לעדכן את התוכנות שאנו רוכשים (כדוגמאת LiveUpdate של Microsoft או מנגנוני עדכון החתימות של תוכנות האנטי-וירוסים למניהם).

נניח וכותב ה-Botnet יישם תולעת המפיצה את עצמה בעזרת ניצול החשיפה MS08-067, מה שצריך לעשות בכדי לעצור את התולעת מלהמשיך ולהפיץ את עצמה זה פשוט לעדכן את המערכת בעדכון הרלוונטי. בכדי להתגבר על מקרים כאלה, כותבי התולעים מיישמים מנגנוני עדכון שמאפשרות להן לעדכן את וקטורי התקיפה של התולעים ב-0day חדש, וכך, במידה ויצא עדכון לחשיפה שאותה הוא ניצל- הוא מעדכן את התולעת להמשיך לתקוף בעזרת וקטור חשיפה חדש, וכך להמשיך להפיץ את עצמה.

שיתוף פעולה בין רשתות Botnets

לטכניקה הזאת אין עדיין הוכחות ממשיות, אבל לאחרונה חוקרים סבורים כי אכן יש שימוש בטכניקה כזאת, כדוגמאת Kneber. מצד שני, חוקרים אחרים סוברים כי מדובר בעצם ב-Botnet המוכר Zbot/ZeuS.

הרעיון הוא שבמידה ותולעת אחת הצליחה לחדור לתוך מחשב, היא מורידה אליו ומדביקה אותו בתולעים אחרות, וכך גם הן עושות, הדבר מקשה מאוד על הסרתן ובמידה והצליחו להסיר את אחת התולעים - התולעים האחרות דואגות להוריד גירסא מחודשת שלה. טכניקה זו מגדילה בהרבה את יכולת ההשרדות של התולעת על המחשב בנוסף על כך גם מוכפלת מהירות ההתרבות שלה.

שימוש במנגנוני ניהול מתוחכמים

מנגנונים כאלה לא נצפו במספר רב של Botnets, אך דוגמא טובה אפשר למצוא ב-Botnet המכונה Storm. כיום, דרכי השליטה המוכרות ביותר ב-Botnets הן:

- **בעזרת פרוטוקול ה-HTTP:** מנהל הרשת מעדכן קובץ מוגדר מראש, והמחשבים הנגועים יודעים לבדוק כל פרק זמן קצר האם יש שינויים בקובץ.

- **בעזרת פרוטוקול ה-IRC:** המחשבים הנגועים מחוברים 24 שעות לשרת ה-IRC ומקבלים פקודות און ליין ממנהל הרשת.

בשני המקרים, נתוני ההתחברות לשרת רשומים Hard-Coded בתוך קוד התולעת. בעזרת ביצוע Sniffing למידע הנשלח מהתולעת או בעזרת Reverse Engineering חוקרי תולעים מסוגלים לשלוף את נתוני השרת, בין אם מדובר בסיסמא לערוץ ה-IRC שאליו מתחברים כלל התולעים, או אם מדובר ב-Credentials שדורש שרת ה-HTTP לזיהוי.

צורת הניהול של ה-Storm מתבצעת בעזרת רשתות Peer to Peer, באופן הבא:

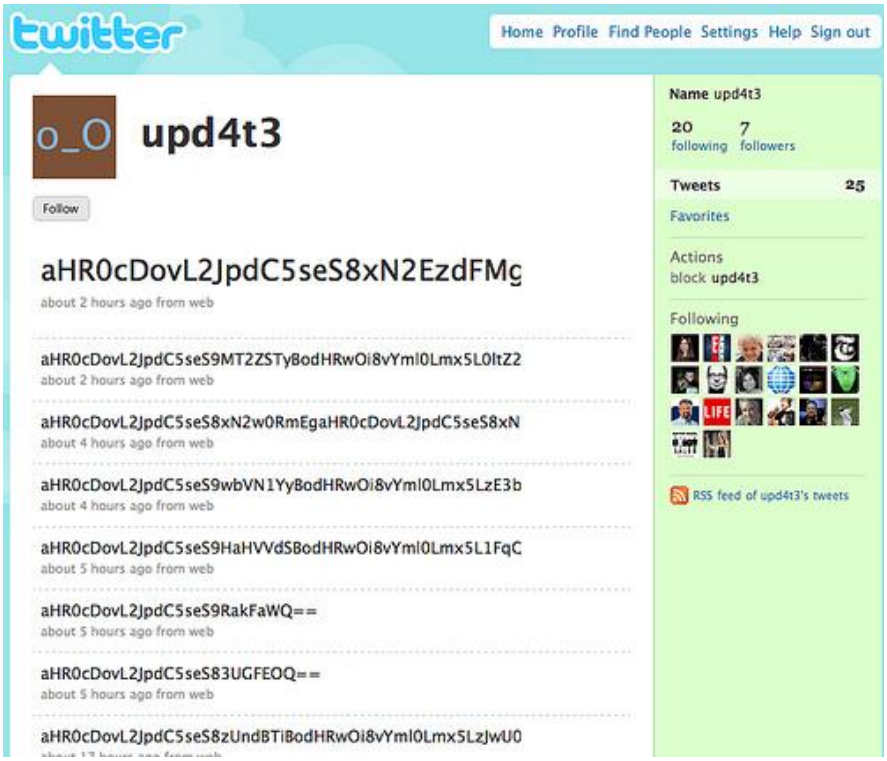
- מנהל הרשת מפרסם ברשת ה-p2p מחרוזת מסויימת שהוגדרה מראש ובנוסף- צמוד לאותה המחרוזת, מפרסם המנהל ערך מוצפן, לדוגמא:
  a@432&dAB=/a3sfaSFwFA5f35aFfW3462sAfASdefraUpO
- המחרוזת שאותה מפרסם מנהל הרשת הוגדרה קודם לכן (Hard-Coded) בתולעים, והן יודעות לחפש אותה (a@432&dAB=) באותה הרשת (לפעמים מדובר במספר מחרוזות שונות שעל התולעים לחפש וכל פעם מחרוזת אחת נמצאת בשימוש) ולשלוף ממנה את הערך המוצפן (a3sfaSFwFA5f35aFfW3462sAfASdefraUpO).
- בתוך התולעים מיושם מנגנון אשר יודע לפענח את המחרוזת ולקבל ממנה כתובת IP או מיקום של קובץ על שרת אינטרנט.
- מנהל הרשת העלה מבעוד מועד קבצים לאותו שרת המכילים פקודות/Payloads לתולעים.
- התולעים מפענחות את המחרוזת המוצפנת, ניגשות לכתובת ה-IP, מורידות את הקבצים ומבצעות את הפקודות שהשאיר מנהל הרשת.

מדובר במנגנון ניהול קצת פחות אמין, אך בצורה כזאת, מנהל הרשת מרוויח מספר דברים:

- **קושי חיזוי-** קשה לעקוב אחרי ניהול התולעת ומי שלא יודע מה הן המחרוזות שהתולעים מחפשות ברשתות השיתוף לא יוכל לדעת לאיזה שרת יש לפנות. גם אם הוא ביצע האזנה לתעבורת התולעת בעת התכתבותה עם השרת לאחר שפיענחה את המחרוזת המוצפנת, הוא יוכל לדעת רק באיזה שרתים מאוחסנות פקודות ישנות של התולעת, אבל לא שרתים עתידיים.
- **אנונימיות-** מנהל הרשת יכול לקבוע בכל פעם מחדש היכן לאחסן את הפקודות למתקפה הבאה וכן לקבוע כל פעם מהיכן לפרסם את המחרוזות הבאות ברשת שיתוף הקבצים – דבר המקשה באופן ניכר על זיהוי מיקום מנהל הרשת.

ה-Storm הייתה תולעת חכמה שחידשה מספר דברים בכל עולם ה-Botnets, אך פתאום, לקראת סוף שנת 2008, בלי שום סיבה נראת לעין- הפסיקה התולעת את הפעילות שלה. ספקולציות רבות צצו בנושא זה, חלק מהבלוגרים אמרו שחוקרי תולעים הצליחו להשתלט על הרשת ולשתק אותה, חלק אמרו שמדובר בפעילות של ה-FBI ויש אפילו שאמרו שיוצר התולעת פשוט מת.

תולעת נוספת שנצפתה עושה שימוש במנגנון ניהול מיוחד היא תולעת אנונימית שמנהל הרשת שלה ניהל אותה בעזרת חשבונות באתרי ה-Micro-blogging המוכרים Twitter, Tumblr ו-Jaiku.com. בשני האתרים נפתחו חשבונות משתמש תחת השם "upd4t3" ובעזרת "Status Massages" מקודדות שלח מנהל הרשת פקודות לתולעים שידעו להאזין לאותם החשבונות דרך שירותי RSS:



(במקור: http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/)

תולעת זאת התגלתה במקרה ע"י Jose Nazario. במקרה זה יוצר התולעת פחות הקפיד על שימוש במנגנוני הצפנה ורק קידד את המידע שהוכנס ל-"Status Massages" ב-Base64, כך שלא הייתה בעיה להתחקות אחר השרתים. לדוגמא, ה-"Status Massage" הבא:

```
aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYml0Lmx5L0ltZ2
```

תורגם ע"י התולעת (Base64):

```
http://bit.ly/LOfRO http://bit.ly/ImZ2
```

כתובות אלו יכולות להיות או מטרות לתקיפה, או עדכונים שעל התולעת להוריד וכו'. שיטה נוספת היא השיטה שנצפתה בגרסאות שונות של ה-ZeuS משתמשות לניהול ובקרה- שירותי ה-EC2 של Amazon.

שימוש בהצפנה, מנגנוני אימות ו-Obfuscation

במספר לא קטן של תולעים נצפה השימוש בהצפנת הפקודות והמידע בתקשורת הנתונים המשמשת את ה-Botnets, נצפה שימוש בחתימות דיגיטליות מבוססות אלגוריתמים מתקדמים כגון MD6, שימוש ב-PKE, יישום מנגנוני RSA בעלי מפתחות גבוהים ועוד. בנוסף, נצפה שימוש רב בשיטות Obfuscation שונות, בין אם מדובר בביצוע Code Obfuscation או בזיהוי נסיונות התחקות אחר התולעת ואז שינוי דפוס ההתנהגות שלה.

בגליון זה מפורסם מאמר על ה-Conficker שנכתב על ידי הרצל לוי ועל-ידי, בו פירטנו באופן מובן ומפורט יותר את השימוש בשיטות אלו הנמצאות בגרסאות השונות של ה-Conficker.

היקף הנזק

קשה מאוד לאמוד את כמות הנזק הנגרמת מרשתות ה-Botnets, גם מפני גודל רשת האינטרנט, גם מפני שחברות וגופים אשר נפגעו מהן לא ממהרות לפרט כמה נזק נגרם להם (פגיעה בתדמית) ומעדיפות לנסות להתמודד עם התופעה לבד, וגם מפני שקשה מאוד לצפות מה יהיה הצעד הבא של מנהלי הרשתות הללו. בעזרת כח מיחשוב עצום שכזה ניתן לבצע כמעט כל דבר וכשגופים כגון ה- Russian Business Network שולחים יד ומקדמים תופעות דומות, כסף לא חסר והכיוון הוא רע מאוד. אם בעבר היקף נזק של תולעי האינטרנט הראשונות הגיעה ל-6000 מחשבים (תולעת ה- Morris) וזה היה נחשב לנזק רציני ביותר, הרי שהיום מדובר בבדיחה.

עד לפני כמעט שנתיים, תולעת ה-SQL Slammer עמדה בראש רשימת התולעים שהדביקו את הכמות המירבית של המחשבים (שרתי MS SQL) – המספר כמעט בלתי נתפס, מדובר ב-75,000 מחשבים בפחות מעשר דקות! יש עדויות לכך שהתולעת אף **גרמה להאטה בקצב רשת האינטרנט העולמית**.

ככל שעובר הזמן כך מתפתחות טכנולוגיות חדשות ולא רק בשוק התוכנה ה-"רגיל", אלא גם בעולם הוירוסים. בתחילת שנת 2009, היקף ההדבקה של ה-Conficker עמד על כמעט 9 מיליון מחשבים! קשה להבין איזה כח עיבוד יש בכזאת כמות של מחשבים וקשה עוד יותר לחשב את כמות הנזק שיכולה להגרם ממנו, שלא נדבר על כמות המידע הרגיש שמאוחסן על מחשבים אלו.

סיכום

אם בעבר שמענו על סיפורים כמו הסיפור של GRC.Com, כיום אנחנו שומעים על מקרים כאלה בתדירות יומיומית. במידה ותתרחש Cyber-Attack רצינית, רשתות ה-Botnets יהיו לכלי הנשק המרכזי והמשפיע ביותר במלחמה זו. חשוב להיות מעודכנים תמיד ובמידה והתגלו פרצות באפליקציות כמו דפדפנים או יישומי אינטרנט אחרים - יש עדיפות עליונה לא להשתמש בהן עד שלא יפתרו בעיות אלו. כמו במקרה של תולעת ה-Conficker, חברת Microsoft שיחררה טלאי אבטחה לכשל שאותו ניצלה התולעת מספר חודשים לפני שהתולעת שוחררה. במקרים אחרים אין יותר מדי מה לעשות, כמו במקרה של Operation Aurora- שחברת Microsoft ידעה על כשל האבטחה כמעט ארבעה חודשים לפני המתקפה ולא שחררה שום טלאי.